Ira Närhinen

EU:N YLEISEN TIETOSUOJA-ASETUKSEN KÄYTTÖÖNOTON TUKEMISEN KEINOJA PIENYRITYKSESSÄ

(CASE ICT-PALVELUNTUOTTAJA JÄRVI-SUOMEN KIINTEISTÖKONSULTIT OY)

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Närhinen, Ira
EU:n yleisen tietosuoja-asetuksen käyttöönoton tukemisen keinoja pienyrityksessä (case ICT-palveluntuottaja Järvi-Suomen Kiinteistökonsultit Oy)
Jyväskylä: Jyväskylän yliopisto, 2022, 86 s.
Tietojärjestelmätiede, Pro gradu -tutkielma
Ohjaaja: Pulkkinen, Mirja

Euroopan unionin yleinen tietosuoja-asetus (GDPR) tuli voimaan 25.5.2018, josta lähtien sitä on pitänyt noudattaa kaikissa niissä organisaatioissa yli EU-alueen rajojen, jotka käsittelevät EU-kansalaisten henkilötietoja. Praktisen tason tarkastelunäkökulma kohdentuu erityisesti siihen, miten ja millä työkaluilla pk-yrityksen tiedon hallinnan ekosysteemissä voidaan tukea GDPR-asetuksen käyttöönottoa. Monimenetelmäinen tutkimusprosessi, jossa hyödynnettiin sekä tutkijan että tapausorganisaation asiantuntijuutta, mahdollisti toimivan ratkaisun kehittämisen todellisessa tilanteessa toimeksiantajan Järvi-Suomen Kiinteistökonsultit Oy:n tarpeisiin. Tutkimus toteutettiin suunnittelutieteen periaatteita noudattaen. Tietoa, informaatiota ja aineistoja kerättiin kirjallisuuskatsauksen lisäksi haastattelemalla ja havainnoimalla, ja empiirinen tutkimus toteutettiin tapausorganisaation tiedon hallinnan ekosysteemissä DSRM-prosessin avulla. Raportissa esitellään kehittelemäni mentaalitason ratkaisumalli, joka on sellaisenaan hyödynnettävissä pk-yrityksissä tietosuoja-asetusta käyttöönotettaessa. Ratkaisukokonaisuuden sisältämien useiden artefaktien avulla voidaan selvittää ja tarvittaessa muuttaa henkilötietojen käsittelyn käytäntöjä, prosesseja asetuksen vaatimustenmukaisiksi. Tutkimus ja sen tulokset sekä tutkimusprosessin myötä esiin nostetut tai kehitellyt artefaktit ovat hyödynnettävissä myös muissa pk-yrityksissä. Lisäksi raportissa esitellyt asiat auttavat meitä yksilötasolla kiinnittämään paremmin huomiota ja lisäämään tietosuutta henkilötietojemme käsittelyyn, niiden suojaamiseen ja oikeuksiin.

Asiasanat: EU:n yleinen tietosuoja-asetus, GDPR, tiedon hallinta, tietosuoja-asetuksen käyttöönotto, DSRM-prosessi

ABSTRACT

Närhinen, Ira
Ways to support implementation of the European Union's General Data Protection Regulation in a small business (case ICT service provider Järvi-Suomen Kiinteistökonsultit Oy)
Jyväskylä: University of Jyväskylä, 2022, 86 pp.
Information Systems, Master's Thesis
Supervisor: Pulkkinen, Mirja

The European Union's General Data Protection Regulation (GDPR) entered into force on 25 May 2018. Since then, it has been complied with by all organizations that process the personal data of EU citizens. In this study practical perspective focuses in particular on how and with tools an introduction of the GDPR can be supported in an information governance ecosystem of SME. The multi-method research process, which utilized the expertise of both the researcher and the case organization, enabled development of a workable solution to the needs of the client Järvi-Suomen Kiinteistökonsultit Oy in a real-world situation. The research was carried out in accordance with the principles of design science. In addition to the literature review, data, information, and materials were collected through interviews and observations. The empirical research was conducted by using the DSRM process. The report presents the mental model I have developed that can be used to implement GDPR in an SME. With the help of a solution package that contains several artefacts, it is possible to find out and, if necessary, change the practices and processes of processing personal data to comply with the requirements of the regulation. The research and its results, as well as the artifacts highlighted or developed during the research process, can also be utilized in other SMEs. In addition, the issues raised in the report help us to pay attention to the processing, protection and rights of our personal data at an individual level.

Keywords: General Data Protection Regulation, GDPR, information governance, implementation of GDPR, DSRM-process

TERMILUETTELO

Anonymisointi	Henkilötiedon tekeminen tunnistamattomaksi siten, ettei tietoa voi yhdistää tiettyyn rekisteröityyn.
Artikla	Euroopan Unionin yleisen tietosuoja-asetuksen yksittäinen pykälä.
eDiscovery	Sähköisesti tallennettujen tietojen (esim. sähköpostit, esitykset, tietokannat) määrittämistä, keräämistä ja toimittamista. Tietoja voidaan mm. käyttää todisteena oikeustapauksissa.
Euroopan komissio	Euroopan Unionin toimeenpaneva elin, joka edistää EU:n yleistä etua.
Euroopan unioni (EU)	Euroopan unioni on liitto, johon kuuluvat siihen liittyneet Euroopan maat. Jäsenmaita on 28. (Tilanne 08/2018.)
GDPR	Euroopan Unionin yleinen tietosuoja-asetus (General Data Protection Regulation)
WP 29	EU:n tietosuojaviranomaisista koostuva työryhmä, joka on julkaissut ohjeita GDPR-asetuksen soveltamisesta.
Henkilötietojen käsittelijä	Käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta dokumentoituihin ohjeisiin pohjautuen. Käsittelijä voi olla myös organisaation ulkopuolinen osapuoli, ja sillä on vastuu itses-

	sään myös varmistua, että toiminta vastaa EU:n lainsäädännön ohjeita.
Henkilötieto	Henkilötieto kuvaa luonnollista henkilöä, hänen ominaisuuksiaan tai elinolosuhteitaan. Henkilötietomerkinnästä voi tunnistaa hänet, hänen perheensä tai yhteisessä taloudessa eläviä. Myös erilliset tiedot, jotka yhdistettyinä toisiinsa mahdollistavat henkilön tunnistamisen, ovat henkilötietoja.
Henkilötietojen käsittelijä	Käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta dokumentoituihin ohjeisiin pohjautuen. Käsittelijä voi olla myös organisaation ulkopuolinen osapuoli, ja sillä on vastuu itsessään myös varmistua, että toiminta vastaa EU:n lainsäädännön ohjeita.
Henkilötietojen käyttäjä	Henkilörekisteriin talletettujen tai kerättävien henkilötietojen käyttäjä rekisterinpitäjän toiminnassa.
Identifioida	Tunnistaa.
Rakenteeton tieto	Rakenteeton tieto on organisaation keräämää tietoa, joka jää käyttämättä sekä analysoimatta, ja tiedolla ei ole selkeää omistajaa
Rekisterin pitäjä	Rekisterinpitäjä, jonka käyttöä varten rekisteri perustetaan, ja joka voi olla esimerkiksi luonnollinen henkilö, yhteisö, virasto tai säätiö, on ensisijaisesti vastuussa henkilötietojen käsittelystä ja määrittelee käsittelyn tarkoitukset.

Rekisteröity	Luonnollinen henkilö, jota henkilötieto koskee.
SaaS (Software as a Service)	SaaS-palvelulla tarkoitetaan pilvessä sijaitsevaa ohjelmistoa, jota ylläpidetään palveluntarjoajan toimesta.
syntaksi	Määrittää kielioppisäännöt.

KUVIOT

SISÄLLYS

1 JOHDANTO

Tämän tutkimuksen motivaattorina toimi Järvi-Suomen Kiinteistökonsultit Oy:n (JSK Oy) käytännönläheinen ongelma. Yrityksen tuli monien muiden organisaatioiden tavoin alkaa soveltaa viimeistään 25.5.2018 mennessä henkilötietojen käsittelyä sääntelevää EU:n yleistä tietosuoja-asetusta (GDPR). Haaste muodostui siitä, ettei kertomansa mukaan pienyritys JSK Oy:llä ollut ymmärrystä, miten implementointityö polkaistaisiin käyntiin, eikä myöskään käsitystä mitä muutoksia asetuksen käyttöönottaminen aiheuttaa henkilötietojen käsittelyyn. Tämän vuoksi yritys kääntyi puoleeni ja pyysi auttamaan asetuksen käyttöönotossa. Aihealue on varsin kiinnostava tutkielman kirjoittajasta jo yksilönkin tietoturvan sekä oikeuksien näkökulmasta tarkasteltuna, joten tartuin innolla selvitystyöhaasteeseen ”Miten EU-yleisen tietosuoja-asetuksen käyttöönottoa voidaan tukea pienyrityksessä?”.

Luvussa 2 kerrotaan tutkimusmenetelmistä, joita hyödynnetään tutkimusongelmaa ratkaistaessa. Seuraavassa luvussa 3 pureudutaan kirjallisuuskatsauksen avulla tutkimuksen pääkäsitteisiin, jotka ovat tiedon hallinta ja GDPR-asetus. Neljännessä luvussa esitellään teoreettis-käsitteellisen osion yhteenveto ja mentaalitason rakennelma, joka toimii ratkaisumallina suunnittelutieteen periaattein toteutettavassa tutkimuksessa sekä käytännön tutkimustyössä. Luvussa 5 selostetaan DSRM-prosessin vaiheiden kautta, miten ja millä työkaluilla GDPR-asetus otettiin käyttöön tapausorganisaatiossa kevään 2018 aikana.

1.1 Aikaisempi tutkimus

EU:n yleinen tietosuoja-asetus on yksi ajankohtainen esimerkki lainsäädännöllisestä viitekehyksestä tiedon hallinnan laajassa abstraktiossa, joka saattaa saada organisaatiot kiirehtimään tiedon hallinnan (IG) kehittämisen toimia sekä nostamaan IG:n strategisen merkityksen eturintamaan (Schoch, 2016). Termi tiedon hallinta (engl. information governance) on esitelty

tiedemaailmalle vasta vajaat kaksikymmentä vuotta sitten (Kooper, Maes & Lindgreen, 2011). Tutkittavana ilmiönä se on siten varsin nuori, vaikka rakenteet ja aktiviteetit sen ympärillä ovat olleet jo pitkään olemassa (Blair, 2011; Smallwood, 2014).

Tietosuoja-asetuksen käyttöönotto on osoittautunut monista syistä haasteelliseksi pienyrityksissä. Erään tutkimuksen johtopäätösten mukaan pk-yritykset, joiden olennainen osa toimintaa on tietoturvallisuus, pitävät yleisellä tasolla GDPR:n noudattamista järkevänä sekä toteutettavissa olevana. Sen sijaan pk-yritykset, jotka keskittyvät vähemmän tietosuojaan, kamppailevat saadakseen mielestään tyydyttävän tuloksen asetuksen sääntöjen noudattamisessa. Suurimmaksi ongelmaksi koettiin asetuksen laajuus ja kysymykset siitä, kuinka asetus pannaan täytäntöön. Lisäksi koettiin haasteelliseksi kartoittaa yritysten monimutkaisten tietoverkkojen kokonaisuus. (Sirur, Nurse & Webb, 2018.) On väitetty, että GDPR-asetuksen noudattaminen saattaa estää pk-yritysten kehittymistä ja kilpailuetua, koska niiden käytettävissä olevat resurssit asetuksen käyttöönottamisessa sekä sen täytäntöönpanossa ovat pienemmät kuin kokoluokaltaan suuremmissa yrityksissä. Erityisesti on tarkasteltu aloja, joilla pilviteknologia on auttanut pk-yrityksiä kilpailemaan suurempia globaaleja toimijoita vastaan. (Wilkinson, 2018.)

iWelcomen julkaiseman helmikuun 2018 raportin mukaan GDPR-asetuksen vaatimustenmukaisuutta arvioitaessa tiettyihin asetuksen (artiklat 5.1 e, 6,7, 15, 16,17 ja 25) artikloihin 76,4 prosenttia 89:stä organisaatiosta ei pystynyt toimimaan asetuksen vaatimusten mukaisesti. Tutkimukseen osallistuneet maat ovat: Alankomaat, Britannia, Saksa, Ranska, Sveitsi, Espanja ja Ruotsi. (Stultjens, 2018.) Eräässä akateemisessa konferenssijulkaisussa on tunnistettu ja analysoitu tutkimustriangulaation avulla valmiuksia GDPR-asetuksen vaatimustenmukaiseen toimintaan. Kuuden tutkimuksen triangulaatio osoitti vain pienen osan yrityksistä olevan täysin valmistautunut asetuksen vaatimusten mukaiseen henkilötietojen käsittelyyn. Yksi merkittävimmistä syistä osoittautui olevan asetuksen tulkinnan vaikeus ja sen täytäntöönpano. Ei ollut riittävästi tietoutta eikä käsitystä tarvittavista toimenpiteistä. Toiseksi organisaatiot eivät tietosuoja-asetuksen käyttöönoton siirtymäaikana olleet osoittaneet riittävästi resursseja, kuten aikaa tai kouluttaneet henkilöstöään, GDPR-asetuksen käyttöönottoon ja sen soveltamiseen. (Fair & Januska, 2018.)

Organisaatioiden on itse määriteltävä ratkaisut tietosuoja-asetuksen käyttöönottamiseksi, koska se itsessään ei anna täytäntöönpano-ohjeita (Fair & Januska, 2018; Lievens & Verdoodt, 2018; Tikkinen-Piri, Rohunen & Markkula, 2018). Tietosuoja-asetuksen sanamuotojen on koettu jättävän liian paljon tulkinnan varaa (De Hert, Papakonstantinou, Malgieri, Beslay & Sanchez, 2018; Wachter, 2018). Tämä saattaa herättää epävarmuutta ja voi johtaa sekä ristiriitatilanteisiin että laajoihin epäselvyyksiin GDPR-asetusta käyttöönotettaessa ja sen velvoitteiden mukaisessa toiminnassa (Tsormpatzoudi, Berendt, Coudert, 2016; Bihari, 2018; Kindt, 2018).

1.2 Tutkimuksen tavoitteet ja tutkimusongelma

Aiempaan tutkimukseen perehtymisen kautta kävi ilmi, että EU:n yleisen tietosuoja-asetuksen käyttöönotto on koettu haasteelliseksi. Tietosuoja-asetukseen liittyviä asioita, merkityksiä, tulkintoja ja soveltamisen haasteita on puntaroitu tutkimuksissa poikkitieteellisesti sekä käsitelty myös eri viranomaistahoilla. Sen soveltamisen tueksi on julkaistuja oppaita (Talus, Autio, Hänninen, Pihamaa & Kantonen, 2017) ja työkaluja, jotka keskittyvät asetuksen tiettyyn osa-alueeseen, esimerkiksi rekisteröityjen oikeuksien toteutumiseen (Valtiovarainministeriö, 2016) tai asetuksen mukaisen riskiarvion (Gellert, 2018) tekemiseen. Kirjallisuudessa muun muassa tähdennetään, että henkilötietojen sijainnit tietojärjestelmistä ja -verkoista tulee selvittää, mutta työkaluehdotuksia tai -suosituksia henkilötietojen esiin kaivelemisen tueksi tai niihin ei näyttäisi olevan sisällytetty.

Tämän tutkimuksen tavoitteena tuottaa ratkaisu, jonka avulla voidaan tukea GDPR-asetuksen käyttöönottoa pienyrityksessä. Toisena tavoitteena on tuotetun etenemispolun avulla käyttöönottaa tietosuoja-asetus tapausorganisaatio JSK Oy:ssä. Tutkimuksen tavoitteena on ratkaista reaalimaailman ongelma seuraavanlaisella kysymyksenasettelulla:

Miten EU:n yleisen tietosuoja-asetuksen käyttöönottoa voidaan tukea pienyrityksessä?

EU:n yleinen tietosuoja-asetus on yksi lakisääteinen esimerkki, joka on patistanut organisaatioita kiinnittämään entistä enemmän huomiota tiedon hallinnan ilmiöön (Schoch, 2016). Näin ollen tutkimuksen pääongelman analyysissä päädyttiin kahteen osaongelmaan:

Mikä on tiedon hallinnan merkitys organisaatiossa, ja mistä se koostuu?

Mitkä seikat saattavat hankaloittaa GDPR-asetuksen käyttöönottoa?

Tässä pro gradu -tutkielmassa ei oteta kantaa muihin olemassa oleviin lakeihin, säädöksiin tai asetuksiin, joilla on vaikutusta henkilötietojen käsittelyyn, hallintaan tai muunlaiseen operointiin liittyen. Tällaisia kansallisia lakeja ovat esimerkiksi kansallinen tietosuojalaki ja tiedonhallintalaki, joista jälkimmäinen koskee julkista hallintoa. Tutkimuksessa tarkastellaan GDPR-asetuksen käyttöönottamista pk-yrityksen lähtökohdista, jollaista tapausorganisaatio edustaa. Päätutkimusongelman ratkaisemisessa ei hyödynnetä markkinoilla olevia kaupallisia työkaluja tai muita vastaavia GDPR-asetuksen käyttöönottoa tukevia systeemejä. Tutkielmassa on tavoitteena selostaa GDPR-asetuksen käyttöönoton eteneminen tapausorganisaatiossa DSRM-prosessin vaiheiden avulla, mutta täydellisen yksityiskohtaista raportointia ei ole tarkoituksenmukaista antaa, koska organisaatiot ja niiden ekosysteemit ovat uniikkeja.

1.3 Tutkimuksen tulokset

Tässä tutkimuksessa tuotettiin SaaS-palvelutuottaja Järvi-Suomen Kiinteistökonsultit Oy:n ekosysteemin ratkaisu, jonka avulla GDPR-asetus otettiin käyttöön toimeksiantajan tiedon hallinnan ympäristössä kevään 2018 aikana. Tiedon, informaation ja tietämyksen konstruktion lisäksi iteratiivisen tutkimusprosessin myötä löydetyt jo valmiit, että luodut artefaktit toimivat käytännön työkaluina GDPR-asetuksen käyttöönotossa ja jatkossa myös sen soveltamisessa. Havainnot ja löydökset auttoivat sekä hallinnollisella että operatiivisella tasolla, kun yrityksessä tehtiin muutoksia henkilötietojen käsittelyn prosesseihin, tapoihin sekä toimiin. Lisäksi työ tuotti syötteitä tietosuojavaatimusten sisällyttämistä osaksi kehitysyhteistyötä toimeksiantajan yhteistyökumppaninTarmo-ohjelmistokehittäjien kanssa. Sinällään tiedon hallinta ei ollut uusi asia ilmiönä tapausorganisaatiossa, mutta teoriaan ja käytäntöön pohjautuva kehittelemäni ratkaisumalli auttoi GDPR-asetuksen käyttöönoton lisäksi jäsentämään tiedon hallinnan teoreettisen viitekehyksen tukipilarien ja toiminnan osa-alueiden täytäntöönpanoa tosielämän kontekstissa.

Työn toimeksiantajan antaman kirjallisen lausunnon mukaan iteratiivinen prosessi ja menetelmä tuottivat yrityksen käyttöön uutta informaatiota ja tietoa sekä syvälle luotaavaa ymmärrystä. Tämä auttoi ensinnäkin hahmottamaan paremmin yrityksen toimintaympäristöä. Ratkaisu auttoi yritystä sopeuttamaan toimintansa tietosuoja-asetuksen vaatimustenmukaiseksi. Kerrytetyn ymmärryksen myötä saatiin perusteet yrityksen tekemien päätösten tueksi ja tietosuoja-asetuksen käyttöönottamiseksi. Prosessi auttoi JSK Oy:tä tuottamaan GDPR-asetuksen vaatimustenmukaisia tietosuoja-asiakirjoja ja dokumentteja sekä päivittämään liiketoimintasopimukset. Lisäksi saavutetun tietämyksen myötä JSK Oy pystyi konsultoimaan omia asiakkaitaan GDPR-asetuksen soveltamisen kiemuroissa.

Haasteet GDPR-asetuksen implementoimiseksi ovat laajalti samankaltaisia pk-yritysten keskuudessa. Raportissa esiteltyä ratkaisumallia soveltamalla vastaavanlainen prosessi voidaan viedä läpi myös muissa pienyritysympäristöissä, ja esitellyt artefaktit ovat sellaisenaan käyttövalmiita käyttöotettaessa tietosuoja-asetusta.

2 TUTKIMUSMENETELMÄT

Tutkimusta tehtäessä hyödynnetään monimenetelmällistä tutkimusotetta, josta käytetään myös termiä triangulaatio. Triangulaatiolla tarkoitetaan eri tutkimusmenetelmien, tutkijoiden, tietolähteiden tai teorioiden yhdistämistä tutkimuksessa (Hirsjärvi, Remes, Sajavaara & Sinivuori, 2010). Jo lähtökohtaisesti tämän kaltainen tapaustutkimus, jossa yksittäistapausta tutkitaan yhteydessä ympäristöönsä ja tuotetaan tutkittavaan kohteeseen ratkaisu, pitää sisällään aineiston keruuta eri metodeja hyödyntämällä (Hirsjärvi ym., 2010, s. 135; Golafshani, 2003).

Luvussa 2.1. kerrotaan kirjallisuuskatsauksesta tutkimusmenetelmänä, ja kuinka aineistonkeruu toteutettiin tässä tutkimuksessa. Kirjallisuuskatsauksen tarkoituksena on antaa lukijalle kattava yleiskäsitys tutkittavista ilmiöistä, tiedon hallinnasta ja GDPR-asetuksesta, ja niiden merkityksestä. Sen avulla pyritään selvittämään mitä tiedon hallinta on, ja mitä se pitää sisällään. Aiempien tutkimusten mukaan EU:n yleisen tietoasetuksen käyttöönotto on takunnut organisaatioissa, joten kirjallisuuskatsauksen avulla pyritään syventämään ymmärtämystä asetuksen vaikutuksista ja sen soveltamisen haasteista organisaatioissa. Tutkimusongelmaan ratkaisu tuotetaan tosielämän kontekstissa, josta kerätään tietoa haastatteluin ja havainnoimalla. Noiden menetelmien hyödyntämisestä kerron luvussa 2.2 lisää. Luvussa 2.3. paneudun suunnittelutieteelliseen tutkimusprosessimalliin (engl. design science research method, DSRM), jota höystetään referenssimallin opein. Suunnittelutieteellinen tutkimusote on erinomaisen hyvin sopiva työkalu tämän työn käytännön läheisen tutkimusongelman ratkaisemiseksi, koska konstruktiivisena prosessina sen nimenomaisena tavoitteena on tuottaa uutta tietämystä sekä artefakteja, joiden avulla voidaan helpottaa sekä suunnittelutyötä että käytännön toteutusta tutkimusongelmaa ratkaistaessa (Hevner, Marh & Ram, 2004; Peffers, Tuunanen, Rothenberger & Chatterjee, 2008).

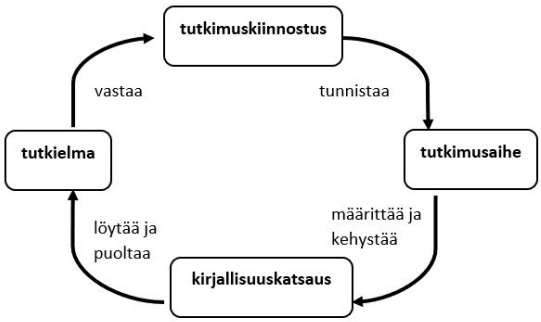
Tutkimuksen aikana pidin tutkimuspäiväkirjaa, jonne kirjasin tutkimuksen kulun ja konkreettiset tapahtumat. Tutkimuspäiväkirjaan koostin myös aineistot, joita hyödynnettiin ratkaisun tuottamisessa tutkimusprosessin aikana. Systemaattisesti yllä pidetyn tutkimuspäiväkirjan myötä pystyin myös seuraa-

maan tutkimuksen etenemistä omasta näkökulmastani tarkastellen, ja tarvittaessa kehittämään kontribuutiotani iteratiivisen työskentelyn aikana.

2.1 Kirjallisuuskatsaus ja tiedon haku

Lähtökohtaisesti tutkimus rakentuu aina käsitteellisiin ratkaisuihin ja merkitystulkintoihin (Hirsjärvi ym., 2010). Tutkimusmenetelmänä kirjallisuuskatsaus on kirjallinen perustelu, jolla edistetään opinnäytetyön tekemistä vakuuttavien aineistojen, jotka perustuvat aiempiin tutkimuksiin, hyödyntämisellä (Machi & McEvoy, 2016). Kirjallisuuskatsaus voi toimia tausta-aineistona empiiriselle tutkimukselle tai se voi olla itsenäinen kokonaisuus, joka tarjoaa arvokasta tietoa itsessään (Templier & Paré, 2015). Ennen kirjallisuuskatsaukseen ryhtymistä on hyvä esittää itselleen kysymys, onko opinnäytteessä tavoitteena esittää valitun aihealueen nykytilatietämys vaiko löytää tutkimusongelma jatkotutkimukselle. (Machi & McEvoy, 2016). Tässä työssä tavoitteena on esittää sekä tiedon hallinnan että GDPR-asetuksen nykytilatietämys. Kirjallisuuskatsaus tuottaa koostettua ajantasaista tietoa valittujen käsitteiden osalta. Toiseksi katsauksen tarkoituksena on toimia tietopankkina sekä tausta-aineistokokonaisuutena empiiriselle tutkimukselle. Kolmanneksi kirjallisuuskatsauksen avulla pyritään tunnistamaan sekä havainnoimaan GDPR-aihealueeseen liittyviä ongelmia tai haasteita – erityisesti sellaisia, jotka saattavat hankaloittaa asetuksen käyttöönottamista sekä soveltamista.

Järjestelmällisyyteen pyrkivä kirjallisuuskatsauksen tiedonhaku oli monivaiheinen. Se noudatteli Machin ja McEvoyn (2016) esittelemää neljän vaiheen pelkistettyä kirjallisuuskatsauksen prosessia (kuvio 1). Pelkistetyn kirjallisuuskatsauksen tekeminen on perusteltua, koska nimenomaisesti tässä työssä pyritään esittämään nykyhetken tietämys aihealueesta ja käyttää tuota tietoa tutkimusongelman ratkaisemisessa. Prosessin ensimmäisessä vaiheessa tunnistetaan ja valitaan tutkimuksen kiinnostuksen kohteet. Ensimmäisen vaiheen löydöksiin pohjautuen seuraavaksi kirkastetaan tutkimusaihe, jonka jälkeen tuotetaan kirjallisuuskatsaus. (Machi & McEvoy, 2016.) Prosessin myötä tutkimusongelma kirkastui kysymykseen ”Miten EU:n yleisen tietosuoja-asetuksen käyttöönottoa voidaan tukea pienyrityksessä”. Kirjallisuuskatsausta tuotettaessa lisäksi tukeduttiin Templierin ja Parén (2015) artikkeliin, joka pureutuu itsenäisten kirjallisuuskatsausten ohjenuoriin.



KUVIO 1 Kirjallisuuskatsauksen vaiheet (Machi & McEvoy, 2016, s. 3 mukaellen)

Järjestelmällisyyteen pyrkivässä tiedonhaussa hyödynnettiin Elsevierin tuottamaa sekä ylläpitämää Scopus-tietokantaa, joka on monitieteinen vertaisarvioidun kirjallisuuden viittaus- ja tiivistelmätietokanta. Tietokannassa haku kohdistettiin tieteellisten lehtien artikkeleihin, konferenssipapereihin sekä kokoomateosten artikkeleihin. Koska tiedon haussa on tärkeää yhdistellä eri lähteitä, jotta varmistettaisiin hakujen kattavuus (Templier & Paré, 2015), haettiin materiaaleja myös ProQuest Central:n kautta. ProQuestin monitieteisestä tietokannassa haku laajennettiin vertaisarvioimattomien teosten joukkoon. Lisäksi hyödynnettiin viranomaistahojen sekä tunnettujen tutkimus- ja konsultointiyritysten että tietokirjailijoiden tuottamia materiaaleja.

Tiedon hallinnasta etsittiin tietoa avainsanahakutermillä ”information governance”. Tavoitteena on selvittää, mitä tiedon hallinnan laajan paradigman käsitetään pitävän sisällään. Täten apukysymyksinä toimivat 1) Mitä tiedon hallinta on? ja 2) Mitä elementtejä tiedon hallinta pitää sisällään? Scopus-kannassa aihealueeksi valittiin ”computer science”, jolloin dokumentteja löytyi hakurajauksella 44 kappaletta yhden ollessa duplikaatti ja yhden ollessa saavuttamattomissa maksutta. ProQuest kannassa hakutuloksiin valittiin mukaan myös vertaisarvioimatonta kirjallisuutta, joka edustaa alan asiantuntijoiden tiedon hallinnan käsityksiä.

Etsittäessä kirjallisuutta EU:n yleisestä tietosuoja-asetuksesta käytettiin haussa termiä ”General Data Protection Regulation” ja sen lyhennettä ”GDPR”. Haku kohdistui tekstin otsikkoon, johdantoon sekä avainsanoihin. Aihealueiksi valittiin Scopus-kannassa ”computer science”. Koska GDPR-asetus on julkaistu vuonna 2016, sisällytettiin hakuun kyseisen vuoden ja sitä myöhäisemmät kirjalliset julkaisut elokuuhun 2018 asti, jolloin tutkielmaraportin puhtaaksikirjoittaminen aloitettiin. Ensimmäisellä alustavalla kirjallisuuden hakukerralla (Machi & McEvoy, 2016) englanninkielistä kirjallisuutta ja artikkeleita sekä konferenssipapereita löytyi hakurajauksilla yhteensä 206 kappaletta. Jotta saatiin käsitys teemoista, ensin perehdyttiin otsikoiden lisäksi hakurajauksilla löytyneen kirjallisuuden tiivistelmiin sekä silmäiltiin tekstit läpi. Kirjallisuuskatsauksen tekeminen jatkui kiinnostuksen kohteiden valinnalla rajaten ja selkeyttäen näkemystä käsiteltävistä asioista (Machi & McEvoy, 2016). Jotta syntyisi ymmärrys, miksi GDPR-asetus on laadittu ja mitä haasteita sen käyttöönottoon

saattaisi liittyä, valittiin perusteellisempaan tarkasteluun kirjoitukset, joista käy ilmi: 1) mitkä asiat ovat olleet taustavaikuttajina lain syntymiseen, 2) mitkä asiat ovat kaikkein keskeisimpiä laissa, ja 3) mitä mahdollisia haasteita yleisellä tasolla organisaatioissa GDPR:n soveltamiseen sekä noudattamiseen voi liittyä. Tarkasteluun tämän jälkeen tekstejä jäi 85 kappaletta. Perusteellisemman lukemisen ja analyyttisemmän tarkastelun jälkeen (Templier & Paré, 2015) valittiin lähdeviitteiksi Scopus-kannasta 22 tekstiä. Valinta tehtiin aiemmin määriteltyjen apukysymyksen (Templier & Paré, 2015) perusteella. EU:n tietosuoja-asetuksen taustatietoja etsittäessä itse GDPR-asetustekstin lisäksi hyödynnettiin eri viranomaistahojen tuottamaa tietoa, kuten muun muassa EU:n virallista internetsivustoa sekä Suomen oikeusministeriön että Suomen tietosuojavaltuutetun toimiston tuottamia julkaisuja.

2.2 Haastattelu ja havainnointi

Hyvin usein kvalitatiivisissa sekä empiirisissä tutkimuksissa päämenetelmänä toimivat puolistrukturoidut haastattelut. Tällaisessa strukturoiden ja avoimen haastattelun välimaastoon asettuvassa metodissa haastattelija miettii etukäteen teoreettiseen viitekehykseen pohjautuvat aihepiirit eli teemat. Toisin kuin strukturoidussa haastattelussa, teemahaastattelussa etukäteen mietittyjen kysymysten lisäksi haastattelija voi esittää lisäkysymyksiä pohjautuen esimerkiksi haastateltavan vastauksiin. Avoimesta haastattelusta poiketen puolistrukturoitu haastattelu sisältää kuitenkin selkeän haastattelurungon, jota hyödyntäen myös vuorovaikutteinen dialogi onnistuu. (Hirsjärvi ym., 2010.) Tässä tapaustutkimuksessa haastattelun avulla kerättiin tietoa tutkittavasta kohteesta ja tutkittiin ilmiötä yhteydessä ympäristöönsä, eli toimeksiantaja JSK Oy:n kontekstissa.

Puolistrukturoituja haastatteluita tehtiin tutkimusprosessin eri iteraatioiden vaiheissa. Haastatteluiden avulla saatiin tietoa muun muassa toimeksiantajasta, sen liiketoimintaympäristöstä ja henkilötietojen käsittelystä sekä missä GDPR-asetuksen soveltamisen alaisia henkilötietoja sijaitsee. Ensinnäkin haastattelut valikoituivat pääasialliseksi tiedonkeruutavaksi koskien toimeksiantajaa ja sen kontekstista, koska aiheena GDPR-asetus ja sen käyttöönotto organisaatiossa on melko tuntematon alue sekä haastattelijalle että haastateltaville. Näin ollen haastattelun aikana esiin nouseviin kysymyksiin vastausten suuntia oli etukäteen mahdotonta tietää, ja siten suoralle kielelliselle vuorovaikutukselle oli selkeä tarve (Hirsjärvi ym., 2010). Niin ikään aihealueena henkilötietojen tiedonhallinnan uudet vaatimukset liittyen EU:n yleiseen tietosuoja-asetukseen ja sen soveltamisen haasteisiin tuottivat oletetusti tutkimustyöskentelyn aikana lisäkysymyksiä sekä vastauksia monitahoisesti. Tällöin puolistrukturoitu tutkimushaastattelu soi mahdollisuuden selventää saatuja vastauksia, ja lisäkysymyksillä syvennettiin saatuja tietoja (Hirsjärvi ym., 2010).

Tapauksesta ja sen ekosysteemistä ymmärtämystä ja tietoa kerrytettiin haastattelemalla Järvi-Suomen Kiinteistökonsultit Oy:n omistajayrittäjää ja toi-

mitusjohtajaa Jorma Lifländeriä yrityksen toimitiloissa viisi kertaa. Kuitenkin, välttääkseni kapeaa katsontakantaa ensimmäiseen haastattelukertaan osallistui myös tapausyrityksen yksi merkittävistä kumppaneista eli ohjelmistotoimittajan asiantuntija. Lisäksi ensimmäisen tapaamisen jälkeen yrittäjä toimi ohjelmistotoimittajan sekä tarvittaessa yrityksen asiakkaiden ja muiden sidosryhmien suuntaan tarkentavien jatkokysymysten sekä huomioiden välittäjänä. Tutkimushaastatteluiden lisäksi dialogia toimitusjohtajan kanssa käytiin sähköpostitse sekä puhelimitse joidenkin kuriositeettien tarkentamista varten. Haastattelun lisänä hyödynnettiin havainnointia, jonka avulla saatiin välitöntä suoraa tietoa toiminnasta ja käyttäytymisestä luonnollisessa ympäristössä (Hirsjärvi ym., 2010).

Havainnointia tässä tutkimuksessa hyödynnettiin tarkkailemalla tapausorganisaation liiketoimintaympäristöön kuuluvan Tarmo-tietojärjestelmän käyttöä sekä myös tutkijana käytin järjestelmää sen testikannassa. Tietojärjestelmän käyttöä havainnoimalla kerrytettiin ymmärtämystä sekä tietoutta liittyen järjestelmän henkilötietovirtoihin. Kollaboratiivisen työskentelyn ja havainnon lomassa käytiin dialogia. Dialogin ja havainnoinnin suuri etu olikin se, että saatiin välitöntä suoraa tietoa kohteesta – tässä tapauksessa yrityksen henkilötietojen käsittely-ympäristöstä, liiketoimintaympäristöstä ja ekosysteemiin kuuluvasta Tarmo-ohjelmiston toiminnasta. Havainnoinnin ja dialogien taustaaineistoina käytettiin JSK Oy:n tuottamia dokumentteja, kuten esimerkiksi esittelymateriaaleja ja muita presentaatioita JSK Oy:stä sekä Tarmo-ohjelmistosta, tilaus- ja toimitussopimuksia ja teknisiä kuvauksia.

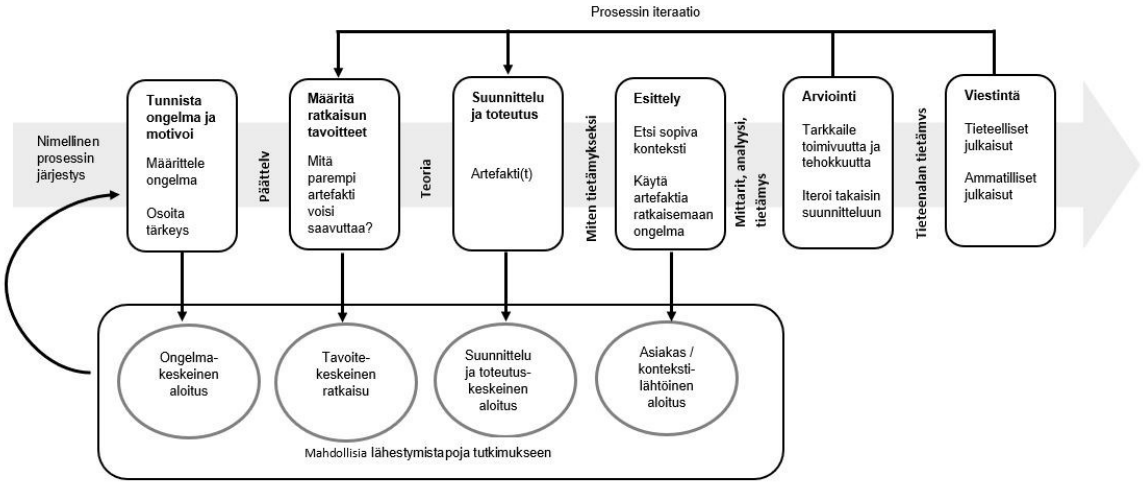
Haastattelut dokumentoitiin kirjalliseen muotoon. Myös sähköpostikirjeenvaihdosta ja puhelinkeskusteluista laadittiin muistiinpanot. Näitä dokumentteja hyödynnettiin ratkaisun tuottamiseksi JSK Oy:n kontekstiin iteratiivisen DSRM-prosessin, jonka aikana aineistoa tuotettiin konkretian kautta lisää tutkimuksen käyttöön, aikana. Myös kaaviot, kuviota ja miellekartat, joista kerron tuonnempana lisää, toimivat ratkaisua tuotettaessa tausta-aineistona. Haastattelu ja havainnointi mahdollistivat yhteistyössä toimeksiantajan asiantuntijoiden kanssa ymmärryksen syventämisen tutkittavia ilmiöitä kohtaan. Käyty dialogi oli merkittävässä roolissa toimivan ratkaisun kehittämisessä JSK Oy:n liiketoimintaympäristöön. Seuraavaksi luvussa 2.3 kerron DSRM-prosessin toteuttamisen vaiheet. Sen käytännön soveltamisen tapausorganisaatiossa kuvaan vaiheittain luvussa 5.

2.3 Suunnittelutieteellinen tutkimusmenetelmä

Käytännön läheinen tutkimusongelma ratkaistiin suunnittelutieteellisen tutkimusmenetelmän (engl. design science, DS) avulla. Menetelmän tarkoituksena on tuottaa ratkaisuja sekä artefakteja organisaation tunnistettuihin ongelmiin. Prosessiin sisältyy myös artefaktien tai tuotetun ratkaisun arviointi. (Hevner ym., 2004.) Suunnittelutieteellisen tutkimusmenetelmän tueksi on laadittu DSRM-prosessi, jonka mukaisesti tätä

tutkimusta toteutettaessa edettiin. Peffers, Tuunanen, Rothenberger ja Chatterjee (2008) ovat esitelleet DSRM-prosessin suunnittelutieteellisen tutkimuksen tueksi tutkimuskentällä havaitsemiensa kehityskohteiden vuoksi. Ensinnäkin se on yhdenmukainen aiemman suunnittelutieteellisen (engl. design science, DS) kirjallisuuden kanssa, toiseksi se tarjoaa nimellisen prosessimallin DS-tutkimuksen tekemiseen ja kolmanneksi se antaa mentaalimallin tutkimuksen esittelyyn sekä arviointiin. (Peffers ym., 2008.) Suunnittelutieteellistä tutkimusmenetelmää höystettiin Ostrowskin ja Helfertin (2012) esittelemän referenssimallin opein. Se sisältää kaksi prosessia: kirjallisuuskatsauksen ja kollaboraation ammatinharjoittajien kanssa. Prosessien avulla kerättiin tietoa tutkittavista ilmiöistä sekä esiteltiin ne ymmärrettävällä tavalla sidosryhmille. (Ostrowski & Helfert, 2012.)

Koska DSRM-prosessin avulla on tarkoitus luoda käytännön ongelmaan ratkaisu ja parannusehdotuksia konstruktioiden myötä, sopi se erinomaisen hyvin käytettäväksi tässä tutkimuksessa. Kuviossa 4 esitetään prosessille määriteltyä kuusi eri toimintavaihetta, jotka ovat: 1) ongelman tunnistaminen ja motivointi (engl. indetify problem and motivate), 2) ratkaisun tavoitteiden määrittäminen (engl. define the objectives of a solution), 3) suunnittelu ja toteutus (engl. design and development),4) esittely (engl. demonstration), 5) arviointi (engl. evaluation) ja 6) viestintä (engl. communication). Toimintavaiheiden lisäksi prosessilla on neljä eri lähestymistapaa: ongelmakeskeinen aloitustapa, tavoitekeskeinen ratkaisu, suunnittelu ja toteutuskeskeinen aloitus ja asiakas tai kontekstilähtöinen aloitus. (Peffers ym., 2008.)



KUVIO 2 Suunnittelutieteellinen tutkimusprosessi (Peffers ym., 2008, s. 54 mukaellen).

1) **Ongelman tunnistaminen ja motivointi** (engl. indetify problem and motivate) vaiheessa määritellään tutkimusongelma ja perustellaan ratkaisun arvo. Mikäli ongelma on moniulotteinen, kannattaa pilkkoa se pienempiin kokonaisuuksiin. Ongelman määrittely on tärkeää, koska sen perusteella kehitetään artefakti ratkaisun saamiseksi ja autetaan

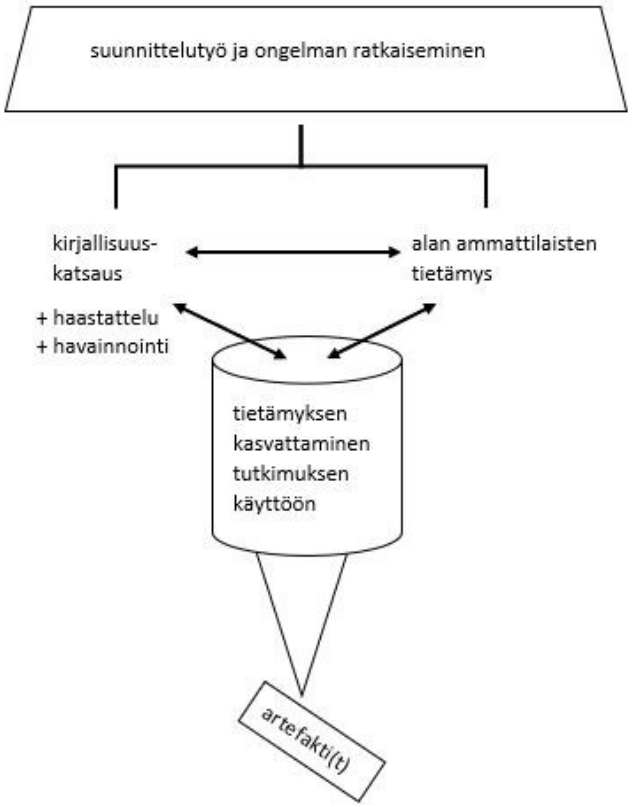
ymmärtämään itse ongelmaa. Määrittelyn avulla motivoidaan tutkijoita sekä yleisöä hyväksymään ratkaisu sekä hyödyntämään sitä.

2) Määriteltyyn ongelmaan pohjautuen, ja suhteessa siihen mitä on mahdollista toteuttaa, johdetaan **ratkaisun tavoitteet** (engl. define the objectives of a solution). Tavoitteet voivat olla määrällisiä tai laadullisia. Esimerkiksi tuotettavan artefaktin suorituskyvyn paremmuuden osoittaminen verrattuna aiempiin, tai kuvaus siitä, millä tavoin tuotos jatkossa tukisi ongelmien ratkaisemista. Tässä vaiheessa on tärkeätä hahmottaa ongelman nykytila sekä tietää nykyiset ratkaisut, mikäli niitä on.
3) **Suunnittelu- ja toteutusvaiheessa** (engl. design and development) muodostetaan tuotos eli rakennetaan artefakti(t). Tässä toimintavaiheessa tulisi määritellä artefaktin toivotut toiminnallisuudet sekä sen arkkitehtuuri.
4) Seuraavaksi tapahtuu **demonstraatio eli esittely** (engl. demonstration), jonka tarkoituksena on selventää, millä tavoin uusi tuotos ratkaisee ennalta määritellyn tutkimusongelman tai -ongelmat. Esittely voidaan toteuttaa tieteellisellä testauksella, simulaatiolla, tapaustutkimuksella tai muulla käyttötarkoitukseen sopivalla tavalla.
5) Vaiheessa viisi, **arviointi** (engl. evaluation), havainnoidaan ja mitataan, kuinka hyvin tuotos tukee määritellyn ongelman ratkaisemista. Arvioitaessa artefaktia verrataan ratkaisua demonstraatioon pohjautuen. Mikäli tuotos ei vastaa odotuksia tai siinä on epäkohtia, voidaan palata prosessissa aiempiin aktiviteetteihin tai jättää kehitystyö tuleviin myöhempiin projekteihin.
6) **Viestintä** (engl. communication) on DSRM-prosessin viimeinen tärkeä vaihe. Olennaista on tuoda ilmi tutkimuksen ongelma ja tuotetun ratkaisun merkitys. Lisäksi kuvataan artefakti, sen hyödyllisyys ja uutuus, suunnittelun tarkkuus ja tuotoksen vaikuttavuus tutkijoille ja muulle yleisölle. Viestinnän on hyvä tapahtua kunkin tieteenalan kulttuurin ja normien mukaisesti. (Peffers ym., 2008.)

DSRM-prosessi sisältää neljä lähestymistapaa. Tutkija voi valita aloituksen mistä vaiheesta tahansa sekä siirtyä vaiheesta toiseen ilman tietyn järjestyksen noudattamisen velvoitusta. Ongelmakeskeinen lähestymistapa alkaa DSRM-prosessin ensimmäisestä vaiheesta. Mikäli haetaan tavoitekeskeistä ratkaisua, aloitetaan vaiheesta kaksi. Kolmannesta vaiheesta aloittaminen soveltuu suunnittelu ja kehityskeskeiseen lähestymistapaan. Mikäli havainnoidaan toimivaa käytännön ratkaisua, aloitetaan vaiheesta neljä. (Peffers ym., 2008.)

Suunnittelutieteellisen tutkimusotteen tarkoituksena on uuden tiedon tuottamisen lisäksi tuottaa ratkaisu eli artefaktit nimenomaisesti tutkimuskohteen käyttöön. Tässä tutkimuksessa DSRM-prosessia höystetään referenssimallin ajatuksin. Alun perin tieto -ja informaatiojärjestelmäprojekteja silmällä pitäen kehitetyn referenssimallin mukaan, kuten kaikessa tutkimustoiminnassa, on tärkeää kerätä informaatiota tutkittavaan aiheeseen liittyen kirjallisuuden avulla. Toiseksi informaatio tulisi esittää ymmärrettävässä muodossa sidosryhmille.

Referenssimallissa korostetaan erityisesti yhteistyötä ammatinharjoittajien kanssa. (Ostrowski & Helfert, 2012.) Kuviossa 3 esitetään referenssimallista lainaamani kollaboraatioajatus. Informaatiota ja tietoa ongelman ratkaisemista varten kartutettiin tässä työssä sekä kirjallisuuskatsauksen avulla että alan ammattilaisilta. Tavoitteena on ammattilaisten kanssa yhteistyössä etsiä parhaimmat käytännön ratkaisut tutkimusongelman tai -ongelmien ratkaisemiseksi. Hyvin usein kollaboraatio sisältää myös strukturoituja haastatteluita sekä suoraa havainnointia. (Ostrowski & Helfert, 2012.)



KUVIO 3 Referenssimallin soveltaminen tutkimuksessa.

Kirjallisuuskatsauksen lisäksi, tietämyksen sekä syvällisemmän ymmärryksen kasvattamisen vuoksi, tässäkin tutkimuksessa on erittäin tarpeellista hyödyntää haastattelujen ja havainnoinnin tuomia mahdollisuuksia. Niiden avulla kerrytetään tietoa tapausorganisaatiosta ja sen henkilötietojen tiedon hallinnan ekosysteemistä. Tekstituotosten lisäksi työn hedelmät visualisoituivat muun muassa kuvioiksi, kaavioiksi sekä miellekartoiksi, joita tutkimuksen alkuvaiheessa laadittiin yhteistyössä toimeksiantajan kanssa. Yhteistyö ammatinharjoittajan kanssa on tässä tapaustutkimuksessa sangen perusteltua ja lähestulkoon välttämätöntä, koska organisaatio itsessään omaa parhaan tietämyksen henkilötietojen tiedon hallinnan nykytilasta ekosysteemissään.

3 TEOREETTIS-KÄSITTEELLINEN TAUSTA

Taustoitan tutkimusongelman ratkaisemista seuraavaksi pureutumalla yleisellä tasolla tiedon hallinnan laajaan paradigmaan. Tiedon hallinta (engl. information governance, IG) on organisaatiolle elintärkeää, ja tiedon arvo on yhä enenevissä määrin kasvamassa yhteiskunnassa (Blair, 2011; Kooper, 2011; Smallwood, 2014). Tiedon hallinnan ratkaisut organisaatioissa ovat kriittisiä menestystekijöitä, jonka vuoksi johtajat yhä enenevissä määrin ovat kiinnostuneita tarkastelemaan mahdollisuuksia hallita ja hyödyntää tietoa (Smallwood, 2014). Organisaatiot ovat joutuneet kiinnittämään huomiota entistä enemmän tiedon hallintaan toukokuussa vuonna 2018 voimaan tulleen Euroopan Unionin yleisen tietosuoja-asetuksen vuoksi (Scoch, 2018). Täten toisena laajempana asiakokonaisuutena taustoittamaan tutkimusongelman ratkaisemista tutkielmassa perehdytään EU:n yleisin tietosuoja-asetuksen tematiikkaan. Tietosuoja-asetuksen yhtenä tärkeänä tavoitteena on parantaa yksilöiden henkilötietojen suojaa. Sen toisena tavoitteena on luoda Euroopan unionille yhtenäinen tietosuojan viitekehys, jonka avulla pyritään mahdollistamaan entistä paremmin digitaaliset sisämarkkinat. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016.)

Tiedon hallinta, IG, on laaja-alainen paradigma. Koska termeinä tieto, hallinto sekä hallinta voidaan käsittää eri tavoin kontekstista ja tarkastelukulmista riippuen, avataan seuraavissa alaluvuissa lyhyesti tiedon paradigmaa. Lisäksi pureudutaan tiedon hallinnan kannalta olennaisimpiin informaatiotekonologia-toimialan (engl. ICT, information and communication technologies) tiedon sekä hallinnon (engl. governance) että hallinnan (engl. management) termeihin. Termi ”governance” on esiintynyt organisaatiokirjallisuudessa vuodesta 1960 lähtien (Tallon, Ramirez & Short, 2013).

Seuraavissa alaluvuissa puretaan auki edellä mainittujen käsitteiden eroavaisuuksia sekä yhteneväisyyksiä ja sitä, miten termien merkityksiä voidaan tulkita.

3.1 Tiedon sekä hallinnon ja hallinnan termiviidakossa

Aikaisempaan tutkimukseen sekä muuhun kirjallisuuteen perehtyessäni havaitsin, että esimerkiksi sanojen data ja informaatio käyttö ei aina ole johdonmukaista. Samoin termejä tiedon hallinta (engl. ”information governance”) ja tiedon hallinta (engl. ”data governance”) saatetaan käyttää jopa toisilleen rinnasteisina (Alhassan, Sammon & Daly, 2016; Burgin, 2010; Tallon ym., 2013). Tähän aiempien tutkimusten perusteella saatuun tietoisuuteen pohjautuen katson tarpeelliseksi perehtyä hieman ICT-alan termiviidakkoon. Se on nähdäkseni tarpeellista, koska kirjallisuudesta käy ilmi, että toisinaan sekaannuksiakin on tapahtunut termien käytöstä johtuen, ja väärinkäsityksistä pääsääntöisesti koitunee haittaa. Tieteenhistoriasta löytyy paljon esimerkkejä käsitteisiin liittyvistä vaikeuksista sekä ristiriitaisuuksista, ja pahimmillaan tutkimusta ei ole pystytty edistämään epäselvyyksien vuoksi (Hirsjärvi ym., 2010, s. 148). Alaan liittyvien termien, kuten sanojen, sanaliittojen tai lyhenteiden käyttö voi olla moninaista. Näin on myös tietojärjestelmätieteiden alalla. Akateemisessa kirjallisuudessa esiintyy eri termejä ja erilaisia lähestymistapoja, jotka tarkastelevat muun muassa sanoja data ja informaatio (Alhassan ym., 2016). Termejä data, informaatio ja tietämys saatetaan käyttää jopa toisilleen rinnasteisina (Burgin, 2010). Vastaavasti englanninkielisten termien ”information governance”, ”IT governance” ja ”data governance” ympärillä on kerrottu olleen sekaannuksia sekä erilaisia käsityksiä siitä, kuinka ne eroavat muista samankaltaisista ICT-alan termeistä (Smallwood, 2014; Guetat & Dakhli, 2015).

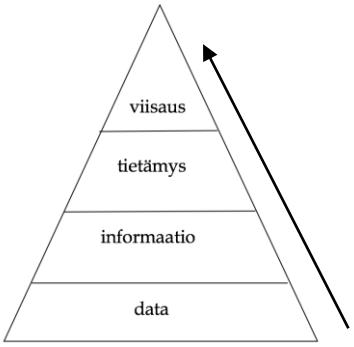
Seuraavassa luvussa esitellään lyhyesti erittäin tunnettu tietokäsitys. Tieteenalasta riippuen kyseistä tietokäsityksen artefaktia, jonka hierarkkista esittämistapaa on kritisoitukin, kutsutaan eri nimillä. Artefakti tunnetaan lyhenteellä DIK, joka muodostuu englanninkielisistä sanoista ”data”, ”information” ja ”knowledge”. Käsitteiden välistä suhdetta kuvataan tiedon pyramidin avulla. Laajennetussa tiedon mallissa lisätään pyramidin huipulle viisaus (engl. wisedom), jolloin sananelikon lyhenteeksi muodostuu DIKW. (Burgin, 2010, s. 185-197.)

3.1.1 Tiedon tasot: data, informaatio, tietämys ja viisaus

Data (engl. data), informaatio (engl. information) ja tietämys (engl. knowledge) muodostavat tiedon skeeman. Näitä kolmea olennaista tiedon skeeman termiä on määritelty ja käytetty monin eri tavoin kontekstista riippuen, ja jopa tutkimuskentällä niiden merkitystä saatetaan pitää itsestään selvänä (Burgin, 2010). Suomen kielessä tieto sanana on moniselitteinen ja -merkityksellinen. Terminä se voi liittyä informaatioon, tietämykseen tai tosiasiaan, ja sitä saatetaan käyttää edellisten synonyyminä (Kotimaisten kielten keskus, 2017). Sen sijaan englanninkieliset sanojen ”information” ja ”knowledge” merkitys on selkeästi erotettavissa.

Tiedon hierarkkinen pyramidi, jossa data on sijoitettu alimmaisemmaksi ja tietämys ylimmäksi elementiksi, on yksi tunnetuimista tavoista jaotella tiedon tasoja. Dataan on erotettavissa kaksi lähestymistapaa. Se koetaan resurssina ja manipuloitavina objekteina. Tietojärjestelmätieteessä data nähdään käsittelemättömänä informaationa (Burgin, 2010), jonka merkkimuotoista ilmentymää organisaatiot keräävät ja syöttävät systeemeissä (Smallwood, 2014).

Informaatio on muotoon prosessoitua dataa, joka on vastaanottajalle merkityksellistä (Hevner, Chatterjee, Gray & Baldwin, 2010). Se on tietämyksen lisäämistä vastaanottamalla dataa, tarkkailemalla todellisuutta tai sisäisiä prosesseja, joiden avulla henkilö järjestää, vertailee tai arvioi tietämystään (Leppänen, 2014). Tällöin data muuntuu informaatioksi, jolloin sitä käytetään päätöksen teon tukena (Tallon ym., 2013). Informaatiolla on todellista arvoa nykyisissä tai tulevissa toimissa tai päätöksissä (Hevner ym., 2010). Datan ja informaation ero on toiminnallinen, ei rakenteellinen. Suositun lähestymisnäkökulman mukaan tietojärjestelmätieteessä relaatio datan ja informaation välillä tarkoittaa sitä, että informaatio on järjestelty tosiasioiden ja datan kokoelma. Tietämys kasvaa ja jalostuu informaation avulla tiedon pyramidissa (kuvio 4). Pyramidin huipulle asettuu viisaus. Tiedon kolminaisuudesta, data – informaatio – tietämys, tutkijat alkoivat ottaa selvää 1980-luvulta lähtien yhä enenevissä määrin. (Burgin, 2010.)



KUVIO 4 Datan, informaation ja tietämyksen avulla kohti viisautta.

Data voi olla joko konekielisesti tai kielellisesti käsiteltävää raaka-ainetta. Kun informaation vastaanottaja tulkitsee saamaansa aineistoa ja antaa sille merkityksen, muodostuu siitä tietoa. Tietämys on inhimillistä pääomaa. Tietämys nousi tieteen aihealueeksi viime vuosituhannella 1900-luvulla tietokoneiden tulon myötä. Informaation käsite nousi tutkijoiden mielenkiinnon kohteeksi vuosikymmenien kuluessa. Kiinnostus pureutua skeeman kolmanteen elementtiin dataan virisi siinä vaiheessa, kun tietokoneet tulivat pääasiallisiksi informaation käsittelyn laitteiksi. (Burgin, 2010.)

Datan voisi käsittää olevan symboleja tai itsenäisiä entiteettejä, joilla sellaisenaan ei juurikaan ole merkitystä, eikä niihin pohjautuen voi tehdä päätelmiä. Data voisi olla sisältöä, jota käsitellään lähtökohtaisesti tietojärjestelmissä, - ei siis esimerkiksi paperilla. Sellaisenaan osa dataa ei välttämättä tuota tietoa, informaatiota tai tietämystä, mutta mahdollisesti sen eri osien yhdistelmät kyllä-

kin. Toisaalta data voidaan nähdä myös resurssina ja objekteina lähestymistavan ollessa tällöin kielellinen. Dataa ja informaatiota prosessoimalla kasvatetaan tietämystä. Toistaiseksi teknologiset IT-ratkaisut jättänevät tietoteknisissä systeemeissä inhimillisen ja organisatorisen tiedon käsittelyn tietojenkäsittelyjärjestelmien ulkopuolelle, mutta ne auttavat inhimillisen tietämyksen lisäämisessä sekä viisauden saavuttamisessa. Tiedon hierarkkisen tietokäsityksen mukaan vaikuttaa siltä, että yksittäiset tiedon ilmentymät, dataentiteetit, ovat merkityksettömiä sellaisenaan tai niiden informaatiosisältö on lähestulkoon arvoton tarkastelijalleen.

Tieto, data ja informaatio käsitteiden lisäksi johtamis- ja hallintatermit ”governance” sekä ”management” saattavat aiheuttaa sekaannuksia. Seuraavaksi avataan näiden termien merkitystä, sekä niiden erityisesti tietoon viittaavien sanayhdistelmien eroja. Inhimillisten resurssien johtamisen kannalta termien käyttöä vain sivutaan.

3.1.2 Hallinnon ”governance” ja hallinnan ”management” eroja

Tässä luvussa pureudutaan lyhyesti tiedon hallinnan paradigmaan olennaisesti liittyviin termeihin hallinto (engl. governance) ja hallinta (engl. management) ja kyseisten sanayhdistelmiin, joita vilisee sekä tietojärjestelmätieteiden tieteentekijöiden että alan ammattilaisten keskuudessa. Joitakin termejä saatetaan toisinaan käsittää jopa täysin synonyymeiksi, joka saattaa johtaa väärinkäsityksiin.

Esimerkiksi termien ”data governance” (suom. datan hallinta) ja ”data management” (suom. tiedonhallinta) saatetaan käsittää tarkoittavan samaa asiaa, vaikka merkityksillä on havaittavissa selkeitä eroja. Merkittävin ero termien välillä on se, että ”governance” viittaa päätöksiin, jotka täytyy tehdä tehokkaan johtamisen ja resurssien hyödyntämisen varmistamiseksi ja ”management” voidaan yksinkertaisesti nähdä päätösten täytäntöönpanona (Fu, Wojak, Neagu, Ridley & Kim, 2011; Khatri & Brown, 2010; Alhassan, Sammon & Daly, 2016 mukaan). Tällöin voidaan tulkita, että ”management” on saanut vaikutteita käsityksestä ”governance” (Alhassan ym., 2016).

Vastaavasti termejä tiedon hallinta (engl. information governance, IG) ja datan hallinta (engl. data management) käytetään usein vaihtoehtoina toisilleen, vaikka konseptit eroavat toisistaan. Datan hallinta keskittyy eri lähteistä kerättyihin elementteihin (Guetat & Dakhli, 2015) ja tiedon alimmalla tasolla sen laatuun (Smallwood, 2014). Datan laadun ja ylimäärän poistamiseksi se sisältää tekniikat datan siivoamiseen ja duplikaattien poistamiseen. Se sisältää myös prosessit ja kontrollit, joilla varmistetaan datan olevan oikeaa, paikkansapitävää ja tarpeellista. Se viittaa ihmisten, prosessien ja teknologioiden kokonaisuuteen, jonka avulla organisaatiossa hallitaan tietoa, ja se voidaan nähdä tiedon hallinnan alkeistasona. (Smallwood, 2014.) Tällöin datan sijoittaminen tiedon alimmalle tasolle (vrt. Burgin, 2010) saattaa viitata hierarkkiseen tietokäsitykseen. Datan hallinta muodostaa yrityksen laajuisen viitekehyksen asettaen päätöksentekoon liittyvät oikeudet ja velvollisuudet, ja näin ollen dataa voidaan asianmukaisesti käsitellä osana yrityksen varallisuutta (Alhassan ym., 2016).

Muun muassa datan hallinta (engl. data governance), hyvä tiedonhallintatapa (engl. information technology (IT) governance) ja tiedon hallinta (engl. information governance, IG) ovat ammentaneet vaikutteita hyvästä liikkeenjohtotavasta tai toisin suomennettuna hyvästä hallintotavasta (engl. corporate governance) (Smallwood, 2014). Hyvä liikkeenjohtotapa on hallinnon ylin taso organisaatiossa (Smallwood, 2014) ja ”governance”, kuten aiemmin jo mainittu, fokusoituu organisaation johtajien rooliin ja tavoitteisiin edustaa sekä suojella osakkaiden etuja (Kooper ym., 2011). Taloudellisen yhteistyön ja kehityksen järjestön (Organization for Economic and Development, OECD), joka ensimmäisen määritteli ”governance”-termiä (Pulkkinen, 2018), mukaan hallintoa voidaan kuvata kokonaisuudeksi, joka kehkeytyy sosiaalisten, poliittisten ja hallinnollisten aktiviteettien tuloksena. Hyvä hallintotapa sisältää prosessit, tavat, politiikat ja lait sekä instituutiot, jotka vaikuttavat tapaan ohjata ja hallita yritystä. Se pitää sisällään myös sidosryhmien suhteet ja yrityksen tavoitteet. Yrityksen hallinnointi- ja ohjausjärjestelmänä se tarjoaa rakenteet määritellä organisatoriset tavoitteet sekä suorituskyvyn seurannan tavoitteiden saavuttamisen varmistamiseksi. (OECD, 2015.)

Tieto- ja viestintätekniikan (engl. information and communication technology, ICT) alalla hyvä tiedonhallintatapa (engl. IT governance) ja sen synonyymi ”ICT Governance” ovat vakiintuneita käsitteitä (Kooper ym., 2011). Se linkittää yhteen yrityksen päämäärät, liiketoiminnan tavoitteet sekä tieto- ja informaatiotekniikan (Smallwood, 2014). ”IT governance”, eli hyvä tiedonhallintatapa fokusoituu nimenomaan informaatioteknologian järjestelmiin, niiden suorituskykyyn ja riskien hallintaan. Se koostuu johtajuudesta ja organisaatiorakenteista sekä -prosesseista. Sen avulla pyritään varmistamaan organisaation strategioiden ja tavoitteiden ylläpitäminen (Kooper ym., 2011). Se on ensisijainen tapa edistää liiketoiminnan tavoitteiden saavuttamista, ja sen avulla sidosryhmät, kuten johtajat, osakkeenomistajat sekä työntekijät voivat varmistaa informaatiotekniikan (engl. information technology, IT) tuottavan arvoa liiketoiminnalle (Kooper ym., 2011; Smallwood, 2014).

Hierarkiassa ”corporate governance” eli hyvä hallintotapa on ylimpänä valtuuttaen johtamisen ”management”-tasolle, ja esimerkiksi tietohallinto (engl. information management) toteuttaa IT governancea (Pulkkinen, 2018), joka taasen on alisteinen hyvälle hallintotavalle. Forrester Research -tutkimusyhtiön käytännön läheisen määritelmän (Pulkkinen, 2018) mukaan tietohallinto kattaa prosessit, toimintatavat, teknologiat ja arkkitehtuurit. Näiden avulla kerätään, käytetään ja hallitaan organisaation ”structured dataa” eli koostettua tietoa sekä jäsentelemättömiä sisältöjä eli ”unstructured information”. (Weintraub, Owens & Jedinak, 2013.) Hyvä tiedonhallintatapa ”IT governance” voidaan nähdä ylemmän luokan kokonaisuutena, jolla ohjataan, kontrolloidaan ja koordinoidaan alemman luokan hallinto- ja valvontatehtäviä. (Tallon ym., 2013). Tällöin esimerkiksi tietohallinto (engl. information management) voidaan nähdä alisteisena hyvälle tiedonhallintatavalle.

”Governancen” strategisena tehtävänä on asettaa organisaatiossa kehykset tavoitteille, suunnalle ja rajoituksille. ”Management” huolehtii resurssien jaka-

misesta ja organisaation päivittäisen toiminnan valvonnasta. Yleisellä tasolla hyvä hallintotapa ”governance” voitaisiin yksinkertaisen tiivistetysti hahmottaa organisaation systeemiksi tai järjestelmäksi, jonka avulla johdetaan ja valvotaan organisaation toimintaa, ja hallinta ”management” myös päätös- ja suunnitteluvaltaisena toteuttaa asioita. Kiteytettynä IT:n roolina on lisätä mukaan tietotekniikka, teknologiat sekä tietojärjestelmät.

3.2 Kohti tiedon hallinnan viitekehystä

Seuraavaksi kerrotaan poimintoja tiedon hallinnan viitekehyksen muodostumisen vaiheista. Tiedon hallinta on laaja-alainen paradigma, joka on kehittynyt ensinnäkin liiketoimintaa kattavan uuden ja tiukennetun lainsäädännön ja toiseksi ulkoisten uhkien, kuten hakkeroinnin ja tietomurtojen seurauksena (Smallwood, 2014). Se on olennainen osa hyvää liikkeenjohtotapaa.

Termin tiedon hallinta, IG, tiedemaailmalle ensiesittelivät Donaldson ja Walker vuonna 2004 artikkelissa, jossa kuvataan viitekehys, jonka avulla julkisen terveydenhuoltotoimialan organisaatio National Health Service NHS voisi kehittää artefakteja vastaamaan kyseisen toimijakokonaisuuden tarpeita (Kooper ym., 2011). Tiedon hallinnan kehittämiseksi NHS:n ekosysteemissä tutkijat korostivat tarvetta pohtia monipuolisesti erilaisia soveltuvia aiheita vastuullisen ja laajennettavan lähestymistavan määrittelemiseksi (Donaldson & Walker, 2004). Sittemmin tiedon hallinnan ensiesittelyn jälkeen sitä on määritelty ja lähestytty eri näkökulmia painottaen sekä akateemisesti että alan asiantuntijoiden toimesta. Terminä tiedon hallinta on melko uusi, mutta asiat ja aktiviteetit sen ympärillä ovat olleet jo pitkään olemassa (Blair, 2011). Viitekehyksenä tiedon hallinta on uudehko monitieteinen ilmiö, joka on saavuttanut suosiota viimeisen vuosikymmenen aikana (Smallwood, 2014) eikä vakiintunutta määritelmää vielä ole olemassa (Guetat & Dakhli, 2015).

Tallon, Ramirez ja Short (2013) ovat erotelleen tutkimuksessaan kaksi tiedon hallinnan tavoitetta. Tutkimuksen johtopäätökset pohjautuvat alan asiantuntijoiden tuottamaan kirjallisuuteen. Ensinnäkin pyrkimyksenä on organisaatiossa tiedon arvon maksimointi varmistamalla, että tieto on luotettavaa, turvallista ja käytettävissä päätöstentekoa varten. Toiseksi tavoitteena on suojata tietoa, jottei sen arvo heikkene teknologisten ratkaisujen tai ihmisen tekemän virheen vaikutuksesta. (Tallon ym., 2013.)

Seuraavassa luvussa syvennytään eri tieteentekijöiden ja alan ammattilaisten muodostamiin tiedon hallinnan näkökulmiin, määrittelyihin sekä käsityksiin tiedon hallinnan viitekehyksestä.

3.3 Tiedon hallinta – mitä se on?

Tunnetun ICT-alan kansainvälisen tutkimus- ja konsultointiyrityksen Gartnerin mukaan IG on päätöksenteon vastuullisuuskehys, jolla varmistetaan asianmukainen toiminta tietojen arvostuksessa, luomisessa, käyttämisessä, tallentamisessa, arkistoinnissa ja poistamisessa. Se sisältää prosessit, roolit, politiikat, menetelmät, standardit ja mittaamisen, joilla varmistetaan tiedon vaikuttava sekä tehokas käyttö, jotta organisaatio voi saavuttaa tavoitteensa. (Gartner, 2018.)

Koska tiedon hallinnan taustalla vaikuttaa ideologia hyvästä liikkeenjohtotavasta, on IG:n rinnastettu olevan tiedon ja siihen liittyvien riskien hallintaa sekä tietoa koskevien lakien, sääntöjen ja määräysten noudattamista (engl. GRC for information, kirjain-sanayhdistelmä muodostuu sanoista governance, risk management, and compliance for information). Tällöin tiedon hallinnan osa-alueita on lueteltu muun muassa olevan tiedon suojaamisen, rekisterihallinnan, tiedonhallinnan, hyvän hallintotavan, yksityisyyden, tietämyksenhallinnan, yrityssisällön, dokumenttihallinnan, yritysriskihallinnan, arkistoinnin, jatkuvuudenhallinnan, tiedon varmistuksen, palautuksen ja varastoinnin, eDiscoveryn ja yrityshaun. (Blair, 2011.)

Tiedon hallinta on kokoelma kyvykkyyksiä tai toimia, joiden avulla luodaan, tallennetaan, arvostetaan, varastoidaan, käytetään, kontrolloidaan, hallitaan pääsyä, arkistoidaan ja poistetaan tietoa sen elinkaaren aikana (Tallon ym., 2013). Tiedon on tarkoitus tuottaa arvoa omistajalleen ja tietoa käyttäville tahoille. Kooper ym., (2011) kertovat IG:n olevan joukon aktiviteetteja, joiden tarkoituksena on luoda normatiivinen perusta helpottamaan ja stimuloimaan älyllistä vuorovaikutusta. Tiedon hallinta keskittyy etsimään ja löytämään, luomaan ja käyttämään sekä vaihtamaan tietoa, ei pelkästään tuottamaan sitä. He korostavat tiedon arvon optimoimista, ja IG voidaan nähdä viitekehyksenä, jolla optimoidaan mukana oleville toimijoille jollakin tavalla tiedon arvo. Toimintaan tulisi sisällyttää inhimillinen vuorovaikutus toimijoihin, dataan ja taustalla oleviin järjestelmiin. (Kooper ym., 2011.)

Johtava asiantuntija ja tietokirjailija Smallwood (2014) on kuvannut kirjassaan kattavan näkemyksen tiedon hallinnan konsepteista, strategioista ja parhaista käytännöistä. Hän korostaa tiedon hallinnan roolia siinä, miten organisaatio ylläpitää turvallisuutta, noudattaa asetuksia ja lakeja sekä täyttää eettiset normit. Smallwood linjaa tiedon hallinnan avulla etsittävän keinoja hallita ja kontrolloida tietovarantoja ristien pienentämiseksi. IG:n avulla varmistetaan säännösten noudattaminen ja parannetaan tiedon laatua sekä saavutettavuutta samaan aikaan, kun toteutetaan tietoturvaa suojaamaan ja säilyttämään tietoa, jolla on liiketoiminnallinen arvo. Tiedon hallinnan keskiössä ovat politiikat, menetelmät ja prosessit. Se sisältää rekisterin- ja sisällönhallinnan avainkonseptit, informaatiotekniikan ja tiedon hallitsemisen, informaatioturvan, tietosuojan, riskien hallinnan, valmiuden oikeudenkäyntiin, lainsäädännön noudattamisen ja pitkäaikaisen digitaalisen tiedon säilyttämisen. Tiedon hallinta on myös liiketoimintatiedon (engl. business intelligence) hyödyntämistä, jolloin liiketoimin-

taan liittyvää ulkoista ja sisäistä tietoa analysoidaan systemaattisesti. Tällöin tiedon hallinta sisältää myös siihen liittyvät teknologiat sekä tiettyjä kategorioita kuten dokumenttien hallinnan, tietämyksen ja liiketoiminnan jatkuvuuden hallinnan. (Smallwood, 2014.)

Myös Guetat ja Dakhli (2015) päättelevät tutkimuksessaan tiedon olevan nykyaikaisten organisaatioiden yksi tärkeimmistä aineettomista hyödykkeistä, koska sillä on ratkaiseva merkitys niiden kilpailuedussa ja selviytymisessä. Tieto tukee kaikkia organisaation päätöksiä sekä päivittäisellä operatiivisella että taktisella sekä strategisella päätöksentekotasolla. Tutkijat ovat kritisoineet, että monissa tiedon hallinnan viitekehyksissä on laiminlyöty tietoarkkitehtuurin (engl. information archtitecture) osuus. He korostavat arkkitehtuurin olevan tiedon hallinnan laajassa abstraktiossa merkittävä ydinelementti, joka toimii ajurina, ja jonka tarkoituksena on lisätä organisaation hallinnoimien tietojen liiketoiminta-arvoa. Ensinnäkin tietoarkkitehtuurin tehtävänä on luoda ja ylläpitää mukautuva ratkaisu, joka on suunniteltu helpottamaan tietojen saatavuutta, määrittelyä, hallintaa, turvallisuutta ja eheyttä koko organisaatiossa. Toiseksi se kattaa myös tietoresurssien määrittelemisen, jäsentämisen ja dokumentoinnin sekä ylläpidon laadukkaasti, ja kolmanneksi yleensä työt ja toimenpiteet toteutetaan useiden sovellusten, mallien, infrastruktuurien sekä ohjeiden avulla. Tutkijoiden mukaan tietoarkkitehtuurin systeemisessä analyysissä otetaan huomioon sekä tiedon rakenteellinen että systeeminen monimutkaisuus. (Guetat & Dakhli, 2015.)

Guetat ja Dakhli (2015) luettelevat tiedon hallintaa kehystävät neljä toiminnan elementtiä. Näille toiminnan artefaktille luovat rajoituksia sekä mahdollisuuksia niin ikään neljä muuta asiakokonaisuutta. Tiedon hallinnan skeema sijoittuu siten tiedon hallinnan viitekehyksessä kuvion 5 keskelle. Heidän kuvaamansa tiedon hallinnan viitekehyksen neljä toiminnan osa-aluetta ovat: 1) organisaatio ja liiketoiminta, 2) arkkitehtuuri, 3) kommunikaatio ja muutoshallinta ja 4) menetelmät ja työkalut. Näille rajoituksia tai mahdollisuuksia luovia elementtejä ovat 1) lakien ja sääntelyn noudattaminen, 2) tiedon laatu, 3) organisaation politiikka ja strategia sekä 4) tietoturva.

KUVIO 5 Tiedon hallinnan viitekehys (Guetat & Dakhli, 2015, s. 1092 mukaellen).

Kuviossa 5 esitetyissä rajoittavista mahdollistavista elementeistä organisaation politiikka ja strategia merkitsevät sitä että, tiedon hallinnan strategian tulisi olla linjassa organisaation strategian kanssa. Tässä määritellään päämäärät ja tavoitteet organisaation sisällön hallinnalle (engl. content management) sekä kuvataan siihen kohdistetut säännöt ja rajoitteet. Lait ja sääntely kuvaavat liiketoiminnalle asetetut sisäiset ja ulkoiset rajoitteet, jotka vaikuttavat tiedon hallinnan prosesseihin. Tiedon laatuun liittyy organisaatiotasolla paljon sekä tavoitteita että rajoitteita. Neljäs osa-alue tietoturva luettelee tietoturvavaatimukset ja rajoitukset, joita on tarkkailtava kaikissa muissa edellä esitetyissä kolmessa tiedon hallinnan aktiviteeteissä. (Guetat & Dakhli, 2015.)

Kehyksessä toiminnan elementit ovat keinoja ja välineitä, jotka mahdollistavat tiedon hallinnan aktiviteettien toteuttamisen organisaatiossa. Organisaatio ja liiketoiminta kuvaavat vastuita, rooleja, menettelytapoja, sekä inhimillisiä että materiaaliresursseja tiedon hallinnan aktiviteettien toteuttamiseksi. Arkkitehtuuri viittaa yritysarkkitehtuuriin sekä tietojärjestelmien arkkitehtuuristandardeihin ja periaatteisiin sekä sääntöihin, joilla rakennetaan organisaation tiedon säilytyspaikat ja integroidaan ne organisaation tietojärjestelmiin. Toisaalta näillä säännöillä on kiinteä yhteys tiedon mallinnukseen, prosessointiin, käyttöön ja vaihtoon sekä toisaalta myös tiedon säilytyspaikkojen rakentamiseen ja ylläpitoon. Kolmas toiminnan elementti kommunikaatio ja muutoksenhallinta kuvailee organisaation muutosprosessit ja aktiviteetit, joita ovat esimerkiksi viestintä ja koulutus, ja joiden avulla selvitään muutosvastarinnasta. Neljäs toiminnan elementti on menetelmät ja työkalut. Se sisältää lähestymistavat, menetelmät ja työkalut, jotka tukevat seurantaa, mittaamista ja arkkitehtuurisääntöjen sekä -standardien, oikeudellisten rajoitusten, tiedon laadun ja tietoturvan vaatimusten mukaista valvontaa. (Guetat & Dakhli, 2015.)

Seuraavissa luvuissa pureudutaan EU:n yleiseen tietosuoja-asetukseen, joka on uudenlaisena entistä tiukempana lainsäädännöllisenä viitekehyksenä patistanut organisaatioita kiinnittämään entistä enemmän huomiota tiedon hallintaan ja sen kehittämisen toimiin (Smallwood, 2014; Schoch, 2016; Khan, 2018).

3.4 EU:n yleinen tietosuoja-asetus GDPR

Henkilökohtaisten tietojen asianmukainen käsittely on yksi aikakautemme suurimmista haasteista (Antignac, Scandariato & Schneider, 2016). Kehittyvien teknologisten ratkaisujen lisäksi haasteeseen pyritään vastamaan erilaisilla säännöksillä henkilötietojen asianmukaisen käsittelyn turvaamiseksi. EU:n yleinen tietosuoja-asetus eli ”General Data Protection Regulation”, GDPR) on huomattava merkkipaalu henkilöiden yksityisyyden suojan kehittämisessä (Goddard, 2017). Kyseistä tietosuoja-asetusta kutsutaan myös nimellä 2016/679. Kansainvälisiä ja alueellisia lakeja ja yleissopimuksia tarvitaan sekä vaaditaan henkilötietojen suojelemiseksi ja yksityisyyden turvaamiseksi. Viimeisten kahdenkymmenen vuoden aikana hallitukset ovat rakentaneet ja kehittäneet kattavia tietosuojalakeja, ja lisänneet sekä julkisten että yksityisten organisaatioiden vel-

vollisuuksia tietosuojalainsäädännön noudattamiseksi niiden kerätessä ja käyttäessään henkilökohtaisia tietoja. (Kabanov, 2016.) Tietosuoja-asetus on lainsäädännöllinen virstanpylväs yksityisyyden ja henkilötietojen suojaamisessa, ja sen avulla pyritään luomaan uudenlainen ajattelutapa sekä kulttuuri koskien yksilön henkilötietoja (Martínez-Martínez, 2018).

GDPR-asetus koskettaa lähestulkoon jokaista yritystä ja organisaatiota unohtamatta eri yhteisöjä tai muita vastaavanlaisia tahoja, jotka käsittelevät henkilötietoja. Merkittävin vaikutus asetuksella lienee globaaleihin yrityksiin, joilla on laajat kansainväliset verkostot. Organisaatiot voivat olla monimutkaisia ekosysteemejä käsitellen suuria määriä erilaisia henkilötietoja. Ne saattavat käyttää ulkoistettuja kumppaneita tai tytäryhtiöitä, jotka ovat hajautettuja maantieteellisesti, ja joissa sovelletaan erilaisia lainsäädännöllisiä viitekehyksiä. Monimutkaisten dynaamisten toimintojen ja rakenteiden viidakossa voi olla hankalaa täyttää velvollisuudet. Tietosuoja-asetusta on noudatettava yli EU:n rajojen silloin kun operoinnin kohteena ovat EU-kansalaisten henkilötiedot, ja lähtökohtaisesti se koskee kaikenlaista henkilötietojen käsittelyä (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Tällöin siis myös EU:n ulkopuolisten ja kansainvälisten yritysten on noudatettava sekä omaa kansallista lainsäädäntöään että GDPR-asetusta (Tikkinen-Piri ym., 2018). Lainsäädännöllisen viitekehyksen tavoitteena on vahvistaa yksilön oikeuksia, lujittaa EU:n sisämarkkinoita sekä tavoittaa tietosuojan huomioiminen globaalisti että tehostaa tietosuojan noudattamisen valvontaa.

3.4.1 Henkilötiedot asetuksen ytimessä

Euroopan unionin yleinen tietosuoja-asetus on yksi esimerkki uudesta sekä tiukennetusta lainsäädännöstä, joka vaikuttaa laaja-alaisesti organisaatioiden henkilötietojen tiedon hallinnan systeemiin. Aiemmin yksilöillä on ollut vähän tai ei ollenkaan keinoja valvoa tietojaan, niiden keräämistä tai käyttöä. Kehittyneissä maissa henkilösuojaa koskevat sääntelyvaatimukset keskittyvät varmentamaan kansalaisille yhtäläisiä oikeuksia omiin henkilötietoihinsa (Kabanov, 2016). Vaatimustenmukainen (engl. compliance) toiminta ei suinkaan ole uusi haaste organisaatiolle, mutta GDPR-asetus on saanut yritykset maailmanlaajuisesti kiinnittämään huomiota entistä tiukempiin määräyksiin ja henkilötietojen käsittelyyn (Schoch, 2016; Khan, 2018).

EU:n yhtenä tavoitteena on edistää digitaalisten sisämarkkinoiden kehittymistä. Hyvin usein tuotetavia palveluita varten kerätään, siirretään, käytetään tai taltioidaan henkilökohtaisia tietoja. Henkilötietojen suoja on olennaista Euroopan digistrategiassa, ja se on nostettu esiin yleisemmällä tasolla myös Eurooppa 2020 -strategiassa (Euroopan komissio, 2012). ”Digitaalisten sisämarkkinoiden strategia Euroopalle” julkaistiin vuonna 2015 toukokuussa (Euroopan komissio, 2015). Se merkitsi uuden digitaalisen talouden lainsäädäntöpolitiikan alkua (Martínez-Martínez, 2018).

Digitalisaatio leviää toimialariippumattomasti. Sen nopeatahtisuus luo uusia haasteita sekä yrityksille että julkishallinnon organisaatioille, kun raken-

netaan asiakkaiden ja kumppaneiden luottamusta digitaalisia systeemejä kohtaan sekä varmistetaan asianmukaisesti henkilötietojen käsittelykäytännöt että tietosuojaprosessit lakien ja määräysten vaatimusten mukaisiksi. Jokaisen yrityksen tavoitteena on varmastikin menetellä sillä tavoin, että se ylläpitää kasvua ja kannattavuutta. Vaatimustenmukainen toiminta olisikin hyvä nähdä organisaatioissa monipuolisena kokonaisuutena, joka muuttuu jatkuvasti, ja jonka tulisi tukea kaikkia liiketoimintaprosesseja (Kabanov, 2016).

Sovellukset ja palvelut keräävät merkittäviä määriä henkilötietoja, joita käytetään ja jatkokäsitellään liiketoimintahyödyn saavuttamiseksi. (Kabanov, 2016). Smallwoodin (2014) mukaan Maailman talousfoorumi käsittää tiedon olevan uusi omaisuuserä sekä kilpailuvaltti, ja henkilötiedot ovat ”uusi öljy” ekosysteemeissä. Henkilötietojen on myös kuvattu olevan digitaalisen talouden uusi valuutta. On jopa sanottu, että sosiaalisen median palveluissa käyttäjät eivät ole asiakkaita, vaan tuotteita, joiden tietoja käytetään hyödyksi taloudellisen menestyksen tavoittelemiseksi. (Martínez-Martínez, 2018.) Jättämämme jäljet verkkoon ovat erittäin arvokkaita online-palveluiden tuottajille sekä mainoskoneistoille (Lievens & Verdoodt, 2018).

GDPR-asetus pyrkii turvaamaan yksilön fundamentaalisen oikeuden omien henkilötietojensa keräämiseen ja käyttöön. Euroopan Unionin perusoikeuskirjan artiklassa 8 (Euroopan parlamentti, neuvosto ja komissio, 2012) kuvataan seuraavasti yksilön perusoikeuksia henkilötietojensa osalta:

> 1. Jokaisella on oikeus henkilötietojensa suojaan.
>
> 2. Tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.
>
> 3. Riippumaton viranomainen valvoo näiden sääntöjen noudattamista. (Euroopan parlamentti, neuvosto ja komissio, 2012.)

Henkilötiedoilla GDPR-asetuksessa tarkoitetaan

> kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

EU:n yleinen tietosuoja-asetus on lainsäädännöllinen viitekehys, jolla pyritään lisäämään yksilön valtaa omiin henkilötietoihinsa. GDPR-asetus määrittelee henkilötiedoiksi kaikki tiedot, jotka voidaan linkittää tiettyyn henkilöön. (Quelle, 2016.) Henkilötietoa on mikä tahansa sellainen tieto, jonka avulla henkilön voi tunnistaa. Esimerkiksi nimen lisäksi kuva, verkkotunnisteet kuten IP-osoite tai sijanititieto, evästeet, ajoneuvon rekisteritunnus, sähköpostisoite, biometri-

nen tieto ja dna ovat henkilötietoja. Sellaisia tietoja, jotka ovat GDPR:n mukaan arkaluonteisia henkilötietoja, tulee käsitellä ja suojella erityisellä huolellisuudella. Lähtökohtaisesti edellä mainittujen tietojen käsittely on kielletty, ellei siihen ole olemassa erityisen painavaa syytä (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

Asetuksessa määritellyn henkilötietokäsitteen lisäksi otan tarkastelun alle informaatioidentiteetin, joka koostuu rekisteröidyn yksittäisten henkilötietojen summasta. Informaatioidentiteetin tiedot, joita voidaan hyödyntää muun muassa profiloinnissa, voivat olla monenlaisia. Tällaista tietoa edustavat esimerkiksi henkilöllisyystodistukset, identiteetin digitaaliset tunnisteet, kuten verkkojen käyttäjätilit sekä asetukset ja attribuutit, jotka liittyvät käyttöön tai käyttäytymistietoihin. (Wachter, 2018.) Teknologiaa hyödyntämällä ja sopivilla tietojen yhdistelmillä voidaan informaatioidentiteettiin pohjautuen saada selville identiteetin fyysinen ilmentymä eli luonnollinen henkilö.

EU:n yleisessä tietosuoja-asetuksessa henkilötietojen käsittelyyn kohdentuvat laiminlyönnit ovat arvostettu korkealle. Mikäli organisaatio ei toimi GDPR-asetuksen vaatimustenmukaisesti, voi seuraamusmaksu korkeimmillaan olla vakavissa rikkomuksissa neljä prosenttia kokonaisliikevaihdosta tai 20 miljoonaa euroa riippuen siitä, kumpi laskentatavasta tuottaa suuremman maksuun pantavan erän rangaistavalle taholle (Talus ym., 2017). Vähäpätöisemmissä rikkomustapauksissa sanktio on kaksi prosenttia tai kymmenen miljoonaa euroa liikevaihdosta. Myös lievempiä keinoja, esimerkiksi huomatusta, voidaan käyttää (Oikeusministeriö, 2018a) tai tietosuojaviranomainen voi määrätä henkilötietojen käsittelyn lopettamisen.

GDPR-asetuksen merkittävän maailmanlaajuisen vaikutuksen varmistavat laajennettu henkilötietojen määritelmä ja laaja alueellinen soveltamisala. Voidaan todeta, että asetuksen myötä on alkanut uudenlainen henkilötietojen suojaamisen aikakausi. (Goddard, 2017.) GDPR-asetus on perustavaa laatua oleva luoden uudenlaisen asetelman organisaatioiden ja yksilöiden välille yli EU:n rajojen. Tietosuoja-asetusta tulee soveltaa silloin, kun käsitellään rekisteröityyn liittyviä tietoja. Asetus tuo uusia oikeuksia rekisteröidyille luonnollisille henkilöille ja velvoitteita sekä rekisterin pitäjän että käsittelijän roolissa toimiville. (Talus ym., 2017.) Tietosuoja ja yksityisyys kulkevat käsi kädessä EU:n yleisessä tietosuoja-asetuksessa. Asetuksella pyritään kattamaan kaikki henkilötietojen käsittelyyn liittyvät globaalin nykymaailman ratkaisut. Se on viitekehys, jolla pyritään varmistamaan henkilötietojen yksityisyyden suoja. Tietosuoja ei ole pelkästään tekniikkaa ja teknologiaa, vaan keskustelu sen ympärillä pohjautuu myös fundamentaaliseen käsitykseen ihmisen perusoikeuksista.

Oikeus henkilökohtaisten tietojen siirrettävyyteen on yksi GDPR-asetuksen uutuuksista. Henkilökohtaisen puhelinnumeron siirtäminen operaattorilta toiselle on onnistunut jo kauan, ja nyt uuden asetuksen myötä oikeus on ulotettu koskemaan kaikenlaisia digitaalisia palveluita. GDPR-asetus voidaan nähdä teoriatasolla ensimmäisenä askeleena kohti yksilön oletettua oikeutta omistaa omat henkilötietonsa ja vaikuttaa niiden käyttöön. Se on merkityksellistä sekä yrityksille, jotka harjoittavat toimintaa digitaalisilla markkinoilla, että

yksilöille, joista tietoja on kerätty. (De Hert ym., 2018.) Henkilökohtaisen datan ja informaation siirrettävyys voi mahdollistaa suurten tietoaineistojen (engl. big data) maksimaalisen hyödyntämisen läpinäkyvällä ja puolueettomalla tavalla. Henkilökohtaisten tietojen siirrettävyys voi olla tilaisuus edistää palveluiden yhteen toimivuutta, lisätä digitaalisten palveluiden välistä kilpailua sekä kehittää yhä enemmän käyttäjäkeskeisiä foorumeja (Tikkinen-Piri ym., 2018). Ilman selkeää teknologian käytön sääntelyä riskinä on, että ihmisiä ilman yksilön suostumusta tai muuta pätevää perustetta syyttä suotta tunnistetaan, seurataan, jäljitetään, valvotaan, manipuloidaan ja leimataan (Kindt, 2018).

Haasteet GDPR-asetuksen käyttöönotossa ja soveltamisessa ovat kaikenkokoisille organisaatioille samankaltaisia. Henkilötietojen suojaamisen sääntelyn määrä ja monimutkaisuus ovat lisääntyneet erityisesti Euroopan Unionissa, Yhdysvalloissa (Schoch, 2016) ja muissa kehittyvissä maissa. Globaalien yritysten on noudatettava erilaisia kansallisia sääntelyitä sekä lakeja ja varmistettava vaatimusten mukainen toiminta kansainvälisissä liiketoimintaympäristöissä (Kabanov, 2016). Tietosuoja-asetus on lainsäädännöllinen viitekehys, jonka yhtenä tavoitteena on ottaa huomioon ennennäkemättömän teknisen kehityksen vaiheet (Poullet, 2018).

3.4.2 Direktiivit asetuksen edeltäjinä

Olennaisimmat kaksi direktiiviä GDPR-asetuksen takana ovat 95/46/EC ja 2002/58/EC (Bihari, 2018). Direktiivi on luonteeltaan ohjaava, eikä se suoraan muuta EU:n jäsenvaltion lainsäädäntöä, vaan valtion on direktiivin ohjauksen mukaisesti laadittava lakinsa. Sen sijaan tietosuoja-asetusta tulee noudattaa, ja se astuu voimaan jokaisessa jäsenmaassa voimaan sellaisenaan.

Käytännössä EU:n yleinen tietosuoja-asetus korvaa vuonna 1995 voimaan tulleen tietosuojadirektiivin 95/46/EC (Kabanov, 2016; Bihari, 2018). Suomessa direktiiviä kutsutaan myös henkilötietodirektiiviksi 95/46/EY. Direktiivin 95/46/EY tavoitteena on ollut Euroopan unionin alueella edesauttaa tietojen vapaata liikkuvuutta sekä turvata yksilöille heidän perusoikeutensa ja -vapautensa henkilötietojen käsittelyyn liittyen. Erityisesti on haluttu turvata luonnollisten henkilöiden oikeus yksityisyyteen. Direktiivin toisena samanarvoisena tavoitteena Euroopan yhdentymiskehityksen vuoksi on ollut vahvistaa sisämarkkinoiden toteuttamista, joka direktiivissä tarkoittaa henkilötietojen vapaata liikkuvuutta. (Euroopan parlamentti ja neuvosto, 1995.) Euroopan unionin jäsenvaltiot ovat velvoitettu muuttamaan kansallinen lainsäädäntönsä vastaamaan vuoden 1995 tietosuojadirektiiviä. Suomessa kansallinen lainsäädäntö on linjattu vastaamaan direktiiviä 1.6.1999 voimaan tulleella henkilötietolailla 523/1999. (Tietosuojavaltuutetun toimisto, 2015.)

GDPR-asetuksen taustallavaikuttajana voidaan nähdä myös olevan sähköisen viestinnän tietosuojadirektiivin 2002/58/EC (Bihari, 2018), suom. 2002/58/EY. Vuonna 2009 päivitetyn sähköisen viestinnän tietosuojadirektiivin (Poullet, 2018) avulla pyritään luomaan yhdenmukaistettu järjestelmä viestintäverkkojen eli siirtojärjestelmien sääntelytoimenpiteitä varten tarkoituksenaan

turvata yksityisyyden suojaa (Euroopan parlamentti ja neuvosto, 2015). Suomessa kansallinen lainsäädäntö on saatettu 1.9.2004 vastaamaan sähköisen viestinnän tietosuojadirektiiviä 2002/58/EY sähköisen viestinnän tietosuojalailla.

Vaikkakin GDPR-asetus 2016/679 tuli voimaan sellaisenaan, on jäsenvaltioissa mahdollista kansallisella tasolla täydentää lakia ja säätää tiettyjä poikkeuksia (Oikeusministeriö, 2018a). Samana päivänä 25.5.2018 kun GDPR-asetus tuli voimaan, oli Suomessa tarkoituksena julkaista uusi tietosuojalaki, jonka vaikutuksen alaisena kumottaisiin voimassa oleva henkilötietolaki ja lait tietosuojalautakunnasta sekä tietosuojavaltuutetusta (Tietosuojavaltuutetun toimisto, 2018). Kansallisen liikkumavaran perusteella Suomessa on esitetty, ettei seuraamusmaksua sovellettaisi julkisella sektorilla, koska viranomaisia sitovat virka- ja vahingonkorvausvastuu sekä hallinnon lainmukaisuusvaatimukset (Oikeusministeriö, 2018a). Uuden tietosuojalain julkaiseminen viivästyi, mutta tällä asialla ei ollut vaikutusta EU:n tietosuoja-asetuksen käyttöönottoon toukokuussa 2018 tapaustutkimusyrityksessä. Tutkielmaraportin puhtaaksikirjoittamisen aikana uusi kansallinen tietosuojalaki, joka tarkentaa henkilötietojen käsittelyn velvoitteita täydentäen Euroopan unionin yleistä tietosuoja-asetusta, ja jota sovelletaan rinnakkain tietosuoja-asetuksen kanssa, on tullut voimaan 1.1.2019 (Finlex, 2018).

3.4.3 Tarve EU:n yleiselle tietosuoja-asetukselle

Teknologisen kehityksen myötä oli noussut esiin tarve mennä kohti yhtenäistä ja johdonmukaisesti sovellettavaa tietosuojamallia. Vuonna 1995 julkaistu tietosuojadirektiivi kehitettiin ennen internetin, pilvipalveluiden ja suurten tietomassojen (engl. big datan) aikakautta. Luonteeltaan ohjaava direktiivi on ollut Euroopassa merkittävä rajapyykki henkilötietojen suojaamisen historiassa, koska aiemmin tietojen suojaamisen täytäntöönpano on ollut hajanaista eri puolilla Euroopan unionia. (Poullet, 2018.) Vuosina 2009 ja 2010 Euroopan komissio ja EU:n tietosuojaviranomaisista koostuva tietosuojaryhmä pyrki lisäämään rekisteröityjen henkilöiden oikeuksia. Etsittiin myös varmistamaan keinoja, joilla rekisterinpitäjät ottavat käyttöön tehokkaita politiikkoja sekä mekanismeja, ja joiden avulla varmistetaan myös tietosuojasääntöjen noudattaminen. (Quelle, 2016.) Työn seurauksena julkaistiin COM (2010) 609 tiedonanto ”Kattava lähestymistapa henkilötietojen suojaan Euroopan unionissa”. Suosituksen mukaan yksilön tietosuojan perusoikeutta tulisi noudattaa täysimääräisesti sekä EU:ssa että myös EU:n ulkopuolella. (Euroopan komissio, 2010.)

Vuosi 2010 toimi lähtölaukauksena uudelle tietosuoja-asetukselle. Rekisteröityjen oikeuksia tuli parantaa sekä lisätä rekisterin pitäjien vastuuvelvollisuuksia (Quelle, 2016). Vuonna 2010 Euroopan komissio antoi ehdotuksen tietosuojasääntelyn uudistamiseksi, koska sääntely oli jäänyt teknologisten sekä muiden ympäristötekijöiden jalkoihin, eikä se enää pystynyt vastaamaan olosuhteissa ja toimintamalleissa tapahtuneisiin muutoksiin. Sen lisäksi, että uudistus pyrki turvaamaan henkilötietojen suojan perusoikeutena, niin sen myötä

pyrittiin myös turvaamaan digitalisoituneen talouden kehittyminen sekä tehostamaan rikollisuuden ja terrorismin torjuntaa. (Euroopan komissio, 2012.)

Neljä vuotta kestäneen työn tuloksena 25.5.2016 julkaistiin yleinen tietosuoja-asetus. EU:n jäsenvaltioille annettiin aikaa kaksi vuotta valmistella henkilötietojen käsittelyn käytännöt vastaamaan GDPR-asetusta. Uutta tietosuoja-asetusta, joka edistää Euroopassa entisestään tietosuojan standardointia (Poullet, 2018) alettiin soveltaa 25.5.2018. Unionin valmistelema laki ulottaa lonkeronsa globaaliin maailmaan Euroopan ulkopuolelle tavoitteenaan turvata unionin kansalaisten perusoikeuksiin kuuluvan henkilötietojen suojaamisen. GDPR-asetus koskee kaikkia organisaatioita tai muita tietojenkäsittelijöitä aina, kun henkilötietojen käsittely kohdistuu EU-alueen asukkaisiin (Poullet, 2018).

Talouden globalisoituminen ja digitalisoituminen on vaikuttanut kaikkiin tuotannon ja palveluiden sektoreihin. Yhteen liitetyt tietokoneet ja verkkoon liitetyt objektit tarjoavat aivan uudenlaisen innovatiivisen ajattelutavan informaation käsittelylle ja hyödyntämiselle (Euroopan yhteisöjen komissio, 2009). Euroopan unioni odottaa tapahtuvan suuria investointeja muun muassa älykkäiden kotien, henkilökohtaisten hyvinvoinnin ja päälle puettavien asioiden, älykkään energian, älykkäiden kaupunkien ja älykkään liikenteen aloilla (Wachter, 2018). GDPR-asetuksen tarkoituksena on ottaa huomioon teknologian kehittymisen myötä digitaalinen maailma ja sen uudenlaiset asiat, kuten esineiden internet (engl. internet of things, IoT), pilvipalvelut ja tietotekniikan, nanoteknologian, bioteknologian sekä kognitiotieteen sovellutukset (Poullet, 2018). Nämä ovat asioita, jotka laajentavat merkittävästi henkilötietojen keräämisen mahdollisuuksia ja niiden prosessointia, taltioimista sekä tietojen hyväksikäyttöä. Samalla ne myös asettavat haasteita henkilötietojen suojaamiselle sekä yksityisyyden turvaamiselle.

Henkilötietojen suojaamisen lisäksi asetuksen tavoitteena on harmonisoida tietojen suojaamista EU:ssa (Tikkinen-Piri ym., 2018). Teknologisen kehityksen ja ripeästi laajentuneen digitalisaation vuoksi nousi esiin tarve koordinoivalle, kattavalle ja johdonmukaiselle henkilötietojen käsittelyn viitekehykselle. Tietosuojalainsäädäntö oli jäänyt kehityksen jalkoihin. Se ei enää kyennyt vastaamaan muuttuneen globaalin tietojenkäsittelyn ympäristöjen olosuhteisiin eikä liiketoimintamalleihin.

3.5 GDPR:n tietosuojaperiaatteet

EU:n yleinen tietosuoja-asetus patistaa organisaatiot ottamaan tietoturva-asiat huomioon jo järjestelmien ja palveluiden suunnitteluvaiheessa. Kaksi velvollisuutta ovat ylitse muiden (Goddard, 2017). Asetuksessa suunnitteluvelvollisuus (engl. privacy by design) tarkoittaa henkilötietojen suojan rakentamista systeemin alusta lähtien (Blix, Elshekeil & Laoyookhong, 2017). Toiseksi toimintaa tulee toteuttaa siten, että sisäänrakennetun tietosuojan periaate toteutuu oletusarvoisesti (engl. privacy by default). Organisaatioiden

tulee huolehtia siitä, että ne rekisterinpitäjinä keräävät ja käsittelevät asianmukaisesti henkilötietoja ja niiden käytön tulee olla perusteltua.

Lukuun ottamatta tiettyjä poikkeuksia GDPR-asetuksen mukaan geneettisten ja biometristen tietojen käsittely on kielletty. Lisäksi sellainen henkilötietojen käsittely, josta käy ilmi rotu, etninen alkuperä, ammattiliiton jäsenyys, poliittinen tai seksuaalinen suuntautuneisuus tai vakaumus on lähtökohtaisesti kiellettyä. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016.) Käsittelykiellon suhteen on olemassa lukuisia poikkeuksia. Esimerkiksi arkaluontoisiksi luokiteltuja henkilötietoja voidaan käsitellä, mikäli rekisteröity yksilö on antanut tähän suostumuksensa. Lisäksi henkilötietojen käsittely on sallittua, mikäli on olemassa lakiin perustuva velvollisuus tai oikeutus niiden käsittelyyn.

Kahden tietosuojaperiaatevelvollisuuden kehittelyn juuret johtavat Yhdysvaltojen hallituksen vuonna 1973 esittelemään FIP-perusteisiin (engl. fair information practices). GDPR-asetus velvoittaa yritykset integroimaan nämä periaatteet liiketoimintaprosesseihinsa. (Tikkinen-Piri ym., 2018.) Sisäänrakennetun (engl. privacy by desing) tietosuoja-ajatusmallin esitteli vuonna 1990 Ann Cavoukian. Se sisältää seitsemän yleisluontoista ohjenuoraa yksityisyyden turvaamiksesi suunnittelun alkuvaiheista lähtien (Cavoukian, 2010). Konseptia on hyödynnetty laajalti (Blix ym., 2017) ja myös GDPR-asetus näyttää saaneen vaikutteita siitä. Asetuksen artikla 5 sisältää seuraavat kuusi tietosuojaperiaatetta, jotka ohjaavat käsittelemään henkilötietoja tietosuoja-asetuksen vaatimustenmukaisesti:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys,
- käyttötarkoitussidonnaisuus,
- tietojen minimointi,
- säilytyksen rajoittaminen,
- eheys ja luottamuksellisuus,
- täsmällisyys (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016.)

Rekisterin pitäjällä on osoitusvelvollisuus siitä, että se on noudattanut edellä mainittuja periaatteita (Blix ym., 2017; Talus ym., 2017). Täten rekisterin pitäjän velvollisuuksiin kuulu osoittaa, että henkilötietojen käsittelyn tietosuojaperiaatteet ovat valideja ja henkilön yksityisyys on turvattu.

Yksityisyyden turvaamiseksi ja oikeudellisten säännösten noudattamisen varmistamiseksi GDPR-asetukseen on sisällytetty tietosuoja teknologian ytimeen (Poullet, 2018). Verkkoon liitetyt sensorein varustetut älykkäät objektit keräävät ja levittävät meidän jokapäiväisestä elämästä, mielipiteistä ja mieltymyksistä yhä enenevissä määrin tietoja lisäten yksityisyyden loukkaamisen riskiä. Henkilötietojen käsittelyn prosessit (Tsormpatzoudi ym., 2016) sekä niiden käsittely-ympäristöt tulisi suunnitella sillä tavoin, että heti alusta lähtien yksityisyyden turvaaminen otetaan huomioon (Antignac ym., 2016). Yksityisyyden suojan voidaan käsittää koostuvan kuudesta ulottuvuudesta:

- Henkilötietojen keräämisestä.

- Tietoisuudesta siitä, että henkilötietoja kerätään ja miten niitä säilytetään.
- Henkilötietojen käytön valvonnasta.
- Henkilötietojen toissijaisesta käytöstä (käytetään henkilötietoja muuhun tarkoitukseen, kuin mitä alun perin ne on kerätty) ja niiden jakamisesta kolmansille osapuolille.
- Henkilötietojen suojaamisesta sääntöjenvastaiselta käyttöoikeudelta.
- Virheistä henkilötiedoissa ja mahdollisuudesta korjata virheelliset tiedot. (Sokolovska & Kocarev, 2018.)

GDPR-asetuksessa korostetaan riskiperusteista lähestymistapaa (Gellert, 2018). Sisäänrakennetun ja oletusarvoisen tietosuojan saavuttaminen sekä myös muiden GDPR-asetuksen tuomien velvollisuuksien toteuttaminen vaatii arvion henkilötietoihin kohdistuvista riskeistä (Talus ym., 2017). Riski voidaan määritellä tapahtumaksi, jolla on tietty vakavuusaste, useita esiintymistodennäköisyyksiä ja useita seuraamuksia. Riskienhallinnan tai riskianalyysin tehtävänä on tunnistaa riskit ja päättää toimenpiteistä riskien minimoimiseksi. Tietosuojaa koskeva vaikutustenarvio (engl. data protection impact assessment, DPIA), jota aiemmin kutsuttiin nimellä PIA (engl. privacy impact assessment (Kindt, 2018) on ensimmäinen asetuksessa vahvistettu riskinhallintatyökalu. (Gellert, 2018.) Sen tarkoituksena on toimia organisaatioissa riskien arviointi- ja päätöksentekotyökaluna (Blix ym., 2017). Ideaalitilanteessa vaikutustenarvioinnin avulla arvioidaan datan prosessoinnin riskit ja esitetään ratkaisuja tunnistettujen riskien pienentämiseksi (Wachter, 2018). Esimerkiksi sellaisissa tilanteissa, joissa henkilötietojen käsittelyyn liittyy rekisteröityjen kannalta merkittäviä tietosuojariskejä, tai joissa yksilön henkilökohtaisten ominaisuuksien arviointi perustuu automaattiseen tietojenkäsittelyyn, kuten profilointiin, täytyy suorittaa vaikutustenarviointi (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Riskit toteutuvat, mikäli määräyksiä ei noudateta tai toiminta on niiden vastaista. Vaatimustenmukaiseen toimintaan liittyvät riskit voivat olla hallinnollisia, taloudellisia, oikeudellisia tai maineeseen liittyviä riskejä (Blair, 2011; Tallon, 2013; Smallwood, 2014; Schoch, 2016). Periaatteet sisäänrakennetusta ja oletusarvoisesta tietosuojasta kannustavat organisaatioita sekä järjestelmän, sen komponenttien, että erilaisten palveluiden tuottamisessa ottamaan huomioon tietoturvan. Periaatteet myös kannustavat organisaatiossa kollaboraatioon, jolloin elementtien välinen inhimillinen vuorovaikutus toteutuu. (Kooper ym., 2011.) Organisaation eri toiminnoista vastaavien tahot saadaan keskustelemaan ja suunnittelemaan yhdessä parhaan mahdollisen tavan henkilötietosuojan toteuttamiseksi - sekä teknisesti että toiminto- ja prosessilähtöisesti, GDPR-asetuksen vaatimusten mukaisesti.

3.6 GDPR-asetuksen soveltamisen haasteista

Henkilötietojen ja yksityisyyden turvaaminen vaikuttaa haastavalta tehtävältä. Uudet teknologiset ratkaisut aiheuttavat monimutkaisia henkilötietojen keräämiseen ja käyttöön liittyviä haasteita eri toimialoilla samanaikaisesti vaikuttaen toinen toisiinsa monimutkaistaen entisestään asioita (Martínez-Martínez, 2018). Systeemit relaatioineen saattavat olla erittäin monimutkaisia. Merkittävimpiä datan keräämisen ja sen hyödyntämisen ilmiöitä lienevät massadata (engl. big data), pilvipalvelut (engl. cloud computing), tekoäly (engl. artificial intelligence), koneoppiminen (engl. machine learning), esineiden internet (engl. internet of things, IoT), web-analytiikka (engl. web analytics) sekä tehokkaat algoritmit. Verkostot, joissa toimimme sekä äärettömän pienet sirut tai muut objektit käyttämissämme tavaroissa ja esineissä ja jopa kehossamme mahdollistavat todella kattavan informaation keruun (Poullet, 2018).

GDPR-asetuksen määrittelyn mukaisen tietosuojan ja yksityisyyden turvaaminen on haastavaa monestakin syystä. Asetus ohjeistaa sääntöjen toteuttamista, mutta se ei suoraan anna erityisiä ohjeita itse säännösten täytäntöönpanosta, vaan käytännössä todelliset ratkaisut säännösten käyttöönotosta on organisaatioiden itse määriteltävä (Tikkinen-Piri ym., 2018). Lain luonnostelusta valmiiseen lakitekstiin on ollut pitkä matka. Sanmuodot ovat matkan varrella valittu siten, että ne tyydyttävät eri instanssien vaatimuksia (Bihari, 2018). Asetuksen valotetaan jättävän tulkinnan varaa käsitteiden suhteen (Kindt, 2018; Wachter, 2018), joka voi johtaa erheellisiin käsityksiin. Ohjelmistoarkkitehtuurin teknisten konseptien ja voimassa olevien sekä tulevien lakien ja määräysten ja teknisten käsitteiden välillä voi olla eroavaisuuksia tai ristiriitoja (Antignac ym., 2016; Blix ym., 2017). Käsitteelliset ja terminologiset haasteet voivat kasvaa, kun lakitekstiä käännetään kuvauksiksi ja ohjeiksi eri tieteenalojen sidosryhmille, kuten insinööreille tai liike-elämän toimijoille (Tsormpatzoudi ym., 2016). On päätelty, että yksityisyyden suojan turvaamiseksi esimerkiksi IoT-maailmassa tulisi kiireellisesti yksityiskohtaisesti määritellä ja implementoida ne IoT-teknologioiden suunnitteluun ja käyttöönottoon (Wachter, 2018). Lisäksi asetuksen sanamuodot näyttävät jättävän toisinaan turhan paljon tulkinnan varaa (De Hert ym., 2018) ja saattavat johtaa laajoihin epäselvyyksiin (Bihari, 2018). Teksti ei kovin selkeästi kerro varsinaisesta toimeenpanosta, ja lausekkeiden tulkinta voi herättää epävarmuutta (Lievens & Verdoodt, 2018).

Älykkäiden ympäristöjen järjestelmät käyttävät paljon dataa ja henkilökohtaisia tietoja. Järjestelmät auttavat ihmisiä päivittäisissä toimissa, jalostavat heidän kokemuksiaan ja sopeutuvat ihmisten tarpeisiin. Nämä suuret datamäärät ruokkivat muun muassa big datan ja pilviteknologioiden käyttöä. (Tikkinen-Piri ym., 2018.) Muun muassa kyberturvallisuudessa olevat heikkoudet sekä pseudo- ja anonymisointitekniikat saattavat olla riittämättömiä yksilön identiteetin suojelutarkoitusta varten (Hadziselimovic, Fatema, Pandit & Lewis, 2017; Wachter, 2018). Lisäksi on harmiteltu, ettei GDPR-asetuksessa ole käsitelty tek-

nisiä standardeja, sertifikaatteja tai nimiöitä, joilla varmistettaisiin päätelaitteiden ja ohjelmistosovellusten yhteensopivuus lakisääteisten vaatimusten kanssa (Poullet, 2018).

Bioteknologia on yksi poikkitieteellisestä alasta, jonka soveltaminen on hyvin yleistä eri toimialoilla. Biometrisen datan käytön lisääntyminen kuluttajasegmentillä sekä eri tahojen käyttämissä valvontasovelluksissa on lisääntynyt voimakkaasti (Kindt, 2018). ICT-alalla bioteknologian avulla voidaan nostaa tietoturvan tasoa ja luoda tunnistus- sekä todentamismenetelmistä vaivattomia. Kiitos ripeästi kehittyneiden teknologioiden biometristen tietojen käyttäminen mahdollistaa muun muassa automatisoidun henkilön tunnistamisen sekä tarkkailun. (Štitilis & Laurinaitis, 2017.) Pelkästään esimerkiksi sormenjälkeä tai valokuvaa ei välttämättä luokitella biometriseksi dataksi. Biometrisestä tiedosta tai tiedoista muodostuu silloin henkilötieto, kun datan avulla voidaan suorittaa identifiointi.

Biometrinen tieto voi olla luokiteltavissa myös arkaluonteiseksi henkilötiedoksi (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Otaksutaan, että voi olla haastavaa löytää tasapaino biometristen tietojen ja vapaan liikkuvuuden sekä kansalaisten suojaamisen välillä (Hadziselimocic ym,. 2017). On puntaroitu, ettei biometristen tietojen määrittelyn tulisi tapahtua pelkästään tietojen käytön perusteella, vaan myös biometristen tietojen keräämistä ja säilyttämistä tietokannoissa tulisi säännöstellä erikseen (Kindt, 2018). Yksilöiltä kerättyjen tietojen tunnistettavuuteen täytyy kiinnittää huomiota myös tiedekentällä, ja onkin muun muassa pohdittu rajoittaako asetus jollakin tapaa tieteen tekemistä (Hadziselimovic ym., 2017). Jäsenvaltioiden on mahdollista tarkentaa biometristen tietojen käsittelyä valtiollisella tasolla (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). On puntaroitu, tulisiko sellaisissa tapauksissa, joissa riski yksityisyydelle on pieni, sallia biometristen teknologioiden käyttö prosessoitaessa henkilödataa (Štitilis & Laurinaitis, 2017). Tällöin voitaneen kuitenkin kyseenalaistaa, toteutuisiko lain henki yksilöiden kohdalla sillä tavoin kuin on alun perin suunniteltu. Taltioiduilla biometrisillä tiedoilla on varmastikin paljon hyötyä ja niiden käytölle on olemassa erityistarkoituksissa oikeudellinen peruste, kuten viranomaisten suorittamassa rikostutkinnassa. Riskinä on, että teknologian käyttö ilman selkeää oikeudellista kehystä voi johtaa pahimmillaan väärinkäytöksiin (Kindt, 2018), jolloin yhtenäinen käytäntö pirstaloituu asettaen yksilöt ja organisaatiot eriarvoiseen asemaan.

Erityisesti IoT -toimialaan GDPR-asetuksella odotetaan olevan huomattava vaikutus. Tutkimuslaitos Gartnerin ennusteen mukaan IoT-ratkaisuja, jotka keräävät tai välittävät dataa, on vuonna 2018 käytössä 8,4, miljardia yksikköä (Junwoo, Kyoungmin, Mookyu, Moosung & Kyungho, 2017). Esineiden internetin (Internet of Things, IoT) tunnistus- ja kulunvalvontatekniikat tarjoavat infrastruktuurin, jonka avulla yhdistetään data käyttäjän laitteiden ja identiteetin välillä. Laitteet voivat kerätä suuren määrän monenlaista henkilökohtaista dataa, kuten sijainti- ja terveystietoja. (Wachter, 2018.) Suuri määrä dataa analysoidaan, jotta ymmärrettäisiin paremmin systeemejä sekä käyttäjien käyttäytymistä. Toiminnan tavoitteena on arvon tuottaminen kuluttajille ja liiketoiminnan tuot-

tavuuden kasvattaminen (Junwoo ym., 2017.) IoT-laitteet ja -palvelut tuottavat dataa, joka voidaan muuntaa kuvaavaksi informaatioksi. Käyttäjän informaatioidentiteetti rakennetaan tai muunnetaan lisäämällä häntä kuvaavia tietoja. Informaatio ja kommunikaatioteknologiat luovat uusia informaatiovirtoja, jotka kuvaavat käyttäjiä, joka edelleen vaikuttaa siihen, kuinka yksilö kokee identiteettinsä ja millaisena muut ymmärtävät sen. Tämä saattaa johtaa syrjivään profilointiin. (Wachter, 2018.)

Teknologiset ratkaisut tarjoavat datan keräys- ja tallentamisenkapasiteettia valtavat määrät. Tietoja voidaan kerätä, käsitellä ja tallentaa yksityiskohtaisesti profiileihin esimerkiksi ottamalla käyttöön evästeet tai muita käyttötarkoitukseen soveltuvia seurannan työkaluja (Lievens & Verdoodt, 2018). Datan profilointimenetelmät, jotka pohjautuvat linkitettyihin tiedostoihin, voivat paljastaa odottamattomia yksityiskohtia käyttäjien identiteetistä ja yksityiselämästä. Tämän kaltaiset profilointimenetelmät voivat olla ristiriidassa yksityisyyden suojaan, ja sen rikkoutuminen voi johtaa taloudelliseen, sosiaaliseen ja muuhun syrjivään kohteluun. (Wachter, 2018.) Profiileja hyödyntämällä voidaan luokitella yksilöitä ja ennustaa käyttäytymistä tilastollisilla menetelmillä. Profiilit ovat arvokkaita verkkopalvelujen tarjoajille ja markkinointikoneistoille. (Lievens & Verdoodt, 2018.) Web-analytiikka ja yleisömittausdata (engl. audience measurement) koskettavat jokaista internetin käyttäjää (Martínez-Martínez, 2018). Henkilöllä on oikeus vastustaa tietojensa käyttöä profiloinnissa, mutta välttämättä kansalainen ei edes hahmota monimutkaisia verkostoja, joissa hänen tietojaan liikutellaan tai minkälaisia jälkiä hän jättää käyttäessään erilaisia sähköisiä palveluita tai elektroniikkaa sisältäviä hyödykkeitä. Lisäksi profiloinnin käsite vaikuttaa olevan epäselvä laissa eikä profiloinnin sääntely vaikuttaisi suojelevan tehokkaasti rekisteröityjä yksilöitä (Poullet, 2018). Profilointia GDPR-asetuksen mukaisesti voidaan tehdä, mikäli rekisterinpitäjä voi osoittaa profiloinnilla olevan perusteltu ja huomattavan tärkeä syyn (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

Informaatio- ja kommunikaatioteknologiat luovat uudenlaisia käyttäjiä kuvaavia informaatiovirtoja. Muun muassa big dataa hyödyntävissä sovelluksissa anonymisoitujen tietojen käyttö on yhä yleisempää. (Poullet, 2018). Big data käsitteenä viittaa yritysten, hallitusten ja muiden suurten organisaatioiden valtaviin tietojärjestelmiin, joissa informaatiota analysoidaan tietokonealgoritmien avulla. Käsite ei viittaa pelkästään datan suureen määrään, vaan myös tiedon käsittelyn kompleksisuuteen (Pormeister, 2017.) Big dataa voidaan käyttää yleisten suuntausten ja korrelaatioiden tunnistamiseen. Sitä voidaan käsitellä siksi, että sen avulla yritetään vaikuttaa suoraan yksilöihin (Pormeister, 2017), kuten mielipiteisiin, ajatuksiin, käyttäytymiseen tai tekoihin. Lähes jokainen verkkosivusto ja mobiilisovellus hyödyntää jonkinlaista käyttäjien seurantaa etenkin silloin, kun tietoja käytetään kaupallisiin tarkoituksiin ja havitellaan liiketoimintahyötyä (Passmann, Lauber-Roensberg & Strufe, 2017). Yhdistettynä anonymisoitu henkilötieto anonymisoimattomaan tietoon, voidaan sopivilla tietojen yhdistelmillä selvittää henkilötietojen laatu ja aiheuttaa yksilöllistä sekä kollektiivista syrjintää (Wachter, 2018). Huomionarvoista on tällöin se että, alun

perin anonyymista tiedosta, jota ei GDPR-asetuksen mukaan lueta henkilötiedoksi ja siten lainsäädännölle alisteiseksi, muodostuukin henkilötieto, johon tulee soveltaa GDPR-asetuksen mukaisia sääntelytoimia.

4 IG:n ja GDPR:n sekä tutkimustyön konstruktio

Tiedon hallinta ei ole suinkaan uusi ilmiönä, mutta sen sijaan terminä tuorehko. Termin esittely tiedemaailmalle tapahtui vuonna 2004 (Kooper ym., 2011), jonka jälkeen sitä on määritelty sekä tiedemiesten että alan asiantuntijoiden toimesta. EU:n yleinen tietosuoja-asetus ja muut vastaavanlaiset sääntelyviitekehykset osaltaan eivät vain patista vaan myös auttavat rakentamaan ja kehittämään tiedon hallintaa. Tiedon hallinnan kehittämistoimien ja sen aktiviteettien avulla saadaan saman neuvottelupöydän äärelle liiketoimintaympäristön eri sidosryhmät. Tiedon hallinnan osaamisen merkitystä voidaan tähdentää esittelemällä riskeihin liittyvät sekä aineelliset että aineettomat kustannukset. Konkreettisia seuraamuksia organisaatiolle voivat esimerkiksi olla: oikeudenkäynnit, sakot ja rangaistukset, asiakasuskollisuuden menetys, tulojen menetys, osakekurssin putoaminen, negatiivinen julkisuus, brändin arvon laskeminen, yrityksen maineen vahingoittuminen, toimintakustannusten kasvaminen, immateriaaliomaisuuden menetys ja kohtuuttoman suuret vakuutusmaksut. (Schoch, 2016.)

EU:n yleistä tietosuoja-asetusta tulee noudattaa sekä yksityisellä että julkisella sektorilla, ja myös EU-alueen ulkopuolella käsiteltäessä EU-kansalaisen henkilötietoja. Sen soveltamiseen eivät vaikuta organisaation koko tai henkilötietojen käsittelyn laajuus, käytetyt teknologiat eikä henkilötietojen käsittelyn luonne. Tietosuoja-asetus sisältää yksityiskohtaisia vaatimuksia 87 sivua ja 99 artiklaa. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016.) Suomessa GDPR-asetuksen noudattamista valvoo tietosuojavaltuutettu. Näennäisesti jopa vähäpätöiset horjahdukset henkilötietojen tiedon hallinnassa, sen käsittelyssä, organisoinnissa ja tallentamisessa voivat altistaa oikeudellisille riskeille ja julkiselle häpeälle (Kooper ym., 2011) sekä luottamuksen menettämiselle. Pienikin lipsahdus henkilötietojen käsittelyssä saattaa koitua kalliiksi organisaatiolle hallinnollisten sakkojen ja maineen menettämisen vuoksi. Mikäli ei toimita GDPR-asetuksen mukaisesti käsiteltäessä henkilötietoja, voi hallinnollinen sakko olla organisaatioille korkeimmillaan olla 20 miljoonaa euroa tai neljä prosenttia yrityksen vuotuisesta liikevaihdosta. Hallinnollisten sakkojen lisäksi organisaatiol-

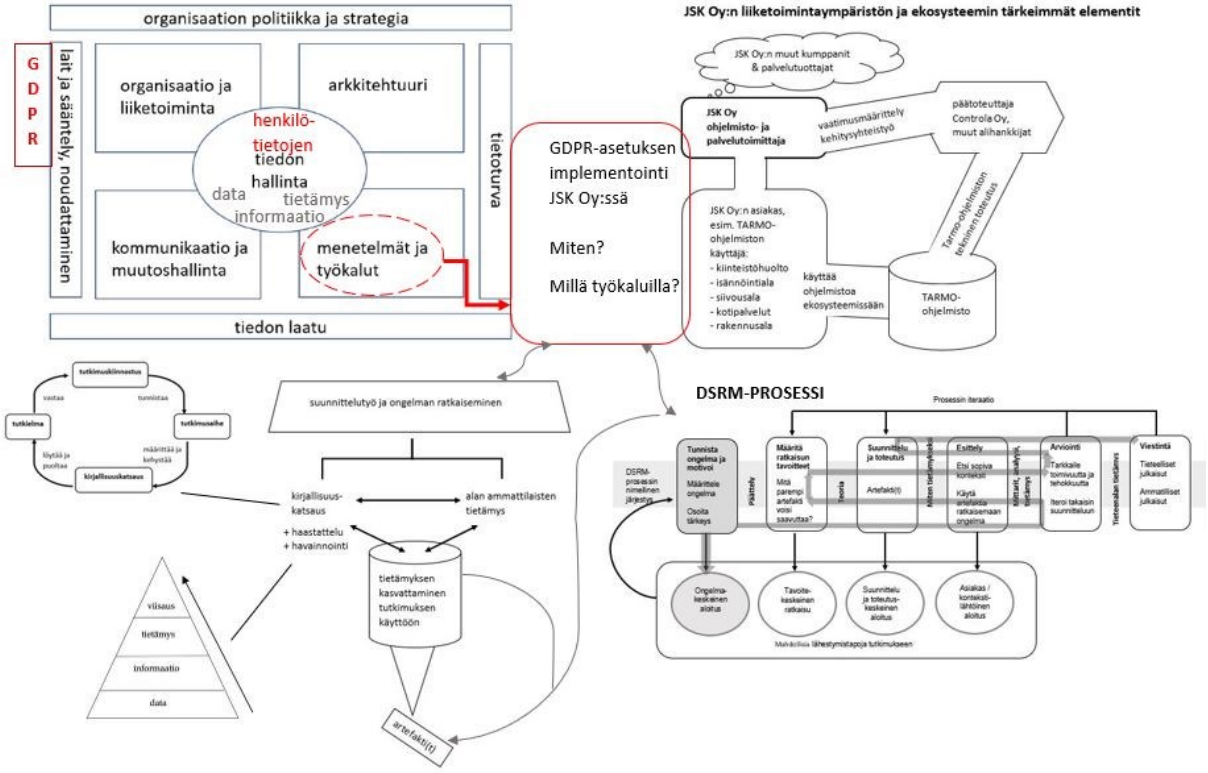
le voidaan langettaa vahingonkorvausvelvollisuus, mikäli ilmenee, että henkilötietoja on käytetty väärin. (Oikeusministeriö, 2018b.)

Aineettoman pääoman, tiedon, turvaaminen ja arvon kasvattaminen tapahtuu hallinnon (engl. governance) ja hallinnan (engl. management) keinoin. Yksinkertaistettuna hallinnon voidaan mieltää viittaavan päätöksiin, joita tehdään tehokkaan johtamisen ja resurssien hyödyntämisen varmistamiseksi. Sen strategisena tehtävänä luoda organisaation suunnitelma ja asettaa kehykset sekä tavoitteille että rajoituksille. Hallinnan keinoin varmistetaan päätösten täytäntöönpano. Se huolehtii resurssien jakamisesta ja päivittäisen operatiivisen toiminnan valvonnasta. Mitä monimutkaisempi organisaatio sitä vaikeampi on varmistaa, että tietosuojatoimenpiteet, -ohjelmat tai -aloitteet ovat integroitu koko organisaation käytänteisiin ja prosesseihin.

Tiedon, jota virtaa organisaatioissa ja niiden välillä, määrä kasvaa jatkuvasti eksponentiaalisesti (Junwoo ym., 2017). Yhä enenevässä määrin tietoa on joustavampi ja nopeampi eritellä sekä jäsennellä analysointityökalujen ja -tekniikoiden kehittymisen vuoksi. (Smallwood, 2014). Tyypillisesti IT-ekosysteemi on sidoksissa myyjiin ja palvelun tarjoajiin. Teknisillä ratkaisulla ei pelkästään saavuteta tietosuoja-asetuksen vaatimusten mukaista henkilötietojen käsittelyä, vaan muutoksia tarvitaan toimijoiden välisiin sopimuksiin varmistamaan henkilötietojen käsittelyyn osallistuvien osapuolien toimimisen asetuksen vaatimustenmukaisesti (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Asetus voi lisäksi johtaa tarkempiin asiakas-toimittajakyselyihin ja liiketoiminnan auditointeihin, kun halutaan varmistua siitä, että sekä rekisterinpitäjä ja käsittelijä toimivat tietosuoaja-asetuksen vaatimusten mukaisesti. GDPR-asetuksen osalta suhteessa käyttötarkoitukseen liian tiukalla sääntelyllä saatetaan hidastaa edistyneiden teknologioiden käyttöä ja siten myös vähentää kilpailukykyä EU:ssa. (Štitilis & Laurinaitis, 2017.) Skenaariona tällöin on digitaalisen ekosysteemin kehittymisen häiriintyminen. Luvussa 3.6. esittämiini haasteisiin perustuen saattaa olla, että GDPR-asetus hankaloittaa ja hillitsee joitain tietointensiivisiä liiketoimintamalleja. Nykyiset tiedonkeruu- ja lähestymistavat sekä teknisen integraation puuttuminen ohjelmistojen kanssa vaatinevat myös huomattavia ei-tietotekniikan avulla toteuttavia resursseja tietosuojan ja tietosuojavaatimusten täyttämiseksi.

Guetat ja Dakhli (2016) linjaavat tutkimuksessaan tiedon hallinnan neljä toiminnan osa-aluetta. Arkkitehtuuri koskee käsitteellisiä näkökohtia esittäen kysymyksen Mitä? Organisaatio ja liiketoiminta sekä kommunikaatio ja muutoshallinta toiminnan osa-alueina ovat omistettu organisaatioon liittyviin kysymyksiin: Kuka?, Milloin?, Missä? ja Millä resursseilla?. Edellä mainituissa kahdessa toiminnan osa-alueessa korostetaan tiedon hallinnan tehokkuuden edellytyksiä. Neljäs toiminnan osa-alue kuvaa lähestymistapoja sekä menetelmiä ja työkaluja, jotka sekä tukevat implementointia että tiedon hallinnan aktiviteettejä, kuten esimerkiksi oikeudellisten rajoitusten valvontaa. Tällöin esitetään kaksi kysymystä: Millä työkaluilla? ja Miten?, jolloin kysymysten avulla keskitytään toiminnallisiin näkökulmiin. (Guetat ja Dakhli, 2016.)

Tietosuoja-asesetuksen käyttöönoton sekä soveltamisen yksi suuri haaste on ollut, ettei se itsessään anna ohjeita täytäntöönpanosta eikä ohjaile sen implementointia. Se ei myöskään ota kantaa tekniikoihin tai teknologiaan, joita voisi hyödyntää vaatimustenmukaisuuden saavuttamiseksi. (Bihari, 2018; Blix, 2018; De Hert ym., Kindt, 2018; Tikkinen-Piri ym., 2018.) Tässä tapaustutkimuksessa selvitetään miten ja millä artefakteilla GDPR-asetuksen käyttöönottoa voitaisiin tukea Järvi-Suomen Kiinteistökonsultit Oy:n ekosysteemissä. Kuviosta 6 käy ilmi metatasolla tutkimusongelman ratkaisumalli.



KUVIO 6 IG:n ja GDPR:n sekä tutkimustyön konstruktio

Suunnittelutieteellinen tutkimus yhdistettynä käytännön työhön tuottaa ratkaisun toimeksiantajan kontekstiin kuviossa 6 esitetyn etenemispolun avulla. Tutkimuksen teoreettis-käsitteellisessä luvuissa perehdytään kirjallisuuskatsauksen avulla tutkimuksen pääkäsitteisiin ajatusrakennelmien ja niiden tarkastelun avulla. Teoreettis-käsitteellinen osuus luo tietopohjaa ja ymmärrystä empiirisen tutkimustyön toteuttamiselle iteratiivisen DSRM-prosessin vaihein. Syvälle luotaavaa ymmärrystä tietosuoja-asetuksen käyttöönottamiseksi kontekstissaan kasvatetaan koko tutkimusprosessin ajan myös haastattelujen ja havainnoinnin avulla. Tutkimustyön myötä esiin nousevat käytännön esimerkit sitovat teoreettisen tarkastelun tosielämään. Teoreettinen tarkastelu puolestaan tukee ja vahvistaa käytännönläheisen aineiston käyttökelpoisuutta. Tutkimuksen kautta esiin nostetaan tai tuotetaan artefakteja, jotka auttavat yritystä GDPR-asetuksen implementoinnissa ja sen

soveltamista käyttöönoton jälkeenkin. Seuraavassa luvussa 5 selostetaan DSRM-prosessin läpivieminen tapausorganisaatiossa.

5 DSRM-PROSESSIN LÄPIVIENTI JSK OY:SSÄ

Tutkimusongelma ratkaistiin laajalti tietojärjestelmätieteen tutkimuksissa hyödynnetyn (Hevner ym., 2010) suunnittelutieteellisellä (engl. Design Science, DS) tutkimusotteella. Koska JSK Oy:n käytännön läheinen ongelma toimi yhtenä tutkimuksen lähtökohtana, sopi DS erittäin hyvin menetelmäksi, sillä sen nimenomaisena tavoitteena on ongelmien ratkaiseminen organisaatoissa (Hevner ym., 2004) tosielämän kontekstissa. Suunnittelutieteellinen tutkimus on pohjimmiltaan ongelman ratkaisun paradigma, jonka avulla pyritään tuottamaan artefakti(t) ratkaisemaan tutkimusongelma(t). Artefaktilla tarkoitetaan ihmisen rakentamaa tuotosta. (Hevner ym., 2010.) Artefaktit voivat olla materialistisia konstruktioita tai immateriaalisia tuotoksia, kuten esimerkiksi malleja, menetelmiä (Peffers ym., 2008) tai prosesseja. Erityisesti tieto- ja informaatiojärjestelmien DS-tutkimusta ja sen esittämistä varten Peffers, Tuunanen, Rotherberger ja Chatterjee (2008) kehittivät kuusi toiminnallista vaihetta sisältävän DSRM-prosessin. Prosessin päätavoite on tarjota tutkimuksen läpiviemiseksi mentaalimalli. Se on pienimuotoinen malli todellisuudesta, joka voidaan rakentaa pohjautuen käsitykseen, kekseliäisyyteen tai diskurssin ymmärtämiseen. (Peffers ym., 2008.) Tämän tutkimustyön konstruktion myötä tuotettu mentaalimalli esitellään kuviossa 6, jonka käytännön implementointi JSK Oy:n ekosysteemissä esitellään tässä luvussa.

DSRM-prosessin aktiviteetit on esitelty raportin luvussa 2.3. Vaikka prosessi on jäsennelty kuuteen eri vaiheeseen, ei sen nimellistä järjestystä ole tarkoitettu noudatettavan, vaan tutkija voi valita tilannekohtaisesti, mistä prosessin vaiheesta aloittaa ja mihin siirtyy seuraavaksi. (Peffers ym., 2008.) Prosessi on siis iteratiivinen, ja prosessin sisällä voidaan palata arvioinnin sekä viestinnän vaiheesta takaisin määrittelemään ratkaisun tavoitteita tai suunnittelu- ja toteutusvaiheeseen. Tässä tapaustutkimuksessa tutkimusprosessin lähestymistavaksi valittiin ongelmakeskeinen lähestyminen, ja DSRM-prosessin aloituspisteenä toimi sen ensimmäinen vaihe, eli ongelman tunnistaminen ja motivaatio.

Koska ratkaisu toteutettiin tiettyyn kontekstiin, esittelen seuraavassa alaluvussa tapausorganisaation. Sen jälkeisissä luvuissa selostan DSRM-prosessin soveltamisen vaiheet.

5.1 Tapausorganisaation esittely

Yksityisomisteinen Järvi-Suomen Kiinteistökonsultit Oy on vuonna 1993 perustettu ICT-alan asiantuntijayritys. JSK Oy toimittaa asiakkailleen yksinmyyntioikeudella SaaS-palveluna (engl. software as a service) Tarmo-ohjelmistoa, joka on keskittynyt kiinteistöhuollon eri toimintojen työnohjaukseen. SaaS-ratkaisussa ohjelmistoja ei asenneta asiakkaan laitteille, vaan niitä käytetään pilvipalveluna internet-yhteydellä. Ohjelmistopalvelu sisältää palvelinkapasiteetin ja ylläpidon. Selainpohjainen Tarmo-palveluratkaisu on alun perin kehitetty kiinteistöhuoltotoimialalle alan keskeisten toimintojen hallintaa, kuten töiden suunnittelua ja työnohjausta varten. Sittemmin ohjelmiston käyttö on laajentunut kiinteistön huolto- ja korjaustoimialan lisäksi siivouksen ja kotipalvelun toimialoille, rakennus- ja koneurakoinnin yrityksiin sekä isännöitsijätoimistoihin.

Tarmo-tietojärjestelmää voidaan käyttää erilaisilla päätelaitteilla, kuten tietokoneilla ja mobiililaitteilla. Mobiilisovelluksen avulla voidaan esimerkiksi kirjata tehdyt työtunnit kohteittain ylös, ja se mahdollistaa puheella tapahtuvat työkuittaukset. Tarmo-ohjelmistoa toimittaa JSK Oy:lle ohjelmistotalo Controla Oy, joka on erilaisten tietoteknisten ratkaisujen päätoteuttaja. Järvi-Suomen Kiinteistökonsultit Oy työskentelee kiinteässä yhteistyössä toiminnallisen tuotekehityksen parissa ohjelmistotoimittaja Controla Oy:n kanssa. Tarvittaessa tilataan myös muilta alihankkijoilta kehittämis- ja ylläpitotyötä. Tarmo-palveluratkaisun lisäksi asiakkaille voidaan toimittaa erinäisiä lisä- ja tukipalveluita. JSK Oy:n palveluvalikoimaan kuuluvat muun muassa yritysten työnohjauksen suunnittelu sekä konsultointi, ohjelmistojen vaatimusmäärittely, ICT-ratkaisujen kilpailutus sekä projektijohtaminen. Edellä mainittujen lisäksi JSK Oy voi huolehtia tarjoamiinsa projekteihin liittyen palvelupaketin kokonaistoimituksen, joka sisältää laitteet, ohjelmistot, käyttöönoton, koulutuksen sekä ylläpidon.

5.2 Ongelman tunnistaminen ja motivaatio

DSRM-prosessin ongelman tunnistaminen ja motivaatio vaiheessa on tärkeää tutkimusongelman määrittäminen ja perustella sen arvo. On syytä tuoda esiin, miksi kyseinen ongelma on tutkimuksen arvoinen. (Peffers ym., 2008.) Aiemmin tehdyissä tutkimuksissa on havaittu, että merkittävimmät haasteet tietosuoja-asetuksen käyttöönotossa ja sen soveltamisessa liittyvät tiedon, ymmärryksen ja implementointiohjeiden puutteeseen. Tutkimusongelma ”Miten EU:n

yleisen tietosuoja-asetuksen käyttöönottoa voidaan tukea pienyrityksessä?" on ilmiselvästi tutkimisen arvoinen.

Koska tutkimusongelma on moniulotteinen, pilkottiin se pienempiin osakokonaisuuksiin. Ongelman osittamisella käsitteellisesti voidaan saada käsitys ratkaisun monimutkaisuudesta. (Peffers ym., 2008.) Tässä pro gradu -tutkielmassa moniulotteista tutkimusongelmaa lähestyttiin teoreettis-käsitteellisestä näkökulmasta pilkkomalla päätutkimusongelma osaongelmiin (luku 1.2.), joihin etsittiin vastauksia apukysymysten (luku 2.1) kautta. Lisäksi ratkaisua etsittäessä käytännönläheiseen tutkimusongelmaan, lähestyttiin sitä kahden kysymyksen avulla: Miten? ja Millä työkaluilla? Tällöin myös artefaktien kehittely pilkkoontui osakokonaisuuksiin.

5.3 Ratkaisun tavoitteet

DSRM-prosessin nimellisessä toisessa vaiheessa johdetaan ratkaisun tavoitteet, jotka voivat olla määrällisiä, tai tavoite voi olla kuvaus siitä, miten uuden artefaktin odotetaan tukevan ongelman ratkaisua. Ratkaisut tavoitteet tulee päätellä järkevästi ongelman määrittelystä. Toimintavaiheessa on tärkeää hahmottaa ongelman nykytila, sekä tietää nykyiset ratkaisut ja niiden tehokkuus, jos sellaisia on. Kartoitetun tiedon avulla voidaan arvioida, mitä on mahdollista tehdä ja mitä ei. (Peffers ym., 2008.)

Asetetun tutkimusongelman ratkaisemiseksi tämän käytännön toimintavaiheen olennaisin päämäärä on saada seuraavaksi riittävästi tietoa toimeksiantajan ekosysteemistä tutkimuksen käyttöön. Kuvio 7 avulla esitellään, kuinka muodostettiin käsitys JSK Oy:n henkilötietojen käsittelyn nyky-ympäristöstä. Kuvioon on merkitty toimeksiantajan liiketoimintaympäristön oleellisimpia sidosryhmiä. Koska toimeksiantajalla on GDPR-asetuksen alaisia vastuita ja velvollisuuksia muun muassa liiketoimintasuhteen vuoksi sekä SaaS-palveluratkaisun tuottajana että myös toiminnallisena kehittäjänä Tarmo-järjestelmään liittyen, on tämän yksittäisen tietojärjestelmän olemassaolon huomioonottaminen tutkimusongelmaa ratkaistaessa perusteltua. Liiketoimintaympäristöllä tarkoitetaan yrityksen ulkoista ympäristöä, johon vaikuttavat monet tekijät – tässä tapauksessa vaikuttava asia, jota erityisesti tarkastellaan, on GDPR-asetus ja sen vaikutus henkilötietojen käsittelyn aktiviteetteihin.

KUVIO 7 JSK Oy:n liiketoimintaympäristön kuvaus yksinkertaistettuna karkealla tasolla

Tiedon hallinta ja sen kehittäminen ei ole uusi asia ilmiönä JSK Oy:n ekosysteemissä (vrt. Blair, 2011). Esimerkkinä mainittakoon, että Tarmo-järjestelmä on rekisteröity Valviran B luokkaan. Jotta tietojärjestelmä voidaan rekisteröidä, tulee sen täyttää tietyt kriteerit, ja tietojärjestelmän valmistaja on vastuussa vaatimustenmukaisuuden osoittamisesta. Toinen esimerkki löytyy systeemin kehittämisestä, jonka avulla kiinteistönhuoltoyritys voi tarkistaa ovenavaustapauksessa sisään pyrkivältä henkilön asumisoikeuden. Tarmo-järjestelmästä on suora liitäntä Digi- ja väestötietoviraston (DVV) väestötietojärjestelmään. Sisään pyrkivän henkilön henkilötunnus syötetään sovellukseen, ja paluuviestissä DVV:n järjestelmästä palautuu tieto henkilön nimestä ja osoitetiedosta (kuvio 12). Tällöin oven avaaja voi todentaa, onko henkilöllä oikeus päästä sisään kyseiseen asuntoon

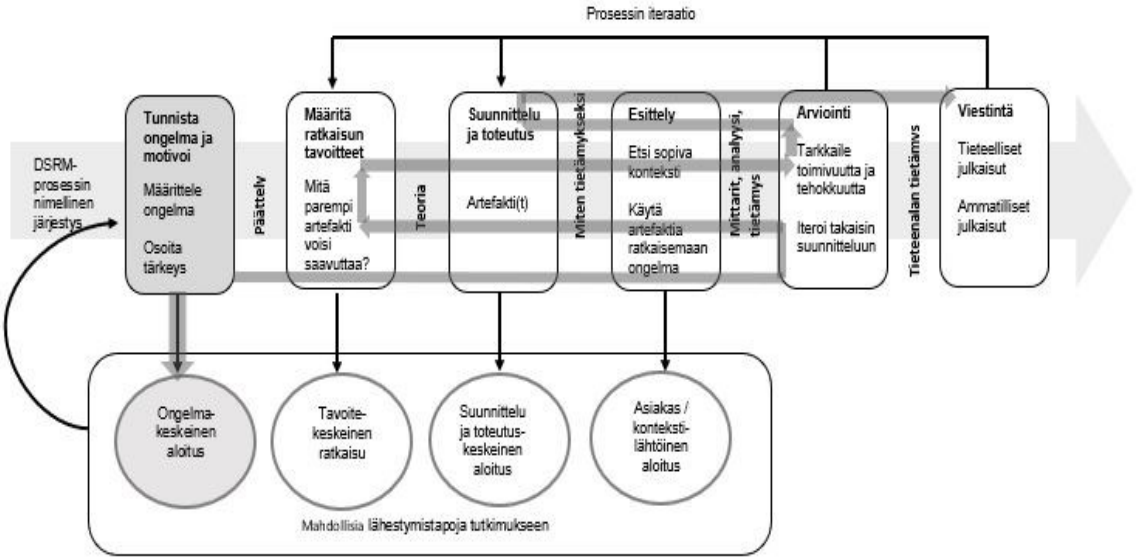
EU:n yleinen tietosuoja-asetus tiukkana lainsäädännöllisenä viitekehyksenä tiedon hallinnan laajassa abstraktiossa edellyttää uudenlaista suhtautumista tietosuojaan ja henkilötietojen tiedon hallintaan. Tavoitteena tässä työssä on tuottaa toimeksiantajalle nykytilan liiketoimintaympäristön ekosysteemiin soveltuvaa informaatiota ja tietoa GDPR-asetuksesta, suosituksia sekä kehitysehdotuksia että esitellä artefakteja, joiden avulla asetuksen käyttöönottoa voidaan tukea yrityksessä. Tarkastelunäkökulma painottuu ensisijaisesti rekisterin pitäjän vastuisiin sekä velvollisuuksiin, mutta toimeksiantajan toiveen mukaisesti myös rekisterin käsittelijän rooliin kuuluvia vastuita ja velvollisuuksia sivutaan. Muun muassa liiketoimintasuhteiden ja Tarmo-ohjelmiston kehitysyhteistyön

myötä vastuita tietoturvallisuuden toteuttamisesta koituu ohjelmistokehittäjien lisäksi JSK Oy:lle.

5.4 Suunnittelu ja toteutus

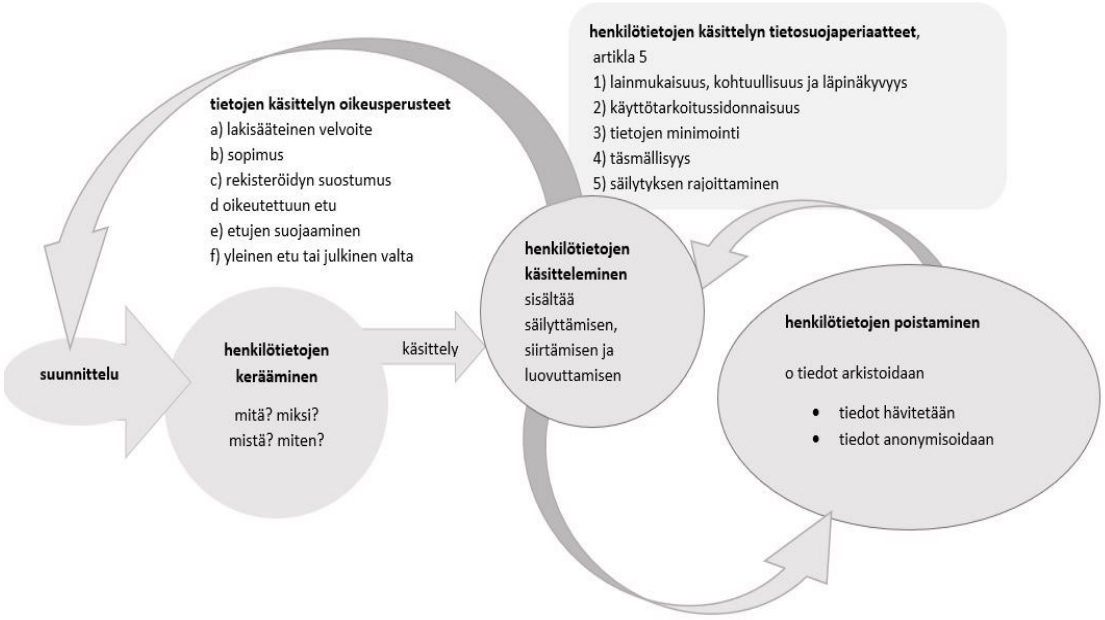
DSRM-prosessin suunnittelun ja kehittämisen vaiheessa luodaan artefakti(t) sekä määritellään artefaktin haluttu toiminallisuus ja myös tuotetaan se. Artefakti voi olla mikä tahansa objekti, jota hyödynnetään tutkimuksessa. Sen suunnittelu sisältää teoriatietoa, jota voidaan hyödyntää ratkaisussa. (Peffers ym., 2008.) Sekä tuotosten suunnittelussa että toteutuksessa hyödynnettiin kuvion 6 mukaista konstruktiota, joka mahdollisti teoriatiedon hyödyntämisen tämän tutkimuksen käyttöön. Lisäksi suunnittelutieteellistä tutkimusotetta höystettiin Ostrowskin ja Helfertin (2012) esittelemän referenssimallin opein, joka sisältää kirjallisuuskatsauksen lisäksi kollaboraation ammatinharjoittajien kanssa. Näiden avulla kerättiin tutkittavaan ilmiöön ja aihealueeseen liittyviä tietoja sekä teoreettis-käsitteellisistä että käytännön lähtökohdista DSRM-prosessin iteraatioiden vaiheissa. Konkreettinen ja koottu tutkimusaineisto on tutkimuksen keskiössä ja toimii siten ratkaisun kehittämisen lähtökohtana. Tässä luvussa esittelen lähtökohtia ja artefakteja, joita hyödynnettiin ratkaisun tuottamisessa kontekstiinsa.

Tutkimusongelman ratkaiseminen aloitettiin DSRM-prosessin vaiheesta ongelman tunnistaminen ja motivointi lähestymistavan ollessa ongelmakeskeinen. Iteratiivisessa prosessissa palattiin arviointivaiheesta takaisin ratkaisun tavoitteiden määrittelemiseen ja uudelleen vielä suunnittelu- ja toteutusvaiheeseen. Tutkimuksen edetessä DSRM-prosessin iteraatiokierrosten tutkijan ja prosessityöskentelyyn osallistuneen toimeksiantajan yhteistyön myötä syntyi syvälle luotaavaa ymmärrystä, jonka myötä tietämys tutkittavaa ilmiötä kohtaan lisääntyi. Iteraatiokierrokset ja tiedon karttuminen mahdollistivat myös artefaktien parantelun, joiden toimivuutta sekä tehokkuutta arvioitiin kontekstissaan yhdessä toimeksiantajan kanssa. Tiedon, informaation sekä tietämyksen kartuttaminen onkin olennaista artefaktien suunnittelussa ja kehittämisessä (Hevner ym., 2010). Kun artefaktissa havaittiin virheitä tai puutteita, ne korjattiin, ja tarvittaessa palattiin suunnittelu- ja kehitysvaiheeseen. Kuvion 8 mukainen iterointiprosessi kasvatti syvälle luotaavaa tietämyspohjaa ja prosessilla parannettiin artefaktin tehokkuutta. (Peffers ym., 2008.)



KUVIO 8 DSRM-prosessin toteuttamisen lähtökohdat ja iteraatiot JSK Oy:ssä

Henkilötiedot ovat GDPR-asetuksen ytimessä. Se sanelee henkilötietojen keräämisen, säilytyksen ja hallinnoinnin vaatimuksia. Henkilötietojen elinkaaren hallintaa määrittävät luvussa 3.5. luetellut tietosuojaperiaatteet. Ne ohjaavat sekä rekisterinpitäjiä että henkilötietojen käsittelijöitä operoimaan henkilötietoja yksilön oikeuksia ja vapauksia kunnioittavalla tavalla. Tietosuojaperiaatteet ohjaavat organisaatioissa myös henkilötietojen elinkaaren hallintaa. Laatimani kuvio 9 tukee käsitteellisellä tasolla GDPR-asetuksen käyttöönottoa ja vaatimusten mukaista toimintaa henkilötietojen elinkaaren eri vaiheissa.



KUVIO 9 Elinkaari, henkilötietojen käsittelyn tietosuojaperiaatteet ja oikeusperusteet

Henkilötietojen elinkaaren hallinta alkaa elinkaaren suunnittelulla päättyen keräämisen ja käsittelyn jälkeen henkilötietojen poistamiseen. Asetus sisältää kuviossa 9, kohdat a-f, luetellut kuusi oikeusperustetta, joihin henkilötietojen käsittely voi pohjautua. Arkistoituja henkilötietoja tulee käsitellä elinkaaren hallinnan mukaisesti. Henkilötiedon elinkaari päättyy, kun se hävitetään tai anonymisoidaan peruuttamattomasti. Henkilötietojen käsittelijän tulee pystyä osoittamaan noudattavansa kaikessa toiminnassaan ja käsittelyn kaikissa eri vaiheissa Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 artiklan 5 periaatteita (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

Henkilötietojen tietosuojaperiaatteiden ja oikeusperusteiden lisäksi henkilötietojen käsittelyssä tulee ottaa huomioon rekisteröidyn oikeudet. Rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet rekisteröityjen tietosuoja-oikeuksientoteuttamiseksi. Asetuksesta on erotettavissa kuviossa 10 luetellut rekisteröidyn oikeudet. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016.)

KUVIO 10 GDPR-asetuksessa määritellyt rekisteröidyn oikeudet

Guetat ja Dakhli (2015) ovat vakuutelleet tietoarkkitehtuurin (engl. information architecture) olevan tiedon hallinnan veturin. Sen tärkeimpiä tehtäviä on hallita, kuvata ja mallintaa tietovirtoihin liittyviä käsitteitä, tietomalleja, tietovarantoja ja prosesseja. Tietoarkkitehtuurin systeeminen analyysi mahdollistaa tiedon sekä rakenteellisen että systeemisen monimutkaisuuden huomioon ottamisen. (Gueat ja Dakhli, 2015.) DSRM-prosessia toteutettaessa pyrittiin pelkistettyyn systeemiseen analyysiin henkilötietojen käsittelyn ja niiden hallinnan sekä tietovirtojen osalta. Tässä tapauksessa kuvaamisen tarkoituksena on tunnistaa ja kuvata eri järjestelmissä olevat henkilötiedot, sekä niiden rakenteet että riippuvuudet toisistaan.

GDPR-asetuksen käyttöönottoa varten on ensin selvitettävä henkilötietojen tallennuspaikat, sekä miten niitä kerätään että operoidaan eri järjestelmissä tai järjestelmien välillä. Käytännössä tehdään henkilötietojen inventaario. Henkilötietojen inventoinnin avulla on mahdollista saada kokonaisvaltainen näkymä omaan organisaatioon ja sen toimintaan. Inventaariossa kartoitettiin ne tietojärjestelmät, joita JSK Oy käyttää operoidessaan henkilötietoja rekisterinpitäjän roolissa sekä selvitettiin missä henkilötietoja sijaitsee. Nykytila-analyysissä ja inventaarion alkuvaiheessa hyödynnettiin käyttökelpoiseksi havaittua miellekarttatyökalua. Parhaimmillaan miellekarttojen luomisen prosessin etuna on se, että työstettäessä asiaa hyödynnetään aivojen muovautuvuutta ja mielenlaatua, koska mieli ei toimi lineaarisesti vaan pikemminkin kuin magneetti, joka piirtää informaatiota kaikista suunnista (Bihari, 2018).

Tietosuoja-asetus on muuttanut myös sopimuskäytäntöjä. Kaikesta henkilötietojen käsittelyyn liittyvästä tulee olla sovittu kirjallisesti, ja sopimusvelvoite koskee henkilötietojen käsittelyä, luovuttamista, jakamista tai siirtoa toiselle osapuolelle (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). On mahdollista, että yrityksen rekisterissä olevia henkilötietoja joudutaan luovuttamaan alihankkijoille tai yhteistyökumppanit tarvitsevat henkilötietoja projektien toteuttamisessa. Täten sopimusinventaari tulee tehdä, ja esimerkiksi toimitus- ja palvelusopimukset tulee päivittää ajan tasalle tietosisällöltään vastaamaan EU:n yleisen tietosuoja-asetuksen velvoitteita.

Tutkimusongelmaa ratkaistaessa itse tietosuoja-asetustekstin lisäksi hyödynnettiin eri viranomaistahojen julkaisemia dokumentteja ja ohjeistuksia. Esimerkiksi Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän julkaisema Excel-pohjainen Tietosuojan tukityökalu (Valtiovarainministeriö, 2016) on hyödyllinen yksityiskohtaisemmassa rekisteröityjen oikeuksien ja rekisterinpitäjän velvollisuuksien selvittämisessä. Sen avulla voidaan kartoittaa GDPR-asetukseen liittyvien asioiden nykytilaa. Toiseksi se auttaa käymään läpi rekisteröidyn oikeudet sekä rekisterinpitäjän velvollisuudet tehtäväkohtaisesti. Kolmanneksi se mahdollistaa tehtävien seurannan edistymisen tarkkailun sekä aikataulutavoitteiden asettamisen, että tehtävän toteuttajan nimeämisen.

Seuraavassa luvussa kerrotaan lisää artefakteista, joita hyödynnettiin tapausorganisaatiossa GDPR-asetusta käyttöönotettaessa.

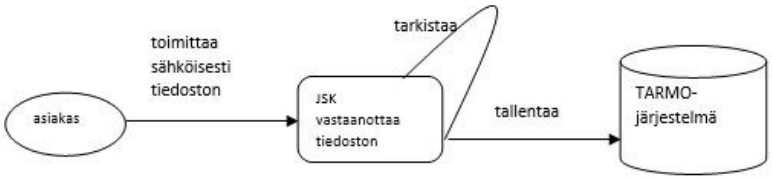
5.5 Ratkaisun esittely tapausorganisaation käyttöön

DSRM-prosessin esittelyvaiheessa artefaktin demonstraatiolla osoitetaan yhden tai useamman ongelman ratkaiseminen. Vaihe voi sisältää esimerkiksi artefaktin käytännön kokeiluja ja sen hyödyntämistä voidaan simuloida. Lisäksi tapaustutkimuksen avulla tai muilla soveltuvilla tavoilla voidaan osoittaa tuotetun ratkaisun toimivuus. Samalla voidaan verrata uutta ratkaisua vanhaan toteutustapaan, ja löytää näin etuja uuden ratkaisun käytöstä. (Hevner ym., 2010; Peffers ym., 2008.) Seuraavaksi tarkennetaan, millä tavoin tutkimustyön löydöksiä sekä tuotoksia hyödynnettiin tutkimusongelman ratkaisemisessa eli

GDPR-asetusta käyttöönotettaessa Järvi-Suomen Kiinteistökonsultit Oy:n ekosysteemissä.

JSK Oy:n henkilötietojen käsittelyn nykytilan selvittäminen aloitettiin kuvioiden ja miellekarttojen avulla. Kuvio 13 on yksi esimerkki tutkimuksessa hyödynnetystä miellekartasta, jonka avulla pyrin mallintamaan, millä tavoin nykytila-analyysia sekä henkilötietojen inventointia tehtiin tutkimusprosessin aikana. Nykytilan kartoittamisen ja sen analysoimisen jälkeen ratkaisuja tuotettaessa GDPR-asetuksen käyttöönottoa varten otettiin huomioon kuviossa 9 esitellyt henkilötietojen käsittelyn tietosuojaperiaatteet ja oikeusperusteet, sekä asetuksessa määritellyt rekisteröidyn oikeudet kuvio 10 mukaisesti. Nuo oikeudet, periaatteet ja perusteet on otettava huomioon, kun pohditaan ja kehitetään henkilötietojen elinkaaren hallintaa tietosuoja-asetuksen vaatimusten mukaisiksi.

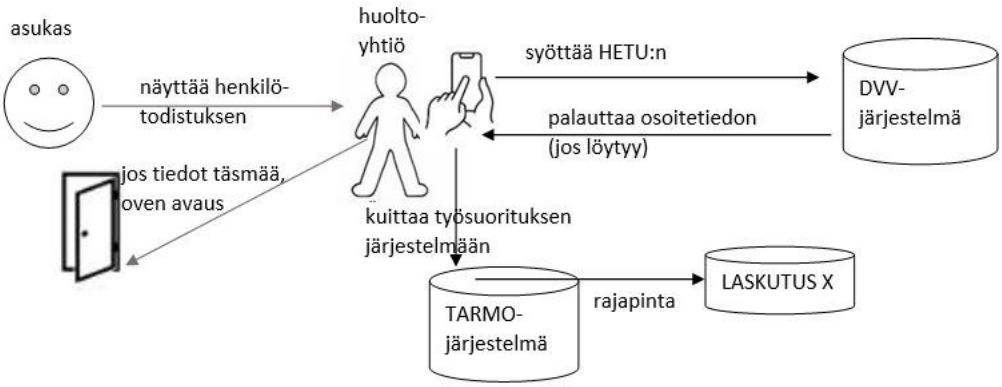
Miellekarttakuvioon 13 on esimerkinomaisesti merkitty yksi havainto, joka johti prosessimuutokseen (kuvio 11). Inventaarissa kävi ilmi, että JSK Oy:n Tarmo-tietojärjestelmää käyttävä taho saattaa toimittaa henkilötietoja sähköisesti, jonka jälkeen JSK Oy tallentaa tiedoston tarkistamisen jälkeen järjestelmään asiakkaan saataville.



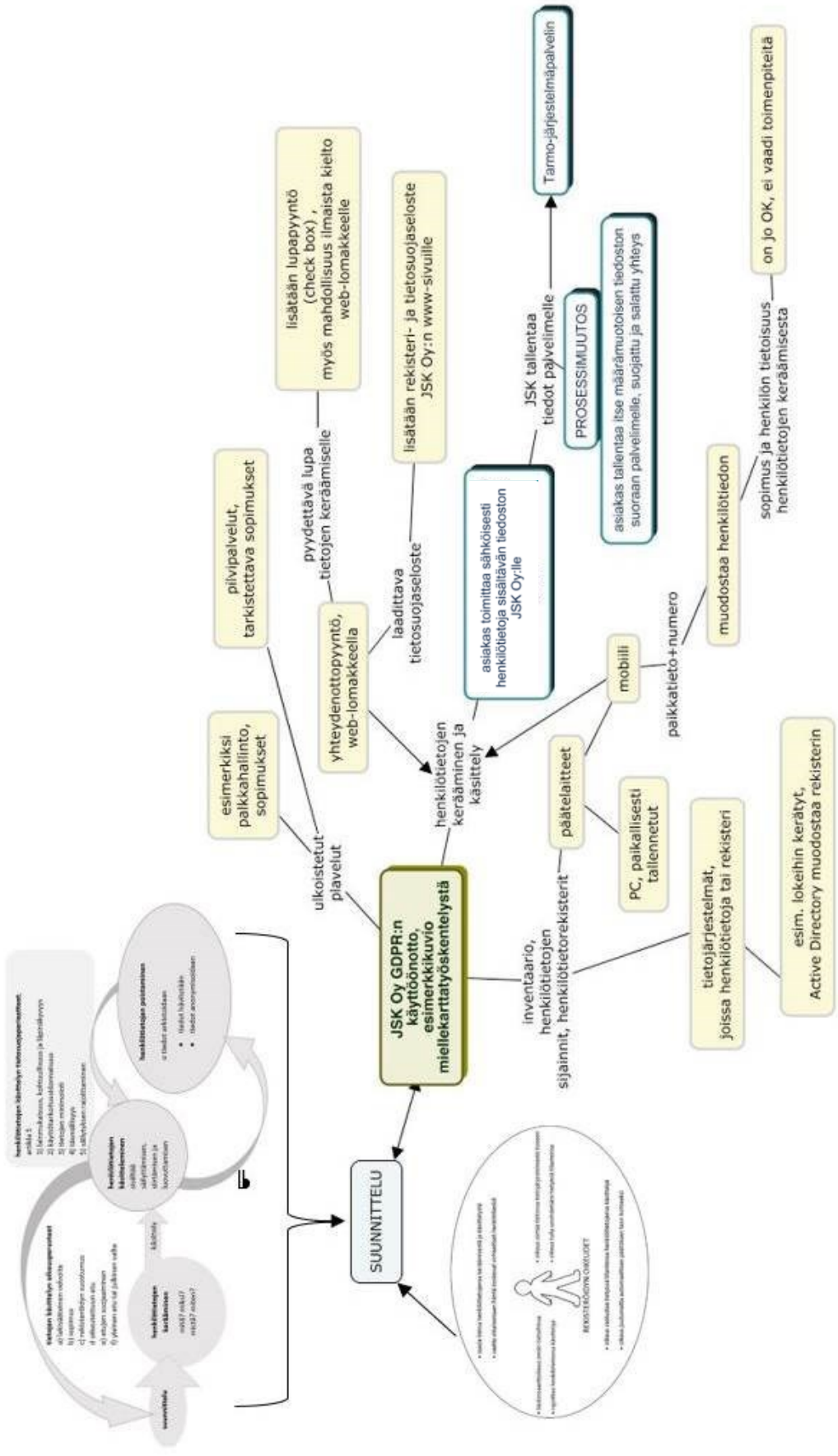
KUVIO 11 Inventaarin prosessiesimerkki

Jotta vältetään JSK Oy:ssä turhaa henkilötietojen käsittelyä, prosessia muutettiin sillä tavoin, että asiakas voi tallentaa salatulla sekä suojatulla tietoliikenneyhteydellä ja tietyllä formaatilla haluamansa henkilötiedot itse suoraan Tarmo-järjestelmään, jossa myös tiedoston syntaksi tarkistetaan.

Jatkojalostuksen jälkeen nykyisen käytössä olevan systeemin ansiosta taloyhtiön asukastietoja ei tarvitse tallentaa ollenkaan Tarmoon, vaan tarvittavat tiedot haetaan DVV:n järjestelmästä, jolloin vastuu osoitetiedon ajantasaisuudesta on asukkaan itsensä ilmoittaman tiedon varassa.



KUVIO 12 Tiedonkulkukaavioesimerkki oven avaaminen



KUVIO 13 Esimerkkinäkymä miellekarttatyöskentelystä

Miellekarttojen sekä kuvioiden avulla, joita työstettiin alkuvaiheessa toimeksiantajan kanssa yhteistyössä, pystyttiin havainnollistamaan ja selkeyttämään käsiteltävän kohteen rakenteita sekä yhteyksiä. Miellekartat ovatkin eritoten hyödyllisiä silloin, kun opiskellaan, järjestellään tai vahvistetaan tietoja (Bihari, 2018). Niin ikään, DS:n tutkimuksen toteuttamiseen liittyvän pohdinnan mukaisesti (Hevner ym., 2004) miellekartan avulla tutkimusprosessia ja sen löydöksiä voidaan esitellä toimivalla tavalla sekä teknologiasta vastaaville että johdolle. Miellekartta voidaan käsittää abstraktioksi todellisuudesta, jonka avulla voidaan yksinkertaistaa asiakokonaisuuden näkemystä nostamalla esiin olennaisia tekijöitä sekä piirteitä (Bihari, 2018). Tutkielmaraportissa esiteltyjen kuvioiden tarkoituksena on havainnollistaa ja selkeyttää käsiteltävän kohteen rakenteita sekä yhteyksiä. Niiden hyödyllisyys korostuu referenssimallin mukaisessa kollaboratiivisessa yhteistyössä asiantuntijoiden kanssa.

Haastavinta tässä työssä nykytila-analyysia laadittaessa oli selvittää rakenteettoman tiedon (engl. dark data) lähteet, kuten esimerkiksi paperiset arkistot, sähköposti, Excel-taulukot, pilvitallennustilat tai tiedostopalvelimet, joissa henkilötietoja voi sijaita. Organisaatiolla saattaa olla jo lähtökohtaisesti rajallinen näkyvyys kyseisenlaiseen jäsentämättömään dataan. Tällaisten ikään kuin hieman pimennossa olevien tietojen, jotka eivät itsessään selkeästi muodosta rekisteriä tai tietoja ei hyödynnetä tai ne eivät ole tarpeellisia omassa liiketoiminnassa, selvittäminen saattaa olla hankalaa. Huomionarvoista on myös muistaa, että erilliset tiedot, kuten esimerkiksi tiedon pyramidin dataentiteetit, jotka yhdistettyinä toisiinsa mahdollistavat henkilön tunnistamisen, ovat tietosuoja-asetuksen mukaisia henkilötietoja (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Myöskään ei sovi unohtaa luvussa 3.6 mainittuja tilanteita, joissa informaatioidentiteetti tai anonymisoidut tiedot muodostavat lainsäädännön alaisen henkilötiedon.

Pelkistetyn systeemisen analyysin, jonka avulla tunnistettiin ja kuvattiin eri järjestelmissä olevan henkilötiedot sekä niiden rakenteet että riippuvuudet, jälkeen siirryttiin hyödyntämään tiedonkulkukaavioita. Tiedonkulkukaaviolla (engl. data flow diagrams) kuvattiin rakenteita ja yhteyksiä yksityiskohtaisemmalla tasolla. Graafisina notaatioina ne mahdollistavat datavirtojen mallintamisen tietojärjestelmissä. Niiden yleisyys ja modulaarisuus tekevät niistä sopivia laajoihin konteksteihin, joka on yksi tärkeimmistä syistä, miksi ICT-alan asiantuntijat hyödyntävät niitä. (Antignac ym., 2016.) Kuvioissa 11 ja 12 esitetään erään henkilötietoilmentymän liikkumista ihmisten ja järjestelmien välillä. Tämän tarkemmalla tasolla tutkimuksessa käytettyjä tiedonkulkukaavioita ei esitellä, koska ne ovat JSK Oy:n liiketoiminnan aineetonta omaisuutta, jonka ei ole tarkoituksenmukaista olla julkisesti saatavilla.

Käyttöönoton ja lain soveltamisen tukena hyödynnettiin itse tietosuoja-asetustekstin lisäksi myös eri viranomaistahojen tuottamia julkaisuja ja ohjeita, joista seuraavaksi kerrotaan muutamia poimintoja.

GDPR-asetuksen mukaan organisaation on rekisterinpitäjän roolissa toteutettava tietosuojaa koskevaa vaikutustenarviointia, mikäli henkilötietojen

käsittely aiheuttaa korkean riskin rekisteröidyille yksilöille. Tietosuojatyöryhmän laatiman ohjeistuksen tuella tehtiin vaikutustenarviointi. Vaikutustenarvioinnin työkalu auttaa riskien tunnistamisessa, arvioimisessa sekä hallitsemisessa. (Tietosuojatyöryhmä, 2017.) Apua GDPR-asetuksen tulkintaan haettiin myös Working Party 29:n (WP29), joka on EU:n yleisen tietosuoja-asetuksen artiklan 29 mukainen työryhmä, tuottamista julkaisuista (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). EU:n tietosuojaviranomaisten yhteistyöelin tietosuojatyöryhmä WP29 on käsitellyt yksilöiden suojelua henkilötietojen käsittelyssä koskevia kysymyksiä asetuksen soveltamisen alkamiseen 25.5.2018 asti (European Data Protection Board, 2018). Suuntaviivoja ja myös käytännön ohjeita on julkaistu liittyen automatisoituun päätöksentekoon ja profilointiin (29 artiklan mukainen tietosuojatyöryhmä, 2018). Viranomaistahojen julkaisemat ohjeet ovat käytännönkin läheisiä, ja esimerkiksi ohjeistus koskien henkilötietojen tietoturvaloukkauksia sisältää vuokaavion ilmoittamisvaatimuksista, sekä siinä on lueteltu tilanteita, jolloin loukkauksesta ei tarvitse ilmoittaa tai tulee ilmoittaa. (Tietosuojatyöryhmä, 2018). Dokumentti tietosuojaa koskevasta vaikutustenarvioinnista sisältää ohjeita GDPR-asetuksen periaatteiden tulkintaan, se määrittelee vaikutustenarvioinnin käsitteen ja sisältää iteratiivisen menettelyprosessin tietosuojaa koskevan vaikutusten arvioinnin tekemiseksi (Tietosuojatyöryhmä, 2017).

Valtiovarainministeriön julkaisema Excel-pohjainen Tietosuojan tukityökalu auttoi jäsentelemään rekisteröidyn oikeuksiin ja rekisterinpitäjän velvollisuuksiin kohdistuvia GDPR-asetuksen monimutkaisia vaatimuksia tehtäviksi. Työkalun avulla arvoitiin JSK Oy:ssä asetuksen vaatimusten nykytilaa, ja sen avulla pystyttiin asettamaan sekä keino- että toimenpidetavoitteita rekisteröityjen oikeuksiin ja reksiterinpitäjän velvollisuuksiin liittyen. Lisäksi sillä seurattiin valittujen tehtävien valmistumisen tilannetta. Työkalun riski- ja uhka osioon kirjattiin tunnistetut riskit. Kuviossa 14 esitetään ensin näkymä Tietosuojan tukityökalun kehittämisalueet välilehdestä. Sen alla on näkymä raportoinnin välilehdestä.

Tietosuojan tukityökalu - TIKU
ver 1.00 - 4.10.2016

Kehittämisalueet välilehti

VAHTI raportti 1/2016 osa-alue

	Tehtävä | toimenpide | raportissa kuvattu osa-alue, joka organisaation on käytävä läpi [riittävä ymmärrys | osaaminen]	Nykytilan arviointi	Tavoitetila
4. Rekisteröidyn oikeudet	Keskiarvo osa-alueesta:	1,07	
	4.1 Rekisterinpitäjän tiedonantovelvoitteet	75% valmiina	Huolehditaan ohjeistuksel
	4.2 Oikeus saada pääsy tietoihin	50% valmiina	Jokin muu ratkaisu
	4.3 Oikeus tietojen oikaisemiseen	100% valmiina	Huolehditaan koulutuksel
	4.4 Oikeus poistaa tiedot ("oikeus tulla unohdetuksi")	75% valmiina	Jokin muu ratkaisu
	4.5 Oikeus siirtää tiedot järjestelmästä toiseen	Ymmärretty	Huolehditaan ohjeistuksel
	4.6 Oikeus vastustaa käsittelyä, automaattista päätöksentekoa ja profilointia	*** valitse listalta ***	Huolehdittava sopimuksel
	4.7 Oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta	25% valmiina	*** valitse listalta ***
5 Rekisterinpitäjän velvollisuudet	Keskiarvo osa-alueesta:	0,12	
	5.1 Käsittelyn oikeusperusta	75% valmiina	*** valitse listalta ***
	5.2 Tietosuojan hallinnointi, roolit ja vastuut	25% valmiina	*** valitse listalta ***
	5.2.1 Tietosuojavastaava		
	Tietosuojavastaavan nimeäminen ja oikea asema organisaatiossa	Ymmärretty	*** valitse listalta ***
	Tietosuojavastaavan tehtävänkuva	Ymmärretty	*** valitse listalta ***
	5.2.2 Tietosuojaorganisaatio	Ymmärretty	*** valitse listalta ***
	5.2.3 Vuosikello	25% valmiina	*** valitse listalta ***
	5.3 Tietosuojariskienhallinta	Ymmärretty	*** valitse listalta ***
	5.3.1 Tietosuojan vaikutustenarvioinnit	*** valitse listalta ***	*** valitse listalta ***
	5.4 Sisäänrakennettu- ja oletusarvoinen tietosuoja		
	5.4.1 Tietosuoja järjestelmä- ja sovelluskehityksessä	*** valitse listalta ***	*** valitse listalta ***
	5.4.2 Tietosuoja hankinnoissa ja projektinhallinnassa	*** valitse listalta ***	*** valitse listalta ***
	5.4.3 Tiedon elinkaaren hallinta	*** valitse listalta ***	*** valitse listalta ***
	5.5 Tietoturvallisuuden toteuttaminen		
	Riskienarviointiprosessi	*** valitse listalta ***	*** valitse listalta ***
	Turva-arkkitehtuuri	100% valmiina	*** valitse listalta ***
	Tietojärjestelmien hankinta, kehitys ja ylläpito	*** valitse listalta ***	*** valitse listalta ***

Tietosuojan tukityökalu -
TIKU
ver 1.00 - 4.10.2016

Raportointi välilehti

VAHTI raportti 1/2016 osa-alue	Nykytila	Arvio	Toimenpiteiden eteneminen	Arvio
4. Rekisteröideyn oikeudet	1,07	25% valmiusaste	1,54	75% valmiusaste
5 Rekisterinpitäjän velvollisuudet	0,12	25% valmiusaste	-0,60	Erittäin pahasti kesken
6. Toimenpiteitä	0,18	25% valmiusaste	-1,00	Erittäin pahasti kesken
Kokonaisuus	0,46	25% valmis	-0,02	Pahasti kesken

KUVIO 14 Esimerkkinäkymä Tietosuojan tukityökalusta

GDPR-asetus vaikuttaa moniin sopimuksiin. Sopimusvelvoite koskee henkilötietojen käsittelyä, luovutusta, jakamista tai siirtoa. Asetuksen artikloissa 28, 32 ja 33 luetellaan asioita, jotka tulee ottaa huomioon palvelusopimuksissa rekisterinpitäjän ja käsittelijän välillä. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016.) Palvelu- ja konsultointisopimukset ja tietojärjestelmätoimittajien ja muiden henkilötietojen käsittelijöiden kanssa solmitut sopimukset tulee päivittää. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee sopia kirjallisesti rekisterinpitäjän lukuun tapahtuvasta henkilötietojen käsittelystä. Uusiin palvelusopimuksiin tietosuojaa koskevat ehdot voidaan sisällyttää tai laatia niihin erillinen sopimusliite. Jo voimassa olevat JSK Oy:n palvelusopimukset päivitettiin erillisellä liitteellä, esimerkkinä toimeksiantajan toimitussopimusliite ”Tietosuojaliite” (Järvi-Suomen Kiinteistökonsultit, 2018b) vastaamaan GDPR-asetuksen vaatimuksia. Myös muita asetuksen vaatimia dokumentteja laadittiin, kuten liitteen 1 mukainen Tarmo asiakasrekisterin rekisteri -ja tietosuojaseloste (Järvi-Suomen Kiinteistökonsultit Oy, 2018a). Artikla 30 ohjaa rekisteriselosteen laadintaa (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

GDPR-asetuksen mukaan rekisteröidyllä on oikeus tulla unohdetuksi eli hänellä on oikeus tietyissä tapauksissa, jotka on lueteltu artiklassa 17, pyytää poistamaan ilman aiheeton viivytystä tietonsa. Myös mahdollisista tietojen varmuuskopioista tulee tiedot poistaa edellyttäen, että jokin artiklan 17 perusteista täyttyy. Tosin artiklassa 25 todetaan, että toteutusta mietittäessä on syytä ottaa huomioon riskien taso, tekniikka että toteuttamiskustannukset. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016.) JSK Oy:ssä suunniteltiin uusi prosessi, joka ohjaa henkilötietojen poistamisen pyyntöä aina itse poistotoimenpiteeseen asti. Lisäksi prosessin suunnittelun vaiheessa otettiin huomioon rekisteröidyn tiedonsaantioikeus omiin tietoihinsa ja oikeus siirtää omat tietonsa tietyissä tapauksissa tietojärjestelmästä toiseen.

Palveluntuottajana JSK Oy toimii myös GDPR-asetuksen määrittämän käsittelijän roolissa, joten seuraavaksi nostan esiin kyseisen roolin mukanaan tuomia vastuita sekä velvollisuuksia. Käsittelijä on velvoitettu avustamaan sekä neuvomaan rekisterinpitäjää joidenkin asetuksen velvoitteiden noudattamisessa, ja käsittelijän on noudatettava GDPR-asetuksen vaatimuksia rekisteröityjen henkilöiden oikeuksien suojelemiseksi ottaen huomioon myös mahdolliset alihankkijat. Velvoitteita ovat muun muassa tietosuojaa koskevat vaikutusten arvioinnit, tietojen tuhoaminen, tietoturvan toteutuminen, mahdollisiin auditointeihin osallistuminen ja ilmoitukset henkilötietojen tietoturvaloukkauksista.

Luonnollisestikin rekisterin käsittelijän tulee toteuttaa toiminnassaan omalta osaltaan sekä tekniset että organisatoriset suojaustoimenpiteet, ja käsittelyssä tulee toteutua EU:n yleisen tietosuoja-asetuksen vaatimukset rekisteröityjen oikeuksien suojelemiseksi. Lähtökohtaisesti rekisterinpitäjällä on osoitusvelvollisuus tietosuojaperiaatteiden toteutumisesta silloinkin, kun käsittelijä käsittelee henkilötietoja rekisterin pitäjän lukuun. (Euroopan parlamentti ja Euroopan unionin neuvosto 2016.)

5.5.1 GDPR-asetuksen käyttöönottajan muistilista

Käyttöönottajan muistilista luvun sisältö pohjautuu aiemmin esiteltyihin kirjallisiin materiaaleihin sekä DSRM-prosessin myötä tehtyihin havaintoihin.

Organisaation ensisijainen tehtävä on asetuksen käyttöönotossa ja sen soveltamisessa varmistua henkilötietojen tietoturvasta ja niiden käsittelystä GDPR-asetuksen vaatimustenmukaisesti. Tietosuoja-asetuksen lähestymisnäkökulma on riskiperusteinen. Tietoturvallisuus sisältää teknisten suojaustoimien lisäksi prosessit ja hallinnolliset toimenpiteet. Kootusti listataan alle tärkeimmät muistettavat ja huomioon otettavat asiat GDPR-asetusta käyttöönotettaessa:

- rekisteriseloste(et) laadittava
- dokumentoiva, miten käsittelee henkilötietoja
- varmistettava ja dokumentoitava prosessit ja tietojärjestelmät, siten että henkilötietojen käsittelylle löytyy aina peruste, suostumus tai sopimus
- ulkoistettaessa henkilötietojen käsittely toiselle yritykselle on laadittava sopimus käsittelijän kanssa, ja varmistuttava että rekisteröityjen henkilöiden oikeudet on suojattu asetuksen vaatimusten mukaisesti
- asetuksessa määriteltyjen velvoitteiden täyttämiseksi prosessien ja järjestelmien varmistaminen sekä riittävä dokumentointi rekisteröityjen oikeuksien toteuttamiseksi ja tietovuototapauksissa ilmoittaminen
- tietynlaisissa tapauksissa ilmoitusvelvollisuus viranomaisille ja rekisteröidylle tietoturvaloukkauksesta 72 tunnin kuluessa loukkauksen ilmitulosta
- yrityksen tietosuojavastaavan nimeäminen
- jos yli 250 työntekijää yrityksessä, tulee laatia käsittelyselosteet
- vapaaehtoisesti laadittavalla tietotilinpäätöksellä voidaan täyttää GDPR-asetuksen todistusvelvoite

Ensimmäisiin käytännön tehtäviin kuuluu henkilötietoihin liittyvien data- ja tietovirtojen hahmottaminen. Inventoidaan, mitä henkilötietoja yrityksessä on ja kerätään, sekä mitä käyttötarkoitusta varten. Tämän jälkeen selvitetään, missä tiedot sijaitsevat sekä miten niitä käsitellään. Lisäksi on hyvä puntaroida henkilötietojen elinkaaren hallinnan prosesseja. Huomionarvoista on, että myös ulkoistettujen datavarantojen, esimerkiksi hyödynnettyjen pilvipalveluiden, suhteen on varmistuttava siitä, että kyseisten palveluiden tuottajat toimivat EU:n

yleisen tietosuoja-asetuksen mukaisesti. Mikäli ulkoistettuja palveluita käytetään, tulee päivittää tarvittaessa henkilötietojen käsittelyyn liittyvät sopimuslausekkeet palveluntarjoajien kanssa. Sopimusten on pitänyt olla EU:n yleisen tietosuoja-asetuksen mukaisia sen soveltamisen alkaessa eli 25.5.2018 alkaen.

Rekisterinpitäjän sekä käsittelijän tulee toteuttaa tarvittavat organisatoriset sekä tekniset toimenpiteet. Rekisterillä tarkoitetaan henkilötietoja sisältävää jäsenneltyä tietojoukkoa, josta tiedot ovat saatavilla. Vaatimusten mukaisen toiminnan teknisten ja hallinnollisten toimenpiteiden toteuttamisen ohella täytyy kirjallinen tietosuojaa koskevia käytäntöjä ja periaatteita koskeva dokumentaatio laatia tai päivittää, ja myös toimintaohjeiden tulee olla ajan tasalla. Riskiarvio on hyvä tehdä uhkatilanteiden varalle sekä myös dokumentoida, miten toimitaan tilanteessa, jossa henkilötiedot vaikkapa tietomurron seurauksena joutuvat väärin käsiin. On muistettava myös organisaation osoitusvelvollisuus. Se tarkoittaa sitä, että henkilötietojen käsittelyssä rekisterinpitäjän on pystyttävä osoittamaan noudattavansa GDPR-asetusta. Organisaation on kyettävä osoittamaan, mihin sen oikeus käsitellä henkilötietoja perustuu. Lähtökohtaisesti osoitusvelvollisuus tarkoittaa myös dokumentoinnin velvollisuutta. Käsittelyn laillisuus tai oikeusperusteet tulee olla selvillä ja periaatteet tulee dokumentoida asianmukaisella tavalla. Asetuksen mukaisesti organisaation tulee olla kyvykäs osoittamaan myös jälkikäteen toiminnassa huomioon otetuksi riskit sekä lainsäädännön vaatimukset. Ohjeistuksilla sekä koulutuksella voidaan edesauttaa kaikkien organisaatiossa työskentelevien toimimisen tietosuoja-asetuksen vaatimusten mukaisesti. Organisaatioissa on varauduttava rekisteröidyn tietopyyntöihin, vaatimuksiin tietojensa poistamiseksi ja niiden siirtämiseen. Tähän liittyy myös yleisellä tasolla henkilötietojen elinkaaren hallinnan prosessit. Organisaatioiden tulee myös varautua auditointeihin, joissa arvioidaan tehtyjä GDPR:n toimenpiteitä riippumattoman tahon toimesta. Kaikkien osapuolien on pystyttävä luottamaan tietojen käsittelyn asianmukaisuuteen GDPR-asetuksen vaatimusten mukaisesti.

5.5.2 GDPR-asetuksen soveltaminen jatkuvana prosessina

Tapausorganisaatiossa GDPR-asetuksen käyttöönotto tapahtui kevään 2018 aikana. Tämän jälkeen EU:n yleisen tietosuoja-asetuksen tulkintaa on tarkennettu eri viranomaistahojen, alan asiantuntijoiden ja oikeuskäytäntöjen myötä. Ajantasaisia suomennettuja että englanninkielisiä hyväksyttyjä ohjeita löytyy muun muassa Tietosuojavaltuutetun toimiston internetsivustolta. Nykyään Euroopan tietosuojaneuvosto tuottaa ohjeita ja suosituksia ollen vastaavanlainen EU:n tietosuojaviranomaisten yhteistyöelin kuin WP29 aikoinaan.

Yhtenä kuriositeettiesimerkkinä kerrottakoon evästeisiin ja niiden käyttöön liittyvästä suostumuskäytäntöjen muuttuneista linjauksista. Evästeisiin tallennettavat tiedot tai evästetiedot muihin tietoihin yhdistettäessä voivat johtaa luonnollisen henkilön profilointiin sekä tunnistamiseen (Euroopan parlamentti

ja Euroopan unionin neuvosto, 2016). Evästeasiaa on puitu eri viranomaistahojen toimesta ja oikeusteitsekin.

Alun perin GDPR-asetusta käyttöönotettaessa on tulkittu ainakin Suomessa, että päätelaitteen internetselaimen asetuksessa annettava suostumus riittää suostumukseksi ei-pakollisten evästeiden käyttöön. Traficomin vuonna 2019 antaman ohjeistuksen mukaan selaimen asetus on ollut edelleen riittävä, eikä internetsivuille tarvita käyttäjältä ei-pakollisten tietojen keräämiseksi suostumusta kysyvää teknistä ratkaisua, kuten esimerkiksi popup-ikkunaa erikseen. Sittemmin vuonna 2020 tietosuojavaltuutetun toimisto on määrännyt muuttamaan tapaa, jolla yritys pyytää suostumusta evästeiden käyttöön. Internetselaimelle asetusten kautta ei enää ollutkaan mahdollista antaa suostumusta muille kuin välttämättömien evästeiden käytölle. Traficom muutti yhteistyössä tietosuojavaltuutetun toimiston kanssa vuonna 2021 palveluntarjoajille laatimaansa evästeohjeistustaan vastaamaan tietosuojavaltuutetun linjausta. (Tietosuojavaltuutetun toimisto, 2020; Finlex, 2020; Traficom 2021.) On linjattu, että evästeille, jotka eivät ole välttämättömiä palvelun käytölle, tarvitaan GDPR-asetuksen mukainen suostumus käyttäjältä, ja käyttäjille on annettava mahdollisuus kieltäytyä ei-välttämättömistä evästeistä. Sivuston käyttäjältä ei tarvitse kysyä lupaa erikseen välttämättömien evästeiden asettamiselle. (Tietosuojavaltuutetun toimisto, 2020).

EU:n yleisen tietosuoja-asetuksen käyttöönotto ja sen soveltaminen käyttöönoton jälkeen vaatii ponnisteluja kaiken kokoisissa yrityksissä sekä organisaatioissa. Ajan tasalla on pysyttävä, ja GDPR-asetuksen vaatimusten mukainen toiminta henkilötietojen elinkaaren hallinnassa on jatkuva prosessi. Käyttöönoton jälkeenkin tulee kiinnittää huomiota tietosuojaan liittyvien riskien tunnistamiseen ja niiden ehkäisemiseen, riittävän kattavan ajantasaiseen dokumentaation ylläpitämiseen ja sisäisten toimintamallien kehittämiseen. Yhtenä ajankohtaisena esimerkkinä lakisääteinen viitekehys EU:n yleinen tietosuoja-asetus ruokkii organisaatioita kiinnittämään huomiota ja kehittämään holistisesta näkökulmasta tarkasteltuna kokonaisuudessaan tiedon hallintaa (Schoch, 2016).

5.6 Viestintä ja arviointi

Viestintä on olennainen osa tutkimusprosessia. Sen avulla esitellään ja jaetaan tutkimuksen tulokset sekä tutkijoille että muulle yleisölle. Esittelemällä artefaktit ja sen tuottamiseen liittyvä prosessi varmistetaan, että suunnittelutieteellisen tutkimuksen tulokset ovat hyödynnettävissä käytännössä sekä myös muissa tulevissa tutkimuksissa. (Hevner ym., 2004.) DSRM-prosessin viimeisessä vaiheessa arvioidaan asetettujen tavoitteiden saavuttamista. Arviointi voidaan toteuttaa selittävänä, jolloin artefaktia peilataan sen tietopohjalta löytyviin argumentteihin. Tällaista arviointia hyödynnetään erityisesti niissä tapauksissa, kun artefakti on hyvin innovatiivinen. Selittävää arviointia käytetään myös silloin, kun muunlaiset arviointimenetelmät eivät palvele arvioinnin tarkoitusta. (Hevner ym., 2004.)

Tässä tutkimuksessa kommunikoidaan tutkielmaraportin muodossa yleisölle ongelma ja sen tärkeys sekä tutkijoille että ammattilaisille. Vaiheeseen kuuluu myös tuoda esiin artefaktin hyödyllisyys, sen tietopohja, uutuusarvo sekä sen vaikuttavuus. (Peffers ym., 2008.)

Tapausorganisaatiossa tutkimuksen tuotoksia esiteltiin sekä kirjallisten materiaalien että dialogin avulla. Tutkimusprosessin aikana kerättyjen tutkimusaineistojen ja kollaboraation myötä inhimillinen pääoma – tietämys, syventyi. Kartutetun tietämyksen ja ymmärryksen lisäksi tapausorganisaatio sai käyttöönsä konkreettisia artefakteja, kuten työkaluja, kuvioita, kaavioita, muisti- ja tehtävälistoja ja viranomaistahojen tuottamia dokumentteja GDPR-käyttöönoton ja sen soveltamisen tueksi. Tutkimuksessa esiteltyä kehittelemääni kuvion 6 mukaista ratkaisumallia – tutkimukseen ja käytäntöön perustuvaa konstruktiota, voidaan hyödyntää sellaisenaan myös muissa pk-yrityksissä.

Tutkimustyön myötä tuotettu ratkaisu on ollut JSK Oy:ssä käytössä keväästä 2018 lähtien. Omistajayrittäjä Jorma Lifländerin 22.4.2022 antaman kirjallisten kommentoinnin mukaan (liite 2) valitut menetelmät ja työkalut tukivat toiminnan kehittämistä tietosuoja-asetuksen vaatimusten mukaiseksi. Menetelmien ja työkalujen hyödyllisyys konkretisoitui käytännön toteutuksessa tuottaen artefakteja käyttöönotettavaksi. Toinen suuri saavutettu hyöty on se, että kokonaisuudessaan tutkimustyö tuotti uutta informaatiota ja tietoa, joka jalostui tapausorganisaatiossa tietämykseksi. Lifländerin mukaan tutkimuksen tärkein anti onkin ymmärrys siitä, miten asioita tulee ja voi tehdä. Yritys on hyödyntänyt tiesuoja-asetuksen käyttöönoton jälkeen tutkimustyön antia muun muassa Tarmo-ohjelmiston uuden version kehitystyössä.

6 POHDINTAA JA JOHTOPÄÄTÖKSET

Tässä pro gradu tutkielmassa esitellään kehittelemäni mentaalitason ratkaisumalli tietosuoja-asetuksen käyttöönoton tueksi pk-yrityksissä. Tutkimustyön tuloksia sekä tuotoksia voidaan hyödyntää niin tutkimuksen kuin myös käytännön näkökulmista tarkasteltuna. Raportissa esitettyjä asioita voidaan soveltaa tai ottaa sellaisenaan käyttöön pienyritysympäristöissä sekä tiedon hallinnan kehittämisen toimissa että GDPR-asetusta käyttöönotettaessa. Lisäksi tutkielmaraportin sisältöä voidaan hyödyntää GDPR-asetuksen käytännön soveltamisessa sen käyttöönoton jälkeenkin. Raportti tarjoaa myös yksilötasolla informaatiota henkilötietoihimme kohdistuvista uhista ja riskeistä sekä oikeuksista.

6.1 Pohdintaluku

Tutkimus tuotti konkreettisen ratkaisun tutkimusongelmaan ”Miten EU:n yleisen tietosuoja-asetuksen käyttöönottoa voidaan tukea pienyrityksessä?” Tutkimus täytti perimmäisen tehtävänsä, ja GDPR-asetus käyttöönotettiin kehittämäni ratkaisumallin – etenemispolun, avulla SaaS-palvelutuottaja Järvi-Suomen Kiinteistökonsultit Oy:n ekosysteemissä vuoden 2018 keväällä.

Tapausorganisaatiolla ei ollut kertomansa mukaan ”mitään käsitystä, mitä meidän olisi pitänyt tehdä” (liite 2) tietosuoja-asetuksen implementoimiseksi. GDPR-asetuksen implementoinnin haasteet tapausorganisaatiossa olivatkin hyvin samankaltaisia kuin mitä aiemmin tehdyistä tutkimuksista on käynyt ilmi. Suureksi haasteeksi yleisellä tasolla organisaatioissa on koettu tietämättömyys siitä, miten ja millä tavoin ylipäätään käyttöönoton työtä tulisi tehdä. Toiseksi, kuten tässäkin tutkimuksessa, asetuksen sääntelyn alaisten henkilötietojen esiin kaiveleminen on koettu haasteelliseksi eri tallennuspaikoista, monimutkaisista järjestelmistä ja tietoverkoista. Kolmanneksi, tietosuoja-asetus on laaja eikä itsessään anna asetuksen täytäntöönpano-ohjeita. Tämä aiheutti paljon päänvaivaa tapausorganisaatossa ja tulkinnan haasteellisuus konkretisoitui

asetuksen artikloja sovellettaessa käytännön tosielämässä. Asetuksen sanamuotoihin, käsitteisiin ja terminologiaan liittyvät haasteet saattavat herättää epäröintiä, ja jopa ristiriitaisia tulkintoja että tilanteita organisaatioissa. Neljänneksi tilannetta ei ole yhtään helpottanut se, ettei kattavia viranomaisohjeita tai geneerisiä viitekehyksiä oltu julkaistu käyttöönoton tueksi ennen tietosuoja-asetuksen voimaan astumista, vaan organisaatioiden on itse määriteltävä ratkaisut säännösten käyttöönottamiseksi (Antignac ym., 2016; Bihari, 2018: De Hert ym., 2018; Fair & Januska, 2018; Kindt, 2018; Lievens & Verdoodt, 2018; Martinínez- Martinínez, 2018; 2018; Sirur, ym., 2018; Poullet, 2018; Stultjens, 2018; Tikkuinen-Piri ym., 2018; Wachter, 2018.)

Vaikka asetuksen voimaan tulemisesta on vierähtänyt jo neljä vuotta, organisaatiot edelleenkin painivat samankaltaisten ongelmien kanssa. Vuonna 2021 on julkaistu tietosuojavaltuutetun toimiston ja TIEKE:n toteuttaman verkkokyselyyn pohjatuen, että EU:n yleinen tietosuoja-asetus tunnetaan yrityksissä, mutta sen käytännön soveltamisessa on riittänyt haasteita. Kaikkein haasteellisimmiksi osa-alueiksi pk-yrityksissä on koettu osoitusvelvollisuus ja tietoturvaan liittyvät vaatimukset eli henkilötietojen käsittelyn turvallisuus. Lisäksi yritykset ovat toivoneet saavansa apua rekisteröityjen oikeuksia ja sekä informointia koskeviin alueisiin että vaikutustenarvointiin. (Simell, 2021.) Verkkokyselyn taustalla on yritysten tietosuojatietoisuutta kehittävä kaksivuotinen hanke GDPR2DSM (GDPR opening doors to the digital single market: SME centric online tools and support for leveraging the opportunity), jonka tavoitteena on auttaa suomalaisia yrityksiä parantamaan tietosuojaosaamistaan. Hankkeessa pyritään luomaan työkalu, jonka avulla yritys voi arvioida tietosuojakäytäntöjään. Ensimmäinen versio työkalusta julkaistiin 28.1.2022, ja sen odotetaan valmistuvan pk-yritysten avoimeen käyttöön lokakuun 2022 loppuun mennessä. (Tieke, 2022.)

EU:n yleisen tietosuoja-asetuksen tarkoituksena on varmistaa, että organisaatiot käsittelevät kansalaisten henkilötietoja laillisin perustein, jolloin pyritään varmistamaan tietojen turvallisuus, yksityisyys ja luottamuksellisuus. Toinen asetuksen tärkeänä päämääränä on edistää EU:ssa digitaalisten sisämarkkinoiden kehittymistä. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016.) Sähköistymisen ja digitaalisten palveluiden kehittämisen myötävaikutuksesta datan, tiedon ja informaation käsittelyn merkitys on kasvanut (Burgin, 2010; Hevner ym., 2010; Kooper, 2011; Tallon 2013; Smallwood, 2014; Guetat & Dakhli, 2015; Alhassan ym., 2016) ja vaikuttaisi eksponentiaalisesti kasvavan organisaatioissa (Junwoo ym., 2017). Dataa hyödynnetään entistä kattavammin eri toimialoilla. Henkilötiedot voidaan käsittää sähköisten palveluiden sekä digitalisaation polttoaineeksi. Uusi polttoaine – siis henkilötiedot, ruokkivat tarpeita kehitellä uudenlaisia päätelaitteita sekä palveluita ja niiden hyödyntämistä.

Informaatioidentiteetin (Watcher, 2018) turvaamisen ja yksilön tietosuojan toteutumisen merkitystä ei voi liiaksi korostaa, sillä pohjimmiltaan tällöin tarkastellaan fundamentaalista (Euroopan parlamentti, neuvosto ja komissio, 2012) digitaalisen maailman perusoikeuden toteutumista. Globaalien yritysten velvollisuus on noudattaa toiminta-alueensa kansallisia lakeja ja varmistettava vaati-

musten mukainen toiminta. Silti ei voi olla pohtimatta IoT-kehityksen ja muiden älykkäiden ympäristöjen mukanaan tuomaa kasvavaa (Junwoo ym., 2017) informaatiovirtaa (Kind, 2018; Tikkinen-Piri ym., 2018; Poullet, 2018), jossa informaatioidentiteettiä muokataan sisällyttäen siihen myös monenlaisia henkilökohtaisia sijainti- ja terveystietoja. Datan profilointimenetelmät voivat paljastaa yksityiskohtaisia tietoja käyttäjien identiteetistä ja yksityiselämästä (Junwoo, ym., 2017; Štitilis & Laurinaitis, 2017; Lievens & Verdoodt, 2018). Vaikka henkilöllä on oikeus vastustaa tietojensa käyttöä profiloinnissa, on sähköisten verkostojen hahmottaminen palveluiden käyttäjälle lähes mahdotonta. Big dataa hyödyntäen voidaan tunnistaa yleisiä suuntauksia ja korrelaatioita (Kindt, 2018; Poullet, 2018; Lievens & Verdoodt, 2018; Tikkinen-Piri ym., 2018), mutta myös saatetaan pyrkiä vaikuttamaan yksilöihin ja heidän toimintaansa. Sopivilla yhdistelmillä anonymisoitua henkilötietoa ja anonymisoimatonta, voidaan aiheuttaa yksilöllistä tai kollektiivista syrjintää, ja paljon myös muuta harmia (Hadziselimovic ym., 2017; Kindt, 2018; Štitilis & Laurinaitis, 2017; Wachter, 2018). Huomionarvioista olisi toimijoiden tai palveluntarjoajien vastuuntuntoisina tunnistaa ja ymmärtää, että tällöin muodostuu GDPR:ssa määriteltyä henkilötietoa, johon tulee soveltaa asetuksen mukaisia sääntelytoimia. Toisaalta kuluttajat eivät vain ole markkinointikoneiston hyödykkeitä, vaan he itse voivat hyötyä kerätyistä tiedoista (Junwoo ym., 2017; Kindt, 2018; Štitilis & Laurinaitis, 2017) ja voivat hyödyntää niitä vaikkapa terveydentilansa seurannassa.

Tieto on organisaation arvokkainta pääomaa, ja sen on sanottu olevan uusi öljy (Smallwood, 2014). Sen tarkoituksena on tuottaa arvoa sekä omistajalleen että sitä hyödyntäville (Kooper ym., 2011; Tallon ym., 2013; Guetat & Dakhli, 2015). Arvokkuudeltaan tietoa ja sen hallinnan osaamista voitaneen verrata esimerkiksi patenttisalkkuun tai pääomien sijoitustoimiin. Tiedon hallinnan ytimen voidaan ajatella muodostuvan tiedon pyramidin kolminaisuudesta: datasta, informaatiosta ja tietämyksestä. Pääomana tiedon arvo kasvaa sitä jalostettaessa ja jaettaessa, ja tiedon voidaan käsittää olevan digitaalisen datatalouden raaka- ja polttoainetta. Uusi polttoaine – henkilötiedot, ja niiden hyödyntämisen mahdollisuudet sekä uhat ovat havahduttaneet myös lainsäätäjät toimimaan. GDPR-asetus sääntelee organisaatiossa henkilötietojen keräämistä, säilytystä ja hallinnointia EU:ssa, ja silloin kun tietojen käsittely kohdistuu EU:n kansalaisiin (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

Tietosuoja-asetuksen velvoitteiden täyttämiseksi on organisaatioiden kiinnitettävä huomiota entistä enemmän henkilötietojen tiedon hallintaan, tietoturvaan ja riskien hallintaan. Käsitteenä yksityisyyden suoja toimii kehityshankkeissa tärkeänä keskustelun lähtökohtana, ja tuo keskustelu korostaa tiedon hallinnan (IG) tärkeyttä nostaen sen organisaatiostrategian etulinjaan (Schoch, 2016). Organisaatiot ovat paneutuneet tiedon hallinnan laajaan paradigmaan yhä tiiviimmin ensinnäkin tiukennetun lainsäädännön seurauksena, toiseksi tiedon arvon maksimoinnin ja sen suojaamisen vuoksi ja kolmanneksi organisaation selviytymisen ja kilpailukyvyn vahvistamiseksi (Blair, 2011; Tallon, 2013; Smallwood, 2014; Guetat & Dakhli, 2015).

Tapausorganisaatiossa tiedon hallinta, sen tukipilarit ja toiminnan osa-alueet (Guetat & Dakhli, 2015), ei suinkaan ole uusi asia ilmiönä, mutta omistajayrittäjän mukaan tutkimustyö konkretisoi nämä käsitteet ja niiden hyödyntämisen tiedon hallinnan kehittämisessä. Tiedon hallinta on nimittäin myös liiketoimintatiedon hyödyntämistä, jolloin toimintaan liittyvää ulkoista ja sisäistä tietoa analysoidaan systemaattisesti (Smallwood, 2014). Tiedon hallinnan osaaminen on myös selkeästi kilpailuvaltti sisältäen inhimillisen vuorovaikutuksen toimijoihin, dataan ja taustalla oleviin järjestelmiin (Kooper ym., 2011). Tapausorganisaatiolla on muun muassa rekisteröinti Valviran B luokkaan ja osoitetietoja hakeva systeemi DVV:n järjestelmästä, jollaista ei ole tarjota muilla saman toimialan yrityksillä. Tällöin tiedon hallinta sisältää siihen liittyvät teknologiat, dokumenttien hallinnan, tietämyksen ja liiketoiminnan jatkuvuuden hallinnan (Smallwood, 2014). Tietotalouden yhdeksi kestävimmäksi kilpailuedun lähteeksi esitän tietopääomaa. Tietopääoman sekä digitalisoidun datan arvon kasvun myötä ovat organisaatiot yhä enenevissä määrin kiinnittäneet huomiota tiedon hallintaan.

Tiedon hallinnan moottoriksi on esitetty tietoarkkitehtuuria (Guetat & Dakhli, 2015), ja tutkittu yritysarkkitehtuurin potentiaalia GDPR:n käyttöönotossa (Rozehnal & Vítêzslav, 2018). Tietoarkkitehtuurin systeemisen analyysin, jota tässä tutkimuksessa sovellettiin karkealla tasolla, otetaan huomioon sekä tiedon rakenteellinen että systeeminen monimutkaisuus. Tutkimuksessa keskityttiin etsimään vastauksia tutkimusongelmaan IG:n toiminnan osa-alueen menetelmiin ja työkaluihin viittaavien kysymysten avulla, miten ja millä työkaluilla tietosuoja-asetuksen käyttöönottoa voitaisiin tukea pienyrityksessä. (Guetat & Dakhli, 2015.) Yritysarkkitehtuurilähestymisnäkökulma olisi saattanut tarjota holistisemman lähestymistavan tiedon hallinnan ilmiöön, koska se vangitsee liiketoiminnan olennaiset asiat antaen tietoa yrityksen rakenteesta, niiden elementeistä ja suhteista. Kun yritys nähdään järjestelmänä, voidaan helposti seurata osien välisiä suhteita ja ratkaista ongelmia (Rozehnal & Vítêzslav, 2018). Tällöin tiedon laatu ja vaatimusten mukaisuus voidaan määritellä ekosysteemissään kiinnittäen tavoitteellisemmin ja kokonaisvaltaisemmin huomiota kuviossa 5 esitettyihin tiedon hallinnan tukipilareihin ja toiminnan osa-alueisiin. On ehdotettu käytettäväksi soveltuvin osin pk-ympäristöissä GDPR:n implementoimiseksi tunnettua TOGAF® (the open group architecture framework) kokonaisarkkitehtuuriviitekehystä, ja COBIT® (control objectives for information and related technology) saattaisi olla myös varteenotettava vaihtoehto (Rozehnal & Vítêzslav, 2018). Viitekehyksenä COBIT® auttaa IT-yritystä toteuttamaan EGIT (enterprise governance of information and technology) osakokonaisuutta, eli ymmärtämään hallintoa edistäen sekä asioiden suunnittelua että toteuttamista (Iivonen, 2021).

On yleisesti tunnettua, että pienemmissä ICT-palveluita tarjoavissa yrityksissä, joiden organisaatioon ei sisälly tietohallinnosta tai tietoturvasta vastaavaa henkilöstöä, joutuvat ponnistelemaan tietosuoja-asetuksen käyttöönottovaiheessa usein ulkopuolelta hankitun osaamisen turvin. Tässä tapaustutkimuksessa toimin konsultin roolissa ollen ulkopuolinen asiantuntija antaen toimeksi-

antajan kanssa käytyyn dialogiin pohjautuen suuntaviivoja, jotka auttoivat tekemään käyttökelpoisia ratkaisuja tapausorganisaation hyväksi.

Lähtötilanne ja muutostarpeet kartoitettiin yhteistyössä tapausorganisaation asiantuntijoiden kanssa iteratiivisen DSRM-prosessin vaiheiden aikana. Työkalut käytännön ongelman ratkaisemiseksi valikoituivat osin myös tutkijan omien mieltymysten ja vahvuuksien mukaan. Jonkin verran työlääksi JSK Oy:ssä koettiin rekisteröityjen tietojen esiin kaivelu ekosysteemistä nimenomaisesti jäsentelemättömien sisältöjen (Weintarub, 2013), käsittelemättömän informaation (Burgin, 2010), jäsentelemättömän datan merkkimuotoisen ilmentymien (Smallwood, 2014), rakenteettoman tiedon ja sinällään merkityksettömien yksittäisten dataentiteettien osalta. Henkilötietodataentiteettien kartoittamisessa olisi voitu käyttää jotain kaupallista työkalua tai liiketoimintakumppani ohjelmistotalo olisi sellaisen voinut jopa koodata. Koska tutkittavalla kohteella on vahva asiantuntijuus ja tietämys tiedon hallinnan ympäristöstään, sellaisen hyödyntämistä ei katsottu tarpeelliseksi selvitettäessä rekisteröityjen tietoja. Kaupallisten työkalujen sijaan työskentelyssä kohdeyrityksen kanssa hyödynnettiin tarjolla ollutta vapaasti saatavilla olevaa taulukointityökalua (kuvio 14) asetuksen implementoinnin tukena. Erilaisten kaupallisten työkalujen ja palveluiden hankkiminen vaatii aina resursseja, ja niihin liittyvä kustannukset saattava olla joillekin yrityksille kynnyskysymys (vrt. Wilkinson, 2018).

Iteratiivisen tutkimusprosessin aikana dataa ja informaatiota prosessoimalla kasvatettiin tietämystä (Hevner ym., 2010; Leppänen, 2014) tutkimuksen ja organisaation käyttöön päätöksenteon tueksi (Tallon ym., 2013). Haastattelujen ja havainnoinnin avulla kerättiin tietoa tapausorganisaatiosta ja sen ekosysteemistä. Tämä mahdollisti tutkimuksen teoreettis-käsitteellisen viitekehyksen soveltamisen tosielämän käytännön kontekstiin. Tutkimusprosessin aikana kerätty ja koostettu data ja informaatio jalostuivat tietämykseksi (Burgin, 2010) sekä tutkimuksessa että tapausorganisaatiossa hyödynnettäväksi. Tutkimustyön konstruktio, jonka kehittelemäni mentaalitason rakennelma esitellään kuviossa 6, tuotti ratkaisumallin, jonka etenemispolun avulla GDPR-asetus otettiin käyttöön tapausorganisaatiossa Järvi-Suomen Kiinteistökonsultit Oy:ssä kevään 2018 aikana. Vaikka ratkaisu on tuotettu tietyn yrityksen tarpeisiin, on tässä raportissa esitellyt löydökset, havainnot ja artefaktit hyödynnettävissä sellaisenaan myös muissa pienyritysympäristöissä GDPR-asetusta sekä käyttöönotettaessa ja sitä sovellettaessa. Ratkaisumallia, joka pohjautuu sekä suunnittelutieteellisen tutkimuksen periaatteisiin että käytäntöön, voidaan hyödyntää sellaisenaan muissa pk-yrityksissä GDPR-asetusta käyttöönotettaessa. Lisäksi bonuksena, ennakkoon asetettujen tavoitteiden yli, tutkimus tuotti syötteitä tietosuojavaatimusten sisällyttämistä osaksi kehitysyhteistyötä toimeksiantajan Tarmo-ohjelmistokehittäjien kanssa. Se auttoi keskustelemaan kehitystarpeista ja suunnittelemaan yhteistyössä sekä toiminnallisia, teknisiä että prosessilähtöisiä ratkaisuja GDPR-asetuksen vaatimusten täytäntöönpanoksi JSK Oy:n ekosysteemissä. EU-yleisen tietosuoja-asetuksen vaatimusten mukainen toiminta on jatkuva prosessi. Työn toimeksiantaja, tapausorganisaatio, on hyödyntänyt käyttöönoton jälkeenkin tutkimusprosessin hedelmiä. Vuoden 2022 puolella

valmistuu Saas-palveluna tarjottavasta Tarmo-ohjelmistosta uusi versio, jonka kehitystyössä on hyödynnetty tämän pro gradu -tutkielman antia.

Täten, tutkimustyö täytti tavoitteensa tuottaen tietämystä sekä artefakteja, joiden avulla EU:n yleistä tietosuoja-asetuksen käyttöönottoa voidaan tukea pienyrityksessä. Tapausorganisaation omistajayrittäjän ja toimitusjohtaja Jorma Liflländerin mukaan (liite 2) tutkimuksessa esitellyt menetelmät ja työkalut tukivat GDPR-asetuksen käyttöönottoa ja sen soveltamista sekä avasivat uudenlaisia näkökulmia tiedon hallinnan ilmiöön. Sopimukset ja muu dokumentaatio päivitettiin sekä yrityksen osalta että alihankkijoiden suuntaan GDPR:n vaatimusten mukaiseksi. Tapausorganisaatio on kehittänyt henkilötietojen käsittelyn prosesseja sekä rekisterinpitäjän että käsittelijän roolissa. Lisäksi JSK Oy on pystynyt konsultoimaan omia asiakkaitaan GDPR-asetukseen liittyvissä käytännön kiemuroissa. Liflländerin mielestä tutkimuksen merkittävin anti käytännön tosielämään onkin ymmärrys siitä, miten asioita voi ja tulee tehdä tietosuoja-asetuksen vaatimustenmukaisuuden toiminnan sekä toteuttamiseksi että osoittamiseksi.

6.2 Tutkimuksen rajoitukset, arviointi ja luotettavuus

Tutkimuksen lähtökohtana oli monimenetelmäistä tutkimusotetta hyödyntäen tuottaa ratkaisu toimeksiantajan JSK Oy:n tarpeisiin. Tämän lisäksi kapea-alaisuutta tutkimuksessa saattaa aiheuttaa se, että empiiristä tutkimusta varten tietoa ja aineistoja kerättiin vain yhdestä tapauksesta. Tapaustutkimus tutkimusstrategiana sisältää aina lähtökohtaisesti erilaisia aineistoja ja menetelmiä vastatakseen asetettuun tutkimusongelmaan (Hirsjärvi ym., 2010; Golafshani, 2003). Tässä laadullisessa tutkimuksessa monimenetelmäisellä lähestymistavalla pyrittiin ymmärtämään ilmiöitä todellisen maailman ympäristössä, jota tutkija ei manipuloi tietoisesti (Patton, 2001 s. 39, Golafshani, 2003 mukaan). Triangulaation avulla on mahdollista lisätä tutkimuksen luotettavuutta sekä väitteiden totuudenmukaisuutta (Golafshani, 2003).

Kaiken tutkimuksen reliabiliteettia ja validiteettia tulisi arvioida (Hirsjärvi, ym., 2010). Kyseiset käsitteet ovat saaneet erilaisia tulkintoja, ja termeinä käytettäväksi ne eivät ole ideaalisia arvioitaessa laadullista tutkimusta (Hirsjärvi, ym., 2010; Golafshani, 2003). Sen sijaan laadullista tutkimusta arvioitaessa voidaan käyttää seuraavia sanoja: uskottavuus, siirrettävyys, luotettavuus, laatu ja kurinalaisuus (Golafshani, 2003). Tutkimus voidaan käsittää tieteellisesti pätevästi silloin kun tutkiminen on ollut järjestelmällistä ja tuottanut tutkittavista ilmiöistä tarkentavaa tietoa (Hirsjärvi ym., 2010). Tutkimustyössä pyrittiin järjestelmällisyyteen sekä yleistettävyyteen. Kaikkia yksittäisiä tutkimuksen aikana ilmenneitä kapeikkoja tai oivalluksia ei ole tarkoituksenmukaista raportissa lähteä selvittämään, koska organisaatiot ovat aina uniikkeja ekosysteemejä. Vaikka tutkimuksen ratkaisu on tuotettu tiettyyn ekosysteemin, on tutkimusprosessi – GDPR:n käyttöönoton etenemispolku, toistettavissa kuviossa 6 esitellyn ratkaisumallin avulla muissa pk-ympäristöissä. Raportissa esitetyt viitekehykset, teo-

reettiset ja käytännön näkökulmat ja artefaktit ovat siirrettävissä sellaisenaan hyödynnettäviksi pk-yrityksiin.

Tausta-aineistona (Templier & Paré, 2015) toimineen kirjallisuuskatsauksen toteuttamisessa pyrittiin järjestelmällisyyteen (Machi & Evoy, 2016) sekä selostamaan sen läpivienti raportissa sellaisella tarkkuudella, jotta se on toistettavissa samoin löydöksin. Aineistojen ensisijaisena valintakriteerinä toimivat laatutekijät. Kirjallisuutta kerättiin monitieteisestä vertaisarvioidusta kirjallisuuden viittaus- ja tiivistelmätietokannasta. Tausta-aineistoon lukeutui myös tunnettujen tutkimus- ja konsultointiyritysten sekä tietokirjailijoiden tuottamia materiaaleja. Lisäksi käytännönläheisen tutkimusongelman ratkaisemisessa hyödynnettiin eri viranomaistahojen tuottamia dokumentteja. Tarkkuus koskee tutkimuksen kaikkia vaiheita, joten tutkimuksen luotettavuutta kohentamaan selostetun kirjallisuuskatsauksen lisäksi myös DSRM-prosessin toteuttaminen JSK Oy:n ekosysteemissä kuvattiin raportissa tarkasti (Hirsjärvi ym., 2010) – milteipä kurinalaisesti – vaihe vaiheelta. Tutkimusraportin luotettavuuden ylläpitämiseksi myös sen puhtaaksikirjoittamisen aikana hyödynnettiin systemaattisesti koostettua ja ylläpidettyä tutkimuspäiväkirjaa, josta löytyy tutkimuksessa käytetyt aineistot ja sen konkreettiset tapahtumat.

Kvalitatiivisessa tutkimuksessa on aina tavoitteena saavuttaa syvällistä ymmärrystä tutkittavasta kohteesta (Golafshani, 2003). Tiedon lisäämiseksi sekä käsitysten syventämiseksi tämän tutkimuksen käyttöön kerättiin kielellisesti käsiteltävää raaka-ainetta, dataa (Burgin, 2010), kirjallisuuskatsauksen lisäksi haastattelujen ja havainnoinnin avulla. Näin täydennettiin muun muassa muistiinpanojen ja kuvioiden muodossa suunnittelutieteellisen DSRM-prosessin aikana kokonaisvaltaista tiedon ja aineistojen hankintaa luonnollisessa kontekstissa ja todellisissa tilanteissa (Hirsjärvi ym., 2010). Esimerkiksi lähtötilanne ja muutostarpeet kartoitettiin yhteistyössä tapausorganisaation edustajan kanssa. Lisäksi iteratiivisen tutkimusprosessin aikana arvioitiin yhteistyössä toimeksiantajan asiantuntijoiden kanssa artefaktien toimivuutta tapausorganisaation ekosysteemissä. Tutkimukseen osallistuvat auttoivat tutkijaa tutkimusongelman ratkaisemisessa, ja useiden menetelmien sekä aineistojen käyttö johtivat pätevämpään, luotettavampaan ja monipuolisempaan todellisuuden rakentamiseen (Golafshani, 2003).

Tutkimustyön myötä esitellyt käytännön esimerkit sitovat teoreettisen tarkastelun tosielämään. Teoreettinen tarkastelu puolestaan tukee ja vahvistaa käytännönläheisen aineiston käyttökelpoisuutta. Luottamusta tutkimustuloksiin luo myös tapausorganisaation omistajayrittäjän Jorma Lifländerin antama kirjallinen (liite 2) palaute. Kommentit puolustavat tutkimuksen onnistumista luoden luottamusta raportissa esiteltyihin löydöksiin (Golafshani, 2003) ja tutkimustuloksiin.

6.3 Johtopäätökset

Tiedon kolminaisuus – data, informaatio ja tietämys, on tiedon hallinnan ytimessä. Tiedon hallinnan merkitys on kasvanut vuosikymmenten saatossa. Ensinnäkin tiedon hallinta yhä kiihtyvällä vauhdilla digitalisoituvassa datatalouden toimintaympäristössä on kriittinen menestystekijä. Täten tieto, tuo arvokas kilpailuvaltti ja sekä keskeisin aineeton pääoma, tukee kaikkia päätöksiä sekä strategisella että operatiivisella ratkaisutasolla. Toiseksi tiedon hallinta auttaa organisaatioita suojaamaan omistamansa tiedon arvon, ja sen avulla voidaan tasapainottaa tiedon hallinnan riskejä suhteessa tiedon tuottamaan arvoon. Tietopääoma on arvokkain aineeton organisaation omaisuuserä. Organisaatio tarvitsee sekä hallinnon että hallinnan ekosysteemin, jonka avulla tiedon hallintaa toteutetaan.

Tiedon hallinnan abstraktio on laaja. Kuviossa 5 esitelty holistinen tiedon hallinnan teoreettinen viitekehys auttaa palasteltuna tukipilareihin ja toiminnan osa-alueisiin soveltamaan sitä käytännön kontekstissa. Tällainen lähestymisnäkökulma mahdollistaa inhimillisen vuorovaikutuksen toimijoihin, dataan ja järjestelmiin sekä muihin taustalla oleviin systeemeihin. Tiedon hallinnan ydintä ympäröivät neljä toiminnan osa-aluetta: 1) organisaatio ja liiketoiminta, 2) kommunikaatio ja muutoshallinta, 3) arkkitehtuuri sekä 4) menetelmät ja työkalut mahdollistavat sekä tukevat tiedon hallinnan aktiviteettien käytännön toteuttamista. Toiminnan osa-alueita kehystävät neljä tiedon hallinnan tukipilaria: a) organisaation politiikka ja strategia, b) tiedon laatu, c) tietoturva sekä d) lakien ja sääntelyn noudattaminen. Lain ja sääntelyntoimien noudattamatta jättäminen aiheuttaa organisaatiolle merkittävää haittaa muun muassa hallinnollisten sakkojen, mainehaitan tai luottamuksen menettämisen merkeissä. Tällöin lait ja sääntelytoimien tukipilarin tehtävänä on auttaa lainsäädännön noudattamisessa, toiminnan läpinäkyvyydessä ja estää tai vähentää lakisääteisiä sanktioita ja muita haittavaikutuksia. EU:n yleinen tietosuoja-asetus on yksi esimerkki lainsäädännöllisestä viitekehyksestä, joka on patistanut organisaatioita kiinnittämään huomiota henkilötietoihin, perkaamaan ja kehittämään sekä hallinnon että hallinnan toimia. Hallinnon avulla johdetaan ja ohjataan organisaation toimintaa. Sen strategisena tehtävänä on asettaa organisaatiossa kehykset tavoitteille, suunnalle ja rajoituksille sekä valvoa niiden toteutumista. Hallinta huolehtii operatiivisella tasolla muun muassa resurssien jakamisesta ja päivittäisestä toiminnan kehittämisestä ja valvonnasta.

Henkilökohtaisten tietojemme käsittely asianmukaisilla tavoilla on yksi aikakautemme suurista haasteista digitaalisen datatalouden syövereissä tietopääoman ollessa sen arvokkain kilpailuvaltti. EU:n yleisen tietosuoja-asetuksen, joka tuli voimaan 25.5.2018, ensisijainen tavoite on turvata yksilön oikeudet omiin henkilötietoihinsa. Toiseksi tietosuoja-asetus luo yhtenäiset pelisäännöt ja olosuhteet digimarkkinoille, ja kolmanneksi sen sääntelytoimilla edesautetaan digitaalisen talouden kehitystä EU:ssa. Tietosuoja-asetuksen käyttöönottoa ja sen soveltamista on hankaloittanut ensinnäkin sen laajuus ja tulkinnan moni-

mutkaisuus. Toiseksi asetuksen sääntelyn alaisten henkilötietojen esiin kaiveleminen on haasteellista monimutkaisista tietojärjestelmistä ja -verkoista. Tietosuoja-asetuksen voimaan astuessa tilannetta ei yhtään helpottanut se, ettei kattavia viranomaisohjeita tai geneerisiä viitekehyksiä oltu julkaistu sen implementoimiseksi. Näiden seikkojen vuoksi GDPR:n käyttöönotto ja sen vaatimustenmukainen toiminta on kaikenkokoisissa organisaatoissa haastavaa.

EU sekä kansalliset toimijat ovat kehittäneet tietosuoja-asetuksen käytännön soveltamisen tueksi ohjekokonaisuuksia ja työkaluja. Jatkotutkimusta ajatellen yksi kiinnostava alue voisi olla selvittää, miten tällä hetkellä kaikille helposti saavutettavat työkalut ja soveltamisohjeet ovat vastanneet pk-sektorilla toimivien yritysten tarpeisiin, ja onko käytettävissä oleva aineisto jalostettu riittävän selkeäksi, sekä onko niitä pystytty hyödyntämään. Markkinoilta löytyy myös kaupallisia systeemejä ja työkaluja. Voisi olla mielenkiintoista vertailla onko merkitystä sillä, päätyykö organisaatio valitsemaan kaupallisen toimijan tuottaman systeemin GDPR:n käyttöönoton tueksi vai vapaasti saatavilla olevan. Kenties olisi myös mahdollista hyödyntää tutkielmaraportissa esittelemääni (kuvio 6) metatason ratkaisumallia jossakin toisessa pienyrityksessä. Näin saataisiin tietoa, toimiiko ratkaisumalli muissa ympäristöissä, ja mitä kehitettävää siinä on. Lisäksi saataisiin kokemusta, ovatko raportissa esitellyt artefaktit GDPR:n käyttöönottamiseksi ja sen soveltamiseksi käyttökelpoisia muissa konteksteissa tapausorganisaation lisäksi. Mielenkiintoista olisi myös koestaa sekä puntaroida GDPR2DSM-hankkeen myötä lokakuussa 2022 julkaistavan työkalun ominaisuuksia tietosuoja-asetusta käyttöönotettaessa sekä sovellettaessa. Pk-yritysten parissa toteutettava jatkotutkimus auttaisi muodostamaan käsityksen siitä, millaista tukea yritykset tarvitsevat tai millaiseen suuntaan ohjeita ja työkaluja tulisi edelleen kehittää. Samalla voisi syntyä myös uusia suuntia akateemiselle tutkimukselle kehittää olemassa olevia tutkimusmenetelmiä tai viitekehyksiä, ja tuottaa hedelmällistä yhteistyötä tietojärjestelmien tutkijoiden ja yritysmaailman välisen vuorovaikutuksen kehittämiseksi kokonaisuudessaan tiedon hallinnan kehittämisen pelikentällä.

Tutkimustyöni osoitti, että ulkopuolinen apu ei vielä yksinomaan ratkaise GDPR:n käyttöönoton haasteita, vaan yrityksen sisäinen henkilötietojen käsittelyn toteutustapa ja käytännöt vaativat yrityksen ekosysteemiä ja liiketoimintaprosessia tuntevien henkilöiden aikaa ja sitoutumista. Vain siten kehityskohteet saadaan tunnistettua ja suunniteltua sekä kehittämisen toimia että artefakteja. JSK Oy:n tapaus osoitti myös sen, että käytettävien tietojärjestelmien ohjelmistokehitys vaatii aikaa ja taloudellisia resursseja. Tutkimustyön olennaisimmin saavutuksen kiteyttää tapausorganisaatio omistajayrittäjän kommenttilause: ”Suurin hyöty toiminnassamme tämän asian suhteen (GDPR) on ollut juuri tuo ymmärrys, mitä asioita on pitänyt tehdä.”

Tutkielman antia voidaan hyödyntää niin jatkotutkimuksessa kuin myös organisaatioissa käytännön näkökulmista tarkasteltuna. Tämän lisäksi tietosuoja-asetus on yksilönkin tietoturvan sekä oikeuksien näkökulmasta tarkasteltuna kiinnostava. Tutkimustyön myötä esiin nostetut asiat hoksauttavat myös yksilötasolla meitä kiinnittämään huomiota henkilötietojemme käsittelyyn ja niiden

suojaamiseen. EU:n yleisellä tietosuoja-asetuksella lisätään sekä henkilötietojen käsittelyn avoimuutta että läpinäkyvyyttä. Sen avulla vahvistetaan rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä. Tietoja meistä ei pelkästään kerätä ensisijaista käyttötarkoitustaan varten, kuten palvelun käytön mahdollistamista varten, vaan meistä saatetaan vaivihkaa kerätä dataa toissijaisia käyttötarkoituksia varten. Näiden kerättyjen henkilötietojen avulla seurataan toimintaamme vaikkapa personalisoituja palveluita tai mainontaa varten. Emme välttämättä ole huomanneet antaneemme suostumusta tietojen keräämiselle tai niiden luovuttamiselle eteenpäin. Pahimmillaan vääriin käsiin joutuneilla henkilötiedoilla voidaan aiheuttaa yksilölle henkistä tai taloudellista vahinkoa. GDPR-asetuksen myötä meillä on oikeus henkilökohtaisten tietojen tarkistamiseen, siirrettävyyteen, poistamiseen ja ennen kaikkea tietoon siitä, missä kaikkialla henkilötietojamme käsitellään ja miten niiden tietoturvasta huolehditaan.

LÄHTEET

29 artiklan mukainen tietosuojatyöryhmä. (2018.) *Suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi.* Haettu osoitteesta 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?t=1539252124000

Alhassan, I., Sammon, D. & Daly, M. (2016). Data governance activities: An analysis of the literature. *Journal of Decision Systems, 25(1)*, 64-75.

Antignac, T., Scandariato, R. & Schneider, G. (2016). A privacy-aware conceptual model for handling personal data. Teoksessa T. Margaria & B. Steffen (toim.), *Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques. ISoLA 2016. Lecture Notes in Computer Science, vol 9952. (942-957).* Cham: Springer.

Bihari, E. (2018). GDPR - A Y2K-II for business? *Edpacs, 57(2),* 1-9.

Blair, B. T. (2011). *Making the case for information governance - 10 reasons why IG makes sense*. Haettu osoitteesta https://barclaytblair.files.wordpress.com/2011/08/making-the-case-for-information-governance-barclay-t-blair.pdf

Blix, F., Elshekeil, S. A. & Laoyookhong, S. (2017). Data protection by design in systems development: From legal requirements to technical solutions. Teoksessa *12th International Conference for Internet Technology and Secured Transactions (ICITST), (98-103).* IEEE Xplore.

Burgin, M. (2010). *Theory of information: Fundamentality, diversity and unification*. Singapore: World Scientific Publishing Co. Pte. Ltd.

Cavoukian, A. (2010). *Privacy by desing - the 7 foundational principles, implementation and mapping of fair information practies*. Haettu osoitteesta https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L. & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law and Security Review, 34(2),* 193-203.

Donaldson, A. & Walker, P. (2004). Information governance - a view from the NHS. *International Journal of Medical Informatics, 73(3),* 281-284.

Euroopan komissio. (2010). *Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, Kattava lähestymistapa henkilötietojen suojaan Euroopan unionissa.* Haettu osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri =CELEX:52010DC0609&from=FI

Euroopan komissio. (2012). *Euroopan parlamentin ja neuvoston asetus yksiöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus)*. Haettu osoitteesta https://eur-lex.europa.eu/ legal-content/FI/TXT/PDF/?uri=CELEX:52012PC0011&from=FI

Euroopan komissio. (2015). *Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, digitaalisten sisämarkkinoiden strategia Euroopalle*. Haettu osoitteesta https://eur-lex. europa.eu/legal-content/FI/TXT/PDF/?uri =CELEX:52015DC0192&from=FI

Euroopan parlamentti ja Euroopan unionin neuvosto. (2016). *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).* Haettu osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/? uri=CELEX :32016R0679

Euroopan parlamentti ja neuvosto. (1995). *Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta*. Haettu osoitteesta https://eur-lex.europa.eu /legal-content/FI/TXT/PDF/?uri=CELEX:31995L0046&from=FI

Euroopan parlamentti ja neuvosto. (2015, Syyskuu 30,). Sähköisen viestinnän sääntelyjärjestelmä. Haettu osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=LEGISSUM:l24216a

Euroopan parlamentti, neuvosto ja komissio. (2012). *Euroopan unionin perusoikeuskirja (2012/c 326/02)*. Haettu osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:12012P/TXT

Euroopan yhteisöjen komissio. (2009). *Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, Esineiden internet - toimintasuunnitelma Euroopalle.* Haettu osoitteesta https:// data.consilium.europa.eu /doc/document/ST-11223-2009-INIT/fi/pdf

European Data Protection Board. (2018). Tietoa Euroopan tietosuojaneuvostosta. Haettu 23.3.2022 osoitteesta https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_fi

Faifr, A. & Januska, M. (2018.) Companies´ readiness of GDPR and implementation barriers. Teoksessa J. Rotschedl & K. Cermakova (toim.) *41st international academic conference, Venice, (31-49).* Praha: International Society of Social and Economic Sciences.

Finlex. (2018, 5. joulukuuta). Tietosuojalaki. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2018/20181050

Finlex. (2020, 14. toukokuuta). Evästeisiin annettu suostumus. Haettu osoitteesta https://finlex.fi/fi/viranomaiset/tsv/2020/20200561

Fu, X., Wojak, A., Neagu, D., Ridley, M. & Kim, T. (2011). Data governance in predictive toxicology: A review. *Journal of Cheminformatics, 3(24),* 1-16.

Gartner. (2018, 26. kesäkuuta). IT glossary. Haettu osoitteesta https://www.gartner.com/it-glossary/information-governance

Gellert, R. (2018). Understanding the notion of risk in the general data protection regulation. *Computer Law and Security Review, 34(2),* 279-288.

Goddard, M. (2017). The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research,* 59(6), 703-705.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitive Report,* 8(4), 597-607.

Guetat, S. B. A. & Dakhli, S. B. D. (2015). The architecture facet of information governance: The case of urbanized information systems. *Procedia Computer Science, 64*, 1088-1098.

Hadziselimovic, E., Fatema, K., Pandit, H. & Lewis, D. (2017). Linked data contracts to support data protection and data ethics in the sharing of scientific data. Teoksessa Garijo, D., Hage, W., Kauppinen, T., Kuhn, T. & Zhano, J. (toim.) *Proceedings of the first workshop on enabling open semantic scienceco-located with 16th International Semantic Web Conference (ISWC 2017)* (55-62). Enabling Open Semantic Science.

Hevner, A., Chatterjee, S., Gray, P. & Baldwin, C. Y. (2010). *Design research in information systems: Theory and practice*. New York: Springer.

Hevner, A., Marh, S., Park, J. & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28(1),* 75-105.

Hirsjärvi, S., Remes, P., Sajavaara, P. & Sinivuori, E. (2010). *Tutki ja kirjoita.* (15.-16. painos). Helsinki: Tammi.

Iivonen, J. (2021, 23. elokuuta). COBIT2019 – Enterprise governance for information and technology. Haettu osoitteesta https://blog.wakaru.fi/2021/08/23/ cobit-2019-enterprise-governance-for-information-and-technology/

Junwoo, S., Kyoungmin, K., Mookyu, P., Moosung, P. & Kyungho, L. (2017). An analysis of economic impact on IoT under GDPR. Teoksessa *2017 international conference on information and communication technology convergence (ICTC) (879-881).* IEEE Xplore.

Järvi-Suomen Kiinteistökonsultit Oy. (2018a, 27. huhtikuuta). Rekisteri- ja tietosuojaseloste. Haettu 25.5.2018 osoitteesta https://www.kiinteistokonsultit.fi/images/tarmo/Kiinteistkonsultit_rekisteriseloste_asiakasrekisteri_270418.pdf

Järvi-Suomen Kiinteistökonsultit Oy. (2018b). Toimitussopimuksen liite. Haettu 12.3.2022 osoitteesta https://vaasankorttelihuolto.fi/wp-content/uploads/Tarmo-tietosuojaliite.pdf

Kabanov, I. (2016). Effective frameworks for delivering compliance with personal data privacy regulatory requirements. Teoksessa *14th annual conference on privacy, security and trust, PST 2016 (551-554).* New Jersey: IEEE.

Khan, J. (2018). The need for continuous compliance. *Network Security, 2018(6),* 14-15.

Khatri, V. & Brown, C. V. (2010). Designing data governance. *Communications of the ACM, 53(1),* 148-152.

Kindt, E. J. (2018). Having yes, using no? about the new legal regime for biometric data. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34(3),* 523-538.

Kooper, M. N., Maes, R. & Lindgreen, R. (2011). On the governance of information: Introducing a new concept of governance to support the management of information. *International Journal of Information Management, 31*(3), 195-200.

Kotimaisten kielten keskus. (2017). Kielitoimiston sanakirja. Haettu osoitteesta https://www.kielitoimistonsanakirja.fi/netmot.exe?motportal=80

Leppänen, M. (2014). *TJTSM54 advanced topics system development -kurssin oppimateriaali.* Tietojenkäsittelytieteiden laitos: Jyväskylän yliopisto.

Lievens, E. & Verdoodt, V. (2018). Looking for needles in a haystack: Key issues affecting children's rights in the general data protection regulation. *Comput-*

er Law & Security Review: The International Journal of Technology Law and Practice, 34(2), 269-278.

Machi, L. A. & McEvoy, B. T. (2016). *The literature review: Six steps to success.* (Third edition). California: Sage Publications Ltd.

Martínez-Martínez, D. (2018). Unification of personal data protection in the european union: Challenges and implications. *El Profesional De La Información, 27*(1), 185.

OECD. (2015). *G20/OECD principles of corporate governance*. Paris: OECD Publishing.

Oikeusministeriö. (2018a, 1. maaliskuuta). Tietosuojalaki täydentäisi EU:N tietosuoja-asetusta. Haettu osoitteesta https://oikeusministerio.fi/artikkeli/-/asset_publisher/tietosuojalaki-taydentaisi-eu-n-tietosuoja-asetusta

Oikeusministeriö. (2018b, 5. joulukuuta). Uusi tietosuojalaki voimaan vuoden 2019 alusta. Haettu osoitteesta https://oikeusministerio.fi/ artikkeli/-/asset_publisher/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta

Ostrowski, L. & Helfert, M. (2012). Reference model in design science research to gather and model information. Teoksessa *18th Americas Conference on Information Systems 2012, AMCIS 2012, (3490-3499).* Atlanta: Curran Associates, Inc.

Passmann, S., Lauber-Roensberg, A. & Strufe, T. (2017). Privacy-preserving audience measurement in practice - opportunities and challenges. Teoksessa *2017 IEEE Conference on Communications and Network Security (444-449).* IEEE.

Patton, M. Q. (2002). *Qualitative evaluation and research methods*. (3 painos). Thousand Oaks, CA: Sage Publications, Inc.

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. (2008). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77.

Pormeister, K. (2017). The GDPR and big data: Leading the way for big genetic data? Teoksessa A. Mitrakas, E. Schweighofer, K. Rannenberg & H. Leitold (toim.), *Privacy technologies and policy. APF 2017. Lecture notes in computer science (3-18).* Cham: Springer.

Poullet, Y. (2018). Is the general data protection regulation the solution? *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34(4),* 773-778.

Pulkkinen, M. (2018). *TJTS505 graduseminaari -luennot*. Tietojärjestelmätieteen laitos: Jyväskylän yliopisto.

Quelle, C. (2016). *Not just user control in the general data protection regulation: On the problems with choice and paternalism, and on the point of data protection*. New York: Springer.

Rozehnal, P. & Vítězslav, N. (2018). The core of enterprise architecture as a management tool: GDPR implementation case study. Teoksessa Doucek, P., Chroust, G. & Oškrdal, V. (toim.), *26th Interdisciplinary Information Management Talks: Strategic Modeling in Management, Economy and Society, IDIMT 2018, (359-366).* Kutná Hora: Trauner Verlag.

Schoch, T. P. (2016). EU Privacy Regulations' Impact on Information Goverance. *Information Management. 1(50),* 20-24.

Simell, T. (2021, 14. huhtikuuta). Tietosuoja-asetus tunnetaan, mutta käytännön soveltamisessa riittää vielä haasteita. Haettu 30.3.2022 osoitteesta https://tieke.fi/tietosuoja-asetus-tunnetaan-mutta-kaytannon-soveltamisessa-riittaa-viela-haasteita/

Sirur, S., Nurse, J. & Webb, H. (2018). Are we there yet?: Understanding the challenges faced in complying with the general data protection regulation (GDPR). Teoksessa *Proceedings of the International Workshop on Multimedia Privacy and Security (MPS) at the 25th ACM Conference on Computer and Communications Security (CCS), (88-95).* ACM.

Smallwood, R. F. (2014). *Information governance: Concepts, strategies, and best practices*. New Jersey: John Wiley and Sons, Inc.

Sokolovska, A. & Kocarev, L. (2018). Integrating technical and legal concepts of privacy. *IEEE Access, Vol. 6*, 26543-26557. IEEE.

Štitilis, D. & Laurinaitis, M. (2017). Treatment of biometrically processed personal data: Problem of uniform practice under EU personal data protection law. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 33*(5), 618-628.

Stultjens, M. (2018, 17. huhtikuuta). State of GDPR readiness in Europe (Feb 2018). Haettu 25.11.2018 osoitteesta https://medium.com/ @maartenstultjens /state-of-gdpr-readiness-in-europe-feb-2018-651aacc7041b

Tallon, P. P., Ramirez, R. V. & Short, J. E. (2013). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems, 30*(3), 141-178.

Talus, A., Autio, E., Hänninen, A., Pihamaa, H. & Kantonen, S. (2017). *Miten valmistautua EU:N tietosuoja-asetukseen?* Helsinki: Oikeusministeriö ja tietosuojavaltuutetun toimisto.

Templier, M. & Paré, G. (2015). A Framework for Guiding and Evaluating Literature Reviews. *Communications of the Association for Information Systems. 37(6),* 112-137.

TIEKE, tietoyhteiskunnan kehittämiskeskus ry. (2022, 31. tammikuuta). Tietosuojatyökalun ensimmäinen versio on julkaistu. Haettu 2.4.2022 osoitteesta https://tieke.fi/hankkeet/gdpr2dsm/tietosuoja-on-pk-yrityksen-kilpailuetu-uusi-tyokalu-auttaa-yrittajaa-arvioimaan-tietosuojakaytantojaan/

Tietosuojatyöryhmä. (2017). *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää "liittyykö käsittelyyn todennäköisesti" asetuksessa (EU) 2016/679 tarkoitettu "korkea riski"*. Haettu osoitteesta https://tietosuoja.fi/documents /6927448/8316711/Vaikutustenarviointi+fi.pdf/af51e999-5326-4223-9deb-e21bdd2e0a63/Vaikutustenarviointi+fi.pdf?t=1527059635000

Tietosuojatyöryhmä. (2018). *Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta.* Haettu osoitteesta https://tietosuoja.fi/documents/6927448/8316711/Tietoturvaloukkauksen+ilmoittaminen+fi/9c0f2f46-33b1-4b01-9a50-9320d59bd605/Tietoturvaloukkauksen+ilmoittaminen+fi.pdf

Tietosuojavaltuutetun toimisto. (2015, 28. heinäkuuta). Kansainväliset normit ja ohjeet - tietosuojavaltuutettu. Haettu osoitteesta http://www.tietosuoja.fi/fi/index/lait/kansainvalisetnormitjaohjeet.html

Tietosuojavaltuutetun toimisto. (2018, 24. toukokuuta). Uuden tietosuojalainsäädännön soveltaminen alkaa huomenna. Haettu osoitteesta https://tietosuoja.fi/artikkeli/-/asset_publisher/uuden-tietosuojalainsaadannon-soveltaminen-alkaa-huomenna

Tietosuojavaltuutetun toimisto. (2020, 15. toukokuuta). Apulaistietosuojavaltuutettu määräsi yrityksen muuttamaan tapaa, jolla se pyytää suostumusta evästeiden käyttöön. Haettu osoitteesta https://tietosuoja.fi/-/apulaistietosuojavaltuutettu-maarasi-yrityksen-muuttamaan-tapaa-jolla-se-pyytaa-suostumusta-evasteiden-kayttoon

Tikkinen-Piri, C., Rohunen, A. & Markkula, J. (2018). EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34(1),* 134-153.

Traficom, liikenne- ja viestintävirasto. (2021). *Evästeet ja muut käyttäjien päätelaitteille tallennettavat tiedot sekä näiden tietojen käyttö – Opas palveluntarjoajille.* Haettu osoitteesta https://www.traficom.fi/sites/default/files/media/file/Ev%C3%A4steohjeistus_palveluntarjoajille.pdf

Tsormpatzoudi, P., Berendt, B. & Coudert, F. (2016). Privacy by design: From research and policy to practice – the challenge of multi-disciplinarity. Teoksessa Berendt, B., Engel, T., Ikonomou, D., Le Métayer, D. & Schiffner, S. (toim.), *Privacy technologies and policy (199-212).* Cham: Springer.

Valtiovarainministeriö. (2016, 4.-5. lokakuuta). Excel-tukityökalu. Haettu osoitteesta 15.4.2018 https://vm.fi/vahti-tilaisuuksien-aineistoja

Wachter, S. (2018). Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34(3),* 436-449.

Weintraub, A., Owens, L. & Jedinak, E. (2013). *The enterprise information management barbell strengthens your information value.* Forrester Research, Inc.

Wilkinson, G. (2018). General data protection regulation: No silver bullet for small and medium-sized enterprises. *Journal of Payments Strategy & Systems, 12 (2),* 139-149.

LIITE 1 REKISTERI- JA TIETOSUOJASELOSTE

REKISTERI- JA TIETOSUOJASELOSTE

Henkilötietolaki (523/99) 10 § ja 24 §

Laatimispäivä: 27.4.2018

1. **Rekisterinpitäjä**
   Järvi-Suomen Kiinteistökonsultit Oy
   Saimaankatu 8
   50100 MIKKELI
   Y- tunnus: 0931939-2
   Puhelinnumero: +358400250533
   sähköpostiosoite:jorma(at)tarmok.fi

2. **Rekisteriasioista vastaava henkilö**

   Yhteyshenkilö: Jorma Lifländer
   Puhelin: +358400250533
   Sähköposti: jorma(at)tarmok.fi

3. **Rekisterin nimi**
   Tarmo asiakasrekisteri

4. **Henkilötietojen käsittelyn tarkoitus, rekisterin käyttötarkoitus**
   Tarmo asiakasrekisteriä käytetään Rekisterinpitäjän henkilökunnan ja rekisteröidyn väliseen tiedonvaihtoon, joka liittyy Rekisterinpitäjän palveluiden ylläpitoon, tiedottamiseen ja markkinointiin.

5. **Rekisterin tietosisältö**
   Rekisterissä käsitellään asiakassuhteen hoidon ja markkinoinnin kannalta tarpeellisia tietoja. Tällaisia tietoja voivat olla muun muassa henkilön nimi- ja yhteystiedot, yhteydenottotavat sekä muut mahdolliset työtehtävien hoidon kannalta tarvittavat tiedot.

6. **Rekisterin tietolähteet**
   Rekisteriin talletettavat tiedot voivat tulla Rekisterinpitäjälle sähköisesti erikseen suojattujen lomakkeiden, sähköpostin, puhelinkontaktin, henkilökohtaisen tapaamisen tai muun dokumentin kautta.

   Rekisteriin lisättävät tiedot voi antaa joko rekisteröity tai ennalta sovittu kumppani, jolle rekisteröity on luovuttanut tiedot.

7. Tietojen luovutukset ja tietojen siirto EU:n tai Euroopan talousalueen ulkopuolelle

Rekisterinpitäjä voi luovuttaa tietoja voimassaolevan lainsäädännön sallimissa rajoissa sen yhteistyökumppaneille ja mahdollisille alihankkijoille turvatakseen Rekisterinpitäjän palvelujen häiriöttömän käytön.

8. Rekisterin suojauksen periaatteet

Rekisterinpitäjän tiedot on tallennettu joko Rekisterinpitäjän omaan palveluun tai EU:n alueelta hankittuun asiakasrekisteri- palveluun. Molemmissa tapauksessa rekisteriin tallennettavat henkilötiedot kerätään tietokantaan, joka on palomuurein sekä muilla tarkoituksenmukaisilla teknisillä keinoilla suojattu. Rekisterin palvelinlaitteet säilytetään korkean tietoturvan palvelinsaleissa, johon on pääsy vain ennalta määritellyillä henkilöillä ja ne täyttävät GDPR:n (EU:n Tietosuoja-asetus EU 2016/679) vaatimukset tietojen käsittelylle.

Rekisteriä käytetään Rekisterinpitäjän myöntämillä henkilökohtaisilla käyttöoikeuksilla. Käyttöoikeus päättyy henkilön siirtyessä pois niistä tehtävistä, joiden hoitamista varten käyttöoikeus on hänelle myönnetty. Järjestelmän ylläpitoon ja huoltoon osallistuvilta ulkopuolisilta palveluntuottajilta rekisterinpitäjä edellyttää asianmukaista ja riittävää tietosuojausta sekä sitoumusta olla käyttämättä ja hyödyntämättä mahdollisesti haltuunsa saamia rekisteritietoja.

9. Rekisteröidyn kielto-oikeus

Rekisteröidyllä on oikeus kieltää rekisterinpitäjää käsittelemästä itseään koskevia tietoja. Kielto tulee tehdä kirjallisesti ja osoittaa rekisteriasioista vastaavalle henkilöille.

10. Rekisteröidyn tarkastus-oikeus

Rekisteröidyllä on oikeus tarkastaa rekisteriin tallennetut itseään koskevat tiedot ja saada niistä kopiot. Tarkastuspyyntö tulee tehdä kirjallisesti ja osoittaa rekisteriasioista vastaavalle henkilölle.

11. Rekisteröidyn tietojen poistaminen

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää poistamaan esimerkiksi häntä koskevat vanhentuneet henkilötiedot. Rekisteröidyllä on esimerkiksi oikeus peruuttaa suostumuksensa, johon käsittely on perustunut. Jos rekisteröity peruuttaa suostumuksen, hän voi esittää rekisterinpitäjälle pyynnön poistaa rekisteröityä koskevat tiedot järjestelmistään, minkä jälkeen rekisterinpitäjän on poistettava henkilötiedot, ellei käsittelylle ole muuta laillista perustetta. Poistopyyntö tulee tehdä kirjallisesti ja osoittaa rekisteriasioista vastaavalle henkilölle.

Poisto toteutetaan siten, että rekisteröidyn tiedot merkitään siten, ettei niitä enää käsitellä tuotantojärjestelmissä.

12. Tiedon korjaaminen

Rekisterinpitäjä oikaisee, poistaa tai täydentää rekisterissä olevan, käsittelyn tarkoituksen kannalta virheellisen, tarpeettoman, puutteellisen tai vanhentuneen henkilötiedon joko oma-aloitteisesti tai rekisteröidyn pyynnöstä. Rekisteröidyn tulee ottaa yhteyttä rekisterinpitäjän rekisteriasioista vastaavaan henkilöön tiedon korjaamiseksi.

LIITE 2 TOIMEKSIANTAJAN PRO GRADU KOMMENTIT

Ira Närhinen Pro Gradu:

MITEN EU:N YLEISEN TIETOSUOJA-ASETUKSEN KÄYTTÖÖNOTTOA VOIDAAN TUKEA PIENYRITYKSISSÄ?

Kommentointi Järvi-Suomen Kiinteistökonsultit Oy:n GDPR- prosessista

Yrityksemme Järvi-Suomen Kiinteistökonsultit Oy antoi Ira Närhiselle toimeksiannon, jotta hän avustaisi meitä tietosuoja-asetuksen laadinnassa. Olen tänään lukenut, mielestäni erinomaisen, Iran tekemän Pro Gradu- tutkielman kyseisestä aiheesta, jossa meitä on käytetty esimerkki yrityksenä. Seuraavassa muutamia kommentteja käytännön toteutuksesta ja saavutetuista hyödyistä.

1. **Käytetty tutkimusmenetelmä**

Kun vuonna 2018 käyttöön otettava GDPR- asetus julkaistiin, ei meillä ollut mitään käsitystä, mitä meidän olisi pitänyt tehdä. Uskon, että sama tilanne oli monilla pienyrityksillä.

Kuten tutkielmassa on hyvin kuvattu, läksimme kartoittamaan perusasioita. Ensimmäinen oivallus minulle tuli siitä, kun sain selville, mitä asetuksessa tarkoitettiin rekisterin pitäjällä ja käsittelijällä. Nopea johtopäätökseni tästä oli, että mehän olemme rekisterin pitäjä vain omien asiakkaidemme suhteen ja tämä on meille helppo juttu. Onneksi Iran käyttämä menetelmä paneutui asioihimme tarkemmin ja aloin ymmärtämään paremmin omaa toimintaympäristöämme.

Ohjelmistotoimittajana meillä on monia sidosryhmiä, joita on myös tutkielmassa kuvattu. Esimerkiksi alihankkijoidemme suhteen olemme keränneet heidän omat tietosuojaselosteensa ja vaatineet niihin joitain tarkennuksia, joita oma toimintatapamme vaatii. Tämä oli toinen iso oivallus, jonka Iran työ toi meille.

Kolmas ymmärrys tuli asiakkaittemme osalta. He toimivat rekisterinpitäjinä esim. taloyhtiöiden asukkaiden osalta. Meidän on pitänyt tarkentaa oman ohjelmistomme käyttöoikeusprosesseja siten, että nämä toiminnan kannalta keskeisten henkilötietojen käyttöoikeudet voidaan määrittää siten, että vain tietyt työssään ko. tietoja tarvitsevat henkilöt näkevät ne. Olemme tämän asian suhteen joutuneet konsultoimaan meidän asiakkaitamme moneen otteeseen.

Monessa kiinteistöhuoltoyrityksessä asukastietoja käytetään vain oven avaus- tapauksissa, jossa pitää saada selville, voidaanko henkilölle avata ovi kyseiseen huoneistoon. Vuoden 2018 jälkeen meidän asiakaskunnassa on useita yrityksiä, jotka ovat luopuneet tästä ylimääräisestä työstä, koska meillä on nykyään suora liitäntä Digi- ja väestötietorekisterin järjestelmään.

Oven avaus tapauksessa sisään pyrkivältä henkilöltä katsotaan henkilöpaperit, hänen henkilötunnuksensa kirjoitetaan sovellukseemme ja lähetetään VRK:lle. Paluu viestinä tulee henkilön nimi ja osoitetiedot. Tämä on lisännyt taloyhtiöiden asukasturvallisuutta ja meidän asiakkaittemme varmuutta siitä, että vain oikeat henkilöt päästetään asuntoihin. Samoin ylimääräisen rekisterin pito on jäänyt pois niin työnä kuin vastuunakin.

2. Tutkimuksesta saavutetut hyödyt Järvi-Suomen Kiinteistökonsultit Oy:lle

Iran tekemän tutkimuksen perusteella pystyimme ymmärtämään oman roolimme GDPR-kartalla ja saimme perusteet omien päätösten ja laadittavien dokumenttien pohjaksi. Arvostan Iran toimintatavassa sitä periaatetta, että hän ei pyrkinyt laatimaan meille valmiita dokumentteja, vaan meidän piti itse tehdä ne annettujen raamien puitteissa. Vastuuhan näissä asioissa on aina yrittäjällä itsellään.

Suurin hyöty toiminnassamme tämän asian suhteen on ollut juuri tuo ymmärrys, mitä asioita on pitänyt tehdä. Toimintaympäristömme on aivan viime päivinä muuttunut olennaisesti, sillä koko tuotekehityksen johtovastuu on siirtynyt Controla Oy:ltä meille itsellemme. Koska olen Controlan osaomistaja, sovelsimme Iran menetelmää myös ko. yrityksen GDPR- prosessien tekoon. Meillä oli yhteneväiset prosessit ja nyt kun tietyt toiminnot siirtyivät meille, voimme soveltaa näitä opittuja prosessejamme suoraan.

Teemme Tarmo-ohjelmistostamme uutta versiota, joka valmistuu lähiaikoina. Myös tätä tehtäessä olemme voineet hyödyntää Iran laatimaa prosessia niin alihankkijoiden kuin itse ohjelmiston käyttöoikeusprosessien osalta.

Summa summarum, kiitos Ira!

Mikkeli 21.4.2022

Järvi-Suomen Kiinteistökonsultit Oy

Jorma Lifländer
Yrittäjä