Nina Koivula

EUROOPAN UNIONIN YLEISEN TIETOSUOJA-ASETUKSEN AIHEUTTAMAT MUUTOKSET ORGANISAATIOIDEN TIETOTURVAPOLITIIKKOIHIN

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Koivula, Nina
Euroopan unionin yleisen tietosuoja-asetuksen aiheuttamat muutokset organisaatioiden tietoturvapolitiikkoihin
Jyväskylä: Jyväskylän yliopisto, 2017, 71 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

EU:n yleistä tietosuoja-asetusta aletaan soveltaa toukokuun 25. päivänä 2018 ja sen aiheuttamat muutokset ovat merkittäviä ja kunnianhimoisia. Se on yksi laaja-alaisimpia EU:n lakimuutoksia viimevuosien ajalta. Yleisen tietosuoja-asetuksen vaikutukset ovat merkittäviä organisaatioille, sillä epäonnistuessaan asetuksen vaatimusten noudattamisessa organisaatio joutuu maksamaan merkittävät sakot, korkeimmillaan joko 4% yrityksen globaalista vuosittaisesta liikevaihdosta tai 20 000 000 euroa riippuen siitä, kumpi on korkeampi. Yleinen tietosuoja-asetus tulee luultavasti vaikuttamaan tietoturvapoliitikkojen kehitykseen, kun yritykset pyrkivät noudattamaan uusia vaatimuksia.

Tietoturvapolitiikat sisältävät tyypillisesti yleisiä lausuntoja tavoitteista, uskomuksista, etiikasta ja vastuista, sekä keinot näiden saavuttamiseksi. Politiikat myös tarjoavat hallinnoituja ohjeita siitä, kuinka organisaatio toimii. Politiikat myös osoittavat ne alueet, joihin johdon tulisi kiinnittää erityisesti huomiota. Tietoturvapolitiikkojen tehtävä on myös tarjota johdon ohjausta ja tukea tietoturvallisuuden toteuttamiseen liiketoiminnallisten vaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti.

Tässä tutkielmassa selvitetään yleisen tietosuoja-asetuksen vaikutuksia organisaatioiden tietoturvapolitiikkoihin ja niiden päivittämiseen, sekä selvitetään, mitkä tekijät vaikuttavat organisaation aikomukseen noudattaa lainsäädännön vaatimuksia.

Asiasanat: tietoturvapolitiikka, yleinen tietosuoja-asetus, tietoturvapolitiikkojen kehittäminen, tietoturvapolitiikkojen päivittäminen, kuuliaisuus lainsäädäntöä kohtaan

ABSTRACT

Koivula, Nina
Information security policy changes caused by the European Union's General Data Protection Regulation
Jyväskylä: University of Jyväskylä, 2017, 71 p.
Information Systems, Master's thesis
Supervisor: Siponen, Mikko

The General Data Protection Regulation (GDPR for short) will apply from 25 May 2018. The GDPR will cause significant and ambitious changes. It is one of the most widely recognized pieces of legislation in the EU during the past years. Its effects on organizations are significant, because failure to comply with the regulation will cause remarkable sanctions to an organization. In the worst case, the sanctions can be up to 4% of an organization's annual global turnover or 20 million euros - whichever is higher. Because of this, many organizations will aim to comply with the regulation. Therefore the GDPR will also have an impact on information security policy development. Information security policies often include statements of goals, beliefs, ethics and responsibilities, but also the means to achieve them. Policies also point out the areas that need particular focus from the management and provide instructions on how an organization functions. They aim to provide guidance for management and support in information security regarding business requirements and legislation. This master's thesis examines the effects the GDPR will have on information security policies and the development of information security policies, as well as the reasons to comply with the European Union's legislation.

Keywords: information security policy, General Data Protection Regulation, information security policy development, information security policy maintenance, compliance towards legislation

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Lissabonin sopimuksen mukaan jokaisella on oikeus henkilötietojensa suojaan. Euroopan unionin perusoikeuskirjan mukaan henkilötietojen suoja onkin perusoikeus. Teknologian nopea kehitys tuo mukanaan uusia haasteita henkilötietojen suojeluun. Samaan aikaan luottamuksen rakentaminen verkkoympäristöön olisi sekä talouden että kehityksen kannalta suotavaa. Luottamuspulan vuoksi kuluttajat saattavatkin suhtautua uusiin verkkopalveluihin epäluuloisesti, jopa siinä mittakaavassa, että se uhkaa hidastaa uusien teknologioiden innovatiivisten käyttötapojen kehittämistä. Tästä syystä henkilötietojen suoja on koettu tärkeäksi Euroopan digitaalistrategiassa. Näistä syistä Eurooppa-neuvosto kehotti komissiota arvioimaan EU:n tietosuojasäädösten toimivuutta ja tarvittaessa esittämään lainsäädäntöä koskevia ehdotuksia. Näin syntyi EU:n yleinen tietosuoja-asetus. (Euroopan komissio, 2012)

Tutkielma käsittelee Euroopan unionin yleisen tietosuoja-asetuksen vaikutuksia tietoturvapolitiikkoihin ja niiden kehittämiseen. Euroopan unionin yleistä tietosuoja-asetusta aletaan soveltaa toukokuun 25. päivänä vuonna 2018. Sen aiheuttamat muutokset ovat merkittäviä ja kunnianhimoisia, ja se on yksi laaja-alaisimpia EU:n lakimuutoksia viimevuosien ajalta. (Bird & Bird, 2016). Yleinen tietosuoja-asetus pyrkii yhdenmukaistamaan yksilöiden tietosuojaa Euroopan unionin alueella. Euroopan unionin yleinen tietosuoja-asetus pyrkii myös parantamaan liiketoimintamahdollisuuksia mahdollistamalla henkilötietojen vapaan virtaamisen digitaalisilla sisämarkkinoilla. (Interinstitutional File 2012/0011 (COD), 2015). Koska EU:n yleinen tietosuoja-asetus on varsin pitkä dokumentti joka sisältää paljon vaatimuksia, keskittyy tämä tutkimus yleisen tietosuoja-asetuksen keskeisimpiin mukanaan tuomiin henkilötietojen suojaamiseen tähtääviin periaatteisiin.

Tietoturvapolitiikat ovat yleensä erilaisia eri organisaatioissa, mutta tyypillisesti ne sisältävät yleisiä lausuntoja tavoitteista, uskomuksista, etiikasta ja vastuista, sekä keinot näiden saavuttamiseksi. Politiikat tarjoavat hallinnoituja ohjeita siitä, kuinka organisaatio toimii. Politiikkojen tarkoitus on tarjota ohjausta niille, jotka joutuvat tekemään päätöksiä organisaatiossa. (Wood, 1995). Tietoturvapolitiikkojen tehtävä on tarjota johdon ohjausta ja

tukea tietoturvallisuuden toteuttamiseen liiketoiminnallisten vaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti (Suomen Standardoimisliitto SFS ry, 2014).

Aiheesta ei juurikaan ole aiempaa tutkimusta sen tuoreuden vuoksi. Kuitenkin sekä asetuksesta että tietoturvapolitiikoista löytyy reilusti tieteellisiä artikkeleita. Suurin osa asetukseen liittyvistä artikkeleista esittelee asetusta ja sen merkittävyyttä, sekä sen mahdollisia vaikutuksia. Osa yleistä tietoturva-asetusta käsittelevistä lähteistä on lakitekstiä. Tietoturvapolitiikoista löytyy monenlaisia artikkeleita; osa artikkeleista liittyy tietoturvapolitiikkojen kehittämiseen (Wood, 1995), osa käsittelee tietoturvapolitiikkojen tehokkuutta (Höne & Eloff, 2002), osa taas keskittyy arvioimaan tietoturvapolitiikkojen kehittämistä (Maynard & Ruighaver, 2002).

Aihe on ajankohtainen, sillä asetusta aletaan soveltaa keväällä 2018. Organisaatioiden tulisikin aloittaa valmistautuminen asetuksen voimaantuloon jo hyvissä ajoin, sillä se tulee vaatimaan lukuisia laaja-alaisia muutoksia. Tästä johtuen asetusta ja sen mukanaan tuomia muutoksia tietoturvapolitiikkojen kannalta olisi tärkeää tutkia jo ennen asetuksen voimaantuloa.

Asetuksen vaikutukset ovat merkittäviä organisaatioille, sillä epäonnistuessaan asetuksen vaatimusten noudattamisessa organisaatio joutuu maksamaan merkittävät sakot, korkeimmillaan joko 4% yrityksen globaalista vuosittaisesta liikevaihdosta tai 20 000 000 euroa riippuen siitä, kumpi on korkeampi (Euroopan komissio, 2012). Yleinen tietosuoja-asetus tulee luultavasti vaikuttamaan tietoturvapoliitikkojen kehitykseen, kun yritykset pyrkivät noudattamaan uusia vaatimuksia.

Tutkimus pyrkii vastaamaan kysymykseen siitä, mikä saa organisaatiot päivittämään tietoturvapolitiikkojaan, sekä siihen, mitkä tekijät vaikuttavat organisaation aikomukseen noudattaa lainsäädännön vaatimuksia. Näiden kysymysten avulla pyritään selvittämään, tuleeko yleinen tietosuoja-asetus voimaantullessaan aiheuttamaan tarpeen tietoturvapolitiikkojen päivittämiselle organisaatioissa.

Tutkimuksen teoriaosuudessa on käytetty käsitteellisteoreettista tutkimusmenetelmää, jossa esitetään havaintoja aiemmasta kirjallisuudesta. Tutkimusongelmat ovat:

- Mikä saa organisaation päivittämään tietoturvapolitiikkojaan?
- Mitkä tekijät vaikuttavat organisaation aikomukseen noudattaa lainsäädännön vaatimuksia?

Näiden tutkimusongelmien pohjalta empiirisessä tutkimuksessa pyritään vastaamaan päätutkimusongelmaan, joka on:

- Saako yleinen tietosuoja-asetus organisaatiot päivittämään tietoturvapolitiikkojaan ja millaisia nämä muutokset tulevat olemaan?

Aiheeseen liittyvää tietoa kerätään kirjallisuuskatsausta varten pääasiassa alan kirjallisuudesta, julkaisuista ja tietokannoista, kuten ACM Digital Libraryn, AIS

Electronic Libraryn, IEEE:n ja Google Scholarin kautta. Pääasiallisia hakusanoja olivat ”information security policy”, ”information security policy development”, ”information security policy organization” ”compliance to legislation” ja ”general data protection regulation”.

2 TIETOTURVAPOLITIIKAT

Tässä luvussa käydään läpi tietoturvapolitiikkoja sekä niiden kehittämistä, riskianalyysia ja tietoturvapolitiikkoja organisaatiokontekstissa.

2.1 Tietoturvapolitiikkojen yleiskuvaus

Tieto on yksi organisaation tärkeimmistä kilpailuvalteista (Hedström ym. 2011). Samaan aikaan organisaatiot siirtyvät käyttämään yhä kehittyneempää teknologiaa. Kehitys asettaa myös uusia vaatimuksia tietoturvapolitiikoille ja niiden kehittämiselle. (Baskerville & Siponen, 2002). Suojatakseen tietoa, organisaatioiden tulee ottaa käyttöönsä joukko toimia, kuten turvallisuuskontrolleja, vastatoimenpiteitä ja suojatoimenpiteitä. Nämä toimet ilmenevät monenlaisissa muodoissa, esimerkiksi politiikkoina, toimintaohjeina, suosituksina tai organisaatiorakenteina. Organisaatioiden toimeenpanemien kontrollien lisäksi alan kirjallisuus korostaa myös tietoturvapolitiikkojen merkitystä. (Lopes & Sá-Soares, 2012). Monet näkevät tietoturvan pelkästään teknologisena ongelmana, mutta todellisuudessa mitkään kontrollit tai tietoturvaratkaisut itsessään eivät ole riittäviä, vaan toimiakseen tietoturva vaatii aina ihmisten toiminnan ottamista huomioon. Pelkkä palomuuri ei anna riittävästi suojaa vaan siihen tulisi yhdistää tarpeelliset politiikat, standardit ja muut hallinnolliset ohjeet. (Grobler & von Solms, 2004; Lopes & Sá-Soares, 2012; Tuyikeze & Pottas, 2011; Wood, 1995). Suojatakseen tietoa organisaation sisällä, tulee organisaatiolla olla hyvin suunniteltu, tehokas tietoturvapolitiikka. Politiikka voidaan määritellä i. toimintatavaksi, ohjaavaksi periaatteeksi tai tarkoituksen mukaiseksi menettelytavaksi, sekä ii. vakuutustodistukseksi. (Tuyikeze & Pottas, 2011). Grobler & von Solms (2004) sanovat, että politiikka viittaa i. toimintatapaan, jota pitää noudattaa tai toimintoon, joka tulisi suorittaa, sekä ii. julkilausumaan tai todistukseen. Baskerville & Siponen (2002) jakavat tietoturvapolitiikat kahteen erilaiseen ryhmään: i. teknisiin, eli tietoturvallisuuteen liittyviin, sekä ii. epäteknisiin, eli turvallisuuden hallintaan

liittyviin politiikkoihin. Tämä tutkimus keskittyy pääasiassa jälkimmäisiin, eli turvallisuuden hallintaan liittyviin politiikkoihin.

On yleisesti tiedostettu, että tietoturvapolitiikat ovat tärkeimpiä kontrolleja organisaation sisällä, jotka varmistavat tietoturvan toimeenpanon ja tehokkuuden (Höne & Eloff, 2002). Monesti tietoturvapolitiikat koetaankin pohjana, jonka päälle voidaan rakentaa toimivia turvallisuuskäytänteille (Doherty & Fulford, 2005; Higgins, 1999; Parker 1998; Warman, 1992).). Pohjimmiltaan tietoturvapolitiikat ovat dokumentteja, jotka antavat suunnan organisaatiolle ja määrittävät rajat tietoturvalle. Tietoturvapolitiikat myös osoittavat johdon sitoutumisen ja tuen tietoturvalle, sekä määrittävät tietoturvan roolin organisaation näkemyksen ja tehtävän saavuttamisessa. (Höne & Eloff, 2002). Tietoturvapolitiikat parantavat organisaation turvallisuuden tasoa, mutta myös turvaavat organisaation selustan oikeudellisessa mielessä, jos politiikkojen tai muiden ohjeiden olemassaoloa joskus kyseenalaistetaan (Etsebeth, 2006). Tietoturvapolitiikkojen todellinen arvo monesti huomataankin tietoturvavälikohtauksen yhteydessä (Peltier, 2002).

Tietoturvapolitiikat ovat yleensä erilaisia eri organisaatioissa, mutta tyypillisesti ne sisältävät yleisiä lausuntoja tavoitteista, uskomuksista, etiikasta ja vastuista, sekä keinot näiden saavuttamiseksi. Politiikat tarjoavat hallinnoituja ohjeita siitä, kuinka organisaatio toimii ja politiikkojen tarkoitus onkin tarjota ohjausta niille, jotka joutuvat tekemään päätöksiä organisaatiossa. (Wood, 1995). Tietoturvapolitiikkojen tehtävä on paitsi tarjota johdon ohjausta, mutta myös tukea tietoturvallisuuden toteuttamiseen liiketoiminnallisten vaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti (Suomen Standardoimisliitto SFS ry, 2014). Guel (2007) kuvaa politiikkoja virallisiksi, lyhyiksi ja korkean tason suunnitelmiksi, jotka osoittavat organisaatioin tavoitteet, päämäärät ja hyväksyttävät toimenpiteet tietyssä asiassa. Tietoturvapolitiikat myös määrittelevät tiedon käyttäjien vastuut ja oikeudet. Tehokas tietoturvapolitiikka varmistaa, että tiedon käyttäjät ymmärtävät, mitä on tiedon hyväksyttävä ja vastuullinen käyttö, sekä varmistavat tiedon turvallisen käytön päivittäisissä toimissa. (Höne & Eloff, 2002). Politiikkoja voidaan kuvailla myös generalisoiduiksi vaatimuksiksi ja ne ovat organisaatioissa luonteeltaan pakottavia. Toimiakseen toisin, työntekijän tulee hankkia erityinen lupa. (Wood, 1995).

Politiikat sisältävät yleensä ylemmän tason vaatimuksia kuin standardit. Standardit mainitsevat esimerkiksi organisaatiorakenteen, käytettävät teknologiat ja liiketoimintaprosessit tarkemmin kuin politiikat. Tästä syystä politiikat säilyvät yleensä useita vuosia ennallaan, kun taas standardit muuttuvat muutaman vuoden välein. (Wood, 1995).

Politiikat sisältävät korkeamman tason vaatimuksia myös toimintaohjeisiin verrattuna. Toimintaohjeet ovat operationaalisia toimenpiteitä, joita työntekijöiden on seurattava saavuttaakseen tietyn tavoitteen. Politiikat kuvaavat yleisen tason keinot ratkaista tietty ongelma. Jos politiikasta tulee pitkä tai yksityiskohtainen, ei se ole enää politiikka, vaan toimintaohje. (Wood, 1995).

Politiikat ovat erilaisia myös kontrolleihin verrattuna. Politiikat tarjoavat laajoja tavoitteita, jotka voidaan toteuttaa kontrollien avulla. Politiikka voisi esimerkiksi kieltää mahdolliset eturistiriidat organisaation sisällä. Kontrolli taas voi vaatia, että kaikki työntekijät allekirjoittavat lausunnon, jonka mukaan he ovat lukeneet organisaation menettelyohjeen ja vakuuttavat noudattavansa sitä. (Wood, 1995).

Monesti organisaatiot pyrkivät hallitsemaan tietoturvaansa yksinkertaisesti ostamalla tietyn tietoturvatuotteen ja uskomalla, että se riittää turvaamaan yrityksen tietoturvauhkilta. Usein organisaation johto joutuu kuitenkin vastaavissa tilanteissa pettymään, sillä tietoturvatuote itsessään ei tuotakaan toivottuja tuloksia. Usein tämä johtuu siitä, että organisaatiossa ei vielä ole sopivaa infrastruktuuria kyseiselle tietoturvatuotteelle, sillä organisaatiossa ei ole vielä suoritettu riskianalyysiä eikä organisaatiolla ole tarvittavaa tietoturvapolitiikkaa. Luodakseen tarvittavan infrastruktuurin organisaatioon tarvitsee organisaatio esimerkiksi dokumentoidut politiikat, suositukset, standardit, toimintaohjeet, vastuullisuuslausunnot, riskianalyysiprosessin ja prosessin turvallisuussuunnitelmaa varten. (Wood, 1995).

2.1.1 Tietoturvapolitiikkojen merkitys organisaatiokontekstissa

Politiikat ovat johdolle selkeä tapa osoittaa, että tietoturva on organisaatiolle tärkeää, sekä keino vaatia työntekijöitä kiinnittämään huomiota tietoturvaan. Politiikat saattavatkin olla avuksi sellaisten tilanteiden ratkaisussa, joissa riskinä on tiedon riittämätön suojaus. (Wood, 1995). Woodin (1995) mukaan politiikat ovat organisaatioille edullinen ja vaivaton tapa turvata selustansa, jos väärinkäytöksiä ilmenee. Jos organisaatio ei kuitenkaan ole määritellyt asiallista ja hyväksyttävää tietoturvakäyttäytymistä politiikkojen avulla, saattaa tilanne pahimmillaan eskaloitua oikeusjutuksi. (Leinfuss, 1996; Robinson, 1997; Wood, 1995).

Yksi keskeisimmistä ongelmista tietoturva-alalla ovat sirpaleiset ja epäjohdonmukaiset näkemykset tietoturvan oleellisuudesta. Usein vain jotkin osastot organisaation sisällä tukevat tietoturvapyrkimyksiä, kun taas toiset osastot saattavat olla hyvinkin vastentahtoisia tietoturvaa kohtaan. Todellinen ongelma tilanteesta tulee, jos osastot jakavat resursseja keskenään, jolloin vastentahtoinen osasto saattaa vaarantaa tietoturvapyrkimyksiä tukevan osaston tietoturvallisuuden. (Wood, 1995). Wood (1995) toteaa kuitenkin, ettei organisaation ole järkevää tai tavoiteltavaa kouluttaa kaikkia työntekijöitä tuntemaan tietoturva-alan koko kompleksisuutta. Organisaatioiden olisi kuitenkin tärkeää määritellä politiikkojen avulla jokin minimitaso tietoturvalle, jota kaikki noudattaisivat (Wood, 1995).

Organisaatiot, joilta löytyy riittävät tietoturvapolitiikat, suojaavat itseään monelta harmilta. Kyseiset organisaatiot myös saavuttavat selvää etua verrattuna sellaisiin organisaatioihin, jotka jäävät pikemminkin odottamaan ja katsomaan tilanteen kehittymistä, sen sijaan että ne kehittäisivät tai päivittäisivät tietoturvapolitiikkojaan. Organisaatiot, jotka eivät joko ole

kehittäneet tietoturvapolitiikkaa ollenkaan, tai joilla sitä ei ole otettu käyttöön tehokkaasti, ovat alttiimpia joutumaan hakkereiden ja muiden uhkatekijöiden uhriksi. Lopulta tällaiset tapaukset johtavat asiakkaiden luottamukseen ja osakkaiden arvostukseen. (Tuyikeze & Pottas, 2011).

2.1.2 Tietosuojapolitiikkojen merkitys organisaatiokontekstissa

Smithin (1993) mukaan monilla organisaatioilla, jotka säännöllisesti käsittelevät sensitiivisiä henkilötietoja, esimerkiksi potilastietoja ja varallisuustietoja, ei ole tarvittavia politiikkoja. Lisäksi olemassa olevat politiikat saattavat olla ristiriidassa organisaation käytänteiden kanssa. Teknologisen kehityksen myötä organisaatiot ottavat käyttöön uusia teknologisia sovelluksia, mutta sopiva käyttö saattaa edelleen olla määrittelemättä. Yritysjohto kohtaa usein työssään pulmatilanteita liittyen siihen, kuinka henkilötietoja on soveliasta käyttää. Nämä pulmatilanteet ratkaistaan organisaation sisällä. Tällöin päätöksiin vaikuttaa johdon omat näkemykset oikeasta ja väärästä liittyen henkilötietojen käsittelyyn. (Smith, 1993).

Smithin (1993) mukaan yritysjohto harvoin ottaa proaktiivisen toimintatavan liittyen tietosuojapolitiikkoihin, vaan he odottavat, kunnes jokin ulkoinen tekijä pakottaa heidät toimimaan. Tällaisena ulkoisena tekijänä saattaa toimia esimerkiksi uhka lainsäädäntötoimista. Kun organisaation johto sitten lopulta päättää ryhtyä toimiin, saattaa organisaatio olla siirtymävaiheessa hetken aikaa. Siirtymävaihe on usein työntekijöille haastava, sillä heillä voi olla ristiriitaiset tunteet organisaation nykyisen tietojenkäsittelyn suhteen. (Smith, 1993).

Smith havaitsi jo vuonna 1993 eroavaisuuksia liiketoiminnan ja yksilöiden suhtautumisessa tietosuojaan: yksilöt ovat entistä huolestuneempia tietosuojastaan, kun taas organisaatiot ryhtyvät toimiin tietosuojan parantamiseksi vasta, kun toimialalla on saavutettu siitä yhteisymmärrys, tai kun laki velvoittaa parantamaan tietosuojatilannetta. (Smith, 1993).

Smithin (1993) mukaan epäviralliset tietosuojan käytänteet monesti ajavat organisaation työntekijät vähitellen tekemään vain vähimmäismäärän työtä liittyen tietosuojaan, kunnes organisaatio havaitsee jonkin ulkoisen uhkan, esimerkiksi negatiivisen julkisuuden uhkan tai lainsäädännöllisiä vaatimuksia. Ennen ulkoisen uhkan havaitsemista tietosuojatoimet ovat lähinnä keskijohdon vastuulla, jolloin toimintatavat ovat reaktiivisia. (Smith, 1993). Smithin (1993) tutkimuksessa havaittiin, että kun organisaatiota uhkaa ulkoinen uhka, muistetaan organisaation sisällä, että toimintaympäristö on muuttunut ja että politiikkoja tulisi muokata sen vuoksi. Tämän seurauksena organisaatio päätyi reaktiivisesti tutkimaan ja koodaamaan politiikat ja harkitsemaan niiden sisältöä. Huomionarvoista on se, että ylin johto osallistui tähän toimintaan, sekä se, että vastaus tietosuojauhkiin oli juuri virallinen dokumentti politiikan muodossa. (Smith, 1993).

Koska organisaatiot monesti luovat tarvittavat politiikat vasta ulkoisen uhkatekijän kohdatessaan, joutuvat organisaation työntekijät, yksilöt, olemaan tekemisissä organisaation riittämättömien politiikkojen kanssa. Tästä johtuen

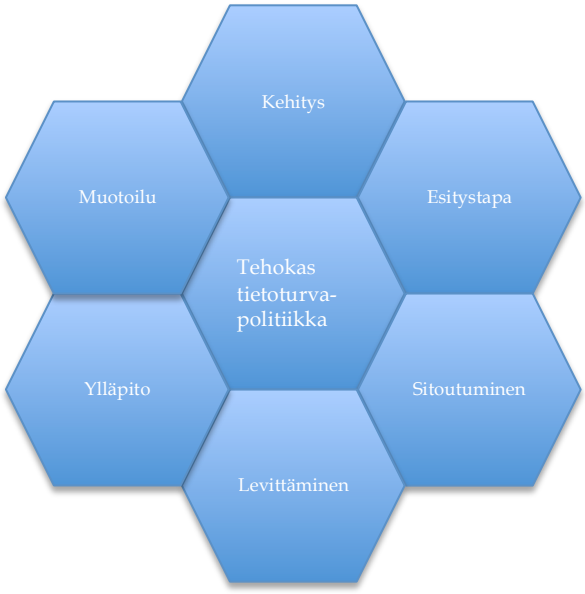
työntekijät saattavat kokea arvoihin liittyviä konflikteja liittyen organisaation tietojenkäsittelyyn. Organisaation johto taas ei käyttäydy kuten yksilöt, vaan organisaation ilmapiirin mukaan. Tästä johtuen organisaation henkilöstö eivät aina ole yhtä mieltä organisaation henkilötietojen käsittelystä, vaan se saattaa aiheuttaa jopa epämukavuutta ja vaivautuneisuutta yksilöissä. (Smith, 1993).

2.2 Tehokas tietoturvapolitiikka

On epäselvää, kuinka hyvin organisaatiot hyödyntävät kirjallisuudessa esiteltyjä keinoja tietoturvapolitiikkojen toimeenpanemiseksi (Maynard & Ruighaver, 2003). Yleinen ongelma liittyen tietoturvapolitiikkoihin on se, että ne eivät vaikuta varsinaisiin käyttäjiin ja toimeenpanijoihin. Sellaisen tietoturvapolitiikan kehittäminen, joka heijastaa organisaation näkemystä ja tehtävää, ja sen juurruttamien organisaation sellaisella tavalla, että siitä tulee normaali osa päivittäisiä toimia, on vähintäänkin haastavaa. Monesti käyttäjät päätyvätkin jättämään tietoturvapolitiikkojen olemassaolon huomioitta. Tähän voi olla syynä esimerkiksi se, että käyttäjät eivät ymmärrä politiikkoja tai se, että politiikka on liian pitkä tai liian tekninen sisällöltään. Käyttäjät eivät välttämättä myöskään ymmärrä politiikan ja päivittäisten työtehtävien välistä yhteyttä. Tehokas tietoturvapolitiikka auttaa organisaatiota saavuttamaan sen tietoturvatavoitteet. Koska liiketoiminta muuttuu jatkuvasti enemmän tiedosta riippuvaiseksi, tulee myös tiedon turvaamisesta organisaatiolle tärkeämpää. (Höne & Eloff, 2002).

Ollakseen todella tehokkaita, tietoturvapolitiikkojen tulee yhdistää sekä käyttäjien tarve täsmälliseen ja luotettavaan tietoon, sekä organisaation tarve saavuttaa sen strategiset tavoitteet. Näin käyttäjät kokevat, että tietoturvapolitiikat ovat olemassa taatakseen tarpeellisen tiedon saatavuuden oikea-aikaisesti, jotta asiantuntevia päätöksiä voidaan tehdä. Tehokas tietoturvapolitiikka siis on ymmärrettävä, merkityksellinen, käytännöllinen ja kutsuva dokumentti, joka omistaa sanansa käyttäjälle ja vakuuttaa heidät käsittelemään tietoa turvallisesti. (Höne & Eloff, 2002).

Koska tietoturva liittyy yhä enenemissä määrin ihmisiin ja liiketoimintaan, tulisi myös tietoturvapolitiikkoja muokata vastaamaan nykytilannetta, sillä lopulta käyttäjien toiminta määrittää, kuinka tehokas tietoturvapolitiikka todella on. Tämän vuoksi tietoturvapolitiikan ja sitä tukevien toimintojen tulisi keskittyä käyttäjään, sisältäen esimerkiksi tietoturvapolitiikan kirjoitustyylin, esitystyylin sekä dokumentin levityksen. Tukevat toiminnot vaikuttavat paljon tietoturvapolitiikan menestykseen ja tehokkuuteen, jonka vuoksi niihin tulisi kiinnittää huomiota tietoturvapolitiikkoja kehitettäessä. Kuvio 1 kuvaa tietoturvapolitiikan riippuvuutta tukevista toiminnoista. (Höne & Eloff, 2002).



KUVIO 1 Tehokasta tietoturvapolitiikkaa tukevat toiminnot (mukaillen Höne & Eloff, 2002).

Muotoilun, jolla tarkoitetaan dokumentin kirjoitustyyliä, tulisi aina olla yhdenmukainen organisaation kommunikointityylin ja organisaation kulttuurin kanssa. Näin varmistetaan, ettei politiikka eroa muista organisaation virallisista dokumenteista. Monesti organisaatiossa työskentelevät tekniseen henkilökuntaan kuuluvat työntekijät päätyvät ottamaan päävastuun myös tietoturvapolitiikkojen kehittämisestä. Tekninen henkilökunta toki tuntee tietoturvaan liittyvät teknologiat hyvin, mutta monesti heillä ei ole ymmärrystä käyttäjistä ja heidän tarpeistaan. Kyseinen ongelma on kuitenkin ehkäistävissä, kunhan politiikan kehitystyöhön osallistuu edustajia kaikista sidosryhmistä. Tärkeää olisi myös esittää politiikka muodossa, joka on hauska ja houkutteleva. Näin käyttäjät panevat sen merkille. (Höne & Eloff, 2002). Hone & Eloff (2002) esimerkiksi ehdottavat, että politiikka voisi sisältää sarjakuvia.

Tehokkaan tietoturvapolitiikan kannalta johdon sitoutuminen ja tuki ovat elintärkeitä asioita. Tämä johtuu siitä, että työntekijät monesti kaipaavat esimerkillistä käytöstä. Käyttäjät monesti eivät usko tietoturvapolitiikkaan, jos he eivät näe johdon seuraavan politiikkojen ohjeita. (Höne & Eloff, 2002).

Tietoturvapolitiikka ei voi myöskään olla tehokas, jos käyttäjät eivät ole tietoisia siitä. Tästä johtuen on tärkeää, että politiikka on levitetty kauttaaltaan koko organisaatioon. Politiikan levittämiseen on useita eri tekniikoita, esimerkiksi paperikopioiden levittäminen, elektroniset kopiot, dokumentin julkaiseminen organisaation intranetissä tai vaikkapa julisteiden levittäminen.

Dokumentin levitystavan tulisi vastata mahdollisimman hyvin vastaavien dokumenttien perinteisiä levittämistapoja.

Organisaation tulisi myös pitää mielessä, että tietoturvapolitiikkaa tulee muokata säännöllisesti vastaamaan paremmin organisaation tarpeita. Politiikan säännöllisellä päivittämisellä on monia etuja. Politiikan päivittäminen auttaa esimerkiksi pysymään ajan tasalla organisaation kehityssuunnasta ja varmistamaan, että politiikasta ei tule vanhentunut ja liian staattinen dokumentti. Monesti politiikkojen katselmointi tuokin mukanaan muutoksia. Tästä johtuen katselmoinnin olisi hyvä istua organisaation normaaliin liiketoiminnan kiertokulkuun. Yleensä käyttäjätkin ovat tietyissä vaiheissa liiketoiminnan kiertokulkua vastaanottavaisempia muutokselle ja uusien ajatusten täytäntöönpanolle. (Höne & Eloff, 2002).

Taatakseen tietoturvapolitiikan tehokkuuden, tulisi edellä mainitut tukevat toiminnot huomioida ja panna täytäntöön, sillä lopulta tietoturvapolitiikan tehokkuus vaikuttaa suoraan organisaation tietoturvan tehokkuuteen. (Höne & Eloff, 2002).

2.3 Tietoturvapolitiikkojen kehittäminen

Tehokkain yhdistelmä erilaisia tietoturvatoimenpiteitä on erilainen eri organisaatioille. Kirjallisuudesta löytyy monenlaisia lähestymistapoja ja metodeja, joiden avulla organisaatiot voivat kehittää tietoturvapolitiikan ja näitä lähestymistapoja käsitellään seuraavaksi.

2.3.1 Taustatoimenpiteet ennen politiikkojen kehittämistä

Organisaation tulisi määritellä vastuuhenkilö tietoturvapolitiikkojen julkaisijaksi ja ylläpitäjäksi ennen tietoturvapolitiikkojen kehittämisen aloittamista. Toinen tärkeä edellytys tietoturvapolitiikkojen kehittämiselle on organisaation johdon ymmärrys siitä, että tieto on yksi organisaation kilpailuvalteista, ja että he ovat vastuussa tiedon hallinnasta. Johdon tulee myös tukea uusien työkalujen ja tekniikoiden kehittämistä, sillä johdon tuella on suuri merkitys sen kannalta, kehitetäänkö tietoturvapolitiikkoja organisaatiossa. (Wood, 1995).

Tietoturvapolitiikat voidaan kehittää samalla, kun organisaation tietoturvamanuaalia valmistellaan. Kyseistä manuaalia levitetään yleensä laajalti organisaatiossa, jonka vuoksi sen yhteydessä olisi hyvä esittää myös tietoturvapolitiikka. Tietoturvapolitiikat voidaan myös valmistella samalla, kun organisaatiossa valmistellaan materiaalia koulutuksiin ja tietoisuuskampanjoihin. Tähän tarkoitukseen voidaan valmistella esimerkiksi videoita, luentoja, julisteita tai lehtiartikkeleita sisäiseen käyttöön. Osa organisaatioista alkaa kehittää tietoturvapolitiikkoja merkittävän tietoturvarikkomuksen seurauksena, epäsuotuisan tarkastusraportin

seurauksena tai turvallisuuteen liittyvän oikeusjutun seurauksena. Tällaisen tilanteen seurauksena johto monesti tukee tietoturvapolitiikkojen kehittämistä. (Wood, 1995).

Organisaation tulisi kuitenkin kehittää tietoturvapolitiikat jo aikaisessa vaiheessa, ennen esimerkiksi pääsynhallintaan, järjestelmäkehitykseen ja teknisiin standardeihin liittyvien ohjeiden kehittämistä. Monesti ensimmäiset politiikat ovatkin lyhyitä, ja niitä seuraa yksityiskohtaisemmat politiikat. Politiikkoja kehittäessä tulisi pitää mielessä, että politiikat pitäisi kirjoittaa sillä tavalla, että niitä ei tarvitse muokata seuraavaan viiteen vuoteen. Ollakseen ajan tasalla esimerkiksi organisaation tietojenkäsittelyyn käytettävästä teknologiasta, laeista, asetuksista ja organisaatiomallista, tulisi politiikkoja kuitenkin muokata säännöllisesti. (Wood, 1995).

Monesti organisaatioista on löydettävissä politiikkoja, jotka ovat keskenään ristiriidassa. Organisaation johdon tulisikin määritellä politiikkojen keskinäinen suhde, jotta työntekijät eivät joudu itse tekemään päätöksiä sen suhteen, miten politiikkoja noudatetaan. Politiikkojen kehittäminen vaatii monesti kompromisseja organisaation sisällä. Kompromisseja joudutaan monesti tekemään esimerkiksi kustannusten ja turvallisuuden, joustavuuden ja turvallisuuden sekä helppokäyttöisyyden ja turvallisuuden välillä. Tietoturvapolitiikkojen kehittämiseen liittyy monesti myös ehtoja ja rajoituksia, jotka tulee ottaa huomioon. Tietoturvapolitiikkojen tulee esimerkiksi olla yhteensopivia voimassa olevan lainsäädännön kanssa. Tietoturvapolitiikkojen kehittäjän tuleekin olla tietoinen organisaatioon liittyvistä ehdoista ja rajoituksista. Kehittäjä voi hankkia ymmärrystä näistä ehdoista ja rajoituksista esimerkiksi sisäisen tarkastuksen raporteista, riskianalyysin dokumentaatiosta ja voimassa olevista, muita alueita koskettavista politiikoista. (Wood, 1995).

2.3.2 Tietoturvapolitiikan kehittämisprosessi

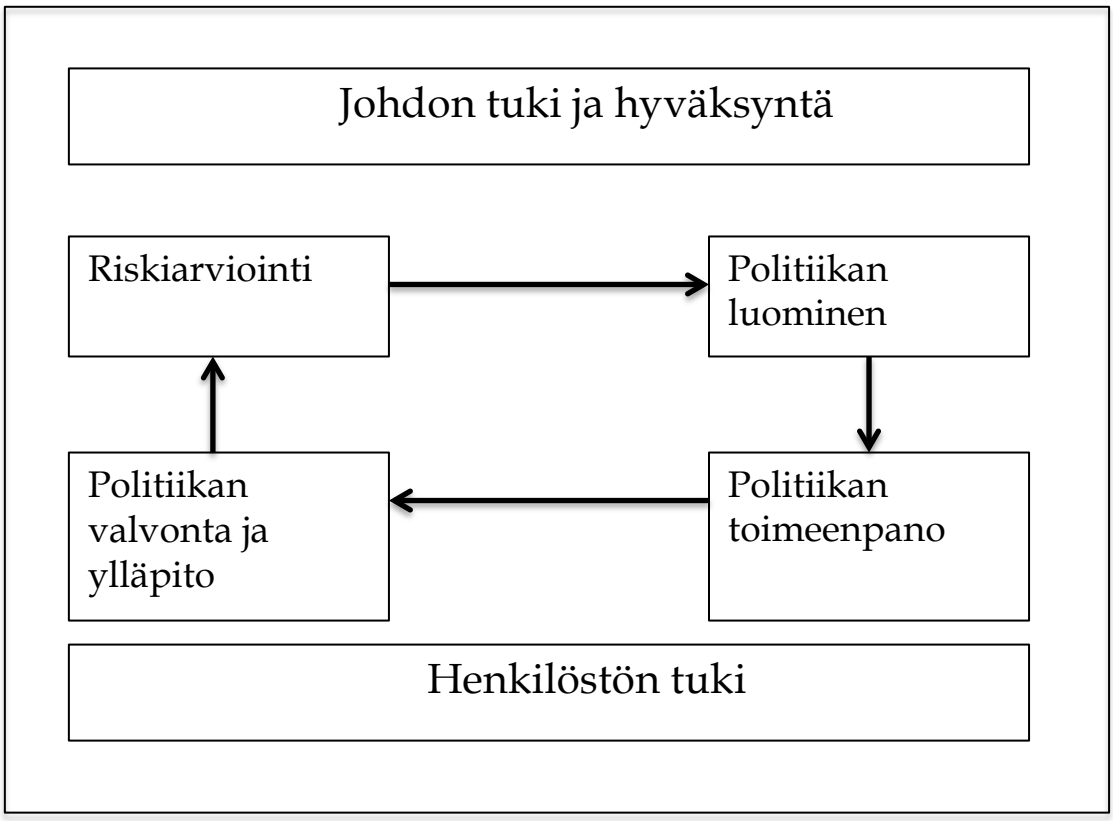
Seuraavaksi käsitellään erilaisia lähestymistapoja tietoturvapolitiikkojen kehittämiseen. Monesti organisaatioita kehotetaan kehittämään tietoturvapolitiikkojaan käyttämällä apuna yleisiä tietoturvan hallinnan standardeja (Gaskell, 2000; Janczewski, 1999). Yleisen tietoturvan hallintaan käytettävän standardin soveltaminen saattaa lyhentää politiikan kehittämiseen käytettävää aikaa (Janczewski, 1999). Yleensä nämä yleiset standardit eivät kuitenkaan kykene huomiomaan organisaatioiden erilaisuutta ja erilaisia turvallisuusvaatimuksia (Baskerville, 1993). Yleiset standardit myös epäonnistuvat ottamaan huomioon ongelmien sosiaalisen luonteen (Dhillon & Backhouse, 2001). Yleiset tietoturvan hallintaan käytettävät standardit eivät myöskään monesti kykene huomioimaan liiketoiminnan vaatimuksia, jolloin turvallisuuspolitiikan osoittamat turvallisuusvaatimukset saattavat olla ristiriidassa liiketoiminnan vaatimusten kanssa. Yleiset standardit ovat yleensä sisällöltään yleisluontoisia, jolloin johto ei välttämättä voi perustaa päätöksiään politiikkoihin. (Ferris, 1994). Organisaatioiden uniikit toimintaympäristöt tulisikin ottaa huomioon tietoturvapolitiikkoja kehitettäessä (Schweitzer, 1982). Näitä lähestymistapoja vertaillaan taulukossa 1. Alla oleva taulukko tarjoaa

viisi yleistä esimerkkiä tietoturvapolitiikan kehittämiselle. Taulukossa kehittämisprosessi on jaettu kuuteen ryhmään, joiden perusteella eri lähestymistapoja voidaan vertailla. Lähestymistavoissa on paljon samaa, mutta ne eroavat merkittävästi esimerkiksi suhtautumisessa riskiarvioinnin tarpeellisuuteen. (Tuyikeze & Pottas, 2011).

TAULUKKO 1 Tietoturvapolitiikkojen kehittämismetodit (mukaillen Tuyikeze & Pottas, 2011).

Tekijä	**Control Data (2000)**	**Computer Technology Research Group (1998)**	**DTI (1999)**	**SANS Institute (2007)**	**Woodward (2000)**
Ryhmä 1 **Riskiarvioinnin toimenpiteet**	1. Tunnista mahdolliset uhkat ja riskit 2. Määrittele suojattava omaisuus	1. Tunnista, mitä omaisuutta tulisi suojata 2. Määrittele kunkin omaisuuserän suojaustaso 3. Määrittele internetin käyttöä 4. Määrittele olemassa olevat uhkat 5. Perehdy siihen, kuinka ottaa tunnistetut uhkat huomioon 6. Suorita vaikutusarviointi			1. Tutki riskejä
Ryhmä 2 **Politiikan luomisen toimenpiteet**		7. Luonnostele turvallisuuspolitiikka 9. Lisää palautumisosio politiikkaan	1. Tutki politiikan sisältöä 2. Luonnostele politiikka	1. Kirjoita politiikka	2. Muotoile politiikka
Ryhmä 3 **Politiikan toimeenpano toimenpiteet**	2. Toimeenpane strategia omaisuuden suojaamiseksi	8. Kehitä toimeenpanosuunnitelma 10. Käyttäjien koulutus	3. Julkaise politiikka henkilöstölle	2. Julkaise politiikka	3. Kehitä standardeja politiikan toimeenpanosta
Ryhmä 4 **Politiikan valvontaan ja ylläpitoon liittyvät toimenpiteet**	4. Testaa politiikka varmistaaksesi sen varmuus		4. Valvo ja ylläpidä	3. Pyydä muutoksia	5. Katselmoi
Ryhmä 5 **Johdon tukeen ja hyväksyntään liittyvät toimenpiteet**			5. Hanki johdon hyväksyntä		4. Saavuta johdon myötävaikutus
Ryhmä 6 **Henkilöstön tukeen liittyvät toimenpiteet**		11. Vastaa välikohtauksiin			

Yllä olevan taulukon pohjalta Tuyikeze & Pottas (2011) hahmottelivat tietoturvapolitiikan kehittämiselle elinkaaren, joka pitää sisällään seuraavat neljä vaihetta: i. riskiarviointi, ii. politiikan luominen, iii. politiikan toimeenpano ja iv. politiikan valvonta ja ylläpito. Tuyikeze & Pottas (2011) tahtovat muistuttaa, että politiikan kehittäminen on iteratiivinen ja jatkuva prosessi muuttuvan teknologian, liiketoimintaympäristön ja muuttuvien lainsäädännöllisten vaatimusten vuoksi. Tästä johtuen politiikan toimeenpanoa tulisi aina seurata ylläpitoon liittyvät toimenpiteet. Alla oleva Kuvio 2 kuvaa tätä tietoturvapolitiikan kehittämisen elinkaarta. (Tuyikeze & Pottas, 2011).



KUVIO 2 Tietoturvapolitiikan kehittämisen elinkaari (mukaillen Tuyikeze & Pottas, 2011).

Johdon tuki ja hyväksyntä on sijoitettu kuvassa ylälaitaan, sillä se vaikuttaa kaikkiin muihin vaiheisiin kriittisenä komponenttina menestyksekkäälle politiikan kehittämisen elinkaarelle. Organisaation johto on myös lopulta vastuussa organisaation hyvinvoinnista. Ilman johdon tukea tietoturvapolitiikoille, on politiikkojen vaikutus sama, kun jos politiikkoja ei olisi ollenkaan. Politiikat kommunikoidaan henkilöstölle, joka on sijoitettu kuvassa alalaitaan kuvaamaan henkilöstön tukea. Henkilöstön tulee tietää, mitä he voivat tehdä, ja mitä heidän ei tulisi tehdä taatakseen riittävän

turvallisuustason. Tästä johtuen organisaatiolla tulisi olla kommunikaatiostrategia johdolle ja henkilöstölle koko tietoturvapolitiikan kehityksen elinkaaren ajaksi. (Tuyikeze & Pottas, 2011).

Löytääkseen tehokkaimman yhdistelmän erilaisia tietoturvatoimenpiteitä tietylle organisaatiolle, tulee organisaatiolle suorittaa ensin riskianalyysi. Riskianalyysin avulla organisaatiosta saadaan uniikkia tietoa siihen kohdistuvista riskeistä ja kontrolleista. (Wood, 1995). Riskianalyysi tunnistaa sen liiketoiminnan omaisuuden, jonka organisaatio tahtoo turvata. Riskianalyysi myös tunnistaa mahdolliset uhkat, jotka saattaisivat vaikuttaa omaisuuteen. (Tuyikeze & Pottas, 2011). Organisaation tulisikin kysyä itseltään seuraavat kysymykset:

- Mitä tulisi suojata? (esimerkiksi omaisuus)
- Miltä omaisuutta tulisi suojata? (esimerkiksi uhkat ja haavoittuvuudet)
- Kuinka paljon resursseja organisaatio on halukas käyttämään taatakseen riittävän suojauksen?
- Mikä on kustannusten ja hyötyjen suhde liiketoiminnalle?

Tämä vaihe sisältää neljä alavaihetta: i. tunnista omaisuus, ii. tunnista haavoittuvuudet ja uhkat, iii. tiivistä riskiarvioinnin tulokset ja iv. arvioi mahdolliset toimenpiteet ja kontrollit. Nämä vaiheet tulisi suorittaa järjestyksessä, ja niiden tuloksia tulisi käyttää päätettäessä siitä, mitä tietoturvapolitiikkaan lopulta sisällytetään, jotta tunnistetut riskit saadaan hallintaan. Riskiarvioinnin tuloksiin pohjaten johto voi arvioida kustannuksia ja etuja, joita riskien hallitsemiseksi suositeltujen kontrollien toimeenpanemisesta koituu. (Tuyikeze & Pottas, 2011). Tietoturvapolitiikkojen kehittäminen on mahdollista vasta riskiarvioinnin suorittamisen jälkeen. Näin voidaan varmistaa riittävä ymmärrys organisaation erityisistä tarpeista ennen johdolle suunnattujen, yksityiskohtaisten ja kirjallisten ohjeiden tuottamista. Riskiarviointi voidaan suorittaa monella tapaa. Suosittuja tapoja ovat esimerkiksi erilaiset vertailut, kvantitatiiviset riskiarvioinnit, skenaarioanalyysit ja penetraatiohyökkäykset. Riskiarvioinnin tulisi myös luokitella kyseessä olevan tiedon arvo organisaatiolle, kyseiseen tietoon kohdistuvat riskit, sekä nykyiseen tiedon käsittelytapaan liittyvät haavoittuvuudet. (Wood, 1995).

Riskiarvioinnin löydöksien ja suositusten pohjalta on mahdollista aloittaa tietoturvapolitiikkojen luominen. Tässä vaiheessa otetaan huomioon myös liiketoimintastrategia ja –tavoitteet, sekä lainsäädännön vaatimukset. (Tuyikeze & Pottas, 2011). Aloitettaessa tietoturvapolitiikkojen kehittäminen, tulisi kehittäjän tutustua riskiarviointiin, joka osoittaa organisaation tarpeet tietoturvan saralla. Jotta huomiota vaativat alueet voidaan tunnistaa tietoturvapolitiikkojen kehittämistä varten, tulisi kaikki muut voimassa olevat politiikat lukea ensin. Nämä politiikat saattavat liittyä esimerkiksi hankintaprosessiin, työvoimaan, fyysiseen turvallisuuteen tai sovelluskehittämiseen. Monesti myös muiden samalla alalla toimivien organisaatioiden politiikat tarjoavat hyödyllistä tietoa. Jos organisaatio liittyy läheisesti johonkin toiseen organisaatioon, tulisi kehittäjän ottaa huomioon myös tämän organisaation politiikat. Kun taustalukeminen on suoritettu,

voidaan valmistella lista aiheista, joita tietoturvapolitiikan tulisi käsitellä. (Wood, 1995). Wood (1995) ehdottaa, että saatuaan valmiiksi listan aiheista, joita tietoturvapolitiikkojen tulisi käsitellä, ja tutustuttuaan tapaan, jolla organisaatio käyttää politiikkoja, voi kehittäjä luoda matriisin aiheista, joita politiikat tulevat käsittelemään. Tämä kattavuusmatriisi pitää huolen siitä, että tietoturvapolitiikat tulevat varmasti esitetyiksi kaikille asiaankuuluville yleisöille. Matriisia voi tarvittaessa käyttää myös todisteena oikeusjutussa sellaisessa tapauksessa, jossa organisaatiota syytetään riittämättömästä riskien huomioimisesta ja politiikkojen valmistelusta. Matriisia voidaan myös käyttää taustamateriaalina sisäisessä tai ulkoisessa tarkastuksessa. (Wood, 1995).

Tietoturvapolitiikkojen luomiseen sisältyy seuraavat alavaiheet: i. luonnostele yhden sivun mittainen politiikka ja ylätason hahmotelma turvallisuusvaatimuksista, ii. katselmoi ja hyväksy ylätason politiikka, iii. luonnostele tarkemmat politiikat, iv. katselmoi ja hyväksy tarkemmat politiikat, v. julkaise hyväksytyt tietoturvapolitiikat. Tietoturvapolitiikkojen kontrolleille tulisi myös valita sopivat päämäärät, jotka kuvaavat tavoitetilaa, joka voidaan saavuttaa toimeenpanemalla kontrolleihin liittyvät toimenpiteet. Kontrollien päämäärät voivat myös olla tietoturva-alan parhaita käytänteitä, jotka voidaan toimeenpanna käyttämällä vakiintuneita kontrolleja, kuten esimerkiksi ISO 27002. (Tuyikeze & Pottas, 2011). Kehittäjän tulisi myös määrittää se, tuleeko politiikat käyttöön heti vai tulevaisuudessa. Politiikoille tulisi määritellä myös käyttötapa sekä politiikkojen pakottavuuden aste, samoin kuin niiden yksityiskohtaisuus. Myös uusien politiikkojen suhde jo olemassa oleviin politiikkoihin, standardeihin ja proseduureihin tulisi määrittää. (Wood, 1995). Johdolla on tietoturvapolitiikkojen luomisessa keskeinen rooli paitsi niiden katselmoijana ja hyväksyjänä, myös heidän tukensa politiikoille on tärkeää, kun politiikkoja lähdetään kommunikoimaan henkilöstölle. Politiikan luomisvaiheessa olisikin suositeltavaa ylläpitää kommunikointisuunnitelmaa, joka mahdollistaa palautteenannon, sillä tämä valmistaa organisaatiota tuleviin muutoksiin ja antaa yksilöille mahdollisuuden vaikuttaa uuden politiikan kehittämiseen. Yksilöiden osallistuminen on tärkeää, jotta heidät saadaan sitoutettua kaikkiin vaiheisiin aina politiikan valmistelusta sen hyväksyntään ja sitoutumiseen. Uusi politiikka muuttaa aina työntekijöiden työskentelyä, joten sen mukanaan tuomiin muutoksiin on tärkeää kiinnittää huomiota, jotta politiikka voidaan toimeenpanna menestyksekkäästi. Nykyisen ympäristön arviointi olisikin tärkeää, joten seuraavat kysymykset tulisi kysyä politiikan luomisen aikana, jotta henkilöstön kykyä tukea uutta politiikkaa voitaisiin arvioida:

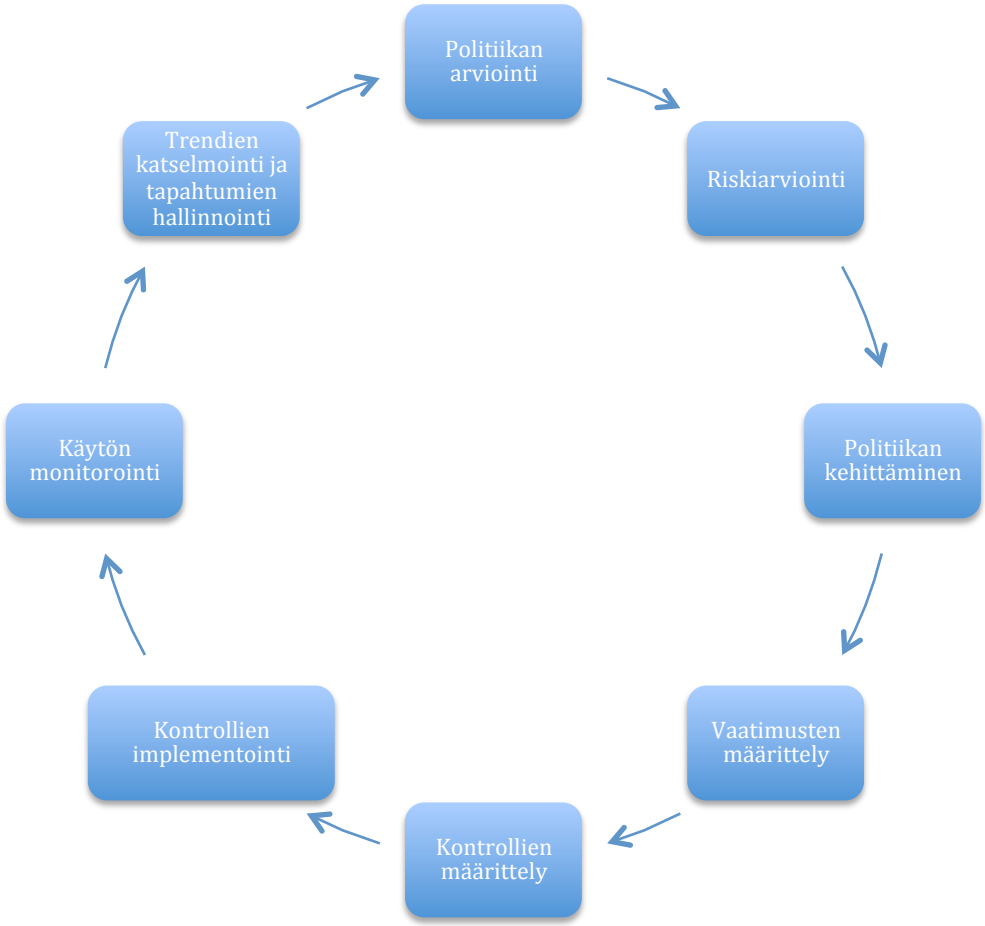
- Keneen muutokset vaikuttaa?
- Onko organisaatiokulttuuri turvallisuuden merkityksen tiedostava?
- Millaisia vaatimuksia kulttuuri asettaa uuden politiikan osien ja toimeenpanoon liittyvien kysymysten esittelylle?
- Mitä odotetaan tapahtuvan, kun uusi politiikka toimeenpannaan?

Edellä mainitut näkökulmat tulee ottaa huomioon politiikan toimeenpanovaiheessa, jotta henkilöstön hyväksyntä ja tuki uudelle politiikalle

voidaan varmistaa. (Tuyikeze & Pottas, 2011). Koska politiikat yleensä koskettavat erilaisia yleisöjä organisaation sisällä, suosittelee Wood (1995) luomaan useita erilaisia versioita politiikoista. Loppukäyttäjille voidaan esimerkiksi luoda oma lyhyempi versionsa, joka sisältää vain olennaisimmat tietoturvapolitiikat. Järjestelmäkehittäjät ja muut teknisemmät työntekijät taas saisivat huomattavasti pidemmän ja yksityiskohtaisemman dokumentin. (Wood, 1995).

Kun politiikka on luotu, voidaan se toimeenpanna. Tätä varten tulisi kehittää yksityiskohtainen toimeenpanosuunnitelma. Tämä vaihe sisältää seuraava alavaiheet: i. määrittele turvallisuus- ja kontrollivaatimukset toimintaohjeiden ja muiden ohjeiden avulla, ii. määrittele tietoturvavastuut, iii. testaa turvallisuus- ja kontrollivaatimukset, iv. toimeenpane turvallisuus- ja kontrollivaatimukset, v. toimeenpane jatkuva koulutus tietoturvapolitiikalle. Tietoturvapolitiikan tulisi olla helposti saatavilla kaikille työntekijöille. Se tulisi kommunikoida kaikille käyttäjille virallisesti, ja käyttäjien tulisi ilmaista, että he ovat tutustuneet ja ymmärtäneet politiikan sisällön ja aikovat noudattaa sitä. Seuraavaksi organisaation tulisi kehittää tietoturvalle tietoisuus- ja koulutusohjelma. Tällainen ohjelma on kriittinen vaihe politiikan toimeenpanossa, sillä niiden tarkoitus on muokata asenteita ja rohkaista työntekijöitä toimimaan aktiivisessa roolissa politiikan toimeenpanossa. (Tuyikeze & Pottas, 2011). Elinkaarimallin viimeistä vaihetta, politiikan valvontaa ja ylläpitoa, käsitellään osuudessa 2.4 Tietoturvapolitiikan ylläpito.

Myös Rees ym. (2003) ovat luoneet elinkaarimallin (PFIRES-malli) tietoturvapolitiikoille. Tämä malli keskittyy riskien analysoimiseen ja kaikkein arvokkaimman omaisuuden suojaamiseen. Elinkaarimalli onkin kehitetty tuotekehityksen elinkaarimallin ja järjestelmäkehityksen elinkaarimallin pohjalta. PFIRES-malli koostuu neljästä vaiheesta: i. arvioi, ii. suunnittele, iii. toimita, iv. käytä. (Rees ym. 2003). Näitä vaiheita kuvataan kuviossa 3.



KUVIO 3 PFIRES-elinkaarimalli (mukaillen Rees ym. 2003).

Politiikan kehittäminen on iteratiivinen prosessi, joten mallin jokaiseen askeleeseen kuuluu lisäksi palautesilmukat. Näin voidaan varmistaa, että edellisen vaiheen vaatimukset on täytetty. (Rees ym. 2003). Organisaation muutos on jatkuvaa, joten sillä on taktinen ja strateginen päätepiste. Taktiset päätökset sisältävät lyhyen aikavälin tavoitteiden saavuttamista, sekä tavoitteiden saavuttamiseen liittyvän prosessin kontrolloimista ja arviointia. Strategiset muutokset taas ovat yleensä laajoja ja sijoittuvat pitkälle aikavälille. Monesti muutoksissa on mukana ylintä johtoa. (Porter, 2008). Useimmissa organisaatioissa muutos sijoittuu näiden kahden päätepisteen välille. (Rees ym. 2003).

TAULUKKO 2 Politiikan elinkaari (mukaillen Rees ym. 2003)

Vaihe	Askel	Välivaihe
Arvioi	Politiikan arviointi	Analysoi politiikan ympäristöä
		Tunnista puutteet ja ristiriidat
		Tee tiivistelmä politiikan arvioinnin tuloksista
		Kehitä suositukset politiikalle
	Riskiarviointi	Turvallisuusarviointi
		Liiketoimintariskin arvioiminen
		Turvallisuussuositusten kehittäminen
		Tiivistelmä arvioinnin tuloksista
Suunnittelu	Politiikan kehittäminen	Kehitä/päivitä turvallisuusstrategia
		Kehitä/päivitä turvallisuuspolitiikka
	Vaatimusten määrittely	Suositusten kääntäminen vaatimuksiksi
		Yksityiskohtaisten turvallisuusvaatimusten kehittäminen
		Vahvista vaatimukset
Toimitus	Kontrollien määrittely	Suunnittele infrastruktuuri
		Määrittele kontrollit
		Arvioi ratkaisut
		Valitse kontrollit
	Kontrollien käyttöönotto	Luo käyttöönottosuunnitelma
		Rakenna
		Testaa
		Pilotointi ja käyttöönotto
Käyttö	Käytön monitorointi	Hallinnointi ja käyttö
		Viestintä
		Tutkinta
		Turvallisuuspalvelut
		Määräystenmukaisuus
	Trendien katselmointi ja tapahtumien hallinnointi	Tapahtumien hallinnointi
		Tunnista ulkopuolisia trendejä
		Tunnista sisäisiä trendejä
		Laajenna arviointivaiheeseen

PFIRES-elinkaarimallissa ensimmäinen vaihe on arviointivaihe. Siihen sisältyy edellä kuvatusta kuviosta askeleet ”Politiikan arviointi” ja ”Riskiarviointi”. Tämän vaiheen voi panna alulle joko päätös suorittaa koko elinkaarimalli alusta alkaen, tai tarve vastata muissa elinkaarimallin askelmissa havaittuun tarpeeseen. Vaiheen tarkoitus on arvioida ehdotettua muutosta senhetkistä politiikkaa ja toimintaympäristöä vasten. Jos organisaatio suorittaa PFIRES-elinkaarimallia ensimmäistä kertaa, on arviointivaihe looginen aloituspiste. Organisaatioiden tulisi kuitenkin katselmoida olemassa olevat politiikat ja suorittaa riskiarviointi ennen turvallisuuspolitiikkojen toimeenpanoa. Politiikkojen katselmointiin tulisi sisällyttää myös organisaation standardit, toimintaohjeet ja muut suositukset. Politiikkojen arviointiin sisältyy neljä

välivaihetta: i. analysoi politiikan ympäristöä, ii. tunnista puutteet ja ristiriidat, iii. tee tiivistelmä politiikan arvioinnin tuloksista ja iv. kehitä suositukset politiikalle. Kun politiikkojen arviointi on suoritettu, voidaan tehdä päätöksiä siitä, mihin kohtaan muutosjatkumoa ehdotetut muutokset sijoittuvat. Sijoittuminen muutosjatkumolla saattaa auttaa määrittämään riskiarvioinnin laajuutta ja täten vaikuttaa seuraavien askelien toimeenpanoon. Mikäli organisaatio suorittaa PFIRES-elinkaarimallia ensimmäistä kertaa, ovat tapahtuvat muutokset strategisia. Muissa tapauksissa muutokset saattavat olla joko strategisia tai taktisia, millä on vaikutusta myös seuraavien vaiheiden läpikäymiseen. Riskiarvioinnin tarkoitus taas on tunnistaa se liiketoiminnan omaisuus, jota tahdotaan suojella. Riskiarvioinnin avulla kyetään tunnistamaan myös potentiaalisia uhkia tälle suojattavalle omaisuudelle. Riskiarviointiin sisältyy useita välivaiheita:

- Turvallisuusarviointi tunnistaa ne elementit ympäristössä, jotka voisivat olla haavoittuvaisia uhkille ja täten vaarantaa omaisuuden.
- Liiketoimintariskin arvioimisella tunnistetaan turvallisuuden kannalta tärkeimmän omaisuuden.
- Turvallisuussuositusten kehittäminen sisältää turvallisuuteen liittyvien vaihtoehtojen tunnistamisen, rahallisten ja muiden kustannusten määrittämisen, vaihtoehtojen priorisoimisen, tulosten varmistamisen ja kustannus-hyötymatriisin kehittämisen.
- Tiivistelmä arvioinnin tuloksista sisältää tulokset sekä riskiarvioinnista että politiikan arvioinnista. Näin johto voi päättää, haluavatko he hyväksyä ehdotetut muutokset. Mikäli johto hyväksyy ehdotetut muutokset, siirrytään elinkaarimallissa seuraavaan vaiheeseen, eli suunnitteluun. Johto saattaa myös hylätä ehdotetut muutokset, mutta havaita, että muunlaisia muutoksia tarvitaan, jolloin siirrytään myös suunnitteluvaiheeseen. Muissa tapauksissa siirrytään takaisin käyttövaiheeseen.

Suunnitteluvaiheessa valmistaudutaan ehdotettujen muutosten täytäntöönpanoon, sisältäen politiikan luomisen tai sen päivittämisen, sekä ehdotettujen muutosten vaatimusten määrittelyn. Suunnitteluvaihe sisältää kaksi askelta, politiikan kehittämisen ja vaatimusten määrittelyn. Politiikan luomiseen liittyvät toimet varmistavat, että organisaatio kehittää turvallisuusstrategiaansa ja turvallisuuspolitiikkaansa yhdessä liiketoimintastrategian ja –politiikan kanssa. Politiikan kehittämiseen liittyy kaksi alavaihetta, luo/päivitä turvallisuusstrategia ja luo/päivitä turvallisuuspolitiikka. Turvallisuusstrategia on katsaus liiketoiminnan suuntaan tulevaisuudessa, sisältäen tarvittavat turvallisuuskontrollit. (Rees ym. 2003). Rees ym. (2003) suositteleekin organisaatioita pitämään ylimmälle johdolle strategiatilaisuuden, jonka aikana voidaan tunnistaa tulevaisuuden liiketoimintahankkeet ja niihin liittyvät riskit ja turvallisuusvaihtoehdot, sekä priorisoimaan turvallisuushankkeet ja dokumentoimaan turvallisuusstrategian. Luodessaan tai päivittäessään turvallisuuspolitiikkaansa organisaation tulisi tunnistaa alueet, jotka turvallisuuspolitiikan tulisi kattaa, jonka jälkeen politiikka voidaan hahmotella, katselmoida ja vihdoin julkaista.

Vaatimusmäärittelyyn sisältyy turvallisuuspolitiikan analysointi, jotta saadaan vaatimukset päivitetylle politiikalle. Vaatimusmäärittely jakautuu kolmeen välivaiheeseen: i. suositusten kääntäminen vaatimuksiksi, ii. yksityiskohtaisten turvallisuusvaatimusten kehittäminen ja iii. vaatimusten vahvistaminen. Suositusten kääntämisellä vaatimuksiksi tarkoitetaan sitä, että korkean tason prioriteetteja jotka kehitettiin riskiarvioinnin aikana, käytetään sellaisen turvallisuusinfrastruktuurin rakentamisessa, mikä voi tukea muutosta. Yksityiskohtaisia turvallisuusvaatimuksia kehitettäessä korkean tason vaatimuksia aiemmasta välivaiheesta tarkennetaan, jotta niille voidaan alkaa valita sopivia kontrolleja. Tämä välivaihe ottaa teknisen ympäristön huomioon, jotta ehdotettu muutos tukee olemassa olevaa ympäristöä. Vaatimuksia vahvistettaessa varmistetaan, että kaikki vaatimukset pohjautuvat tiettyyn riskiin, joita määriteltiin aiemmin riskiarvioinnin yhteydessä. Vaatimuksia tulisi myös arvioida alan parhaita käytänteitä vasten. Myös tietyt lait tulisi ottaa tässä vaiheessa huomioon. (Rees ym. 2003).

Toimitusvaiheessa politiikka otetaan käyttöön. Toimitusvaihe koostuu kahdesta välivaiheesta, kontrollien määrittelystä ja kontrollien käyttöönotosta. Kontrollit ovat käytäntöjä, tapoja tai mekanismeja, jotka vähentävät turvallisuusriskiä. Kontrollien määrittely määrittelee ne kontrollit, joita tarvitaan turvallisuuspolitiikan vaatimusten noudattamiseksi. Kontrollien määrittely jakautuu neljään välivaiheeseen: i. suunnittele infrastruktuuri, ii. määrittele kontrollit, iii. arvioi ratkaisut ja iv. valitse kontrollit. (Rees ym. 2003). Nämä välivaiheet ovat peräkkäisiä ja noudattavat yleisesti käytettyä järjestelmäkehityksen elinkaarta (Hoffer ym. 1999). Infrastruktuurin suunnittelussa käytetään vaatimuksia suunnitteluvaiheesta korkean tason turvallisuusinfrastruktuurin suunnitteluun, sisältäen esimerkiksi tekniset tekijät, toimintatavat ja organisatoriset tekijät. Kontrollien määritellyssä korkean tason suunnitelmat käännetään kontrolleiksi ja niiden vaatimuksiksi. Vaihtoehtojen arviointi taas liittyy siihen, että organisaatiolle valitaan parhaat ratkaisut markkinoilta, jotta vaatimuksiin voidaan vastata. Tämän jälkeen voidaan valita sopivat kontrollit, jotka vastaavat parhaiten kontrollien vaatimuksiin. Lopulta kontrolleja voidaan ottaa käyttöön. Käyttöönottoon liittyy kolme toimintoa: i. rakentaminen, ii. testaus ja iii. lopullisen turvallisuus infrastruktuurin käyttöönotto. Käyttöönotto voidaan suorittaa neljän välivaiheen kautta: i. luo käyttöönottosuunnitelma, ii. rakenna, iii. testaa ja iv. pilotoi ja käyttöönota. Käyttöönottosuunnitelma luodaan, jotta suunnitelma saadaan tuotua todellisuuteen. Kunnollisen suunnitelman avulla turvallisuusinfrastruktuuri on todennäköisemmin rakennettu ajallaan ja vaatimusten mukaan. Rakennusvaihe riippuu paljon valituista kontrolleista, mutta yleensä tässä vaiheessa kehitetään yksityiskohtaiset toimintatavat ja riittävä tuki. Tämä vaihe sisältää myös koulutusmateriaalin, kuten manuaalien ja tukitiedostojen, kehittämisen. Kun turvallisuusinfrastruktuuri on rakennettu, tulee se testata. Näin varmistetaan, että suunnitelmat on toteutettu kuten piti, ja uhkat on otettu huomioon. Tässä välivaiheessa suoritetaan kolmenlaista testaamista: i. haavoittuvuuksien arviointia, ii. turvallisuusinfrastruktuurin vahvistusta ja iii. ohjelmistojen turvallisuuden testaamista. Kun turvallisuusinfrastruktuuri on testattu, voidaan se levittää tuotantoympäristöön. Pilotoinnin tarve riippuu käyttöönoton

laajuudesta. Käyttöönotto sisältää turvallisuusarkkitehtuurin komponenttien konfiguroinnin ja asentamisen, sekä uusien prosessien ja toimintatapojen viestimisen ja kouluttamisen. Käyttöönoton tulisi varmistaa, että politiikassa esiteltyjä turvallisuusvaatimuksia noudatetaan. (Rees ym. 2003).

Käyttövaihe tapahtuu päivittäin ja sen tarkoitus on monitoroida niitä kontrolleja, jotka on sijoitettu organisaatioon, sekä hoitaa vastatoimet, kun poikkeuksia ilmenee. Vaiheeseen sisältyy lisäksi liiketoimintaan ja teknologiaan liittyvien trendien seuraaminen ja analysointi. Monitoroinnin tarkoituksena on määritellä organisaation päivittäiset toimet, jotta voidaan varmistaa turvallisuuspolitiikan käyttö koko turvallisuusinfrastruktuurissa. Hallinnointi ja käyttö sisältää esimerkiksi käyttäjien hallinnoinnin ja korjaustiedostojen arvioinnin ja lisäämisen. Viestinnällä on merkittävä rooli monitoroinnissa, sillä erilaisille yleisöille tulee viestiä eri tavalla. Monitorointiin sisältyy myös erilaiset tutkinnat, joiden yhteydessä tarkastellaan tietoturvapoikkeamia, niiden syitä sekä mahdollisia vastatoimia. Turvallisuuspalveluilla tarkoitetaan monitoroinnin yhteydessä palvelua, joka tarjoaa turvallisuusspesialistin projektiryhmien käyttöön. Turvallisuusspesialisti voi tulla joko organisaation sisältä tai ulkoiselta palveluntarjoajalta. Määräystenmukaisuudella tarkoitetaan niitä toimia, jotka varmistavat, että infrastruktuuri seuraa turvallisuuspolitiikan ohjeita. Monesti määräystenmukaisuuden seuraamisesta on vastuussa sisäinen tarkastus, mutta prosessin tulisi olla proaktiivisempi kuin neljä kertaa vuodessa tapahtuva sisäinen tarkastus. Käyttövaiheen toinen askel on trendien katselmointi ja tapahtumien hallinnointi, johon sisältyy neljä välivaihetta: i. tapahtumien hallinnointi, ii. ulkopuolisten trendien tunnistaminen, iii. sisäisten trendien tunnistaminen ja iv. arviointivaiheeseen laajentaminen. Toisin kuin monitorointiin liittyvät välivaiheet, näiden välivaiheiden ei tarvitse tapahtua järjestyksessä, vaikkakin arviointivaiheeseen laajentaminen on aina viimeinen välivaihe. Tähän askeleeseen kuuluu niiden tapahtumien tai trendien tunnistaminen, jotka saattaisivat aiheuttaa tarpeen turvallisuuspolitiikan uudelleenarvioinnille. (Rees ym. 2003). Rees ym. (2003) toteavat, että turvallisuuspolitiikalla, jota ei säännöllisesti arvioida ja päivitetä, ole arvoa organisaatiolle. Tapahtumien hallinnalla tarkoitetaan organisaatiolle epänormaalien tilanteiden hallintaa. Nämä tilanteet saattavat hyvin ennustettavissa ja kontrolloitavissa, mutta toisaalta ne saattavat olla hyvin odottamattomia ja haastavia. Etenkin odottamattomat tilanteet vaativat usein tietoturvapoikkeamaan vastaavan prosessin tuekseen. Ulkopuolisten trendien tunnistamisella pyritään havaitsemaan kehityssuuntia, jotka saattavat vaatia turvallisuuspolitiikan uudelleenarviointia. Kehityssuuntien tunnistamisessa tärkein tekijä on sellaisen tiedon tunnistaminen, jolla saattaa olla turvallisuuden kannalta merkitystä. Sisäiset trendit liittyvät usein uusiin liiketoimintamahdollisuuksiin, uusiin kyvykkyyksiin tai uusiin sovelluksiin. Kun muutoksia organisaatiossa havaitaan, pitää vielä päättää, laajennetaanko prosessia arviointivaiheeseen. Tässä vaiheessa tulisi käyttää tervettä järkeä ja jonkinlaisia kriteerejä. Ainakin muutosten laajuutta, aikataulua ja sekä organisaation yleistä toiminta-alttiutta, eli tarvittavaa tukea muilta liiketoimintayksiköiltä. (Rees ym. 2003).

2.3.3 Tietoturvapolitiikkojen ylläpito

Keskeinen osa tietoturvapolitiikan tehokkuutta on sen päivittäminen. (Höne & Eloff, 2002). On kuitenkin havaittu, että monesti politiikkojen päivittämiselle ei anneta riittävästi huomiota. Huolimatta siitä, että useissa organisaatiossa tietoturvapolitiikkojen kehittämiseen käytetään merkittäviä määriä resursseja, ei tietoturvapolitiikkojen käyttö kuitenkaan aina onnistu. Tietoturvapolitiikat saatetaan monesti julkaista organisaation käyttöön, mutta niitä ei katselmoida säännöllisesti, jotta esimerkiksi muuttunut lainsäädäntö tai muuttunut liiketoimintaympäristö saataisiin sisällytettyä politiikkaan. Tämä johtaa välillä oikeudellisten velvollisuuksien laiminlyömiseen ja vanhentuneisiin politiikkoihin. Kuitenkin tietoturvapolitiikkojen päivitys ja niiden noudattamisen tarkkailu ovat vähintään yhtä tärkeitä toimenpiteitä, kuin tietoturvapolitiikkojen kehittäminen. (Tuyikeze & Pottas, 2011).

Lopes & Sá-Soares (2012) toteavatkin, että tutkimistaan 25 politiikasta vain yksi määrittelee, milloin kyseinen dokumentti tulisi katselmoida uudelleen. Myös Tuyikeze & Pottas (2011) havaitsivat, että tietoturvapolitiikkojen päivitystoimet eivät monesti saa tarvitsemaansa huomiota.

Wood (1995) suosittelee katselmoimaan voimassa olevat tietoturvapolitiikat vuosittain. Wood (1995) toteaa myös, että politiikkoja ei tarvitsi uusia kuin viiden vuoden välein, mutta toisaalta politiikkoja tulisi välillä muokata vastaamaan paremmin esimerkiksi muuttuneeseen teknologiaan, lakeihin ja asetuksiin. Myös Mattord & Whitman (2004) kehottavat sisällyttämään politiikkoihin niiden katselmointiaikataulun.

Tuyikeze & Pottas (2011) kehittivät mallin tietoturvapolitiikkojen kehittämisen elinkaarelle. Elinkaarta esitellään tämän tutkielman kappaleessa 2.3.2 Tietoturvapolitiikan kehittämisprosessi tarkemmin, mutta mallin viimeinen komponentti, politiikan valvominen ja ylläpito, käsitellään tässä kappaleessa. Kun tietoturvapolitiikka on toimeenpantu, tulisi organisaation sisällyttää siihen sopivat valvontamekanismit, jotta voidaan varmistaa, että politiikkaa todella on toimeenpantu koko organisaatiossa. Seuraavat alavaiheet tulisi toteuttaa tässä vaiheessa: i. tuota mitattavia tuloksia kuvaamaan käyttäjien käytöstä, ii. toteuta järjestelmän auditointeja ja katselmointeja, iii. testaa tunkeutumisen havainnointia ja suorita penetraatiotestejä, iv. analysoi käyttäjien suorittamien toimien auditointijälkeä, sekä v. auditoi politiikan noudattamista. Valvonnan päätavoite on varmistaa, että henkilöstö noudattaa uutta politiikkaa ja sen vaatimuksia. Politiikan vaatimusten noudattaminen on välttämätöntä, kun pyritään turvaamaan tietoturvapolitiikkojen vakaus. (Tuyikeze & Pottas, 2011)

Politiikan ylläpito pitää sisällään seuraavat alavaiheet: i. katselmoi raportit, jotka liittyvät tietoturvatapauksiin, ii. katselmoi turvallisuus- ja teknologiainfrastruktuuria, iii. katselmoi liiketoimintastrategioita, iv. katselmoi kehityssuuntaa ja odottamattomia tapahtumia, v. katselmoi lainsäädännöllisiä vaatimuksia, vi. laadi ehdotuksia politiikkojen muutoksista, sekä vii. toista tietoturvapolitiikan kehittämisen elinkaarta. Organisaation turvallisuusinfrastruktuuria on tärkeää katselmoida säännöllisesti, jotta mahdolliset uhkat voidaan tunnistaa. Nämä uhkat saattavat johtua myös

tietyistä teknologioista, joita käytetään jossain osassa organisaatiota. On myös mahdollista, että uudet vaatimukset lainsäädännössä pitää ottaa huomioon organisaation tietoturvapolitiikoissa. Näistä ja monista muista syistä johtuen organisaation tietoturvapolitiikat saattavat vanhentua. Politiikat tulee siis päivittää ja tarvittavat muutokset pitää tehdä. Näitä muutoksia tehdään ylläpitovaiheessa. Ylläpitovaiheessa tulisi käydä uudelleen läpi myös muut elinkaarimallissa esitellyt vaiheet, eli riskiarviointi, politiikan luominen ja politiikan toimeenpano, jotta muutoksia politiikkoihin ei tehdä hätäisesti. Tähän vaiheeseen liittyy paljon epävarmuutta, ja monesti organisaatio saattaakin havaita uuden uhkan jota ei otettu huomioon politiikan päivittämisessä, tai esimerkiksi havaita tarpeen uudelle teknologialle. (Tuyikeze & Pottas, 2011)

Politiikan valvomisen ja ylläpidon kannalta on tärkeää, että johto tarkistaa riittävien menettelytapojen ja järjestelmien senhetkisen tilanteen. Näin voidaan varmistaa, että henkilöstö ymmärtää toimeenpannut politiikat ja menettelytavat, sekä sen, että politiikkoja ja menettelytapoja todella seurataan. Johdon tulee myös varmistaa, että politiikan noudattamatta jättämisellä on seurauksensa. Rangaistuksia tuleekin jakaa järjestelmällisesti, ja niiden sisältö tulisi kommunikoida henkilöstölle. (Tuyikeze & Pottas, 2011)

Voidaan siis sanoa, että tietoturvapolitiikan kehittäminen ei ole kerralla suoritettava toimenpide, vaan se vaatii jatkuvaa sitoutumista, jotta voidaan varmistaa että politiikat luovat merkitystä organisaatiolle. Tämä voidaan saavuttaa tutkielmassa esiteltyjen tietoturvapolitiikan kehittämisen elinkaarimallin avulla. Voidaan myös sanoa, että jos politiikka on käynyt elinkaarimallin läpi useamman kerran, on se kypsempi sekä tukemaan organisaation turvallisuusvaatimuksia, mutta myös operationaalisesti juurtuneempi, sillä organisaatiossa on olemassa sopivat menettelytavat, jotka ohjaavat sen toimeenpanoa. Kyseinen malli varmistaa myös, että politiikka ei ole kehittämisen ainoa lopputuote, vaan kehittäminen tuo mukanaan myös pysyvyyttä ja varmuutta, sekä vakuuden siitä, että politiikkaa myös noudatetaan. (Tuyikeze & Pottas, 2011).

3 YLEINEN TIETOSUOJA-ASETUS

Tämä luku käsittelee henkilötietojen arvoa, Euroopan Unionin yleistä tietosuoja-asetusta, sen vaikutusaluetta ja merkittävimpiä muutoksia lainsäädäntöön.

3.1 Henkilötietojen arvo

Henkilötietoja on kuvattu esimerkiksi digitaalisen maailman valuutaksi, sillä henkilötietoja kerätään yhä enenemissä määrin ja niitä käytetään kaupallisiin tarkoituksiin. Henkilötiedoilla voidaankin nähdä olevan rahallista arvoa, mutta toisaalta henkilötiedot liittyvät olennaisesti yksityisyyteen. (Baars, 2016).

Nykypäivänä valtavista määristä dataa on mahdollista yhdistellä tietoa, jotka voidaan yhdistää tiettyyn yksilöön. Tällainen data on luonnollisesti kiinnostavaa esimerkiksi mainostajille, mutta myös muille yrityksille. Henkilötietojen hyödyntäminen onkin herättänyt paljon kysymyksiä, josta todisteena toimii EU:n yleisen tietosuoja-asetuksen hyväksyminen. Yleisen tietosuoja-asetuksen olisikin tarkoitus antaa valta henkilötietojen hallitsemisesta takaisin yksilölle. Yleisen tietosuoja-asetuksen riittävyys tarjota yksilöille valta henkilötietojensa hallitsemisesta on kuitenkin kyseenalaistettu, ja on ehdotettu, että myös kilpailulainsäädännössä tulisi ottaa kantaa yksityisyyteen. (Baars, 2016).

Yksi ongelma henkilötietoihin liittyen on se, ettei henkilötietojen arvoa tunneta. Henkilötietojen arvon arvioimisen keinot voidaan tyypillisesti jakaa kahteen luokkaan, markkinoiden arvioon ja yksilön arvioon. Henkilötietojen arvoa voidaan esimerkiksi verrata siihen hintaan, jolla datanvälittäjät tarjoavat niitä markkinoille. Toinen keino arvioida henkilötietojen arvoa on verrata sitä siihen hintaan, jonka yritykset ovat valmiita maksamaan yksilöille henkilötietojensa käytöstä. (Baars, 2016). Tämän metodin ongelmana on kuitenkin se, että yksilöt eivät usein osaa arvioida henkilötietojensa arvoa (Froomkin, 2000). Froomkin (2000) kutsui tätä ilmiötä yksityisyyden lyhytnäköisyydeksi. Vaikka yleinen tietosuoja-asetus pyrkii antamaan yksilöille

takaisin hallinnan henkilötietojensa suhteen, on silti huomattava, että siihen liittyy haasteita. Ihmiset eivät esimerkiksi ole kovin hyviä tekemään rationaalisia päätöksiä, kun heidän saamansa informaatio on vaikeaselkoista, ja kun saatavilla on mahdollisuus nopeaan hyötyyn, jonka kustannukset on pitkälle ajalle jakautuvia. (Moerel, 2014).

3.2 Yleisen tietosuoja-asetuksen tausta

Friedin (1984) mukaan yksityisyys on ”moraalista pääomaa”, jota käytetään suhteiden luomiseen. Tästä johtuen yhteiskunnan tulisi mahdollistaa tietosuoja. Yksilöiden tulee kuitenkin jakaa tietty määrä henkilötietoa, jotta yhteiskunnan on mahdollista toimia. (Smith, 1993). Lissabonin sopimuksen mukaan jokaisella on oikeus henkilötietojensa suojaan. Euroopan unionin perusoikeuskirjan mukaan henkilötietojen suoja onkin perusoikeus. (Euroopan komissio, 2012).

Euroopan Unionin nykyinen tietosuojalainsäädännön keskeinen säädös, direktiivi 95/46/EC, tuli voimaan vuonna 1995. Direktiivillä oli kaksi tavoitetta: suojata tietosuojaa koskeva perusoikeus ja taata henkilötietojen vapaa liikkuvuus EU:n jäsenvaltioiden välillä. (Euroopan komissio, 2012). EU:n yleinen tietosuoja-asetus tulee korvaamaan kyseisen direktiivin (De Hert & Papakonstantinou, 2012).

Teknologian nopea kehitys tuo kuitenkin mukanaan uusia haasteita henkilötietojen suojeluun, sillä tietoja jaetaan ja kerätään nykyään enemmän kuin ennen. Teknologian kehityksen vuoksi sekä yksityiset yritykset kuin viranomaisetkin voivat käyttää henkilötietoja aiempaa laajemmin. (Euroopan komissio, 2012). Aiemmin datan kerääminen oli aikaavievää ja raskasta, mutta nykyään datan käsittely vie vain sekunteja (Baars, 2016). Samaan aikaan luottamuksen rakentaminen verkkoympäristöön olisi sekä talouden että kehityksen kannalta suotavaa. Luottamuspulan vuoksi kuluttajat saattavat suhtautua uusiin verkkopalveluihin epäluuloisesti, jopa siinä mittakaavassa, että se uhkaa hidastaa uusien teknologioiden uusien, innovatiivisten käyttötapojen kehittämistä. Tästä syystä henkilötietojen suoja on koettu tärkeäksi Euroopan digistrategiassa. (Euroopan komissio, 2012).

Näistä syistä Eurooppa-neuvosto kehotti komissiota arvioimaan EU:n tietosuojasäädösten toimivuutta ja tarvittaessa esittämään lainsäädäntöä koskevia ehdotuksia. Euroopan parlamentti katsoikin päätöslauselmassaan, että EU:ssa tulisi laatia kattava järjestelmä henkilötietojen turvaamiseksi. (Euroopan komissio, 2012). Komissio katsoi, että EU:ssa olisi tarvetta nykyistä kattavammalle ja johdonmukaisemmalle politiikalle henkilötietojen suojaa koskevan perusoikeuden toteuttamiseksi (Euroopan komissio, 2010). Nykyinen tietosuojakehys on edelleen pätevä tavoitteiden ja periaatteeiden osalta, mutta sen avulla ei ole pystytty estämään henkilötietojen suojan täytäntöönpanon hajanaisuutta eri puolilla Euroopan unionia, eikä myöskään oikeudellista epävarmuutta tai laajalle levinnyttä näkemystä siitä, että erityisesti verkkoympäristössä toimimiseen liittyy merkittäviä riskejä. EU:lle tulikin laatia vahvempi ja johdonmukaisempi tietosuojakehys, jotta digitaalitalous voi

kehittyä sisämarkkinoiden alueella, ja jotta yksilöt voivat valvoa omia tietojaan. Etenkin talouden toimijat ovat arvostelleet EU:n nykyisen henkilötietojen suojan hajanaisuutta ja vaatineet tietosuojasääntöjen yhtenäistämistä. Talouden toimijat katsoivat myös, että henkilötietojen kansainvälisiin siirtoihin liittyvien sääntöjen monimutkaisuus haittaa niiden toimintaa, koska niiden on säännöllisesti siirrettävä henkilötietoja EU:n ulkopuolelle. (Euroopan komissio, 2012).

Tammikuussa 2012 Euroopan komissio ehdottikin EU:n henkilötietokehyksen uudistamista esittelemällä ehdotuksen tietosuoja-asetuksesta. (Baars, 2016). Euroopan komissio on asettanut yleiselle tietosuoja-asetukselle kolme toimintatavoitetta, joiden avulla pyritään parantamaan sisämarkkinaulottuvuutta, tehostamaan yksilöiden tietosuojaoikeuksien käyttöä ja luomaan kattava ja johdonmukainen säädöskehys. (Euroopan komissio, 2012). Yleinen tietosuoja-asetus vahvistaa etenkin rekisteröidyn määritelmää, ja ottaa samalla huomioon lisääntyneen internetin käytön. (De Hert & Papakonstantinou, 2012).

3.3 Yleisen tietosuoja-asetuksen vaikutusalue

Puhuttaessa henkilötietojen käsittelystä sekä siitä, onko yleinen tietosuoja-asetus käyttökelpoinen puhuttaessa tietystä tiedosta, on tärkeää määritellä myös se, mikä oikeastaan on henkilötietoa. Yleisen tietosuoja-asetuksen vaatimukset koskevat henkilöihin liittyvän tiedon käsittelyä. (De Hert & Papakonstantinou, 2012). Henkilötiedoksi määritellään sellainen tieto, joka liittyy rekisteröityyn yksilöön siten, että rekisteröity on siitä tunnistettavissa. Ratkaistaessa sitä, onko henkilö tunnistettavissa, tulisi ottaa huomioon kaikki keinot, joita joko rekisterinpitäjä tai muu henkilö voi kohtuuden rajoissa käyttää mainitun henkilön tunnistamiseksi. (Euroopan komissio, 2010; Baars, 2016). Myös esimerkiksi paikkatiedot ja IP osoitteet voivat siis olla henkilötietoa. (De Hert & Papakonstantinou, 2012).

Yleinen tietosuoja-asetus nostaa erikseen esiin myös arkaluontoisen henkilötiedon, jonka käsittelyä rajoitetaan enemmän, kuin tavallisten henkilötietojen. Arkaluontoisella henkilötiedolla voidaan viitata esimerkiksi uskonnolliseen vakaukseen, poliittiseen kantaan tai vaikkapa rikosrekisteriin. (Baars, 2016; De Hert & Papakonstantinou, 2012). Ehdot arkaluontoisen henkilötiedon käsittelyyn ovat tiukemmat, kuin muille henkilötiedoille. Yleisen tietosuoja-asetuksen mukaan rekisteröidyn tulee antaa yksiselitteinen suostumus arkaluontoisten henkilötietojen käsittelylle. (Baars, 2016).

Yleinen tietosuoja-asetus tulee olemaan yhteinen kaikille Euroopan unionin jäsenmaille. Näin ollen organisaatioiden on tulevaisuudessa helpompi ymmärtää muiden Euroopan unioniin kuuluvien maiden tietosuojalainsäädäntöä. Yleinen tietosuoja-asetus lisää organisaatioiden velvoitteita ja lisää yksilöiden oikeuksia, mutta samalla myös poistaa tiettyjä hallinnollisia taakkoja, joiden arvioidaan nykyisellään maksavan miljardeja euroja organisaatioille. (Gilbert, 2011). Soveltamisen alettua yleinen tietosuoja-

asetus tulee vaikuttamaan kaikkiin organisaatioihin, joilla on EU-alueella liiketoimintaa, johon liittyy henkilötietojen käsittelyä. Yleinen tietosuoja-asetus tulee vaikuttamaan myös organisaatioihin, jotka eivät varsinaisesti harjoita liiketoimintaa EU-alueella, mutta jotka käsittelevät EU-kansalaisen henkilötietoja liittyen organisaation tuotteisiin tai palveluihin. (Bird & Bird, 2016).

Vaikka kyseessä on asetus, antaa yleinen tietosuoja-asetus silti jäsenmaille mahdollisuuden säännellä asetuksen vaikutusta monilla osa-alueilla. Tämä saattaa hankaloittaa Euroopan komission pyrkimyksiä yhdenmukaistaa henkilötietojen käsittelyä jäsenmaissa. (Bird & Bird, 2016).

3.4 Yleisen tietosuoja-asetuksen aiheuttamat muutokset

Vuonna 2018 voimaantulevan EU:n yleisen tietosuoja-asetuksen aiheuttamat muutokset ovat merkittäviä ja kunnianhimoisia. Se on yksi laaja-alaisimpia EU:n lakimuutoksia viimevuosien ajalta. (Bird & Bird, 2016). Yleinen tietosuoja-asetus tulee korvaamaan EU:n koko nykyisen tietosuojarakennelman. Direktiivin 95/46/EC korvaaminen on tärkeä ja kauaskantoinen kehitysaskel, sillä voimaantullessaan yleinen tietosuoja-asetus tulee eurooppalaisten tapaan työskennellä ja elää yhdessä. (De Hert & Papakonstantinou, 2012).

Tietosuojan periaatteet pysyvät aiempaan lainsäädäntöön verrattuna melko samanlaisena, mutta yleinen tietosuoja-asetus pyrkii antamaan yksilölle aiempaa enemmän valtaa hallita henkilötietojaan. Yleinen tietosuoja-asetus lisääkin yksilön oikeuksia varmistaakseen tämän pyrkimyksen. (Baars, 2016). Yleisen tietosuoja-asetuksen vaatimukset tulevat velvoittamaan organisaatioilta esimerkiksi politiikkojen ja toimintaohjeiden kehittämistä, dokumentointia ja järjestelmätason muutoksia. Organisaatioiden tulee myös tulevaisuudessa ilmoittaa tietomurroista, sekä luoda suunnitelmia erilaistan tietoturvahäiriöiden varalta. (Gilbert, 2011). Seuraavaksi esitellään yleisen tietosuoja-asetuksen mukanaan tuomia merkittävimpiä muutoksia, mutta on huomioitava, että lista ei kata kaikkia tulevia muutoksia tietosuojalainsäädäntöön.

3.4.1 Rekisterinpitäjä ja henkilötietojen käsittelijä

Henkilötietojen käsittelyn syistä ja keinoista vastaavaa tahoa kutsutaan yleisessä tietosuoja-asetuksessa rekisterinpitäjäksi. Rekisterinpitäjänä voi toimia yksi tai useampi taho. Rekisterinpitäjä on vastuussa lainsäädännön noudattamisesta henkilötietoja käsiteltäessä. Noudattaakseen lainsäädäntöä, on rekisterinpitäjän varmistettava riittävä tietoturvan taso ja organisaation prosessien turvallisuus, sekä rekisteröityjen mahdollisiin pyyntöihin vastaaminen. (Baars, 2016).

Rekisterinpitäjät taas ohjeistavat henkilötietojen käsittelijää käsittelemään henkilötietoja puolestaan. Henkilötietojen käsittelijää rajoittavat ne ohjeet, joita

rekisterinpitäjä on käsittelijälle tarjonnut. Monesti nämä käsittelyohjeet sisältyvät esimerkiksi sopimukseen. (Baars, 2016).

Yleistä tietosuoja-asetusta edeltäneen henkilötietodirektiivin aikana henkilötietojen käsittelijää ei pidetty vastuussa mahdollisesta lainvastaisesta henkilötietojen käsittelystä, mutta yleisen tietosuoja-asetuksen soveltamisen alettua toukokuussa 2018, tulee tämä muuttumaan. Yleinen tietosuoja-asetus esittelee jaetun vastuun käsitteen, jonka vuoksi rekisterinpitäjän ja henkilötietojen käsittelijän vastuista tulisi määrätä tarkasti. Rekisterinpitäjää voidaan pitää vastuussa vahingoista, jotka koituivat lainsäädännön noudattamatta jättämisestä. Henkilötietojen käsittelijää voidaan pitää vastuussa vain käsittelystä, joka ei noudata yleisen tietosuoja-asetuksen vaatimuksia tai rekisterinpitäjältä saatuja ohjeita käsittelylle. Rekisteröidyt voivat vaatia korvauksia sekä rekisterinpitäjältä, että henkilötietojen käsittelijältä. (Baars, 2016).

3.4.2 Henkilötietojen käsittelyn oikeudellinen peruste

Henkilötietojen käsittely on yleisen tietosuoja-asetuksen mukaan sallittua vain, kun sillä on oikeudellinen peruste. Käsittelylle on kuusi erilaista perustetta: i. suostumus, ii. käsittely on välttämätöntä sopimuksen vaatimusten noudattamiseksi, iii. käsittely on välttämätöntä lainsäädännön noudattamiseksi, iv. käsittely on välttämätöntä rekisteröidyn hengen kannalta olennaisten etujen suojelemiseksi, v. käsittely on välttämätöntä yleisen edun vuoksi toteutettavan tehtävän vuoksi tai vi. kun käsittely on välttämätöntä rekisterinpitäjän oikeutetun edun vuoksi. (Baars, 2016).

Suostumuksella tarkoitetaan selkeästi ilmaistavaa toimea, jolla rekisteröity antaa vapaaehtoisen, yksilöidyn, tietoisen ja yksiselitteiden tahdonilmaisun, jolla hän hyväksyy henkilötietojensa käsittelyn (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016 ja Gilbert, 2011). Tarkkaa muotoa suostumuksen antamiselle ei ole määritelty, vaan suostumusta voidaan osoittaa missä tahansa muodossa (Article 29 Data Protection Working Party, 2011). Passiivista toimintaa ei kuitenkaan voida katsoa suostumukseksi. (Baars, 2016). Organisaatioille tämä tarkoittaa sitä, että niillä on vastuu osoittaa rekisteröidyn todella antaneen suostumuksensa henkilötietojensa käsittelyyn. Organisaatioiden tuleekin kehittää tapa pitää kirjaa rekisteröidyiltä saaduista suostumuksista. (Gilbert, 2011). Vaikka yleinen tietosuoja-asetus ei aseta henkilötietojen käsittelyn oikeudellisia perusteita arvojärjestykseen, on suostumuksen arvioitu olevan keskeisin oikeudellisista perusteista, sillä sen katsotaan antavan rekisteröidyille suurin mahdollinen valta määrätä henkilötietojensa käsittelystä. (Baars, 2016).

Henkilötietojen käsittely on laillista myös silloin, kun se on välttämätöntä rekisterinpitäjän, tai kolmannen osapuolen, jolle henkilötiedot on luovutettu, oikeutetun edun vuoksi. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Oikeutetun edun tulee perustua laillisuuteen, olla riittävän yksityiskohtainen, eikä se saa olla spekulatiivinen. (Article 29 Data Protection Working Party, 2014). Oikeutettuun etuun perustuva käsittely vaatii

rekisterinpitäjää tasapainottelemaan oman etunsa, tai kolmannen osapuolen, sekä rekisteröidyn edun välillä. Jos henkilötietojen käsittelyyn liittyy merkittävä tietosuojariski, tulee rekisteröidyn oikeutettua etua pitää etusijalla olevana asiana. Tällaisessa tilanteessa rekisteröidyltä tulisikin pyytää yksiselitteistä suostumusta. (Baars, 2016).

3.4.3 Tietosuojaperiaatteet

Yleisen tietosuoja-asetuksen toisen luvun viidennessä artiklassa säädetään henkilötietojen käsittelyä koskevista periaatteista (Euroopan komissio, 2012). Yleinen tietosuoja-asetus esittelee joukon periaatteita, joista monet ovat tuttuja jo aiemmasta tietosuojalainsäädännöstä, eli tietosuojadirektiivistä (Bird & Bird, 2016; Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Uusia elementtejä lainsäädäntöön tuovat erityisesti läpinäkyvyysperiaate, tietojen minimoinnin periaate sekä rekisterinpitäjän kattavan vastuun vahvistaminen. (Euroopan komissio, 2012).

Henkilötietoja tulisikin käsitellä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Henkilötietoja saa kerätä vain tiettyä laillista tarkoitusta varten, eikä niitä saisi käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Tätä periaatetta kutsutaan myös käyttötarkoitussidonnaisuudeksi. Myös tietojen minimoinnin periaate on uusi, ja sillä tarkoitetaan sitä, että henkilötietojen tulee olla riittäviä, relevantteja ja rajoitettu vain niihin, joita todella tarvitaan sellaiseen käyttöön, jonka vuoksi kyseisiä henkilötietoja käsitellään. Henkilötietoja olisi säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan, kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Yleinen tietosuoja-asetus tulee siis rajoittamaan myös henkilötietojen säilytystä. Samaan aikaan henkilötietoja olisi käsiteltävä tavalla, jolla varmistetaan henkilötietojen turvallisuus ja suojaaminen luvattomalta ja lainvastaiselta käsittelyltä, sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta ja vahingoittumiselta. Organisaatioiden tuleekin käyttää asianmukaisia teknisiä ja organisatorisia toimia suojatakseen henkilötietoja. (Bird & Bird, 2016; Euroopan parlamentti ja Euroopan unionin neuvosto, 2016 ja Gilbert, 2011).

Yksi keskeisimmistä muutoksista on osoitusvelvollisuus, joka tarkoittaa sitä, että organisaation tulee olla kykenevä osoittamaan noudattavansa yleisen tietosuoja-asetuksen vaatimuksia. (Bird & Bird, 2016; Euroopan parlamentti ja Euroopan unionin neuvosto, 2016 ja Gilbert, 2011). Rekisterinpitäjien ja henkilötietojen käsittelijöiden tulisikin luoda omat rakenteensa ja politiikkansa suojatakseen henkilötietoja. Nämä toimenpiteet tulisi myös dokumentoida huolella. Tietosuojaviranomaisella on oikeus tarkistaa toimenpiteiden riittävyys ja rekisterinpitäjän ja henkilötietojen käsittelijän tulee voida osoittaa, että vaaditut rakenteet ja politiikat ovat paikallaan. (Gilbert, 2011).

3.4.4 Tietosuojavastaava

Tietyissä tilanteissa organisaatioiden tulee nimittää itselleen tietosuojavastaava. Tietosuojavastaava tulisi nimittää esimerkiksi silloin, kun i. julkishallinnon elin, joka ei ole lainkäyttötehtäviään hoitava tuomioistuin, suorittaa tietojenkäsittelyä, kun ii. rekisterinpitäjä tai henkilötietojenkäsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka luonteensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa tai kun iii. rekisterinpitäjä tai henkilötietojenkäsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

Tietosuojavastaavalla tulee olla ammattipätevyys ja asiantuntemus tietosuojalainsäädännöstä. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee myös varmistaa, että tietosuojavastaava otetaan riittävän ajoissa mukaan henkilötietojen suojaa koskevien kysymysten käsittelyyn. Tietosuojavastaavalla tulisi myös olla riittävä tuki ja riittävät resurssit tehtäviensä täyttämiseksi. Tietosuojavastaava voi samaan aikaan suorittaa myös muita tehtäviä ja velvollisuuksia, mutta rekisterinpitäjän tai henkilötietojen käsittelijän tulee tällöin varmistaa, että nämä tehtävät eivät aiheuta eturistiriitoja. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

Tietosuojavastaavan tehtäviin kuuluu esimerkiksi antaa neuvoja rekisterinpitäjälle tai henkilötietojen käsittelijälle, sekä heidän henkilötietoja käsitteleville työntekijöilleen. Tietosuojavastaavan tulisi myös seurata, että organisaatiossa noudatetaan yleisen tietosuoja-asetuksen vaatimuksia, sekä tehdä yhteistyötä valvontaviranomaisen kanssa. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

3.4.5 IT-järjestelmien muutokset

Asetus esittelee myös uusia vaatimuksia, jotka saattavat aiheuttaa muutoksia organisaatioiden IT-järjestelmiin. Nämä muutokset sisältävät esimerkiksi rekisteröityjen oikeuden pyytää henkilötietojensa poistoa, sekä organisaatioiden velvollisuudesta ilmoittaa mahdollisista tietomurroista viranomaisille. Myös sisäänrakennetun ja oletusarvoisen tietosuojan käsite on uusi. (Bird & Bird, 2016; Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Vastatakseen yleisen tietosuoja-asetuksen vaatimuksiin, tulee organisaatioiden IT- ja tietoturvaosastojen resursseja kasvattaa merkittävästi. Voidakseen vastata näihin uusiin vaatimuksiin esimerkiksi hankkimalla lisää henkilökuntaa, kouluttamalla työntekijöitä, kehittämällä politiikkoja ja toimintaohjeita sekä kehittämällä ja käyttöönottamalla uutta tekniikkaa, tulee organisaatioiden IT- ja tietoturvaosastojen budjetin olla riittävä. (Gilbert, 2011).

Yksi yleisen tietosuoja-asetuksen merkittävistä järjestelmätason muutoksista on se, että rekisteröidyillä on tulevaisuudessa oikeus pyytää rekisterinpitäjää ja henkilötietojensa käsittelijää poistamaan kaikki rekisteröidyn henkilötiedot.

Tätä muutosta on kutsuttu myös ”oikeudeksi tulla unohdetuksi”. (Victor, 2013).

Osa yleisen tietosuoja-asetuksen vaatimuksista saattaa edellyttää suurempiakin muutoksia ja mahdollisesti uusia prosesseja ja dokumentaatiota organisaatioilta. (Bird & Bird, 2016; Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Yksi esimerkki on ilmoitusvelvollisuus viranomaisille, jos organisaatiossa tapahtuu tietomurto (Gilbert, 2011). Organisaatioiden tulee tällöin olla kykeneviä ilmoittamaan viranomaisille mahdollisista tietomurroista viimeistään 72 tuntia sen havaitsemisen jälkeen. Ilmoituksen tulisi sisältää tietoa tietomurron luonteesta, esimerkiksi osallisena olevien rekisteröityjen määrä. (Bird & Bird, 2016; Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

Myös sisäänrakennetun ja oletusarvoisen tietosuojan vaatimusten noudattaminen saattaa vaatia suuria muutoksia organisaatioissa. Sisäänrakennetulla ja oletusarvoisella tietosuojalla tarkoitetaan sitä, että organisaatoiden tulee sisällyttää tietosuoja prosesseihinsa, esimerkiksi politiikkojen ja muiden ohjeistusten avulla. Käytönnössä organisaatioiden tulee siis ottaa käyttöön erilaisia teknologisia ja organisatorisia toimenpiteitä henkilötietojen suojaamiseksi. (Bird & Bird, 2016; Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

Vahvistaakseen rekisteröidyn oikeutta valvoa henkilötietojensa käyttöä entisestään silloin, kun henkilötietojen käsittely suoritetaan automaattisesti, on rekisteröidyllä myös oikeus pyytää ja saada rekisterinpitäjälle luovuttamansa henkilötiedot jäsennellyssä, koneellisesti luettavassa muodossa. Henkilötiedot pitää olla siirrettävissä toiselle rekisterinpitäjälle. Näin ollen rekisterinpitäjiä tulisikin kannustaa kehittämään yhteensopivia muotoja, jotka mahdollistaisivat henkilötietojen siirtämisen. Tämä oikeus kuitenkin on voimassa vain silloin, kun rekisteröity on antanut tietonsa omaan suostumukseensa perustuen, tai kun käsittely perustuu sopimuksen täytäntöönpanoon. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

3.5 Kritiikki yleistä tietosuoja-asetusta kohtaan

Yleistä tietosuoja-asetusta ei ole vielä edes alettu soveltaa, mutta silti sen sisältö on jo kiistanalainen. Etenkin yleisen tietosuoja-asetuksen käytettävyyttä yrityksissä, jotka käsittelevät EU-kansalaisen dataa, on kyseenalaistettu. (Victor, 2013). Asiantuntijat ovat olleet huolissaan esimerkiksi yleisen tietosuoja-asetuksen ”oikeuden tulla unohdetuksi” vaikutuksista sananvapauteen (Rosen, 2011). Samoin oikeudella tulla unohdetuksi on nähty olevan negatiivisia vaikutuksia rikostutkintoihin (Victor, 2013). Oikeuden tulla unohdetuksi on myös nähty olevan teknisesti mahdotonta. (Druschel ym. 2012).

Yleistä tietosuoja-asetusta on kritisoitu myös siitä, että vaikka uusi tietosuojalainsäädäntö on esitetty perustavanlaatuisena ihmisoikeutena, voidaan asetusta silti tarkastella myös omistusoikeuden näkökulmasta. Yleisen tietosuoja-asetuksen voidaankin katsoa rakentavan menettelytapaa

henkilötietojen omistajuudelle. Tällöin henkilötietojen omistusoikeus kuuluisi rekisteröidylle, mutta ne olisivat tarvittaessa myytävissä ja siirrettävissä. Näin yleisessä tietosuoja-asetuksessa lähdettäisiin siitä oletuksesta, että henkilötietoista on tullut kauppatavaraa. (Victor, 2013).

4 KUULIAISUUS EUROOPAN UNIONIN LAINSÄÄDÄNTÖÄ KOHTAAN

Seuraava osuus käsittelee Euroopan unionin lainsäädännön noudattamista, sekä niitä tekijöitä, jotka vaikuttavat aikomukseen noudattaa EU:n lainsäädäntöä.

4.1 Aikomukseen noudattaa EU lainsäädäntöä vaikuttavat tekijät

Organisaatioiden tottelevaisuusvaatimukset ja niiden kompleksisuus kasvaa jatkuvasti. (Panitz ym. 2011). Haasin (1998) mukaan tutkimuksissa on havaittu, että lainsäädännön noudattamisessa on eroja maiden välillä. Tallbergin (2002) mukaan kysymykseen siitä, mikä määrittelee aikomuksen noudattaa kansainvälistä lainsäädäntöä löytyy kaksi erilaista lähestymistapaa: johtaminen ja toimeenpano. Johtamiseen uskovat painottavat yleensä ongelmanratkaisuun pohjautuvaa lähestymistapaa, joka perustuu kapasiteetin rakentamiseen, sääntöjen tulkitsemiseen ja läpinäkyvyyteen, kun taas toimeenpanon puolella olevat painottavat pakottavan strategian tarpeellisuutta, sisältäen valvonan ja sanktiot. Nämä kaksi teoriaa nähdään yleensä kilpailevina, sekä teoriassa että käytännössä. (Tallberg, 2002). Victor ym. (1998) toteaa, että kaksi erilaista teoriaa heijastavat myös erilaisia visioita siitä, kuinka kansainvälinen lainsäädäntö toimii, sekä erilaisista mahdollisuuksista hallinnoida kansainvälisen lainsäädännön rajoja, ja politiikoista, joita tulisi käyttää toteutuksen apuna. Tallbergin (2002) mukaan nämä kaksi teoriaa ovat kuitenkin tehokkaimmillaan yhdistettynä, kun kontekstina on EU:n lainsäädäntö. Tosielämän kansainvälisessä yhteistyössä nämä kaksi strategiaa olisivatkin toisiaan tukevia. Säädösten noudattamiseen tähtäävät järjestelmät, jotka yhdistävät molempia strategioita, tapaavat olla erityisen tehokkaita, kun taas järjestelmät, jotka luottavat vain yhteen strategiaan, kärsivät monesti siitä. (Tallberg, 2002).

EU:n säädösten noudattamiseen tähtäävä järjestelmä koostuu sekä keskitetystä, aktiivisesta ja suorasta ”poliisipartio” valvonnasta, jonka suorittaa

ylikansalliset instituutiot, että hajautetusta, reaktiivisesta ja epäsuorasta ”palohälytys” valvonnasta, joita hyödyntäen kansalliset tuomioistuimet ja yhteiskunnalliset valvojat saavat aikaan kuuliaisuuden. EU:n säädösten noudattamiseen tähtäävä järjestelmä hyödyntää molemmilla tasoilla sekä johtamisen että toimeenpanon lähestymistapoja. Sekä yhteistoiminnallisten että pakottavien instrumenttien hyödyntäminen mahdollistaa EU:n tehokkuuden, kun se taistelee rikkomuksia vastaan, tehden sääntöjen rikkomisesta nopeasti ohimenevän ilmiön. (Tallberg, 2002). EU:n sisällä suurin osa lainsäädännön rikkomuksista johtuukin siirtymisestä kansallisesta lainsäädännöstä EU–lainsäädäntöön ja siihen sopeutumisesta, sekä rajoituksista lainsäädännöllisessä ja hallinnollisessa kyvykkyydessä. (Tallberg, 2002).

4.1.1 Toimeenpano lähestymistapana

Toimeenpano lähestymistapana liittyy kiinteästi peliteoriaan ja kollektiiviseen toimintateoriaan. Sen mukaan organisaatiot nähdään rationaalisina toimijoina, jotka punnitsevat erilaisten vaihtoehtojen hyötyjä ja kustannuksia tehdessään päätöksiä kuuliaisuuden suhteen. Sekä syy että ratkaisu sääntöjen noudattamatta jättämiseen kumpuaa kannustinrakenteesta. Lainsäädäntöä päätetään jättää noudattamatta, kun kannustinrakenne on sellainen, että noudattamatta jättämisen hyöty on suurempi kuin kiinnijäämisen kustannukset. Näin ollen paras tapa varmistaa kuuliaisuus on huolehtimalla riittävän korkeasta kiinnijäämisen todennäköisyydestä ja sen kustannuksista sekä sanktioiden uhkasta. (Tallberg, 2002).

Monesti painotetaan, että esimerkiksi yhteistyötilanteet kannustavat jättämään noudattamatta lainsäädäntöä, sillä tällöin kannustin hylätä sitoumus on olemassa, sillä suurempi hyöty saavutetaan korjaamalla kaiken hyödyn sopimuksista osallistumatta itse sopimuksen toimeenpanoon. Yhteistyö on dominoiva rakenne liittyen kansainväliseen lainsäädäntöön, joten vapaamatkustajuus on keskeinen ongelma. (Tallberg, 2002).

Jotta yhteistyö voisi luoda kollektiivista hyötyä, toimeenpanoa kaivataan ehkäisemään lainsäädännön noudattamatta jättämistä. Valvonta ja sanktiot ovat kaksi keskeistä strategiaa ehkäisemään lainsäädännön noudattamatta jättämistä toimeenpanon avulla. Valvonta lisää läpinäkyvyyttä ja täten paljastaa mahdolliset loikkarit, kun taas sanktiot nostavat lainsäädännön noudattamatta jättämisen kustannuksia ja täten tekee siitä vähemmän houkuttelevaa. Yhdessä valvonta ja sanktiot ehkäisevät loikkaamista ja tukevat kuuliaisuutta. (Tallberg, 2002). Downs ym. (1996) totesivatkin, että rankaiseminen strategiana on riittävä sopimuksen toimeenpanemiseksi, kun molemmat osapuolet tietävät, että huijatessaan ne kärsivät rangaistuksesta niin paljon, että nettohyöty on negatiivinen. Downs ym. (1996) esittelivät myös käsitteen yhteistyön syvyydestä, jolla tarkoitetaan sitä, kuinka paljon molemmat sopijaosapuolet joutuvat muuttamaan toimintaansa siitä, miten olisivat toimineet ilman kyseistä sopimusta. Sopimuksen syvyys taas vaikuttaa sekä tottelemattomuuden yllykkeisiin sekä toimeenpanon tarpeeseen. Tämä tarkoittaa, että mitä

suurempia muutoksia käytökseen kansainvälinen lainsäädäntö vaatii, sitä suurempi on yllyke tottelemattomuudelle. Lisäksi voidaan sanoa, että mitä syvempi sopimus on, sitä suurempia rangaistuksia tarvitaan tukemaan sitä. (Downs ym. 1996). Monesti nykypäivän sopimukset vaativatkin vain pienehköjä muutoksia toimintaan, jolloin sanktiotkin voivat olla pienempiä. Jos sopimus kuitenkin vaatii suurempia muutoksia toimintaan, on toimeenpano olennainen työkalu varmistettaessa kuuliaisuutta. (Tallberg, 2002).

4.1.2 Johtaminen lähestymistapana

Johtaminen lähestymistapana on monessa mielessä ristiriidassa toimeenpanon lähestymistavan kanssa. Teoreetikot, jotka uskovat johtamiseen lähestymistapana, painottavat sitä, kuinka kansainvälisen lainsäädännön noudattaminen on yleistä ja johtuu tehokkuudesta, kiinnostuksesta ja normeista. Lainsäädännön noudattamatta jättäminen ei suinkaan johdu tahallisista päätöksistä rikkoa sopimuksia, vaan rajallisista kapasiteeteista ja vaikeaselkoisista säännöistä. Näin ollen paras ratkaisu lainsäädännön noudattamatta jättämiseen on ongelmanratkaisuun pohjautuva strategia sisältäen kapasiteetin kasvattamisen, sääntöjen tulkitsemisen ja avoimuuden, eikä suinkaan pakottava toimeenpano. (Tallberg, 2002).

Etenkin poliittisilla ja ekonomisilla rajoitteilla kapasiteetissa on suuri merkitys tottelemattomuuden alkuperänä. Poliittiset rajoitteet kapasiteetissa johtuvat monesti siitä, että hallinto epäonnistuu varmistamaan, että sekä julkiset että yksityiset toimijat noudattavat kansainvälisiä velvoitteita. Ekonomiset ongelmat kapasiteettiin liittyen taas syntyvät, kun taloudelliset pakotteet hankaloittavat kansainvälisten velvoitteiden täyttämistä. Rajoitteet resursseissa saattavat hankaloittaa lainsäädännön noudattamista, ja makrotaloustieteelliset tekijät voivat olla epäsuorasti tärkeitä taloudellisten ja poliittisten puitteiden luomisessa julkisille ja yksityisille toimijoille. (Tallberg, 2002).

Johtamisen lähestymistapaan uskovat teoreetikot uskovat, että sääntöjen noudattamatta jättäminen saattaa olla tahatonta. Monesti sopimuksissa käytettävä kieli on epäselvää ja epätarkkaa, joka johtaa väärinymmärryksiin. Tahaton sääntöjen noudattamatta jättäminen saattaa myös olla seurausta poliittisen strategian valitsemiseen liittyvästä epävarmuudesta. (Tallberg, 2002).

Johtamisen lähestymistapaan uskovat teoreetikot suosittelevat kapasiteetin kasvattamista, sääntöjen tulkintaa ja läpinäkyvyyttä ratkaisuna sääntöjen noudattamatta jättämiseen. Esimerkiksi puutteet teknisessä osaamisessa, byrokraattinen kapasiteetti ja taloudelliset resurssit voivat osittain vaikuttaa mahdollisuuteen kasvattaa kapasiteettia. Vähentääkseen tottelemattomuutta, joka johtuu epäselvästä sopimuskielestä, teoreetikot ehdottavat sääntöjen tulkitsemista kansainvälisissä lakielimissä. Tämän tulkitsemisen ei tarvitse välttämättä olla oikeuden päätös, vaan epäviralliset ja sitomattomatkin prosessit voivat selkeyttää sääntöjä. Kolmas ratkaisu sääntöjen noudattamatta jättämiselle on läpinäkyvyys, joka parantaa tottelevaisuutta helpottamalla sopimusnormien koordinointia ja tarjoamalla varmuutta siitä, että

lainsäädännön tarkoitus ei ole hyötyä toimijoista. Läpinäkyvyydellä pyritään siis ehkäisemään tottelemattomuutta sosiaalisella paineella ja täten vakuuttamalla toimijoita muuttamaan käytöstään. (Tallberg, 2002).

5 KIRJALLISUUSKATSAUKSEN YHTEENVETO

Organisaatioiden tulisi päivittää tietoturvapolitiikkojaan säännöllisesti, jotta ne vastaavat organisaation toimintaympäristön muuttuneisiin vaatimuksiin, sekä mahdollisesti muuttuneeseen lainsäädäntöön. Tietoturvapolitiikkojen tulisi kuitenkin kuvata riittävän korkean tason toimintaa, jotta niitä ei tarvitse päivittää esimerkiksi aina, kun organisaation sisällä käytettävä teknologia muuttuu. On kuitenkin huomattu, että organisaatiot eivät aina päivitä ja katselmoi politiikkojaan riittävän säännöllisesti. Monet organisaatiot kuitenkin päätyvät päivittämään politiikkojaan siinä vaiheessa, kun organisaatio kohtaa ulkoisen uhkan, kuten esimerkiksi muuttuvan lainsäädännön.

EU:n yleinen tietosuoja-asetus tulee koskemaan kaikkia henkilötietoja käsitteleviä organisaatioita, jotka toimivat EU:n alueella, tai jotka käsittelevät EU alueen asukkaan henkilötietoja. Käytännössä asetus koskee siis laajaa joukkoa hyvin erilaisia organisaatioita. Kaikkien näiden organisaatioiden tulisi kyetä käsittelemään henkilötietoja turvallisesti, sekä myös osoittamaan, että henkilötietojen käsittelyn turvallisuuteen on kiinnitetty huomiota. Yksi keino osoittaa tämä on dokumentoida organisaation toimet tietosuojan varmistamiseksi, esimerkiksi politiikkojen avulla.

Politiikkojen päivittäminen jää helposti toissijaiseksi organisaatioiden toiminnassa, vaikka politiikkoja tulisikin päivittää osana niiden elinkaarta. Tarve politiikkojen päivittämiselle saattaa johtua esimerkiksi organisaation toimintaympäristön muutoksesta. Vaikka organisaatiot olisivatkin toisinaan haluttomia päivittämään politiikkojaan, pakottaa ulkoinen tekijä organisaatiot toimimaan. Tällainen ulkoinen tekijä voi olla esimerkiksi muuttuva lainsäädäntö. Tutkimusten mukaan virallinen dokumentti politiikan muodossa olisikin tehokas vastaus tietosuojauhkiin.

Organisaatioiden on siis havaittu päivittävän politiikkojaan juuri ulkoisen tekijän, kuten esimerkiksi muuttuvan lainsäädännön, vaikutuksesta. Tässä valossa voitaisiin katsoa, että EU:n yleisen tietosuoja-asetuksen voimaantulo saisi organisaatiot päivittämään politiikkojaan, etenkin kun politiikkojen päivittämisen on todettu olevan vastaus tietosuojauhkiin.

Sitä, tulevatko organisaatiot noudattamaan yleisen tietosuoja-asetuksen vaatimuksia, voidaan tarkastella myös muista näkökulmista. Tutkimusten

mukaan lainsäädäntöä päätetään jättää noudattamatta, kun noudattamatta jättämisen hyöty on suurempi kuin kiinnijäämisen kustannukset. Yleisen tietosuoja-asetuksen vaatimusten noudattamatta jättämiselle on määritelty korkeat sakot, korkeimmillaan jopa 20 000 000 euroa tai 4% yrityksen vuosittaisesta globaalista liikevaihdosta. Tämäkin tukee osaltaan oletusta siitä, että organisaatiot pyrkivät noudattamaan yleisen tietosuoja-asetuksen vaatimuksia, ja täten mahdollisesti myös päivittämään tietoturvapolitiikkojaan. Toisaalta voidaan todeta, että rajoitteet käytettävissä olevissa resursseissa johtavat monesti lainsäädännön noudattamatta jättämiseen. Tietoturvapolitiikan päivittäminen vastaamaan yleisen tietosuoja-asetuksen vaatimuksiin vaatii resursseja, samoin kuin monet yleisen tietosuoja-asetuksen vaatimuksista edellyttävät muutoksia organisaatiossa, joka taas vaatii ylimääräisiä resursseja. Tästä näkökulmasta voitaisiin kyseenalaistaa organisaatioiden aikomus päivittää tietoturvapolitiikat vastaamaan yleisen tietosuoja-asetuksen vaatimuksiin.

Voidaan kuitenkin katsoa, että verrattuna yleisen tietosuoja-asetuksen vaatimusten noudattamatta jättämiseen ja siitä koituviin sakkoihin, on tietoturvapolitiikkojen päivitykseen mahdollisesti osoitettavat resurssit pienehkö investointi, etenkin ottaen huomioon niiden keskeisen roolin osoittamassa suuntaa organisaation tietoturvaan liittyville toiminnoille.

6 EMPIIRISEN TUTKIMUKSEN TOTEUTUS

Tässä luvussa käsitellään empiirisen tutkimuksen toteutusta esittelemällä ensin tutkimuksen tavoite ja tutkimusmenetelmät. Tämän jälkeen tutustutaan tiedonkeruumalliin ja haastateltavien valintaan, sekä käydään läpi haastatteluiden suunnittelu ja toteutus. Lopuksi esitellään menetelmät, joilla tutkimusaineistoa analysoitiin.

6.1 Tutkimuksen tavoite ja tutkimusote

Tutkimuksen tavoitteena on kartoittaa, tuleeko yleinen tietosuoja-asetus ja sen vaatimukset aiheuttamaan muutoksia organisaatioiden tietoturva- ja tietosuojapolitiikkoihin, sekä millaisia nämä muutokset tulevat olemaan. Tutkimuksen tavoitteeseen pyritään vastaamalla seuraavaan tutkimuskysymykseen:

- Saako yleinen tietosuoja-asetus organisaatiot päivittämään tietosuojapolitiikkojaan, ja millaisia nämä muutokset tulevat olemaan?

Tutkimuskysymystä tarkasteltiin tutkielman teoriaosuudessa seuraavien osaongelmien pohjalta:

- Mikä saa organisaation päivittämään tietoturvapolitiikkojaan?
- Mitkä tekijät vaikuttavat organisaation aikomukseen noudattaa lainsäädännön vaatimuksia?

Haastatteluiden pohjalta selvitetään, tuleeko yleinen tietosuoja-asetus aiheuttamaan organisaatioissa tarpeen päivittää tietoturva- tai tietosuojapolitiikkojaan, sekä sen, millaisia muutoksia organisaatiot tulevat politiikkoihinsa tekemään. Lisäksi selvitetään myös haastateltavien asenteita yleistä tietosuoja-asetusta kohtaan, sekä millaisia haasteita se tulee aiheuttamaan organisaatioille lainsäädännön soveltamisen alettua.

Tutkimuksen strategisten valintojen tekemiseen on neljä erilaista tarkoitusta; kartoittava, kuvaileva, selittävä ja ennustava. Kartoittava tutkimus pyrkii löytämään uusia ilmiöitä tai luomaan uusia hypoteeseja, selittävä tutkimus taas keskittyy syy-seuraussuhteiden etsimiseen. Kuvaileva tutkimus kuvaa, kartoittaa ja dokumentoi tiettyä ilmiötä ja ennustava tutkimus ennustaa tapahtumia tai ilmiöitä. (Hirsjärvi ym., 2009). Tämän tutkimuksen tavoite on selvittää millaisia muutoksia lakimuutos saa aikaan organisaation tietoturvapolitiikoissa, joten sen tutkimusstrategia on kartoittava.

6.2 Tutkimusmenetelmät

Seuraavaksi esitellään empiirisen tutkimuksen toteuttamisessa käytettyjä tutkimusmenetelmiä.

6.2.1 Kvalitatiivinen tutkimus

Tutkimus toteutetaan kvalitatiivisena tutkimuksena, sillä sen avulla ei pyritä löytämään tilastollisia säännönmukaisuuksia, vaan pikemminkin kartoittamaan ja selittämään tutkittavaa ilmiötä. Kvalitatiivinen tutkimusstrategian periaatteena on mahdollisimman kokonaisvaltaisen todellisen elämän kuvaaminen. Kvalitatiivinen tutkimus huomioi todellisuuden kompleksisuuden, ja siksi siinä ei voikaan täysin valita mieleisiään osa-alueita tutkittavaksi. (Hirsjärvi ym., 2009).

Kvalitatiivisen tutkimuksen tarkoituksena on löytää tutkimuksen kohteesta uusia, todellisia ja paikkansa pitäviä elementtejä vanhojen vahvistamisen sijaan. Kvalitatiivisessa tutkimuksessa yleensä kerätään monipuolista ja kokonaisvaltaista tietoa luonnollisissa olosuhteissa. (Hirsjärvi ym., 2009). Kvalitatiivinen tutkimusmenetelmä mahdollistaa myös erilaisten motivaatioiden ja aikomusten selvittämisen (Schultze & Avital, 2011). Kvalitatiivisen tutkimuksen kohdejoukko on yleensä valittu tutkimuksen tarkoituksen perusteella, eikä satunnaisotoksena (Hirsjärvi ym., 2009).

6.2.2 Teemahaastattelu

Tavallisia tiedonkeruumenetelmiä ovat esimerkiksi haastattelu, havainnointi ja kysely (Järvinen & Järvinen, 2011). Tässä tutkimuksessa tiedonkeruumenetelmänä käytetään haastatteluita. Haastattelu valittiin tiedonkeruumenetelmäksi siksi, että sen avulla on mahdollista hyödyntää sitä, että tutkimuskohde voi itse kertoa organisaationsa tilanteesta. Haastatteluissa pyritään kartoittamaan alan asiantuntijoiden näkemyksiä siitä, miten organisaation tietoturvapolitiikat tulevat muuttumaan yleisen tietoturva-asetuksen tullessa voimaan. Haastattelu on käytetyin tiedonkeruumenetelmä

kvalitatiivisessa tutkimuksessa ja sitä käytetään tässäkin tutkimuksessa. Haastattelu on mukautuva tutkimusmenetelmä, joka sopii hyvin erilaisiin tutkimuksiin. (Hirsjärvi ym., 2009).

Teemahaastattelu valikoitui tutkimusmetodiksi tutkimuksen aiheen tuoreuden ja aiemman tutkimuksen puuttumisen vuoksi. Teemahaastattelu onkin sopiva tutkimusmetodi, kun ei ennalta tiedetä, millaisia vastauksia tullaan saamaan sekä silloin, kun kysymyksessä on vähän kartoitettu, tuntematon aihe. (Hirsjärvi ym., 2009). Teemahaastattelu mahdollistaa teemojen vapaan käsittelyjärjestyksen ja eri teemoista voi puhua eri laajuudessa eri haastateltavien kanssa. Teemahaastattelun luonteeseen kuuluu lisäksi se, että tarvittaessa myös tutkittavat voivat esittää kysymyksiä ja tarvittaessa tarkentaa kysymyksiä ja vastauksia. Teemahaastattelu sopii hyvin tilanteisiin, joissa tutkitaan haastateltavien ajatuksia, tuntemuksia sekä kokemuksia. (Hirsjärvi & Hurme, 2000).

Haastattelu luotettavuutta saattaa toisaalta heikentää se, että haastateltavilla on taipumus antaa sosiaalisesti suotavia vastauksia. Näin ollen haastateltavat saattavat antaa paljon tietoa positiivisista teemoista, kun taas negatiiviseksi koetut teemat saattavat jäädä vähemmälle huomiolle. Haastattelijan kyky tulkita haastateltavien vastauksia onkin tärkeässä roolissa haastateltaessa. (Hirsjärvi ym., 2009). Kyseinen tekijä tulee ottaa huomioon tässä tutkimuksessa, sillä lainsäädännön noudattaminen tai sen noudattamatta jättäminen on aiheena sellainen, että ihmiset saattavat pyrkiä kaunistelemaan totuutta.

Teemahaastatteluiden sujuvuuden varmistamiseksi olisi suositeltavaa tehdä esihaastatteluita, joiden aikana voidaan tarkentaa esimerkiksi kohdejoukkoa ja teemoja (Hirsjärvi & Hurme, 2000). Tähän tutkimukseen liittyen suoritettiin kaksi esihaastattelua, joiden perusteella kohdejoukkoa vaihdettiin pienistä ja keskisuurista yrityksistä suuriin yrityksiin, sekä muokattiin muutamaa teemaa helpommin ymmärrettäväksi.

6.3 Tutkittavien valinta

Haastateltavien valinta tulisi tehdä harkintaa käyttäen, eikä haastateltavia tulisi valita täysin satunnaisesti. Haastateltavat tulisi valita sen perusteella, keneltä uskotaan saatavan hyvää aineistoa tutkimuksen teemoihin liittyen. (Hirsjärvi & Hurme, 2000).

Tämän tutkimuksen kohderyhmänä pidettiin Suomessa toimivia, henkilöstömäärällä mitattuna suureksi määriteltyjä organisaatioita (Suomen Yrittäjät, 2017). Tutkittaviksi organisaatioiksi valittiin suuria organisaatioita, sillä esihaastatteluiden perusteella kävi ilmi, että pienemmillä organisaatioilla ei usein ole voimassa olevaa tietoturva- tai tietosuojapolitiikkaa. Tästä puutteesta johtuen haastattelun teemoihin, jotka käsittelivät tietoturva- ja tietosuojapolitiikkoja, ei olisi saatu mielekkäitä vastauksia.

Koska tutkimus tähtää etenkin kuvaamaan ilmiötä eikä tuloksia pyritä yleistämään, voitiin haastateltavien määrä pitää maltillisena. Kvalitatiiviseen tutkimukseen liittyen käytetään monesti aineiston riittävyyttä kuvaamaan

saturaation käsitettä. Tällä tarkoitetaan sitä, että aineisto on riittävä, kun samat asiat alkavat kertautua haastatteluissa. Näin ollen olisi siis olemassa sellainen määrä aineistoa, joka tuo esiin teoreettisesti merkittävän tuloksen. (Hirsjärvi ym., 2009). Tähän tutkimukseen liittyen arvioitiin, että saturaatio saavutetaan 5-10 haastattelun aikana. Tutkimuksen aineisto koostuu kahdeksasta tutkittavasta.

6.4 Haastatteluiden suunnittelu ja toteutus

Haastattelut olisi suositeltavaa sopia hyvissä ajoin (Hirsjärvi & Hurme, 2000). Tutkimukseen liittyvät haastattelut sovittiin noin viikkoa tai kahta etukäteen. Haastateltavat löydettiin LinkedIn-sivustoa apuna käyttäen, ja haastattelukutsut lähetettiin sähköpostitse. Haastatteluita pidettiin yhteensä kahdeksan, ja ne pidettiin Etelä-Suomessa kesä-heinäkuussa 2017. Haastatteluista kaksi suoritettiin Skype-ohjelman välityksellä ja loput kuusi tapahtuivat haastateltavien organisaatioiden tiloissa. Sovitut tapaamispaikat olivat rauhallisia, sillä luottamuksellisuus on tärkeää teemahaastatteluissa (Hirsjärvi & Hurme, 2000).

Haastattelut kestivät n. 30-90 minuuttia. Haastattelijalla oli haastattelussa mukana muistiinpanot käsiteltävistä teemoista (liite 1). Nämä muistiinpanot jaettiin myös kahdelle tutkittavalle ennen haastattelua heidän niin pyytäessään. Haastatteluiden aikana haastattelija dokumentoi vastaukset kirjalliseen muotoon muistiinpanotekniikalla, jolla tärkeimmät esille tulleet asiat saatiin kirjattua muistiin. Haastattelut myös nauhoitettiin haastateltavien suostumuksella kahdella matkapuhelimella. Haastatteluita ei litteroitu kokonaisuudessaan, vaan haastattelija kävi nauhoitteet läpi haastatteluiden jälkeen ja varmisti, että haastatteluiden pääkohdat oli kirjattu ylös. Tarvittaessa muistiinpanoja täydennettiin jälkikäteen nauhoitusten perusteella.

Haastattelun aluksi tutkittaville kerrottiin vielä tutkimuksen tarkoitus ja tutkimusaihe, sekä varmistettiin, että tutkittavat tuntevat EU:n yleisen tietosuoja-asetuksen entuudestaan. Tutkimuksen aluksi varmistettiin myös, että kaikki organisaatiot käsittelevät henkilötietoja toimintaansa liittyen. Haastateltavista kerättiin taustatietona heidän toimenkuvansa organisaatiossa.

Tutkimuksessa käsiteltävät teemat on etsitty aiemmasta kirjallisuudesta, jota on esitelty tämän tutkielman kirjallisuuskatsauksessa. Teemat olivat kaikissa haastatteluissa samoja, joskin niitä saatettiin käsitellä eri laajuudessa eri tutkittavien kohdalla. Haastattelurunkoa testattiin kahdessa esihaastattelussa, joiden jälkeen sitä muokattiin soveltumaan paremmin käyttötarkoitukseensa.

Teemahaastattelu koostui tutkittavien organisaatioiden aiempien EU:n yleisen tietosuoja-asetuksen voimaantuloon valmistavien toimenpiteiden kartoittamisesta sekä tietoturva- ja tietosuojapolitiikkojen keskinäisen suhteen sekä niiden päivitysaikataulun selvittämisellä. Tutkittavilta kysyttiin myös, millaisia muutoksia organisaation tietoturva- ja tietosuojapolitiikkoihin on odotettavissa yleisen tietosuoja-asetuksen soveltamisen aloittamisen takia, sekä sitä, olisiko muutokset ollut jotenkin vältettävissä. Tutkittavia pyydettiin myös kuvaamaan suurimpia haasteita, joita he ovat kohdanneet yleiseen tietosuoja-

asetukseen valmistautuessaan. Tutkimuksessa selvitettiin myös sitä, kuinka halukas organisaation johto on ollut tarjoamaan riittäviä resursseja yleisen tietosuoja-asetukseen valmistauduttaessa. Tutkittavilta kysyttiin lisäksi heidän henkilökohtaista mielipidettään yleisen tietosuoja-asetuksen tarpeellisuudesta, sekä sitä, uskovatko he yleisen tietosuoja-asetuksen noudattamisen olevan kilpailuvaltti tulevaisuudessa. Haastattelut lopetettiin kysymällä tutkittavilta, kuinka hyvin he uskovat edustamansa organisaation kykenevän vastaamaan yleisen tietosuoja-asetuksen vaatimuksiin sen soveltamisen alkaessa toukokuussa 2018. (Liite 1, Teemahaastattelun runko).

6.5 Haastatteluaineiston käsittely ja analyysi

Haastatteluiden jälkeen nauhoitetut äänitiedostot kuunneltiin ja haastatteluiden aikana tehtyjä muistiinpanoja täydennettiin tarvittaessa. Nauhoitteet kuunneltiin heti haastatteluiden pitämisen jälkeen, eli kesä-heinäkuussa 2017.

Muistiinpanoja luokiteltiin Excel-ohjelmaa hyödyntäen. Valmiit muistiinpanot luettiin läpi, ja siihen merkittiin teemojen perusteella erilaisia avainsanoja. Avainsanoja apuna käyttäen haastateltujen vastauksia luokiteltiin teemojen mukaan Excel-taulukkoon. Taulukoiduista vastauksista pystyttiin sitten hahmottamaan yhteneväisyyksiä ja eroavaisuuksia tutkittavien ilmiöiden välillä.

7 EMPIIRISEN TUTKIMUKSEN TULOKSET

Tässä luvussa käsitellään tutkimuksen tuloksia. Aluksi esitellään taustaa tutkittavista, jonka jälkeen käsitellään haastatteluiden pohjalta tehtyjä havaintoja yleisen tietosuoja-asetuksen aiheuttamista muutoksista organisaatioiden tietoturva- ja tietosuojapolitiikkoihin.

7.1 Tutkittavien taustatiedot

Tämän tutkimuksen kohderyhmäksi valittiin kahdeksan Suomessa toimivaa, henkilöstömäärällä mitattuna suureksi määriteltyjä organisaatioita (Suomen Yrittäjät, 2017). Organisaatioiden henkilöstömäärä vaihteli noin 400 ja yli 5000 välillä. Taulukko 3 havainnollistaa haastateltujen organisaatioiden toimialoja.

TAULUKKO 3 Haastateltavien toimialat

Toimiala	Tutkittavien määrä
Julkinen sektori	1
Rakennusala	1
Kiinteistöpalvelut	2
Terveydenhuolto (yksityinen)	1
Vähittäiskauppa	2
Valmistava teollisuus	1
Yht.	8

Alun perin tutkittaviksi valittiin tutkittavan organisaation tietohallintojohtaja, mutta yhdessä organisaatiossa asiantuntevammaksi haastateltavaksi tunnistettiin lakiasianjohtaja, ja toisessa organisaatiossa haastateltavaksi tunnistettiin tietoturvapäällikkö.

TAULUKKO 4 Haastateltavien taustatiedot

Tutkittavan titteli	Tutkittavien määrä
Tietohallintojohtaja	6
Lakiasiainjohtaja	1
Tietoturvapäällikkö	1

Kaikki tutkittavat organisaatiot käsittelevät henkilötietoja, ja osa (2) organisaatioista käsittelee lisäksi arkaluontoiseksi luokiteltavia henkilötietoja. Kaikki haastateltavista olivat kuulleet EU:n yleisestä tietosuoja-asetuksesta etukäteen, sekä tunsivat asetuksen sisällön ainakin pääpiirteissään.

7.2 Organisaatioiden tietosuojan nykytila

Suurin osa haastatelluista organisaatioista (6) oli aloittanut yleiseen tietosuoja-asetukseen valmistautumisen suorittamalla organisaation tietosuojatilanteen nykytilanarvioinnin. Kaksi organisaatioista, jotka eivät olleet vielä suorittaneet minkäänlaista nykytilanarviointia, olivat valinneet erilaisen lähestymistavan: toinen organisaatio aikoi aloittaa tietosuojavastaavan rekrytoinnin, jonka jälkeen tarkoitus on rakentaa tietosuojaorganisaatio vastaamaan yleisen tietosuoja-asetuksen vaatimuksiin, kun taas toinen organisaatio oli jo lähtenyt tekemään tarvittavia muutoksia organisaation toimintaan ilman varsinaista nykytilanarviointia. Kaikissa organisaatioissa kuitenkin tunnistettu tarve tehdä muutoksia organisaation toimintaan vastatakseen paremmin yleisen tietosuoja-asetuksen vaatimuksiin.

Kaikki kahdeksan organisaatioista oli osoittanut vastuun yleisen tietosuoja-asetuksen vaatimuksiin vastaamisesta organisaation sisällä. Kaikissa kahdeksassa organisaatiossa vastuu jakautui tietohallinnon ja organisaation lakimiesten kesken. Kolme organisaatioista oli jo päättänyt nimetä organisaatiolle tietosuojavastaavan. Kaksi organisaatioista oli muodostanut organisaation sisällä tietosuojatyöryhmän, joka vastaa yleisen tietosuoja-asetuksen vaatimuksiin vastaamisesta.

Kuusi organisaatioista oli valinnut kumppanin avukseen yleisen tietosuoja-asetuksen vaatimuksiin vastaamisessa. Yhdellä organisaatiolla oli kaksi kumppania. Näistä seitsemästä kumppanista viisi oli asianajotoimistoja ja kaksi oli konsultointiyrityksiä. Kaikki kuudesta kumppaneihin turvautuneesta organisaatiosta oli käyttänyt kumppaniaan arvioidakseen organisaation tietosuojan nykytilaa. Yksi organisaatio oli lisäksi hankkinut toisen kumppanin vastaamaan teknisestä tietoturvasta. Lisäksi yksi organisaatio oli hiljattain havainnut tarpeen toiselle kumppanille, joka vastaisi tulevaisuudessa teknisestä tietoturvasta. Kyseinen organisaatio etsikin parhaillaan sopivaa kumppania.

Suurin osa organisaatioista (5) kertoi lähteneensä vastaamaan yleisen tietosuoja-asetuksen vaatimuksiin viemällä samanaikaisesti eteenpäin sekä tietosuoja- että tietoturvakyvykkyyksiään, sillä yleinen tietosuoja-asetus vaatii organisaatioilta myös riittävää tietoturvan tasoa. Organisaatioista kolme olikin

jo tehnyt muutoksia tietojärjestelmiin tai kartoittanut tarvetta muutoksille. Kolme organisaatiota oli jo kartoittanut tietojen virtaamista tekemällä tietovuokaavioita.

Yleisin jo suoritettu toimenpide oli sopimusten läpikäyminen ja mahdollisten muutostarpeiden kartoittaminen, jonka oli suorittanut viisi organisaatioista. Kaikki organisaatiot olivat kuitenkin havainneet tarpeen katselmoida ja tarvittaessa tehdä muutoksia sopimuksiin.

Neljässä organisaatiossa oli jo aloitettu henkilökunnan kouluttaminen. Myös ne neljä organisaatiota, jotka eivät vielä olleet järjestäneet tietosuojakoulutuksia olivat tunnistaneet tarpeen niille. Yksi organisaatio oli lisäksi laajentanut koulutuksen koskemaan organisaation kaikkia politiikkoja. Politiikkojen tuntemusta olisi tulevaisuudessa tarkoitus testata vuosittain. Yksi organisaatio oli myös harkinnut sulauttavansa koulutuksen osaksi organisaation uutta, suurempaa compliance-ohjelmaa.

Kolme organisaatioista olivat jo aloittaneet politiikkojen ja ohjeistusten, kuten esimerkiksi toimintaohjeiden, päivittämisen tai luomisen. Kolme organisaatioista olivat jo päivittäneet jo julkisia tietosuojaselosteitaan. Vain yksi organisaatio oli jo lähtenyt luomaan hallintomallia tietosuojalle. Samoin vain yksi organisaatio oli aloittanut henkilötietojen käsittelyn perustan määrittelyn ja dokumentoinnin. Näitä tuloksia kuvataan alapuolella olevassa taulukossa 5.

TAULUKKO 5 Organisaatioissa suoritetut yleiseen tietosuoja-asetukseen vastaavat toimenpiteet

Organisaatiossa suoritetut yleiseen tietosuoja-asetukseen vastaavat toimenpiteet	Organisaatioiden lukumäärä
Tietosuojaseloste	3
Sopimukset	5
Koulutus	4
IT-järjestelmien muutokset	3
Politiikkojen ja ohjeistusten päivittäminen/luominen	3
Käsittelyn perustan määrittely ja dokumentointi	1
Hallintomallin luominen	1
Tietovuokaaviot	3

7.3 Tietoturva- ja tietosuojapolitiikkojen katselmointi ja päivittäminen

Tutkittavista organisaatioista suurimmalla osalla (7) oli voimassaoleva tietoturvapolitiikka. Yhdellä organisaatiolla ei ollut virallista politiikkaa, vaan vastaava sisältö oli ilmaistu standardeissa ja toimintaohjeissa. Kuudella organisaatioista oli politiikkojen lisäksi myös standardeja, toimintaohjeita ja muita alemman tason politiikkoja. Puolilla organisaatioista (4) oli voimassaoleva tietosuojapolitiikka. On huomattava, että näistä neljästä organisaatiosta kolme oli kehittänyt tietosuojapolitiikan viimeisen vuoden

aikana vastatakseen paremmin yleisen tietosuoja-asetuksen vaatimuksiin. Kahdella organisaatioista tietosuojapolitiikka sisältyi tietoturvapolitiikkaan. Näitä tuloksia kuvataan alla taulukossa 6.

TAULUKKO 6 Organisaatioiden politiikkakehys

Organisaation vastaus	Organisaatiolla on tietoturvapolitiikka	Organisaatiolla on tietosuojapolitiikka	Tietosuojapolitiikka sisältyy tietoturvapolitiikkaan
Kyllä	7	4	2
Ei	1	4	6

Suurin osa organisaatioista (7) olivat havainneet tarpeen päivittää voimassa olevia turvallisuuspolitiikkojaan yleisen tietosuoja-asetuksen vaatimuksiin vastatakseen. Yksi organisaatio oli jo todennut, että organisaation politiikat ovat lähtökohtaisesti niin korkealla tasolla, ettei niitä ole tarpeen päivittää yleisen tietosuoja-asetuksen vuoksi. Kyseinen organisaatio oli kuitenkin tunnistanut tarpeen päivittää organisaation toimintaohjeita.

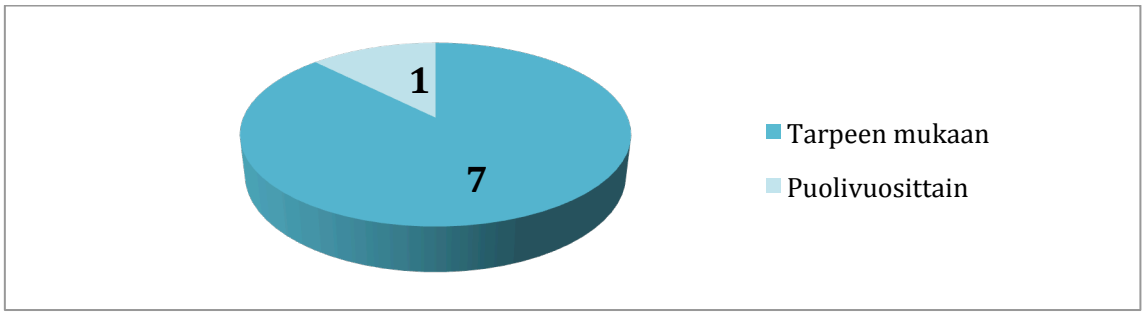
Viisi organisaatioista olivat havainneet tarpeen kehittää organisaatiolle tietosuojapolitiikka yleisen tietosuoja-asetuksen vuoksi. Kolme näistä organisaatioista oli jo kehittänyt organisaatiolle tietosuojapolitiikan. Tuloksia lukiessa tulisi huomata, että kolme organisaatiota ei kokenut tarvetta kehittää organisaatiolle tietosuojapolitiikkaa, mutta yhdellä näistä organisaatioista oli jo valmiiksi ajan tasalla oleva tietosuojapolitiikka, joten kehitystarvetta ei oltu havaittu.

Suurin osa (7) organisaatioista koki, että tarve päivittää politiikkoja ei olisi ollut vältettävissä. Yleisen tietosuoja-asetuksen aiheuttama muutos lainsäädäntöön koettiin organisaatioissa niin suureksi, että se vaati muutoksia politiikkoihin. Yhden organisaation politiikat olivat niin korkealla tasolla kuvattuja, ettei muutoksia politiikkoihin ollut välttämätöntä tehdä. Organisaatio aikoikin tehdä muutoksia toimintaohjeisiinsa ja viitata tulevaisuudessa politiikoissaan näihin toimintaohjeisiin. Taulukko 7 kuvaa edellä mainittuja tuloksia.

TAULUKKO 7 Muutokset organisaation politiikkoihin

Organisaation vastaus	Tullaanko politiikkoja päivittämään?	Kehitetäänkö tietosuojapolitiikka uutena?	Olisiko tarve päivittämiselle ollut vältettävissä?
Kyllä	7	5	1
Ei	1	3	7

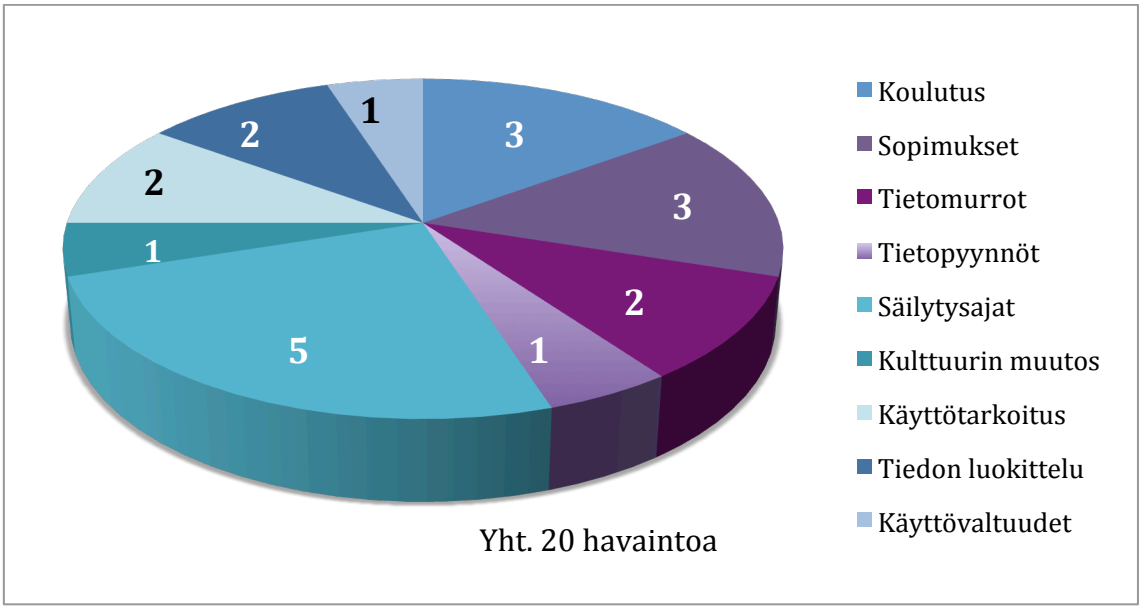
Kuvio 4 kuvaa politiikkojen päivitysaikataulua tutkituissa organisaatioissa. Tutkituista organisaatioista peräti seitsemällä ei ollut sovittua aikataulua politiikkojen katselmoinnille ja päivittämiselle, vaan katselmointi ja päivittäminen tapahtui satunnaisesti tai tarpeen mukaan. Vain yhdessä organisaatiossa politiikat katselmoitiin ja päivitettiin aikataulun mukaan puolivuosittain. Kaikki organisaatiot, jotka päivittivät politiikkojaan tarpeen mukaan, kokivat että organisaatioiden turvallisuuspolitiikat eivät aina vastaa organisaation toimintaympäristöä, vaan muutokset tehdään monesti liian myöhään. Toimintatapa koettiin organisaatioissa liian reaktiiviseksi. Organisaatio, joka katselmoi ja päivittää politiikkojaan puolivuosittain, katsoi politiikkojensa vastaavan organisaation toimintaympäristöä.



KUVIO 4 Politiikkojen päivitysaikataulu

Kuvio 5 kuvaa niitä konkreettisia muutoksia politiikkoihin, joita tutkittavat organisaatiot ovat tunnistaneet tarpeelliseksi tehdä ennen yleisen tietosuoja-asetuksen soveltamisen aloittamista. Suurin osa organisaatioista (5) olivat kokeneet tarpeelliseksi ottaa politiikoissa kantaa henkilötietojen säilytysaikoihin. Kolme organisaatioista koki tarvetta nostaa politiikoissa esille myös ohjeet kolmansien osapuolien kanssa tehtäville sopimuksille sekä henkilötietojen käsittelyyn liittyvän koulutuksen. Organisaatiot, jotka tahtoivat nostaa henkilötietojen käsittelyyn liittyvän koulutuksen esille politiikoissa eivät tahtoneet varsinaisesti määritellä koulutuksen sisältöä tai välttämättä edes aikataulua koulutuksille politiikoissa, vaan tarkoitus oli pikemminkin antaa arvovaltaa henkilötiedoille ja niiden käsittelylle, sekä varmistaa onnistuneen toimintatapojen jalkautuksen. Organisaatioista kaksi aikoi lisätä politiikkaan kohdan mahdollisten tietomurtojen varalta. Kaksi organisaatioista aikoivat sisällyttää tiedon luokittelusta ja henkilötietojen käyttötarkoituksesta maininnan politiikkaan. Tiedon luokittelulla tarkoitetaan tässä yhteydessä sitä, että organisaatiot ilmaisivat tahtovansa tuoda henkilötiedon määritelmän koko organisaation saataville. Tähän liittyen samat organisaatiot tahtoivat myös määritellä henkilötietojen käyttötapaa ja käsittelyä politiikassa. Tutkituista organisaatioista yksi mainitsi aikovansa huomioida käyttövaltuudet päivitetyssä tietoturvapolitiikassaan. Yksi organisaatioista koki tarpeelliseksi ottaa politiikassa kantaa rekisteröidyiltä mahdollisesti tuleviin tietopyyntöihin, jolloin rekisteröity voisi pyytää rekisterinpitäjältä henkilötietojaan, jotta ne voidaan esimerkiksi siirtää toiselle rekisterinpitäjälle. Yksi organisaatioista

tahtoi muutoksilla politiikkaan muuttaa myös organisaation kulttuuria henkilötietojen käsittelyn ympärillä. Organisaatio koki, että henkilötietojen erityisasemaa tulisi korostaa politiikassa. Lisäksi henkilötietojen suojaamisen tahtotila tulisi osoittaa politiikassa.



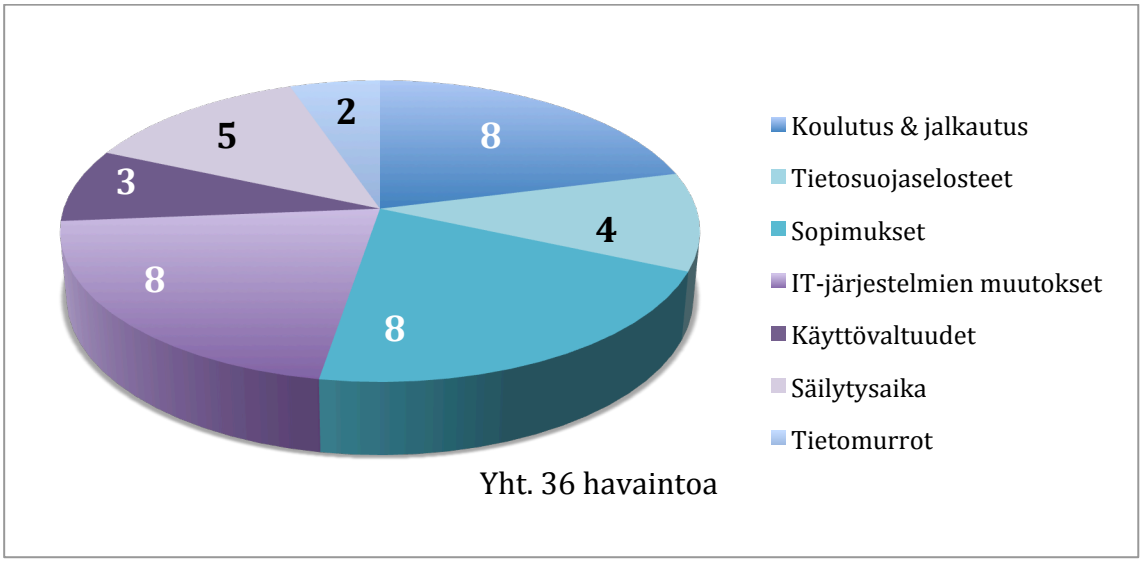
KUVIO 5 Muutokset politiikkoihin

7.4 Organisaatioiden tietosuojan tavoitetila

Organisaatioista suurin osa (7) totesi, etteivät he edes pyri täysin noudattamaan yleisen tietosuoja-asetuksen sen soveltamisen alkaessa toukokuussa 2018. Sen sijaan organisaatiot pyrkivät olemaan valmiita osoittamaan ottaneensa asetuksen vaatimukset tosissaan ja vastanneensa niihin parhaansa mukaan. Suurin osa organisaatioista kertoi aikovansa osoittaa, että he ovat riittävillä pyrkimyksillä ja resursseilla vastanneet yleisen tietosuoja-asetuksen vaatimuksiin. Organisaatioilla oli siis tavoitteena saavuttaa puolustettavissa oleva tila toukokuuhun 2018 mennessä. Vain yksi tutkituista organisaatioista piti tässä vaiheessa tavoitteenaan yleisen tietosuoja-asetuksen vaatimusten noudattamista täysin, joskin suurin syy tähän oli se, että organisaatio koki näin pääsevänsä lähemmäs kaikkien vaatimusten noudattamista verrattuna tilanteeseen, jossa tavoite ei alunperinkään olisi noudattaa kaikkia vaatimuksia.

Kuvio 6 kuvaa niitä muutoksia, joita tutkitut organisaatiot kokivat joutuvansa tekemään toimintaansa noudattaakseen yleisen tietosuoja-asetuksen vaatimuksia. Tutkituista organisaatioista jokainen (8) vastasi aikovansa kouluttaa henkilökuntaansa, sekä pyrkivänsä sitten jalkauttamaan näitä uusia tietosuojan parantamiseen tähtääviä toimintoja organisaatiossa. Monessa organisaatiossa oli jo järjestetty koulutuksia, mutta organisaatiot kokivat tarvetta henkilökunnan kouluttamiselle tietosuojaan liittyen myös tulevaisuudessa. Kaikki organisaatiot (8) myös kokivat joutuvansa

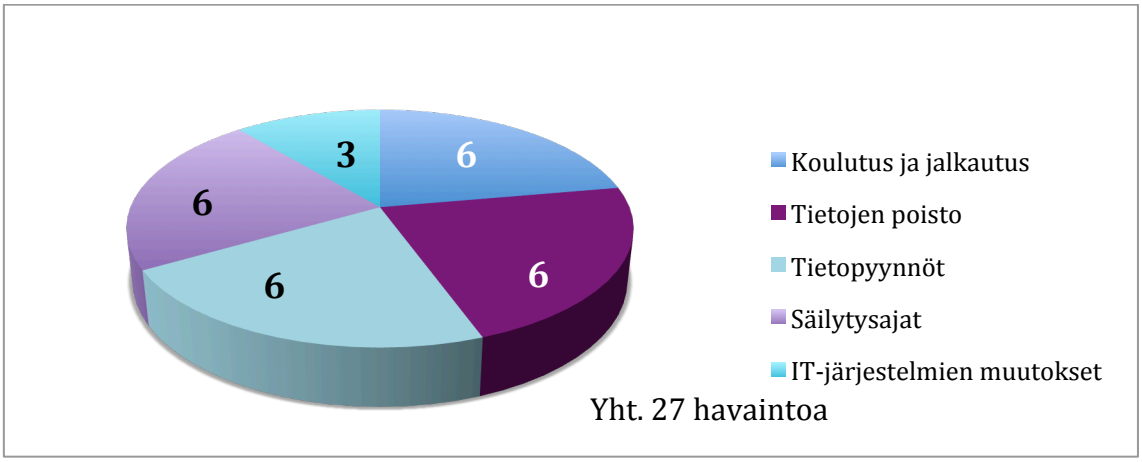
katselmoimaan ja tekemään muutoksia sopimuksiinsa kolmansien osapuolien kanssa. Monet organisaatioista olivatkin jo aloittaneet sopimusten katselmoinnin tai esimerkiksi uusien sopimusliitteiden tekemisen. Samaten kahdeksan organisaatioista katsoi tarpeelliseksi tehdä muutoksia organisaation IT-järjestelmiin. Useimmiten nämä muutokset koskivat rekisteröidyn oikeutta tulla unohdetuksi, eli organisaatioiden tulisi kyetä tulevaisuudessa poistamaan henkilötiedot kokonaan. Nykyisellään organisaatiot kokivat tietojen poistamisen joko mahdottomaksi tai todella aikaa vieväksi. Suurin osa (5) organisaatioista katsoi myös joutuvansa määrittelemään henkilötietojen erilaisia säilytysaikoja uudelleen. Harvassa organisaatiossa oli jo valmiiksi määritelty, kuinka kauan henkilötietoja tulee säilyttää, vaan organisaatiot olivat tähän saakka säilyttäneet kutakuinkin kaikki henkilötiedot. Neljä organisaatioista koki tarpeelliseksi päivittää julkiset tietosuojaselosteensa. Kolme organisaatioista oli jo päivittänyt ainakin suurimman osan tietosuojaselosteistaan. Kolme organisaatioista aikoi tulevaisuudessa katselmoida käyttövaltuuksiaan, sekä tarvittaessa tehdä muutoksia niihin. Kaksi organisaatioista oli tunnistanut tarpeen luoda organisaatiolle oma prosessinsa tietomurtojen varalta.



KUVIO 6 Tulevat muutokset organisaatioiden toimintaan

Kysyttäessä organisaatioilta heidän suurimmista haasteista yleisen tietosuoja-asetuksen noudattamisessa, olivat organisaatiot melko samaa mieltä keskenään. Näitä tuloksia on kuvattu kuviossa 7. Kuusi organisaatioista koki koulutuksen ja etenkin uusien toimintatapojen jalkauttamisen organisaation toimintatavaksi haastavaksi. Organisaatiot olivat ymmärtäneet, että yleisen tietosuoja-asetuksen vaatimukset koskettavat koko organisaatiota, joten koko organisaation henkilökunnan tulee olla tietoinen uusista toimintatavoista. Organisaatiot myös toivoivat, että hyvin koulutettu henkilökunta saattaisi vähentää tarvetta tehdä esimerkiksi tiettyjä suurempia muutoksia IT-järjestelmiin. Suurin osa organisaatioista (6) oli myös huolissaan henkilötietojen poistoista silloin kun

rekisteröity on oikeutettu sitä pyytämään. Monissa organisaatioissa henkilötietojen poistaminen on joko mahdotonta, tai erittäin haastavaa , kuten esimerkiksi henkilötietojen poistaminen verkkolevyiltä tai varmuuskopioiden poistaminen nauhalta. Tähän liittyen suurin osa organisaatioista olivat tunnistaneet haastavaksi myös henkilötietojen säilytysajat. Organisaatiot eivät olleet varmoja, kuinka kauan henkilötietoja tällä hetkellä säilytetään, mutta suurin osa uskoi, ettei kukaan poista säännöllisesti tarpeettomia henkilötietoja. Säilytysaikoja ei myöskään yleisesti ollut määritelty. Organisaatioita huolestutti myös henkilötietojen tietopyynnöt rekisteröidyiltä. Kuusi organisaatioista kokivat tämän haastavaksi, eivätkä olleet varmoja, saisivatko nykytilanteessa kerättyä rekisteröidyistä kaikki henkilötiedot rekisteröidyn niin pyytäessä. Suurin syy edellä mainittuihin ongelmiin oli se, että organisaatioissa henkilötiedot, kuten muukin data, olivat kovin pirstaloituneessa tilassa. Kolme organisaatioista oli havainnut tarpeen tehdä muutoksia IT-järjestelmiin. Näistä havainnoista on karsittu ne havainnot, jotka liittyivät tietojen poistamiseen, säilytysaikoihin tai tietopyyntöihin. Organisaatiot olivat erityisesti havainneet tarpeen tehdä muutoksia järjestelmiinsä tehdäkseen niistä entistä tietoturvallisempia.



KUVIO 7 Organisaatioiden suurimmat haasteet yleisen tietosuoja-asetuksen noudattamisessa

7.5 Organisaatioiden mielipide yleisestä tietosuoja-asetuksesta

Organisaatioilta tiedusteltiin myös heidän yleistä mielipidettään yleiseen tietosuoja-asetukseen liittyen. Erityisesti kuluttajarajapinnassa aiheeseen oli jo panostettu paljon ja aihe koettiin tärkeäksi. Jokaisessa organisaatioissa (8) oli saatu johto mukaan vastaamaan yleisen tietosuoja-asetuksen vaatimuksiin. Suurimmassa osassa tutkittavista organisaatioista (7) johto oli myös kokenut aiheen tärkeäksi. Myös kaikki haastateltavat kokivat yleisen tietosuoja-asetuksen tarpeelliseksi ja hyväksi muutokseksi. Samoin suurin osa organisaatioista (6) oli osoittanut yleisen tietosuoja-asetuksen vaatimuksiin

vastaamiseen riittävän määrän resursseja. Useampi organisaatio oli itse asiassa päättänyt samanaikaisesti lähteä kehittämään tietosuojatilannettaan, mutta myös kehittämään tietoturvakyvykkyyksiään. Myös fyysisen turvallisuuden puolella oli päätetty lähteä kehittämään turvallisuustilannetta. Organisaatiot olivat toiveikkaita, että prosesseja läpi leikattaessa on mahdollista laittaa muitakin piileviä prosesseja kuntoon. Organisaatiot kokivat myös, että tietosuoja- ja tietoturva-asiat otetaan varmasti tulevaisuuden projekteissa paremmin huomioon jo aiemmassa vaiheessa. Näitä tuloksia havainnollistetaan taulukossa 8.

TAULUKKO 8 Organisaatioiden ylimmän johdon mielipide yleisestä tietosuoja-asetuksesta

Organisaatioiden vastaus	Aihe on ollut esillä ylimmässä johdossa	Ylin johto on kokenut aiheen tärkeäksi	Organisaatiolla on ollut riittävät resurssit käytössä
Kyllä	8	7	6
Ei	0	1	2

Suurin osa organisaatioista (5) ei kuitenkaan kokenut, että yleisen tietosuoja-asetuksen vaatimuksien noudattamisesta koituisi organisaatiolle kilpailuetua. Pikemminkin organisaatiot kokivat, että noudattaminen ei johda kilpailuetuun, mutta se, ettei vaatimuksia noudatettaisi, aiheuttaisi väistämättä negatiivisia vaikutuksia liiketoiminnalle. Kaksi organisaatioista oli sitä mieltä, että yleinen tietosuoja-asetus ei mahdollista liiketoimintaa, vaan pikemminkin estää henkilötietojen hyödyntämisen liiketoiminnan kasvattamisessa. Yksi organisaatioista koki, että asetuksella saattaa olla positiivisia vaikutuksia liiketoiminnalle.

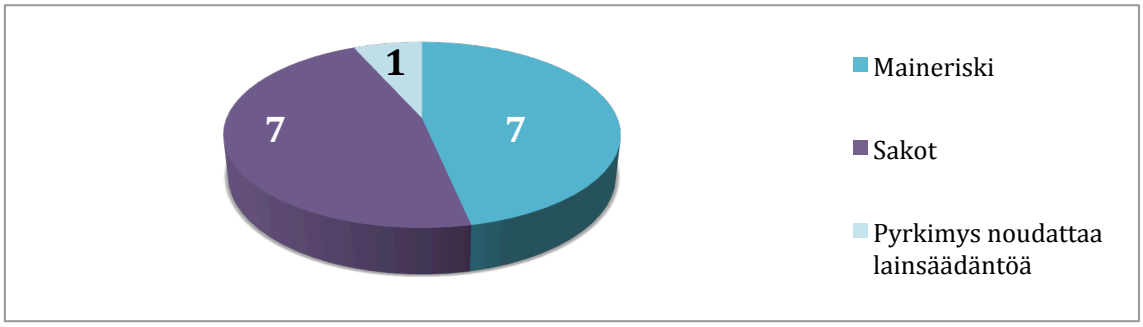
7.6 Syyt noudattaa EU:n yleisen tietosuoja-asetuksen vaatimuksia

Tutkittaville organisaatioille suurimpia syitä noudattaa yleisen tietosuoja-asetuksen vaatimuksia olivat maineriski (7) ja sakot (7). Yksi organisaatioista kertoi myös pyrkivänsä ylipäänsä noudattamaan lainsäädäntöä.

Tuloksia on kuvattu kuviossa 8. Sakot oli erityisesti tunnistettu haastateltavien keskuudessa pääsyyksi sille, että organisaatio on ollut halukas rahoittamaan tietosuojalainsäädännön noudattamiseen tähtääviä toimenpiteitä. Haastateltavat kokivat, että suuret sakot olivat niin konkreettinen hinta lainsäädännön noudattamatta jättämiselle, että siihen oli helppo vedota lisäresursseja tarvittaessa. Haastateltavat kokivatkin, että suuret sakot osaltaan pakottavat organisaatiot noudattamaan tietosuojalainsäädäntöä.

Toisaalta organisaatiot korostivat myös maineriskin mahdollisuutta sekä sitä, että organisaatio tahtoo toimia vastuullisesti asiakkaitaan kohtaan. Etenkin

kuluttajarajapinnassa toimivat organisaatiot korostivat vastuutaan asiakasta kohtaan.



KUVIO 8 Organisaatioiden syyt noudattaa yleisen tietosuoja-asetuksen vaatimuksia

7.7 Yhteenveto tutkimustuloksista

Tutkittavat suhtautuivat pääosin positiivisesti yleiseen tietosuoja-asetukseen. Kaikki tutkittavista organisaatioista olivat jo tunnistaneet tarpeen vastata yleisen tietosuoja-asetuksen vaatimuksiin. Kaikki olivat myös aloittaneet vaatimuksiin vastaamisen.

Tutkittavista organisaatioista suurimmalla osalla oli tietoturvapolitiikka. Puolilla tutkituista organisaatioista oli erillinen tietosuojapolitiikka ja osalla tietosuojapolitiikka sisältyi tietoturvapolitiikkaan. Suurin osa organisaatioista kertoi päivittävänsä turvallisuuspolitiikkojaan tarvittaessa, josta johtuen politiikat eivät aina ole ajan tasalla. Suurin osa organisaatioista koki tarvetta päivittää politiikkojaan ennen yleisen tietosuoja-asetuksen soveltamisen aloittamista. Organisaatiot kokivat lisäksi, että tarve päivittää politiikkoja yleisen tietosuoja-asetuksen vuoksi ei olisi ollut vältettävissä, sillä asetuksen aiheuttama muutos lainsäädäntöön koettiin organisaatioissa niin suureksi. Suurin osa organisaatioista oli kokenut tarpeelliseksi ottaa politiikoissa kantaa esimerkiksi henkilötietojen säilytysaikoihin vielä ennen yleisen tietosuoja-asetuksen soveltamisen aloittamista. Muutama organisaatioista koki tarvetta nostaa politiikoissa esille myös ohjeet kolmansien osapuolien kanssa tehtäville sopimuksille sekä henkilötietojen käsittelyyn liittyvän koulutuksen.

Organisaatioista suurin osa totesi, etteivät he edes pyri täysin noudattamaan yleisen tietosuoja-asetuksen vaatimuksia sen soveltamisen alkaessa. Sen sijaan organisaatiot pyrkivät olemaan valmiita osoittamaan ottaneensa asetuksen vaatimukset tosissaan ja vastanneensa niihin parhaansa mukaan. Suurimmat syyt noudattaa yleisen tietosuoja-asetuksen vaatimuksia olivat asetuksen noudattamatta jättämisestä koituvat sakot sekä mahdollinen maineriski.

8 POHDINTA

Tässä tutkielmassa tarkasteltiin yleisen tietosuoja-asetuksen aiheuttamia muutoksia organisaatioiden tietoturvapolitiikkoihin. Tutkimuksen tarkoituksena oli selvittää, mikä saa organisaatiot päivittämään tietoturvapolitiikkojaan, mikä saa organisaatiot noudattamaan lainsäädännön vaatimuksia ja lopulta selvittää, saako yleinen tietosuoja-asetus organisaatiot päivittämään tietoturvapolitiikkojaan, sekä millaisia nämä muutokset ovat. Tutkimuksen kohderyhmäksi valittiin yleisen tietosuoja-asetuksen soveltamiseen valmistautumisesta vastaavia ammattilaisia suurissa organisaatioissa. Empiirisen tutkimuksen tutkimusmenetelmäksi valittiin teemahaastattelu.

Haastatteluihin osallistui kahdeksan henkilöä. Haastateltavien määrän koetaan olevan tarpeeksi suuri tulosten analysoimista ja johtopäätösten tekemistä varten. Haastatteluihin vastanneet henkilöt tunsivat aiheen entuudestaan ja käsittelivät sitä työtehtävissään. Haastatteluissa oli myös mahdollista varmistaa, että haastateltavat ymmärsivät kysymykset. Tässä luvussa analysoidaan tutkimuksen tuloksia ja esitetään niistä johtopäätöksiä, sekä arvioidaan lisäksi tutkimuksen onnistumista ja esitetään tutkimuksen tulosten hyödyntämismahdollisuuksia ja jatkotutkimusaiheita.

8.1 Tulosten analysointi ja johtopäätökset

Tutkimuksen perusteella voidaan havaita, että tutkitut organisaatiot aikovat päivittää tietoturvapolitiikkojaan vastatakseen paremmin EU:n yleisen tietosuoja-asetuksen vaatimuksiin. Syynä politiikkojen päivittämiselle mainittiin se, että tietosuojalainsäädännön muutokset koettiin niin suuriksi, että politiikkojen päivittäminen oli välttämätöntä. Kuten Wood (1995) on todennut, tulee organisaatioiden päivittää tietoturvapolitiikkojaan vastaamaan esimerkiksi lainsäädännön muuttuviin vaatimuksiin. Myös Smith (1993) on havainnut, että kun organisaatiota uhkaa ulkoinen uhka, muistetaan organisaation sisällä, että toimintaympäristö on muuttunut ja että politiikkoja

tulisi muokata sen vuoksi. Tutkitut organisaatiot olivat siis nyt kohdanneet niin merkittävän muutoksen lainsäädäntöön, että se pakotti ne päivittämään politiikkojaan. Tutkittujen organisaatioiden politiikkojen päivitystahti oli reaktiivinen, eli organisaatiot katselmoivat ja päivittivät politiikkojaan tarvittaessa, joka johti siihen, etteivät politiikat aina olleet ajan tasalla ja vastanneet organisaatioiden toimintaympäristöä. Smithin (1993) mukaan yritysjohto harvoin ottaa proaktiivisen toimintatavan liittyen tietosuojapolitiikkoihin, vaan he odottavat, kunnes jokin ulkoinen tekijä pakottaa heidät toimimaan. Tällaisena ulkoisena tekijänä saattaa toimia esimerkiksi uhka lainsäädäntötoimista. Myös Lopes & Sá-Soares (2012) ja Tuyikeze & Pottas (2011) ovat havainneet saman ilmiön. Wood (1995) suosittelisi kuitenkin katselmoimaan voimassa olevat tietoturvapolitiikat vuosittain.

Tutkimuksessa havaittiin myös, että yleisimmät muutokset tutkittavien organisaatioiden tietoturvapolitiikkoihin koskivat henkilötietojen säilytysajan määrittelyä, sopimuksia kolmansien osapuolien kanssa sekä henkilötietojen turvaamiseen tähtäävien toimintatapojen kouluttamista ja jalkauttamista organisaatiossa. Tuloksista on myös havaittavissa, että organisaatiot kokivat samaan aikaan henkilötietojen säilytysajan määrittelyn ja siihen liittyvät toimenpiteet sekä henkilötietojen turvaamiseen liittyvien toimenpiteiden kouluttamisen ja jalkauttamisen suurimmiksi haasteiksi yleiseen tietosuoja-asetukseen valmistauduttaessa. Vaikuttaisikin siltä, että organisaatiot pyrkivät ottamaan politiikoissaan kantaa juuri haastaviksi kokemiinsa aiheisiin.

Tutkimuksessa selvisi, että pääasialliset syyt noudattaa yleisen tietosuoja-asetuksen vaatimuksia, sisältäen myös politiikkojen päivittämisen, olivat suuret sakot ja mahdollinen maineriski. Myös Tallberg (2002) on havainnut, että paras tapa varmistaa kuuliaisuus lainsäädäntöä kohtaan on huolehtia riittävän korkeasta kiinnijäämisen todennäköisyydestä ja sen kustannuksista, eli toisin sanoen sakoista. Maineriskiä voidaan myös pitää lopulta kustannuksena organisaatiolle, sillä se aiheuttaa ainakin välillistä haittaa organisaation liiketoiminnan kannattavuudelle. Downs ym. (1996) totesivatkin, että rankaiseminen strategiana on riittävä sopimuksen toimeenpanemiseksi, kun molemmat osapuolet tietävät, että huijatessaan ne kärsivät rangaistuksesta niin paljon, että nettohyöty on negatiivinen. Tallberg (2002) totesi myös, että monesti organisaatiot eivät voi noudattaa lainsäädännön vaatimuksia siksi, ettei niillä ole riittävää kapasiteettia tarvittaviin muutoksiin. Tämä oli myös huomattavissa myös tämän tutkimuksen tuloksista, sillä suurin osa tutkituista organisaatioista totesi, etteivät ne kykene noudattamaan kaikkia yleisen tietosuoja-asetuksen vaatimuksia, vaan pyrkivät osoittamaan vastanneensa vaatimuksiin riittävällä tasolla.

Tutkimustulokset ovat linjassa aiemman tutkimuksen kanssa, joten voidaan todeta, etteivät tulokset ole kovin yllättäviä. Tutkimus kuitenkin tuotti uutta tietoa siitä, millaisia muutoksia organisaatiot aikovat tehdä tietoturvapolitiikkoihinsa vastatakseen yleiseen tietosuoja-asetukseen. Oli ilahduttavaa kuulla, että monessa organisaatiossa on myös päätetty tehdä yleiseen tietosuoja-asetukseen valmistautumisen yhteydessä paljon toimia, joita asetus ei varsinaisesti edellytä, kuten esimerkiksi säännöllisiä koulutuksia

liittyen organisaation politiikkoihin, sekä vaadittua laajempia tietoturvatoimia. Mielenkiintoista oli myös se, että tutkituista kahdeksasta organisaatiosta vain yksi pyrkii noudattamaan uutta tietosuojalainsäädäntöä sen soveltamisen alkaessa.

Vaikka henkilötietojen arvoa on edelleen haastavaa määritellä (Baars, 2016; Froomkin, 2000), ovat organisaatiot selvästi lähteneet innokkaasti vastaamaan yleisen tietosuoja-asetuksen vaatimuksiin. Uusi yhtenäisempi Euroopan unionin tietosuojalainsäädäntö koettiin tutkituissa organisaatioissa tarpeelliseksi, vaikkei sen noudattamisen nähty aiheuttavan varsinaista kilpailuetua organisaatioissa. Politiikkojen päivittämisen hyöty oli myös tunnistettu etenkin osoitusvelvollisuuteen vastattaessa.

8.2 Tutkimuksen onnistuminen: reliabiliteetti ja validiteetti

Tutkimuksen onnistumisen arvioinnissa tulee huomioida sekä tutkimuksen reliabiliteetti sekä validiteetti. Reliabiliteetilla tarkoitetaan Hirsjärvi ym. (2009) mukaan tutkimustulosten toistettavuutta, eli tutkimuksen kykyä antaa ei-sattumanvaraisia tuloksia. Validiteetilla tarkoitetaan tutkimusmenetelmän kykyä mitata sitä, mitä on tarkoituskin mitata (Hirsjärvi ym., 2009).

Tutkittavia organisaatioita oli yhteensä kahdeksan. Organisaatioista haastateltiin yleisen tietosuoja-asetuksen vaatimuksiin valmistautumisessa mukana olleita henkilöitä, joten tutkimuskohteet olivat oikeita ihmisiä vastaamaan tutkimuskysymykseen: saako yleinen tietosuoja-asetus organisaatiot päivittämään tietosuojapolitiikkojaan ja millaisia nämä muutokset tulevat olemaan?

Tutkimuksen reliabiliteetin voidaan katsoa olevan hyvä, sillä mikäli toinen tutkija toteuttaisi tutkimuksen uudelleen tulevaisuudessa, uskotaan tutkimuksen saavuttavan samanlaiset vastaukset. Tutkimuksen vastaajien määrä ei kuitenkaan ollut merkittävän suuri, joten reliabiliteettiin vaikuttavat seikat tulee huomioida. On myös huomattava, että haastatellut organisaatiot olivat suuria organisaatioita, joten tulokset eivät välttämättä ole yleistettävissä pienempiin organisaatioihin. Otoskoko koetaan kuitenkin riittävän suureksi tämän laadullisen tutkimuksen kontekstissa, jotta analyysejä ja johtopäätöksiä voidaan tehdä. Suuremmalla otoksella saataisiin oletettavasti vielä luotettavampia ja yleistettävämpiä tuloksia. Tutkittava otos antaa kuitenkin hyvän yleiskuvan, joten tällä otannalla pystyttiin

Tutkimus koetaan validiteetiltaan hyväksi, sillä tutkimus suoritettiin haastatteluna, jolloin voitiin varmistaa, että tutkittavat ymmärsivät kysymykset oikein. Sähköpostitse lähetetyssä haastattelukutsussa esiteltiin aihetta lyhyesti, lisäksi haastattelun aluksi varmistettiin, että haastateltavat tunsivat aiheen entuudestaan. Lisäksi haastateltavien koetaan kuuluvan haluttuun perusjoukkoon, sillä he vastasivat yleiseen tietosuoja-asetukseen valmistautumisesta organisaatiossa.

Tutkimuksen voidaan siis olevan onnistunut, sillä otoskoko oli riittävä laadulliseen tutkimukseen ja otos koostui perusjoukkoon kuuluvista henkilöistä.

Tutkimuksessa saatiin lisäksi vastaus esitettyyn tutkimusongelmaan. Myös tutkimuksen reliabiliteetin ja validiteetin voidaan katsoa olevan riittävän hyvällä tasolla.

8.3 Tulosten hyödyntäminen ja jatkotutkimus

Tutkimustulosten voidaan katsoa olevan käytettävissä sekä käytännön kuin tutkimuksenkin näkökulmasta. Tutkimustuloksia voidaan hyödyntää käytännön työssä organisaatioissa, jotka parhaillaan valmistautuvat yleisen tietosuoja-asetuksen soveltamisen alkamiseen. Tutkimustuloksista on hyötyä varmasti etenkin pienemmille organisaatioille sekä organisaatioille, jotka eivät ole vielä aloittaneet yleiseen tietosuoja-asetukseen valmistautumista. Kyseiset organisaatiot voivat käyttää tämän tutkimuksen tuloksia verratakseen omia suunnitelmiaan siihen, minkä muut organisaatiot ovat jo kokeneet hyväksi lähestymistavaksi. Organisaatiot siis voivat käyttää tutkimuksen tuloksia ikään kuin benchmarking-työkaluna. Koska aiempaa tutkimusta yleisestä tietosuoja-asetuksesta on verrattain vähän, sekä etenkin sen aiheuttamista muutoksista organisaatioiden tietoturvapolitiikkoihin, voidaan tutkimusta käyttää myös pohjana aiheesta tehtävälle jatkotutkimukselle.

Jatkotutkimusaiheeksi esitetään kohdennetumpaa tutkimusta aiheesta. Tutkimus voitaisiin suorittaa kohdennetummin tiettyjen alojen organisaatioille, jolloin olisi mahdollista saada alakohtaisia eroja esiin. Tutkimus voitaisiin myös tehdä laajemmin pieniin, keskisuuriin ja suurin organisaatioihin, jolloin voitaisiin vertailla näiden organisaatioiden turvallisuuspolitiikkoja ja niihin tulevia muutoksia yleisen tietosuoja-asetuksen takia. Tutkimus olisi myös mielenkiintoista toistaa vuoden päästä, kun yleinen tietosuoja-asetus on tullut voimaan. Tällöin nähtäisiin, millaisia muutoksia organisaatioiden turvallisuuspolitiikkoihin todella tehtiin, sekä kuinka hyvin ne silloin vastaavat asetuksen vaatimuksiin.

9 YHTEENVETO

Nykypäivänä valtavista määristä dataa on mahdollista yhdistellä tietoa, jota voidaan käyttää monenlaisissa tarkoituksissa. Tällainen data luonnollisesti kiinnostaa yrityksiä. Määritelläkseen rajat henkilötietojen hyödyntämiselle Euroopan unioni hyväksyi yleisen tietosuoja-asetuksen. Euroopan unionin yleistä tietosuoja-asetusta aletaan soveltaa toukokuun 25. päivä vuonna 2018. Asetus asettaa vaatimuksia esimerkiksi henkilötietojen säilytysajoista, riittävästä tietoturvan tasosta sekä organisaatioiden osoitusvelvollisuudesta. Monet näistä vaadituista muutoksista pitäisi huomioida myös organisaatioiden turvallisuuspolitiikoissa. Kehitys onkin asettanut uusia vaatimuksia tietoturvapolitiikoille ja niiden kehittämiselle. Tietoturvapolitiikat ovat yleensä erilaisia eri organisaatioissa, mutta tyypillisesti ne sisältävät yleisiä lausuntoja tavoitteista, uskomuksista, etiikasta ja vastuista, sekä keinot näiden saavuttamiseksi.

Tässä pro gradu -tutkielmassa tarkasteltiin yleisen tietosuoja-asetuksen aiheuttamia muutoksia organisaatioiden tietoturvapolitiikkoihin. Tutkimuskysymys, johon tässä tutkimuksessa vastattiin, on:

- Saako yleinen tietosuoja-asetus organisaatiot päivittämään tietoturvapolitiikkojaan ja millaisia nämä muutokset tulevat olemaan?

Tutkimuskysymykseen vastattaessa kartoitettiin teoriaosuudessa organisaatioiden syitä päivittää tietoturvapolitiikkojaan ja tekijöitä, jotka vaikuttavat organisaatioiden aikomukseen noudattaa lainsäädännön esittämiä vaatimuksia. Tutkimuksen teoriaosuudessa vastattiin aiemman tutkimuksen pohjalta seuraaviin osaongelmiin:

- Mikä saa organisaation päivittämään tietoturvapolitiikkojaan?
- Mitkä tekijät vaikuttavat organisaation aikomukseen noudattaa lainsäädännön vaatimuksia?

Ensimmäiseen osaongelmaan vastattiin tämän tutkielman luvussa kaksi. Organisaatiot päätyvät monesti päivittämään tietoturvapolitiikkojaan vasta ulkoisen uhkan kohdatessaan. Tällaisia ulkoisia uhkia ovat esimerkiksi liiketoimintaympäristön muutokset ja lainsäädännön muutokset. Tutkimusten mukaan organisaatiot monesti laiminlyövät politiikkojen katselmointia ja päivittämistä, vaikka politiikkojen kehittämiseen olisikin käytetty runsaasti resursseja. Tutkijat suosittelisivatkin katselmoimaan turvallisuuspolitiikat säännöllisesti, esimerkiksi kerran vuodessa. Politiikat tulisi tehdä uusiksi noin viiden vuoden välein.

Toiseen osaongelmaan vastattiin tämän tutkielman luvussa neljä. Tutkimusten mukaan lainsäädäntöä päätetään jättää noudattamatta, kun noudattamatta jättämisen hyöty on suurempi kuin kiinnijäämisen kustannukset. Näin ollen paras tapa varmistaa kuuliaisuus on huolehtia riittävän korkeasta kiinnijäämisen todennäköisyydestä ja sen kustannuksista sekä sanktioiden uhkasta. Valvonta ja sanktiot ovat kaksi keskeistä strategiaa ehkäisemään lainsäädännön noudattamatta jättämistä. Valvonta lisää läpinäkyvyyttä, kun taas sanktiot nostavat lainsäädännön noudattamatta jättämisen kustannuksia ja täten tekee siitä vähemmän houkuttelevaa. Toisaalta voidaan todeta, että rajoitteet käytettävissä olevissa resursseissa johtavat monesti lainsäädännön noudattamatta jättämiseen, samoin kuin vaikeaselkoiset säännöt. Näin ollen teoreetikot suosittelevat kapasiteetin kasvattamista, sääntöjen tulkintaa ja läpinäkyvyyttä ratkaisuna sääntöjen noudattamatta jättämiseen. Esimerkiksi puutteet teknisessä osaamisessa, byrokraattinen kapasiteetti ja taloudelliset resurssit voivat osittain vaikuttaa mahdollisuuteen kasvattaa kapasiteettia.

Varsinaiseen tutkimuskysymykseen ”Saako yleinen tietosuoja-asetus organisaatiot päivittämään tietoturvapolitiikkojaan ja millaisia nämä muutokset tulevat olemaan?” vastattiin luvussa seitsemän, jossa käytiin läpi empiirinen tutkimus. Tässä tutkielmassa esitetyn empiirisen tutkimuksen mukaan organisaatiot tulevat päivittämään tietoturvapolitiikkansa vastatakseen yleisen tietosuoja-asetuksen vaatimuksiin. Osa organisaatioista aikoo myös luoda uuden tietosuojapolitiikan. Tutkimuksessa huomattiin myös, että organisaatiot päivittävät turvallisuuspolitiikkojaan yleensä tarpeen mukaan. Tutkimuksessa havaittiin myös, että yleisimmät muutokset, joita organisaatiot aikovat tehdä tietoturvapolitiikkoihinsa ovat henkilötietojen säilytysajan määrittelyä, sopimuksia kolmansien osapuolien kanssa sekä henkilötietojen turvaamiseen tähtäävien toimintatapojen kouluttamista ja jalkauttamista organisaatiossa. Tuloksista on myös havaittavissa, että organisaatiot kokivat samaan aikaan henkilötietojen säilytysajan määrittelyn ja siihen liittyvät toimenpiteet sekä henkilötietojen turvaamiseen liittyvien toimenpiteiden kouluttamisen ja jalkauttamisen suurimmiksi haasteiksi yleiseen tietosuoja-asetukseen valmistauduttaessa. Vaikuttaisikin siltä, että organisaatiot pyrkivät ottamaan politiikoissaan kantaa juuri haastaviksi kokemiinsa aiheisiin.

Jatkotutkimusaiheeksi esitetään kohdennetumpaa ja suuremman otoksen tutkimista aiheesta. Tutkimus voitaisiin suorittaa kohdennetummin tiettyjen alojen organisaatioille, jolloin olisi mahdollista saada alakohtaisia eroja esiin. Tutkimus voitaisiin vaihtoehtoisesti tehdä laajemmin pieniin, keskisuuriin ja suurin organisaatioihin, jolloin voitaisiin vertailla näiden organisaatioiden

turvallisuuspolitiikkoja ja niihin tulevia muutoksia yleisen tietosuoja-asetuksen takia. Tutkimus olisi myös mielenkiintoista toistaa vuoden päästä, kun yleinen tietosuoja-asetus on tullut voimaan. Tällöin nähtäisiin, millaisia muutoksia organisaatioiden turvallisuuspolitiikkoihin todella tehtiin, sekä kuinka hyvin ne silloin vastaavat asetuksen vaatimuksiin.

LÄHTEET

Article 29 Data Protection Working Party. (2011). Opinion 15/2011 on the definition of consent. Haettu 12.7.2017 osoitteesta http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Article 29 Data Protection Working Party. (2014). Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Haettu 12.7.2017 osoitteesta http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Baars, A. (2016). The value of personal data in a competitive information age (Master's thesis).

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR)*, *25*(4), 375-414.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15*(5/6), 337-346.

Bird & Bird. (2016). Guide to the General Data Protection Regulation. Haettu 5.10.2016 osoitteesta http://www.twobirds.com/en/hot-topics/general-data-protection-regulation.

De Hert, P., & Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*, *28*(2), 130-142.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127-153.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: an exploratory analysis. *IGI Global*.

Downs, G. W., Rocke, D. M., & Barsoom, P. N. (1996). Is the good news about compliance good news about cooperation?. *International Organization*, *50*(03), 379-406.

Druschel, P., Backes, M., & Tirtea, R. (2012). The right to be forgotten–between expectations and practice. *European Network and Information Security Agency (ENISA)*.

Etsebeth, V. (2006). Information Security Policies-The Legal Risk of Uninformed Personnel. In *ISSA* (pp. 1-10).

Euroopan komissio. (2012). *EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus).* EUR-Lex. Haettu 6.2.2017 osoitteesta http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52012PC0011&from=en

Euroopan komissio. (2010). *KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA*

SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE Kattava lähestymistapa henkilötietojen suojaan Euroopan unionissa. EUR-Lex. Haettu 8.2.2017 osoitteesta http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52010DC0609&from=EN

Euroopan parlamentti ja Euroopan unionin neuvosto. (2016). EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). EUR-Lex. Haettu 17.5.2017 osoitteesta http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI

Ferris, J. M. (1994). Using standards as a security policy tool. *StandardView*, *2*(2), 72-77.

Fried, C. (1984). Privacy [a moral analysis]. Philosophical Dimensions of Privacy. F.D. Schoeman, Ed., Cambridge University Press, Cambridge, England.

Froomkin, A. M. (2000). The death of privacy?. *Stanford Law Review*, 1461-1543.

Gaskell, G. (2000). Simplifying the onerous task of writing security policies. In *Proceedings of the First Australian Information Security Management Workshop*.

Gilbert, F. (2011). European data protection 2.0: new compliance requirements in sight-what the proposed EU data protection regulation means for us companies. *Santa Clara Computer & High Tech. LJ*, *28*, 815.

Grobler, T., & Von Solms, S. (2004). Assessing the Policy Dimension. *Johannesburg, South Africa: Technikon Witwatersrand*.

Guel, M. D. (2007). *A Short Primer for Developing Security Policies*. The SANS Institute

Haas, P. M. (1998). Compliance with EU directives: insights from international relations and comparative politics. Journal of European Public Policy, 5(1), 17-37.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), 373-384.

Higgins, H. N. (1999). Corporate system security: towards an integrated management approach. *Information Management & Computer Security*, *7*(5), 217-222.

Hirsjärvi, S. & Hurme, H. (2000). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö.* Helsinki: Yliopistopaino

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita.* 15. painos. Helsinki : Tammi.

Hoffer, J.A., George, J.F., & Valacich, J.S. (1999). *Modern Systems Analysis and Design.* Addison–Wesley, Reading, MA.

Höne, K., & Eloff, J. H. P. (2002). What makes an effective information security policy?. *Network Security*, *2002*(6), 14-16.

Interinstitutional File 2012/0011 (COD). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 11 June 2015.* Haettu 14.11.2016 osoitteesta

http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

Janczewski, L. (1999). Managing security functions using security standards. *Internet and Intranet Security Management: Risks and Solutions*, 81-105.

Järvinen P. & A. Järvinen (2011). *Tutkimustyön metodeista.* Tampere: Opinpajan Kirja

Kuner, C. (2012). The european commission's proposed data protection regulation: A copernican revolution in european data protection law.*Bloomberg BNA Privacy and Security Law Report (2012) February*, *6*(2012), 1-15.

Leinfuss, E. (1996). Policy over policing. *Infoworld*, *18*(34), 55.

Lopes, I. M., & Sá-Soares, F. D. (2012). Information security policies: a content analysis. In *PACIS-The Pacific Asia Conference on Information Systems*.

Mattord, H. J., & Whitman, M. E. (2004). Improving Information Security Through Policy Implementation.

Maynard, S., & Ruighaver, A. B. (2002). Evaluating IS Security Policy Development. *In Third Australian Information Warfare and Security Conference, Perth, Australia*.

Maynard, S., & Ruighaver, A. B. (2003). Development and evaluation of information system security policies. *Information Systems: The Challenges of Theory and Practice*, 366-393.

Moerel, L. (2014). Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof.

Panitz, J. C., Wiener, M., & Amberg, M. (2011). Factors facilitating compliance implementation case study results from multinational enterprises. In *ECIS*.

Parker, D. B. (1998). Fighting computer crime: A new framework for protecting information. John Wiley & Sons, Inc.

Peltier, T. R. (2002). *Information Security Policies. Procedures and Standards: Guideline for Effective Information Security Management*. Boca Raton, Auerbach Publication.

Porter, M. E. (2008). *Competitive strategy: Techniques for analyzing industries and competitors.* Simon and Schuster.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: a policy framework for information security. *Communications of the ACM*, *46*(7), 101-106.

Robinson, T. (1997). Business at risk. *Software Magazine*, *17*(10), 88-91.

Rosen, J. (2011). The right to be forgotten. *Stan. L. Rev. Online*, *64*, 88.

Schultze, U. & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization, 21(1), 1–16.*

Schweitzer, J. A. (1982). Managing information security: a program for the electronic information Age. Butterworth.

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

Suomen Standardoimisliitto SFS ry (2014). SFS-ISO/IEC 27002.

Suomen Yrittäjät. (2017). Yrittäjyys Suomessa. Haettu 4.7.2017 osoitteesta https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363

Tallberg, J. (2002). Paths to compliance: Enforcement, management, and the European Union. *International Organization*, *56*(03), 609-643.

Tuyikeze, T., & Pottas, D. (2011). An Information Security Policy Development Life Cycle. *In Proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010 (p. 165).*

Victor, D. G., Raustiala, K., & Skolnikoff, E. B. (1998). The Impementation and Effectiveness of International Environmental Commitments.

Victor, J. M. (2013). The EU general data protection regulation: Toward a property regime for protecting data privacy. *Yale LJ*, *123*, 513.

Warman, A. R. (1992). Organizational computer security policy: the reality. *European Journal of Information Systems*, *1*(5), 305.

Wood, C. C. (1995). Writing infosec policies. *Computers & Security*, 14(8), 667-674.

LIITE 1 TEEMAHAASTATTELUN RUNKO

1. Haastateltavan taustatiedot

2. Onko organisaatio jo aloittanut yleiseen tietosuoja-asetukseen valmistautumisen?

3. Mikä on tietoturva- ja tietosuojapolitiikkojen keskinäinen suhde? Kuinka usein politiikkoja päivitetään? Onko politiikat yleensä ajan tasalla, eli vastaavatko ne organisaation toimintaympäristöä?

4. Pitääkö organisaation päivittää tietoturva- tai tietosuojapolitiikkojaan vastaamaan paremmin yleisen tietosuoja-asetuksen vaatimuksiin tulevaisuudessa? Millaisia muutoksia politiikkoihin pitäisi tehdä? Olisiko tarve politiikkojen muutoksille ollut jotenkin vältettävissä?

5. Mitkä tulevat olemaan suurimmat haasteet yleisen tietosuoja-asetuksen vaatimuksiin valmistauduttaessa?

6. Onko organisaatio ollut halukas rahoittamaan yleisen tietosuoja-asetuksen voimaantuloon valmistavia toimenpiteitä organisaatiossa? Mikä on ollut suurin syy tähän?

7. Mikä on henkilökohtainen mielipiteesi yleisestä tietosuoja-asetuksesta?

8. Uskotko, että yleinen tietosuoja-asetus ja sen noudattaminen tulee olemaan kilpailuvaltti yrityksille tulevaisuudessa?

9. Millä tasolla edustamasi organisaatio pyrkii vastaamaan yleisen tietosuoja-asetuksen vaatimuksiin toukokuun 25 päivänä vuonna 2018? Asteikko:
   - 1 - Ei pystytä vastaamaan ollenkaan
   - 2 - Pystytään vastaamaan joihinkin vaatimuksiin
   - 3 – Siirtymävaiheessa riittävälle tasolle
   - 4 - Ei pystytä täysin vastaamaan vaatimuksiin, mutta on luultavasti osoitettavissa, että vaatimuksiin on pyritty vastaamaan riittävillä pyrkimyksillä
   - 5 - pystytään täysin vastaamaan vaatimuksiin