Tommi Lipsanen

GDPR:N ARTIKLAN 32 VAATIMUKSET : KÄSITEANALYYSI ASIANMUKAISISTA TEKNISISTÄ JA ORGANISATORISISTA TOIMENPITEISTÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Lipsanen, Tommi
GDPR:n artiklan 32 vaatimukset : käsiteanalyysi asianmukaisista teknisistä ja organisatorisista toimenpiteistä.
Jyväskylä: Jyväskylän yliopisto, 2021, 55 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Siponen, Mikko

Tietotekniikan hyödyntäminen organisaatioiden toiminnassa on kasvanut viime vuosikymmenten aikana. Kasvu ei ole kuitenkaan tapahtunut ilman haasteita. On jo olemassa varoittavia esimerkkejä isoista tietovuodoista, jolloin arkaluontoista tietoa on päätynyt vääriin käsiin. Tietovuodon seurauksena voi syntyä aineellista tai aineetonta vahinkoa organisaatioille sekä yksityisille henkilöille. EU:ssa henkilötietojen turvallisuuden eli tietosuojan haasteisiin on pyritty vastaamaan kokonaisvaltaisesti lainsäädännöllä. Yleinen tietosuoja-asetus eli General Data Protection Regulation (GDPR) astui voimaan vuonna 2016, ja sitä alettiin soveltamaan vuonna 2018. GDPR:n tavoitteena on muun muassa vastata EU:n tasolla teknologian kehityksen ja globalisaation tuomiin haasteisiin, vahvistaa säännöt henkilötietojen käsittelyssä sekä suojella luonnollisten henkilöiden perusoikeuksia ja –vapauksia, erityisesti oikeutta henkilötietojen suojaan. GDPR koostuu 99 artiklasta ja siinä asetetaan paljon säännöksiä liittyen henkilötietojen käsittelyyn. Kyseessä on iso kokonaisuus, ja sen ymmärtämisessä sekä velvoitteiden noudattamisessa voi esiintyä organisaatioille haasteita. GDPR:ssä lisäksi määritellään virallisille valvontaviranomaisille valtuudet hallinnollisten sakkojen antamiselle GDPR:n säännösten rikkomisesta. Tutkimuksen kohteena oli tutkia GDPR:ää, ja tarkemmin sen artiklaa 32. Artikla 32 velvoittaa rekisterinpitäjiä ja henkilötietojen käsittelijöitä ottamaan huomioon monia asioita, kuten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit, ja toteuttamaan asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen käsittelyn turvaamiseksi. Tutkimuksessa analysoitiin artiklan 32 vaatimusten rikkomisen seurauksena annettuja sakkopäätöksiä, jonka avulla pyrittiin ymmärtämään artiklan 32 vaatimuksia ja siinä esiintyvien asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteitä paremmin. Tutkimus toteutettiin käyttäen käsiteanalyysiä tutkimusmenetelmänä. Tutkimuksen tuloksena nousi laaja kirjo konkreettisia toimenpiteitä liittyen artiklan 32 vaatimuksiin asianmukaisista teknisistä ja organisatorisista toimenpiteistä. Näitä toimenpiteitä olivat muun muassa monivaiheinen todentaminen, lokitietojen kerääminen, henkilökunnan säännöllinen tietosuojakoulutus sekä tietoisuus alan yleisessä tiedossa olevista ohjeistuksista liittyen tietoturvallisuusriskeihin ja näiden ohjeistuksien noudattaminen.

Asiasanat: yksityisyys, tietosuoja, tietoturva, GDPR, artikla 32, asianmukaiset tekniset toimenpiteet, asianmukaiset organisatoriset toimenpiteet

ABSTRACT

Lipsanen, Tommi
Obligations under article 32 of GDPR : Conceptual analysis of appropriate technical and organisational measures
Jyväskylä: University of Jyväskylä, 2021, 55 p.
Cyber Security, Master's Thesis
Supervisor(s): Siponen, Mikko

Utilization of information technology within the operations of organizations has increased in the recent decades. However, this has not happened without challenges relating to information technology. There are already warning examples of data breaches where sensitive information has fallen into the wrong hands. Data breach may result in material or non-material damage to organisations and individuals. EU has addressed the challenges relating to security of personal data i.e., data protection by means of comprehensive legislation. General Data Protection Regulation (GDPR) entered into force in 2016 and became applicable in 2018. The objectives of the GDPR includes meeting with the challenges posed by technological development and globalization, to lay down rules for the processing of personal data and to protect fundamental rights and freedoms of natural persons, in particular the right to the protection of personal data. The GDPR consists of 99 articles and lays down many provisions regarding the processing of personal data. The regulation covers a lot of details and there may be challenges for organizations in understanding it and meeting their obligations. The GDPR also defines power for the official supervisory authorities to impose administrative fines for not complying with the GDPR. The purpose of this study was to examine the GDPR, and in particular article 32 of the GDPR. In article 32 there is defined obligations for controllers and processors to consider many issues, such as the risks to the rights and freedoms of individuals, and to implement appropriate technical and organizational measures to ensure the security of processing personal data. The study was conducted using conceptual analysis as a research method. In the study there was analysis done on administrative fines relating to article 32 to gain a better understanding of the requirements of article 32 and the concepts of appropriate technical and organizational measures. Findings of the study revealed multiple concrete measures related to the requirements of article 32 on appropriate technical and organizational measures. These measures included for example multi-factor authentication, collection of log data, regular data protection training for staff, and awareness of publicly available guidelines regarding security risks and adherence to the guidelines.

Keywords: privacy, data protection, information security, GDPR, article 32, appropriate technical measures, appropriate organisational measures

KUVIOT

SISÄLLYS

1 JOHDANTO

Tietojenkäsittely siirtyy jatkuvasti enemmän digitaalisiin ympäristöihin ja yhä useammat organisaatiot harjoittavat liiketoimintaansa täysin digitaalisissa ympäristöissä. Tämä teknologinen kehitys on saanut ihmiset kiinnittämään huomiota näiden digitaalisesti käsiteltävien tietojen turvallisuuteen. On hyvin ajankohtaisia tapauksia, joissa paljon arkaluontoista tietoa on päätynyt vääriin käsiin puutteellisen tietosuojan ja tietoturvan vuoksi. Tietosuojalla tarkoitetaan kaikkien tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvien tietojen - eli henkilötietojen suojaaminen (EDPS, n.d.-a). Tietoturvalla puolestaan tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys (Kyberturvallisuuskeskus, 2020). Voidaan siis nähdä, että tietoturva on yksi tietosuojan toteuttamisen keinoista sekä yksi keskeisimmistä mahdollistajista (Tietosuojavaltuutetun toimisto, n.d.; EDPS, 2021b).

Viime vuosien yksi suurimmista askeleista kohti yhteiskunnallisen ja teknologisen kehityksen mukana pysyvää lainsäädäntöä liittyen tietosuojaan ja tietoturvaan on Euroopan unionin tasolla säädetty yleinen tietosuoja-asetus eli General Data Protection Regulation (GDPR). GDPR astui voimaan vuonna 2016 ja sitä käytiin soveltamaan kahden vuoden siirtymäajan jälkeen vuonna 2018. GDPR on EU:n tasolla säädetty tietosuojalaki, jonka keskeisiä tarkoituksia ovat tietosuojaa koskevan sääntelyn ajantasaistaminen sekä EU:n sisämarkkinoiden digitaalitalouden kehityksen tukeminen (Oikeusministeriö, 2017, s. 9).

GDPR:n keskeisillä tarkoituksilla halutaan vastata teknologian kehitykseen liittyviin haasteisiin koskien henkilötietojen suojaa sekä tukea digitaalitalouden kehitystä sisämarkkinoilla yhdenmukaistamalla jäsenvaltioiden tietosuojasäännöksiä (Oikeusministeriö, 2017, s. 9). Sen ideana on saada koko EU:n kattava yhtenäinen tietosuojalaki, joka parantaisi tietosuojaa sekä velvoittaa jokaista EU:n jäsenvaltioita noudattamaan sitä. GDPR:ssä lain noudattamista pyritään tukemaan tehokkaalla täytäntöönpanolla ja siinä on säädetty aikaisempaa lainsäädäntöä tiukemmat seuraamukset asetuksen vaatimusten vastaisesta toiminnasta (Oikeusministeriö, 2017, s. 9). Vaatimusten noudattamatta jättämisestä voi esimerkiksi määrätä henkilötietojen käsittelyyn liittyviä korjaavia toimenpiteitä ja

hallinnollisia sakkoja, jotka voivat olla suuruudeltaan maksimissaan jopa 20 miljoonaa euroa, tai jos kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 83. artikla).

GDPR:ää on alettu soveltamaan kahden vuoden siirtymäajan jälkeen toukokuussa 2018, ja kahdessa vuodessa asetuksen rikkomisesta on annettu jo paljon hallinnollisia sakkoja. British Airways sai 22 miljoonan euron suuruisen hallinnollisen sakon vuonna 2020 GDPR:n asettamien henkilötietojen suojaamiseen liittyvien vaatimusten rikkomisesta (ICO, 2020). GDPR:ssä on yhteensä 99 artiklaa, joissa määritellään asetuksen sisältöä ja sen asettamia vaatimuksia henkilötietojen suojaamiselle ja käsittelyyn, joten kyseessä on hyvin laaja kokonaisuus. GDPR:n soveltamisen jälkeen on sen asettamat vaatimukset tuoneet haasteita organisaatioille. Presthus, Sørum & Andersen (2018) tutkivat norjalaisten yritysten GDPR:n vaatimustenmukaisuutta ja tulokset osoittivat, että n. 46 % yrityksistä kertoivat heillä olevan rajallinen ymmärrys itse asetuksesta, ja tämän tuovan haasteita GDPR:n noudattamiseen (Presthus ym., 2018).

Tutkimuksella vastataan tähän haasteeseen liittyen GDPR:n vaatimustenmukaisuuteen. Tutkin tarkemmin GDPR:n artiklaa 32, joka koskee henkilötietojen käsittelyn turvallisuutta. Artiklassa velvoitetaan rekisterinpitäjää ja henkilötietojen käsittelijää toteuttamaan luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvien riskejä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 32. artikla). Artiklassa 32 tarkennetaan, että asianmukaisia organisatorisia ja teknisiä toimenpiteitä ovat toimenpiteet, kuten henkilötietojen pseudonymisointi ja salaus, kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus sekä kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 32. artikla).

Artiklan 32 vaatimukset voi nähdä hyvinkin haastavana monille organisaatioille, sillä se jättää paljon määrittelyä, mikä on riskiä vastaava asianmukainen toimenpide itse rekisterinpitäjälle tai henkilötietojen käsittelijälle. Esimerkiksi pk-yritykset eivät välttämättä ole täysin perehtyneitä riskien käsitykseen ja käsittelyyn henkilötietojen näkökulmasta. Ne voisivat hyötyä enemmän ohjatulta lähestymiseltä, joka pyrkisi pienentämään kuilua lainsäädännön ja pk-yritysten ymmärryksen välillä liittyen henkilötietojen käsittelyyn ja sen riskeihin. (ENISA, 2016, s. 6.)

Tämän tutkimuksen tavoitteena on vastata tähän haasteeseen yhden artiklan osalta, ja ymmärtää paremmin artiklan 32 asettamia vaatimuksia henkilötietojen käsittelyn turvallisuudelle. Tätä taustaa vasten tämän pro gradu -tutkielman tutkimuskysymys voidaan esittää seuraavasti:

- Minkälaisia toimenpiteitä GDPR:n artiklan 32 asianmukaiset tekniset ja organisatoriset toimenpiteet käsitteinä kattavat alleen?

Tutkimus toteutettiin käyttäen käsiteanalyysiä tutkimusmenetelmänä. Käsiteanalyysissä on tarkoitus analysoida käsitteitä ja kartoittaa niiden käyttöä ja

soveltamista (Wilson, 1963, s. 10). Käsiteanalyysin avulla tutkija voi ymmärtää paremmin käsitteen kuvaamaa ilmiötä (Puusa, 2008, s. 39). Tässä tutkimuksessa käsiteanalyysin avulla on tarkoitus analysoida asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteitä ja kartoittaa niiden käyttöä ja soveltamista. Tämän analyysin tavoitteena on ymmärtää minkälaisia toimenpiteitä asianmukaiset tekniset ja organisatoriset toimenpiteet käsitteinä kattavat alleen. Tähän tutkimusongelmaan pyrin vastaamaan tutkimuksessa analysoimalla tutkimuksen aineistoa eli valvontaviranomaisten sakkopäätöksiä, joita on annettu artiklan 32 rikkomisesta.

Monessa GDPR:n artiklassa, mukaan lukien artiklassa 32 on omaksuttu riskiperusteinen lähestymistapa vaatimusten noudattamiseen. Riskiperusteinen lähestymistapa tarkoittaa, että henkilötietojen käsittelylle asetetut velvoitteet ja vaaditut käsittelyn turvallisuuteen liittyvät asianmukaiset tekniset ja organisatoriset toimenpiteet ovat suhteutettava rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin (Oikeusministeriö, 2017, s. 16). Oikeusministeriön (2007) julkaisussa nostetaan esille, että rekisterinpitäjien on pääsääntöisesti itse määritettävä asianmukaiset suojatoimet ottaen huomioon monia seikkoja, kuten käytettävissä oleva tekniikka, toteuttamiskustannukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit (Oikeusministeriö, 2007, s. 13).

Tämän pohjalta muodostin tutkimuksen analyysin avuksi kahden eri tietoturvaan ja tietosuojaan liittyvän mallin pohjalta asianmukaisten organisatoristen ja teknisten suojatoimenpiteiden viitekehyksen, joka kattaa kokonaisvaltaisen henkilötietojen käsittelyn riskienhallinnan. Viitekehykseen kuuluu neljä päätoimintoa: tunnistaminen, suojaaminen, havaitseminen sekä vastaaminen ja palautuminen. Nämä päätoiminnot sisältävät myös alakategorioita. Esimerkiksi suojaamisen päätoiminnon yksi alakategoria on identiteetin- ja pääsynhallinta. Tämä viitekehys toimi aineiston analyysin tukena ja sen avulla analysoin aineistoa.

Aineistolle tehdyn analyysin avulla nousi suuri määrä havaintoja liittyen asianmukaisiin teknisiin ja organisatorisiin toimenpiteisiin. Tutkimuksen tuloksena nousi monia teknisiä ja organisatorisia toimenpiteitä, jotka ovat artiklan 32 vaatimustenmukaisia. Asianmukaisia teknisistä toimenpiteitä löytyi eniten havaintoja suojaamisen ja havaitsemisen päätoimintoon. Tutkimuksen tuloksina nousi esille, että artiklan 32 asianmukaisten teknisten toimenpiteiden käsitteeseen ja vaatimuksiin kuuluu teknisiä toimenpiteitä, kuten monivaiheinen todentaminen ja lokitietojen tuottaminen. Tuloksena liittyen asianmukaisten organisatoristen toimenpiteiden käsitteeseen tuloksena nousi suurin määrä toimenpiteitä liittyen tunnistamisen ja suojaamisen päätoimintoihin. Tutkimuksen tuloksina nousi esille, että tärkeitä asianmukaisten organisatoristen toimenpiteiden käsitteeseen kuuluvia toimenpiteitä artiklan 32 vaatimuksiin liittyen ovat muun muassa henkilöstön koulutus, henkilöstön tietoisuuden ja politiikkojen noudattamisen säännöllinen testaaminen sekä toimenpide, jolla varmistetaan henkilöstön tietosuojakoulutusten suorittaminen. Kokonaisuudessaan tulokset ovat nähtävissä luvussa 6.

Tutkimukseen liittyvää olennaista aikaisempaa tutkimusta sekä kirjallisuutta hain käyttäen pääasiassa JYKDOKia ja Google Scholar -hakukonetta.

Keskeisiä hakusanoja, joita käytin tutkimukseen liittyvän olennaisen kirjallisuuden hakemiseen olivat: “GDPR”, “yleinen tietosuoja-asetus", “tietosuoja”, “privacy”, “data protection”, “GDPR article 32”.

Tutkimuksen rakenne etenee seuraavanlaisesti: Luvussa 2 määritellään tutkimuksen kannalta keskeisiä käsitteitä. Luvussa 3 käydään tarkemmin läpi GDPR:ää, sen keskeisiä tavoitteita, käsitteitä ja velvoitteita. Tämän jälkeen luvussa 4 tarkennutaan tutkimuksen kohteena olevaan henkilötietojen käsittelyn turvallisuutta käsittelevään artiklaan 32. Luvussa 5 esitellään tutkimusmenetelmät ja aineisto, jonka jälkeen luvussa 6 siirrytään analyysiin. Viimeisenä luvussa 7 käydään tutkimuksen yhteenveto ja esitellään jatkotutkimusaiheita.

2 YKSITYISYYS, TIETOSUOJA JA TIETOTURVA

GDPR:ää tutkiessa on tärkeää määritellä keskeisiä käsitteitä liittyen asetukseen. Keskeisinä käsitteinä tutkimuksen kannalta ovat yksityisyys, tietosuoja ja tietoturva. Määrittelen tutkielmassa nämä käsitteet sekä käsittelen niiden merkityksiä ja suhteita toisiinsa sekä myös hieman historiaa ja kehityssuuntia. Uskon tämän olevan tutkielman aiheen kannalta tärkeää, koska se auttaa ymmärtämään ja tulkitsemaan GDPR:n keskeisiä tarkoitusperiä.

2.1 Yksityisyys

Käsiteltäessä GDPR:ää sekä tietosuojaa on tärkeää tarkastella yksityisyyden käsitettä, sillä yksityisyys ja tietosuoja ovat käsitteinä yhteydessä toisiinsa, mutta siitä huolimatta ne tunnustetaan yleisesti kaikkialla maailmassa kahtena erillisenä oikeutena (EDPS, n.d.-a). Tätä yksityisyyden ja tietosuojan käsitteiden eroa tarkastellaan myöhemmin tutkielmassa alaluvussa 2.2.

Yksityisyys on käsitteenä hyvin hankala määritellä ja se voidaan nähdä hyvin laajana käsitteenä. Solove (2002) esittää julkaisussaan, että vaikeudet määritellä mitä yksityisyydellä tarkoitetaan, ja miksi se on tärkeää, on usein tehnyt lainsäädännön liittyen yksityisyyteen tehottomaksi ja jättänyt huomiotta laajemmat tarkoitukset, joita sen tulisi palvella (Solove, 2002, s. 1090). Yksityisyyden käsitteen määritelmän vaikeudesta toteaa myös Agre (1997) ja Davies (1997) kuvaillen, että pyrkimisestä yhteen yksityisyyden määritelmään on tullut vakituinen haaste yksityisyyden alalla (Agre, 1997, s. 6; Davies, 1997, s. 153). Gellman (1997) huomauttaa, että lakimiehet, tuomarit, filosofit ja tutkijat ovat yrittäneet määritellä yksityisyyden käsitteen ja sen laajuuden siinä epäonnistumatta, mutta lopputulokset ovat olleet erilaisia (Gellman, 1997, s.193). Yksityisyyden käsitteen laajuudesta Solove (2008) huomauttaa sen käsittävän nykyisenään asioita, kuten ajatuksenvapaus, yksinäisyys omassa kodissa, omien henkilötietojen hallinta sekä vapaus valvonnasta (Solove, 2008, s. 1).

Yksi hyvin merkittävä julkaisu, jossa käsitellään yksityisyyden käsitettä, merkitystä ja oikeutta yksityisyyteen on Warrenin ja Brandeisin (1890) kirjoittama julkaisu "The Right to Privacy" (Warren & Brandeis, 1890). Warren ja Brandeis (1890) sanovat julkaisussaan, että yksilön henkilökohtainen ja omaisuuden suoja ovat yhtä vanhoja periaatteita kuin tavanomainen oikeus, mutta aika ajoin on esiintynyt tarve määritellä tällaisen suojan tarkka luonne ja laajuus uudelleen. He jatkavat, että poliittiset, sosiaaliset ja taloudelliset muutokset edellyttävät uusien oikeuksien tunnustamista, ja tavanomainen oikeus kasvaa vastaamaan yhteiskunnan vaatimuksia. (Warren & Brandeis, 1890 s. 193.) Solove (2002) nostaa myös esille, kuinka yksityiselämän ja yksityisenä pidettyjen asioiden käsitys on muuttunut paljon historian saatossa, johon on vaikuttanut muun muassa pienenevät perhekoot, uusien sosiaalisten paikkojen syntyminen, kasvava varallisuus

ja tila sekä työn ja kodin erottautuminen (Solove, 2002, s. 1141). Tämän voidaan nähdä pätevän hyvin myös nykyiseen tilanteeseen. Teknologian kehityksen myötä on seurannut väistämättä muutosta yhteiskunnan poliittiseen, sosiaaliseen ja taloudelliseen toimintaan, ja sitä kautta myös lakeja on täytynyt muuttaa vastaamaan yhteiskunnan vaatimuksia myös yksityisyyden suojan osalta.

Warren & Brandeis (1890) tuovat lisäksi julkaisussaan hyvin esille, kuinka hyvin varhaisina aikoina laki antoi oikeussuojakeinoja vain ihmisen ja hänen omaisuutensa fyysiseen häiritsemiseen (Warren & Brandeis, 1890, s. 193). He jatkavat, että myöhemmin kuitenkin tunnustettiin myös ihmisen henkinen luonne ja näiden oikeuksien soveltamisala laajeni vähitellen. Nyt oikeus on tullut tarkoittamaan oikeutta nauttia elämästä - ”oikeutta olla rauhassa” (engl. “right to be let alone”) ja henkilön omaisuus on kasvanut kattamaan sekä aineettoman (kuten maineensa), että aineellisen hallinnan. (Warren & Brandeis, 1890, s. 193.) He viittaavat oikeudella olla rauhassa tuomari Cooleyn sanoihin (Warren & Brandeis, 1890, s.195).

Warreinin ja Brandeisin julkaisua ja yksityisyyden määritelmää voidaan pitää yksityisyyden oikeuden kannalta merkittävänä, mutta Solove (2002) huomauttaa, että oikeus olla rauhassa kuvaa vain yhtä yksityisyyden ominaisuutta, eikä se määrittele juurikaan, miten yksityisyyttä tulisi arvostaa suhteessa esimerkiksi sananvapauteen tai muihin tärkeisiin arvoihin (Solove, 2002, s. 1101). Hän jatkaa, että julkaisu sisälsi oivalluksia vankempaan yksityisyyden teoriaan. Sen tarkoituksena oli tutkia yksityisyyden oikeuden juuria ja selvittää, kuinka kyseistä oikeutta voitaisiin kehittää, ja he tekivät sen perusteellisesti (Solove, 2002, s.1002).

Solove (2002) tiivistää laajan kirjon yksityisyyden määritelmistä tieteellisessä ja oikeudellisessa kirjallisuudessa kuuden eri otsikon alle. Nämä otsikot ovat (1) oikeus olla rauhassa, (2) rajoitettu pääsy itselle, (3) salassapito, (4) henkilötietojen hallinta, (5) yksilöllisyys, (6) intiimiys (Solove, 2002, s.1094). Nämä ovat päällekkäisiä käsitteitä, mutta jokaisella on tunnusomainen näkökulma yksityisyyteen (Solove, 2002, s.1094). Solove (2002) toteaa, että yksi tärkeimmistä syistä yksityisyyden suojaamiselle on estää tukahduttavan vallankäytön harjoittaminen tarkoituksena tuhota tai vahingoittaa yksilöitä (Solove, 2002, s. 1151). Tässä tutkimuksessa yksityisyyden ajatellaan koskevan Soloven laajaa määritelmää käsitteistä, jotka kuuluvat yksityisyyden piiriin, eikä lähdetä tätä tarkemmin määrittelemään mitä yksityisyys on.

2.1.1 Yksityisyys lainsäädännössä

Yksityisyyttä on alettu huomioimaan ja suojaamaan historian saatossa lainsäädännöllisesti ympäri maailman, ja sen merkitys on huomattavissa perustuslaeissa ja lainsäädännössä. Yksityisyys on merkittävässä roolissa ympäri maailmaa ja lähes kaikissa valtioissa on säädöksiä ja perustuslaillisia oikeuksia tarkoituksena suojata yksityisyyttä (Solove, 2008, s. 2). Yksityisyys on tunnustettu ihmisen perusoikeudeksi (Solove, 2008, s. 3)

Suomessa yksityisyyttä ja yksityiselämän suojaa on määritelty perustuslaissa. Suomen perustuslaissa määritellään, että "Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu." (PL 2:10.1 §) sekä "Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton."(PL 2:10.2 §). Lisäksi YK:n ihmisoikeuksien yleismaailmallisessa julistuksessa on yksityisyys mainittuna yhtenä perustavanlaatuisena ihmisoikeutena. YK:n Ihmisoikeuksien yleismaailmallisessa julistuksessa oikeutta yksityisyyteen määritellään seuraavanlaisesti: "Älköön mielivaltaisesta puututtako kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon älköönkä loukattako kenenkään kunniaa ja mainetta. Jokaisella on oikeus lain suojaan sellaista puuttumista tai loukkausta vastaan." (Ihmisoikeuksien yleismaailmallinen julistus, 1948, 12. artikla).

Euroopan ihmisoikeussopimuksessa määritellään, että "Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta" (Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi, 1950, 8. artikla). EU:ssa ihmisen kunnia tunnustetaan ehdottomaksi perusoikeudeksi (EDPS, n.d.-a). Tämän myötä yksityisyydellä ja oikeuksilla, kuten oikeudella yksityiselämään, oikeudella hallita itseään koskevia tietoja, oikeudella olla rauhassa on keskeinen rooli (EDPS 2021a). Euroopan tietosuojavaltuutetun toimisto (2021) tarkentaa, että yksityisyys ei ole ainoastaan yksilön oikeus vaan myös sosiaalinen arvo (EDPS, n.d.-a). Voidaan siis hyvin todeta, että ihmisen yksityisyyttä ja sen suojaamista pidetään hyvin merkittävänä ihmisoikeutena ympäri maailman.

On myös tärkeää ottaa huomioon, että muissa valtioissa, kuten esimerkiksi USA:ssa yksityisyyttä on historiallisesti pidetty vapauden tunnusmerkkinä ja oikeutena olla vapaa valtion tunkeutumiselta. Tämän voidaan nähdä myös olevan osana yksityisyyttä EU:ssa. (EDPS, n.d.-a.) Solove (2008) mainitsee, että historian saatossa huoli yksityisyydestä on pysynyt pinnalla teknologian kehittymisen myötä, mutta erityisesti tietotekniikan ja tietokoneiden nopea leviäminen nosti yksityisyyden merkittäväksi kysymykseksi ympäri maailmaa (Solove, 2008, s. 4).

Voidaankin huomata, että huiman teknologisen kehityksen ja sen tuomien haasteiden myötä yksityisyyden suojaan ja tietosuojaan liittyvää lainsäädäntöä on alettu uusia viimevuosina ympäri maailman. Haasteisiin pyritään keksimään ratkaisuita ja yhtenä hyvänä esimerkkinä on tässä tutkimuksessa tutkittava GDPR. Nyt kun yksityisyyteen liittyvää määrittelyä ja historiaa on käyty läpi, tarkastellaan seuraavaksi tietosuojaa.

2.2 Tietosuoja

Tutkielman kannalta keskeisimpänä käsitteenä on tietosuoja. Tietosuojalla tarkoitetaan kaikkien tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvien tietojen suojaamista (EDPS, n.d.-a). Luonnolliseen henkilöön liittyviä tietoja eli henkilötietoja ovat esimerkiksi henkilön nimet, syntymäaika, valokuvat ja puhelinnumero (EDPS, n.d.-a). Suomen tietosuojavaltuutetun toimisto määrittelee tietosuojan seuraavanlaisesti: "Tietosuoja on perusoikeus, joka

turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä" (Tietosuojavaltuutetun toimisto, n.d.).

Tietosuojan tavoitteena on varmistaa luonnolliseen henkilöön liittyvien tietojen oikeudenmukainen käsittely sekä julkisella, että yksityisellä sektorilla (EDPS, n.d.-a). Tärkeänä huomiona on se, että oikeus yksityisyyteen ja oikeus tietosuojaan ovat molemmat kirjattu EU:n perussopimuksiin ja EU:n perusoikeuskirjaan (EDPS, n.d.-a). Tietosuojan avulla voidaan tukea ja toteuttaa ihmisten perusoikeuksia, kuten aikaisemmin mainittiin. Toisaalta, kuten jo yksityisyyden osalta huomattiin, on teknologian kehitys tuonut paljon uusia haasteita myös tietosuojan toteuttamiseen. Tämän seurauksena onkin alettu uudistamaan lainsäädäntöä tietosuojan osalta koko EU:n tasolla sekä ympäri maailman. Tietosuojalakien määrittäminen on maailmanlaajuisesti kasvussa, tästä todisteena se, että yli 100:ssa valtiossa on määritelty tietosuojalaki (EDPS, n.d.-a).

2.2.1 Yhtäläisyydet ja erot yksityisyyteen

Tietosuojan ja yksityisyyden yhtäläisyydet ja erot eivät ole kovin yksiselitteisiä. Tietosuojan käsite itsessään on peräisin oikeudesta yksityisyyteen, ja molemmat – tietosuoja ja yksityisyys ovat tärkeitä perusoikeuksien ja –arvojen säilyttämisessä ja edistämisessä (EDPS, n.d.-a). Molemmat käsitteet ovat myös tärkeitä muiden oikeuksien ja vapauksien harjoittamisen kannalta, kuten sananvapauden ja kokoontumisvapauden kannalta (EDPS, n.d.-a).

Lynskey (2016) huomauttaa kirjassaan, että vaikka Euroopan ihmisoikeusjulistuksen ja tietosuojalainsäädännön antama suoja ovat merkittävästi päällekkäisiä, on yksityisyyden ja tietosuojan oikeudelliset järjestelmät kuitenkin erilaisia (Lynskey, 2016, s. 11). Yksi keskeisistä eroista on se, että oikeus yksityisyyteen käsittää myös fyysisen yksityisyyden häirinnän, kuten tunkeilevan ruumiintarkastuksen, joita tietosuojalainsäädäntö ei käsitä (Lynskey, 2016, s. 11). Lisäksi tietosuojan erottaa tiedon yksityisyydestä se, että tietosuoja käsittää alleen laajemman kirjon henkilötietojen käsittelyn aktiviteetteja, ja antaa yksilöille enemmän oikeuksia laajempaan kirjoon tietoja. Eli tietosuoja antaa yksilöille enemmän kontrollia suuremmalle määrälle henkilötietoja kuin yksityisyys. (Lynskey, 2016, s. 11.) Yhtenä erona on lisäksi se, että yksityisyys on tunnustettu yleiseksi ihmisoikeudeksi ja tietosuojaa ei ole, joka voi tietysti muuttua (EDPS, n.d.-a).

Lynskey (2016) huomauttaa kirjassaan, että perustuen olemassa olevaan kirjallisuuteen, yhteys oikeudella tietosuojaan ja yksityisyyteen voidaan tulkita laajalti kolmella mallilla. Ensimmäinen malli kuuluu siten, että tietosuoja ja yksityisyys ovat toisiaan täydentäviä työkaluja, joiden päätarkoitus on suojella ihmisen kunniaa (Lynskey, 2016, s. 94). Toinen malli esittää, että tietosuoja on osa yksityisyyttä eli tietosuoja palvelee ainoastaan tavoitteita, jotka ovat peräisin oikeudesta yksityisyyteen ja kaikki tietosuojalainsäädännön osat perustellaan yksityisyyden huolilla (Lynskey, 2016, s. 101, 102). Kolmas malli esittää, että oikeus tietosuojaan palvelee monia tarkoituksia, mukaan lukien yksityisyyteen liittyviä tarkoituksia (Lynskey, 2016, s. 103). Kolmannen mallin mukaan tietosuoja ja

yksityisyys ovat hyvinkin päällekkäisiä, mutta kuitenkin erillisiä oikeuksia, ja tietosuojasäännösten yksi monista tarkoituksista on suojata oikeutta yksityisyyteen (Lynskey, 2016, s. 105). Tässä tutkielmassa tietosuojan ja yksityisyyden suhdetta ajatellaan noudattavan kolmannen mallin määritelmää.

GDPR:ää käsiteltäessä on tärkeää huomioida se, että EU:ssa yksityisyys ja tietosuoja eivät ole absoluuttisia oikeuksia. GDPR:ssä määritellään, että "Oikeus henkilötietojen suojaan ei ole absoluuttinen; sitä on tarkasteltava suhteessa sen tehtävään yhteiskunnassa ja sen on suhteellisuusperiaatteen mukaisesti oltava oikeassa suhteessa muihin perusoikeuksiin" (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, johdanto-osa 4).

Oikeutta yksityisyyteen ja tietosuojaan voidaan siis joutua tasapainottelemaan muihin EU arvoihin, ihmisoikeuksiin tai julkisiin ja yksityisiin intresseihin, kuten vaikkapa ilmaisunvapauteen tai lehdistönvapauteen liittyen. Tärkeänä huomiona on myös, että oikeutta yksityisyyteen ja tietosuojaan voidaan joutua myös punnitsemaan kansallista turvallisuutta vasten. Henkilötietojen keräämisen, säilyttämisen ja rajat ylittävän vaihdon laajuus jäsenvaltioiden välillä rikos- ja terrorismiasioissa on valtava. (EDPS, n.d.-a.)

Eurooppalaisten tietokantojen sekä lainvalvontatarkoituksia varten saatavan kaupallisen tiedon lisääntynyt käyttö haastaa yksityisyyden ja turvallisuuden välisen tasapainon (EDPS, n.d.-a). Tietosuojaviranomaisilla on yleisesti keskeinen rooli yksityisyyden ja muiden intressien tasapainottelussa (EDPS, n.d.-a).

2.3 Tietoturva

Yksityisyyttä ja tietosuojaa käsiteltäessä on tärkeää myös määritellä tietoturva. Kaikki organisaatiot käyttävät tietoa päivittäisessä työssään (EDPS, n.d.-b). Tietovarannot, kuten esimerkiksi organisaation taloudelliset tiedot, työntekijätiedot tai liikesalaisuudet ovat organisaatioille arvokkaita, ja tästä syystä niiden tulee varmistaa, että nämä tiedot ovat kelvollisesti suojattuja (EDPS, n.d.-b). Näiden tietojen asianmukaiseen suojaamiseen vaaditaan sekä teknisiä, että hallinnollisia toimenpiteitä.

Tietoturvalla tarkoitetaan näitä hallinnollisia ja teknisiä toimenpiteitä, joilla pyritään varmistaa tiedon kelvollinen luottamuksellisuus, eheys ja käytettävyys (Kyberturvallisuuskeskus, 2021). Yleisin tietoturvan hallintaan tähtäävän viitekehyksen kehittämistä ja käyttöönottoa ohjaava malli on niin kutsuttu CIA kolmikko (engl. CIA triad), tarkoittaen tiedon luottamuksellisuutta (engl. confidentiality), eheyttä (engl. integrity) ja saatavuutta (engl. availability) (ENISA, 2016, s. 10). Luottamuksellisuudella tarkoitetaan sitä, että tiedon tulee olla saatavilla vain niiden käyttöön oikeutetuilla henkilöillä (Kyberturvallisuuskeskus, 2021). Eheydellä tarkoitetaan, että tietoja voi muuttaa vain siihen oikeutetut. Käytettävyydellä puolestaan tarkoitetaan sitä, että tiedot ja tietojärjestelmät ovat saatavilla ja hyödynnettävissä niiden käyttöön oikeutetuille. (Kyberturvallisuuskeskus, 2021.) Tietoturva käsittää kaikki toimenpiteet, jolla pyritään suojaamaan käsiteltävää tietoa muun muassa valtuuttamattomalta pääsyltä, käytöltä, muokkaamiselta tai

tuhoamiselta (ENISA, 2016, s. 10). Organisaatioiden liiketoiminnassaan käsiteltävä arvokas tieto voi myös sisältää henkilötietoja ja on tärkeää huomioida, että tietoturvan tehtävänä on suojella kaikkea tietoa, mukaan lukien henkilötietoja. Voidaan siis nähdä, että tietoturva on yksi tietosuojan toteuttamisen keinoista sekä yksi keskeisimmistä mahdollistajista (Tietosuojavaltuutetun toimisto, n.d.; EDPS, n.d.-b).

Tietoturvan tarkoituksena ja yhtenä tavoitteena on henkilötietojen suojaamisen kautta taata rekisteröidyn henkilön oikeuksien toteutuminen. Tietojen turvaaminen ja hyvän tietoturvan toteuttaminen tuo kuitenkin jatkuvasti haasteita organisaatioille. Jatkuva muutos organisaatioiden toimintaympäristöön liittyen tekee tietoturvan toteuttamisen haastavaksi (EDPS, n.d.-b). Tämä jatkuva muutos johtuu muun muassa teknologisesta kehityksestä, uusien haavoittuvuuksien löytymisestä sekä vaihtuvasta oikeudellisesta hallintojärjestelmästä (EDPS, n.d.-b). Esimerkiksi GDPR, ja tarkemmin artikla 32 tuo vaatimuksia tietoturvan toteuttamiselle henkilötietojen suojaamiseksi. Seuraavaksi perehdytäänkin tietosuojalainsäädäntöön ja GDPR:ään tarkemmin.

3 GDPR

Tietosuojalainsäädännön historia juontaa juurensa 1970-luvulle. Ensimmäinen tietosuojalainsäädäntö otettiin käyttöön Saksan osavaltiossa Hessessä 1970. Ruotsi oli puolestaan ensimmäinen valtio, joka otti kansallisen tietosuojalainsäädännön käyttöön vuonna 1973. (Lynskey, 2016, s. 47.) Tietojenkäsittelyalan ilmaantuminen EU:ssa on yksi syistä miksi Euroopan parlamentti alun perin vaati tietosuojalainsäädäntöä 1970-luvun puolivälissä (Lynskey, 2016, s. 3). Henkilötietojen käsittelyn määrä kasvaa eksponentiaalisesti ja henkilötietoja käsitellään enemmän kuin koskaan ennen historiassa (Lynskey, 2016, s. 1, 2). Teknologinen kehitys mahdollistaa tämän merkittävän henkilötietojen käsittelyn kasvun, mutta sysäys tähän kasvuun on kuitenkin selitettävissä henkilötietojen arvon kasvulla (Lynskey, 2016, s. 2).

Lainsäädäntö on edelleen EU:ssa ensisijainen sääntelytapa vastauksena henkilötietojen käsittelyn ilmiöön (Lynskey, 2016, s. 4). EU:ssa on ollut vuosikymmeniä korkeat tietosuojalainsäädännön vaatimukset (EDPS, n.d.-a). Tietosuojalainsäädäntö oikeuttaa yksilöitä harjoittamaan tietosuojaoikeuksia ja velvoittaa julkisia ja yksityisiä organisaatioita, jotka käsittelevät yksilöiden tietoja kunnioittamaan näitä tietosuojaoikeuksia (EDPS, n.d.-a). Yhtenä maailman merkittävimmistä tietosuojalainsäädännöstä voidaan pitää GDPR:ää, johon perehdytään seuraavaksi.

3.1 GDPR:n tavoitteet

EU hyväksyi huhtikuussa 2016 uuden oikeudellisen kehyksen – GDPR:n (EDPS, n.d.-a). GDPR on täysin sovellettavissa kaikkialla EU:ssa toukokuusta 2018 lähtien, ja sitä pidetään maailman kattavimpana ja edistyneimpänä tietosuojalainsäädäntönä, joka on päivitetty vastaamaan jatkuvasti kehittyvän digitaalisen aikakauden vaikutuksia (EDPS, n.d.-a). GDPR kumosi tietosuojadirektiivin 95/46/EY, joka luotiin vuonna 1995 olennaiseksi osaksi EU:n yksityisyyttä ja ihmisoikeuksia koskevaa lainsäädäntöä (Wilhelm, 2016). Tammikuussa 2012 Euroopan komissio ehdotti kattavaa uudistusta vuoden 1995 tietosuojasäännöksiin vahvistaakseen yksityisyyden suojaa verkossa sekä Euroopan digitaalisen talouden vauhdittamiseksi (Wilhelm, 2016; EDPS, n.d.-c). Tähän selkeinä syinä oli se, että teknologian kehitys ja globalisaatio ovat muuttaneet perusteellisesti tapoja, joilla tietojamme kerätään ja käsitellään (Wilhelm, 2016).

GDPR:ssä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679) linjataan heti asetuksen alussa, että "luonnollisten henkilöiden suojelu henkilötietojen käsittelyn yhteydessä on ihmisen perusoikeus" (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, johdanto-osa 1). Asetuksen yksi keskeinen tarkoitus määritellään seuraavanlaisesti: "Tämän asetuksen tarkoituksena on tukea vapauden, turvallisuuden ja oikeuden alueen ja talousunionin kehittämistä,

taloudellista ja sosiaalista edistystä, talouksien lujittamista ja lähentämistä sisämarkkinoilla sekä luonnollisten henkilöiden hyvinvointia" (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, johdanto-osa 2).

GDPR:n alustuksessa myös nostetaan esille tärkeänä asiana, kuinka teknologian nopea kehitys ja globalisaatio ovat tuoneet henkilötietojen suojeluun uusia haasteita sekä kuinka henkilötietoja voidaan käyttää ennennäkemättömän laajasti niin yritys- kuin viranomaistoiminnassakin (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, johdanto-osa 6). Tärkeänä lisänä mainitaan, että yksityiset henkilöt myös jakavat yhä useammin henkilötietojaan maailmanlaajuisesti julkisuuteen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, johdanto-osa 6). GDPR:ssä jatketaan, että tämän kehityksen vuoksi tarvitaan luottamusta rakentava vahva ja johdonmukaisempi tietosuojakehys, jotta digitalous pystyy kehittymään koko unionin sisämarkkinoiden alueella (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, johdanto-osa 7).

GDPR:n ensimmäisessä artiklassa määritellään asetuksen kohde ja tavoitteet. Asetuksen kohteina ja tavoitteena ovat muun muassa vahvistaa säännöt henkilötietojen käsittelyssä sekä suojella perusoikeuksia ja –vapauksia, erityisesti oikeutta henkilötietojen suojaan (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 1. artikla).

Asetuksen soveltamisalasta on hyvä mainita, että asetusta sovelletaan osittain tai kokonaan automaattiseen henkilötietojen käsittelyyn. Tämän lisäksi asetusta sovelletaan myös muunlaiseen kuin automaattiseen käsittelyyn jos se muodostaa rekisterin osan tai sen on tarkoitus muodostaa rekisterin osa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 2. artikla.)

GDPR:n keskeisinä tavoitteina on siis yhdenmukaistaa sääntöjä henkilötietojen käsittelyssä EU:ssa sekä suojella perusoikeuksia ja –vapauksia nopeasti kehittyvän teknologian ja globalisaation tuomilta haasteilta.

3.2 GDPR:n keskeiset käsitteet

GDPR:ää tutkiessa on asetuksessa esiintyvien keskeisessä asemassa olevien käsitteiden määritelmiä hyvä tarkentaa. Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Henkilötiedoilla voidaan suoraan tai epäsuorasti tunnistaa luonnollinen henkilö ja henkilötietoja ovat muun muassa nimi, henkilötunnus tai sijaintitieto. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 4. artikla.)

Henkilötietojen käsittelyllä puolestaan tarkoitetaan GDPR:ssä henkilötietoihin kohdistettuja toimintoja, kuten tietojen keräämistä, tallentamista tai muokkaamista automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Rekisterillä tarkoitetaan jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein. Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä, oikeushenkilöä, viranomaista tai muuta elintä, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 4. artikla.)

GDPR:ssä määritellään henkilötietojen käsittelijän tarkoittavan luonnollista henkilöä, oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 4. artikla). Valvontaviranomaisella tarkoitetaan artiklan 51 nojalla perustettua riippumatonta viranomaista, joka on vastuussa GDPR:n soveltamisen valvonnasta henkilöiden perusoikeuksien ja vapauksien suojaamiseksi käsittelyssä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 4. artikla, 51. artikla).

Tutkimuksen kannalta myös keskeinen käsite on GDPR:ssä henkilötietojen yhteydessä käytetty termi riski. GDPR:n yhteydessä riskeillä tarkoitetaan henkilöiden oikeuksiin ja vapauksiin kohdistuvia todennäköisyydeltään ja vakavuudeltaan vaihtelevia riskejä, jotka voivat aiheutua henkilötietojen käsittelystä ja jotka voivat aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, johdanto-osa 75).

3.3 GDPR:n periaatteet

GDPR:ssä määritellään asetuksen kannalta hyvin keskeisessä asemassa rekisterinpitäjiä ja henkilötietojen käsittelijöitä noudattamaan tiettyjä henkilötietojen käsittelyä koskevia periaatteita oikeuksien toteutumiseksi. Näitä asetuksen määrittelemiä periaatteita ovat: käsittelyn lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, tietojen täsmällisyys, tietojen säilytyksen rajoittaminen, tietojen eheys ja luottamuksellisuus sekä rekisterinpitäjän osoitusvelvollisuus (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 5. artikla). Edellä mainittuja tietosuojaperiaatteita on noudatettava kaikissa henkilötietojen käsittelyvaiheissa (Oikeusministeriö, 2017, s.12).

Tärkeimpänä periaatteena ja vaatimuksena tämän tutkimuksen kannalta on eheyden ja luottamuksellisuuden vaatimus. Eheyden ja luottamuksellisuuden vaatimuksen osalta määritellään, että käsiteltäessä henkilötietoja tulee varmistaa tietojen asianmukainen turvallisuus ja niitä on suojattava muun muassa luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä tai vahingoittumiselta (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 5. artikla). Vaatimuksessa tarkennetaan, että on käytettävä asianmukaisia teknisiä ja organisatorisia toimia suojatakseen henkilötiedot ja toteuttaakseen vaatimuksen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 5. artikla).

Tämä luottamuksellisuuden ja eheyden periaate voidaan nähdä koskevan laajasti tietoturvan käsitettä ja sen mukaan täytyy toteuttaa asianmukainen suoja henkilötiedoille suojatakseen tietojen vahingollista tai tahallista vaarantumista. Tämä periaate tulee ottaa huomioon artiklan 32 rinnalla, joka sisältää tarkempia vaatimuksia ja tietoja käsittelyn turvallisuudesta. (ICO, 2021.) Tässä tutkimuksessa perehdytään tarkemmin artiklan 32 vaatimuksiin, mutta tämän perusteella voidaan nähdä, että artiklan 32 vaatimusten ymmärtämisen ja noudattamisen avulla voidaan tukea myös luottamuksellisuuden ja eheyden periaatteen noudattamista.

Eheyden ja luottamuksellisuuden periaatteen lisäksi tärkeänä on mainita osoitusvelvollisuus. Osoitusvelvollisuus tarkoittaa, että rekisterinpitäjän on pystyttävä osoittamaan periaatteiden noudattaminen eli rekisterinpitäjän on arvioitava, mitä periaatteet käytännössä tarkoittavat ja miten ne toteutuvat omassa toiminnassa (Oikeusministeriö, 2017, s.12). Tämän voidaan nähdä edellyttävän muun muassa henkilötietojen käsittelyn aiempaa tarkemman dokumentoinnin ja suunnittelun (Oikeusministeriö, 2017, s.12).

GDPR:ssä olennaisena vaatimuksena on myös oletusarvoinen ja sisäänrakennettu tietosuoja (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 25. artikla). Oikeusministeriön julkaisussa (2017) korostetaan, että nämä periaatteet edellyttävät tietosuojaan liittyvien kysymysten ottamista huomioon jo henkilötietojen käsittelyn suunnitteluvaiheessa ja lisäksi esimerkiksi tietojärjestelmät ovat rakennettava jo lähtökohtaisesti mahdollistamaan velvoitteiden toteuttamisen (Oikeusministeriö, 2017, s.13).

Sisäänrakennetulla tietosuojalla tarkoitetaan sitä, että tietosuojaperiaatteet täytyy ottaa tehokkaasti osaksi kaikkiin henkilötietojen käsittelyn vaiheisiin. Oletusarvoisella tietosuojalla puolestaan tarkoitetaan, että tulee käsitellä ainoastaan erityisen tarkoituksen kannalta tarpeellisia henkilötietoja.(Oikeusministeriö, 2017, s.13.)

Lisäksi käsittelytapoja määriteltäessä ja itse käsittelyn yhteydessä on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet tietosuojaperiaatteiden täytäntöönpanoa varten (Oikeusministeriö, 2007, s.13). Oikeusministeriön (2007) julkaisussa nostetaan esille, että rekisterinpitäjien on pääsääntöisesti itse määritettävä asianmukaiset toimenpiteet ottaen huomioon monia seikkoja, kuten käytettävissä oleva tekniikka, toteuttamiskustannukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit (Oikeusministeriö, 2007, s. 13). Tässä tutkimuksessa perehdytään juuri tähän asianmukaisten toimenpiteiden käsitteen tutkimiseen ja pyritään ymmärtämään vaatimuksia paremmin.

Tutkimusta ajatellen on tärkeää myös määritellä, kuinka hallinnollisten sakkojen määrääminen GDPR:ssä esitellään. Jokaisella valvontaviranomaisella on valtuudet määrätä hallinnollinen sakko säännösten rikkomisesta artiklan 83 nojalla (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 58. artikla). Tämän tutkimuksen tarkempana kohteena on artikla 32, jonka säännösten rikkomisen kohdalla voidaan määrätä hallinnollinen sakko, joka on enintään 10 000 000 euroa tai yritykselle kaksi prosenttia edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta riippuen siitä, kumpi näistä määristä on suurempi (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 83. artikla)

Lisäksi on tärkeää ottaa huomioon, että GDPR jättää pienen tilan valtiokohtaisille mukautuksille. Käytännössä artiklat 6,9 ja 10 tarjoavat hieman, mutta rajallisesti tilaa valtiokohtaiselle ohjailulle (Ruohonen & Hjerppe, 2021, s. 2). Nämä jätetään kuitenkin tässä tutkimuksessa pois tarkastelusta.

3.4 Aikaisempaa tutkimusta GDPR:ään liittyen

Kuten aikaisemmin mainittiin, astui GDPR voimaan vuonna 2016 ja sitä alettiin soveltamaan vuonna 2018, joten kyseessä on uusi asetus. Tämän seurauksena aikaisempaa tutkimusta aiheesta on hyvin rajallinen määrä. Tamburri (2020) kuvailee, että GDPR:ään liittyvä tutkimus on vielä niukkaa ja alustavaa (Tamburri, 2020, s. 3). Hän jatkaa, että systemaattista GDPR:n tutkimusta, jolla pyrittäisiin hyödyntämään ammattilaisia ja käyttäjiä liittyen GDPR:ään ei ole saatavilla (Tamburri, 2020, s.3).

Pyrin kuitenkin tuomaan esille tutkimuksen kannalta keskeisiä aikaisempia tutkimuksia ja tutkimustuloksia, joita hain käyttäen pääasiassa JYKDOKia ja Google Scholar -hakukonetta. Aikaisemmat julkaisut ja tutkimukset liittyen GDPR:ään on käsitellyt muun muassa asetuksen tuomia vaikutuksia ja haasteita. Presthus, Sørum & Andersen (2018) tutkivat norjalaisten yritysten GDPR:n vaatimustenmukaisuutta ja noudattamista. He esittelevät tuloksissaan, että 19 % yrityksistä pitävät artiklaa 32 suurimpana huolenaiheena ja n. 46 % yrityksistä kertoivat, että haasteita GDPR:n noudattamiseen tuo se, että heillä on rajallinen ymmärrys itse asetuksesta (Presthus ym., 2018). Yhteenvetona he toteavat heidän tuloksensa osoittavan, että norjalaisilla yrityksillä on enemmän haasteita kuin mahdollisuuksia GDPR:ää ajatellen. He jatkavat, että yrityksillä on erityisesti vaikeuksia ymmärtää asetusta, kuten esimerkiksi siinä esiteltäviä rahallisia seuraamuksia (Presthus ym., 2018). Voidaan siis ajatella, että GDPR vaatii lisää tutkimusta, jonka avulla pyritään tekemään selkeyttä GDPR:n artikloihin ja niiden noudattamiseen liittyen.

Ruohonen ja Hjerppe (2021) tutkivat GDPR:n yksittäisiä artikloja, joihin viitataan GDPR:n rikkomisesta annetuissa sakkopäätöksissä. Heidän tutkimuksensa toteutettiin tutkimalla sakkopäätösten saatavilla olevia metatietoja sekä tekstinlouhinnalla sakkopäätösdokumenteista. Tulokset osoittavat, että artiklat 5, 6 ja 32 ovat useimmiten viitattuina ja mainittuina sakkopäätöksissä (Ruohonen & Hjerppe, 2021). Ruohonen ja Hjerppe (2021) esittävät, että aikaisempi tutkimus GDPR:n vaatimuksista on suurilta osin keskittynyt GDPR:n teknisiin implementointeihin ja niiden vaatimusten noudattamiseen, ja organisatoriset vaatimukset on jätetty huomiotta (Ruohonen & Hjerppe, 2021, s. 3). He myös jatkavat, että hallinnollisen puolen tutkimisella on mahdollista saada uutta näkökulmaa ja sakkopäätösten tutkiminen on saanut vain vähäistä huomiota - muutamia lyhyempiä selostuksia lukuun ottamatta aikaisempaa tutkimusta ei näytä olevan (Ruohonen & Hjerppe, 2021, s. 3). Ruohonen ja Hjerppe (2021) esittelevät myös tulevaisuuden tutkimusideoita, joista yksi on se, että tarkemmalla sakkopäätösten analyysillä voisi olla mahdollista luoda implisiittisiä viitekehyksiä GDPR:n vaatimustenmukaisuuden käyttöönotolle (Ruohonen & Hjerppe, 2021, s. 9). Tämä on yksi tämän tutkimuksen tavoitteista, luoda lisää tietoa GDPR:n vaatimustenmukaisuudesta ja asetuksen noudattamisesta artiklan 32 kohdalla.

Wolters (2017) tutkii GDPR:n henkilötietojen turvallisuuden vaatimuksia ja tarkemmin sitä, onnistuuko GDPR yhdenmukaistamaan lainsäädäntöä ja

yksityisoikeuden velvollisuutta henkilötietojen suojaamiseksi verrattuna aikaisempaan lainsäädäntöön (Wolters, 2017). Hän toteaa johtopäätöksenä, että GDPR:n laajempi lähestyminen, joka ottaa huomioon niin rekisterinpitäjän kuin henkilötietojen käsittelijän henkilötietojen suojaamisessa johtaa huomattavaan yhdenmukaistamiseen. GDPR luo suoraan sovellettavan velvollisuuden, joka on ainakin teoriassa sama kaikille jäsenmaille EU:ssa ja velvollisuuden rikkominen johtaa yksityisoikeudelliseen vastuuseen. (Wolters, 2017, s. 177.)

Goddard puolestaan pohtii julkaisussaan GDPR:n tuomia muutoksia ja vaikutuksia organisaatioille ja yksityishenkilöille (Goddard, 2017). Hän nostaa yhtenä avainuudistuksena ja muutoksena GDPR:stä sen oikeudellisen ulottuvuuden, joka kattaa alleen myös organisaatiot, jotka eivät ole EU:ssa, mutta jotka kohdistavat toimiaan EU:n kansalaisiin tai monitoroivat EU:n kansalaisia (Goddard, 2017, s. 704).

Politou, Alepis & Patsakis (2018) tutkivat haasteita ja mahdollisia ratkaisuja liittyen GDPR:n vaatimuksiin koskien oikeuteen tulla unohdetuksi ja suostumuksen perumiseen (Politou ym., 2018). Politou ym. (2018) huomauttavat, että vaikka organisaatioille annetaan hyvin aikaa GDPR:n soveltamiseen harvat organisaatiot pystyvät todistamaan GDPR:n noudattamista. He jatkavat, että merkittävä tekijä tälle on se, että GDPR on pääasiallisesti lakidokumentti eikä siinä tarjota juurikaan teknisiä ohjeita sen toteuttamiselle (Politou ym., 2018, s. 15). Tärkeä huomio on kuitenkin se, että tämä oli EU:n tarkoituksellinen valinta, koska se ei halunnut sitoa GDPR:ää tiettyihin teknologioihin ja sitä kautta suosia tiettyjä alustoja, mutta tämä lähestymistapa voi aiheuttaa odottamattomia ongelmia organisaatioille pyrkimyksissään noudattamaan GDPR:n säännöksiä (Politou ym., 2018, s. 15). He toteavat johtopäätöksenä, että pystyäkseen toteuttamaan GDPR:n säännöksiä onnistuneesti ja myös osoittamaan tämä noudattaminen tarvitaan matalatasoisia ohjeistuksia täytäntöönpanoon sekä liiketoiminnan vaatimusten mallintamista (Politou ym., 2018, s. 16). Politoun ym. (2018) mukaan virallisten oikeudellisten ja teknisten EU:n elinten täytyy tarjota tapauskohtaisia suosituksia sekä teknologiariippumattomia standardeja (Politou ym., 2018, s. 16).

Kaiken kaikkiaan aikaisempaa GDPR:ään liittyvää tutkimusta on hyvin rajallinen määrä. GDPR on hyvin uusi tietosuojalainsäädäntö ja se vaatii lisää tutkimusta, jotta siihen liittyvät edellä mainitut haasteet vaatimuksenmukaisuuteen liittyen saadaan ratkaistua. Tutkimuksella pyritäänkin juuri vastaamaan tähän tutkimuksen tarpeeseen.

4 ARTIKLA 32 - KÄSITTELYN TURVALLISUUS

GDPR:ssä on yhteensä 99 artiklaa, joten kyseessä on hyvin iso kokonaisuus. Tässä tutkimuksessa artikla 32 on tarkemmassa tarkastelussa. Artiklassa 32 määritellään henkilötietojen käsittelyn turvallisuudesta (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 32). Artikla 32 määrittelee ja velvoittaa henkilötietojen käsittelyn turvallisuudesta seuraavaa:

> 1. Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten
>
> a) henkilötietojen pseudonymisointi ja salaus;
>
> b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;
>
> c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;
>
> d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 32. artikla)

Tämän lisäksi artiklassa vielä tarkennetaan, että ”Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi“ (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 32 artikla). Artikla on kokonaisuudessaan luettavissa tutkimuksen liitteenä (ks. liite 1).

Tutkiessa tarkemmin artiklaa 32, on tärkeää käydä keskeisiä vaatimuksia ja käsitteitä läpi artiklaan liittyen. Yksi keskeisistä velvollisuuksista rekisterinpitäjille ja henkilötietojen käsittelijöille GDPR:ssä ja tarkemmin artiklassa 32 on henkilötietojen turvallisuus (ENISA, 2016, s. 5). Henkilötietojen turvallisuudella GDPR:ssä tarkoitetaan aikaisemmin tutkimuksessa esitettyä tietoturvallisuuden kehystä eli tietojen luottamuksellisuutta, eheyttä ja saatavuutta (ENISA, 2016, s. 5). Euroopan unionin verkko- ja tietoturvaviraston (ENISA) julkaisussa (2016) esitetään tärkeitä huomioita henkilötietojen turvallisuudesta GDPR:ään ja artiklaan 32 liittyen (ENISA, 2016, s. 13).

Ensimmäisenä keskeisenä huomiona on se, että artiklassa 32 on omaksuttu riskiperusteinen lähestymistapa. Tämä tarkoittaa, että tekniset ja organisatoriset turvatoimenpiteet täytyvät olla asianmukaisia henkilötietoihin kohdistuviin

riskeihin nähden, eli mitä isompi riski henkilötietoihin kohdistuu, sitä tiukemmat turvatoimenpiteet on oltava käytössä (ENISA, 2016, s. 5, 13).

Toisena tärkeänä huomiona on se, että GDPR ei velvoita pelkästään tiettyjen turvatoimenpiteiden käyttöönottoa vaan tukee perusteellisen henkilötietojen tiedonhallintajärjestelmän perustamista henkilötietojen luottamuksellisuuden, eheyden, saatavuuden ja toipumiskyvyn turvaamiseksi (ENISA, 2016, s. 13). Kuten artiklan 32 vaatimuksista huomataan, vaaditaan siinä teknisten ja organisatoristen toimenpiteiden tehokkuuden säännöllistä testaamista ja arvioimista. Lisäksi siinä velvoitetaan takaamaan järjestelmien ja palveluiden jatkuva tietoturvallisuus sekä kyky palauttaa nopeasti tietojen saatavuus vian sattuessa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 32. Artikla.)

Tämä tarkoittaa sitä, että GDPR:ssä otetaan huomioon kaikki tietoturvan ulottuvuudet ja siinä selvästi vaaditaan käyttöönotettujen suojatoimenpiteiden testaamista ja tehokkuuden arvioimista (ENISA, 2016, s. 13). Voidaan siis nähdä, että kokonaisvaltaisesta henkilötietojen riskienhallintajärjestelmästä voisi olla hyötyä vaatimusten noudattamisessa.

Tärkeänä huomio artiklaan 32 liittyen on myös se, että siinä viitataan erityisesti pseudonymisointiin ja salaukseen keskeisimpinä suojatoimenpiteinä henkilötietojen turvallisuudelle. Tämän voidaan nähdä osoittavan, että GDPR:ssä henkilötietojen tietoturvaa käsitellään yksityisyyden kontekstissa ja suojatoimenpiteisiin voi kuulua esimerkiksi henkilöllisyyden suojaaminen salausmekanismeilla (ENISA, 2016, s. 13).

Lisäksi artiklassa määritellään tietosuojaparametreja riskien arvioimiseen, kuten käsittelyn luonne, laajuus ja tarkoitukset (ENISA, 2016, s. 13). Euroopan tietosuojaneuvosto (EDPB) on julkaissut virallisen ohjeistuksen koskien artiklaa 25, jossa velvoitetaan rekisterinpitäjää ja henkilötietojen käsittelijää "Ottaen huomioon uusimman tekniikan ja toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset - - rekisterinpitäjän on - -toteutettava tehokkaasti tietosuojaperiaatteiden, kuten tietojen minimoinnin, täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet - -." (EDPS, 2020; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 25. artikla). Kuten nähdään, artiklassa 25 käsitellään samoja asioita kuin artiklassa 32, joten virallisesta ohjeistuksesta voi löytyä apua myös artiklaa 32 tarkastellessa.

Artiklassa 32 esitetty viimeisin tekniikka määritellään Euroopan tietosuojaneuvoston ohjeistuksessa (2020) artiklan 25 osalta tarkoittavan sitä, että määrittäessään asianmukaisia teknisiä ja organisatorisia toimenpiteitä rekisterinpitäjien on velvollisuus ottaa huomioon markkinoilla saatavilla olevan tekniikan nykyinen kehitys. Ohjeistuksessa tarkennetaan, että viimeisin tekniikka on "liukuva käsite, jota on arvioitava jatkuvasti teknisen kehityksen yhteydessä". Tällä tarkoitetaan sitä, että tekniikan kehittyessä voi olla, että vanhat suojatoimenpiteet eivät enää tarjoa riittävää suojan tasoa GDPR:ää ajatellen. (EDPS, 2020, s. 8, 9.)

Tärkeänä huomiona on myös se, että viimeisin tekniikka käsite ei koske vain teknisiä suojatoimenpiteitä vaan koskee lisäksi organisatorisia suojatoimenpiteitä, sillä asianmukaisten organisatoristen toimenpiteiden puute voi heikentää valitun tekniikan tehokkuutta (EDPS, 2020, s.9). Euroopan tietosuojaneuvoston

ohjeistuksessa (2020) tuodaan esille, kuinka eri alojen voimassa olevilla standardeilla, sertifioinneilla tai käytännesäännöillä voidaan mahdollisesti osoittaa viimeisin tekniikka vaatimus (EDPS, 2020, s. 9). Lisäksi ohjeistuksessa kerrotaan, että jos on olemassa vaikkapa standardeja, jotka takaavat rekisteröidylle korkeatasoisen suojan lakisääteisten vaatimusten mukaisesti, on rekisterinpitäjien otettava ne huomioon tietosuojatoimenpiteiden suunnittelussa ja toteuttamisessa (EDPS, 2020, s. 9). Tämä on tärkeää ottaa huomioon artiklan 32 vaatimuksia ajatellen.

Käsittelyn luonteesta Euroopan tietosuojaneuvoston ohjeistuksessa (2020) sanotaan, että käsite voidaan ymmärtää tarkoittavan käsittelyn luontaisia ominaisuuksia, kuten automaattista päätöksentekoa tai ennakoimatonta käsittelyä. Laajuudella tarkoitetaan käsittelytoimien kokoa ja laajuutta. Asiayhteys taas voidaan nähdä liittyvän käsittelyn olosuhteisiin, ja tarkoitus käsittelyn tavoitteisiin. (EDPB, 2020, s. 10.) Nämä kaikki on ulottuvuudet sekä lisäksi henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit ovat otettava huomioon asianmukaisten teknisten ja organisatoristen toimenpiteiden määrittelemisessä. Keskeisenä huomiona on kuitenkin artiklan riskiperusteinen lähestymistapa, johon perehdytään seuraavaksi tarkemmin.

4.1 Riskiperusteinen lähestymistapa ja riskienhallinta

Kuten aikaisemmin mainittiin, on GDPR:ssä omaksuttu riskiperusteinen lähestymistapa velvoitteiden osalta (Oikeusministeriö, 2017, s.16). Tämä tarkoittaa, että henkilötietojen käsittelylle asetetut velvoitteet ja vaaditut asianmukaiset suojatoimet ovat suhteutettava rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin (Oikeusministeriö, 2017, s.16). Oikeusministeriön (2017) julkaisussa huomautetaan, että riskiperusteisella lähestymistavalla pyritään välttämään ylisääntelyä matalariskiselle toiminnalle ja suhteuttamaan tarpeelliset toimenpiteet käsittelyyn kohdistuvien riskien mukaisesti (Oikeusministeriö, 2017, s.16). Kuten aikaisemmin käytiin läpi, on artiklan 32 vaatimusten kannalta riskienhallinta olennainen osa vaatimuksia ja voi henkilötietojen riskienhallintajärjestelmästä olla hyötyä.

Tietoturvan riskienhallinnalla tarkoitetaan prosessia, jolla pyritään tunnistamaan ja hallitsemaan tietoturvariskejä, joita organisaation kohdistuu. Tämän lisäksi tietoturvan riskienhallinnan pyrkimyksenä on saavuttaa tehokas tasapaino hyödyttävien mahdollisuuksien toteuttamisen sekä mahdollisten tappioiden minimoinnin välillä. Tietoturvan hallinnan pitää olla olennainen osa hallintokäytänteitä sekä sen täytyy olla jatkuvaa toimintaa, jolla pyritään tukemaan organisatorista kehittymistä, suorituskykyä ja päätöksentekoa. (ENISA, 2016, s. 11.)

Riskiä ilmaistaan usein funktiona, jossa kerrotaan todennäköisyys uhan toteutumiselle tämän uhan toteutumisen haittavaikutuksen suuruudella, eli vaikutuksella (ENISA, 2016, s. 11). Riskienhallinnan voidaan nähdä koostuvan neljästä päävaiheesta, joita ovat riskien arviointi, riskien käsittely, riskien hyväksyminen ja riskien kommunikointi (ENISA, 2016, s. 11). Arvioinnilla tarkoitetaan

tilannekatsausta tämänhetkisistä riskeistä, joka aloitetaan uhkien tunnistamisella, jonka jälkeen määritellään jokaisen uhan todennäköisyys ja vaikutus. Riskien käsittelyn vaiheessa valitaan ja implementoidaan turvatoimet, joilla käsitellään riski. Riskien käsittelyn toimenpiteet voivat olla erityyppisiä ja niiden vaikutukset riskiin voi vaihdella riskin lieventämisestä riskin säilyttämiseen. (ENISA, 2016, s. 11.)

Seuraavana vaiheena riskienhallinnassa on riskien hyväksyminen, sillä käsittelyvaiheesta voi jäädä jäännösriskejä, jotka johtoportaan täytyy hyväksyä. Viimeisenä vaiheena on riskien kommunikointi eli kaikille sidosryhmille on tiedotettava omaksutut hallintatoimenpiteet sekä hyväksytyt riskit. (ENISA, 2016, s 11.)

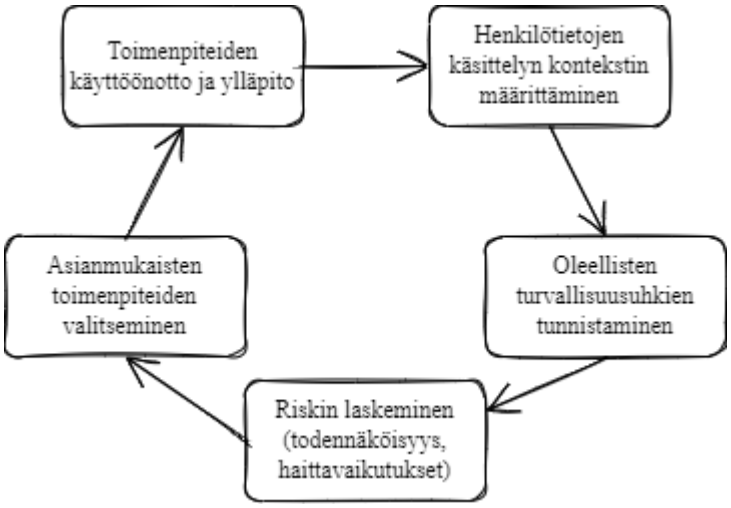
Henkilötietojen turvallisuus noudattaa käytännössä samoja periaatteita kuin tietoturvallisuus ja tietoturvallisuuden riskienhallinta (ENISA, 2016, s. 12). Tämä on tärkeää ottaa huomioon GDPR:ää ja artiklan 32 vaatimuksia ajatellen. On kuitenkin tärkeää huomioida, että henkilötiedoilla on tiettyjä erityispiirteitä, joita tulee ottaa huomioon, kun analysoidaan turvallisuusuhkia ja sen pohjalta otetaan turvatoimenpiteitä käyttöön (ENISA, 2016, s. 12). ENISA:n (2016) julkaisussa esitellään kahdenlaisia erityispiirteitä tavanomaisen tietoturvan riskienhallinnan ja henkilötietojen riskienhallinnan välillä (ENISA, 2016, s. 14).

Ensimmäisenä on haittavaikutuksen käsite. Tavanomaisessa riskienhallintaprosessissa riskit arvioidaan niiden potentiaalisesta haittavaikutuksesta organisaatiolle, kun taas henkilötietojen käsittelyn osalta haittavaikutuksia arvioidaan yksilöiden oikeuksien ja vapauksien toteutumisen osalta. (ENISA, 2016, s. 14) Haittavaikutuksia yksilölle voi olla esimerkiksi taloudellinen menetys, fyysinen tai psykologinen haitta tai maineen vahingoittuminen (ENISA, 2016, s. 14).

Toisena erityispiirteenä henkilötietojen turvallisuuden osalta tavanomaiseen tietoturvallisuuteen on riskienhallinta. Edellä mainittu ero haittavaikutuksista voi tuoda eroja myös riskienhallintaan, sillä vaikka jonkin riskin toteutumisen todennäköisyys on hyvin pieni, niin sen haittavaikutukset voivat olla hyvin vakavat yksilölle, kuten vakava fyysinen vahinko tai hengenvaara, jolloin riskin hyväksyminen olisi väärä ratkaisu. (ENISA, 2016, s. 14.) Tällaisessa tapauksessa tulisi todennäköisesti välttää riski arvioimalla uudelleen koko henkilötietojen käsittelyprosessi tai ottaa käyttöön yksityisyyden suojaa parantavaa tekniikkaa, kuten anonymisointitekniikkaa (ENISA, 2016, s. 14). Nämä seikat huomioon ottaen voidaan siis todeta, että teknisten ja organisatoristen toimenpiteiden arvioimisessa ja käyttöönotossa voi siis esiintyä eroavaisuuksia tavanomaisen riskienhallinnan ja tietosuojan riskienhallinnan välillä.

Tärkeää henkilötietojen turvallisuuden riskinhallinnassa on aluksi määritellä koko henkilötietojen käsittelyn konteksti, kuten käsiteltävien henkilötietojen tyypit ja oikeutetut vastaanottajat (ENISA, 2016, s.14). Tämä koko käsittelyn kontekstin määrittely tukee uhkien ja riskien määrittämistä yksilöihin kohdistuvien haittavaikutuksien perusteella, jonka jälkeen otetaan käyttöön asianmukaiset tekniset ja organisatoriset toimenpiteet riskien hallitsemiseksi ottaen huomioon henkilötietojen turvallisuuteen liittyvät erityispiirteet (ENISA, 2016, s.14). Henkilötietojen turvallisuuden riskienhallinta on esitettynä vaiheittain kuviossa 1.

Tämä kuvio on tärkeä artiklan 32 riskiperusteista lähestymistä ja vaatimuksia ajatellen.



KUVIO 1 Henkilötietojen turvallisuuden riskienhallinta (ENISA, 2016, s. 15 mukaan)

Tärkeänä huomiona riskiperusteisesta lähestymistavasta Euroopan tietosuojaneuvosto (2020) huomauttaa, että kyseinen lähestymistapa ei sulje pois perustasojen, parhaiden käytäntöjen ja standardien käyttöä vaan ne voivat hyödyllisiä työkaluja käsiteltäessä samanlaisia riskejä samanlaisissa tilanteissa (EDPB, 2020, s. 10). Kuitenkin vaikka tällaisia työkaluja käyttäisi apunaan on rekisterinpitäjien tehtävä aina tapauskohtainen arviointi käsittelytoimen aiheuttamista tietosuojariskeistä ja varmistettava ehdotettujen suojatoimenpiteiden tehokkuus (EDPB, 2020, s. 10) Johtopäätöksenä voidaan siis todeta, että toteuttaakseen GDPR:ssä säädettyjä velvollisuuksia täytyy reksiterinpitäjän tehdä perusteellinen riskiarvio henkilötietojen käsittelyyn liittyen (Oikeusministeriö, 2017, s.16).

Nämä edellä mainitut erityispiirteet sekä henkilötietojen riskienhallinta on tärkeää ottaa huomioon, kun tutkitaan tarkemmin artiklaa 32 ja analysoidaan siihen liittyviä sakkopäätöksiä. Yhteenvetona voidaan todeta, että artiklan 32 vaatimukset ovat riskiperusteisia ja vaatimusten noudattamiseen vaaditaan tietosuojan riskienhallintajärjestelmän perustamista. Taatakseen riittävän tietosuojan, organisaatioiden tulee ottaa käyttöön riskienhallintamenetelmä, jolla arvioidaan henkilötietojen käsittelyyn kohdistuvia turvallisuusriskejä (EDPS, n.d.-b). Tämän jälkeen organisaatioiden tulee toteuttaa tietoturvatoimia hallitakseen näitä riskejä (EDPS, n.d.-b).

4.2 Tekniset ja organisatoriset toimenpiteet

Artiklan 32 vaatimuksissa velvoitetaan toteuttamaan riskiä vastaavat asianmukaiset tekniset ja organisatoriset toimenpiteet. Euroopan tietosuojaneuvoston

ohjeistuksessa (2020) huomautetaan, että asianmukaisuuden vaatimus liittyy läheisesti tehokkuuden vaatimukseen, sillä teknisten ja organisatoristen suojatoimenpiteiden avulla on voitava panna tietosuojaperiaatteet täytäntöön tehokkaasti (EDPB, 2020, s. 6). Euroopan tietosuojaneuvosto (2020) määrittelee teknisten ja organisatoristen toimenpiteiden voivan olla "niin kehittyneiden teknisten ratkaisuiden käyttöä kuin peruskoulutuksen järjestämistä henkilökunnalle" (EDPB, 2020, s. 6).

Organisatorisilla toimenpiteillä tarkoitetaan hallinnollisia ei-teknisiä toimenpiteitä henkilötietojen suojaamiseksi ja teknisillä toimenpiteillä teknisesti toteutettavia toimenpiteitä. ENISA:n esittelee julkaisussaan organisatorisia toimenpiteitä, joita ovat muun muassa turvallisuuspolitiikat ja toimintatavat henkilötietojen suojaamiseksi (ENISA, 2016, s. 33).

Teknisiä suojatoimenpiteitä ovat puolestaan esimerkiksi lokitietojen kerääminen ja monitorointi (ENISA, 2016, s. 40). Oikeusministeriön julkaisussa esimerkkejä teknisistä ja organisatorisista suojatoimenpiteistä ovat muun muassa henkilöstön koulutus, tilavalvonta, tietojen salaus ja tekniset rajoitukset (Oikeusministeriö, 2017, s.13). Näistä selkeästi organisatorisena toimenpiteenä voidaan nähdä henkilöstön koulutus ja teknisinä toimenpiteitä tilavalvonta, tietojen salaus ja tekniset rajoitukset.

Tärkeänä huomiona artiklaan 32 liittyen on myös GDPR:ssä velvoitettava osoitusvelvollisuus. Osoitusvelvollisuus tarkoittaa sitä, että rekisterinpitäjän pitäisi dokumentoida toteutetut tekniset ja organisatoriset toimenpiteet, joilla pyritään saamaan haluttu vaikutus tietosuojan kannalta (EDPB, 2020, s.8).

Euroopan tietosuojaneuvoston ohjeistuksessa esitetään, että osoitusvelvollisuuden noudattamiseksi rekisterinpitäjä voi määrittää tulosindikaattoreita (KPI), joilla suojatoimenpiteiden tehokkuus voidaan osoittaa. Tulosindikaattorit voivat olla määrällisiä, kuten esimerkiksi väärien positiivisten tulosten osuus tai laadullisia kuten asiantuntija-arvio. Toinen vaihtoehto periaatteiden tehokkaan täytäntöönpanon osoittamiseen on antamalla perustelut valittujen suojatoimenpiteiden tehokkuuden arvioinnille. (EDPB, 2020, s. 8.)

4.3 Standardit ja GDPR:n vaatimuksenmukaisuus

Kuten aikaisemmin artiklaa 32 tarkasteltaessa tuli esille, vaatii artiklan 32 vaatimusten noudattaminen jatkuvaa suojatoimenpiteiden testaamista, tutkimista sekä tehokkuuden arvioimista ja näin ollen vaatimusten noudattamisessa voi hyötyä kokonaisvaltaisen tietoturvan hallintajärjestelmän perustamisesta. Tärkeänä tutkimuksen kannalta onkin huomioida artiklan 32 kohta, jossa määritellään, että yhtenä tekijänä osoittaa artiklan 32 kohdan 1 asetettujen vaatimusten noudattamista on noudattaa artiklan 40 käytännesääntöjä tai artiklan 42 sertifiointimekanismia (katso Liite 1) (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 32. artikla).

Tietoturvallisuuden hallinnan standardit ovat yleisimmin käytettyjä menetelmiä tietoturvallisuuden hallintaan (Siponen, 2006, s. 97). Tietojenkäsittelyyn

liittyviä standardeja on olemassa useita ja standardisointi voi auttaa organisaatioita osoittamaan vaatimustenmukaisuuden sekä prosessien ja vastuualueiden jäsentämisessä liittyen tietojenkäsittelyyn (Kamara ym., 2019, s. 130). Omaksumalla auktoritatiivisen ohjeistuksen organisaatiot pystyvät osoittamaan sitoutumisensa toimintansa turvaamiseen. Organisaatiot voivat hakea tämän ohjeistuksen noudattamisen jälkeen sertifiointia, joka todistaa organisaation noudattavan tiettyjä sääntöjä ja käytäntöjä. (Siponen & Willison, 2009, s. 267.)

Markkinat tunnustavat tietosuojaan liittyvistä standardeista oleellisimmiksi ISO:n ja IEC:in ajamat standardit, erityisesti ISO 27000 -sarjan (Kamara, ym., 2019, s. 151). ISO 27000 sarjaan kuuluvan ISO 27001 -standardin käyttöönotto johtaa yritysten omaksumaan riittävän mallin tietoturvan hallintajärjestelmän perustamiseksi, toteuttamiseksi, käyttämiseksi, valvomiseksi ja uudelleenarvioimiseksi (Lopes ym., 2019). ISO 27001 –standardi esittelee tehokkaan tietoturvan kolme olennaista näkökohtaa, jotka ovat ihmiset, prosessit ja teknologiat (Lopes ym., 2019).

Voidaan siis päätellä, että tietosuojaan ja tietoturvaan liittyvien standardien noudattaminen voi tukea hyvin yleisesti GDPR:n ja tarkemmin artiklan 32 vaatimusten noudattamista sekä niiden tulkitsemista. Tästä huomauttaa myös Kamaran ym., (2019) tehdyssä tutkimuksessa liittyen GDPR:ään, standardeihin ja sertifiointiin (Kamara ym., 2019). Kamara ym., (2019) kuvaavat tutkimuksessaan, että esimerkiksi ISO 27001 sertifikaatti voi auttaa osoittamaan juuri artiklan 32 noudattamista (Kamara ym., 2019, s. 48, 49). On kuitenkin tärkeää huomioida, että kyseisiä standardeja ei ole välttämättä suunniteltu GDPR:n säännösten noudattamisen auttamiseen (Kamara ym., 2019, s. 49). Kamara ym., (2019) jatkavat, että vaikka ISO standardit ovat relevantteja, on ISO standardien vaatimuksissa myös eroavaisuuksia ja ristiriitoja liittyen GDPR:ään (Kamara ym., 2019, s. 164). Tästä voidaan päätellä, että olemassa olevien standardien ei voida katsoa osoittavan suoraan asetuksen noudattamista.

Kamara ym., (2019) esittävätkin tutkimuksessaan, että standardien, joita voitaisiin suositella osoittavan GDPR:n vaatimuksenmukaisuutta tulisi olla hyvin yhteensopiva GDPR:n periaatteiden, terminologian, mekanismin ja laajuuden kanssa. Tämä ei päde vielä ainakaan merkittävään osaan nykyisistä tietosuojaan liittyvistä standardeista. (Kamara ym., 2019, s. 165.)

Standardien, ja tarkemmin ISO 27001 -standardin noudattamisen hyödyt GDPR:ää ajatellen nostaa myös esille Lopes, Guarda & Oliveira (2019) tutkimuksessaan. He huomauttavat, että ISO 27001 -standardin tarjoaman kokonaisvaltaisen viitekehyksen käyttöönotto voi yksinkertaistaa ja ohjata vaatimustenmukaisuutta GDPR:ää ajatellen (Lopes ym., 2019, s. 5). He kuitenkin nostavat esille, että vaatimustenmukaisuuksissa on monia eroja kuten se, että tietyt kontrollit täytyy mukauttaa ottamaan huomioon henkilötietojen suojaaminen ja ISO 27001 -standardissa ei suoranaisesti käsitellä henkilötietoja ja tiedon yksityisyyttä (Lopes ym., 2019, s. 5). Voidaan siis nähdä, että ISO 27001 -standardi ei takaa GDPR:n vaatimustenmukaisuutta, mutta se voidaan kuitenkin nähdä arvokkaana vaiheena kohti sitä (Lopes ym., 2019, s. 5).

Tämän pohjalta tutkimuksessa luodaankin analyysin tueksi standardeihin ja henkilötietojen riskienhallintaan pohjautuva asianmukaisten teknisten ja organisatoristen toimenpiteiden -viitekehys, joka pyrkii kattamaan alleen olennaiset ulottuvuudet artiklan 32 vaatimuksista. Tätä viitekehystä käytetään analyysin tukena ja se esitellään tarkemmin luvussa 5.

Kuten edellä luvussa käsiteltiin, täytyy rekisterinpitäjien ja henkilötietojen käsittelijöiden pääsääntöisesti itse määrittää riskiä vastaavat asianmukaiset tekniset ja organisatoriset toimenpiteet. Tämä voi olla hyvinkin haastavaa organisaatioille ja paineita velvoitteiden noudattamiselle tuo se, että artiklan velvoitteiden rikkomisesta voidaan määrätä hallinnollisia sakkoja.

Seuraavaksi tarkastellaan tutkimusmenetelmää ja viitekehystä, jonka jälkeen tutkitaan tutkimuksen aineiston avulla, minkälaisia havaintoja jo annetuissa hallinnollisissa sakoissa esiintyy liittyen artiklan 32 vaatimuksiin asianmukaisista teknisistä ja organisatorisista toimenpiteistä. Analyysin avulla pyritään selvittämään, minkälaisia toimenpiteitä ja tarkempia vaatimuksia kyseisen artiklan käsitteet asianmukaiset tekniset ja organisatoriset toimenpiteet pitävät sisällään.

5 METODI JA AINEISTON ESITTELY

Tämä tutkimus toteutetaan käyttäen systemaattista käsiteanalyysia tutkimusmenetelmänä. Nuopponen (2020) esittää, että systemaattisella käsiteanalyysillä on tarkoitus järjestää eri tavoin saatua käsitetietoa yhtenäisiksi, johdonmukaisiksi kokonaisuuksiksi käsitesuhteita selvittämällä (Nuopponen, 2020, s. 100). Wilson (1963) huomauttaa, että käsiteanalyysissä ei olla niinkään kiinnostuneita tietyn sanan tarkoituksesta, sillä sanoilla ei ole vain yhtä tarkoitusta, vaan käsiteanalyysissä ollaan kiinnostuneita todellisista ja mahdollisista sanojen käyttötarkoituksista. Wilson (1963) jatkaa, että käsiteanalyysissä on tarkoitus analysoida käsitteitä ja kartoittaa niiden käyttöä ja soveltamista. Hän myös huomauttaa, että käsitteisiin liittyvät kysymykset eivät ole fakta- tai arvokysymyksiä, vaan käsitteiden analyysi koskee sanojen käyttöä ja kriteereitä tai periaatteita, joiden perusteella sanojen käyttötarkoitukset määritetään. (Wilson, 1963, s. 10, 11.)

Puusa (2008) huomauttaa julkaisussaan käsiteanalyysillä olevan useita erilaisia käyttötarkoituksia, mutta yleisesti käsiteanalyysin avulla jäsennetään tutkittavaa käsitettä, pyritään ymmärtämään käsitteeseen liitettyjä merkityksiä ja selkeyttämään sen suhdetta lähikäsitteisiin. Hän jatkaa, että käsiteanalyysin avulla kyetään tunnistamaan tutkittavasta käsitteestä sen kriittiset ominaispiirteet perehtymällä laajasti saatavilla olevaan kirjalliseen lähdeaineistoon. Lisäksi Puusa (2008) huomauttaa, että käsiteanalyysin avulla tutkija voi ymmärtää paremmin käsitteen kuvaamaa ilmiötä ja analyysin lopputulemaa voi käyttää jonkinlaisena jäsennyksenä eli "työhypoteesina".(Puusa, 2008, s. 36, 39.)

Tässä tutkimuksessa käsiteanalyysin avulla on tarkoitus analysoida asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteitä ja kartoittaa niiden käyttöä ja soveltamista. Tämän analyysin tavoitteena on ymmärtää paremmin artiklan 32 vaatimuksia ja tarkemmin, minkälaisia toimenpiteitä asianmukaiset tekniset ja organisatoriset toimenpiteet käsitteinä kattavat alleen. Tutkimuskysymys on seuraavanlainen:

- Minkälaisia toimenpiteitä GDPR:n artiklan 32 asianmukaiset tekniset ja organisatoriset toimenpiteet käsitteinä kattavat alleen?

On tärkeää huomioida, että kyseisillä käsitteillä ei ole vain yhtä tarkoitusta, kuten Wilson (1963) huomauttaa, vaan ideana onkin juuri tutkia näiden sanojen käyttöä ja kriteereitä, jotka määrittelevät asianmukaisia toimenpiteitä. Nuopponen (2020) kuvaa systemaattista käsiteanalyysiä menetelmänä, joka tarjoaa konkreettisia työkaluja hyvinkin abstraktien ja monitahoisten käsitteiden ja erityisesti käsitteiden välisten suhteiden yksityiskohtaiseen selkeyttämiseen. Hän jatkaa, että systemaattisen käsiteanalyysin avulla voidaan muun muassa koostaa ja analysoida aineistoa, esittää ja pohtia tutkimustuloksia sekä selkeyttää, että johdonmukaistaa tutkielmatekstiä. (Nuopponen, 2020, s. 119.)

Nuopponen (2020) esittää, että systemaattista käsiteanalyysiä voidaan käyttää koko tutkimuksen päämenetelmänä esimerkiksi tilanteessa, jossa aineiston

pohjalta pyritään luomaan kokonaiskuvaa tutkittavasta ilmiöstä (Nuopponen, 2020, s. 116). Puusa (2008) tuo myös esille julkaisussaan, että käsitetutkimusta voidaan pitää itsenäisenä tutkimusotteena, sillä sen avulla voidaan laatia itsenäinen käsitteelliseen tarkasteluun perustuva tutkimuskokonaisuus ilman empiiristä tutkimusosaa (Puusa, 2008, s. 38).

Tässä tutkimuksessa pyritään aineiston pohjalta luomaan kokonaiskuvaa tutkittavasta ilmiöstä, joten systemaattinen käsiteanalyysi sopii koko tutkimuksen päämenetelmäksi. Tutkimus toteutetaan teorialähtöisellä analyysillä. Nuopponen (2020) kuvailee, että teorialähtöisessä analyysissä voidaan eritellä aineistosta havaintoja valmiin tai muokatun luokittelun tai käsitejärjestelmän avulla, eli voidaan edetä yleisestä yksityiseen päin (Nuopponen, 2020, s. 115). Nuopponen (2020) myös huomauttaa, että teoria- ja aineistolähtöinen eteneminen eivät kuitenkaan sulje toisiaan pois, vaan tutkimus voi useinkin olla niiden välimuoto sillä esimerkiksi teorialähtöinen tarkastelukehikko voi tarkentua aineiston avulla. (Nuopponen, 2020, s. 116.)

Tutkimuksessa luokittelen aineistosta havaintoja ennalta määrättyihin luokkiin henkilötietojen riskienhallinnan viitekehykseen pohjautuen, joten kyseessä on teorialähtöinen analyysi. Tärkeää on huomioida myös se, että systemaattisen käsiteanalyysin työmenetelmissä keskeistä on käsitteiden välisten suhteiden esille tuominen käsitejärjestelmien graafisten esitysten avulla (Nuopponen, 2020, s. 119). Tuon tutkimuksessa aineistosta nousevia havaintoja ja käsitteiden välisiä suhteita esille graafisten esitysten avulla, ja käytän analyysin tukena Nuopposen (2020) esittelemää sateelliittimallia.

Satelliittimallissa on yksi keskuskäsite, johon liitetään keskuskäsitteen keskeisimpiä lähikäsitteitä sen ympärille, ja lähikäsitteillä voi edelleen olla omia lähikäsitteitä ja niin edelleen. Mallissa voidaan myös merkitä suhdetyypit näiden käsitteiden välille, mikä on satelliittimallissa keskeistä. (Nuopponen, 2020, s. 103.) Nuopponen (2020) kuitenkin huomauttaa, että esitystapaa voidaan käyttää käsitesuhteiden analyysin ja kuvauksen lisäksi myös ilmiöiden ominaisuuksien erittelyyn (Nuopponen, 2020, s. 103). Tämä on tässä tutkimuksessa keskeisessä osassa, sillä pyrin tutkimaan ilmiön, eli tässä tapauksessa artiklan 32 vaatimien asianmukaisten teknisten ja organisatoristen toimenpiteiden ominaisuuksia ja vaatimuksia.

Systemaattista analyysia ja sateelliittimallia käyttivät esimerkiksi Nissilä ja Nuopponen (2018) tutkimuksessaan ja he esittävät tuloksensa graafisen esityksen avulla. He lisäksi käyttivät aikaisemmassa tutkimuksessa esitettyä jaottelua pääluokkien osalta, johon he luokittelivat aineistosta löytyviä havaintoja (Nissilä & Nuopponen, 2018, s. 178).

Tutkin siis käsiteanalyysin avulla artiklan 32 asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteitä. Pyrin tällä tutkimusmenetelmällä paremmin ymmärtämään, mitä ulottuvuuksia ja toimenpiteitä liittyy asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteisiin. Tutkin kyseistä tutkimusongelmaa alla esiteltävän analyysia tukevan viitekehyksen sekä tutkimukseen valitun aineiston avulla.

5.1 Riskienhallinnan viitekehys

Kuten aikaisemmin luvussa 4.1 määriteltiin, on tärkeänä tekijänä artiklan 32 vaatimuksiin liittyen henkilötietojen riskienhallinta sekä riskienhallintajärjestelmän perustaminen. Muodostin kahden eri tietoturvaan ja tietosuojaan liittyvän mallin pohjalta asianmukaisten organisatoristen ja teknisten suojatoimenpiteiden viitekehyksen, joka kattaa alleen henkilötietojen riskienhallinnan eri ulottuvuuksia. Tämän viitekehyksen tarkoituksena on tukea aineistosta nousevien havaintojen systemaattista luokittelua ennalta määrättyihin kategorioihin liittyen artiklan 32 vaatimuksiin.

National Institute of Standards and Technology (NIST) on julkaissut kyberturvallisuuden viitekehyksen kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi. NIST:in viitekehys kokoaa useita nykypäivän tehokkaasti toimivia standardeja, ohjeistuksia ja käytäntöjä viitekehykseensä, ja tarjoaa yleisen organisointirakenteen useille eri lähestymistavoille kyberturvallisuuteen liittyen (NIST, 2018, s. v-vi). Kyseessä on hyvin kokonaisvaltainen viitekehys kyberturvallisuuden ja tietoturvallisuuden hallintaan organisaatiossa. Käytän tutkimuksessa tätä kyseistä viitekehystä apuna edellä mainitun - myös artiklassa 32 vaaditun tietoturvan riskienhallintajärjestelmän kokonaisuuden hahmottamisessa. Käytän viitekehystä myös aineiston analyysin apuna havaintojen luokittelussa.

On tärkeää kuitenkin huomioida, että NIST:in viitekehys on tarkoitettu kriittisen infrastruktuurin kokonaisvaltaisen kyberturvallisuuden parantamiseen, eikä siinä keskitytä niinkään henkilötietojen turvallisuuteen, kun taas GDPR:n lähtökohtana on henkilötietojen turvallisuus. Uskon kuitenkin, että viitekehys on hyvin kokonaisvaltainen tietoturvallisuuden riskienhallintamalli ja viitekehyksessä mainitaankin sen sopivan hyvin myös muille aloille ja yhteisöille (NIST, 2018, s. v-vi). Otan kuitenkin tämän viitekehyksen tueksi Iso-Britannian kyberturvallisuuskeskuksen (NCSC) ja Iso-Britannian tietosuojavaltuutetun toimiston (ICO) julkaiseman ohjeistuksen henkilötietojen käsittelyn turvallisuudesta ja asianmukaisista suojatoimista (NCSC & ICO, 2018).

NIST:in viitekehyksessä mainitaan sen olevan riskiperusteinen lähestymistapa kyberturvallisuuden riskien hallintaan (NIST, 2018, s. 3). Viitekehyksen voidaan siis nähdä olevan lähestymistavaltaan yhteneväinen GDPR:n riskiperusteiseen lähestymiseen henkilötietojen turvallisuuteen. NIST:in viitekehyksessä esitellään viisi ydintoimintaa, joiden avulla järjestellään kyberturvallisuusaktiviteetit korkeimmalla tasolla (NIST, 2018, s. 6). Niiden tarkoitus on myös auttaa organisaatioita muun muassa mahdollistamalla riskienhallintaan liittyvää päätöksentekoa, uhkien käsittelyssä ja toiminnan kehittämistä aiempien toimien oppimisen avulla (NIST, 2018, s. 6). Jokainen ydintoiminto on vielä jaettu edelleen kategorioihin perustuen kyberturvallisuuteen liittyviin lopputulemiin ja niihin liittyviin aktiviteetteihin (NIST, 2018, s. 7).

Nämä viisi ydintoimintaa ovat tunnistaminen, suojaaminen, havaitseminen, vastaaminen ja palautuminen. Tunnistamisella tarkoitetaan toimia, joiden tarkoituksena on kehittää organisatorista ymmärrystä kyberturvallisuusriskien

hallintaan liittyen esimerkiksi järjestelmiin, ihmisiin ja tietoon. Suojaamisella tarkoitetaan asianmukaisten suojatoimenpiteiden kehittämistä ja käyttöönottoa tarkoituksena varmistaa kriittisten palveluiden toimittaminen. Havaitsemisella puolestaan tarkoitetaan kyberturvallisuustapahtumien havainnointiin tarkoitettujen asianmukaisten toimien kehittämistä ja käyttöönottoa. (NIST, 2018, s. 6, 7.)

Vastaamisen toiminnot sisältävät sellaisten toimenpiteiden kehittämistä ja käyttöönottoa, joilla halutaan toimia kyberturvallisuushäiriön suhteen. Palautumisella tarkoitetaan puolestaan sellaisten toimenpiteiden kehittämistä ja käyttöönottoa, joilla ylläpidetään toipumiskyvyn suunnitelmia sekä sellaisten kykyjen ja palveluiden palauttamista toimintaan, joiden toiminta on heikentynyt kyberturvahäiriön vuoksi (NIST, 2018, s. 8).

Iso-Britannian kansallinen kyberturvallisuuskeskus (NCSC) on julkaissut yhteistyössä Iso-Britannian tietosuojavaltuutetun toimiston (ICO) kanssa ohjeistuksen koskien asianmukaisia teknisiä ja organisatorisia toimenpiteitä GDPR:n vaatimusten mukaisesti (NCSC & ICO, 2018). NCSC ja ICO (2018) huomauttaa, että GDPR:n vaatimukset asianmukaisista toimenpiteistä, ottaen huomioon riskit, viimeisin tekniikka, kustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitus kuvastaa GDPR:n riskiperusteista lähestymistapaa sekä sitä, että ei ole yhtä tiettyä ratkaisua, joka sopisi kaikille (NCSC & ICO, 2018).

Heidän ohjeistuksensa esittelee turvallisuuden lopputuloksia, jotka voivat mahdollisesti muodostaa pohjan asianmukaisten teknisten ja organisatoristen toimenpiteiden kuvailulle ja määrittelyille (NCSC & ICO, 2018). He myös huomauttavat, että vaikkakin nämä ovat minimivaatimuksia, täytyy ottaa huomioon, että tarkemmassa toteuttamisessa suojatoimenpiteiden on vastattava riskejä. Tuloksiin perustuvassa lähestymistavassa lopputulokset pysyvät vakioina ja se, miten näiden toteuttaminen tapahtuu voi vaihdella. Tämä mahdollistaa skaalaamisen minkä kokoiseen yritykseen tai monimutkaiseen henkilötietojen käsittelyyn tahansa. (NCSC & ICO, 2018.)

NCSC ja ICO (2018) esittelevät neljä henkilötietojenkäsittelyn turvallisuuden lopputulemaa, joilla tavoitellaan asianmukaisia teknisiä ja organisatorisia suojatoimenpiteitä. Nämä neljä lopputulemaa ovat turvallisuusriskien hallinta, henkilötietojen suojaaminen kyberhyökkäyksiltä, turvallisuustapahtumien havaitseminen ja haittavaikutuksien minimointi (NCSC & ICO, 2018).

Kategorioissa on samankaltaisuuksia edellä mainitun NIST:in kyberturvallisuuden viitekehyksen kanssa. Toki täytyy ottaa huomioon, että NIST:in viitekehys on tehty kriittisen infrastruktuurin kyberturvallisuuteen tarkoittaen, että sen keskeisimpänä asiana ei ole henkilötietojen suojaaminen, toisin kuin NCSC:n mallissa. Näiden kahden mallin pohjalta olen hahmottanut asianmukaisten organisatoristen ja teknisten suojatoimenpiteiden viitekehyksen, joka kattaa kokonaisvaltaiseen henkilötietojen riskienhallintaan liittyviä ominaisuuksia ja ulottuvuuksia. Viitekehykseen kuuluu neljä päätoimintoa: tunnistaminen, suojaaminen, havaitseminen sekä vastaaminen ja palautuminen. Jokaiseen päätoimintoon sisältyy alakategorioita, jotka vielä luokittelevat päätoimintoon liittyviä organisatorisia ja teknisiä toimenpiteitä yhteen alakategorioiksi. Viitekehys on nähtävissä kokonaan alempana kuviossa 2.

5.1.1 Riskienhallinnan viitekehyksen alakategoriat

Edellä mainittiin viitekehyksen neljä päätoimintoa, joita olivat tunnistaminen, suojaaminen, havaitseminen sekä vastaaminen ja palautuminen. Tunnistamisen päätoimintoon kuuluu alakategoriat hallinto, henkilötietojen riskienhallinta, henkilötietojen käsittelijöiden ja toimitusketjun riskienhallinta sekä turvattavien kohteiden hallinta. Hallintoon kuuluu toimenpiteitä, kuten politiikat ja prosessit, joilla hallinnoidaan ja monitoroidaan organisaation lainmukaisia, riskinmukaisia ja operatiivisia vaatimuksia sekä tiedotetaan johtoportaalle tietoturvariskeistä (NIST, 2018, s. 25, 26).

Henkilötietojen riskienhallinnalla tarkoitetaan riskienhallintaan liittyviä toimia, joilla pyritään tunnistamaan, arvioimaan ja ymmärtämään turvallisuusriskejä liittyen henkilötietoihin ja henkilötietoja käsitteleviin järjestelmiin (NCSC & ICO, 2018). Henkilötietojen käsittelijöiden ja toimitusketjun riskienhallintaa kuuluu sellaisten prosessien luominen ja käyttöönotto, joilla pyritään tunnistamaan, arvioimaan ja hallitsemaan riskejä liittyen toimitusketjuun ja henkilötietojen käsittelijöihin (NIST, 2018, s. 28; NCSC & ICO, 2018). Turvattavien kohteiden hallinnalla tarkoitetaan puolestaan toimia, joilla pyritään ymmärtämään ja luetteloimaan käsiteltävä henkilötieto, käsittelyn tarkoitukset sekä riskit, joita henkilöille voi aiheutua henkilötietojen luvattomasta tai laittomasta käsittelystä tai vahingossa tapahtuvan tuhoutumisen seurauksena (NCSC & ICO, 2018).

Suojaamisen päätoimintoon liittyviä alakategorioita ovat identiteetin- ja pääsynhallinta, henkilökunnan tietoisuus ja koulutus, palveluiden sekä henkilötiedon suojaamisen politiikat ja prosessit sekä henkilötietojen ja järjestelmien turvaaminen. Identiteetin- ja pääsynhallinnalla tarkoitetaan sitä, että pääsy henkilötietoihin ja järjestelmiin, jotka käsittelevät henkilötietoja on ymmärrettyä, dokumentoitua ja hallittua (NCSC & ICO, 2018). Tarkemmin tavoitteena on, että pääsy tietoihin on rajoitettu valtuutettuihin käyttäjiin ja sitä hallitaan luvattomaan käyttöön liittyvien ja arvioitujen riskien mukaisesti (NIST, 2018, s. 29).

Henkilökunnan tietoisuuden ja koulutuksen tarkoituksena on tukea henkilöstöä käsittelemään henkilötietoja turvallisesti (NCSC & ICO, 2018). Tämän saavuttamiseksi täytyy tarjota henkilöstölle koulutusta, joka harjoittaa henkilöstön suorittamaan tehtävänsä politiikkojen, menettelyjen ja sopimusten mukaisesti (NIST, 2018, s. 31).

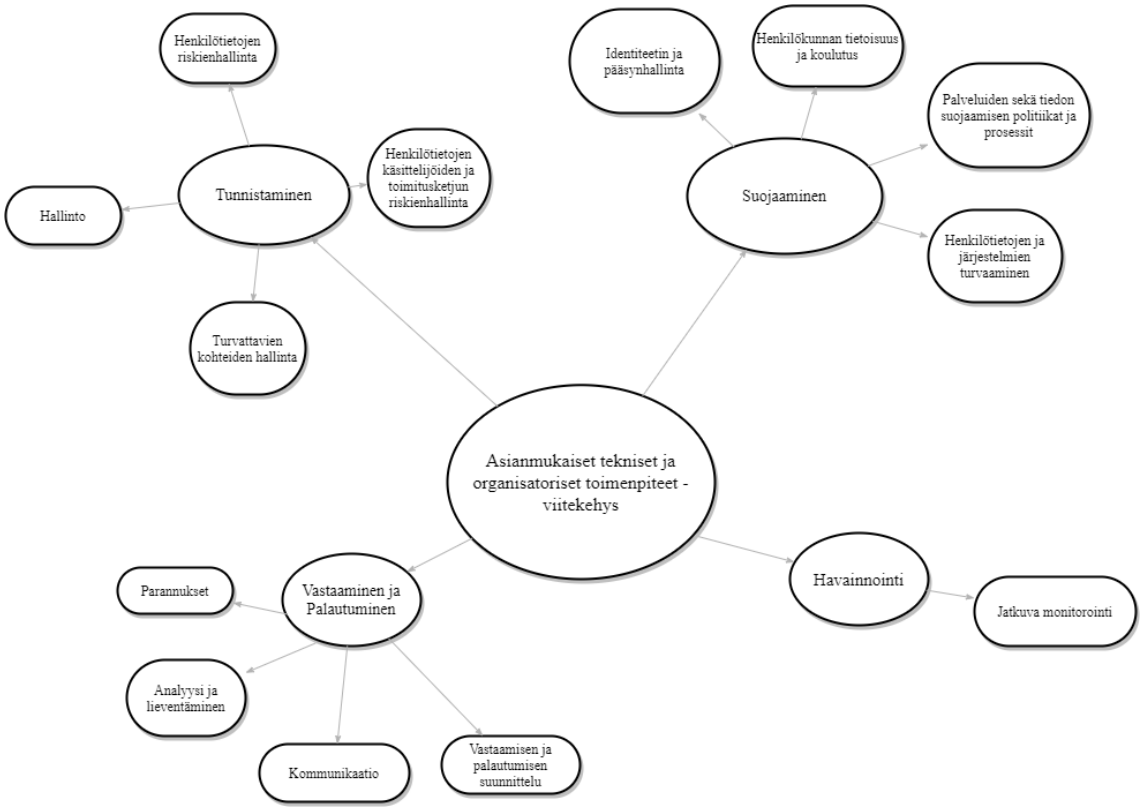
Palveluiden sekä henkilötiedon suojaamisen politiikat ja prosessit sisältävät toimenpiteitä, kuten politiikkojen ja prosessien määrittelemistä, käyttöönottoa ja valvomista, jotka ohjaavat lähestymistapaa henkilötietojen käsittelyyn liittyvien järjestelmien turvaamiseen (NCSC & ICO, 2018). Prosesseilla viitataan joukkoon toimintaperiaatteita tai tietoturvatomintoja, joilla järjestelmät tehdään turvallisiksi (Siponen, 2006, s. 97). Tietosuojan yhteydessä prosesseilla voidaan nähdä viitattavan joukkoon toimintaperiaatteita ja tietoturvatoimintoja, joiden tavoitteena on henkilötietojen käsittelyn tekeminen turvalliseksi. Palveluiden sekä henkilötiedon suojaamisen politiikasta esimerkkinä voisi olla tietoturvapolitiikka, joka velvoittaa työntekijöitä salaamaan arkaluontoisia henkilötietoja sisältävän dokumentin salasanalla.

Henkilötietojen ja järjestelmien turvaaminen käsittää toimet, joilla pyritään varmistamaan henkilötietojen hallinta organisaation riskistrategian mukaisesti turvatakseen tietojen luottamuksellisuuden, eheyden ja saatavuuden (NIST, 2018, s. 32) Tähän alakategoriaan liittyviä toimia voivat olla esimerkiksi tekniset toimenpiteet, joilla pyritään turvaamaan henkilötietojen käsittelyyn käytettävät järjestelmät ja teknologiat kyberhyökkäyksiltä (NCSC & ICO, 2018).

Havaitsemisen päätoimintoon kuuluu yksi alakategoria, joka on jatkuva monitorointi. Jatkuvalla monitoroinnilla tarkoitetaan toimenpiteitä ja ratkaisuita, joilla halutaan valvoa henkilötietoja käsittelevien järjestelmien tilaa, varmistaa käytössä olevien suojatoimenpiteiden tehokkuus sekä tunnistaa poikkeava toiminnallisuus (NCSC & ICO, 2018 ; NIST, 2018, s. 38, 39).

Vastaamiseen ja palautumiseen kuuluu alakategoriat vastaamisen ja palautumisen suunnittelu, kommunikaatio, analyysi ja lieventäminen sekä parannukset. Vastaamisen ja palautumisen suunnittelulla halutaan varmistaa, että tietoturvahäiriöiden vastaamisen ja palautumisen menettelyjä toteutetaan ja ylläpidetään (NIST, 2018, s. 41). Vastaamisen ja palautumisen toimenpiteiden yhtenä tarkoituksena on rajoittaa henkilötietojen määrää, jotka voivat vaarantua tietovuodossa (NCSC & ICO, 2018). Kommunikaatiolla tarkoitetaan palautumistoimien koordinointia tietoturvaloukkauksen jälkeen sisäisten ja ulkoisten osapuolten kanssa (NIST, 2018, s. 44). GDPR:n yhteydessä on myös tärkeää huomioida se, että rikkomuksesta tilanteesta riippuen täytyy myös ilmoittaa rikkomuksesta tietosuojavaltuutetulle ja henkilöille, joita asia koskee (NCSC & ICO, 2018).

Analyysi ja lieventäminen puolestaan sisältää toimenpiteitä, joilla halutaan varmistaa reagoinnin tehokkuus, tapahtuman laajenemisen estäminen ja sen ratkaiseminen (NIST, 2018, s. 42). Parannuksilla puolestaan tarkoitetaan toimenpiteitä, joilla pyritään siihen, että palautumiseen ja vastaamiseen sisältyviä toimenpiteitä ja prosesseja parannetaan sisällyttämällä aikaisemmista tapauksista opitut asiat tulevaan toimintaan (NIST, 2018, s. 43). Asianmukaisiin teknisiin ja organisatorisiin toimenpiteisiin liittyvä viitekehys on kokonaisuudessaan nähtävissä alempana (kuvio 2).



KUVIO 2 Asianmukaiset tekniset ja organisatoriset toimenpiteet -viitekehys (pohjautuen NIST, 2018, NCSC & ICO, 2018)

Näiden päätoimintojen ja alakategorioiden pohjalta luokittelen aineistosta nousevia havaintoja asianmukaisista organisatorisista ja teknisistä toimenpiteistä ennalta määriteltyihin luokkiin. Tutkimuksessa analysoidaan viranomaisten antamia sakkopäätöksiä GDPR:n artiklan 32 rikkomisesta, ja pyritään viitekehyksen pohjalta tehdyn luokittelun avulla aineistoa analysoimalla saamaan lisää tietoa liittyen siihen, mitä asianmukaiset tekniset ja organisatoriset toimenpiteet käsitteenä kattavat alleen.

5.2 Aineiston esittely

Tutkimuksen aineistona toimii valvontaviranomaisten päätökset GDPR:n säännösten rikkomisesta. Valvontaviranomaisten päätökset GDPR:n säännösten rikkomisesta ovat koonneet verkkosivustolle enforcementtracker.com CMS Law.Tax niminen yritys. Käytin kyseistä verkkosivua aineiston etsimisessä. Tutkimuksen aineistoksi hain valvontaviranomaisten antamia sakkopäätöksiä, jotka ovat annettu artiklan 32 rikkomisesta. Sakkopäätökset ovat kirjoitettu monesti kyseisen maan ja valvontaviranomaisen virallisella kielellä, joten tämä osittain rajoitti aineiston mahdollista kokoa. Tutkimusta varten ei löytynyt virallisia käännöksiä suomeksi tai englanniksi muunkielisistä päätöksistä, joten

aineistoksi täytyi valita suomen- ja englannin kielellä kirjoitettuja sakkopäätöksiä. Näiden ehtojen perusteella valitsin seitsemän sakkopäätöstä tarkempaan analyysiin, joista kaikki ovat kirjoitettu englanniksi. Aineistoksi valituista sakkopäätöksistä viisi ovat Ison-Britannian valvontaviranomaisen määräämiä sakkoja GDPR:n rikkomisesta, joissa on rikottu artiklaa 32. Kaksi sakkopäätöksistä ovat Irlannin valvontaviranomaisen antamia. Suomessa ei ole annettu tutkimuksen kirjoittamisen ajankohdassa yhtään sakkoa artiklan 32 rikkomisesta.

Aineistosta kaksi sakkoihin johtanutta rikettä liittyivät fyysisten henkilötietoja sisältävien dokumenttien artiklan 32 vaatimusten vastaiseen henkilötietojen käsittelyyn. Lopuissa neljässä sakkoihin johtaneet rikkeet olivat pääasiassa digitaalisessa muodossa olevan henkilötietojen vaatimusten vastaiseen henkilötietojen suojaamiseen liittyviä ongelmakohtia.

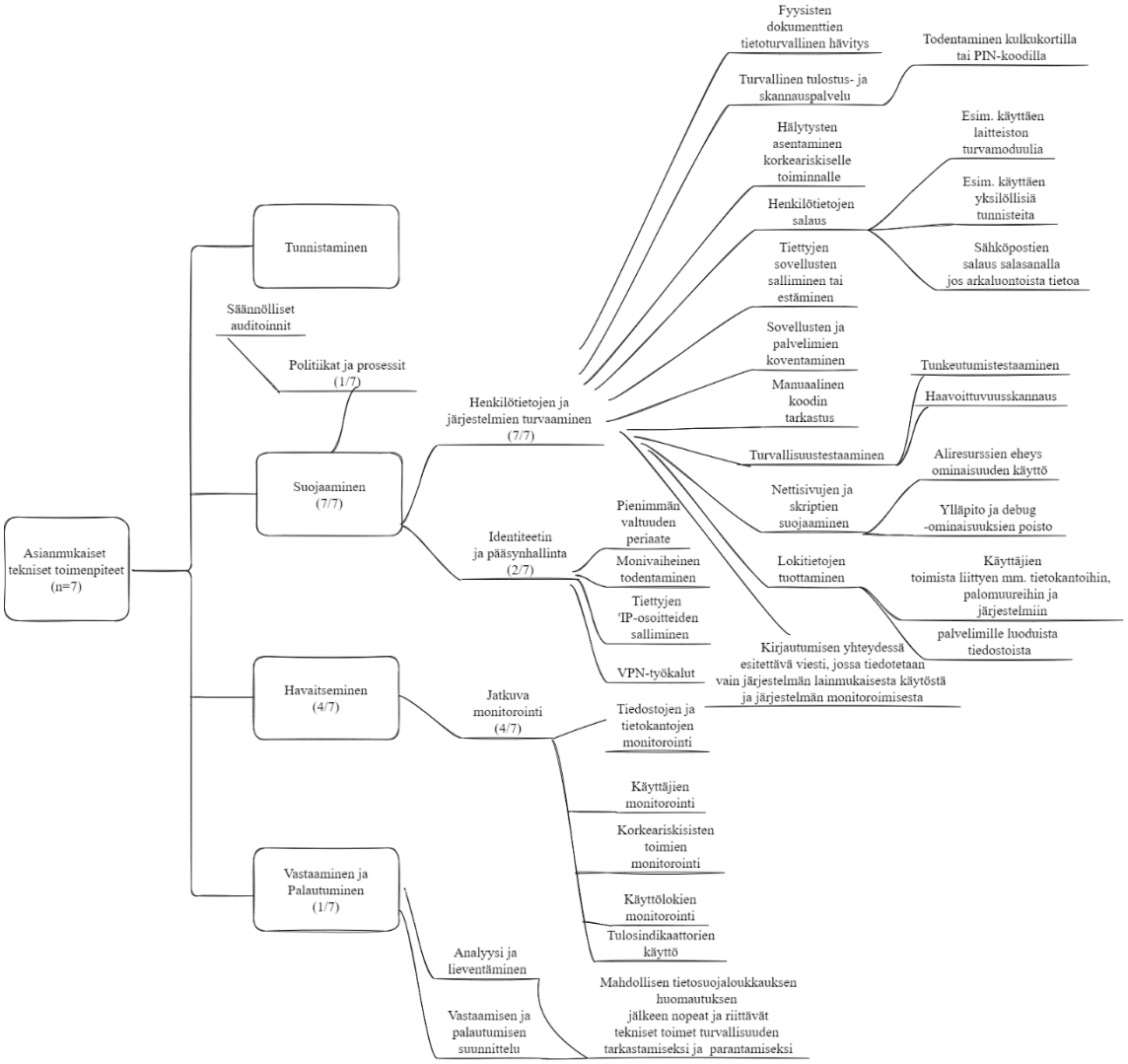
Aineistosta on tärkeää mainita, että jokaisessa sakkopäätökseen johtaneessa tapauksessa henkilötietojen käsittelyyn liittyvä riski on ollut vähintään keskitasoa. Suurimmassa osassa riski on ollut korkea. Tämä korkea riski on johtunut tapauksissa pääasiallisesti siitä, että kyseisissä rikkeissä, jotka ovat johtaneet hallinnolliseen sakkoon on ollut hyvin arkaluontoista tietoa GDPR:n vaatimusten vastaisesti suojattuna. Toisena syynä korkeaan riskiin aineiston tapauksissa on ollut käsittelyn laajuus eli todella suuri määrä henkilötietoja on käsitelty vasten GDPR:n säännöksiä. Tämä on tärkeää huomioida, sillä sakkopäätöksien analyysin pohjalta nousevat tulokset voidaan täten ajatella vastaavan keskitason ja korkean riskitason asianmukaisia toimenpiteitä.

6 ANALYYSI

Tässä luvussa käydään läpi aineistosta nousseet tulokset, niiden tulkinta ja pohdinta. Kuten aikaisemmin tutkimuksessa alaluvussa 3.4 mainittiin, artiklan 32 vaatimusten ymmärtämisen ja noudattamisen avulla voidaan tukea myös luottamuksellisuuden ja eheyden periaatteen noudattamista. Tutkimuksen tuloksista voi täten olla myös hyötyä artiklan 5 noudattamisen kannalta.

6.1 Asianmukaiset tekniset toimenpiteet

Asianmukaisiin teknisiin toimenpiteisiin aineistosta löytyi havaintoja kolmeen päätoimintoon liittyen. Suurin määrä havaintoja liittyen asianmukaisiin teknisiin toimenpiteisiin löytyi suojaamisen päätoimintoon. Havaitsemisen päätoimintoon liittyen löytyi havaintoja neljästä sakkopäätöksestä. Vastaamisen ja palautumisen päätoimintoon löytyi havaintoja yhdestä sakkopäätöksestä. Teknisistä toimenpiteistä ei löytynyt aineistosta havaintoja liittyen tunnistamiseen. Tämä selittyy vahvasti sillä, että toimenpiteet liittyen tunnistamiseen voidaan nähdä koostuvan pääasiallisesti organisatorisista toimenpiteistä. Tunnistamisen päätarkoituksena onkin kehittää organisaatiollista ymmärrystä tietoturvariskien hallintaan liittyen muun muassa järjestelmiin, ihmisiin ja tietoon (NIST, 2018, s. 7). Analyysin avulla nousseet tulokset teknisistä toimenpiteistä ovat kokonaisuudessaan nähtävissä alla olevassa kuviossa (Kuvio 3).



KUVIO 3 Analyysin tulokset asianmukaisista teknisistä toimenpiteistä

6.1.1 Suojaaminen

Suojaamisen päätoimintoon liittyen löytyi vähintään yksi havainto asianmukaisista teknisistä toimenpiteistä jokaisesta seitsemästä sakkopäätöksestä. Eniten havaintoja suojaamiseen liittyen nousi esille henkilötietojen ja järjestelmien turvaamisen alakategoriaan. Tähän alakategoriaan löytyi jokaisesta seitsemästä sakkopäätöksestä kuvauksia hyvistä ja huonoista teknisistä toimenpiteistä, jotka vaikuttavat siihen ovatko henkilötiedot ja henkilötietojen käsittely suojattu artiklan 32 vaatimilla asianmukaisilla teknisillä toimenpiteillä.

Henkilötietojen ja järjestelmien turvaamiseen löytyi hyvin monenlaisia teknisiä toimenpiteitä, joita aineistossa kuvailtiin asianmukaisiksi GDPR:n artiklan 32 vaatimuksia ajatellen. Aineistosta nousseita asianmukaisia teknisiä toimenpiteitä liittyen suojaamiseen ja tarkemmin henkilötietojen ja järjestelmien turvaamiseen olivat muun muassa sovellusten määrittäminen ja listaaminen sallittujen ja estettyjen sovellusten listoille (engl. whitelisting ja blacklisting). Tämä

sallittujen sovellusten listaaminen asianmukaisena teknisenä toimenpiteenä nousi kahdessa sakkopäätöksessä esiin, joten kyseistä toimenpidettä voidaan pitää tärkeänä asianmukaisena teknisenä toimenpiteenä.

Lisäksi kahdessa sakkopäätöksessä nostettiin esille, että tietokantojen, verkon, pääsynhallinnan ja sovellusten lokitietojen kerääminen, tarkastelu sekä hälytysten asentaminen korkeariskiselle toiminnalle on tärkeää asianmukaiselle henkilötietojen suojaamiselle. Muita aineistosta nousseita tärkeänä pidettyjä teknisiä toimenpiteitä liittyen henkilötietojen ja järjestelmien turvaamisen alatoimintoon ovat turvallisuustestaaminen, ja testaamisesta mahdollisesti nousseiden havaittujen turvallisuusriskien lieventäminen. Esimerkkinä tästä aineistosta nousi esille kolmannen osapuolen tarjoaman skriptin turvallisuustestaaminen yrityksen omilla nettisivuilla ja siihen liittyvien riskien lieventäminen. Asianmukaisena teknisenä toimenpiteenä henkilötietojen ja järjestelmien turvaamiseen nousi aineiston perusteella myös muun muassa turvallinen tulostus- ja skannauspalvelu, henkilötietojen salaus sekä sovellusten ja palvelimien koventaminen. Tärkeänä asianmukaisena teknisenä toimenpiteenä tulostus- ja skannauspalveluihin oli palveluita käyttääkseen todentaminen PIN-koodilla tai kulkukortilla. Lisäksi henkilötietojen ja järjestelmien turvaamiseen liittyen yhdessä sakkopäätöksessä esitettiin asianmukaisena teknisenä toimenpiteenä kirjautumisen yhteydessä esitettävä viesti käyttäjälle, jossa tiedotetaan, että järjestelmää saa käyttää vain lainmukaiseen tarkoitukseen ja järjestelmän käyttöä monitoroidaan.

Toinen alakategoria, johon löytyi sakkopäätöksistä havaintoja liittyen suojaamisen päätoimintoon, on identiteetin- ja pääsynhallinta. Identiteetin- ja pääsynhallintaan liittyviä asianmukaisia teknisiä toimenpiteitä, joita aineistossa esiintyi ovat pienimmän valtuuden periaate (engl. least privilege), monivaiheinen todentaminen, VPN työkalu etäyhteyden muodostamiseen ja sallittujen IP-osoitteiden listaaminen (engl. IP-whitelisting). Näitä teknisiä toimenpiteitä voidaan pitää tärkeinä artiklan 32 vaatimusten kannalta.

Pienimmän valtuuden periaatteella tarkoitetaan toimintaperiaatetta ja toiminnallisuutta, jonka mukaan käyttäjälle tulisi määrittää pääsy ainoistaan sellaisiin resursseihin, joita tarvitaan käsillä olevan tehtävän suorittamiseen. Eli esimerkiksi tietojärjestelmän tulisi pystyä määrittämään pienimmät valtuudet, joita käyttäjä tarvitsee tietyn tehtävän suorittamiseen, ja myöntää käyttäjälle ainoastaan nämä valtuudet eikä enempää valtuuksia. (Chen & Crampton, 2007, s. 157.)

Aineistossa määritellään monivaiheisen todentamisen tarkoittavan järjestelmää, joka rajoittaa pääsyn järjestelmiin sellaisille käyttäjille, jotka voivat suorittaa kahden tai useamman vaiheen yhdistelmän todentamista varten. Monivaiheisesta todentamisesta esimerkkinä voidaan pitää vaikkapa salasanan lisäksi mobiililaitteeseen saapuvan koodin käyttöä todentamiseen. Näiden teknisten toimenpiteiden lisäksi yhdessä sakkopäätöksessä mainittiin säännölliset auditoinnit asianmukaisena toimenpiteenä, joka puolestaan kuuluu palveluiden sekä tiedon suojaamisen politiikat ja prosessit alakategoriaan.

6.1.2 Havaitseminen

Toisena päätoimintona, johon liittyen löytyi paljon havaintoja asianmukaisista teknisistä toimenpiteistä, on havaitseminen. Havaitsemiseen kuuluu yksi alakategoria, joka on jatkuva monitorointi. Jatkuva monitorointi nousi hyvin merkittävänä teknisenä toimenpiteenä esille, ja siihen liittyviä havaintoja nousi neljästä sakkopäätöksestä. Tärkeänä jatkuvaan monitorointiin liittyvänä asianmukaisena teknisenä toimenpiteenä nousi aineistosta esiin käyttäjien, ja erityisesti korotettujen käyttöoikeuksien omaavien käyttäjien toiminnan monitorointi. Korkeiden käyttöoikeuksien omaavien käyttäjien lokitietojen kerääminen ja monitorointi nostetaan esille myös ENISA:n julkaisussa keskitason riskiä vastaavaksi asianmukaiseksi tekniseksi toimenpiteeksi (ENISA, 2016, s. 40). Tämä on yhteneväinen tulos analyysin pohjalta nousseiden havaintojen perusteella. Kyseistä toimenpidettä voidaan pitää tärkeänä artiklan 32 noudattamista ajatellen.

Muita tärkeitä jatkuvaan monitorointiin liittyviä asianmukaisia teknisiä toimenpiteitä, joita nousi aineistosta esiin ovat tietokantoihin, järjestelmiin pääsyn, tiedostoihin ja kirjautumisyrityksiin liittyvän toiminnan monitorointi. Aineistosta myös ilmeni, että monitoroinnin tavoitteena on pyrkiä valvomaan mahdollisia tavanomaisesta toiminnasta poikkeavaa toimintaa ja se kuuluu osana asianmukaista henkilötietojen suojaamista. Työkaluista liittyen monitorointiin mainittiin yhdessä sakkopäätöksessä, jossa mainittiin, että lokitietojen kerääminen ja monitorointi voi tapahtua esimerkiksi SIEM-järjestelmää tai manuaalisia hakuja käyttäen. Jatkuvaa monitorointia liittyen edellä mainittuihin toimintoihin voidaan pitää aineiston pohjalta tärkeänä noudattaakseen artiklan 32 asianmukaisten teknisten toimenpiteiden vaatimusta.

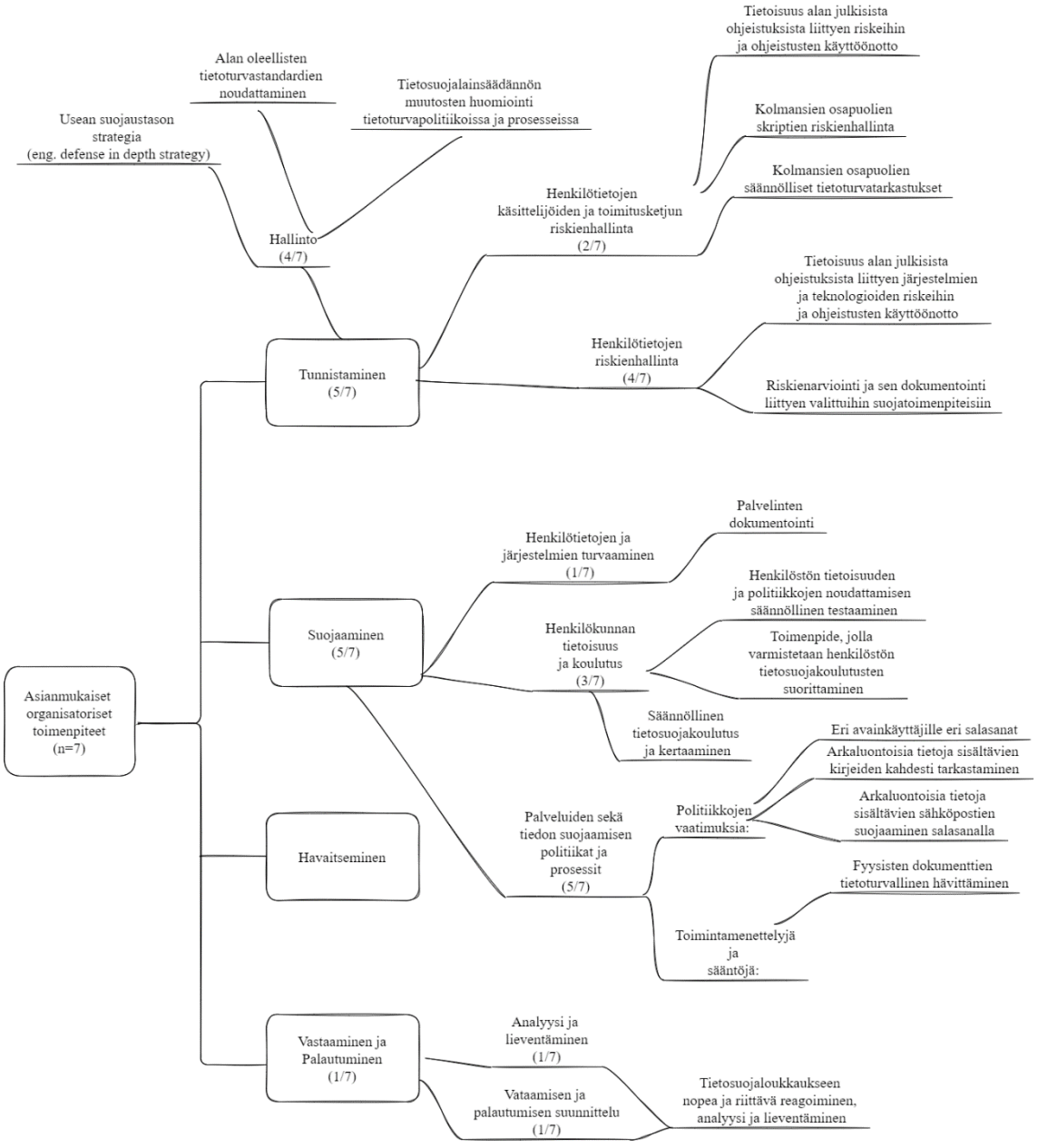
6.1.3 Vastaaminen ja palautuminen

Vastaamiseen ja palautumiseen liittyviä asianmukaisia teknisiä toimenpiteitä löytyi kahdesta sakkopäätöksestä. Tähän päätoimintoon liittyvistä teknisistä toimenpiteistä nousi esiin havaintoja analyysin ja lieventämisen sekä vastaamisen ja palautumisen suunnittelun alakategorioihin liittyviä toimenpiteitä. Aineistossa korostettiin nopeita ja riittäviä toimenpiteitä tietoturvaloukkauksen huomautuksen seurauksena turvallisuuden tarkastamiseksi ja parantamiseksi. Esimerkkinä aineistossa esiintynyt tapaus, jossa organisaatio ei reagoinut ilmoitukseen mahdollisesta tietosuojahäiriöstä yli kuukauteen, jonka valvontaviranomainen tulkitsi liian hitaaksi reagoimiseksi, ja GDPR:n vaatimusten vastaiseksi toiminnaksi.

6.2 Asianmukaiset organisatoriset toimenpiteet

Asianmukaisiin organisatorisiin toimenpiteisiin aineistosta löytyi havaintoja kolmeen päätoimintoon liittyen. Organisatorisista toimenpiteistä analyysin pohjalta

suurin määrä havaintoja aineistosta nousi esiin tunnistamisen ja suojaamisen päätoimintoihin liittyen. Tunnistamisen ja suojaamisen päätoimintoihin liittyen löysin havaintoja viidestä eri sakkopäätöksestä. Vastaamiseen ja palautumiseen löysin havaintoja yhdestä sakkopäätöksestä ja havaitsemisen päätoimintoon liittyen en löytänyt ollenkaan havaintoja asianmukaisista organisatorisista toimenpiteistä. Aineiston analyysin tulokset asianmukaisista organisatorisista toimenpiteistä ovat kokonaisuudessaan nähtävissä alla olevassa kuviossa (Kuvio 4).



KUVIO 4 Analyysin tulokset asianmukaisista organisatorisista toimenpiteistä

6.2.1 Tunnistaminen

Tunnistamisen päätoimintoon liittyviä asianmukaisia organisatorisia toimenpiteitä havaitsin viidestä eri sakkopäätöksestä. Alakategoriat liittyen tunnistamisen päätoimintoon, joihin löytyi paljon havaintoja ovat hallinto ja henkilötietojen riskienhallinta. Hallintoon liittyviä asianmukaisia organisatorisia toimenpiteitä, joita aineistosta nousi esille ovat usean suojaustason strategia (engl. defense in depth strategy), alan oleellisten tietoturvastandardien noudattaminen (esim. PCI-DSS) sekä tietosuojalainsäädännön muutosten huomiointi tietoturvapolitiikoissa ja prosesseissa.

Tärkeitä henkilötietojen riskienhallintaan liittyviä asianmukaisia organisatorisia toimenpiteitä, joita aineistosta nousi esiin ovat tietoisuus alan julkisista ohjeistuksista liittyen järjestelmien ja teknologioiden riskeihin ja näiden ohjeistusten käyttöönotto. Kolmessa sakkopäätöksessä korostettiin, että alalla oli sakon antamisen aikaan hyvin yleisessä tiedossa, minkälaisia riskejä kohdistui kyseisen organisaation henkilötietojen käsittelyyn liittyviin järjestelmiin sekä sovelluksiin. Tämän lisäksi korostettiin, kuinka alalla on ollut jo pidemmän aikaa yleisessä tiedossa ohjeistuksia, kuinka ottaa käyttöön asianmukaisia suojatoimenpiteitä näitä yleisessä tiedossa olevia riskejä vastaan. Aineistossa viitattiin aikaisempiin julkaisuihin liittyen riskeihin ja ohjeistuksiin riskejä lieventävien toimenpiteiden käyttöönottoon. Aineistossa viitattuja lähteitä olivat muun muassa NIST, ENISA ja verkkosivusto stackoverflow.com. Aineistossa viitattiin esimerkiksi tiedossa oleviin riskeihin liittyen korkean käyttöoikeuden käyttäjiin, järjestelmiin ja sovelluksiin. Tietoisuutta alan yleisessä tiedossa oleviin riskeihin ja ohjeistuksiin liittyen sekä näiden ohjeistuksen käyttöönottoa voidaan pitää merkittävänä organisatorisena toimenpiteenä artiklan 32 vaatimuksia ajatellen.

Henkilötietojen käsittelyyn liittyvien teknologioiden ja järjestelmien riskienarvioinnin tekemisen ja sen dokumentoinnin tärkeyttä korostettiin neljässä eri sakkopäätöksessä, joka kertoo riskienarvioinnin tärkeydestä artiklan 32 vaatimusten noudattamista ajatellen.

Asianmukaisista organisatorisista toimenpiteistä henkilötietojen käsittelijöiden ja toimitusketjun riskienhallintaan liittyen nousi aineistosta havaintoja kahdesta eri sakkopäätöksestä. Henkilötietojen käsittelijöiden ja toimitusketjun riskienhallintaan liittyviä tärkeitä asianmukaisia organisatorisia toimenpiteitä, joita aineistosta nousi ovat muun muassa tietoisuus alan julkisista ohjeistuksista liittyen henkilötietojen käsittelijöiden ja toimitusketjun riskeihin ja näiden ohjeistusten käyttöönotto. Tästä yhtenä konkreettisena esimerkkinä aineistossa esiintyi kolmansien osapuolien nettisivuille tarjoamien JavaScript-skriptien riskienhallinta.

6.2.2 Suojaaminen

Toinen päätoiminto, johon liittyen aineistosta nousi paljon havaintoja asianmukaisista organisatorisista toimenpiteistä, on suojaaminen. Suojaamiseen liittyviä asianmukaisia organisatorisia toimenpiteitä nousi viidestä eri sakkopäätöksestä.

Suurin määrä havaintoja suojaamiseen liittyvistä alakategorioista nousi aineistosta palveluiden sekä tiedon suojaamisen politiikkoihin ja prosesseihin liittyen. Aineistosta nousi tietoturvapolitiikkoihin liittyviä vaatimuksia, joiden voidaan aineiston perusteella nähdä olevan GDPR:n artiklan 32 vaatimusten mukaisia organisatorisia toimenpiteitä. Asianmukaisia organisatorisia toimenpiteitä liittyen palveluiden sekä tiedon suojaamisen politiikkoihin ja prosesseihin, joita aineistossa mainittiin, olivat muun muassa politiikka, joka velvoittaa käyttämään keskeisille käyttäjille (engl. key accounts) eri salasanoja ja vakiotoimintatavan määrittäminen henkilötietoja sisältävien paperidokumenttien tietoturvalliseen hävittämiseen. Analyysin tuloksena voidaan todeta, että artiklan 32 asianmukaisten organisatoristen toimenpiteiden piiriin kuuluu tärkeänä toimenpiteenä tietoturvapolitiikkojen määrittäminen ja noudattaminen.

Toinen suojaamiseen liittyvä alakategoria, joka nousi aineistosta esiin, on henkilökunnan tietoisuus ja koulutus. Havaintoja asianmukaisia organisatorisia toimenpiteistä liittyen henkilökunnan tietoisuuden ja koulutuksen alakategoriaan löytyi kolmesta sakkopäätöksestä. Tarkemmin aineiston pohjalta nousseita henkilökunnan tietoisuuteen ja koulutukseen liittyviä asianmukaisia toimenpiteitä ovat henkilökunnan henkilötietojen käsittelyn turvallisuuteen tietoisuuden ja politiikkojen noudattamisen säännöllinen testaaminen sekä perehdyttämisvaiheessa annettavat yksityiskohtaiset ohjeistukset sopimattomasta pääsystä ja käsittelystä liittyen henkilötietoihin. Aineistosta nousi myös yksi havainto organisatorisiin toimenpiteisiin henkilötietojen ja järjestelmien turvaamisen alakategoriaan liittyen. Tämä toimenpide on palvelinten dokumentointi, joka voidaan nähdä artiklan 32 vaatimustenmukaisena organisatorisena toimenpiteenä. Aineistossa määritellään, että palvelinten dokumentointi voi sisältää listan ohjelmistoista ja protokollista, joita sovellus vaatii toimiakseen. Analyysin pohjalta voidaan todeta, että henkilökunnan koulutus ja tietoisuuden säännöllinen testaaminen on merkittävä tekijä noudattaakseen GDPR:n artiklaa 32 ja asianmukaisten organisatoristen toimenpiteiden vaatimusta.

6.2.3 Vastaaminen ja palautuminen

Vastaamisen ja palautumisen päätoimintoon liittyviä asianmukaisia organisatorisia toimenpiteitä löytyi yhdestä sakkopäätöksestä. Asianmukaiset organisatoriset toimenpiteet koskien vastaamista ja palautumista liittyivät vastaamisen ja palautumisen suunnitteluun sekä analyysin ja lieventämisen -alakategorioihin. Asianmukaisena organisatorisena toimenpiteenä näihin alakategorioihin liittyen yhdessä sakkopäätöksessä korostettiin nopeaa ja riittävää reagoimista tietosuojaloukkaukseen sekä mahdolliseen tietosuojaloukkaukseen liittyviin ilmoituksiin nopeasti reagoimista.

Esimerkkinä sakkopäätöksessä yrityksen reagointi mahdolliseen tietosuojaloukkauksen ilmoitukseen kesti yli kuukauden ja tämän valvontaviranomainen tulkitsi liian hitaaksi ja GDPR:n vastaiseksi. Asianmukaisia organisatorisia toimenpiteitä liittyen vastaamiseen ja palautumiseen ovat tästä päätellen vastaamiseen ja palautumiseen liittyvien toimenpiteiden suunnittelu ja toteuttaminen,

joilla pyritään reagoida ilmoituksiin tietosuojahäiriöistä ja aloittaa vaadittavat toimenpiteet varmistaakseen onko häiriöstä tosiaan kyse.

6.3 Pohdinta

Tutkimusongelmana oli vastata seuraavaan tutkimuskysymykseen:

- Minkälaisia toimenpiteitä GDPR:n artiklan 32 asianmukaiset tekniset ja organisatoriset toimenpiteet käsitteinä kattavat alleen?

Tähän tutkimusongelmaan pyrittiin vastaamaan tutkimuksessa käsiteanalyysin avulla. Tutkimuksessa tutkittiin käsiteanalyysin avulla GDPR:n artiklan 32 asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteitä ja kartoitettiin niiden käyttöä sekä soveltamista. Tutkimuksen aineistona toimi valvontaviranomaisten sakkopäätökset, jotka olivat annettu artiklan 32 rikkomisesta.

Tutkimuksen analyysin pohjalta voidaan todeta, että asianmukaisten teknisten toimenpiteiden käsitteeseen ja vaatimuksiin sisältyy laaja kirjo teknisiä toimenpiteitä. Suurin määrä asianmukaisiin teknisiin toimenpiteisiin liittyvistä havainnoista liittyi suojaamisen päätoimintoon, ja tarkemmin henkilötietojen ja järjestelmien suojaamisen -alakategoriaan. Henkilötietojen ja järjestelmien suojaamiseen liittyviä olennaisia asianmukaisia teknisiä toimenpiteitä ovat muun muassa sovellusten palvelimien koventaminen ja turvallisuustestaaminen.

Tuloksena asianmukaisista teknisistä toimenpiteistä löytyi lisäksi identiteetin- ja pääsynhallinnan alakategoriaan liittyviä teknisiä toimenpiteitä, kuten monivaiheinen todentaminen, VPN-työkalut ja pienimmän valtuuden periaatteen noudattaminen. Monivaiheinen todentaminen mainitaan myös ENISA:n julkaisussa korkeaa riskiä vastaavana asianmukaisena suojatoimenpiteenä liittyen henkilötietojen käsittelyn turvallisuuteen (ENISA, 2016, s. 40). Tutkimuksen tuloksena asianmukaisista teknisistä toimenpiteistä merkittäväksi nousi suojaamisen lisäksi havaitsemisen päätoiminto ja jatkuvan monitoroinnin alakategoria. Tutkimuksen tuloksena voidaan todeta, että asianmukaisten teknisten toimenpiteiden käsitteeseen kuuluu tärkeänä ominaisuutena jatkuva monitorointi. Tarkemmin jatkuvaan monitorointiin liittyviä asianmukaisia teknisiä toimenpiteitä ovat muun muassa tiedostojen ja tietokantojen monitorointi sekä käyttölokien monitorointi.

Muita tärkeitä asianmukaisia teknisiä toimenpiteitä, joita tutkimuksen tuloksena nousi vastaamaan keskitason ja korkeantason riskeihin ovat toimenpiteet, kuten estettyjen ja sallittujen sovellusten listaaminen, monivaiheinen todentaminen ja korkeiden käyttöoikeuksien omaavien käyttäjien lokitietojen kerääminen ja monitorointi. Analyysin avulla löytyi paljon teknisiä toimenpiteitä, joita sisältyy asianmukaisten teknisten toimenpiteiden käsitteeseen GDPR:n ja henkilötietojen käsittelyn suojaamisen yhteydessä.

Tutkimuksen tuloksena suurin määrä havaintoja asianmukaisista organisatorisista toimenpiteistä löytyi tunnistamisen ja suojaamisen päätoimintoihin

liittyen. Alakategorioista asianmukaisiin organisatorisiin toimenpiteisiin nousi aineistosta määrällisesti eniten havaintoja hallintoon, henkilökunnan tietoisuuteen ja koulutukseen sekä palveluiden ja henkilötietojen suojaamisen politiikkoihin liittyen. Tutkimuksen tuloksena voidaan siis todeta asianmukaisten organisatoristen toimenpiteiden käsitteen kattavan alleen olennaisina ominaisuuksina hallintoon, henkilökunnan tietoisuuteen ja koulutukseen sekä henkilötietojen suojaamisen politiikkoihin liittyviä organisatorisia toimenpiteitä.

Lisäksi tutkimuksen tuloksena asianmukaisten organisatoristen toimenpiteiden käsitteeseen ja vaatimuksiin voidaan todeta sisältyvän toimenpiteitä, kuten tietoisuus alan yleisessä tiedossa olevista ohjeistuksista liittyen riskeihin ja näiden ohjeistuksien käyttöönotto sekä henkilökunnan henkilötietojen käsittelyn turvallisuuteen liittyvän tietoisuuden ja politiikkojen noudattamisen säännöllinen testaaminen.

Analyysin pohjalta nousseista tuloksista löytyi yhtäläisyyksiä liittyen ENISA:n (2016) julkaisemaan ohjeistukseen henkilötietojen käsittelyn turvallisuuteen sekä asianmukaisiin teknisiin ja organisatorisiin toimenpiteisiin. Analyysin pohjalta aineistosta asianmukaisena organisatorisena toimenpiteenä henkilötietojen käsittelijöiden ja toimitusketjun riskienhallintaan noussut säännölliset tietoturvatarkastukset mainitaan myös ENISA:n julkaisussa keskitason vastaavana asianmukaisena organisatorisena suojatoimenpiteenä (ENISA, 2016, s. 37). Tuloksena nousi myös esille asianmukaisena organisatorisena toimenpiteenä henkilökunnan säännöllinen tietosuojakoulutus ja kertaaminen. Tämä asianmukainen organisatorinen toimenpide mainitaan ENISA:n ohjeistuksessa keskitason riskiä vastaavana asianmukaisena organisatorinen toimenpiteenä (ENISA, 2016, s. 39).

Asianmukaisista teknisistä toimenpiteistä tutkimuksen tuloksena suurin määrä havaintoja löytyi suojaamisen päätoimintoon ja organisatorisista toimenpiteistä tunnistamisen ja suojaamisen päätoimintoon. Tutkimuksen tuloksena voidaan todeta, että asianmukaisten teknisten ja organisatoristen käsitteisiin sisältyy laaja kirjo toimenpiteitä liittyen riskienhallinnan eri päätoimintoihin, ja jokainen toimenpide tulee arvioida riskiä vastaavaksi.

6.4 Tutkimuksen luotettavuus

Aaltio ja Puusa (2020) määrittelevät, että laadullisessa tutkimuksessa luotettavuudella tarkoitetaan tutkimustulosten riippumattomuutta satunnaisista ja epäolennaisista tekijöistä (Aaltio & Puusa, 2020). He jatkavat, että luotettavaan ja hyvään tutkimuskäytäntöön kuuluu esittää perusteet, joiden mukaan tutkimusta voidaan pitää luotettavana (Aaltio & Puusa, 2020).

Tässä tutkimuksessa pyrittiin ymmärtämään paremmin GDPR:n artiklan 32 asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteitä ja niiden asettamia vaatimuksia henkilötietojen käsittelyn turvaamiseksi. Tutkimusmenetelmänä toimi käsiteanalyysi, jonka tarkoituksena on ymmärtää käsitteitä ja niiden kuvaamien ilmiöiden ominaisuuksia. Tutkimuksen aineistona toimi

valvontaviranomaisten antamat sakkopäätökset, joissa artiklan 32 vaatimuksia asianmukaisista toimenpiteistä on rikottu. Sakkopäätöksissä valvontaviranomaiset avaavat hyvinkin yksityiskohtaisesti sakkopäätöksen perusteita ja heidän tulkitsemiaan rikkeitä liittyen artiklan 32 vaatimuksiin. Aineiston voi nähdä soveltuvan hyvin vastaamaan tutkimusongelmaa ja vahvistaa tutkimuksen luotettavuutta.

Lisäksi Aaltio ja Puusa (2020) mainitsevat, että luotettavuutta tarkastellaan sen mukaisesti, millaisia laadullisia menetelmiä työssä on käytetty sekä luotettavuutta arvioitaessa tulee pohtia valittujen metodien soveltuvuutta tutkimuksen kohdeilmiöön ja tutkimuksen tavoitteisiin (Aaltio & Puusa, 2020). Tutkimuksen kohdeilmiönä oli artiklan 32 asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteiden ja vaatimusten tutkiminen. Tutkimus toteutettiin käyttämällä käsiteanalyysiä tutkimusmenetelmänä ja aineiston analyysin tukena käytettiin muokattua tietoturvan ja tietosuojan riskienhallinnan viitekehystä. Jaottelin itse asianmukaisia teknisiä ja organisatorisia toimenpiteitä muodostamani viitekehyksen eri päätoimintoihin ja alakategorioihin. Tässä luokittelussa voi olla puutoksia ja se voi heikentää tutkimuksen luotettavuutta. Osa toimenpiteistä voi kuulua eri näkemyksen mukaan eri luokkiin, tai koko viitekehyksen soveltuvuutta voidaan kyseenalaistaa.

Myös se, että aineistona oli valvontaviranomaisten antamat sakkopäätökset tarkoittavat, että aineistosta nousseet havainnot liittyen asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteisiin liittyvät ainoastaan artiklan 32 vaatimusten vastaiseen toimintaan. Tämä jättää näiden käsitteiden tarkastelun osittain vajavaiseksi, sillä aineistossa käsitteitä käsitellään ja kuvaillaan säännösten vastaisen toiminnan pohjalta. Sakkopäätöksissä ei juurikaan keskitytä esimerkiksi siihen, mitkä kaikki toimenpiteet sakkopäätöksen kohteena olevalla toimijalla ovat olleet vaatimustenmukaisia ja asianmukaisia. Aineisto koostui seitsemästä sakkopäätöksestä, joka on hyvin rajallinen määrä ja voi osaltaan vaikuttaa tutkimuksen luotettavuuteen heikentävästi. Tutkimusmenetelmää ajatellen luotettavuuteen voi vaikuttaa se, että tutkimuksen kohteena oli GDPR, eli kyseessä on oikeudellista tekstiä, joten oikeustieteelliset tutkimusmenetelmät mukaan otettuna voisi parantaa tutkimuksen luotettavuutta.

Tutkimusongelmana haluttiin ymmärtää paremmin asianmukaisten teknisten toimenpiteiden ja asianmukaisten organisatoristen toimenpiteiden käsitteitä. Uskon kuitenkin tutkimusmenetelmänä käytetyn käsiteanalyysin sekä analyysin tueksi muodostetun viitekehyksen tukevan tätä tavoitetta ja vahvistavan tutkimuksen luotettavuutta.

7 YHTEENVETO

Teknologinen kehitys ja tiedon arvon kasvaminen on vauhdittanut tietojenkäsittelyn siirtymistä digitaalisiin ympäristöihin. Tämä kehitys on mahdollistanut paljon uudenlaisia mahdollisuuksia organisaatioille, mutta se on samalla herättänyt paljon huolta näiden digitaalisissa ympäristöissä käsiteltävien tietojen – mukaan lukien henkilötietojen turvallisuudesta. Jatkuvasti kehittyvään henkilötietojen käsittelyn ilmiöön sekä sen turvallisuuteen on vastauksena kehitetty tietosuojalainsäädäntöä. EU:ssa on ollut vuosikymmenien ajan korkeat tietosuojalainsäädännön vaatimukset. Yksi suurimmista viimeaikaisista tavoitteista kohti yhteiskunnallisen ja teknologisen kehityksen mukana pysyvää tietosuojalainsäädäntöä on EU:n tasolla säädetty GDPR. GDPR astui voimaan vuonna 2016 ja sitä käytiin soveltamaan kahden vuoden siirtymäajan jälkeen 25. Toukokuuta 2018.

GDPR:n keskeisiä tavoitteita on tietosuojaa koskevan lainsäädännön ajantasaistaminen, yhdenmukaistaa tietosuojalainsäädäntöä EU:n alueella sekä suojella ihmisten perusoikeuksia kehittyvän teknologian tuomilta haasteilta. GDPR:ssä määritellään periaatteita, joita henkilötietojen käsittelyssä tulee noudattaa. Näitä periaatteita ovat käsittelyn lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, tietojen säilytyksen rajoittaminen, tietojen eheys ja luottamuksellisuus sekä rekisterinpitäjän osoitusvelvollisuus. Keskeisimmäksi periaatteeksi tässä tutkimuksessa nostettiin tietojen eheyden ja luottamuksellisuuden periaate, joka velvoittaa, että tiedot on suojattava asianmukaisesti muun muassa luvattomalta ja lainvastaiselta käsittelyltä. Tarkempia vaatimuksia henkilötietojen käsittelyn turvallisuuteen esitetään GDPR:n artiklassa 32, jota tässä tutkimuksessa tutkittiin.

Artikla 32 velvoittaa rekisterinpitäjiä ja henkilötietojen käsittelijöitä ottamaan huomioon muun muassa uusin tekniikka ja toteuttamiskustannukset ja toteuttamaan henkilöiden oikeuksiin ja vapauksiin kohdistuvia riskejä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Artiklassa 32 on omaksuttu riskipohjainen lähestymistapa, eli suojatoimet ovat suhteutettava henkilöiden oikeuksille ja vapauksille aiheutuvaan riskiin. Artikla 32 jättää kuitenkin pääasiallisesti rekisterinpitäjille ja henkilötietojen käsittelijöille itselleen määriteltäväksi, mitä riskiä vastaavat asianmukaiset organisatoriset ja tekniset toimenpiteet ovat. Tähän tutkimusongelmaan pyrin vastaamaan tällä tutkimuksella.

Tutkimusmenetelmänä toimi käsiteanalyysi ja kohdeilmiönä oli artiklan 32 asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteiden ja vaatimusten tutkiminen. Tutkimuksen tavoitteena oli ymmärtää paremmin artiklan 32 asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteitä ja ominaisuuksia. Tutkimuskysymys, johon tutkimuksella pyrittiin vastaamaan, kuului seuraavanlaisesti:

- Minkälaisia toimenpiteitä GDPR:n artiklan 32 asianmukaiset tekniset ja organisatoriset toimenpiteet käsitteinä kattavat alleen?

Pyrin tutkimuksella tuomaan lisää tietoa artiklan 32 asettamista vaatimuksista henkilötietojen käsittelyn turvallisuudelle sekä selvittämään, minkälaisia toimenpiteitä artiklassa 32 määritellyt asianmukaiset organisatoriset ja tekniset toimenpiteet mahdollisesti pitävät sisällään. Tähän tutkimusongelmaan pyrin vastaamaan tutkimuksessa analysoimalla tutkimukseen valittua aineistoa eli valvontaviranomaisten sakkopäätöksiä, joita on annettu artiklan 32 rikkomisesta.

Muodostin aineiston analyysin tueksi asianmukaisten organisatoristen ja teknisten toimenpiteiden viitekehyksen, joka pohjautui kahteen eri kokonaisvaltaiseen tietoturvan ja tietosuojan riskienhallinnan malliin. Tämän viitekehyksen tarkoituksena oli tukea aineistosta nousevien havaintojen systemaattista luokittelua ennalta määrättyihin kategorioihin, liittyen artiklan 32 vaatimuksiin toimenpiteiden tehokkuuden säännöllisestä arvioimisesta sekä palveluiden ja järjestelmien jatkuvan tietoturvallisuuden takaamisesta. Viitekehykseen kuuluu neljä päätoimintoa: tunnistaminen, suojaaminen, havaitseminen sekä vastaaminen ja palautuminen. Nämä päätoiminnot sisältävät alakategorioita, kuten vaikkapa suojaamisen päätoiminnon alakategoria identiteetin- ja pääsynhallinta.

Analyysin tuloksena löytyi suuri määrä havaintoja liittyen asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteisiin. Tärkeänä on ottaa huomioon se, että aineistona olevissa sakkopäätöksissä henkilötietojen käsittelyyn liittyvä riski on ollut vähintään keskitasoa, ja monissa tapauksissa korkea. Tämä johtui pääasiallisesti siitä, että aineiston tapauksissa käsiteltävä henkilötieto oli hyvin arkaluontoista tai käsittelyn kohteena oli suuri määrä henkilötietoja. Tämä tarkoittaa, että tutkimuksen analyysin pohjalta nousseista tuloksista moni toimenpide vastaa keskitason ja korkean tason riskejä liittyen henkilötietojen käsittelyn turvallisuuteen.

Asianmukaisista teknisistä toimenpiteistä löytyi eniten havaintoja liittyen suojaamisen päätoimintoon. Seuraavaksi eniten havaintoja asianmukaisista teknisistä toimenpiteistä löytyi havaitsemisen päätoimintoon liittyen. Tutkimuksen tuloksina nousi esille, että artiklan 32 asianmukaisten teknisten toimenpiteiden käsitteeseen ja vaatimuksiin kuuluu keskeisenä teknisiä toimenpiteitä, kuten hälytysten asentaminen järjestelmiin korkeariskiselle toiminnalle, lokitietojen tuottaminen ja korkeiden käyttöoikeuksien omaavien käyttäjien monitorointi.

Asianmukaisista organisatorisista toimenpiteistä analyysin tuloksina nousi eniten toimenpiteitä liittyen tunnistamisen ja suojaamisen päätoimintoihin. Tutkimuksen tuloksina nousi esille tärkeitä asianmukaisten organisatoristen toimenpiteiden käsitteeseen kuuluvia toimenpiteitä artiklan 32 vaatimuksiin liittyen, kuten tietoisuus alan yleisessä tiedossa ohjeistuksista liittyen riskeihin ja näiden ohjeistuksien käyttöönotto, henkilöstön koulutus, henkilöstön tietoisuuden ja politiikkojen noudattamisen säännöllinen testaaminen sekä toimenpide, jolla varmistetaan henkilöstön tietosuojakoulutusten suorittaminen. Kaikki havainnot liittyen asianmukaisiin teknisiin ja organisatorisiin toimenpiteisiin ovat nähtävissä luvussa 6.

Kuten aikaisemmin tutkimuksessa mainittiin, on GDPR:ään liittyvää tutkimusta hyvin niukasti olemassa. Tämän tutkimuksen tuloksista nousi kuitenkin esiin yhtäläisyyksiä liittyen aikaisempaan ENISA:n (2016) julkaisuun

henkilötietojen käsittelyn turvallisuudesta ja asianmukaisista toimenpiteistä. Näitä olivat muun muassa korotettujen käyttöoikeuksien omaavien käyttäjien toiminnan monitorointi keskitason riskiä vastaavana teknisenä toimenpiteenä sekä henkilökunnan säännöllinen tietosuojakoulutus ja kertaaminen. Tärkeänä on todeta myös se, että kuten tutkimuksessa tuli esille, on GDPR:ssä omaksuttu riskiperusteinen lähestymistapa, joka tarkoittaa, että ei ole yhtä tiettyä ratkaisua, joka sopisi kaikille ja osoittaisi artiklan 32 vaatimustenmukaisuuden, vaan toimenpiteiden täytyy vastata henkilötietojen käsittelyyn kohdistuvia riskejä.

Kaiken kaikkiaan tutkimuksen tulokset vastaavat tutkimuskysymykseen sekä tutkimuksen tavoitteisiin ymmärtää paremmin asianmukaisten teknisten ja organisatoristen toimenpiteiden käsitteitä ja niihin kuuluvia ominaisuuksia sekä ulottuvuuksia. Tutkimuksen tuloksina nousi monia konkreettisia teknisiä ja organisatorisia toimenpiteitä, joita nämä käsitteet kattavat alleen. Tutkimuksen tuloksista voi olla hyötyä GDPR:n vaatimustenmukaisuutta ajatellen kaikille asetuksen piiriin kuuluville organisaatioille.

Potentiaalisia hyödyttäviä jatkotutkimusaiheita, joita tutkimuksen pohjalta nousi esille, olisi tutkia artiklan 32 vaatimuksia isommalla aineistolla, jolloin voisi saada vielä kokonaisvaltaisemman ja yleistettävämmän tuloksen. Toinen jatkotutkimusaihe, joka tutkimuksen pohjalta heräsi, olisi tutkia minkälaisia haasteita suomalaiset organisaatiot –niin julkiset kuin yksityiset ovat kokeneet GDPR:ään liittyen, ja kuinka näitä haasteita voitaisiin ratkaista? Uskoisin näiden tutkimusten tuovan tärkeää tietoa liittyen GDPR:ään ja sen vaatimuksiin sekä haasteisiin. Mitä paremmin asetusta ymmärretään ja noudatetaan, sitä paremmin sen tavoitteet paremmasta tietosuojasta koko EU:n tasolla olisi saavutettavissa.

LÄHTEET

Aaltio, I. & Puusa. A. (2020). Mitä laadullisen tutkimuksen arvioinnissa tulisi ottaa huomioon? Teoksessa P. Juuti, & A.Puusa (toim.), *Laadullisen tutkimuksen näkökulmat ja menetelmät.* Gaudeamus. Ellibslibrary.com

Agre, P.E. (1997). Introduction. Teoksessa P.E. Agre, & M.Rotenberg (toim.), *Technology and Privacy: The New Landscape* (s. 1-29). MIT Press. ProQuest Ebook Central https://ebookcentral.proquest.com

Chen, L., & Crampton, J. (2007). Inter-domain role mapping and least privilege. *In Proceedings of the 12th ACM symposium on Access control models and technologies (SACMAT '07).* Association for Computing Machinery, New York, NY, USA, 157–162. doi: https://doi.org/10.1145/1266840.1266866

Davies, S.G. (1997). Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity. Teoksessa P.E. Agre, & M.Rotenberg (toim.), *Technology and Privacy: The New Landscape* (s. 143-167). MIT Press. ProQuest Ebook Central https://ebookcentral.proquest.com

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Euroopan unionin virallinen lehti 4.5.2016. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

Euroopan tietosuojaneuvosto (EDPB). (20.10.2020). *Ohjeet 4/2019 25 artiklan mukaisesta sisäänrakennetusta ja oletusarvoisesta tietosuojasta.* [Ohje]. https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fi.pdf

European Data Protection Supervisor (EDPS). (n.d.-a). Data Protection. Haettu osoitteesta https://edps.europa.eu/data-protection_en

European Data Protection Supervisor (EDPS). (n.d.-b). Information security. Haettu osoitteesta https://edps.europa.eu/data-protection/data-protection/reference-library/information-security_en

European Data Protection Supervisor (EDPS). (n.b.-c). The History of the General Data Protection Regulation. Haettu osoitteesta https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Gellman, R. (1997). Does Privacy Law Work? Teoksessa P.E. Agre, & M.Rotenberg (toim.), *Technology and Privacy: The New Landscape* (s. 193-219). MIT Press. ProQuest Ebook Central https://ebookcentral.proquest.com

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. doi: 10.2501/ijmr-2017-050

Ihmisoikeuksien yleismaailmallinen julistus, 10.12.1948. https://ihmisoikeusliitto.fi/wp-content/uploads/2016/05/YK_Ihmisoikeuksien-julistus.pdf

Information Commissioner's Office (ICO). (1.1.2021). Security. Haettu osoitteesta https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

Kamara, I., Leenes, R., Lachaud, Eric., Stuurman, K., Lieshout, M., & Bodea, G. (2019). Data protection certification mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679 : final report - Study. 10.2838/115106.

Kyberturvallisuuskeskus. (09.07.2020). Tietoturva. Haettu osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Lopes, I. M., Guarda, T. and Oliveira, P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. *Journal of Information Systems Engineering & Management, 4(2)*. https://doi.org/10.29333/jisem/5888

Lynskey, O. (2016). *The foundations of eu data protection law.* ProQuest Ebook Central https://ebookcentral.proquest.com

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, https://doi.org/10.6028/NIST.CSWP.04162018

NCSC & ICO. (17.5.2018). GDPR security outcomes. https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

Nissilä, N., & Nuopponen, A. (2018). Teknisen viestinnän taidot ja tehtävät työpaikkailmoituksissa. Teoksessa L. Kääntä, M. Enell Nilsson, & N. Keng (toim.) *Työelämän viestintä: VAKKI symposiumi XXXVIII*. Vaasa 8.-9.2.2018, 225-232. Haettu osoitteesta http://www.vakki.net/publications/no9_fin.html

Nuopponen, A. (2020). Systemaattinen käsiteanalyysi tutkijan työssä. Teoksessa H. Katajamäki (toim.) *Tieteellinen kirjoittaminen tiedeyhteisössä*, 94- 122. VAKKI

Publications 11. Vaasa: VAKKI. https://vakki.net/wp-content/uploads/2020/09/Tieteellinen-kirjoittaminentiedeyhteisossa.pdf

Oikeusministeriö. (27.1.2017). Miten valmistautua EU:n tietosuoja-asetukseen? [Oikeusministeriön julkaisu]. http://urn.fi/URN:ISBN:978-952-259-558-4

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions, *Journal of Cybersecurity, Volume 4, Issue 1,* 2018, tyy001, https://doi.org/10.1093/cybsec/tyy001

Presthus, W., Sørum, H. & Andersen, L.R. (2018). GDPR Compliance in Norwegian Companies. *Paper presented at NOKOBIT 2018*, Svalbard, 18-20 Sept. NOKOBIT, vol. 26, no. 1, Bibsys Open Journal Systems, ISSN 1894-7719

Puusa, A. (2008). Käsiteanalyysi tutkimusmenetelmänä. *Premissi 4/2008*, 36-43. https://www.academia.edu/3310906/K%C3%A4siteanalyysi_tutkimusmenetelm%C3%A4n%C3%A4

Ruohonen, J., & Hjerppe, K. (2021). The GDPR enforcement fines at glance, *Information Systems (2021) 101876*, https://doi.org/10.1016/j.is.2021.101876

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Commun. ACM. 49.* 97-100. 10.1145/1145287.1145316.

Siponen, M., & Willison, R. (2009). Information Security Management Standards: Problems and Solutions. *Information & Management, 46(5)*, 267-270

Solove, D. (2002). *Conceptualizing Privacy.* California Law Review, 90(4), 1087-1155. doi:10.2307/3481326

Solove, D. (2008). Understanding Privacy. *Harvard University Press, GWU Legal Studies Research Paper No. 420*(GWU Law School Public Law Research Paper No. 420).

Suomen perustuslaki 11.6.1999/731. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Tamburri, D.A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems, Volume 91, 101469*, https://doi.org/10.1016/j.is.2019.101469.

The European Union Agency for Cybersecurity (ENISA). (2016). Guidelines for SMEs on the security of personal data processing. https://doi.org/10.2824/867415

Tietosuojavaltuutetun toimisto. (n.d.). Tietosuoja. Haettu osoitteesta https://tietosuoja.fi/tietosuoja

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, 4(5)*, 193-220. doi:10.2307/1321160

Wilhelm, E. O. (2016, February). A brief history of the General Data Protection Regulation. Haettu osoitteesta: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/

Wilson, J. (1963). *Thinking with Concepts.* Cambridge University Press.

Wolters, P. T. J. (2017). The security of personal data under the GDPR: A harmonized duty or a shared responsibility? *International Data Privacy Law, 7(3),* 165-178. doi:http://dx.doi.org.ezproxy.jyu.fi/10.1093/idpl/ipx008

Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi, 04.11.1950. https://www.echr.coe.int/documents/convention_fin.pdf

LIITE 1 GDPR artikla 32

32 artikla

Käsittelyn turvallisuus

1. Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten

a) henkilötietojen pseudonymisointi ja salaus;

b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;

c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;

d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

2. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

3. Jäljempänä 40 artiklassa tarkoitettujen hyväksyttyjen käytännesääntöjen tai 42 artiklassa tarkoitetun hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että tämän artiklan 1 kohdassa asetettuja vaatimuksia noudatetaan.

4. Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 32. artikla