Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2018

Hannu Pohjalainen

GDPR JA SEN VERTAAMINEN YHDYSVALTOJEN TIETOSUOJASÄÄNTELYYN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2018 | 34 sivua

Hannu Pohjalainen

GDPR JA SEN VERTAAMINEN YHDYSVALTOJEN TIETOSUOJASÄÄNTELYYN

GDPR (General Data Protection Regulation) on EU:n uusi yleinen tietosuoja-asetus 2016/679. Opinnäytetyön tarkoituksena oli kartoittaa tietosuoja-asetuksen tuomia keskeisiä muutoksia henkilötietoja ja henkilörekisteriä käsiteltäessä sekä selvittää asetuksen tuomia velvoitteita rekisterinpitäjälle. Opinnäytetyössä tutustuttiin myös Yhdysvaltojen henkilötietojen käsittelyä ja yksityisyyttä koskevan lainsäädännön rakenteeseen ja verrattiin keskeisten lakien pääkohtia EU:n tietosuoja-asetukseen. Tietolähteenä työssä käytettiin pääosin internetistä löytyviä materiaaleja. Tämän lisäksi toteutettiin asiantuntijahaastattelu, josta saatiin käytönnönnäkökulmaa tietosuoja-asetuksen vaatimiin teknisiin edellytyksiin. Erilaisten verkkolähteiden lisäksi suuri osa tiedoista kerättiin viranomaissivustoilta ja Euroopan unionin virallisesta lehdestä, tavoitteena saada mahdollisimman tarkkaa tietoa.

Opinnäytetyön rakenne muodoistui EU:n ja Yhdysvaltojen tietosuojaa koskevan lainsäädännön läpikäynneistä yleisellä tasolla. Uuden tietosuoja-asetuksen tuomiin muutoksiin tutustuttiin syvemmin rekisterinpitäjän, henkilötiedon käsittelijän ja rekisteröidyn näkökulmasta. Neljännessä kappaleessa käytiin läpi organisatorisia ja teknisiä toimenpiteitä, joiden avulla toteuttaa tietosuoja-asetuksen vaatimat velvoitteet henkilötietojen käsittelyssä.

Opinnäytetyön tavoitteessa kartoittaa EU:n yleisen tietosuoja-asetuksen ja Yhdysvaltojen vastaavan lainsäädännön keskeiset kohdat onnistuttiin ja lopputuloksena on sivistävä ja suuntaa antava työ tietosuojan merkityksestä henkilötietoja käsittelevissä yrityksissä.

ASIASANAT:

Tietosuoja-asetus, GDPR, tietosuoja, henkilörekisteri

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information technology

2018 | 34 pages

Hannu Pohjalainen

GDPR AND HOW IT DIFFERS FROM U.S.A. DATA PROTECTION REGULATIONS

The EU General Data Protection Regulation 2016/679 (GDPR) did take effect on 25 May 2018. In this thesis, the objective was to study what effects the GDPR has on personal data controller and point out the legislative changes in EU. This thesis also clarifies the key privacy laws of U.S. legislation and compares the privacy legislation between EU and U.S.A. The sources used in this thesis were GDPR-related online publications and one interview with a GDPR consultant. The main source was the Official Journal of the European Union to obtain as accurate information as possible.

This thesis contains the essential parts of GDPR and U.S. Privacy laws. The effects of GDPR on data controller, data processor and data subject were thoroughly examined. This thesis also lists useful organizational and technical measures to disclose the ways the requirements of GDPR on processing personal data can be managed in organizations.

This thesis' outlined what the compliance of the GDPR means for the data controller and how privacy legislation between U.S. and EU differs. In conclusion, this thesis provides an educative and directive summary about significance of the privacy protection in the organizations which process personal data in both EU and U.S.

KEYWORDS:

GDPR, privacy law, data controller, data handler, data protection

SISÄLTÖ

SANASTO **6**

1 JOHDANTO **7**

2 TIETOSUOJA-ASETUKSEN TAUSTAA **8**

2.1 Lähtökohta 8

2.2 Tavoitteet uudistukselle 9

2.3 EU:n yhtenäisyys, digitalisaatio ja yleinen tekninen kehitys 9

3 TIETOSUOJA-ASETUS KÄYTÄNNÖSSÄ **11**

3.1 Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet 11

3.1.1 Osoitusvelvollisuus 11

3.1.2 Sopimusvaatimukset 12

3.1.3 Tietosuojavastaava 12

3.1.4 Henkilötietojen käsittelyn lainmukaisuus 13

3.1.5 Sisäänrakennettu ja oletusarvoinen tietosuoja 14

3.1.6 Suoramarkkinointi 15

3.1.7 Siirrot kolmansiin maihin 15

3.1.8 Sakot ja sanktiot 16

3.2 Rekisteröidyn oikeudet 16

3.2.1 Läpinäkyvyys ja rekisteröidyn oikeus päästä tietoihin 16

3.2.2 Oikeus tietojen muuttamiseen ja käsittelyn rajoittamiseen 17

3.2.3 Oikeus siirtää tiedot järjestelmästä toiseen 18

3.2.4 Vastustamisoikeus ja automaattisesti tehtävät yksittäispäätökset 18

4 YHDYSVALTOJEN TIETOSUOJALAIT **19**

4.1 Tunnetuimpia liittovaltion tietosuojalakeja 20

4.2 EU:n ja Yhdysvaltojen tietosuojalainsäädännöt vertailussa 21

4.3 Privacy Shield 24

5 MITEN LÄHESTYÄ TIETOTURVA-ASETUKSEN VELVOITTEITA **26**

5.1 Riskiarvio, vaikutustenarviointi ja tietotilinpäätös 26

5.2 Nykytila-analyysi 28

5.3 Pilvipalvelut 29

5.4 Organisatoriset ja tekniset toimenpiteet 30

6 POHDINTA **32**
6.1 Tietosuoja-asetuksen vaikutus 32
6.2 Yhdysvaltojen lait vs GDPR 32
6.3 Työn tavoitteen toteutuminen 33

LÄHTEET **34**

KUVAT

Kuva 1. Asetuksen sisältö ja tavoite 10
Kuva 2. Riskien arviointi 27

SANASTO

Anonymisointi	Henkilötiedon tunnistettavuuden poistaminen siten, että yhdistäminen rekisteröityyn ei enää ole mahdollista (Ohjelmistoyrittäjät ry 2018).
Pseudomisointi	Henkilötietojen käsittelemistä niin, että tietoja ei voida enää suoraan yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja (Ohjelmistoyrittäjät ry 2018).
Transatlanttinen	Atlantin yli tapahtuva; Yhdysvaltain ja Euroopan välinen (Wikisanakirja 2018).

1 JOHDANTO

Tämän opinnäytetyön aiheena on Euroopan Unionin yleinen tietosuoja-asetus GDPR (General data protection regulation) ja sen tuomat velvoitteet rekisterinpitäjän henkilötietojen käsittelyssä. Tarkastelua tehdään sellaisen organisaation näkökulmasta, joka toimii myös Yhdysvalloissa. EU:n tietosuoja-asetusta verrataan Yhdysvaltojen henkilötietojen käsittelyä koskeviin lakeihin ja säädöksiin. Työssä tuodaan esille näiden kahden eroavaisuuksia.

Yleinen tietosuoja-asetus 2016/679 (EU) astui voimaan 24.5.2016. Asetuksella on kahden vuoden siirtymäaika ja sitä tullaan soveltamaan 24.5.2018 kaisissa EU:n jäsenvaltioissa. Tietosuoja-asetus GDPR koskee kaikkia organisaatioita, yrityksiä ja järjestöjä jotka käsittelevät EU:n alueella sijaitsevien luonnollisten henkilöiden henkilötietoja. Asetuksen tarkoituksena on: ”tukea vapauden, turvallisuuden ja oikeuden alueen ja talousunionin kehittämistä, taloudellista ja sosiaalista edistystä, talouksien lujittamista ja lähentämistä sisämarkkinoilla sekä luonnollisten henkilöiden hyvinvointia”. Periaatteena on henkilön perusoikeus henkilötietojen suojaan kansalaisuudesta ja asuinpaikasta riippumatta. Asetus tulee kumoamaan EU:n henkilötietodirektiivin 95/46/EY. (Yleinen tietosuoja-asetus 2016/679, Perus 2).

Yhdysvalloissa ei ole voimassa samanlaista kattavaa yksityisyyttä suojaavaa henkilötietolakia kuten Euroopassa. Yhdysvalloissa henkilötietoja säädellään etupäässä sektorikohtaisilla liittovaltion laeilla ja valtion laeilla. Henkilötietoja koskevat lait ja niiden sääntely perustuu toimialakohtaiseen (eng. sector-specific) lähestymistapaan. Esimerkiksi terveys- ja potilastietoja säätelee The Health Insurance Portability and Accountability Act (HIPAA) ja taloudellisten tietojen keräystä, käyttöä ja julkistamista The Financial Services Modernization Act (Gramm-Leach-Bliley Act(GLB)). (Eaton 2017.)

2 TIETOSUOJA-ASETUKSEN TAUSTAA

Tässä luvussa käydään läpi EU:n yleisen tietosuoja-asetuksen taustaa ja tavoitteita.

2.1 Lähtökohta

Yleinen tietosuoja-asetus otettiin voimaan 24.5.2016 Euroopan parlamentin ja neuvoston toimesta ja sen soveltaminen alkaa 25.5.2018 kaikissa EU:n jäsenvaltioissa. Toukokuussa 2018 henkilötietojen käsittelyn tulee olla tietosuoja-asetuksen mukaista. Sitä sovelletaan niin yksityisellä kuin julkisella sektorilla henkilötietojen käsittelyssä luonteesta, laajuudesta ja käytetystä teknologiasta riippumatta. Asetus koskee kaikkia soveltamisalaan kuuluvia henkilötietoja käsitteleviä organisaatioita, rekisterinpitäjiä ja muita henkilötietojen käsittelijöitä. (Oikeusmininsteriö Tietosuojavaltuutetun toimisto 2017.)

EU:n henkilötietodirektiivi 95/46/EY kumotaan tällä asetuksella. Suomessa Henkilötietolaki (523/1999) on henkilötietojen käsittelyn peruslaki, joka on säädetty turvaamaan yksityiselämän suojaa sekä käsiteltäessä henkilötietoja muissa yksityisyyden suojaa turvaavissa perusoikeuksissa. Laki pyrkii edistämään tietojenkäsittelytavan kehittämistä ja noudattamista. Laki ei kuitenkaan koske henkilötietojen käsittelyä, jonka luonnollinen henkilö suorittaa tavanomaisiin yksityisiin tai yksinomaan henkilökohtaisiin tarkoituksiinsa. (Henkilötietolaki 523/1999, 2. §.) Hallituksen esitys (HE 9/2018) EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi annettiin eduskunnalle 1.3.2018. Tietosuoja-asetuksen mukaiset muutokset esitetään toteutettavan säätämällä uusi tietosuojalaki, joka toimisi GDPR:ää täydentävänä ja täsmentävänä henkilötietojen käsittelyä koskevana yleislakina. (Eduskunta 2018.)

Vaikka henkilötietodirektiivin 95/46/EY tavoitteet ja periaatteet pätevät edelleen, poikkeavat jäsenvaltioiden lainsäädännöt luonnollisten henkilöiden henkilötietojen käsittelyssä liikaa toisistaan. Direktiivin avulla ei ole pystytty estämään tietosuojan hajanaisuutta, oikeudellista epävarmuutta ja laajalle levinnyttä olettamusta, jonka mukaan verkkoympäristössä toimiminen ei ole turvallista ja siihen sisältyy huomattavia riskejä. (Yleinen tietosuoja-asetus 679/2016, Perus 9)

2.2 Tavoitteet uudistukselle

Tietosuoja-asetuksen tarkoituksena on vastata teknologian kehitykseen ja globalisaation liittyviin henkilötietojen suojaa koskeviin haasteisiin sekä ajantasaistaa tietosuojaa koskevaa sääntelyä. Henkilödirektiivin 95/46/EY tavoite sallia jäsenvaltioiden välillä henkilötietojen vapaa liikuteltavuus sekä tavoite yksilön tietosuojan perusoikeuksien suojaamisesta ei ole enää riittävän yksityiskohtaista digitalisaation ja yleisen teknisen kehityksen alla. Tietosuojan hajainaisuus EU:n alueella on luonut epävarmuutta kansalaisten, yritysten ja viranomaisten kesken. Luottamus verkkotoimintaan on laskenut oikeudellisten seikkojen eroavaisuuksien, riskien ja epävarmuustekijöiden johdosta. (Tietosuojavaltuutetun toimisto 4/2017, 9.)

Tietosuoja-asetus pyrkii rakentamaan luottamusta yhdenmukaistamalla jäsenvaltioiden tietosuojaa koskevat säännökset ja tukemalla digitaalitalouden kehitystä sisämarkkinoilla. Luottamusta lisätään vahvistamalla rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä ja lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä. (Tietosuojavaltuutetun toimisto 4/2017, 9.)

2.3 EU:n yhtenäisyys, digitalisaatio ja yleinen tekninen kehitys

Kumottu henkilötietodirektiivi on lainsäädäntöohje, joka asettaa tavoitteet jäsenvaltioille. Jäsenvaltiot ovat soveltaneet henkilötietojen käsittelyä koskevaa henkilötietodirektiiviä omiin lainsäädäntöihinsä mikä on luonut eroavaisuuksia jäsenvaltioiden tietosuojalainsäädännöissä. EU:n jäsenvaltioissa toimiva rekisterinpitäjä on joutunut erikseen asioimaan kunkin maan tietosuojaviranomaisen kanssa sekä tutustumaan jokaisen maan tietosuojalainsäädäntöön. Uusi tietosuoja-asetus tulee yhtenäistämään tietosuojasääntelyn sekä EU:ssa että sen ulkopuolella toimiville rekisterinpitäjille. (Pietikäinen 2016.)

Teknologian kehittyminen ja digitalisoituminen ovat johtaneet yhä globaalimpaan liiketoimintaan. Henkilötietoja, sosiaalista mediaa, sijaintietoja ja pilvipalveluita hyödyntävät palvelut ovat lisääntyneet ja kasvattaneet henkilötietojen käsittelyä sekä muuttaneet tietosuojatarpeiden luonnetta. Eurooppalaisen tietosuojasääntelyn uudistaminen on ollut välttämätöntä uusien teknologioiden ja tiedonkeruumenetelmien kehittyessä sekä liiketoiminnan kansainvälistyessä huomattavasti. Säätellyllä ei pyritä

rajoittamaan digitaalista liiketoimintaa vaan yhtenäistämään käytänteitä ja turvaamaan rekisteröityjen oikeuksia. (Pietikäinen 2016.)

Kuva 1. Asetuksen sisältö ja tavoite (Opitietosuojaa.fi 2016).

3 TIETOSUOJA-ASETUS KÄYTÄNNÖSSÄ

Tässä luvussa käydään läpi tietosuoja-asetuksen tuomia velvoitteita rekisterinpitäjälle sekä henkilötietojen käsittelijälle.

3.1 Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet

Monille organisaatioille syntyy ongelma siitä, että henkilötietoja käsiteltäessä useassa tietojärjestelmässä ja pilvipalvelussa, jotka ovat organisaation suoran valvonnan, tietoturvakäytäntöjen ja lakisääteisten velvoitteiden ulkopuolella. Nämä strukturoimattomat henkilötiedot, joista organisaatio on vastuussa ja joita on läkisääteinen velvollisuus suojata, aiheuttaa organisaatioille haasteita. Henkilötietojen käsittelijä saattaa sekä luoda että käsitellä henkilötietoja omalla laitteellaan ja tietämättään tallentaa tietoja organisaation tietojärjestelmien ja henkilötietojen hallintaketjun ulkopuolelle. Henkilöstön riittävä kouluttaminen ja perehdytys organisaation tietoturvakäytäntöihin on avain asemassa, jotta vältytään ylimääräisiltä tietovuodoilta, ongelmatilanteilta ja mahdollisilta sanktioilta. Organisaatioiden kannattaa valita luotettava pilvipalveluiden tarjoaja ja tehdä henkilötietojen käsittelijän kanssa sopimus ehdoista, jotka ovat organisaation ja tietosuoja-asetuksen vaatimuksen mukaisia. (Netskope 2018.)

3.1.1 Osoitusvelvollisuus

Osoitusvelvollisuus on yksi keskeisimpiä muutoksia sovellettaessa tietoturva-asetusta. Henkilötietodirektiivin aikana on riittänyt, että säännöksiä noudatetaan, mutta nyt organisaatiolla tulee olla kyky myös osoittaa toteuttavansa tietosuojaperiaatteita sekä noudattavansa asetusta henkilötietojen käsittelyssä. Osoitusvelvollisuus edellyttää tietosuojaperiaatteiden käytännön toteuttamisen ja käsittelyyn liittyvien prosessien dokumentointia. Rekisterinpitäjän on toteutettava organisatoriset ja tekniset toimenpiteet, jotta voidaan varmistaa ja osoittaa, että asetusta noudatetaan. (Tietosuojavaltuutetun toimisto 4/2017, 14.)

3.1.2 Sopimusvaatimukset

Yleinen tietosuoja-asetus edellyttää, että henkilötietojen käsittelijän ja rekisterinpitäjän ollessa eri tahoja, on näiden välille asetuksen mukaan laadittava kirjallinen sopimus. Sopimuksella vahvistetaan käsittelyn tarkoitus, kohde, kesto, luonne, henkilötietojen tyyppi ja rekisterinpitäjän sekä käsittelijän oikeudet ja velvollisuudet. (Yleinen tietosuoja-asetus 2016/679, artikla 28.)

Henkilötietojen käsittelijän rooli on määritelty asetuksessa entistä selkeämmin ja lainsäädännöstä johtuvia velvoitteita henkilötietojen käsittelyyn on tarkennettu henkilötietolakiin nähden. Henkilötietojen käsittelijä ei saa tehdä omia alihankintoja ilman erityistä tai yleistä kirjallista ennakkolupaa rekisterinpitäjältä. Henkilötietojen käsittelijän on myös tiedotettava henkilötietojen käsittelyyn liittyvistä muutoksista, tietojen käsittelijöiden lisäyksistä ja vaihdoksista, jotta rekisterinpitäjällä on mahdollisuus vastustaa näitä muutoksia. (Yleinen tietosuoja-asetus 2016/679, artikla 28.)

Rekisterinpitäjän tulee varmistaa, että henkilötietojen käsittelijät toteuttavat riittävät tekniset ja organisatoriset toimet, jotta tietosuoja-asetuksen vaatimukset täyttyvät. Rekisterinpitäjän on määriteltävä myös käytännön vaatimukset omaan henkilötietotoimintaan ja otettava nämä ehdot sisällytettäviksi sopimuksiin. Vanhat henkilötietojen käsittelyyn liittyvät sopimukset tulisi uudelleenarvioida yleisen tietosuoja-asetuksen näkökulmasta. Tälläisia ovat esimerkiksi henkilötietoja käsittelevään tietojärjestelmään liittyvät sopimukset, henkilötietoihin liittyvät ulkoistamissopimukset ja henkilöihin liittyvien palvelujen ostosopimukset. (Netskope 2018.)

3.1.3 Tietosuojavastaava

Tietosuojavastaava on alan käytäntöjä ja tietosuojalainsäädäntöä tunteva henkilö, jonka tarkoituksena on valvoa tietosuoja-asetuksen noudattamista organisaatiossa henkilötietojen käsittelyn osalta. Rekisterinpitäjän tulee nimittää tietosuojavastaava kun ydintehtävät vaativat järjestelmällistä ja säännöllistä rekisteröityjen seurantaa, henkilötietojen käsittely on laajamittaista, käsittely kohdistuu erityisiin henkilötietoryhmiin tai rikoksia koskeviin tietoihin. Tietosuojavastaava on nimettävä myös silloin, kun rekisterinpitäjä on julkishallinnon toimija pois lukien tuomioistuimet. (Tietosuojavaltuutetun toimisto 2017.)

Tietosuojavastaavan on kyettävä hoitamaan tehtävänsä ja velvollisuutensa riippumattomasti. Rekisterinpitäjän tulee mahdollistaa tietosuojavastaavalle riittävät resurssit ja tarvittaessa mahdollisuus kouluttautua. Tietosuoja-asetuksen noudattamatta jättäminen ei ole tietosuojavastaavan vaan rekisterinpitäjän ja henkilötietojen käsittelijän vastuulla. Tietoturvavastaava toimii organisaatiossa henkilötietojen käsittelijöiden ja rekisterinpitäjän tukena. Tietosuojavastaavan tehtävän voi myös ulkoistaa ulkopuoliselle palveluntarjoajalle. (Tietosuojavaltuutetun toimisto 2017.)

3.1.4 Henkilötietojen käsittelyn lainmukaisuus

Tietosuoja-asetuksen artikla 6:n mukaan henkilötietojen käsittely on laillista ainoastaan silloin kun yksi seuraavista edellytyksistä täyttyy (Yleinen tietosuoja-asetus 679/2016, artikla 6):

Rekisteröidyn suostumus

Rekisteröity antaa suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten. Rekisterinpitäjän tulee kyetä osoittamaan annettu suostumus henkilötietojen käsittelyyn. Rekisteröidylle tulee myös ilmoittaa oikeudesta perua suostumus milloin tahansa ja sen tulee olla yhtä helppoa kuin sen antaminen. Tietosuoja-asetus pyrkii erityisesti vaikuttamaan lasten henkilötietojen käsittelyn suojaamiseen sekä riskien vähentämiseen. Lasten yleinen tietämys omista oikeuksistaan, asianomaisista suojatoimista ja seurauksista on usein puuttellista. Tietoyhteiskunnan palvelujen tarjominen lapselle on lainmukaista vain kun lapsi on vähintään 16-vuotias tai lapsen huoltaja on antanut siihen suostumuksen tai valtuutuksen. (Yleinen tietosuoja-asetus 679/2016, artikla 7-8.)

Sopimus

Käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.

Lakisääteinen velvoite

Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi.

Elintärkeä tai yleinen etu

Käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi.

Julkinen tehtävä

Käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi

Oikeutettu etu

Käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi. Tätä kohtaa ei sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtäviensä yhteydessä.

3.1.5 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennetulla tietosuojalla tarkoitetaan yrityksen tai organisaation teknisiä ja organisatorisia käytäntöjä ja ratkaisuja henkilötietojen käsittelyn ja keruun eri vaiheissa. Sisäänrakennetun tietosuojan tavoitteena on tietosuoja- ja yksityisyysperiaateiden huomiointi tietojenkäsittelyprosessin alusta asti. Oletusarvoinen tietosuojalla varmistetaan, että henkilötietoja käsitellään varmistaen korkea yksityisyydensuoja ja estetään rajoittamattomien henkilöiden pääsy tietoihin oletusarvoisesti. (Euroopan komissio, 2018.) Tuotteiden, sovellusten ja palvelujen tuottajia kannustetaan ottamaan kuluttajan oikeus tietosuojaan huomioon jo kehitys- ja suunnitteluvaiheessa, jotta rekisterinpitäjät ja henkilötietojenkäsittelijät pystyvät täyttämään uuden tietosuoja-asetuksen velvoitteensa. (Yleinen tietosuoja-asetus 2016/679, perus 78.)

Rekisterinpitäjän tulee määrittää toimenpiteet ja käsittelytavat oletusarvoisesti niin, että käsitellään vain kunkin tarkoituksen kannalta tarpeellisia tietoja. Tulee huomioida henkilötietojen käsittelyn laajuutta, määriä, läpinäkyvyyttä, saatavilla oloa ja säilytysaikaa. Tietosuojaperiaatteiden ja rekisteröityjen oikeuksien suojaamiseksi voidaan suorittaa tietojen minimointia, anonymisointia tai pseudonymisointia. (Yleinen tietosuoja-asetus 2016/679, artikla 25.)

3.1.6 Suoramarkkinointi

Suoramarkkinointi on jatkossakin sallittua, mutta rekisteröidylle tulee jakaa tieto mahdollisuudesta kieltäytyä suoramarkkinoinnista ja oikeus vastustaa käsittelyä ilman kuluja. Suomessa ei tarvitse erikseen pyytää suostumusta perinteisillä menetelmillä suoritettuun suoramarkkinointiin, kuten postitse tai puhelimitse, ellei vastaanottaja sitä erikseen kiellä. Rekisteröidylle tulee ilmoittaa oikeudesta kieltää suoramarkkinointi. Rekisteröidylle tulisi kertoa asiakassuhteen aloitushetkellä käsittelytoimien selosteessa tai sopimuspaperissa, että rekisteröidyn tietoja tallennetaan suoramarkkinointirekisteriin. (Holopainen 2018.)

Ulkoistetussa suoramarkkinoinnissa markkinoijan eli rekisterinpitäjän ja palveluntarjoajan tulee määrittää sopimuslausekkeita vastaamaan tietosuoja-asetuksen velvoitteita yhteistyö- ja toimeksiantosopimuksessa. Näin rekisterinpitäjä voi varmistaa ulkoistetun tahon käsittelevän henkilötietoja asianmukaisin keinoin ja varmistaa riittävän tietosuojan. (Holopainen 2018.)

Sähköiseen suoramarkkinointiin tulee saada suostumus ennalta. Tässä poikkeuksena on B2B-liiketoiminnassa tapahtuva suoramarkkinointi, joka ei tarvita suostumusta, sillä sen yleensä katsotaan perustuvan oikeutettuun etuun. Suostumusta sähköposti-, teksti-, ääni-, puhe-, ja kuvaviestien avulla tapahtuvaan suoramarkkinointiin tulisi pyytää palvelun tai tuotteen myynti-, osto- tai rekisteröitymishetkellä. Rekisteröidylle tulee ilmaista selkeästi mahdollisuudesta kieltäytyä suoramarkkinoinnista ja markkinoijan on tiedotettava kieltomahdollisuudesta jokaisen sähköisen suoramarkkinointiviestin yhteydessä. (Holopainen 2018.)

3.1.7 Siirrot kolmansiin maihin

Henkilötietojen siirrot EU:n alueen ulkopuolelle vaativat Euroopan komission päätöksen, jossa todetaan kolmannen maan, kolmannen maan alueen tai tietyn kansainvälisen järjestön riittävä tietosuojan taso. Komission päätöksen jälkeen ei tällaisiin kolmanteen maahan kohdistuviin henkilötietojen siirtoihin tarvita erityistä lupaa. Euroopan Unionin virallisessa lehdessä ja verkkosivuilla julkaistaan lista kolmansista maista, kolmannen maan alueista ja tietyistä sektoreista, joiden tietosuojan taso on todettu riittäväksi tai riittämättömäksi. (Yleinen tietosuoja-asetus 2016/679, luku 5.)

3.1.8 Sakot ja sanktiot

Sakkojen ja sanktioiden uhka on noussut vahvasti esille tietoturva-asetuksen uutisoinnissa ja siitä kuulee usein puhuttavan GDPR:ään viitattaessa. Sanktioista on tullut pelote yrityksille ottaa uuden tietoturva-asetuksen muutokset vakavasti. Rekisterinpitäjän laiminlyödessä tietosuoja-asetusta voidaan yritykselle langettaa hallinnollisia sakkoja 20 miljoonaa euroa tai 4% yrityksen edellisen vuoden liikevaihdosta, riippuen kumpi näistä on suurempi. (Yleinen tietosuoja-asetus 2016/679, artikla 83.)

3.2 Rekisteröidyn oikeudet

Nykyisen henkilötietolain mukaiset rekisteröidyn oikeudet vastaavat suurilta osin uuden tietosuoja-asetuksen oikeuksia. Uusi asetus muokkaa oikeuksien toteutumiseen liittyvästä sääntelystä yksityiskohtaisempaa, säätää uusia rekisteröidyn oikeuksia sekä muuttaa oikeuksien toteutumiseen liittyviä prosesseja. Asetus korostaa henkilötietolakia avoimempaa ja yksityiskohtaisempaa rekisterinpitäjän informointivelvollisuutta sekä vastuuta oikeuksien toteutumisesta. Organisaatioiden on otettava huomioon nämä rekisteröidyn oikeudet suunniteltaessa tietojärjestelmiä ja henkilötietojen käsittelyyn liittyviä prosesseja sekä varmistettava nykyisten järjestelmien kyky taipua tietosuoja-asetuksen tuomiin muutoksiin. (Tietosuojavaltuutetun toimisto 4/2017, 23.)

3.2.1 Läpinäkyvyys ja rekisteröidyn oikeus päästä tietoihin

Rekisteröidyllä on oikeus saada henkilötietojaan koskevan käsittelyn tiedot läpinäkyvässä, helposti ymmärrettävässä ja tiiviisti esitetyssä muodossa. Asetus asettaa rekisteröidyn pyynnön perusteella toteutettavien toimenpiteille määräaikoja. Rekisteröidyn pyynnöstä ryhdytyistä toimenpiteistä tulee antaa tieto ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa. Rekisterinpitäjällä on myös kuukauden määräaika ilmoittaa rekisteröidylle syy, miksi ei aio toteuttaa pyydettyjä toimenpiteitä. Kieltäytyessään rekisterinpitäjän on selvitettävä rekisteröidylle tällä olevista oikeussuojakeinoista, kuten mahdollisuudesta tehdä valitus valvontaviranomaisille. Asetuksessa on säädetty hieman yksityiskohtaisempi tietojen tarkastusoikeus henkilötietolakiin nähden. Rekisteröidyllä on oikeus saada häntä koskevista

henkilötiedoista jäljennös. Rekisterinpitäjällä on kuitenkin oikeus pyytää lisätietoja pyynnön tehneeltä luonnolliselta henkilöltä jos tällä on perusteltu syy epäillä tämän henkilöllisyyttä. (Tietosuojavaltuutetun toimisto 4/2017, 23-24.)

Rekisterinpitäjän tulee kyetä toimittamaan rekisteröidyn oikeutta koskeva pyyntö sellaisessa yleisessä sähköisessä muodossa, että se on helposti käytettävissä, ellei rekisteröity toisin pyydä. Lähtökostaisesti nämä pyynnöt ovat maksuttomia, mutta tietyissä tapauksissa rekisterinpitäjällä on oikeus periä pyydetystä toimenpiteestä aiheutuneet hallinnolliset kustannukset tai kieltäytyä toimesta jos pyyntö on perusteeton tai kohtuuton. Tässä tapauksessa rekisterinpitäjän tulee pystyä osoittamaan pyynnön perusteettomuus. Tietosuoja-asetuksen tuoma reagointiaikaraja rekisteröidyn pyyntöön on yksi kuukausi, mutta määräaikaa on mahdollista jatkaa kahdella kuukaudella ottaen huomioon pyyntöjen haastavuus ja määrä. Mahdollisesta määräajan jatkamisesta tulee rekisterinpitäjän informoida rekisteröityä sekä selvitettävä viivästymisen syyt. (Tietosuojavaltuutetun toimisto 4/2017, 24-25.)

3.2.2 Oikeus tietojen muuttamiseen ja käsittelyn rajoittamiseen

Tietosuoja-asetus takaa rekisteröidylle oikeuden tulla unohdetuksi, eli oikeuden omien henkilötietojensa poistamiseen tai niiden oikaisemiseen. Rekisterinpitäjällä on myös velvollisuus ilmoittaa rekisteröidyn pyyntö poistaa tämän henkilötiedot, jäljennökset ja kopiot muille henkilötietoja käsitteleville rekisterinpitäjille, joille rekisterinpitäjä on luovuttanut henkilötietoja tai joilta on vastaanottanut tietoja. (Yleinen tietosuoja-asetus 679/2016, artikla 18.)

Rekisteröidyllä on asetuksen nojalla neljä eri tilannetta, jossa voi vaatia tietojensa käsittelyn rajoittamista (Yleinen tietosuoja-asetus 679/2016, artikla 18):

1. Rekisteröity kiistää henkilötietojensa paikkansapitävyyden, jolloin käsittelyä rajoitetaan ajaksi, jonka kuluessa rekisterinpitäjä voi varmistaa niiden paikkansapitävyyden.
2. Käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajoittamista.
3. Rekisterinpitäjä ei enää tarvitse kyseisiä henkilötietoja käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.
4. Rekisteröity on vastustanut henkilötietojen käsittelyä artikla 21 1 kohdan nojalla odotettaessa sen todentamista, syrjäyttävätkö rekisterinpitäjän oikeutetut perusteet rekisteröidyn perusteet.

3.2.3 Oikeus siirtää tiedot järjestelmästä toiseen

Asetus antaa rekisteröidylle oikeuden siirtää häntä koskevat henkilötiedot rekisterinpitäjältä toiselle silloin, kun käsittely perustuu sopimukseen tai suostumukseen ja jos käsittely suoritetaan automaattisesti. Tiedot tulee siirtää yleisesti käytetyssä, jäsennellyssä ja koneellisesti luettavassa muodossa, mikäli se on teknisesti mahdollista. Oikeutta ei sovelleta, jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi, rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi tai jos oikeus vaikuttaa haitallisesti muiden vapauksiin ja oikeuksiin. (Yleinen tietosuoja-asetus 2016/679, artikla 20.)

3.2.4 Vastustamisoikeus ja automaattisesti tehtävät yksittäispäätökset

Vastustamisoikeus antaa rekisteröidylle oikeuden vastustaa henkilötietojensa käsittelyä erityisen henkilökohtaisen tilanteeseensa liittyvän perusteen nojalla, mutta liittyy vain osaan käsittelyperusteista (Yleinen tietosuoja-asetus 2016/679, artikla 21).

Poikkeustilanteita lukuunottamatta tietosuoja-asetus turvaa henkilölain tapaan rekisteröidylle oikeuden olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi. Poikkeustilanteissa rekisterinpitäjän tulee toteuttaa henkilötietoja käsittelevät toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi. (Yleinen tietosuoja-asetus 2016/679, artikla 22.)

4 YHDYSVALTOJEN TIETOSUOJALAIT

Yhdysvalloissa ei ole yksittäistä, kattavaa kansallista lakia, joka säätelee henkilötietojen keräämistä ja käyttöä. Sen sijaan Yhdysvalloissa on liittovaltion ja valtion lakien ja asetusten ”viidakko”, jossa ilmenee ajoittain päällekkäisyyksiä, ja jossa lait ja asetukset voivat olla ristiriidassa keskenään. Lisäksi valtion virastot ja teollisuusryhmät ovat kehittäneet suuntaviivoja, jotka ovat osa niinsanottua itsesääntelykehystä. Kehystä pidetään yleisesti hyväksyttyinä parhaina käytänteinä, eikä ole lainvoimaa. (Leuan 2017.)

Yhdysvalloissa on yksityisyyttä koskevia yksittäisiä lakeja, jotka sääntelevät henkilötietojen keräämistä ja käyttöä. Osa laeista koskee tiettyjä tietokategorioita kuten terveyttä, rahoitusta tai sähköistä viestintää ja toiset toimintaa jossa käytetään henkilötietoja, kuten telemarkkinointi ja sähköpostimainonta. Lisäksi Yhdysvalloissa on myös laaja kuluttajansuojalaki mikä ei itsessään ole yksityisyyttä suojaava laki, mutta sitä käytetään estämään epäoikeudenmukaisuuksia ja harhaanjohtavia käytäntöjä, jotka koskevat henkilötietojen käsittelyä ja niihin liittyviä käytäntöjä. (Leuan 2017.)

Yksityisyyden merkitys ja tärkeys nousee esille vertailtaessa EU:n ja Yhdysvaltojen lainsäädäntöjä. GDPR alleviivaa yksityisyyden tärkeyttä ja yksilön oikeuksia, kun Yhdysvaltojen lainsäädäntö keskittyy tietoturvan, yksityisten tiedostojen, asiakirjojen ja yleisesti datan suojeluun. Yksityisyys ja yksilön oikeudet jää monesti kokonaan ulkopuolelle. Ongelmana Yhdysvalloissa on lakien määrä ja niiden eroavaisuudet valtioiden välillä. Osa valtioista saattaa yltää GDPR-standardeihin ja toiset taas eivät. Esimerkiksi osalla valtioista on tietoturvamurron ilmoitusvelvollisuuteen kohdistuva laki, kuten Kalifornian California Data Breach Notification Law, mutta toisilla valtioista tällaista ei ole. (Coos 2017.)

Monissa yhteyksissä mainitaan, että Yhdysvalloissa on tapana luoda tietosuojalakeja kun tarve niille ilmenee, perustavanlaatuisen yleisen yksityisyyden sääntelyn sijaan. Yhdysvalloissa henkilötietojen sääntely perustuu alakohtaiseen (eng. sector-spesific) lähestymistapaan. Yhdysvaltojen kansalaisen henkilötietojen sääntely perustuu siihen, mihin kategoriaan tieto kuuluu. Esimerkkinä terveystietoja sääntelee The Health Insurance Portability and Accountability Act (HIPAA), taloustietoja The Financial Services Modernization Act (Gramm-Leach-Bliley Act(GLB)) ja The Fair Credit Reporting Act (FCRA) sekä markkinointia Telephone Consumer Protection Act (TCPA) ja

Telemarketing Sale Rule. Yleisesti alakohtainen lähetymistapa auttaa yrityksiä tiedostamaan mitä sääntelyä näiden tulee noudattaa. EU:n tietosuojamalli suojaa kaikkia henkilötietoluokkia. Sellaisia Yhdysvaltalaisia yrityksiä, jotka haluavat suorittaa EU:n alueella asuvien henkilöiden henkilötietoja sisältävää liikentoimintaa, ja jotka eivät ole toimineet tiukkojen sääntelyjen alla tai jotka eivät toimi vahvasti säädellyillä aloilla, odottaa uuden tietosuojapolitiikan omaksuminen. (Eaton 2017.)

Henkilötietojen siirto EU:n ja Yhdysvaltojen välillä tapahtuu käyttäen Privacy Shield -järjestelyä (Euroopan komissio 2018).

4.1 Tunnetuimpia liittovaltion tietosuojalakeja

The Federal Trade Commission Act (FTC Act)

Federal Trade Commission Act (FTC Act) on liittovaltion kuluttajansuojalaki, joka kieltää epäoikeudenmukaisia tai harhaanjohtavia käytäntöjä. Lakia on myös sovellettu tietosuoja- ja tietoturvapolitiikkaan. Laki on mahdollistanut täytäntöönpanotoimet sellaisia yrityksiä vastaan, jotka eivät ole onnistuneet täyttämään tietosuojakäytäntöjä tai käyttäneet luvattomasti henkilötietoja. Federal Trade Comission (jatkossa FTC) on Yhdysvaltain kuluttajansuojaa valvova elin. (Leuan 2017.)

Children's Online Privacy Protection Act (COPPA)

COPPA on lasten verkossa toimimisen yksityisyyttä suojaava laki, joka pyrkii rajoittamaan lasten verkkokäyttäytymisestä kerätyn tiedon käyttöä ja mainontaa. Yhdysvaltain kuluttajansuojaviranomaisella FTC:llä on valta hallita lain sääntelyä ja valvoa sen toteutumista. (Leuan 2017).

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA säätelee potilas- ja terveystietoja. Sitä voidaan soveltaa laajasti terveydenhuollon tarjoajiin, tietojenkäsittelyyn ja järjestöihin, jotka käsittelevät potilas- ja terveystietoja. HIPAA voidaan jakaa osiin. HIPAA Privacy Rule koskee yksilöllisesti tunnistettavien terveystietojen yksityisyyden suojaa, keräämistä sekä käyttöä ja se määrittää näitä koskevat standardit. HIPAA Security Rule tarjoaa turvallisuusstandardeja sähköisten tietojen suojaamiseksi ja HIPAA Transactions Rule standardeja terveystietojen sähköisten siirtojen suojaamiseksi. HIPAA Omnibus Rule tarkentaa tietoturvaloukkausten ilmoitusvelvollisuutta suojattujen terveystietoihin kohdistuneen

vuodon sattuessa. (Leuan 2017.) HIPAA asettaa vaatimuksia terveydenhuollon toimijoille ja niiden käyttämille järjestelmille. Potilas- ja terveystiedot tulee suojata koko niiden elinkaaren ajan ja potilastietojen dokumentointia tulee hallinnoida keskitetysti. (Health Insurance Portability and Accountability Act 2018.)

The Financial Services Modernization Act (Gramm-Leach-Bliley Act(GLB))

GLB sääntelee taloudellisten tietojen keräämistä, käyttöä ja julkistamista. Sitä sovelletaan laajasti rahoituslaitoksiin kuten pankkeihin, arvopaperiyhtiöihin, vakuutusyhtiöihin ja muihin rahoituspalveluja ja tuotteita tarjoaviin yrityksiin. (Leuan 2017.)

The Fair Credit Reporting Act (FCRA)

FCRA rajoittaa rekisteröidyn luotto- ja taloustietojen käyttöä ja jakamista luotto-, työsuhde- tai vakuutuskelpoisuuden arviointiin. Laki velvoittaa myös rahoituslaitoksia ja luottoa tarjoavien tahoja laatimaan ohjelmia, joilla tunnistaa ja vastata identiteettivarkauksiin. (ICLG 2018.)

The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) ja the Telephone Consumer Protection Act (TCPA)

Sääntelee sähköposti- ja puhelintietojen keräystä ja käyttöä (Leuan 2017).

4.2 EU:n ja Yhdysvaltojen tietosuojalainsäädännöt vertailussa

Kappaleessa verrataan EU:n yleisen tietosuoja-asetuksen pääkohtia Yhdysvaltojen lainsäädäntöön.

Yleistä

Yhdysvallat on 50 valtion liittotasavalta, jossa on yksi yhteinen kieli, englanti. Yhdysvalloissa ei ole yksittäistä kattavaa tietosuojalakia vaan se muodostuu liittovaltion ja valtiokohtaisista tietosuojalaeista. Henkilötietojen käsittelyyn kohdistuvat lait ovat alakohtaisia. (Lee 2018.)

Euroopan unioni on 28 jäsenvaltion muodostama taloudellinen ja poliittinen liitto, jossa on 24 virallista kieltä. EU:n yleistä tietosuoja-asetusta sovelletaan kaikissa

jäsenvaltioissa. Tietosuoaja-asetuksen lisäksi lainsäädäntöön kuuluu lukuisia direktiivejä, joita jäsenvaltiot täytäntöönpanevat omissa lainsäädännöissään. Maiden ja kielten moninaisuus on aiheuttanut kulttuurieroja tietoturvalainsäädännöissä. (Lee 2018.)

Läpinäkyvyys

Yhdysvaltojen tietosuojasäädökset kohdistuvat suurelta osin datan turvallisuuteen. EU:n tietosuojaperiaatteet, kuten tietojen minimointi, laillinen lähtökohta, peruste käsittelylle sekä tietojen säilytysaika, eivät sisälly Yhdysvaltain säädöksiin ainakaan nimenomaisesti. Osassa laeista on kuitenki poikkeuksia tietyn tiedon säilyttämisen osalta. Esimerkiksi työntekijän tietoja tulee säilyttää ennalta määrätyn ajan, mutta tämän ajan jälkeen on yrityksen päätäntävallan alla, mitä tiedoille tehdään. (ICLG 2018.)

Läpinäkyvyys on yksi EU:n ja GDPR:n tärkeimmistä periaatteista. Rekisterinpitäjän on avoimesti ja selvästi tiedotettava rekisteröidyille mihin, miten ja kuinka kauan heitä koskevia henkilötietoja tullaan käsittelemään. (Tietosuojavaltuutetun toimisto 4/2017.)

Tietojen minimointi

Yhdysvalloilla ei ole tietojen minimointiin kohdistuvaa lakia. Federal Trade Comission kuitenkin suosittelee organisaatioita noudattamaan periaatetta, jossa kerätään vain tarvittava tieto. (ICLG 2018.)

EU:n tietosuoja-asetus velvoittaa organisaatioita keräämään vain tarvittavat tiedot ja kerätylle tiedolle tulee olla peruste.

Tiedonsiirto järjestelmästä toiseen

Yhdysvalloissa ei ole yleistä lakia tietojen siirtoon järjestelmästä toiseen, mutta potilas- ja terveystietoja säätelevä HIPAA antaa rekisteröidylle oikeuden pyytää terveystietojen siirtoa terveyspalvelun tarjoajalta toiselle. (ICLG 2018.)

EU:n tietosuoja-asetus velvoittaa rekisterinpitäjää toimittamaan rekisteröidyn pyynnöstä tätä koskevat henkilötiedot toiselle rekisterinpitäjälle silloin, kun käsittely perustuu suostumukseen tai sopimukseen ja käsittely suoritetaan automaattisesti. (Yleinen tietosuoja-asetus 2016/679, artikla 20.)

Henkilötietojen siirrot kolmansiin maihin

Yhdysvalloissa ei ole henkilötietojen siirtoa rajoittavaa lakia. (ICLG 2018.)

Henkilötietojen siirrot EU:n alueen ulkopuolelle vaativat Euroopan komission päätöksen, jossa todetaan kolmannen maan, kolmannen maan alueen tai tietyn kansainvälisen järjestön riittävä tietosuojan taso. Komission päätöksen jälkeen ei tällaisiin henkilötietojen siirtoihin tarvita erityistä lupaa. (Yleinen tietosuoja-asetus 2016/679, luku 5.)

Rekisteröidyn oikeus saada, oikaista tai poistaa tietoja

Yhdysvaltojen lait eivät yleisesti oikeuta rekisteröityä saamaan hänestä kerättyjä henkilötietoja tai vaatimaan näiden tietojen oikaisua tai poistoa. Poikkeuksia löytyy, kuten terveys- ja potilastietoja sääntelevä HIPAA, joka oikeuttaa pääsyn tietoihin sekä Fair Credit Reporting Act (FCRA), joka säätää oikeudesta kiistää epätarkka tieto ja vaatia kyseessä olevan tahon korjaamaan tieto. (ICLG 2018.)

EU:n yleinen tietosuoja-asetus antaa rekisteröidylle oikeuden saada pääsy hänestä kerättyihin henkilötietoihin vaivattomasti ja kohtuullisin väliajoin, jotta rekisteröity voi varmistaa käsittelyn lainmukaisuuden ja tietojen oikeudellisuuden. Rekisteröidyllä on myös oikeus korjata häntä koskevat virheelliset tiedot sekä oikeus tulla unohdetuksi. (Tietosuojavaltuutetun toimisto 4/2017.)

Tietosuojavastaava

Yhdysvalloissa ei ole tietosuojavaltuutetun nimeämistä koskevaa lakia. Kattavaa potilas- ja terveystietoja sisältävää toimintaa harjoittavien tahojen tulee kuitenkin nimetä tietosuojakysymyksistä vastuussa oleva henkilö (ICLG 2018).

EU:n tietosuoja-asetus velvoittaa tietosuojavastaavan nimeämistä silloin, kun organisaation toiminta käsittää säännöllistä ja järjestelmällistä henkilötietojen käsittelyä. Tietosuojavastaava nimetään myös silloin, kun käsittely on laajamittaista ja kohdistuu erityisiin henkilötietoryhmiin ja arkaluontoisiin tietoihin. (Tietosuojavaltuutetun toimisto 2017)

Valitus viranomaiselle

Yhdysvalloissa kuluttaja voi tehdä ilmoituksen tietosuojalain rikkomisesta valtiolliselle sääntelyviranomaiselle edellä lueteltujen erityisten sektorikohtaisten lakien puitteissa.

Tälläisiä viranomaisia ovat Federal Trade Commission (FTC) ja oikeusministeriö. (ICLG 2018.)

Jokaisen EU:n jäsenvaltion tulee nimetä vähintään yksi valvontaviranomainen. Suomessa valvontaviranomainen on Tietosuojavaltuutetun toimisto. Jokaisella rekisteröidyllä on oikeus tehdä valitus, jos hänen asetukseen perustuvia oikeuksiaan on loukattu (Yleinen tietosuoja-asetus 2016/679, artikla 33).

4.3 Privacy Shield

Euroopan komissio hyväksyi 12.7.2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn. Järjestely turvaa EU-kansalaisen perusoikeuksia, kun tämän henkilötietoja siirretään Yhdysvaltoihin ja luo selkeät periaatteet yrityksille, jotka siirtävät henkilötietoja EU:n ja Yhdysvaltojen välillä. EU:n lainsäädäntö edellyttää Yhdysvaltoihin siirretyille henkilötiedoille korkeatasoista suojaa. Tämän päivän globaalissa digitaalitaloudessa taloudelliset siteet Euroopan unionin ja yhdysvaltojen välillä ovat vahvat. Transatlanttiset henkilötietojen siirrot ovat merkittävä ja välttämätön osa alueiden välisiä taloudellisia siteitä. Privacy Shield -järjestelyssä sallitaan henkilötietojen siirto EU:sta yhdysvaltalaiselle yritykselle, jos tämä yritys säilyttää, käyttää ja siirtää edelleen henkilötietoja niin, että se noudattaa määriteltyjä tietosuojasäännöksiä ja soveltaa lukuisia suojatoimia. (Euroopan komissio 2017.)

Yhdysvaltalaisten yritysten on ilmoittauduttava Yhdysvaltojen kauppaministeriössä (U.S. Deparment of Commerce) tullakseen Privacy Shield -yrityksiksi. Yhdysvaltain kauppaministeriö hallinnoi Privacy Shield -järjestelyä ja varmistaa yritysten täyttävän velvoitteensa yksityisyyden suojaa koskevissa periaatteissa. Yhdysvaltalaisten organisaatioiden ja yritysten tulee vuosittain uudistaa jäsenyytensä, jotta ne voivat hyödyntää Privacy Shield -järjestelyä henkilötietojen siirrossa, todentamalla niiden tietosuojaperiaatteiden ja velvoitteiden täyttyminen. Verkkosivustolta https://www.privacyshield.gov/welcome voi tarkastaa kuuluuko yhdysvaltalainen yritys Privacy Shield -järjestelyyn. (Euroopan komissio 2017.)

Euroopan komissio ylläpitää määrittelyä Privacy Shield -yrityksen henkilötietojen käyttöön liittyvistä velvoitteista, ja luonnollisten henkilöiden oikeuksista tietoihin (Euroopan komissio 2017):

1. Oikeus saada tietoja.
2. Rajoitukset, jotka koskevat henkilötietojen käyttöä eri tarkoituksiin.
3. Tietojen minimointi ja velvollisuus säilyttää tiedot vain niin kauan kuin se on tarpeellista.
4. Velvollisuus varmistaa tietojen turvallinen säilytys.
5. Velvollisuus suojata henkilötietoja, jotka siirretään toiselle yritykselle.
6. Oikeus tutustua tietoihin ja oikaista niitä.
7. Oikeus tehdä valitus ja saada puutteet korjatuiksi.
8. Oikeussuojakeinoista tapauksissa, joissa on kyse tietojen luovuttamisesta Yhdysvaltojen viranomaisille.

5 MITEN LÄHESTYÄ TIETOTURVA-ASETUKSEN VELVOITTEITA

EU:n tietosuoja-asetuksen tavoitteena on luoda yhtenäinen ja vahva tietosuojakehys. Asetus vaatii rekisterinpitäjiä tarkastamaan tietosuojakäytäntöjensä lainmukaisuus ja varmistamaan henkilötietojen käsittelyn riittävä läpinäkyvyys. Organisaatioille on tietosuoja-asetusten vaatimusten täyttymiseksi olemassa lukuisia työkaluja, joilla varmistaa henkilötietojen käsittelyn ja tietosuojakäytänteiden lainmukaisuus. Työkalujen, joita tässä luvussa kuvataan, keskeisenä tavoitteena on auttaa rekisterinpitäjää hahmottamaan henkilötietojen käsittelyn nykytila, mahdolliset käsittelystä aiheutuvat riskit ja osoittaa toiminnan mahdolliset puutteet, joihin tulee tehdä muutoksia.

Uusi tietosuoja-asetus ei tietoturvan näkökulmasta tuo suurta muutosta entiseen. Organisaatioiden tulee edelleen huolehtia virustorjunnan, päivitysten, tietoliikenteen, palomuurien ja erillaisten salausten tasosta ja ajantaisaisuudesta. Asetuksen osoitusvelvollisuuden toteutumiseksi on kuitenki hyvä kuvata ja dokumentoida henkilötietojen tietoturvan toteutus.

5.1 Riskiarvio, vaikutustenarviointi ja tietotilinpäätös

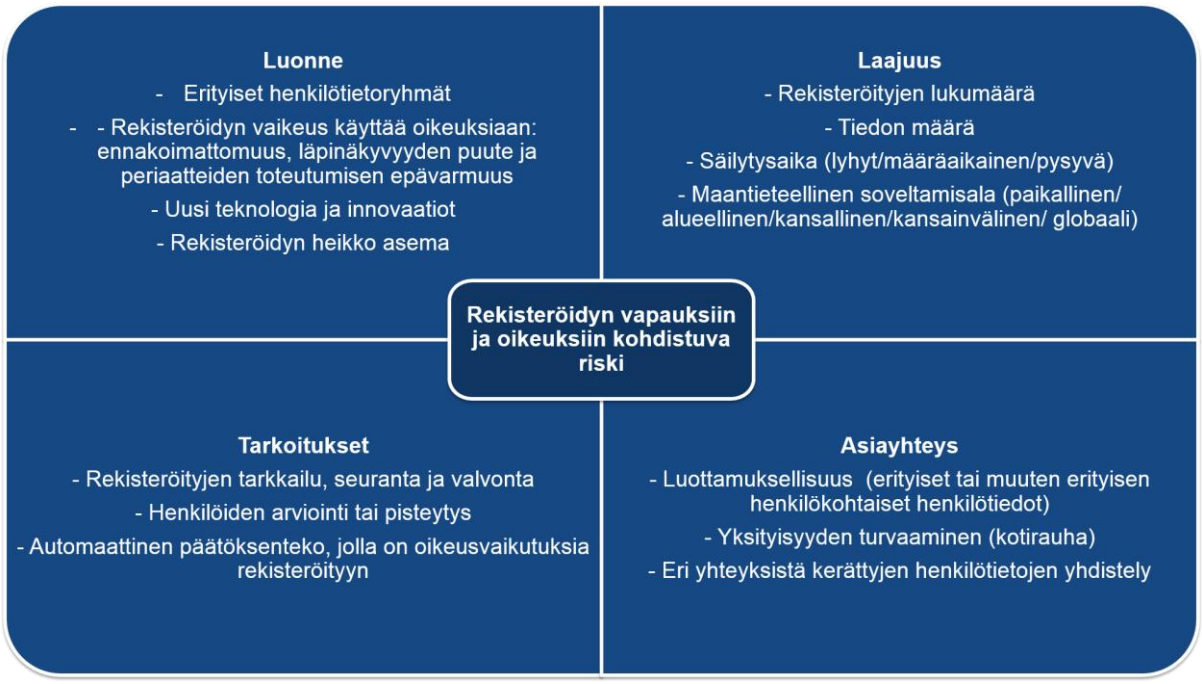
Riskiarvio

”Riskillä tarkoitetaan skenaariota, jolla kuvataan tapahtumaa ja sen seurauksia ja arvioidaan niiden vakavuutta ja todennäköisyyttä. Riskinhallinta voidaan puolestaan määritellä koordinoiduksi toiminnaksi, jolla ohjataan ja valvotaan organisaatiota riskien osalta.” (Tietosuojatyöryhmä 2017.)

Privacy Impact Assessment (PIA) on tietosuoja-asetuksen riskipohjainen lähestymistapa, jonka mukaan riskit henkilötietojen käsittelyyn arvioidaan etukäteen, eikä arvioinnin ansiosta toimintaan kohdisteta ylimitoitettuja toimenpidevaatimuksia.

Rekisterinpitäjän käsitellessä henkilötietoja, tulee tämän aina arvioida käsittelyyn liittyviä riskejä. Riskiarvio tehdään rekisteröidyn näkökulmasta ja sen tarkoituksena on selvittää henkilötietojen käsittelystä aiheutuvan vahingon mahdollisuus. Henkilötietojen käsittelystä aiheutuva vahinko voi rekisteröidylle olla fyysistä, aineellista tai aineetonta.

Vahingosta saattaa seurata rekisteröidylle sosiaalista- tai taloudellista vahinkoa, pseudonymisoinnin kumoutuminen tai rekisteröity voi joutoa petoksen kohteeksi. Rekisterinpitäjällä tulee olla selkeä käsitys organisaation henkilötietojen käsittelyn luonteesta, laajuudesta, asiayhteydestä ja tarkoituksesta. Rekisterinpitäjä arvioi käsittelystä aiheutuvan haitan todennäköisyyttä ja vakavuutta rekisteröidyn oikeuksille ja vapauksille. Tietosuojavaltuutetun toimiston julkaisema kuva 2, avaa riskiarvion keskeisiä aiheita rekisteröidyn vapauksiin ja oikeuksiin kodistuvien riskien tunnistamisen avuksi. (Tietosuojavaltuutetun toimisto 2018.)



Kuva 2. Riskien arviointi

Riskien tunnistaminen ja arviointi on tärkeä osa organisaation teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan tietosuoja-asetuksen mukaisen tietosuojan toteutuminen henkilötietojen käsittelyssä. Tietosuojaa koskeva vaikutustenarviointi on yksi riskien arvioinnin työkalu. Vaikutustenarviointi on tietosuoja-asetuksen mukaan pakollinen silloin, kun henkilötietojen käsittely voi aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille, mutta vaikutustenarviointia voi hyödyntää myös organisaation henkilötietojen käsittelytoimien suunnittelussa. (Tietosuojavaltuutetun toimisto 2018.)

Vaikutustenarviointi

Vaikutustenarvioinnin tarkoituksena on osoittaa henkilötietojen käsittelyn tarpeellisuutta ja kuvata itse käsittelyä. Vaikutustenarviointi arvioi luonnollisiin henkilöihin kohdistuvan henkilötietojen käsittelystä aiheutuvia riskejä. Siinä pyritään myös määrittelemään toimenpiteet, joilla havaittuihin riskeihin voidaan puuttua, jotta tietosuoja-asetuksen määrittämät luonnollisten henkilöiden vapaudet ja oikeudet toteutuisivat. Vaikutustenarviointi auttaa rekisterinpitäjää osoittamaan, että tietosuoja-asetuksen vaatimuksia käsitellään asianmukaisin toimenpitein ja on näin tärkeä työkalu osoitusvelvollisuuden näkökulmasta. (Tietosuojatyöryhmä 2017.) Tietosuojaa koskeva vaikutustenarviointi on toisin sanoen menettely, jolla parannetaan vaatimusten noudattamista ja osoitetaan niiden noudattaminen (Yleinen tietosuoja-asetus, artikla 24).

Tietotilinpäätös

Tietotilinpäätös on tietosuojavaltuuten suosittelema työkalu tietosuoja-asetuksen velvoitteiden noudattamisen osoittamiseksi, mutta ei ole läkisääteinen velvoite. Tietosuojavaltuutetun mukaan tietotilinpäätös on raportti, joka syntyy organisaation sisäisen tarkastelun tuloksena ja tarjoaa kokonaiskuvan tietojenkäsittelyn nykytilasta sekä kuvaa myös henkilötietolain mukaisen hyvän tietojenkäsittelytavan noudattamista. (Tietosuojavaltuutetun toimisto 2014.)

5.2 Nykytila-analyysi

Nykytila-analyysi tarkoittaa tietosuojakyvykkyyksien ja henkilötietojen käsittelyn nykytilan arviointia organisaatiossa. Analyysissa arvioidaan organisaation tietosuojan nykytilaa suhteessa EU:n yleisen tietosuoja-asetuksen vaatimuksiin. Tietosuojavastaavan kannattaa yleisen tietoturva-asetuksen siirtymäaikana panostaa nykytila-arvion ja -analyysin suorittamiseen, jotta organisaation tietosuojakyvykkyys olisi mahdollisimman lähellä EU:n tietoturva-asetuksen vaatimaa tasoa. Mikäli organisaatiolla ei ole nimettyä tietosuojavastaavaa, kannattaa tehtävä antaa henkilölle, jolla on riittävä tieto- ja taitotaso koskien tietoturva- ja henkilörekisterikäytänteitä sekä riittävät valtuudet organisaation sisällä suorittaa nykytila-analyysi. Analyysin pääkohteet vaihtelevat, mutta yleisimpiä ovat asiakastiedot, tietoturva, henkilöstöhallinnon tiedot, tietojen siirrot ulkomaille, sopimukset sekä ulkoistukset. (Andreasson & Ylipartanen 2016.)

Ari Andreasson ja Arto Ylipartanen (2016) listaavat tietosuojavastaaville nykytila-arvion ja -analyysin tekemisen tueksi seuraavia asioita:

1. Selvitä tilivelvollisen johdon käsitys organisaation tietosuojasta
2. Kartoita olemassa oleva tietoturvan- ja tietosuojan johtamismalli
3. Tunnista organisaation tietovarannot ja niiden hallintajärjestelmä
4. Tunnista myös organisaation henkilötietojen tietovirrat
5. Läpikäy rekisterihallintoon liittyvät linjaukset
6. Kartoita ja analysoi tietosuojariskit
7. Varmista toimeksiantosopimuksien sisältö
8. Mieti miten tietojohtaminen onnistuu
9. Varmista käytönvalvonnan organisointi
10. Selvitä rekisteröityken oikeuksien toteuttaminen ja toteutuminen

5.3 Pilvipalvelut

Rekisterinpitäjän tulee valita tarpeisiinsa sopiva pilvi. Yritys ja organisaation käyttämä luotettava pilvipalvelu lisää yrityksen tietoturvaa, luottamusta ja sitä voi käyttää esimerkiksi yhtenä vahvuutena myynnin tukena. Organisaation tulee määritellä palveluntarjoajan kanssa vastuut, varmistaa palvelun riittävät varmennukset ja, että se on suojattu asianmukaisen menetelmin. (Terhi Meriläinen, 2017.)

Pilvipalveita käytettäessä tieto on useasti tallennettuna useaan paikkaan samanaikaisesti. Pilvipalveluiden luotettava toiminta varmistetaan tietojen varmuuskopioinnilla tai pilvipalvelun kahdennuksella. Pilvipalvelun kahdennus tarkoittaa palvelun replikointia toiseen paikkaan, tarkoituksena varmistaa palvelun käytettävyys tilanteessa, jossa ensisijainen palveluun kohdistuu tietoinen tai tahaton palvelukatko. Pilvipalvelut, varmuuskopiot ja kahdennukset voivat sijaita missä tahansa maapallolla. Rekisterin pitäjän tulee huomioida minkä maan lainsäädäntöä pilvipalvelun tarjoajan toimintaan sovelletaan ja varmistaa EU:n komission hyväksymät maat, jotka toteuttavat tietosuoja-asetuksen vaatiman tietosuojan. (Kyberturvallisuuskeskus 2014.)

Tyypillisesti pilvipalveluiden tarjoaja toteuttaa omat tietosuojatoimenpiteensä, eikä palvelun ostavalla organisaatiolla ole mahdollista valvoa tietoturvan toteutumista. Pilvipalvelun käytettyjen teknologioiden, toimintamallien ja periaatteiden toimintaa voi olla mahdotonta vaikuttaa. Pilvipalvelua valitessa saatavilla olevat tekniset tiedot, palvelun mahdolliset sertifioinnit ja kolmansien osapuolten tekemät auditoinnit palvelusta auttavat vaatimusten ja luotettavuuden osalta. Palveluntarjoajan

toimintakulttuurin, maineen ja muiden tuotteiden perusteella voi myös luoda johtopääksiä. (Kyberturvallisuuskeskus 2014.)

Henkilötietoja tallennettaessa pilvipalveluun on rekisterinpitäjä vastuussa koko tietojen käsittelyprosessin ajan, että henkilötietoja käsitellään asetuksen mukaisesti. Yleissääntönä on, että vastuuta henkilötiedoista ei voi ulkoistaa. Tietosuoja-asetus asettaa rekisterinpitäjälle velvoitteen varmistaa, että henkilötietoja käsitellään tietosuoja-asetuksen mukaisesti.

Internetissä tarjottavat pilvipalvelut voidaan karkeasti jakaa karkeasti kolmeen pääluokkaan (NIST 2011):

- SaaS (Software as Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)

Palvelut joissa vuokrataan tallennustilaa asiakkaan tarpeisiin (tietovarasto pilvipalvelussa, Big Data) pohjautuvat IaaS-malliin ja palveluntarjoajia on satoja pienistä yrityksistä maailmanlaajuisiin. Isoimmat ja laajimmat pilvipalvelut tarjoavat Google ja Microsoft. Tiedostojen ja tietojen siirtyessä pilveen, on tietoturvan näkökulmasta huomioitava myös liikenne pilvipalveluun. (Kyberturvallisuuskeskus 2014.)

5.4 Organisatoriset ja tekniset toimenpiteet

Organisaatioiden kannattaa kiinnittää huomiota myös seuraaviin teknisiin ja organisatorisiin toimenpiteisiin.

Henkilöstöturvallisuus ja -koulutukset

Henkilöstöturvallisuudella tarkoitetaan henkilöstöön liittyviä uhkia, kuten inhimillisiä virheitä, väärinkäytöksiä ja varkauksia. Organisaation henkilöstö tulee perehdyttää tietoturvakäytänteihin ja -politiikkaan, sillä juuri ihmisen toiminta on suurin tietoturvaa uhkaava tekijä. Tietosuoja-asetus velvoittaa järjestämään henkilötietoja käsitteleville henkilöille tietosuojakoulutuksia (Yleinen tietosuoja-asetus, artikla 47). Henkilötietojen käsittelijän ja rekisterinpitäjän tulee myös laatia tarvittavat salassapito- ja vastuusopimukset.

Sertifioinnit

Yleisen tietosuoja-asetuksen ja läpinäkyvyyden noudattamisen tehostamiseksi olisi sertifiointimekanismien ja tietosuojamerkkien käyttöönottoa edistettävä. Rekisteröidyn tulisi nopeasti pystya arvioimaan asianomaisten tuotteiden ja palvelujen tietosuojan tasoa, ja että rekisterinpitäjä ja henkilötietojen kösittelijä noudattavat asetuksen mukaisia käsittelytoimia. Sertifiointielin tai toimivaltainen valvontaviranomainen myöntää ja uusii sertifioinnit. Sertifiointi myönnetään enintään kolmeksi vuodeksi kerrallaan ja sitten sen on uusittava. Valvontaviranomaisella on myös mahdollisuus peruutta sertifiointi, jos sertifiointia ja tietosuoja-asetusta koskevat vaatimukset eivät enää täyty. Tietosuojaneuvosto kerää sertifiointimekanismit, tietosuojamerkit ja -sinetit julkisesti saataville. (Yleinen tietosuoja-asetus, artikla 42.)

Asiantuntijahaastattelu

Fiarone Oy:n tietosuojakonsultti Tiia Summe painotti seuraavien tietoturvaa koskevien teknisten ratkaisujen tärkeyttä, joista henkilötietoja käsittelevän organisaation tulisi huolehtia, mutta joihin ei tässä opinnäytetyössä pystytä syvemmin perehtymään (Summe 2018):

- Tietoliikenteen salaukset
- Palvelinten ja käyttäjien päätelaitteiden suojaus
- Lokitietojen hallinta
- Palvelinten kovennukset
- Tietosuojatestaukset
- Tietojen sijainti
- Pääsyn hallinnan toteutus
- Verkkojen eriyttäminen

6 POHDINTA

6.1 Tietosuoja-asetuksen vaikutus

Tietosuoja ja tietoturva koskettaa tämän päivän digitaalisessa maailmassa kaikkia kansalaisia. Aihealue ei kuitenkaan ole kovinkaan monelle tuttu ja sen on koettu kuuluvan asiantuntijoille. Uuden tietosuoja-asetuksen näkyvyys ja sen keskeiset muutokset, rekisterinpitäjän vastuun ja rekisteröidyn oikeuksien kasvaminen, lisäävät mahdollisesti EU:n kansalaisten luottamusta verkkotoimintaan ja tukevat näin asetuksen yhtä tavoitetta.

Opinnäytetyön perusteella voidaan todeta asetuksen osoitusvelvollisuuden tuovan rekisterinpitäjille velvoitteita tarkistaa tai uudistaa organisaation sisäiset henkilötietojen käsittelyn käytänteet. Organisaatioiden tulee selvittää omassa toiminnassaan vaadittavat dokumentoitavat asiat ja panostaa aikaa organisaation sisällä sen tietoturvakäytänteihin, jotta se olisi mahdollisimman ketterää ja sen ylläpito tehokasta. Kattava dokumentaatio, tarkat sopimukset vastuunjaosta sekä tietoturvan teknisen puolen ajantasaisuus varmistaa osoitusvelvollisuuden täyttymisen ongelmatilanteissa ja pienentää riskiä sanktioista.

6.2 Yhdysvaltojen lait vs GDPR

Opinnäytetyöstä välittyy kuva Yhdysvaltojen henkilötietoihin kohdistuvan lainsäädännön hajanaisuudesta, ja että EU:n henkilötietosuoja on kattavuudessaan ja kokonaisvaltaisuudessaan Yhdysvaltoja edellä. Osa EU:n tietosuoja-asetuksen keskeisistä kohdista löytyy kuitenkin myös Yhdysvaltojen alakohtaisista laeista. Ongelmana Yhdysvalloissa on lakien ristiriidat, madonreijät ja valtiokohtaiset eroavaisuudet. Yksityisyys käsitteenä saa Yhdysvaltojen lainsäädännössä paljon pienemmän arvon kuin EU:ssa. Aiheen laajuus vaatii opinnäytetyötä kattavampaa selvitystyötä.

6.3 Työn tavoitteen toteutuminen

Opinnäytetyössä onnistuttiin luoda tiivis ja selkeä kuvaus henkilötietojen ja henkilörekisterin ylläpitämisen velvoitteista uuden tietosuoja-asetuksen näkökulmasta, vertaamaan Yhdysvaltojen henkilötietojen lainsäädännön pääkohtia GDPR:ään sekä luomaan käytännönläheinen toimintaehdotus, kuinka GDPR:n vaatimuksia voisi lähestyä. Aiheen laajuus ja tiukka aikataulu rajoittivat työn melko suuntaa antavaksi, eikä sitä kyetty suoraan räätälöidä toimeksiantoyrityksen tuotekehitysprojektia varten. Työstä kuitenkin välittyy tietosuoja-asetuksen keskeiset vaatimukset yrityksille ja organisaatioille.

Opinnäytetyön aihe oli kiinnostava, koulutustani ajatellen ajankohtainen ja uskon työstä olevan minulle hyötyä tulevaisuudessa. Tietosuojan merkityksen ymmärtäminen, IT-alan ratkaisujen tekemisen tukena, saattaa olla ratkaiseva tekijä onnistumisen ja epäonnistumisen välillä.

LÄHTEET

Andreasson, A. & Ylipartanen, A. 2016. Näin teet tietosuojan nykytila-analyysin. Viitattu 23.4.2018 https://opitietosuojaa.fi/index.php/fi/extrat/blogi/109-nait-teet-tietosuojan-nykytila-analyysin.

Coos, A. 2017. EU vs US: How Do Their Data Protection Regulations Square Off. Viitattu 26.5.2018 https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/.

Eaton, B. 2017. GDPR: How is it Different from U.S. Law & Why this Matters?. Viitattu 25.5.2018 https://www.privacyanddatasecurityinsight.com/2017/09/gdpr-how-is-it-different-from-u-s-law-why-this-matters/.

Eduskunta. 2018. EU:n yleisen tietosuoja-asetuksen (GDPR) täytäntöönpano. Viitattu 13.6.2018 https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/EUn-tietosuojauudistus/Sivut/EUn-yleinen-tietosuoja-asetus.aspx.

Euroopan komissio 2017. Opas EU:n ja yhdysvaltojen privacy shield -järjestelyyn. Viitattu 29.4.2018 https://ec.europa.eu/commission/index.fi.

Euroopan komissio 2018. Mitä tarkoittaa ’sisäänrakennettu’ ja ’oletusarvoinen’ tietosuoja. Viitattu 12.4.2018 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_fi.

Euroopan parlamentin ja neuvoston yleinen tietosuoja-asetus 2016/679. Annettu 27.4.2016 Saatavilla sähköisesti osoitteessa http://www.privacy-regulation.eu/fi/.

Henkilötietolaki 523/1999. Annettu 22.4.1999. Saatavilla sähköisesti osoitteessa https://www.finlex.fi/fi/.

Holopainen, P. 2018. Yrittäjän tietosuojaopas. Viitattu 10.4.2018 https://www.yrittajat.fi/yrittajan-abc/yritystoiminnan-abc/yrittajan-tietosuojaopas-570864.

ICLG 2018. Data Protection 2018, USA. Viitattu 7.6.2018 https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

Kyberturvallisuuskeskus 2014. Pilvipalveluiden tietoturva. Viestintävirasto. Viitattu 6.6.2018 https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf.

Lee, P. 2017. The differences between EU and US data protections laws. Viitattu 1.6.2018 https://www.youtube.com/watch?v=-_zLeGKHOpc.

Leuan, J. 2017. Data protection in the United States: overview. Viitattu 26.5.2018 https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.

Netskope 2018. EU:n uusi yleinen tietosuoja-asetus ja pilvipalveluihin liittyvien haasteiden hallinta. Viitattu 23.5.2018 https://ymon.fi/materiaalit/pdf/EU%20GDPR%20Finnish.pdf.

NIST 2011. The NIST Definition of Cloud Computing. Viitattu 6.6.2018 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Ohjelmistoyrittäjät ry. 2018. EU:n tietosuoja-asetu – sanasto. Viitattu 13.6.2018 https://gdpr.fi/sanasto/.

OpiTietosuojaa.fi 2017. EU:n yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt. Viitattu 28.4.2016 https://opitietosuojaa.fi/fi/oikeus/lait/eu-n-tietosuoja-asetus/23-eun-tietosuoja-asetus.

Pietikäinen, S. 2016. Lainsäädännön taustaa. Viitattu 3.5.2018 https://www.vahtiohje.fi/web/guest/lainsaadannon-taustaa.

Summe 2018. Haastattelu. Fiarone Oy:n tietosuoja konsultti Tiia Summetta haastatteli 28.5.2018 opinnäytetyöntekijä Hannu Pohjalainen.

Terhi Meriläinen, 2017. Pilvipalvelut yrityksen tietoturvan kulmakivenä. Viitattu 6.6.2018 https://magiccloud.fi/pilvipalvelut-yrityksen-tietoturvan-kulmakivena/.

Tietosuojatyöryhmä 2017. Vaikutustenarviointi. Viitattu 24.4.2018. https://tietosuoja.fi/documents/6927448/8316711/Vaikutustenarviointi+fi.pdf/af51e999-5326-4223-9deb-e21bdd2e0a63/Vaikutustenarviointi+fi.pdf.pdf.

Tietosuojavaltuutetun toimisto 2014. Laadi tietotilinpäätös. Viitattu 29.4.2018 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/tiedotteet/6JEcJrDjj/Laadi_tietotilinpaatos.pdf

Tietosuojavaltuutetun toimisto 2017. Tietosuojavastaavat. Viitattu 18.4.2018 http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/tietosuojavastaavat.html.

Tietosuojavaltuutetun toimisto 2018a. EU:n tietosuojauudistus. Viitattu 10.5.2018 http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html#mitenvalmistautuatietosuoja-asetukseen.

Tietosuojavaltuutetun toimisto 2018b. Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi. Viitattu 10.6.2018 https://tietosuoja.fi/arvioi-riskit.

Tietosuojavaltuutetun toimisto 4/2017. Miten valmistautua EU:n tietosuoja-asetukseen. Viitattu 7.4.2017 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf.

Tietoturvallinen Suomi 2017. EU:n tietosuoja-asetus ja sen vaikutukset Mikko Hyppönen (F-Secure) - #TietoturvallinenSuomi. https://www.youtube.com/watch?v=XiMVzR7byFg.

Valtionvarainministeriö 2009. Vahti-ohjeet: Lokien säilytys, kerääminen ja suojaaminen. Viitattu 2.6.2018 https://www.vahtiohje.fi/web/guest/lokien-sailytys-keraaminen-ja-suojaaminen.