Tuomas Tervo

ISO/IEC 27001 -STANDARDI YLEISEN TIETOSUOJA-ASETUKSEN KONTEKSTISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2017

TIIVISTELMÄ

Tervo Tuomas
ISO/IEC 27001 -standardi yleisen tietosuoja-asetuksen kontekstissa
Jyväskylä: Jyväskylän yliopisto, 2017, 34 s.
Tietojärjestelmätiede, kandidaatin -tutkielma)
Ohjaaja(t): Lehto, Martti

EU:n tietosuojalainsäädäntö uudistui 24.5.2016, kun yleinen tietosuoja-asetus astui voimaan ja lakia aletaan soveltaa käytännössä kahden vuoden siirtymäajan jälkeen 25.5.2018. Tämä yleinen tietosuoja-asetus on merkittävä uudistus, joka esittelee monia lisäyksiä ja tarkennuksia vanhaan henkilödirektiiviin ja tutkielman kirjoittamisen ajankohtana siirtymäaika on jo käynnissä. Tutkielma toteutettiin kirjallisuuskatsauksena ja tutkielman varsinaisena tarkoituksena oli selvittää, pystyykö tunnettu tietoturvallisuuden hallintajärjestelmä -standardi, ISO/IEC 27001:2013, vastaamaan yleisen tietosuoja-asetuksen moniin vaatimuksiin. Toisin sanoen tarkoituksena oli vertailla standardin ja asetuksen vaatimuksia toisiinsa ja näin yrittää selvittää pystyvätkö organisaatiot käyttämään kyseistä standardia työkaluna yrittäessään valmistautua lähestyvään lakiuudistukseen. Tutkielmassa esiteltiin myös lukijalle sekä tämä standardi että yleinen tietosuoja-asetus pääpiirteissään. Vertailussa selvisi, että ISO/IEC 27001:2013, vastaa monilta osin yleisen tietosuoja-asetuksen vaatimuksia, mutta ei kuitenkaan täysin niiden ollessa eri kokonaisuuksia ja standardi toimii parhaiten yhtenä tärkeänä rakennuspalikkana kohti täyttä vaatimustenmukaisuutta.

Asiasanat: EU-lainsäädäntö, henkilötiedot, standardit, tietosuoja

ABSTRACT

Tervo, Tuomas
ISO/IEC 27001 -standard in context of the general data protection regulation
Jyväskylä: University of Jyväskylä, 2017, 34 p.
Information Systems, Bachelor's Thesis
Supervisor(s): Lehto, Martti

EU data protection legislation underwent a reform in 24.5.2016 when general data protection regulation, or GDPR, came into effect and the new legislation will be applied after a two-year transition period from 25.5.2018 onwards. This GDPR is a major reform and it will introduce many additions and refinements to the previous data protection directive and at the time of writing this thesis the transition period is already underway. This thesis was carried out as a literary review and the main focus of the thesis was to solve if a well known information security management system -standard, ISO/IEC 27001:2013, can meet the many requirements of the GDPR. In other words the purpose was to compare the requirements of the standard to the requirements of the GDPR and in doing so solve if organizations can use the standard as a tool while preparing themselves for the impending reform. The thesis also broadly introduced the reader to both the standard and the GDPR. In the comparison of the requirements it was discovered that the ISO/IEC 27001:2013 meets the requirements of the GDPR for the most part but not complitely as they are different entities and the standard functions best as an important building block towards full compliance with the GDPR.

Keywords: EU-legislation, personal data, standards, data privacy

KUVIO

KUVIO 1 PDCA -malli. (Humphreys, 2008).....11

SISÄLLYS

1 JOHDANTO....6

2 TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄT....9
- 2.1 ISO, IEC ja JTC1....9
- 2.2 Miksi ISO/IEC 27001?....10
- 2.3 ISO/IEC 27001....10

3 YLEINEN TIETOSUOJA-ASETUS....13
- 3.1 Asetuksen tausta....13
- 3.2 Asetuksen keskeinen termistö....15
- 3.3 Keskeiset uudistukset....16
  - 3.3.1 Alueellinen soveltamisala....16
  - 3.3.2 Sanktiot....16
  - 3.3.3 Suostumus....17
  - 3.3.4 Ilmoitusvelvollisuus....17
  - 3.3.5 Oikeus itseään koskevien tietojen poistamiseen, ”Oikeus tulla unohdetuksi”....18
  - 3.3.6 Datan siirrettävyys eli oikeus siirtää tiedot järjestelmästä toiseen sekä oikeus saada pääsy itseään koskeviin tietoihin....18
  - 3.3.7 Sisäänrakennettu- ja oletusarvoinen tietosuoja sekä osoitusvelvollisuus....19
  - 3.3.8 Tietosuojavastaava....20
  - 3.3.9 Sopimukset rekisterinpitäjien ja henkilötietojen käsittelijöiden välillä sekä tietojen siirtäminen Euroopan talousalueen ulkopuolelle....21
- 3.4 Asetuksen ongelmakohtia....22

4 YLEISEN TIETOSUOJA-ASETUKSEN JA ISO/IEC 27001 -STANDARDIN VERTAILUA....24
- 4.1 Yleistä vertailusta....24
- 4.2 Vertailu....25

5 YHTEENVETO....29

1 Johdanto

EU:n tietosuojalainsäädäntö uudistui kun yleinen tietosuoja-asetus tuli voimaan 24.5.2016. Asetusta ryhdytään soveltamaan kahden vuoden siirtymäajan jälkeen 25.5.2018 alkaen, josta eteenpäin käytäntöjen on oltava linjassa asetuksen kanssa. (Talus, Autio, Hänninen, Pihamaa & Kantonen, 2017.). Asetus korvaa aiemman vuoden 1995 henkilödirektiivin, joka on luonnollisesti peräisin ajalta, jolloin henkilötietoja käsiteltiin ja hyödynnettiin liiketoiminnassa hyvin erilaisella tavalla (VAHTI-raportti, 2016).

VAHTI -raportissa (2016) huomautetaan, että oikeastaan EU:n tietosuojauudistuksella viitataan terminä sekä yleiseen tietosuoja-asetukseen että direktiiviin lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta, joka siis on tarkoitettu ohjaamaan EU:n viranomaisten henkilötietojen käsittelyä muun muassa rikosten tutkinnassa. Tässä tutkielmassa kuitenkin tarkastellaan vain ensiksi mainittua yleistä tietosuoja-asetusta ja jälkimmäinen direktiivi jätetään tarkastelun ulkopuolelle. Kun tutkielmassa siis puhutaan myöhemmin uudistuksesta tai tietosuojauudistuksesta, tarkoitetaan sillä siis vain yleistä tietosuoja-asetusta.

Tietoturvallisuus on jo pelkkänä käsitteenä erittäin laaja ja sen hallinnassa erityisen tärkeää on ymmärtää, että siihen kuuluu paljon muutakin kuin vain laitteet ja ohjelmistot (Vacca, 2013). Kirjassaan Vacca (2013) toteaakin ettei mikään ohjelmisto tai apuväline itsessään riitä takaamaan tietoturvallisuutta, sillä lähtökohtaisesti ne ovat vain yhtä varmoja kuin niitä käyttävät ihmiset.

Organisaatio voi saavuttaa monia potentiaalisia hyötyjä huolehtimalla riittävästä tietoturvan tasosta. Luotettava tietoturva voi esimerkiksi toimia markkinointietuna ja laskea jopa vakuutusmaksujen kuluja. Lisäksi tietoturvastaan huolehtiva organisaatio todennäköisesti myös säästää sekä aikaa että rahaa, joka muuten kuluisi tietomurtojen etsimiseen ja niiden seurauksista huolehtimiseen. Nämä tietomurrot saattavat tulla organisaatiolle hyvinkin kalliiksi negatiivisen julkisuuden, menetettyjen asiakkaiden sekä viranomaisten määräämien sanktioiden myötä. Tästä huolimatta monien organisaatioiden tietoturvan

taso on huono. (Vacca, 2013.). Koska tämä tietoturvan taso on monissa organisaatioissa laiminlyöty, yleinen tietosuoja-asetus monine vaatimuksineen saattaa yllättää monet organisaatiot, joissa tietoturva ei ole ollut aiemmin etualalla.

Vaikka mitään täysin varmaa kaavaa tietoturvallisuuteen ei löydykään, on kuitenkin kehitetty erilaisia mittareita ja standardeja, joilla pyritään varmistamaan parhaiden käytänteiden soveltaminen ja huolehtimaan siitä, että organisaatioissa tietoturvakysymykset otetaan huomioon. Siksi onkin erittäin tärkeää, että organisaatio ottaa käyttöönsä tietoturvallisuuden hallintajärjestelmän, jotta se pystyy hallinnoimaan turvallisesti ja tehokkaasti omia tietovarantojaan. (Susanto, Almunawar & Tuan, 2011.).

Tässä tutkielmassa on tarkoitus selvittää tietoturvallisuuden hallintaa pitäen kiinnostus tietoturvallisuuden hallintajärjestelmien (eng. information security management system eli ISMS) standardeissa ja jo edellä mainitussa yleisessä tietosuoja-asetuksessa. Tutkielmassa pyritään alan kirjallisuuteen, lakitekstei-hin ja standardiin nojaten selvittää kuinka hyvin tietoturvallisuuden hallintajärjestelmät kykenevät vastaamaan lainsäädännön muutokseen. Tutkielmassa on valittu aiheen rajauksena tarkasteltavaksi yksi tunnettu tietoturvallisuuden hallintajärjestelmä standardi eli ISO/IEC 27001:2013. Lisäksi tutkielmassa pyritään perustelemaan sitä, miksi juuri tämä standardi on luontevin vertailukohde yleiseen tietosuoja-asetukseen tämän tutkielman kontekstissa. Tutkielmassa pyritään myös pohtimaan tämän standardin tulevaisuutta lakimuutoksen suhteen eli sitä, miten tämä lakimuutos tulee vaikuttamaan standardin seuraavaan versioon vai tuleeko lainkaan. Tutkielma toteutetaan kirjallisuuskatsauksena ja tutkielmassa pyritään vastaamaan seuraaviin kysymyksiin:

- Mitkä ovat yleinen tietosuoja-asetus ja ISO/IEC 27001:2013 -standardi ja mitä ne pitävät sisällään?
- Miten ISO/IEC 27001:2013 -standardi kykenee vastaamaan yleisen tietosuoja-asetuksen vaatimuksiin?

Standardeilla halutaan viestittää sidosryhmille, että organisaatiossa huolehditaan tietoturva-asioista. Siksi onkin erittäin tärkeää varmistaa, että standardit todella vastaavat osaltaan uudistuksessa voimaan tulleita määräyksiä ja näin antavat luotettavan kuvan organisaation tietoturvasta. Lisäksi uudistus tulee tämän tutkielman kirjoittamisesta katsottuna vajaan vuoden päästä sovellettavaksi 25.5.2018, joten tutkimusaihe on hyvinkin ajankohtainen.

Tutkielmassa pyritään mahdollisimman lyhyesti esittelemään uudistuksen pääpiirteitä käyttäen apuna viranomaisten julkaisemia ohjeistuksia ja itse lakitekstiä. Viranomaisten ohjeistuksien käyttäminen tutkielmassa on perusteltua, sillä ohjeistukset on laadittu huolellisesti ja ne on nimenomaan suunnattu rekisterinpitäjien luettaviksi. Ohjeistukset on siksi myös kirjoitettu tiiviisti ja selkokielisesti. Lisäksi ottaen huomioon aiheen tuoreus, on selvää ettei aiheen kan-

nalta relevanttia tieteellistä tekstiä ole vielä ehditty tuottamaan niin paljoa, että yksinomaan sen käyttö olisi tässä tapauksessa perusteltua ja välttämätöntä.

Tutkielmassa kokonaisuutena kirjallista materiaalia on haettu pääosin Google Scholar -palvelusta, mutta lakiuudistuksesta, ISO:sta ja IEC:sta soveltuvia lähteitä on etsitty myös Googlesta. Hakusanoina on käytetty mm. seuraavia: ”GDPR”, ”General Data Protection Regulation”, ”ISMS” ja ”ISO/IEC 27001”. Tutkielman aihe on niin tuore, että soveltuvaa ja relevanttia tieteellistä tekstiä ei ole vielä ehditty julkaista suuria määriä eivätkä nämä tekstit ole ehtineet vielä luonnollisesti kerätä kovin montaa viittausta. Tutkielmassa on käytetty 28:aa lähdettä, joista suurin osa on tieteellisiä artikkeleita, jotka ovat suurelta osin julkaisutasoa 1, mutta mukana on myös artikkeleita, jotka ovat julkaisutasoa 2 tai 3.

Tutkielman rakenne on tämän johdanto luvun jälkeen seuraavanlainen: seuraavaksi luvussa kaksi tarkastellaan tietoturvallisuuden hallintajärjestelmä -standardia ISO/IEC 27001 ja sitä, miksi juuri tätä standardia on järkevää verrata yleiseen tietosuoja-asetukseen. Tämän jälkeen luvussa kolme siirrytään itse tietosuoja-asetukseen ja käydään läpi lakiuudistuksen taustat ja keskeisimmät muutokset sekä joitain asetuksesta esiin nousseita kysymyksiä ja kritiikkiä. Kun sekä ISO/IEC 27001 -standardi että tietosuoja-asetus on esitelty aiemmissa luvuissa, voidaan siirtyä niiden keskinäiseen vertailuun luvussa neljä, jossa pyritään selvittämään kuinka hyvin standardin ja asetuksen vaatimukset vastaavat toisiaan. Viimeinen ja viides luku on yhteenveto, jossa käydään vielä lyhyesti läpi tutkielman pääkohdat ja johtopäätökset sekä pyritään pohtimaan mahdollisia aiheita jatkotutkimukselle.

2 Tietoturvallisuuden hallintajärjestelmät

Tietoturvallisuuden hallintajärjestelmällä eli ISMS:llä tarkoitetaan järjestelmää, joka koostuu organisaation eri käytännöistä, joilla pyritään määrittelemään, rakentamaan, kehittämään ja säilyttämään tietoteknisten resurssien turvallisuus. Nämä käytännöt määrittelevät kuinka organisaatiossa voidaan käyttää näitä resursseja. Tietoturvallisuuden hallintajärjestelmä on siis organisaatiolle keino hallinnoida tietovarastojaan tehokkaasti. (Susanto ym., 2011.).

Turvallisuuden voidaan ajatella muodostuvan järjestelmien, toimintojen ja valvonnan yhdistyessä tiedon ja toimenpiteiden luotettavuuden säilyttämiseksi. Käyttäjien roolit tietojärjestelmien käyttäjinä ovat kehittyneet ajan myötä eivätkä järjestelmiä enää suinkaan käytä pelkät IT asiantuntijat. (Hong, Chi, Chao & Tang, 2003.).

Tietoturvallisuuden hallintajärjestelmä -standardeja on useita eikä tämän tutkielman laajuudessa ole perusteltua tutkia uudistuksen vastaavuutta kaikkiin näihin. Sen sijaan aiempaan tutkimukseen nojaten tarkasteltavaksi on valittu ISO/IEC 27001 -standardi, jonka valintaa perustellaan kappaleessa 2.2 ja joka esitellään pääpiirteissään kappaleessa 2.3. Standardin taustalla olevat organisaatiot esitellään lyhyesti seuraavaksi kappaleessa 2.1, joka pyrkii selventämään standardin monimutkaista nimeä lukijalle.

2.1 ISO, IEC ja JTC1

ISO eli International Organization for Standardization on vuonna 1947 toimintansa aloittanut, voittoa tavoittelematon kansainvälinen organisaatio, jolla on 163 jäsenmaata. ISO on julkaissut yhteensä 21731 standardia ja asiakirjaa kattavasti lähes jokaiselta teollisuuden alalta. (ISO: All about ISO.).

IEC eli International Electrotechnical Commission on puolestaan vuonna 1906 perustettu vastaavasti voittoa tavoittelematon kansainvälinen organisaatio,

joka on johtava kansainvälisten standardien laatija ja julkaisija sähkön, elektroniikan ja niihin liittyvien tekniikoiden alalta (IEC: About the IEC, 2017).

ISO ja IEC muodostavat yhdessä järjestelmän, joka on erikoistunut maailmanlaajuiseen standardisointiin ja tietotekniikan alalla organisaatiot ovat perustaneet yhteisen teknisen komitean nimeltä ISO/IEC JTC1, jonka alakomitea on puolestaan laatinut ISO/IEC 27001 -standardin (SFS-ISO/IEC 27001:2013).

2.2 Miksi ISO/IEC 27001?

Tutkielmassa on päädytty tutkimaan ISMS:iä ISO/IEC 27001 -standardin kautta. Tämän standardin valintaa voidaan perustella muutamalla syyllä: ensinnäkin se on suurimmista ja tunnetuimmista ISMS:stä kaikkein laajimmin käytössä oleva. Levinneisyyden syyksi arvioidaan muihin suurimpiin ISMS:iin verrattuna helpompaa käyttöönottoa ja parempaa tunnistettavuutta sidosryhmille.(Susanto ym., 2011.). Lisäksi ISO:n vuonna 2015 toteuttama kyselytutkimus vahvistaa, että standardin käyttö on kasvanut edelleen kaikkialla maailmassa (ISO Survey of certifications to management system standards - Full results, 2015).

Toiseksi toisin kuin muut suurimmat ISMS -standardit BS, PCIDSS, ITIL tai COBIT, ISO/IEC 27001 on saatettu aluille jopa 25 valtion toimesta (Susanto ym., 2011). Kansainvälisen levinneisyytensä lisäksi standardilla on siis myös kansainväliset lähtökohdat.

Kolmanneksi ISO/IEC 27001 on laajalti ympäri maailmaa, sekä julkisella että yksityisellä sektorilla toimivilla pienillä, keskikokoisilla ja suurilla organisaatioilla käytössä oleva standardi ja sitä voidaan pitää jo yleiskielenä tietoturvallisuuden hallinnalle (Humphreys, 2008).

Kansainvälisen luonteensa ja laajan levinneisyytensä vuoksi ISO/IEC 27001 on tutkielman kannalta ihanteellinen standardi, jonka kautta tarkastella tietosuojauudistusta, joka on myös luonteeltaan kansainvälinen ja jonka soveltamisala on myös laaja koskettaen monien eri valtioiden alueella toimivia organisaatioita.

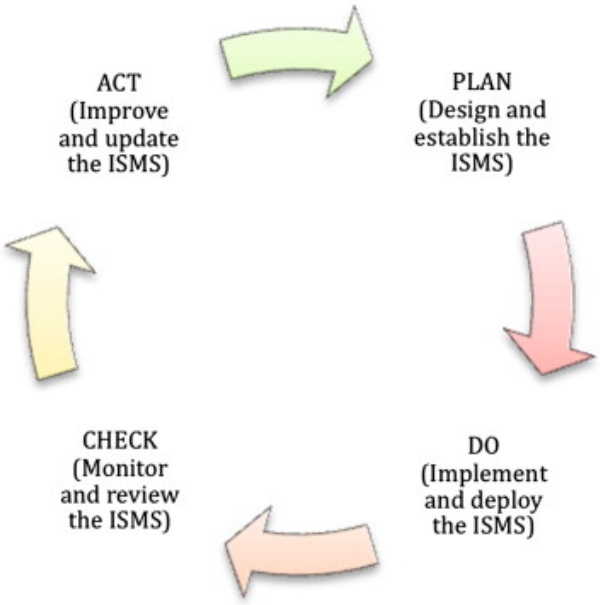
2.3 ISO/IEC 27001

ISO/IEC 27001 -standardin tämänhetkinen tuorein versio on ISO/IEC 27001:2013, joka pohjautuu aiempaan ISO/IEC 27001:2005 -versioon ja tätä tuoreinta versiota käytetään myös luonnollisesti tässä tutkielmassa (SFS-ISO/IEC 27001:2013). ISO/IEC 27001 on osa laajempaa ISO/IEC 27000 -standardiperhettä, johon kuuluu lukuisia muita standardeja, joista ISO/IEC 27001 on kuitenkin tunnetuin (ISO - International Organization for Standardization: ISO/IEC 27001

Information security management). ISO/IEC 27001 syntyi toisen suuren ISMS -standardin, BS7799:n, pohjalta (Susanto ym., 2011).

ISO/IEC 27001 käyttää ns. PDCA -mallia (plan-do-check-act) (KUVIO 1), jota kutsutaan myös jatkuvaksi kehittämiseksi, sillä mallia käyttämällä ISMS:ää tarkastellaan säännöllisesti. Näin voidaan varmistua siitä, että tehdyt toimenpiteet ovat yhä tehokkaita. (Humphreys, 2008.). Malli tarkoitettiin sekä ISMS:n parantamiseen että sen sertifiointitarkoituksiin ja malli koostuu siis neljästä vaiheesta:

- **Suunnittele** (Plan): luo tietoturvallisuuden hallintajärjestelmä määrittelemällä organisaation tavoitteiden ja politiikan suhteen linjassa olevat tietoturvapolitiikka, -tavoitteet, -päämäärät, -prosessit ja -menettelytavat, jotka liittyvät oleellisesti riskien hallintaan ja tietoturvallisuuden kehittämiseen organisaatiossa. Perustele myös valintasi.
- **Toteuta** (Do): toteuta ja ota käyttöön suunnitteluvaiheessa määritetyt tietoturvapolitiikka, turvamekanismit, prosessit sekä menettelytavat.
- **Arvioi** (Check): seuraa ja katselmoi toteutettua tietoturvallisuuden hallintajärjestelmää ja mittaa prosessien suorituskykyä, vertaa sitä aiemmin asetettuihin tietoturvapolitiikkaan ja tavoitteisiin sekä käytännön kokemukseen ja raportoi tuloksista johdolle.
- **Toimi** (Act): ylläpidä tietoturvallisuuden hallintajärjestelmää ja paranna sitä ryhtymällä tarvittaviin korjaaviin ja ehkäiseviin toimenpiteisiin, joihin on päädytty arvioinnin tuloksien ja sen pohjalta toteutettujen johdon katselmointien tai muun olennaisen tiedon perusteella, jotta voidaan saavuttaa tietoturvallisuuden hallintajärjestelmän jatkuva kehittyminen. (SFS-käsikirja, 2012, Siponen & Willison, 2009.).



KUVIO 1 PDCA -malli. (Humphreys, 2008)

ISO/IEC 27001 tarjoaa spesifikaation, jonka pohjalta organisaatio voi itsenäisesti hakea sertifikaattia ISMS:lleen, mikäli ISMS on linjassa standardin vaatimusten kanssa. Sertifikaatti voi tuoda organisaatiolle lisäarvoa toimimalla virallisena todisteena siitä, että järjestelmä todella vastaa odotuksia ja näin ollen organisaatio noudattaa alan parhaita käytäntöjä. ISO ei organisaationa vastaa näiden järjestelmien sertifioinnista, vaan sertifikaattia toivova organisaatio tilaa tarkastuksen ulkoiselta, mieluiten valtuutetulta tarkastajalta. Tällaisen valtuutetun tarkastajan myöntämä sertifikaatti on yleensä voimassa kolme vuotta.(Calder, 2013, ISO - International Organization for Standardization: Certification.).

ISO/IEC 27001 ei ole tarkoitettu kaikenkattavaksi ja jäykäksi malliksi, vaan se on tarkoitettu muuttumaan organisaation mukana. Se kuuluu mitoittaa organisaation tarpeisiin ja sen odotetaan muuttuvan ajan kuluessa. Standardi on tarkoitettu kaikenkokoisille organisaatioille toimialasta ja maantieteellisesti sijainnista riippumatta ja se siis sisältää vaatimukset tietoturvallisuuden hallintajärjestelmälle. (Calder, 2013.).

3 Yleinen tietosuoja-asetus

Tässä luvussa tarkastelemme tarkemmin jo edellä mainittua uutta tietosuoja-asetusta. Tarkastelemme ensin luvussa 3.1 uudistuksen taustat ja syitä sille miksi tämä uudistus edes laadittiin. Seuraavaksi luvussa 3.2 käymme hieman läpi tietosuoja-asetuksen termistöä ja luvussa 3.3 tarkastelemme tietosuoja-asetuksen keskeisimpiä uudistuksia. Luvussa 3.4 puolestaan tarkastelemme joitain asetuksesta esiin nousseita huolenaiheita ja kysymyksiä.

3.1 Asetuksen tausta

Aiempi EU:n henkilötietodirektiivi on siis vuodelta 1995 ja on siten jo auttamattoman vanhanaikainen etenkin kun otetaan huomioon kuinka paljon tietojenkäsittely on alana uudistunut. Lisäksi henkilötietodirektiiviä ei oltu päivitetty lainkaan julkaisuvuotensa jälkeen (Krystlik, 2017).

Lainsäädäntöä uudistaessa tunnistettiin kaksi päähuolenaihetta. Ensinnäkin aiempaan direktiiviin nähden internetin valtavasti korostunut asema ja yhä monimutkaisemmat tietojärjestelmät vaativat yksilöille parempaa suojausta. Toiseksi aiemman direktiivin aikaiset käytännöt ja siten suojauksen taso vaihteli suuresti eri jäsenvaltioiden välillä. (Lloyd, 2017.).

Uudet palvelualustat kuten SaaS (software as a service) ja pilvilaskennan suosion kasvaminen ovat muuttaneet toimintaympäristön peruuttamattomasti ja tämän teknologian monimutkaistuessa myös erinäiset kyberuhat ovat monimutkaistuneet samaa vauhtia viime vuosien aikana. Viimein vuonna 2011 perustettiin ajatushautomo ja lopulta tehtiin päätös uusia henkilötietosuojaa koskeva säätely. (Krystlik, 2017.).

Teknologian kehittyessä myös siihen liittyvän lainsäädännön on kehityttävä. Tavat, joilla dataa edellä mainitun direktiivin aikaan kerättiin, säilöttiin ja päästiin käsiksi, ovat muuttuneet valtavasti viimeisten vuosikymmenten aikana.

Lisäksi eri jäsenvaltiot tulkitsivat ja valvoivat direktiivin noudattamista eri tavoin ja tämä käytänteiden vaihtelevuus toi yrityksille suuria hallinnollisia kustannuksia. (eurobarometri, 2015.).

McDermott (2017) nostaa artikkelissa esiin myös toisen näkökulman lakiuudistuksen puolesta. Hänen mukaansa uudistuksessa voidaan nähdä perinteistä eurooppalaista arvopohjaa kuten yksityisyyden, itsemääräämisoikeuden, läpinäkyvyyden ja syrjimättömyyden, jotka uudistus pyrkii turvaamaan kansalaisille. Näinä suurten muutosten aikoina on entistä suurempi tarve tälle arvopohjalle ja tärkeää tunnistaa oikeus yksityisyydensuojaan perustavanlaatuisena ihmisoikeutena, joka kuuluu kaikille. (McDermott, 2017.). On erittäin järkeenkäypää, että Euroopan unioni pyrkii pitämään kiinni arvopohjastaan myös tietojenkäsittelyn osalta.

Martin ja Myrphy (2017) nostavat artikkelissaan esiin huomion, että tämä lakiuudistus on siinä mielessä ainutlaatuinen, että se edustaa paljon laajempaa yksityisyydensuojaa kuin tähänastiset Yhdysvaltojen kokeilut. Toisaalta eurooppalaiset pitävät yksityisyyttään myös suurempana huolenaiheena kuin yhdysvaltalaiset. Mitä kuluttajien yksityisyydensuojaan tulee, virallinen tieto alalta on suurelta osin länsimaista ja muiden alueiden, kuten Aasian, kansalaisten kohdalla tiedot yksityisyyden suojaa koskettavista huolista ja toimenpiteistä millään tasolla ovat varsin puutteellisia. (Martin & Murphy, 2017.). Nämä erot eurooppalaisten ja muun maailman välillä antavat ymmärtää, että ainakin toistaiseksi Eurooppa on yksityisyydensuojan edelläkävijä.

Vuoden 2015 eurobarometri osoittaa, että kansalaiset ovat ilmeisen huolissaan henkilötietojensa käsittelystä. Valtaosa kokee myös epämiellyttäväksi esimerkiksi sen, että internet-yhtiöt käyttävät tietoja ihmisten verkkoaktiviteeteista räätälöidessään mainontaa. Moni myös pelkää, että heiltä kerättyjä tietoja käytetään eri tarkoitukseen kuin ne on alun perin kerätty. Kuitenkin kansalaiset tiedostavat sen, että tietojen luovuttaminen on usein ainoa tapa päästä palveluihin käsiksi. (eurobarometri, 2015.).

Jopa yhdeksän kymmenestä vastanneesta pitää tärkeänä sitä, että heillä on samat oikeudet ja henkilökohtaisten tietojen suojelun taso pysyy samana riippumatta siitä, missä maassa heidän käyttämäänsä palvelua tarjotaan. Lisäksi valtaosa ihmisistä piti myös tärkeänä sitä, että henkilökohtaiset tiedot voidaan siirtää tarvittaessa vanhan ja uuden palveluntarjoajan välillä. Lähes kaikki vastanneet olivat myös sitä mieltä, että he haluaisivat saada tietää, mikäli heidän tietonsa oltaisiin varastettu tai kadotettu ja valtaosa oli myös sitä mieltä, että he haluaisivat kuulla tästä nimenomaan siltä organisaatiolta joka tietoja käsitteli. (eurobarometri, 2015.).

Yhteiselle säätelylle on siis myös kansalaisten toimesta kysyntää. Seuraavaksi tarkastellaankin tietosuoja-asetuksen keskeistä termistöä sekä uudistuksia, joilla edellä mainittuja kansalaisten huolenaiheita on pyritty paikkaamaan.

3.2 Asetuksen keskeinen termistö

Ennen uudistuksien tarkempaa tarkastelua alle on listattu muutama tietosuoja-asetuksen kannalta oleellinen termi merkityksineen käyttäen tietosuojavaltuutetun toimiston sanastoa ja VAHTI -raporttia:

- **Rekisterinpitäjä**: ”Luonnollinen tai oikeushenkilö, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.” (Tietosuojavaltuutetun toimisto: Sanastoa tietosuojauudistukseen liittyen, 2016).
- **Henkilötieto**: ”Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto)” (Tietosuojavaltuutetun toimisto: Sanastoa tietosuojauudistukseen liittyen, 2016). Henkilö on tunnistettavissa silloin, kun hänen henkilöllisyytensä voidaan päätellä eli hänet voidaan tunnistaa tietojen, kuten esimerkiksi nimen, perusteella (VAHTI -raportti, 2016). Itse asiassa koko uudistuksen kannalta on erittäin tärkeää ymmärtää se, että tietosuoja-asetuksen myötä käytännössä jokainen yritys pitää hallussaan henkilötietoja, jotka kuuluvat asetuksen toimivallan piiriin. Aiemmin tietosuoja kosketti ennen kaikkea pankki- ja terveydenhuoltosektoria, mutta nyt henkilötiedon määritelmä on laajentunut koskemaan käytännössä mitä vain tietoa, joka liittyy johonkin henkilöön. (Krystlik, 2017.).
- **Henkilötietojen käsittelijä**: ”Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.” (VAHTI -raportti, 2016, s.10).
- **Henkilötietojen käsittely**: ”Kaikki henkilötietoihin kohdistuvat toimet (tiedon elinkaari; suunnittelusta → hävittämiseen)”(Tietosuojavaltuutetun toimisto: Sanastoa tietosuojauudistukseen liittyen, 2016). Henkilötietojen käsittelyä ovat esimerkiksi toimenpiteet kuten henkilötietojen haku, järjestäminen, kerääminen, tallentaminen, muokkaaminen ja poistaminen (VAHTI -raportti, 2016).
- **Suostumus**: ”Mikä tahansa vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaus, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn joko antamalla lausumansa tai toteuttamalla selkeästi suostumusta ilmaisevan toimen.” (Tietosuojavaltuutetun toimisto: Sanastoa tietosuojauudistukseen liittyen, 2016).

3.3 Keskeiset uudistukset

Tässä luvussa tarkastellaan asetuksen keskeisimpiä uudistuksia. Nämä yleisessä tietosuoja-asetuksessa esitetyt keskeiset uudistukset on listattu alle sattumanvaraisessa järjestyksessä, eikä järjestyksen ole tarkoitus edustaa uudistusten keskinäistä tärkeysjärjestystä.

3.3.1 Alueellinen soveltamisala

Suurena uudistuksena aiempaan lainsäädäntöön esitellään aiempaa laajempi alueellinen soveltamisala. Asetus tulee koskemaan jokaista organisaatiota, joka toimii EU:n alueella, riippumatta siitä, tapahtuuko itse tietojen käsittely unionin alueella vai ei. Lisäksi asetus koskee myös niitä unionin ulkopuolella toimivia organisaatioita, jotka käsittelevät EU-kansalaisten henkilötietoja tarjotakseen näille tuotteita tai palveluita. Soveltamisen kannalta ei ole merkitystä tarjoaako organisaatio näitä palveluita rekisteröidyille maksua vastaan vai ei. Unionin ulkopuolella sijaitsevien organisaatioiden henkilötietojenkäsittely, joka liittyy EU-kansalaisten käyttäytymisen seuraamiseen, kuuluu myös asetuksen soveltamisalaan siltä osin kuin EU-kansalaisten käyttäytyminen tapahtuu unionin alueella. (EUGDPR.org, Euroopan unionin virallinen lehti, 2016.). Lopuksi vielä huomautuksena, että asetusta ei sovelleta kuolleiden henkilötietojen käsittelyyn, vaan jäsenvaltiot voivat itsenäisesti päättää heihin liittyvistä säännöistä (Euroopan unionin virallinen lehti, 2016).

3.3.2 Sanktiot

Asetuksen myötä valvontaviranomaiset voivat määrätä rekisterinpitäjälle ja tietojenkäsittelijälle asetuksen velvoitteiden laiminlyönneistä sakkoja tai hallinnollisia seuraamuksia. Sakot voidaan jakaa kolmeen luokkaan riippuen laiminlyönnin vakavuudesta. Enimmäismäärä tälle sakolle pahimmista rikkeistä on joko 20 miljoonaa euroa tai yrityksen tapauksessa vaihtoehtoisesti ”neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta”(Euroopan unionin virallinen lehti, 2016), riippuen siitä kumpi on suurempi. Sakon lisäksi tai vaihtoehtona sille valvontaviranomaiset voivat määrätä myös hallinnollisia seurauksia, kuten tietojenkäsittelyn kieltämisen, kunnes asetuksen vaatimusten laiminlyönnit on korjattu. (VAHTI -raportti, 2016, EUGDPR.org, Euroopan unionin virallinen lehti, 2016.).

3.3.3 Suostumus

Suostumuksen antamisen ehtoja on vahvistettu merkittävästi ja tästä eteenpäin se on annettava selkeästi jollain suostumusta ilmaisevalla tavalla niin, että suostumus on ymmärrettävässä muodossa, selkokielinen, yksilöity ja yksiselitteinen. Suostumus on annettava vapaaehtoisesti eli suostumuksen antamisesta on voitava kieltäytyä ja se on voitava perua ilman, että rekisteröidylle aiheutuu haittaa toimenpiteestä. Lisäksi rekisteröidyn on oltava tietoinen suostumuksensa ehdoista, rekisterinpitäjän henkilöllisyydestä sekä siitä, mihin kerättyjä henkilötietoja aiotaan käyttää eikä suostumusta pitäisi voida antaa vaikenemalla, hyväksymällä valmiiksi täytetty ruutu tai jättämällä jokin toimenpide suorittamatta. Rekisterinpitäjän velvollisuus on kyetä osoittamaan, että rekisteröity on todella antanut suostumuksensa henkilötietojensa käsittelyyn. (EUGDPR.org, Euroopan unionin virallinen lehti, 2016.). Suostumuksen perumisen tulee lisäksi olla yhtä vaivatonta kuin sen antaminenkin (VAHTI -raportti, 2016, EUGDPR.org, Euroopan unionin virallinen lehti, 2016).

3.3.4 Ilmoitusvelvollisuus

Uutena velvollisuutena rekisterinpitäjälle asetetaan ilmoitusvelvollisuus. Asetuksen myötä rekisterinpitäjän täytyy ilmoittaa valvontaviranomaisille ja rekisteröidylle tapauksissa, joissa rekisteröidyn henkilötiedot ovat vuotaneet ulkopuolisille niin, että loukkaus todennäköisesti aiheuttaa rekisteröidyn oikeuksille suuren riskin. Ilmoittaminen loukkauksesta tulee mahdollisuuksien mukaan tehdä valvontaviranomaiselle 72 tunnin kuluessa loukkauksen havaitsemisesta ja rekisteröidylle, jota loukkaus koskettaa, tulee henkilökohtainen ilmoitus tehdä ilman kohtuutonta viivästystä. (VAHTI -raportti, 2016, Talus ym., 2017, Euroopan unionin virallinen lehti, 2016.).

Henkilökohtaisesta ilmoituksesta rekisteröidylle tulisi löytyä ainakin ymmärrettävä kuvaus tapahtuneesta loukkauksesta, jokin taho, jolta rekisteröity voi halutessaan kysyä lisätietoja kuten tietosuojavastaava, tietoa loukkauksen mahdollisista vaikutuksista rekisteröidylle sekä kuvaus toimenpiteistä, joilla rekisterinpitäjä aikoo ratkaista tilanteen tai lievittää loukkauksesta aiheutuvaa haittaa. (VAHTI -raportti, 2016.).

Henkilötietojen käsittelijän puolestaan on ilmoitettava havaitsemastaan loukkauksesta rekisterinpitäjälle ilman aiheetonta viivästystä. Ilmoittamisen rekisterinpitäjä voi hoitaa tietyissä tapauksissa myös esimerkiksi median välityksellä. Tämä voi tulla kyseeseen esim. silloin kun loukattujen määrä on niin suuri, että henkilökohtaisesta ilmoittelusta aiheutuisi kohtuutonta vaivaa. (VAHTI -raportti, 2016.).

Huomioitavaa on myös, että rekisterinpitäjä on velvollinen dokumentoimaan kaikki henkilötietojen tietoturvaan liittyvät loukkaukset, sekä muut siihen

liittyvät seikat kuten loukkauksen vaikutukset ja sen korjaamiseen tähtäävät toimenpiteet. Dokumentoinnin on lisäksi oltava tarpeeksi tarkkaa, jotta valvontaviranomainen voi sen avulla tarkistaa, onko rekisterinpitäjä noudattanut ilmoitusvelvollisuuttaan. (Talus ym., 2017, Euroopan unionin virallinen lehti, 2016.).

3.3.5 Oikeus itseään koskevien tietojen poistamiseen, ”Oikeus tulla unohdetuksi”

Rekisteröidyllä on oikeus tietyin edellytyksin saada tietonsa poistetuksi eli ”tulla unohdetuksi”, jolloin rekisteröity esimerkiksi voi perua aiemmin antamansa suostumuksen henkilötietojensa käsittelyyn ja rekisterinpitäjä joutuu poistamaan tiedot järjestelmästään ilman aiheetonta viivästystä (VAHTI -raportti, 2016, Euroopan unionin virallinen lehti, 2016).

Jos rekisterinpitäjä on julkaissut nämä henkilötiedot ja poistamisen edellytykset täyttyvät, rekisterinpitäjän velvollisuudeksi asetetaan myös ilmoittaminen henkilön pyynnöstä poistaa tiedot muille henkilötietoja käsitteleville rekisterinpitäjille (Talus ym., 2017, Euroopan unionin virallinen lehti, 2016). Tässä velvollisuudessa kuitenkin noudatetaan kohtuullisuutta ja otetaan huomioon rekisterinpitäjän käytettävissä oleva teknologia ja noudattamisen toteuttamiskustannukset. Lisäksi tätä oikeutta itseään koskevien tietojen poistamiseen saatetaan olla soveltamatta tietyin edellytyksin mm. silloin kuin soveltaminen olisi sananvapauden tai yhteisen edun vastaista. (Euroopan unionin virallinen lehti, 2016 .).

3.3.6 Datan siirrettävyys eli oikeus siirtää tiedot järjestelmästä toiseen sekä oikeus saada pääsy itseään koskeviin tietoihin.

Rekisteröidyllä on asetuksen mukaan oikeus saada rekisterinpitäjälle antamansa sekä itseään koskevat henkilötiedot ja siirtää nämä tiedot rekisterinpitäjältä toiselle rekisterinpitäjälle. Tiedot on luovutettava yleisesti käytössä olevassa siirtomuodossa ja niin, että ne ovat myös koneellisesti luettavassa muodossa. Lisäksi mikäli tämä on mahdollista, on rekisterinpitäjän siirrettävä tiedot suoraan toisen rekisterinpitäjän järjestelmään. Asetus ei kuitenkaan velvoita rekisterinpitäjiä suunnittelemaan tai toteuttamaan järjestelmistään yhteensopivia tietojen siirtämistä varten ja niinpä tietojen siirtoa suoraan järjestelmästä toiseen ei vaadita, mikäli se ei ole teknisesti mahdollista. (EUGDPR.org, VAHTI -raportti, 2016, Talus ym., 2017, Euroopan unionin virallinen lehti, 2016.).

Tämän siirto-oikeuden toteutuminen edellyttää sitä, että tietojenkäsittely tapahtuu automatisoidusti ja käsittely perustuu rekisteröidyn suostumukseen tai sopimukseen. Lisäksi täytyy huomata, ettei oikeutta sovelleta silloin kun käsittely on tarpeellista yleisen edun mukaisen tehtävän suorittamiseksi, silloin kun se on tarpeellista rekisterinpitäjän julkisen vallan käyttämiseksi tai silloin

jos siirto-oikeus vaikuttaisi haitallisesti muiden oikeuksiin ja vapauksiin. (VAHTI -raportti, 2016, Talus ym., 2017, Euroopan unionin virallinen lehti, 2016.).

Rekisteröidyllä on myös oikeus saada rekisterinpitäjältä vahvistus siitä, käsitelläänkö häntä koskevia tietoja ja mikäli käsitellään, hänellä on myös oikeus saada pääsy itseään koskeviin tietoihin. Rekisteröidyllä on lisäksi oikeus saada tietää esimerkiksi miten, kuka, missä, mihin tarkoitukseen ja mahdollisuuksien mukaan kuinka kauan hänen tietojaan aiotaan käsitellä. (EUGDPR.org, Euroopan unionin virallinen lehti, 2016.).

3.3.7 Sisäänrakennettu- ja oletusarvoinen tietosuoja sekä osoitusvelvollisuus.

Sisäänrakennetulla- ja oletusarvoisella tietosuojalla tarkoitetaan sitä, että asetus velvoittaa rekisterinpitäjän jo aikaisessa vaiheessa henkilötietojenkäsittelyä aina henkilötietojenkäsittelyn loppuun saakka pitämään huolta siitä, että käsittelyssä toteutuvat oletusarvoisesti tietyt periaatteet (Talus ym., 2017, Euroopan unionin virallinen lehti, 2016). Näitä periaatteita kutsutaan myös nimellä tietosuojaperiaatteet, joita itse asetus (Euroopan unionin virallinen lehti, 2016) mainitsee kuusi:

1. **Lainmukaisuus, kohtuullisuus ja läpinäkyvyys**.
2. **Käyttötarkoitussidonnaisuus**, jolla tarkoitetaan sitä, että oletusarvoisesti kerätään vain sellaisia tietoja, jotka ovat olennaisia ja välttämättömiä jonkin tietyn, laillisen käyttötarkoituksen kannalta. Näitä johonkin tiettyyn tarkoitukseen kerättyjä tietoja ei saa enää myöhemmin käsitellä alkuperäisen tarkoituksen kanssa yhteensopimattomalla tavalla.
3. **Tietojen minimointi**, jolla tarkoitetaan sitä, että lähtökohtaisesti tietoja saa kerätä vain sen verran kuin on välttämätöntä tietojenkäsittelyn tarkoituksen kannalta.
4. **Täsmällisyys**, jolla tarkoitetaan sitä, että henkilötietojen tulee olla täsmällisiä ja rekisterinpitäjän tulee huolehtia kaikista kohtuullisista toimenpiteistä, jotta käsittelyä varten tarvittavat henkilötiedot on päivitetty ja mahdolliset epätarkkuudet on viipymättä joko oikaistu tai kokonaan poistettu.
5. **Säilytyksen rajoittaminen**, joka tarkoittaa sitä, että henkilötietoja, joista rekisteröity on tunnistettavissa saa säilyttää vain niin kauan kuin on tarpeen tietojenkäsittelyn varsinaisen käyttötarkoituksen toteuttamisen kannalta. Henkilötietoja voidaan toisaalta tietyin edellytyksin säilyttää myös pidempiä aikoja silloin, kun niitä käytetään ainoastaan mm. yleisen edun mukaiseen arkistointitarkoitukseen tai johonkin tieteelliseen tarkoitukseen. Myös silloin, kun edellytykset tähän pidempään säilytysaikaan täyttyvät, on huolehdittava, että rekisteröidyn oikeudet ja vapaudet turvataan asianmukaisesti.

6. **Eheys ja luottamuksellisuus**, joilla tarkoitetaan sitä, että henkilötietoja tulee käsitellä tavalla, jolla varmistetaan tietojen asianmukainen turvaaminen. Tällöin täytyy pitää huolta, että asianmukaisia teknisiä ja organisatorisia toimenpiteitä käyttäen tietoa suojataan kaikelta vahingossa tapahtuvalta haitalta, kuten häviämiseltä, vahingoittumiselta ja tuhoutumiselta. Lisäksi henkilötietoja täytyy myös suojata luvattomalta ja lainvastaiselta käsittelyltä eikä tietoja ”saateta rajoittamattoman henkilömäärän saataville” (Euroopan unionin virallinen lehti, 2016).

Lisäksi rekisterinpitäjällä on tietosuojaperiaatteiden kohdalla ns. osoitusvelvollisuus, joka tarkoittaa sitä, että nimenomaan rekisterinpitäjän tulee pystyä osoittamaan, että tämä on noudattanut ylempänä lueteltuja tietosuojaperiaatteita tietojenkäsittelyssään (VAHTI -raportti, 2016, Euroopan unionin virallinen lehti, 2016). Näiden tietosuojaperiaatteiden avulla halutaan varmistua siitä, että tietosuoja-asetuksen vaatimuksia noudatetaan ja siten rekisterinpitäjän on toteutettava kaikki tarvittavat tekniset ja organisatoriset toimenpiteet, jotta tietojenkäsittelyssä nämä periaatteet toteutuvat (Euroopan unionin virallinen lehti, 2016).

3.3.8 Tietosuojavastaava

Uudistus tuo myös hallinnollisia uudistuksia rekisterinpitäjälle ja uudistuksen myötä määrättyjen rekisterinpitäjien täytyykin nimittää virallinen tietosuojavastaava (VAHTI -raportti, 2016). Rekisterinpitäjien ja henkilötietojen käsittelijöiden tulee itse varmistaa, onko heillä velvollisuus nimittää organisaatioonsa tietosuojavastaava. Tämä velvollisuus riippuu siitä, onko kyseessä julkisen sektorin toimija, pois lukien tuomioistuin, tai siitä, millaisten henkilötietojen käsittely muodostaa organisaation ydintehtävät. (Talus ym., 2017 .).

Tietosuojavastaava voi kuulua rekisterinpitäjän tai tietojenkäsittelyä tekevän organisaation henkilöstöön tai vastaavasti tämä tehtävä voi olla ulkoistettu. Joka tapauksessa tietosuojavastaavan täytyy omata riittävä pätevyys sekä asiantuntemus ja hänelle on myös taattava riittävä pääsy tietoihin ja niiden käsittelytoimenpiteisiin sekä muut tarvittavat resurssit tehtäviensä hoitamiseksi. Tehtävässään tietosuojavastaava raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle ja hänen asemansa tulee olla riippumaton. Häntä ei saada ohjeistaa tehtäviensä suorittamisessa eikä häntä luonnollisesti voida rangaista tehtävänsä asiallisesta suorittamisesta. (VAHTI -raportti, 2016, Talus ym., 2017, Euroopan unionin virallinen lehti, 2016.).

Tietosuojavastaavan tehtävänä on mm. rekisterinpitäjän tai henkilötietoja käsittelevien työntekijöiden neuvominen asetukseen kuuluvissa velvollisuuksissa, asetuksen toimeenpanon ja soveltamisen seuranta sekä tarvittavasta dokumentaatiosta huolehtiminen. Tietosuojavastaavan tehtäviin kuuluu lisäksi

myös yhteistyö ja muu yhteydenpito sekä valvontaviranomaisten että rekisteröityjen kanssa ja siksi nimitetyn tietosuojavastaavan yhteystiedot tulee julkistaa ja ilmoittaa valvontaviranomaiselle. (VAHTI -raportti, 2016, Talus ym., 2017, Euroopan unionin virallinen lehti, 2016.).

3.3.9 Sopimukset rekisterinpitäjien ja henkilötietojen käsittelijöiden välillä sekä tietojen siirtäminen Euroopan talousalueen ulkopuolelle.

Asetuksen mukaan rekisterinpitäjällä on oikeus ulkoistaa haluamansa osa tietojenkäsittelystä toiselle tietojenkäsittelijälle, mutta vain silloin kun myös tässä tietojenkäsittelyssä toteutuvat asetuksen vaatimukset ja rekisteröityjen oikeudet (VAHTI -raportti, 2016, Talus ym., 2017, Euroopan unionin virallinen lehti, 2016). Rekisterinpitäjän velvollisuus on varmistua siitä, että myös toimija, jolle tietojenkäsittely tai sen osa on ulkoistettu toteuttaa asetuksen vaatimukset toiminnassaan. Tätä varten rekisterinpitäjien ja tietojenkäsittelijöiden välille tulee solmia kirjallinen sopimus, jossa määritellään ainakin tietojenkäsittelyn kesto ja kohde, käsitellyn luonne ja tarkoitus, käsiteltävien henkilötietojen tyyppi sekä rekisterinpitäjän velvollisuudet ja oikeudet. Rekisterinpitäjän on myös varmistuttava siitä, että henkilötietojenkäsittelijä mm. noudattaa tietojenkäsittelyssä tarkoin ennalta dokumentoituja rekisterinpitäjän ohjeita sekä salassapitovelvollisuuttaan ja poistaa tai palauttaa henkilötiedot rekisterinpitäjälle kun käsittelypalvelut on saatettu päätökseen. (VAHTI -raportti, Euroopan unionin virallinen lehti, 2016.).

Myös toimijalla, jolle rekisterinpitäjä on siirtänyt osan tietojenkäsittelystä, on oikeus siirtää tiettyjen ehtojen toteutuessa, esim. rekisterinpitäjän kirjallisen luvan tähän saatuaan, tietojenkäsittely jollekin toiselle toimijalle. Siinäkin tapauksessa, että tietojenkäsittelijä ulkoistaa vaikkapa osan saamastaan toimeksiannosta toiselle tietojenkäsittelijälle, on tämä edelleen vastuussa ulkoistamansa tietojenkäsittelyn lainmukaisuudesta. (Euroopan unionin virallinen lehti, 2016.). Uudistuksen myötä siis ainakaan teoriassa kukaan ei pysty välttämään velvollisuuksiaan suhteessa asetukseen ulkoistamalla vastuuta kokonaan toiselle toimijalle.

Asetuksessa on myös vaatimuksia liittyen tietojen siirtämiseen Euroopan talousalueen ulkopuolelle eli kolmansiin maihin esimerkiksi juuri tietojenkäsittelyn ulkoistamisen yhteydessä. Asetuksen mukaan tämä voidaan tehdä ainoastaan tiettyjen ehtojen toteutuessa eli silloin kun Euroopan komissio on päättänyt, että kohdemaassa on varmistettu riittävä tietosuojan taso, jolloin erityistä lupaa siirtämiselle ei tarvita. Muussa tapauksessa siirto on mahdollista vain jos rekisterinpitäjä tai henkilötietojenkäsittelijä, joka on siirtämässä henkilötietoja kolmanteen maahan, on huolehtinut asianmukaisten suojakeinojen toteuttamisesta ja siitä, että rekisteröidyille on saatavilla asianmukaiset oikeussuojakeinot. (VAHTI -raportti, Euroopan unionin virallinen lehti, 2016.).

3.4 Asetuksen ongelmakohtia

Tässä luvussa käydään läpi joitain yleisestä tietosuoja-asetuksesta nousseitta kysymyksiä ja huolenaiheita. Nämä ongelmakohdat eivät sinällään ole olennaisia tämän tutkielman tai ISO/IEC 27001 -standardin ja tämän asetuksen vertailun kannalta, mutta silti myös asetukseen kohdistettu kritiikki voidaan nähdä osana asetuksen kattavaa esittelyä ja siksi joitain näitä esiin nostettuja kysymyksiä esitellään lyhyesti tässä luvussa. Tämän kappaleen tarkoitus onkin etupäässä vain osoittaa, että monien muiden uudistusten tavoin myöskään tämä asetus ei ole välttynyt kritiikiltä ja antaa tällä tavoin lukijalle kokonaisvaltaisempi kuva asetuksesta.

Eräs esiin noussut kritiikki asetusta kohtaan on se miten asetus mahdollisesti vaikeuttaa esimerkiksi tulevaisuuden lääketieteellistä tutkimusta nyt kun tietotekniikan kehittyessä myös lääketieteellinen tutkimus on muuttunut entistä dataintensiivisemmäksi ja suurten datamäärien käyttö tutkimuksessa on yleisempää kuin koskaan. Siitä huolimatta, että asetuksen vaatimuksissa on tiettyjä poikkeuksia käsittelyn liittyessä tieteelliseen tutkimukseen, saattavat asetuksessa annetut vaatimukset liittyen käsittelyyn vaadittavan suostumuksen hankkimiseen tai tietojen anonymisointiin olla kohtuuttomia ja erittäin haitallisia tutkimukselle. (Mostert, Bredenoord, Biesaart & van Delden, 2016.). Ongelmana siis on hankaloittavatko tiukat vaatimukset suostumuksen antamisesta käsittelyyn tai vaatimukset tietojen anonymisointiin myös yleisen edun mukaista tutkimustyötä.

Lisäksi on mahdollista, että asetuksen vaatimukset pystyä selvittämään rekisteröidylle automatisoitujen päätösten taustat sulkee käytöstä ison osan algoritmeja, joita tällä hetkellä käytetään automaattisessa päätöksenteossa mm. suosittelujärjestelmissä ja mainonnassa. Päätökset pitäisi pystyä tarvittaessa perustelemaan rekisteröidylle ja tämä aiheuttaa jo itsessään ongelman siitä, miten algoritmin toiminta pitäisi rekisteröidylle perustella. Lisäksi oppivat algoritmit lähtökohtaisesti keskittyvät löytämään ratkaisun eivätkä perustelemaan löydettyä ratkaisua. Ei ainakaan niin, että sen voisi yksinkertaisesti selvittää rekisteröidylle. (Goodman & Flaxman, 2016.).

Automaattisen päätöksenteon täytyy asetuksen mukaan myös olla syrjimätöntä eikä se saa siten sisältää arkaluontoiseen tietoon, kuten etnisyyteen, perustuvia syrjiviä päätöksiä. Kuitenkin jopa näennäisesti puolueettomat oppivat algoritmit saattavat sisältää olemassa olevia syrjinnän malleja, joita pelkkä tiettyjen arkaluontoisten tietojen puuttuminen ei poista eikä siten syrjimättömyys välttämättä toteudu. Näillä ongelmilla liittyen algoritmien tämänhetkiseen toimintaan on myös positiiviset puolensa, sillä asetus pakottaa nämä teknologiat muuttumaan läpinäkyvimmiksi, joka todella saattaa myös ehkäistä syrjintää. Toisaalta edelleen on epäselvää riittääkö annettu siirtymäaika näiden teknolo-

gioiden muokkaamiseen asetusta vastaaviksi. (Goodman & Flaxman, 2016.). Ongelmana siis on riittääkö asetuksessa annettu siirtymäaika näin suurten muutosten toteuttamiseen.

Myös asetuksessa näkyvästi edustettu suostumus henkilötietojen käsittelyyn ja sen antaminen ovat herättäneet kysymyksiä siitä, voidaanko tällaista internetin kautta annettua suostumusta todella pitää luotettavana kuvaajana käyttäjän toiveista yksityisyyden suhteen. Tämä pätee siitä huolimatta, että asetus on pyrkinyt parantamaan käyttäjän asemaa vaatimalla suostumuksen olevan mm. täsmällinen ja yksiselitteinen. Etenkin verkkoympäristössä annettu suostumus on kuitenkin monesti palvelun suhteen puolueellinen ja palvelut johdattelevat ja rohkaisevat käyttäjää monin tavoin, mukaan lukien palkitsemalla käyttäjää, antamaan suostumuksensa tietojen käsittelyyn. Siten suostumusta vahvasti painottava lähestymistapa ei välttämättä olekaan niin neutraali ja käyttäjäystävällinen kuin alustavasti voisi kuvitella. (Carolan, 2016.).

Myös tietosuojaviranomaisten asema uudistuksessa on herättänyt huolenaihetta. EU:n tietosuojaviranomaiset ovat siis itsenäisiä toimijoita omine valtuuksineen, jotka on tähän asti johdettu aiemmasta, vuoden 1995 henkilödirektiivistä. Tietosuojaviranomaisten tehtävä on valvoa tietosuojaa unionissa ja näiden viranomaisten välinen yhteistyö on lisääntynyt viime vuosina. Tietosuojaviranomaiset epäilevät, että uudistus tulee vaikuttamaan heihin merkittävästi ja vaikutukset heijastuvat etenkin eri tietosuojaviranomaisten väliseen EU:n sisäiseen yhteistyöhön. Uudistus tulee lisäämään tätä yhteistyötä, mutta epäselvää on kuitenkin tämän yhteistyön tiivistyessä se, kuinka paljon asetus tulee lopulta yhdentämään käytäntöjä ja kuinka paljon tai missä asioissa tietosuojaviranomaisille jää kansallista liikkumavaraa. Myös epäselvyys ja ongelmat esimerkiksi kieliasioissa yhteistyön lisääntyessä ovat nousseet esiin. Tietosuojaviranomaiset näkevät pääosin uudistuksen ja lisääntyvän viranomaisten välisen yhteistyön tärkeänä, mutta asetuksen epäillään lisäävän hallinnollisia tehtäviä sekä vaativan lisäresursseja ja uusia hallinnollisia mekanismeja. (Barnard-Wills, Chulvi & De Hert, 2016.). Uudistus ei siis vaikuta olevan vielä täysin selkeä edes niin keskeisille toimijoille kuin tietosuojaviranomaisille.

4 Yleisen tietosuoja-asetuksen ja ISO/IEC 27001 -standardin vertailua

Nyt kun luvuissa kaksi ja kolme on käyty läpi sekä ISO/IEC 27001 -standardia että yleistä tietosuoja-asetusta, voidaan siirtyä seuraavaksi näiden kahden keskinäiseen vertailuun, jotta voidaan saada vastaus siihen, kuinka hyvän lähtökohdan uudistuksen noudattamiseen standardi tarjoaa.

Aluksi käydään läpi muutamia yleisiä asioita vertailuun liittyen luvussa 4.1. Tämän jälkeen luvussa 4.2 suoritetaan itse vaatimusten vertailua. Vertailua ei tietenkään suoriteta lause lauseelta, vaan tutkitaan molempien kohdalla keskeisimpien linjausten yhteneväisyyksiä.

4.1 Yleistä vertailusta

Yleisellä tietosuoja-asetuksella ja ISO/IEC 27001 -standardilla on selvä yhteys molempien pyrkiessä turvallisempaan tietojen käsittelyyn. VAHTI -raportissa huomautetaan, että yleinen tietosuoja-asetus velvoittaa organisaation turvaamaan henkilötietojen käsittelyn toteuttamalla sopivat tekniset ja organisatoriset toimenpiteet ja näin varmistamaan se, että aiemmin määritelty tietosuojaperiaate eli eheys ja luottamuksellisuus toteutuu. Apukeinoksi organisaatioille näiden vaatimusten täyttämiselle ehdotetaan tietoturvallisuuden hallintamalleja ja nimenomaisesti ehdotetaan ”kansainvälisesti tunnettua standardia ISO/IEC 27001”(VAHTI -raportti, 2016, s.24). (VAHTI -raportti, 2016.).

Ensinnäkin on tärkeää huomata ISO/IEC 27001 -standardista puhuttaessa, että standardi vaatii sen pohjalta toteutettavalta ISMS:ltä lakien noudattamista ja tavoitteeksi nimenomaisesti ”kaikkien tietoturvallisuuteen liittyvien lakien ja asetusten, säännösten ja sopimusten velvoitteiden sekä mahdollisten turvallisuusvaatimusten noudattaminen”(SFS-ISO/IEC 27001, 2013, s.42). Hallintakeinona tähän esitetään kaikkien sovellettavien lakisääteisten ja sopimuksellisten

vaatimusten yksilöintiä, eli tarkemmin ”Kaikki asiaankuuluvat lakien, viranomaisten ja sopimusten asettamat vaatimukset sekä organisaation toimintamalli niiden täyttämistä varten on yksilöitävä yksiselitteisesti ja dokumentoitava sekä pidettävä ajan tasalla kutakin tietojärjestelmää ja organisaatiota varten”(SFS-ISO/IEC 27001, 2013, s.42). (SFS-ISO/IEC 27001, 2013 .).

Kuitenkin tämä on helpommin sanottu kuin tehty ja tässä tutkielmassa yritetään tarkastella kuinka hyvin standardin pohjalta toteutettu ja hyväksytty ISMS pystyisi vastaamaan tietosuoja-asetuksen organisaatioille tuomiin haasteisiin eli siihen kuinka hyvin standardin vaatimukset vastaavat lainsäädännöllisiä vaatimuksia. Täten, vaikka periaatteessa voitaisiinkin väittää, että standardin mukaisena hyväksytty ISMS vastaa täysin kaikkea soveltuvaa lainsäädäntöä sen ollessa edellytys hyväksymiselle, tämä jätetään tutkielmassa huomioimatta ja keskitytään mieluummin siihen kuinka standardi vaatimuksiltaan ja hallintakeinoiltaan vastaa tietosuoja-asetusta.

4.2 Vertailu

VAHTI -raportti nostaa esiin yleisen tietosuoja-asetuksen vaatimuksen rekisterinpitäjälle huolehtia tietoturvallisuudesta koko henkilötietojen elinkaaren ajan. Apuvälineiksi näihin velvoitteisiin raportissa on listattu yleisimpiä tietoturvallisuuden osa-alueita, joita rekisterinpitäjien tulisi ottaa huomioon henkilötietoja käsitellessään. Listaan kuuluvat ehdotettuine toimenpiteineen riskianalyysi, tietojärjestelmien hankinta, kehitys ja ylläpito, pääsynhallinta, omaisuuden ja tiedon hallinta, päivitysten ja muutosten hallinta, fyysinen turvallisuus, henkilöstöturvallisuus, toimittajien ja sopimusten hallinta, toiminnan jatkuvuuden hallinta, käsittelyn valvonta ja seuranta sekä viimeisenä tietoturvallisuuden hallinta. (VAHTI -raportti, 2016.).

ISO/IEC 27001:2013 ei ole teknologinen spesifikaatio ja siten se jättää varsinaisen toteutuksen tarkemmalla teknologisella tasolla itse organisaatiolle ja tarjoaa vaatimusmäärittelyn, johon organisaation ISMS:n täytyy pystyä vastaamaan saadakseen sertifikaatin. Kuitenkin standardi huomioi kaikki VAHTI -raportin yllä mainittujen tietoturvallisuuden osa-alueiden kohdat ja vaatii niihin toteutettavaksi soveltuvia hallintakeinoja (SFS-ISO/IEC 27001, 2013).

Hong ym. (2003) esittelevät artikkelissaan riskinhallinta teorian, jonka mukaan organisaation riskien analysoinnin ja arvioinnin kautta erinäiset tietoturvauhat ja -haavoittuvuudet voidaan arvioida ja tämän arvioinnin tuloksia voidaan käyttää päätettäessä tarkoituksenmukaisista turvallisuusvaatimuksista ja toimenpiteistä, jotta riski tietoturvalle saadaan hyväksyttävälle tasolle. Sekä yleinen tietosuoja-asetus että ISO/IEC 27001:2013 käyttävät tätä samaa riskiperusteista lähestymistapaa, jolla tarkoitetaan sitä, että velvoitteet ja toimenpiteet

on suhteutettava riskiin arvioimalla riskin toteutumisen seurauksia ja todennäköisyyttä. Tietosuoja-asetuksen tapauksessa riski kohdistuisi rekisteröityyn henkilötietoja käsiteltäessä, jolloin hänelle voisi toiminasta aiheutua haittaa esimerkiksi taloudellisen menetyksen muodossa. Riskiperusteisuudella pyritään siis suitsimaan matalariskisen toiminnan ylisäätelyä ja toisaalta suhtautumaan varovaisemmin korkeariskiseen toimintaan. (SFS-ISO/IEC 27001, 2013, Talus ym., 2017.).

ISO/IEC 27001:2013 -standardissa ei suoraan mainita tietosuojavaltuutettua eikä siten luonnollisesti tälle kuuluvaa asemaa tai tehtäviä, kuten tietosuoja-asetuksessa. Tästä huolimatta standardi kuitenkin tunnistaa ylimmän johdon vastuun määritellä kenellä on vastuu ja valtuudet varmistaa tietoturvallisuuden hallintajärjestelmän vaatimuksenmukaisuus standardiin nähden ja raportoida sen toiminnasta ylimmälle johdolle. Organisaatiossa täytyy myös määritellä niiden henkilöiden pätevyys, joiden työskentely vaikuttaa tietoturvallisuuden tasoon. Organisaation täytyy myös varmistaa, että näillä henkilöillä on todella riittävä pätevyys tehtäviinsä ja tarvittaessa hankkia heille tällainen pätevyys. Lisäksi organisaation on ”säilytettävä asianmukaista dokumentoitua tietoa näyttönä pätevyydestä”(SFS-ISO/IEC 27001, 2013, s.16). Organisaatiossa on jaettava kaikki tietoturvavastuut ja viestinnästä organisaation sisällä ja yhteydestä asianmukaisiin viranomaisiin täytyy huolehtia. Sisällöltään standardissa vaaditaan siis varsin samanlaisia asioita määrätyiltä henkilöiltä kuin tietosuojavaltuutetulta vaaditaan asetuksessa. (SFS-ISO/IEC 27001, 2013 .).

Standardi huomioi omalla tavallaan myös asetuksen vaatimukset rekisterinpitäjän ja tietojenkäsittelijän välisistä sopimuksista. Luonnollisesti nimenomaan yleisen tietosuoja-asetuksen noudattamista ei näissä sopimussuhteissa käsitellä, mutta standardissa on tarkkaan määritelty tietoturvallisuuden säilyttäminen toimittajasuhteissa. Esimerkiksi kaikista tietoturvavaatimuksista, joilla pyritään turvaamaan suojeltava omaisuus kuten henkilötiedot, täytyy sopia toimittajan kanssa ja nämä vaatimukset tulee myös dokumentoida. Nämä sopimukset on tehtävä kaikkien niiden toimijoiden kanssa, joilla saattaa olla pääsy tähän suojattavaan omaisuuteen, joten tämä ulottuu esimerkiksi tietosuoja-asetuksen kontekstissa myös niihin toimijoihin, joille alkuperäinen toimittaja edelleen ulkoistaa palveluitaan. Lisäksi organisaation on myös säännöllisesti seurattava ja katselmoitava toimittajien palveluiden toimittamista ja huolehdittava tarvittaessa muutosten hallinnasta toimittajan palveluissa. Lopulta standardi tarjoaa siis hyvät lähtökohdat myös näistä sopimuksista huolehtimiseen. (SFS-ISO/IEC 27001, 2013.).

Eräs todella hyvin edustettu piirre ISO/IEC 27001 -standardissa on dokumentointi ja sen merkitys. Standardissa on siis vahva painotus dokumentaatioon lähes kaikissa järjestelmän osissa ja päätöksenteossa. Dokumentaation tuottamiseen ja päivittämiseen on lisäksi asetettu standardissa myös tarkemmat säännöt ja ohjeistukset sekä se, miten dokumentaatiota tulee hallita. Huomatta-

vaa on kuitenkin, että standardi tunnistaa sen, että vaikka tiettyjen vaatimusten dokumentaation suhteen täytyy toteutua, eri organisaatiot tuottavat kuitenkin eri laajuista dokumentoitua tietoa johtuen organisaatioiden välisistä eroista. Dokumentaatiota käytetään esimerkiksi auditointeihin ja sertifiointitarkoituksiin. (SFS-ISO/IEC 27001, 2013.).

Tämä dokumentoinnin suuri merkitys käy hyvin yhteen yleisen tietosuoja-asetuksen kanssa ja jo aiemmin mainittu osoitusvelvollisuus, eli organisaation velvoite itse osoittaa toimenpiteidensä lainmukaisuus, on organisaatiolle potentiaalisesti erittäin suuri velvoite, eräänlainen syyttömyysolettaman vastakohta. Organisaatio saisi varsin kattavan apukeinon standardin dokumentointikäytännöistä, jonka avulla se potentiaalisesti pystyisi suoriutumaan hyvin tästä velvollisuudesta.

Lisäksi organisaation on mahdollista hakea sertifikaattia todistuksena asetuksen vaatimusten täyttämisestä ja sitoutumisestaan tietosuojaan. Koska ISO/IEC 27001 käyttää laajaa dokumentointia osaltaan myös sertifiointitarkoituksessa antaisi standardin dokumentointikäytäntö varmasti myös hyvät lähtökohdat tietosuoja-asetuksen vaatimusten mukaisen sertifikaatin hakemiseen. On kuitenkin pidettävä mielessä, että mikään sertifikaatti ei lain mukaan vähennä organisaation vastuuta noudattaa asetusta eikä vähennä toimivaltaisen viranomaisen tehtäviä tai valtuuksia. (Euroopan unionin virallinen lehti, 2016.).

De Hert, Papakonstantinou ja Kamara (2016) huomauttavat artikkelissaan, että luodessaan standardia ISO/IEC 27018:2014, joka siis käsittelee pilvilaskentaa ja kuuluu samaan standardiperheeseen kuin ISO/IEC 27001, ISO huomioi EU:n tietosuoja-asetuksen pääpiirteissään, mutta on pyrkinyt myös ottamaan etäisyyttä siihen ja halunnut säilyttää kansainvälisen luonteensa. Standardi ei siis yritäkään korvata lainsäädäntöä tai olla kaikenkattava, sillä standardi, joka vastaisi kaikkien eri alueiden lainsäädäntöä on pelkästään ajatuksena epärealistinen ja saattaisi menettää käytettävyyttään. Tämän sijaan standardi painottaa asettavansa eräänlaiset minimivaatimukset lakien ja sopimusten noudattamiselle ja pyrkii siis pikemminkin avustamaan ja toimimaan yhtenä rakennuspalikkana, jonka pohjalta organisaatio kykenee vastaamaan lainsäädännöllisiin velvoitteisiinsa. Standardin käyttäminen toimiikin viestinä sekä asiakkaille, että viranomaisille organisaation sitoutumisesta henkilötietojen suojaamiseen ja toimii merkkinä organisaation halusta vastata velvoitteisiinsa, vaikka standardi ei täysin vastaisikaan lainsäädäntöä. (De Hert ym., 2016.).

Tässä luvussa esitettyjen vertailujen perusteella voidaan todeta, että tilanne on varsin samankaltainen kuin De Hert ym. (2016) artikkelissa. Kuten samaan standardiperheeseen kuuluva ISO/IEC 27018:2014, myös ISO/IEC 27001:2013 tarjoaa erinomaisen perustan, jonka pohjalta organisaatio voi lähteä tavoittelemaan täyttä tietosuoja-asetuksen vaatimuksienmukaisuutta. Vertailu on osoittanut, että tietosuoja-asetuksessa ja ISO/IEC 27001:2013 -standardissa on monia yhtäläisyyksiä ja standardi on epäilemättä loistava työkalu organisaatiol-

le, joka haluaa vastata asetuksen velvoitteisiin. ISO/IEC 27001:2013 ei välttämättä vastaa täysin lainsäädäntöä kaikilta vaatimuksiltaan, eikä sen maailmanlaajuisen levinneisyytensä vuoksi välttämättä kannatakaan, sillä näin standardi kykenee säilyttämään neutraalin asemansa koko maailman standardina.

Toisaalta standardin seuraavaa versiota ajatellen tähän saattaa tulla muutos, sillä kuten aiemmin kävimme läpi, asetuksen soveltamisala on varsin laaja ja EU:n ollessa varsin keskeinen talousalue monet lähtökohtaisesti EU:n ulkopuoliset organisaatiot tulevat olemaan asetuksen soveltamisalan piirissä. Tällöin asetuksen soveltamisalan kasvaessa ISO:n ja IEC:n kannattaa harkita uudelleen haluavatko ne edelleen standardin säilyttävän etäisyytensä EU-lainsäädäntöön silloinkin kun tarpeeksi suuri osa standardin käyttäjistä kuuluu tämän soveltamisalan piiriin.

5 Yhteenveto

Tässä tutkielmassa tarkasteltiin tietoturvallisuuden hallintaa tietoturvallisuuden hallintajärjestelmien, käytännössä ISO/IEC 27001 -standardin kautta. Tutkielmassa tarkasteltiin tietoturvallisuuden hallintajärjestelmien tarkoitusta ja ISO/IEC 27001 -standardia erityisen tarkasti. Standardi on siis kahden kansainvälisen toimijan ISO:n ja IEC:n perustaman yhteisen teknisen komitean tuotos (SFS-ISO/IEC 27001:2013). Standardi perustuu PDCA -malliin eli jatkuvaan kehittämiseen (Humphreys, 2008). Standardi siis sisältää vaatimukset tietoturvallisuuden hallintajärjestelmälle eikä sitä ole tarkoitettu kaikenkattavaksi ja jäykäksi malliksi, vaan se on tarkoitettu kaikille organisaatioille toimialasta, koosta tai maantieteellisestä sijainnista riippumatta ja sen on tarkoitus muuttua organisaation mukana (Calder, 2013).

ISO/IEC 27001 -standardilla on kansainväliset lähtökohdat sekä laaja levinneisyys (Susanto ym., 2011). Nämä seikat tekevät siitä ihanteellisen vertailtavan yleiseen tietosuoja-asetukseen, jolla on myös kansainväliset lähtökohdat ja laaja levinneisyys. Standardi on muutoinkin vakiinnuttanut paikkansa tietoturvallisuuden hallinnan alalla ja sitä käytetään sekä julkisella että yksityisellä sektorilla kaiken kokoisissa organisaatioissa (Humphreys, 2008). Tutkielman pohjalta lukija ymmärtää standardin historian sekä sen, miten standardi toimii ja mitä se pitää sisällään sekä sen, miksi nimenomaan tätä standardia kannatti verrata tietosuoja-asetuksen vaatimuksiin.

Tietosuojauudistuksen myötä voidaan sanoa, että henkilötietojen käsittelyssä alkavat näkymään myös EU:n yhteinen arvomaailma kun käsittelystä on pyritty tekemään sellaista, joka turvaisi rekisteröityjen yksityisyyden, itsemääräämisoikeuden, syrjimättömyyden ja toisi käsittelyyn lisää kaivattua läpinäkyvyyttä (McDermott, 2017). Kyseessä onkin maailmanlaajuisesti ennennäkemätön pyrkimys parantaa kansalaisten yksityisyydensuojaa (Martin & Murphy, 2017).

Uudistus oli suunnitteilla useita vuosia ja se tarkoitettiin paikkaamaan auttamattomasti vanhentunutta vuoden 1995 henkilödirektiiviä, jota ei oltu päi-

vitetty lainkaan direktiivin julkaisuvuoden jälkeen (Krystlik, 2017). Lainsäädännön uudistusta suunniteltaessa esille nousi erityisesti kaksi suurta huolenaihetta: internetin korostunut asema ja tietojärjestelmien monimutkaistuminen (Lloyd, 2017). Myös EU:n kansalaiset ovat ilmaisseet huolensa monista niistä ongelmakohdista, joita asetus pyrkii nyt paikkaamaan (eurobarometri, 2015).

Yleinen tietosuoja-asetus tuo mukanaan monia rekisteröityjen oikeuksia ja toisaalta rekisterinpitäjien velvollisuuksia, joista keskeisimpinä tutkielmassa esiteltiin:

- laajennukset maantieteellisessä toimivallassa,
- uudet ankarammat sanktiot velvollisuuksiaan laiminlyöville rekisterinpitäjille,
- vahvemmat ehdot suostumuksen antamiselle tietojen käsittelyyn,
- rekisterinpitäjän ja toisaalta henkilötietojen käsittelijän ilmoitusvelvollisuuden,
- rekisteröidyn oikeus ”tulla unohdetuksi” eli saada itseään koskevat tiedot poistetuksi rekisteristä,
- rekisteröidyn oikeus siirtää tietonsa järjestelmästä toiseen ja saada pääsy omiin tietoihinsa,
- rekisterinpitäjän velvollisuus huolehtia, että tietojen käsittelyssä toteutuvat oletusarvoisesti tietosuojaperiaatteet, joiden noudattamista tämän on myös pystyttävä tarvittaessa osoittamaan,
- rekisterinpitäjän velvollisuus osoittaa tehtäväänsä soveltuva tietosuojavaltuutettu, jonka tehtäviin kuuluu monia eri velvollisuuksia asetuksen toimeenpanemisessa organisaatiossa,
- rekisterinpitäjän ja tietojenkäsittelijän velvollisuus huolehtia sopimuksilla siitä, että asetusta noudatetaan myös silloin kun tietojenkäsittely ulkoistetaan sekä siitä, että henkilötiedot voidaan siirtää kolmansiin maihin vain tiettyjen ehtojen täyttyessä. (VAHTI -raportti, Talus ym., 2017, EUGDPR.org, Euroopan unionin virallinen lehti, 2016.).

Tutkielman laajuuteen nähden käytiin siis melko kattavasti läpi tätä yleistä tietosuoja-asetusta, sen taustaa, sen keskeisimpiä uudistuksia sekä joitain esiin nousseita huolenaiheita ja lukija tietää nyt paremmin, mistä asetuksessa on kyse. Kun tutkielmassa on käyty läpi mistä sekä tietosuoja-asetuksessa että ISO/IEC 27001 -standardissa on kyse, vertailtiin asetuksen vaatimuksia standardiin, jotta voitiin selvittää kuinka hyvän pohjan asetuksen velvoitteista suoriutumiseen standardin mukainen tietoturvallisuuden hallintajärjestelmä antaisi. Vertailusta selvisi, että standardi vastaa vaatimuksiin varsin hyvin antaen sitä käyttävälle organisaatiolle hyvät lähtökohdat asetuksen tuomista laillisista velvoitteista suoriutumiseen.

Varsin hyvästä suoriutumisestaan huolimatta standardin on kuitenkin tarkoitus toimia pikemminkin rakennuspalikkana kohti täysin asetuksen velvoit-

teet kattavaa tietojen käsittelyä kuin valmiina pakettiratkaisuna ja standardi on tarkoituksella pyrkinyt pitämään etäisyytensä tietosuoja-asetukseen pitäen kiinni kansainvälisestä luonteestaan (De Hert ym., 2016).

Yleinen tietosuoja-asetus tuo siis mukanaan monia uudistuksia, jotka teettävät taatusti lisätyötä organisaatioille, mutta täytyy kuitenkin muistaa, että asetus ei ole vielä tullut sovellettavaksi, joten merkittävimmät seuraukset uudistuksesta nähdään vasta todennäköisesti usean vuoden päästä kun asetusta aletaan soveltamaan käytännössä. Tämän pohjalta alkaa muodostumaan hiljalleen oikeuskäytäntöä, jolloin vasta saadaan parempi kuva siitä, kykeneekö asetus todella korjaamaan ne ongelmat, joita varten se laadittiin.

Tämä yhdistettynä vertailun hyviin tuloksiin antaa aihetta jatkotutkimukselle. Tulevaisuudessa voidaan esimerkiksi jo ihan käytännössä tutkia kuinka hyvin standardi vastaa asetuksen velvoitteisiin esimerkiksi seuraamalla ISO/IEC 27001 -sertifioituja organisaatioita. Voidaan esimerkiksi tutkia sitä, onko näille virallisen sertifioinnin ansainneille organisaatioille määrätty, ilmeisestä sitoutumisesta tietoturvallisuuteen huolimatta, asetuksen laiminlyönnistä sanktioita. Toisaalta voidaan myös seurata tulevaisuudessa uusien myönnettyjen sertifikaattien määrien mahdollisia muutoksia ja tutkia onko sillä yhteyttä standardin suoriutumiseen yleisen tietosuoja-asetuksen vaatimuksista.

LÄHTEET

Barnard-Wills, D., Chulvi, C. P., & De Hert, P. (2016). Data protection authority perspectives on the impact of data protection reform on cooperation in the EU. *Computer Law & Security Review*, *32*(4), 587-598. Haettu 19.9.2017: http://www.sciencedirect.com/science/article/pii/S026736491630084X

Calder, A. (2013). ISO27001/ISO27002: A pocket guide. IT Governance Publishing. Haettu 6.8.2017 osoitteesta:
https://books.google.fi/books?hl=en&lr=&id=uFObBAAAQBAJ&oi=fnd&pg=PA5&dq=9)+Calder,+A.+(2013).+ISO27001/ISO27002:+A+pocket+guide.+IT+Governance+Publishing.&ots=bU9ifol6Uo&sig=7vy05cyMCEQendPI6PJib0J4eB4&redir_es

Carolan, E. (2016). The continuing problems with online consent under the EU's emerging data protection principles. *Computer Law & Security Review*, *32*(3), 462-473. Haettu 19.9.2017 osoitteesta: http://www.sciencedirect.com/science/article/pii/S0267364916300322

De Hert, P., Papakonstantinou, V., & Kamara, I. (2016). The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. Computer Law & Security Review, 32(1), 16-30. Haettu 6.8.2017 osoitteesta: http://www.sciencedirect.com/science/article/pii/S0267364915001703#s0060

EUGDPR.org: GDPR Key Changes. Haettu 6.8.2017 osoitteesta: http://www.eugdpr.org/key-changes.html

Eurobarometri. Haettu 6.8.2017 osoitteesta: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

Euroopan unionin virallinen lehti, suomenkielinen laitos (2016). Haettu 6.8.2017 osoitteesta: http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=FI

Goodman, B., & Flaxman, S. (2016, June). EU regulations on algorithmic decision-making and a "right to explanation". In *ICML workshop on human interpretability in machine learning (WHI 2016), New York, NY. http://arxiv.org/abs/1606.08813 v1*. Haettu 19.9.2017 osoitteesta: https://pdfs.semanticscholar.org/f051/55c4d7d77f32855b80a86bb987818838d50d.pdf

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. Information Management & Computer Security, 11(5), 243-248.
Haettu 6.8.2017 osoitteesta:
http://www.emeraldinsight.com/doi/full/10.1108/09685220310500153

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. information security technical report, 13(4), 247-255. haettu 6.8.2017 osoitteesta: http://www.sciencedirect.com/science/article/pii/S1363412708000514

IEC - International Electrotechnical Commission: About the IEC (2017). Haettu 7.8.2017 osoitteesta: http://www.iec.ch/about/

ISO - International Organization for Standardization: All about ISO. Haettu 7.8.2017 osoitteesta: https://www.iso.org/about-us.html

ISO - International Organization for Standardization: Certification. Haettu 6.8.2017 osoitteesta: https://www.iso.org/certification.html

ISO - International Organization for Standardization: ISO/IEC 27001 Information security management. Haettu 6.8.2017 osoitteesta: https://www.iso.org/isoiec-27001-information-security.html

ISO - International Organization for Standardization: ISO Survey of certifications to management system standards - Full results (2015). Haettu 6.8.2017 osoitteesta: http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

Krystlik, J. (2017). With GDPR, preparation is everything. Computer Fraud & Security, 2017(6), 5-8. Haettu 5.8.2017 http://www.sciencedirect.com/science/article/pii/S1361372317300507

Lloyd, I. (2017). Information technology law. Oxford University Press. (tyylii sivulta 44? lakiuudistuksen taustoihin) Haettu 6.8.2017 osoitteesta:

https://books.google.fi/books?hl=fi&lr=&id=Bt1KDgAAQBAJ&oi=fnd&pg=PP1&dq=general+data+protection+regulation&ots=Cqpi5H0KrC&sig=t1rv2LynQ8-wA9k2HgD6y443WlPs&redir_esc=y#v=onepage&q=general%20data%20protection%20regulation&f=false

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. Journal of the Academy of Marketing Science, 45(2), 135-155. Haettu 6.8.2017 osoitteesta: https://link.springer.com/article/10.1007/s11747-016-0495-4

McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. Big Data & Society, 4(1), 2053951716686994. Haettu 6.8.2017 osoitteesta: http://journals.sagepub.com/doi/full/10.1177/2053951716686994

Mostert, M., Bredenoord, A. L., Biesaart, M. C., & van Delden, J. J. (2016). Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. *European Journal of Human Genetics*, *24*(7), 956-960. Haettu 19.9.2017 osoitteesta: http://www.nature.com/ejhg/journal/v24/n7/full/ejhg2015239a.html

SFS-ISO/IEC 27001 (2013). ISO/IEC 27001:2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270. Haettu 6.8.2017 osoitteesta: http://www.sciencedirect.com/science/article/pii/S0378720609000561

Suomen standardoimisliitto SFS ry (2012). SFS-Käsikirja 327. ISO/IEC 27001:2005.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences IJECSIJENS, 11(5), 23-29. Haettu 6.8.2017 osoitteesta: http://www.academia.edu/download/30294093/113505-6969-ijecs-ijens.pdf

Talus, A., Autio, E., Hänninen, A., Pihamaa, H-T., Kantonen, S. ”Miten valmistautua EU:n tietosuoja-asetukseen?”, Oikeusministeriön julkaisu, January 2017. Haettu 6.8.2017 osoitteesta:
http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Tietosuojavaltuutetun toimisto: Sanastoa tietosuojauudistukseen liittyen (2016, 5. huhtikuuta). Haettu 6.8.2017 osoitteesta: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/sanastoa.html

Vacca, J.R. (2013). Computer and Information Security Handbook. (Second Edition). Waltham, Massachusetts: Elsevier Inc. Haettu 6.8.2017 osoitteesta:
https://books.google.fi/books?hl=fi&lr=&id=zb916YOr16wC&oi=fnd&pg=PP1&dq=information+security+management+handbook&ots=PRhKcMt1Xy&sig=zbCS4GL9XH-Liw2LhH_vB2XuPSHU&redir_esc=y#v=onepage&q=information%20security%20management%20handbook&f=false

VAHTI-raportti – 1/2016. ”EU-tietosuojan kokonaisuudistus”, 2016. Haettu 6.8.2017 osoitteesta: https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128