Veijo Lyytikäinen

GDPR-ASETUS JA NOUDATTAMINEN ALFAME SYSTEMS OY:SSÄ

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Teknologiaosaamisen johtamisen koulutusohjelma
Toukokuu 2020

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Yksikkö Kokkola	**Aika** Toukokuu 2020	**Tekijä/tekijät** Veijo Lyytikäinen
Koulutusohjelma Teknologiaosaamisen johtaminen		
Työn nimi GDPR-ASETUS JA NOUDATTAMINEN ALFAME SYSTEMS OY:SSÄ		
Työn ohjaaja Pekka Makkonen		**Sivumäärä** 54 + 1
Työelämäohjaaja		

Euroopan unionin yleinen tietosuoja-asetus astui voimaan toukokuun 25. päivänä 2018. Voimaantulo asetti henkilötietojen käsittelijöille ja rekisterien pitäjille suoria velvoitteita.

Opinnäytetyöni tavoitteena tutustuin Euroopan Unionin uuteen tietosuoja-asetukseen ja pohdin sen vaikutuksia Alfame Systems Oy:n toiminnan kannalta. Tietosuoja-asetukseen tutustuin osallistumalla useampaan aihepiiriin liittyvään koulutukseen ja tutustumalla aihepiiriin liittyvään kirjallisuuteen. Teoriaan tutustuessani toteutin tarvittavat dokumentaatiot osoitusvelvollisuuden tueksi.

Opinnäytetyön teoriaosuudessa käsitellään ensiksi Suomessa aikaisemmin vallinnutta tapaa käsitellä henkilötietoja, jonka jälkeen syvennytään tarkemmin GDPR:n sisältöön ja vaatimuksiin. Tutkimusosuudessa selvitin kyselyn ja haastatteluiden avulla, miten organisaatiossa tunnistetaan tietoturva ja -suoja asiat ja tietosuoja-asetus.

Tutkimuksen tuloksena havaitsin, että tietoturva pitää saada osaksi yrityskulttuuria. Tietoturvaan liittyvät dokumentaatiot täytyy olla helposti löydettäviä ja sisällöt täytyy tuoda lähelle arkipäiväistä toimintaa. Lisäksi tavat oppia vaihtelevat henkilöiden mukaan, joten täytyy huomioida erilaiset tavat tietoisuuden lisäämiseksi. Tutkimustuloksien avulla on tarkoitus jatkokehittää yrityksen tietoturvaa.

Asiasanat
Tietosuoja-asetus, rekisteri, rekisterinpitäjä, rekisteröity, henkilötieto, osoitusvelvollisuus, tietosuoja, tietoturva

ABSTRACT

CENTRIA UNIVERSITY OF APPLIED SCIENCES Kokkola	**Date** May 2020	**Author** Veijo Lyytikäinen
Degree programme Technology Management		
Name of thesis General Data Protection Regulation in the Alfame Systems Oy		
Instructor Pekka Makkonen		**Pages** 54 + 1
Supervisor		

The General Data Protection Regulation of the European Union entered into force on 25 May 2018. The entry into force imposed direct obligations on processors of personal data and registrars.

The aim of my thesis was to get acquainted with the new data protection regulation of the European Union and to consider its effects on the operations of Alfame Systems Oy. I became acquainted with the Data Protection Regulation by participating in training on several topics and by getting familiar with literature on the topic. After getting acquainted with the theory, I implemented the necessary documentation to support the obligation to demonstrate compliance.

The theoretical part of the thesis first describes with the way of processing personal data that previously prevailed in Finland, after which we delve deeper into the content and requirements of the GDPR. In the research part, I used a survey and interviews to find out how information security and protection issues and the data protection regulation are understood in the organization.

As a result of the research, I observed that information security needs to be integrated into the corporate culture. Security-related documentation must be easy to find and the content must be brought close to everyday activities. In addition, ways of learning vary from person to person, so different ways of raising awareness need to be considered. The research results enable further developing the information security of the company.

Key words
General Data Protection Regulation, register, data controller, registered customer, personal data, accountability, privacy, information security

KÄSITTEIDEN MÄÄRITTELY

GDPR-asetus (General Data Protection Regulation)
EU:n tietosuoja-asetus, mikä tuli voimaan keväällä 2016 ja asetusta aletaan soveltaa 25.5.2018 alkaen. Asetus korvaa henkilötietolain ja vaikuttaa siten niin julkisella kuin yksityisellä sektorilla.

Henkilötieto (personal data)
Asetuksen mukaan kaikki henkilöä yksilöivä tieto on henkilötietoa. Henkilötietoa ovat näin ollen esimerkiksi nimi, kotiosoite, valokuva, sähköpostiosoite, sosiaalisen median päivitykset, tilaukset ja ostokset, pankkitiedot, käyttäjätunnus ja salasana, maksukorttinumero sekä IP-osoite.

Henkilötietojen käsittelijä (data processor)
Taho, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.

Osoitusvelvollisuus (accountability)
Tarkoittaa rekisterinpitäjän velvollisuutta kyetä osoittamaan noudattavansa tietosuojalainsäädäntöä.

Pilvipalvelut (cloud services)
Verkon yli käytettävien palvelimien verkosto, jotka mahdollistavat pääsyn dataan paikasta ja ajasta riippumatta.

Rekisterinpitäjä (data controller)
Henkilörekisterin vastaava, voi olla myös yritys, viranomainen, yhdistys, laitos tai säätiö. On juridisessa vastuussa rekisteristä, määrää rekisterin käytöstä, sekä on taho, jonka käyttöä varten rekisteri on luotu. Rekisterinpitäjän on lain mukaan laadittava rekisteriseloste, josta käy ilmi muun muassa rekisterin käyttötarkoitus, kerättävät tiedot ja niiden tietolähteet, rekisterin suojaus sekä rekisterinpitäjän yhteystiedot.

Tietosuoja (privacy)
Sisältää henkilötietojen luottamuksellisuuden lisäksi rikoslain kunniaa, yksityisen suojaa ja tietoliikennettä koskevat säännökset. Perustuu viime kädessä perustuslain säännöksiin.

Tietosuojavastaava (data protection officer)

Organisaatioon on nimettävä tietosuojavastaava, jos organisaation ydintoimintoihin kuuluu arkojen henkilötietojen tai laajojen henkilötietorekisterien käsittely. Asetuksessa suositellaan nimeämään kaikkiin yrityksiin tietosuojavastaava. Tietosuojavastaavan tehtäviin kuuluu asiantuntija-avun antaminen sekä organisaation henkilöstölle että organisaation johdolle tietosuojaan liittyvissä kysymyksissä. Tietosuojavastaavan tulee myös toimia organisaation henkilötietojen käsittelyä valvovana tahona sekä yhdyssitteenä valvontaviranomaisiin, kuten tietosuojavaltuutettuun.

Tietotilinpäätös (data balance sheet)

Tietosuoja-asetus edellyttää yrityksiä dokumentoimaan rekisterien hallintaan liittyvät tietoturvakäytännöt. Dokumentoinnin voi tehdä muullakin tapaa kuin tietotilinpäätöksellä, mutta se on ollut tietosuojavaltuutetun suosittelema tapa jo ennen uutta lainsäädäntöä. Tietosuojavaltuutetun julkaiseman oppaan mukaan tietotilinpäätöksen tavoitteena on antaa kuvaus tietojen käsittelyn nykytilasta sekä arvio tietosuojan ja tietoturvan toteutumisesta. Tietotilinpäätös osoittaa organisaation noudattavan hyvää tietojenkäsittelytapaa ja se toimii myös yhtenä keinona tietosuoja-asetuksen osoitusvelvollisuuden toteuttamisessa.

Tietoturva (information security)

Tarkoittaa tiedon saatavuuden, luottamuksellisuuden ja eheyden ylläpitämistä. Tietoturva koskee myös tiedon suojaamista sen siirtämisen aikana.

Tietoturvauhka (security threat)

Tietoturvauhkia ovat luvaton pääsy, tiedon luvaton käyttö, salaisen tiedon paljastuminen, tiedon sekaannus, tiedon muuntuminen, salaisen tiedon tutkituksi tuleminen, tiedon kopioituminen ja tiedon hävittäminen.

Tietosuojavaltuutettu (data protection supervisor)

Viranomainen, joka valvoo henkilötietojen rekisteröintiä, käyttöä ja luovutusta. Hän voi antaa ohjeita rekisterinpitäjälle, mutta ne eivät ole sitovia. Jos rekisterinpitäjä ei noudata ohjeistusta, tietosuojavaltuutettu voi viedä asian tietosuojalautakunnan käsiteltäväksi

LYHENTEET

1050/2018 – Suomen kansallinen tietosuojalaki, jolla täsmennetään ja täydennetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY-kumoamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 (yleinen tietosuoja-asetus). ja sen kansallista soveltamista.

1054/2018 – Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä.

2008/977/YOS – Neuvoston puitepäätös rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta.

2016/679 – Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.

621/1999 – Laki viranomaisten toiminnan julkisuudesta. Tarkoituksena toteuttaa avoimuutta viranomaisten toiminnassa sekä antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan.

634/2011 – Laki julkisen hallinnon tietohallinnon ohjauksesta. Tarkoituksena tehostaa julkisen hallinnon toimintaa sekä parantaa julkisia palveluja ja niiden saatavuutta säätämällä julkisen hallinnon tietohallinnon ohjauksesta ja tietojärjestelmien yhteentoimivuuden edistämisestä ja varmistamisesta.

95/46/EY – Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.

API – Ohjelmointirajapinta, jossa määritetään kuinka eri ohjelmat voivat tehdä pyyntöjä ja vaihtaa tietoja keskenään.

ASA – Alfame Systems Oy:n tietoturva ja turvallisuuspalvelu, jonka tehtävä on vastata yrityksen tietoturva-asioista.

CLI – Komentokehote, joka mahdollistaa kommunikoinnin ihmisen ja tietokoneen välillä.

DPIA – Vaikutustenarviointi, mikä tulee toteuttaa, jos henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin luonnollisen henkilön oikeuksille ja vapauksille.

EDPB – Euroopan tietosuojaneuvosto, joka koostuu kansallisten tietosuojaviranomaisten ja Euroopan tietosuojavaltuutetun (EDPS) edustajista.

EDPS – Euroopan tietosuojavaltuutettu on Euroopan unioin toimielin, joka tehtävänä on valvoa, että kaikki Euroopan unionin elimet noudattavat määräyksiä ihmisten oikeudesta yksityisyyteen niiden käsitellessä henkilötietoja.

ETA – Euroopan talousalue, johon kuuluvat Euroopan unionin jäsenvaltiot (Alankomaat, Belgia, Bulgaria, Espanja, Irlanti, Iso-Britannia (Iso-Britannian ja Pohjois-Irlannin yhdistys kuningaskunta ja Gibraltar), Italia, Itävalta, Kreikka, Kroatia, Kypros, Latvia, Liettua, Luxemburg, Malta, Portugali, Puola, Ranska, Romania, Ruotsi, Saksa, Slovakia, Slovenia, Suomi, Tanska, Tsekin tasavalta, Unkari ja Viro) lisäksi Islanti, Liechtenstein ja Norja.

EU – Euroopan unioni

FTP – TCP-protokollaa hyödyntävä tiedostonsiirtomenetelmä kahden laitteiston (tietokoneen) välillä.

GDPR – General Data Protection Regulation, suomessa yleisesti EU:n tietosuoja-asetus.

HaVM 13/2018 – Hallintovaliokunnan mietintö 13/2018

HaVM 14/2018 – Hallintovaliokunnan mietintö 14/2018

JSON – Ohjelmointikielestä riippumaton avoimen standardin tiedostomuoto, jonka tiedostopääte on .json.

SFTP – Tiedonkäsittelymenetelmä SSH-protokollan yli.

SSH – Protokolla, joka mahdollistaa salatun tietoliikenteen kahden laitteiston (tietokoneen) välillä.

WP29 – 29 artiklan mukainen työryhmä, riippumaton EU:n tietoryhmä, joka käsitteli yksilöiden suojelua henkilötietojen käsittelyssä koskevia kysymyksiä 25. toukokuuta 2018 asti. Tietosuojaryhmä koostuu niin että jäseninä on yksi edustaja kustakin EU-maasta. Muita dokumentaatiossa käsiteltyjä työryhmiä on myös WP168 ja WP248 työryhmät.

XML – Tekstimuotoisia, parsittavia tiedostoja, jotka sisältävät XML (Extensible Markup Language) -kielen mukaisesti esitettyä dataa. Sen tiedostopääte on .xml.

1 JOHDANTO

1.1 Työn tavoitteet ja tarkoitus

EU:n yleinen tietosuoja-asetus (EU) 2016/679 hyväksyttiin huhtikuussa 2016 (14.4.2016) Euroopan parlamentin ja neuvoston päätöksillä. Toimin Alfame Systems Oy:ssä tietosuojavastaavan roolissa, tehtäväalueena vastata tietoturvasta ja -suojasta. Lopputyön teoriaosuuden tavoitteena on tutustua tietosuoja-asetukseen ja toteuttaa tarvittavat dokumentaatiot osoitusvelvollisuuden avuksi. Henkilötietojen käsittelyn tulee olla aina lainmukaista ja käsittelyn yhteydessä täytyy aina varmistaa kaikkien tietosuojaperiaatteiden ja muiden tietojenkäsittelyä koskevien vaatimusten toteutuminen. EU:n tietosuoja-asetus astui voimaan 25.5.2018 alkaen koko EU:n alueella.

Tutkimuksen tarkoituksena on selvittää:

1. Kuinka Alfame Systems Oy:ssä tunnetaan tietoturvaan ja -suojaan liittyvät ohjeistukset, noudatetaanko niitä ja koetaanko niiden noudattaminen työtä haittaaviksi tai edistäviksi toimenpiteiksi ja koetaanko nykyiset tietoturvallisuuskäytännöt riittäviksi?
2. Mitkä asiat koetaan Alfame Systems Oy:n kannalta pahimmiksi tietoturvauhkiksi?
3. Tunnetaanko yrityksessä tietosuojakäytännöt ja kuinka hyvin niitä noudatetaan?
4. Tunnetaanko yrityksessä käytettävät pilviratkaisut, kuinka huolissaan ollaan niiden turvallisuudesta, tunnistetaanko erilaiset pilviratkaisut ja tunnistetaanko erilaisten pilviratkaisujen palvelun tilaajan ja palvelun tuottajan vastuut?
5. Kuinka hyvin Alfame Systems Oy:ssä tunnetaan riskienhallintaan liittyvät ohjeistukset ja koetaanko nykyiset ratkaisut riittäviksi?
6. Kuinka hyvin Alfame Systems Oy:ssä tunnetaan tietosuojalaki, tarvitaanko asiaan liittyvää lisäkoulutusta, tunnistetaanko tietosuojalain kannalta tärkeimmät termit, koetaanko tietosuojalaki toimintaa haittaavaksi vai edistäväksi asiaksi?
7. Pohtia kyselytutkimuksen ja haastattelujen perusteella saadun informaation perusteella tärkeimpiä kehitysvaiheita organisaation tietoturvan parantamiseksi.

Tutkimuksessa on tarkoitus kartoittaa yrityksessä tarvittavaa lisäkoulutusta ja mahdollisia lisätoimenpiteitä riittävän tietoturvan ja riskienhallinnan varmistamiseksi. Tutkimuksessa kertynyttä informaatiota on tarkoitus myös käyttää jatkuvan tietoturvan ylläpitämiseksi ja lainmukaisen henkilötietojen käsittelyn toteuttamiseksi. Lisäksi opinnäytetyön ohessa varmistetaan yrityksen henkilökunnan tietämystä EU:n

yleisestä tietosuoja-asetuksesta. Henkilökohtainen tavoitteeni on ohessa kehittää ammatillista osaamistani tietoturvasta ja -suojasta ja tietosuojalain noudattamisesta. Oppimisprosessistani on hyötyä myös toimenkuvani kannalta yrityksessä, koska vastaan osaltani organisaation tietoturva-asioista.

1.2 Taustaa

Alfame Systems Oy on 2004 Kokkolassa alkunsa saanut IT-alan laajasti menestynyt yritys, joka tuottaa kokonaisvaltaisia digitaalisia integraatio ratkaisuja. Työskentelemme paikasta riippumatta, joten tietoturva-asiat on huomioitava myös etäratkaisujen kannalta. Toimipisteitä yrityksellä on nykyään neljä: Kokkola, Helsinki, Tampere ja Rovaniemi. Opinnäytetyössäni huomioin tietoturvallisuuden vain toimistotilojen osalta jo anonyymisyydenkin lähtökohdasta ajatellen.

Tietosuoja-asetuksen vaatimiin muutoksiin lähdettiin valmistautumaan 2017 vuoden puolivälissä siitä lähtökohdasta, että tutustuin ensin yrityksen sen hetkisiin tietoturvaa ja -suojaa kuvaaviin dokumentaatioihin. Tietosuoja-asetuksen mukaisten valmistautumisten alkaessa yrityksemme oli verrattain pieni reilu 30 henkeä ja silloin yrityksellä oli vain kaksi toimistoa. Muodostimme kahden hengen tiimin, jonka vastuulla tulisi olemaan tietoturvasta huolehtiminen. Tiimiin kuuluu lisäkseni yrityksen tuotantojohtaja. Annoimme tiimille nimeksi: Tietoturva ja turvallisuuspalvelu (ASA). EU:n yleinen tietosuoja-asetus ei ollut minulle entuudestaan tuttu, joten sekin oli syy lähteä perehtymään aihepiiriin ja sen säännöksiin opinnäytetyön ohessa.

1.3 Tutkimuksen toteutus ja työn rakenne

Opinnäytetyöni teoreettinen lähtökohta pohjautuu EU:n tietosuoja-asetuksen mukaiseen lainsäädäntöön henkilötietojen käsittelystä. Työn empiirisessä osiossa tarkastellaan tietosuoja-asetuksen tilannetta Alfame Systems Oy:ssä ja miten eri tehtävissä toimivat henkilöt ovat omaksuneet EU:n tietosuoja-asetuksen osaksi heidän työtehtäviään. Lisäksi pohditaan jatkokehityskohteita tietoturvan ja siitä tiedottamisen suhteen.

Tutkimukseen liittyvän aineiston hankintamenetelminä käytin varsinaisten yrityksen sisäisten dokumentaatioiden luonnissa tietosuoja-asetukseen liittyvien koulutusten materiaalia ja tutkimuksen empiiriseen osaan opinnäytetyön ohessa toteutettua kyselytutkimusta. Tietosuoja-asetukseen tutustuin osallistumalla

useisiin koulutuksiin aihepiiristä. Ensimmäinen aihepiiriin liittyvä koulutus oli 10 toukokuuta 2017 Canorama Oy:n järjestämä EU:n tietosuoja-asetusseminaari Kokkolassa.

Perehtymistäni jatkoin KOSEK – Kokkolanseudun Kehitys Oy:n koulutuksesta 9 tammikuuta 2018 – Miten valmistautua EU:n tietosuoja-asetukseen? Lisäksi kävin Insinööriliiton järjestöjohdon neuvottelupäivillä Turussa 26 tammikuuta – EU:n tietosuoja-asetus liiton ja jäsenjärjestöjen toiminnan kannalta koulutuksen ja Patentti ja rekisterihallituksen GDPR koulutuksen, jossa oli puhujana Päivi Korpisaari, joka on viestintäoikeuden professori ja oikeusministeriön asettaman tietosuojaryhmän jäsen. Koulutusten kautta sain hyvän teoriapohjan, jota täydensin useilla aihepiiristä kirjoitetuilla teoksilla. Kyselytutkimuksen avulla selvitin, kuinka hyvin lopputyön ohessa dokumentoitu ohjeistus tunnetaan yrityksen sisällä ja kuinka hyvin yleisellä tasolla tunnetaan EU:n tietosuoja-asetuksen sisältö.

Opinnäytetyössäni käsitellään teoriaosassa ensin tietoturvapolitiikkaa ja riskienhallintaa ja siihen liittyvää vaikutustenarviointia. Sitten tutustutaan lainsäädännön taustaan ja lopuksi käydään läpi EU:n tietosuoja-asetuksen keskeiset osiot. Asetuksen osalta käsitellään osoitusvelvollisuus, asetuksen tuomat muutokset, rekisteröidyn oikeudet, rekisterinpitäjän ja käsittelijän velvollisuudet ja mahdollisten väärinkäytösten sanktiot. Lisäksi työssä käsitellään yleisesti tietoturvallisuutta, koska se liittyy keskeisesti asetuksen mukaiseen henkilötietojen käsittelyyn. Teoria osan jälkeen käsitellään tietosuojakyselyn tulokset ja arvioidaan kehitystoimenpiteitä. Lopuksi pohditaan työn onnistumista ja matkan varrelta huomattuja asioita.

2 TIETOTURVAPOLITIIKKA

Tietoturva- ja tietosuojapolitiikka ovat olennainen osa EU:n tietosuojadirektiiviä. Riskienhallinta muodostaa myös olennaisen osan yrityksen tietoturvaa. EU:n yleinen tietosuoja-asetus vaatii myös henkilötietojen tietojenkäsittelyyn liittyvien riskien ennakoivaa hallintaa, niihin varautumista ja niistä ilmoittamista. Lisäksi vaaditaan kykyä todistaa tehdyt toimenpiteet viranomaisille. (Tietosuoja-asetus 2016/679.)

2.1 Yleiskuvaus

Tieto on yrityksen pääomaa ja tietämys toimii kilpailuvalttina. Organisaatiot tutkivat jatkuvasti uusia työkaluja ja näiden tuomia mahdollisuuksia. Kehittyneempää teknologiaa otetaan säännöllisesti käyttöön. Säännölliset muutokset työkaluissa asettavat samalla uusia vaatimuksia tietoturvapolitiikoille ja niiden säännölliselle kehittämiselle. Tiedon suojaamiseksi täytyy kehittää eritasoista tietoturvaa. Tietoturva jaetaan hallinnolliseen ja fyysiseen tietoturvaan. Tietoturvallinen toiminta kaipaa johtamista ja toimintatapojen kehittämistä.

Hallinnollinen tietoturva koostuu menettelytavoista fyysisen tietoturvan osa-alueiden ohjaamiseen. Tietoturvalliset toimintatavat täytyy myös sisällyttää yrityksen päivittäisiin prosesseihin. Tällöin varmistetaan tietoturvan huomiointi työntekijöiden ja yritysjohdon tasolla päivittäisessä tekemisessä. Hallinnollisessa tietoturvassa huomioidaan ja dokumentoidaan seuraavat asiat: nykytilan kartoitus, riskienhallinta, sopimukset, suunnitelmat, tietoturvapolitiikka, tietoturvaohjelman laatiminen. Henkilöstön organisointi, suhteet asiakkaisiin ja muut yleiset linjaukset kuuluvat myös hallinnollisen tietoturvan tehtäviin.

Fyysisessä tietoturvassa huomioidaan vastaavasti: henkilöstön tietoturvallinen toiminta, käyttöturvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus ja tietoaineistoturvallisuus. (Valtiovarainministeriö 2003.) Lisäksi yrityksen täytyy pystyä arvioimaan ja mittaamaan tietoturvan taso säännöllisesti.

Tietoturvan mittaamiset toimivat tietoturvan jatkuvan kehittämisen apuvälineenä. Organisaation johdon tulee ymmärtää yrityksen tietojärjestelmät, niiden toiminta ja niihin liittyvät tietoturvariskit. Lisäksi tarvitaan erillinen tietoturvaryhmä, joka muodostuu organisaation eri tason työntekijöistä muodostaakseen riittävän laajan ymmärryksen tiedosta ja sen käyttötavoista.

Useimmiten tietoturvan heikoimpina lenkkeinä pidetään ihmisen inhimillistä virhettä, pilvipalveluita ja puhelinten käyttöön liittyviä riskejä (Check Point Security Report 2019). Näiden tekijöiden perusteella voimme todeta, että tärkein avaintekijä tietoturvallisen toiminnan toteuttamiseksi on asian ymmärtävä henkilöstö ja avoimuus ja vuorovaikutteinen viestintä kaikilla organisaation tasoilla. Henkilöstön täytyy tietää, miten tietoturvallisuutta seurataan ja mitä seuraamuksia rikkomuksista seuraa. Löytyneisiin puutteisiin on puututtava nopeasti ja henkilöstöä ohjeistettava säännöllisesti ja riittävällä tasolla.

2.2 Riskienhallinta tietojenkäsittelyssä

EU:n yleinen tietosuoja-asetuksen lähtökohta henkilötietojen käsittelyyn on siihen liittyvien riskien tunnistaminen ja niiden hallinta (Tietosuoja-asetus 2016/679). Henkilötietojen käsittelyyn liittyvät riskit on arvioitava ja pyrittävä riittävällä tasolla minimoimaan arvioituun riskitasoon nähden. Riskitasoon vaikuttavia tekijöitä ovat: henkilöstön osaaminen, rekisteröityjen oikeudet, järjestelmän luonne, käyttäjien määrä, henkilötietojen arkaluonteisuus ja määrä ja tietojenkäsittelyn ulkoistuksen luonne. Riskienhallinta pitää olla hallittua ja jatkuvaa pysyäkseen lisääntyvien ja jatkuvasti kehittyvien uhkien tasolla.

Arvioidessa tietoturvariskejä täytyy huomioida uhkia monesta eri suunnasta. Uhkat voivat syntyä organisaation sisältä tai ulkopuolelta ja voivat olla tahattomia tai tahallisia. Riskit on mahdollista määritellä maltillisesti (riski lasketaan tilastollisesti ja saadaan todennäköisyydet onnistumiselle ja epäonnistumiselle) ja radikaalisti (saadun ymmärryksen mukaisesti arvioidaan asioita epävarmuudessa pystymättä ennakoimaan seurauksia) ja ne ovat kontekstisidonnaisia ja henkilöiden riskiarviot muuttuvat ajan ja paikan suhteen (Korja 2016, 158). Riskienhallintatyön tavoitteisiin kuuluu virheistä oppiminen.

Tietoturvariskien systemaattinen hallinta on ratkaisu palvelujen turvalliseen toteutukseen, tehokkuuteen ja laatuun. Järjestelmällisyys auttaa hallitsemaan myös parhaiten aikatauluja ja kustannuksia. (Andreasson, Riikonen, Ylipartanen 2019, 57.)

Hyvin suunniteltu riskienhallinta on keskeinen apukeino toteuttaa jatkuva prosessi, missä riskit tunnistetaan etukäteen mahdollisimman hyvin ja niihin voidaan varautua (Andreasson ym. 2019, 57).

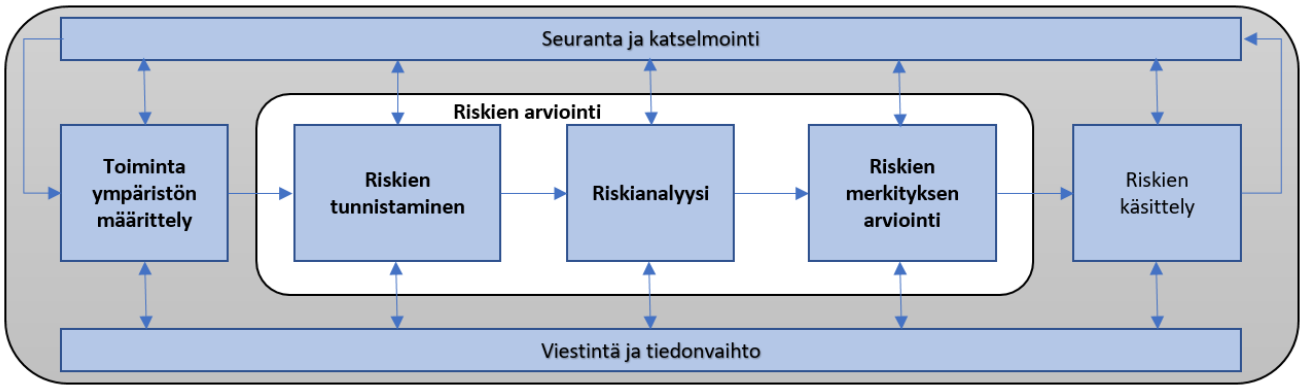
Taulukko 1. Tietoturvallisuuden arvioinnin eri osa-alueet (Tietoturvariskien arviointi 2019)

Termi	Merkitys
Hallinnollinen tietoturvallisuus	- Organisaation johdon ymmärrys tietoturvariskeistä. - Hallittu tietoturvatyö, osaamisen hyödyntäminen ja riskienhallinnan muiden lähtökohtien luominen, hankinnat ja organisaation suhteet asiakkaisiin ja sidosryhmiin.
Henkilöstöturvallisuus	- Henkilöstöön liittyvien riskien hallinta käytännön työssä. - Tietoisuus uhkista, osaamisen lisääminen kouluttamalla.
Fyysinen turvallisuus	- Organisaation tuotanto- ja toimitilojen fyysiseen suojaamiseen liittyvät asiat, joilla pyritään estämään tietojen tuhoutuminen, vahingoittuminen tai joutuminen vääriin käsiin.
Tietoliikenneturvallisuus	- Tietoliikennelaitteiston kokoonpano, luettelointi, ylläpito ja muutosten valvonta, ongelmatilanteiden kirjaus, käytön valvonta, verkon hallinta, viestinnän salaus ja varmistaminen, tietoturvallisuuden kannalta merkityksellisten tapahtumien tarkkailu, kirjaus ja selvittäminen sekä tietoliikenne ohjelmien testaus ja hyväksyminen.
Laitteistoturvallisuus	- Tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyden, toiminnan, kokoonpanon, kunnossapidon ja laadunvarmistuksen.
Ohjelmistoturvallisuus	- Organisaation käyttämät käyttöjärjestelmät, ohjelmistot sekä sovellus- ja tietoliikenneohjelmat. - Ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta-, ja varmistusmenettelyt, tarkkailu ja paljastustoimet, lokimenettelyt, ohjelmistojen laadunvarmistus sekä turvallisuustoimet.
Tietoaineistoturvallisuus	- Asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden. - Tietoaineistojen luokitus ja luettelointi, tietovälineiden asianmukainen hallinta, käsittely, säilytys ja hävittäminen.

Käyttöturvallisuus	- Kattaa tietokoneen käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvän turvallisuuden. - Riskianalyysissä arvioidaan etätyöhön kohdistuvia uhkia, niiden todennäköisyyksiä ja vaikutuksia ja valitaan toimenpiteet, joilla riski saadaan halutulle tasolle.

Organisaation johdolle kiinnostavimmat ovat riskien todennäköisyydet, niiden vakavuudet ja toteutuessaan riskien kustannusvaikutukset. Jokaisen riskin osalta on arvioitava todennäköisyys ja mitä toteutuessaan organisaatiolle seuraa ja millainen riskin kustannusvaikutus on. Arvioidut riskit luokitellaan todennäköisyyksien mukaisesti alhaisen-, keski- ja korkeantason riskeihin. Myös niiden vaikutukset organisaatiolle arvioidaan vastaavasti vähäisiin, vakaviin ja erittäin vakaviin riskeihin.

Saatujen arviointien perusteella riskit jaetaan yleisesti 5 riskikategoriaan: merkityksetön, vähäinen, kohtalainen, merkittävä ja sietämätön riski. Jokaiselle riskikategorialle määritellään tietoturvatoimenpiteet, joiden mukaan niiden kanssa toimitaan. Aloitetaan riskien hallinta ja niiden seuraaminen. Sovittuja toimenpiteitä tulisi seurata vähintään kerran vuodessa, mieluummin kerran kuussa. Seurannan tarkoitus on tunnistaa ja poistaa mahdolliset tietoturvauhat. (Tietoturvariskien arviointi 2019.)



KUVA 1. Riskienhallintaprosessi

Riskienhallinta on tehokkainta, kun se kuuluu osana johtamisen ja toiminnan prosesseja sekä suunnittelua ja seurantaa. Tavoitteena ajantasainen ja kattava käsitys riskeistä ja riskienhallinnan vastuista ja seurantajärjestelmä niitä varten. Riskienhallinta on jokaisen organisaation työntekijän vastuulla kuten myös poikkeamien havaitseminen ja niistä ilmoittaminen. (Valtiovarainministeriö 2017.)

2.3 Vaikutustenarviointi (DPIA)

Vaikutustenarvioinnissa dokumentoidaan yrityksen henkilötietojen käsittely, arvioidaan käsittelyn tarpeellisuus ja niihin kohdistuvat riskit sekä toimenpiteet, miten niihin puututaan (Andreasson ym. 2019, 69-70).

2.3.1 Määritelmä ja oikeusperuste

Vaikutustenarviointia edellyttää riskien arviointi koska vain korkeariskisistä toimenpiteistä on lain mukaan tehtävä arviointi. EU:n tietosuoja-asetuksessa vaikutustenarvioinnista on säädetty 35 artiklassa.

> 1. Jos tietyntyyppinen käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa – käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen – luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin, rekisterinpitäjän on ennen käsittelyä toteutettava arviointi suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle. Yhtä arviota voidaan käyttää samankaltaisiin vastaavia korkeita riskejä aiheuttaviin käsittelytoimiin.

(Tietosuoja-asetus 2016/679, artikla 35)

Direktiivin 95/46/EY 29 artiklalla perustettiin tietosuojaryhmä, joka on tuottanut ohjeet, joissa selvitetään ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”. Tietosuoja-asetuksen 35 artiklassa viitatulla ”luonnollisen henkilön oikeuksien ja vapauksien kannalta” tarkoitetaan:

Tietosuojaryhmä WP248 lausunnossa esitetään, viittaaminen rekisteröityjen ”oikeuksiin ja vapauksiin” koskee ensisijaisesti oikeutta tietosuojaan ja oikeutta yksityisyyteen mutta voi myös sisältää muita perusoikeuksia, kuten sananvapauden, ajatuksenvapauden, liikkumisvapauden, syrjintäkiellon, oikeuden vapauteen sekä omantunnon ja uskonnon vapauden (Tietosuojaryhmä WP248 2017, 7).

2.3.2 Milloin vaikutustenarviointi täytyy toteuttaa?

Tekijöitä, jotka nostavat henkilötietojen käsittelyn riskiluokkaa:

- Järjestelmään rekisteröityjen henkilöiden suuri määrä.
- Henkilötietojen laajuus.
- Arkaluontoisuus (terveystiedot, rotu/etnisyys, ammattiliittoasiat, geneettiset/biometriset tunnistustiedot, seksuaalinen käyttäytyminen, uskonto/filosofinen vakaumus, rikokset)
- Heikossa asemassa olevat rekisteröidyt (lapset, yrityksen omat työntekijät)
- Automaattinen päätöksenteko, rekisteröidyn arviointi tai pisteytys (luottopäätös, profilointi)
- Rekisteröityjen järjestelmällinen valvonta (sijaintitiedot, verkkokäyttäytyminen)
- Tietojensiirrot EU/ETA-maiden ulkopuolella
- Tietojen yhdistely (lähteiden yhdistely)
- Uusien teknologioiden käyttöönotto
- Käsittely, joka estää rekisteröityä käyttämästä palvelua tai oikeuksiaan (luottohakemuksen hylkäys automaattisen arvioinnin perusteella)
- Poikkeaminen rekisteröidyn informoinnista tietosuoja-asetuksen 14.5 artiklan nojalla

Mitä useampi riskitekijöistä täyttyy, sitä tärkeämpää on varmistaa vaikutustenarvioinnin toteutus. (Andreasson ym. 2019, 69; Tietosuojavaltuutetun toimisto 2018a).

2.3.3 Milloin vaikutustenarviointia ei tarvitse toteuttaa?

Vaikutustenarviointia ei vaadita WP29-tietosuojaryhmän mielestä jos:

- Henkilötietojen käsittelyn ei nähdä aiheuttavan luonnollisen henkilön oikeuksien ja vapauksien kannalta korkeaa riskiä.
- Samankaltaiseen käsittelyyn liittyen on jo toteutettu vaikutustenarviointi, huomioiden käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Silloin voidaan käyttää aiemmin laaditun vaikutustenarvioinnin tuloksia.
- Milloin valvontaviranomainen on tarkastanut henkilötietojen käsittelytoimet ennen toukokuuta 2018, eivätkä olosuhteet ole muuttuneet.

- Milloin käsittelytoimella on tietosuoja-asetuksen 6 artiklan 1 kohdan c (lakisääteisen velvoitteen noudattaminen) tai e (yleinen etu tai julkisen vallan käyttö) nojalla oikeusperuste EU:n oikeudessa tai jäsenvaltion lainsäädännössä ja milloin tietosuoja koskeva vaikutustenarviointi on jo aiemmin tehty kyseisen käsittelyn oikeusperusteen määrittämisen yhteydessä.
- Missä käsittely sisältyy valvontaviranomaisen laatimaan vapaaehtoisuuden periaatteeseen perustuvaan luetteloon käsittelytoimista.

(Tietosuojaryhmä WP248 2017)

Rekisterinpitäjän vastuulla on arvioida, tarvitaanko vaikutuksenarviointi niissä tilanteissa, joissa se ei lain mukaan ole pakollinen. Niinpä on suositeltavaa toteuttaa vaikutuksenarviointi myös epäselvissä tilanteissa varmistaakseen tietosuojalainsäädännön noudattaminen. (Hanninen, Laine, Rantala, Rusi, Varhela 2017., 117)

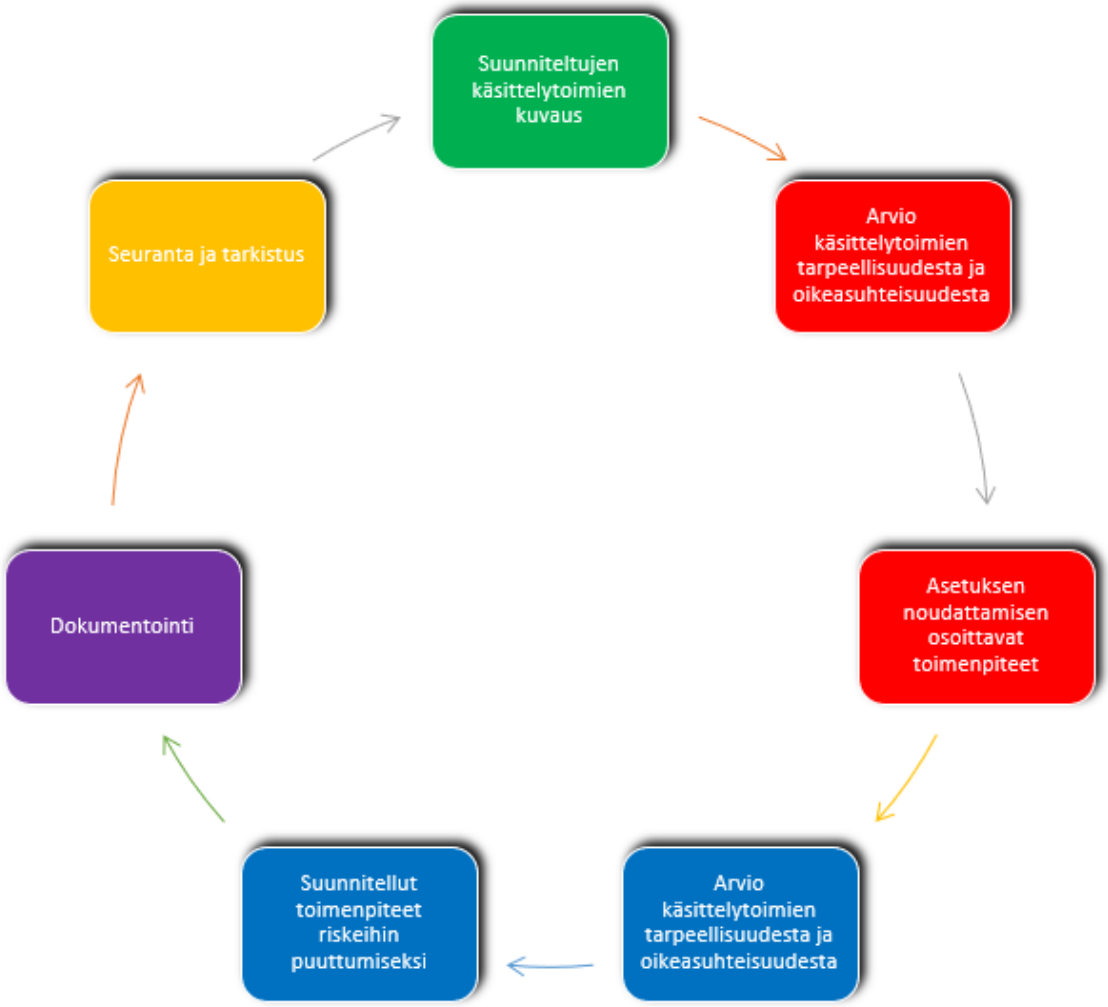
2.3.4 Vaikutustenarviointi käytännön työssä

EU:n tietosuoja-asetuksen 35 artiklan 7 kohdassa määritetään seuraavasti:

> 7. Arvioinnin on sisällettävä vähintään:
> a) järjestelmällinen kuvaus suunnitelluista käsittelytoimista, ja käsittelyn tarkoituksista, mukaan lukien tarvittaessa rekisterinpitäjän oikeutetut edut;
> b) arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden;
> c) arvio 1 kohdassa tarkoitetuista rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä; ja
> d) suunnitellut toimenpiteet riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että tätä asetusta on noudatettu ottaen huomioon rekisteröityjen ja muiden asianomaisten oikeudet ja oikeutetut edut.

(Tietosuoja-asetus 2016/679, artikla 35)

Vaikutustenarvioinnin on tarkoitus olla jatkuvaluonteinen prosessi, millä varmistetaan tietosuojan vaatimusten noudattaminen ja osoitetaan tarvittaessa myös niiden noudattaminen organisaatiossa. Riskien määrät käsittelyssä voi nousta erilaisin käytännön vaikutuksin kuten: uuden tekniikan käyttöönoton vaikutuksesta, automaattisen päätöksenteon kasvun tai syrjinnän vaikutuksesta. Riskien kasvaessa riskit vaativat uudelleen arviointia. Alla oleva WP29 työryhmän menettely prosessi kuvaa vaikutustenarvioinnin toistuvaa menettelyä.



KUVA 2. Iteratiivinen menettely tietosuojaa koskevan vaikutustenarvioinnin tekemiseksi. (Tietosuojaryhmä WP248 2017, 19)

Vaikutustenarvioinnin vaiheet:

1. Laaditaan järjestelmällinen kuvaus suunnitelluista käsittelytoimenpiteistä ja käsittelyn tarkoituksista.
2. Arvioidaan käsittelytoimien tarpeellisuus ja asianmukaisuus
3. Arvioidaan rekisteröityjen oikeuksiin ja vapauksiin liittyvät riskit
4. Suunnitellaan toimenpiteet, joilla riskeihin puututaan
5. Dokumentoidaan tulokset ja otetaan käytännön suorittamiseen ja seurataan ja analysoidaan saatuja tuloksia

Jos vaikutustenarvioinnissa todetaan käsittelyn aiheuttavan korkean riskin rekisteröidylle ja omilla toimenpiteillä koetaan riskin jäävän korkeaksi, voidaan toteuttaa ennakkokuuleminen. Ennakkokuulemisen toteuttaa tietosuojaviranomainen. Ennakkokuuleminen tapahtuu ennen henkilötietojen käsittelyn aloittamista. (Tietosuoja-asetus 2016/679, artikla 36; Hanninen ym. 2017, 128)

2.4 Tietoturvapolitiikka

Tiedon suojaaminen lähtee hyvin suunnitellusta tietoturvapolitiikasta. Tietoturvapolitiikka koostuu yrityksessä hyväksytyistä tietoturvaan ja tietosuojaan liittyvistä määräyksistä ja ohjeista. Tietoturvatoimintaa ohjaa EU:n direktiivit ja maassa hyväksytyt säädökset ja määräykset. Toiminnan kannalta tärkeimmät turvattavat asiat ovat: henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, palvelut, sekä tieto eri olomuodoissaan. Tavoitteena operatiivisten järjestelmien ja sisäisen tietoverkon toiminnan turvaaminen sekä tarvittavien palvelujen tuottaminen kaikissa tilanteissa.

Tietoturvapolitiikassa täytyy huomioida ainakin: keskeisten käsitteiden määrittely, tietoturvaperiaatteet, tietoturvavastuut, tietoturvallisuuden hallintajärjestelmä, tietoturvallisuuden toteutumista tukevat käytännöt, turvatoimien priorisointi, tietoturva- ja tietosuojakoulutus ja -ohjeet, tietoturvallisuuden toteutumisen valvonta, toiminta häiriötilanteissa ja poikkeusoloissa, tiedottaminen, tietoturvapolitiikan ajantasalla pitäminen ja oikeudet tehdä siihen tarvittavia muutoksia. (Opitietosuojaa.fi Noviisista Mestariksi 2019a.) Tietoturvan tavoitteet viestitään koko organisaatiolle. Tietoturvaan sisältyy käytännön toimenpiteet mitkä varmistavat tietojen eheyden, saatavuuden, oikeellisuuden ja luottamuksellisen säilyttämisen.

Taulukko 2. Tietoturvan periaatteet (Hanninen ym. 2017)

Termi	**Merkitys**
Luottamuksellisuus	- Tiedot vain oikeutettujen käytössä, muilla ei pääsyä tietoihin. - Yrityksen sisälläkin pääsy vain niillä, jotka joutuvat tietoja käsittelemään. - Tehokkaat salasanat, tiedostojen metatiedon poistaminen, tietojen salaaminen ja turvallinen hävittäminen.

Eheys	- Tiedon muuttumaton säilytys tiedon keruun, käsittelyn ja siirtämisen aikana. - Tiedon muuttumattomuus oikeudettomien toimesta tai tahattomasti niiden käsittelyn aikana. - Tarkistussummat, tarkistuskoodit ja digitaalinen allekirjoitus.
Käytettävyys	- Käsittelyyn oikeutetut henkilöt pääsevät tietoon käsiksi aina tarvittaessa. - Pääsy tietoihin kyetään palauttamaan nopeasti fyysisen tai teknisen vian sattuessa. - Tietojen varmistus, suojaaminen haittaohjelmien ja verkkohyökkäysten varalta, riittävä tiedonsiirtokapasiteetti.
Vikasietoisuus	- Tallennusratkaisujen tulee teknisesti olla sellaisia, jotka voivat vian sattuessa jatkaa toimintaansa. - Järjestelmän tulee selvitä vikaantumisesta itse ainakin niin pitkälle, että vika ei aiheuta lisää vikoja.

2.5 Tietosuojapolitiikka

Tietosuojalla varmistetaan henkilön yksityisyys, edut, oikeudet, vapaudet ja oikeusturva (Opitietosuojaa.fi Noviisista Mestariksi 2019b). Tavoitteena suojata henkilötiedot. EU:n tietosuoja-asetuksen myötä noudattaminen ei ainoastaan riitä vaan yrityksen on pystyttävä tarvittaessa myös todistamaan asetuksen seuraaminen kirjallisella tietosuojapolitiikalla (Hanninen ym. 2017, 51). Tietosuojapolitiikassa yrityksen tietosuojariskit ja toimintatavat on suunniteltu ja dokumentoitu.

Tietosuojapolitiikka on ylin tietosuojaa ohjaava dokumentti yrityksessä ja se täytyy olla kaikkien organisaatiossa olevien, yrityksen sidosryhmien ja kaikkien rekisteröityjen luettavissa. Tietosuojapolitiikan tarkoituksena on käyttäjien tiedottaminen, käyttäjistä kerätyistä tiedoista ja niiden käyttötavoista. Henkilötietojen käsittelyn tulee noudattaa voimassa olevaa lainsäädäntöä ja yrityksen tietosuojapolitiikkaa. Tietosuojapolitiikan tulee täyttää EU:n tietosuoja-asetuksen ja muun lainsäädännön vaatimukset. (Valtiovarainministeriö 2016a.)

3 EU:N YLEINEN TIETOSUOJA-ASETUS

Asetuksesta käytetään Suomessa yleisesti nimitystä tietosuoja-asetus, lyhenteenä GDPR (General Data Protection Regulation). Asetus koskettaa kaikkia rekisterinpitäjiä, jotka käsittelevät henkilödataa, sisältäen yrityksen työntekijöistä kerättyjä tietoja. Asetus on luotu erityisesti yksityisen ihmisen suojaksi.

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Tietosuojassa kyse on asiakkaan luottamuksesta ja koko organisaation tietosuojaosaamisesta eli asiakastietojen asianmukaisesti perustellusta ja oikeaoppisesta sujuvasta käsittelystä henkilötiedon elinkaaren eri vaiheissa. Henkilötietojen käsittelyvaiheita ovat esimerkiksi asiakastietojen kerääminen, tallentaminen, käyttö, yhdistäminen, siirto, luovuttaminen, säilyttäminen, hävittäminen ja kaikenlainen muu asiakastietojen käsittely. (Andreasson, Riikonen, Ylipartanen 2017, 19.)

3.1 Henkilötietodirektiivistä EU:n yleiseen tietosuoja-asetukseen

Tietosuojauudistuksen valmistelu alkoi 2009, hyväksyttiin huhtikuussa 2016 ja EU:n yleinen tietosuoja-asetus 2016/679 korvasi 25.5.2018 Suomessa aiemmin noudatetun henkilötietodirektiivin 95/46/EY (Working Party WP168 2009; Tietosuoja-asetus 2016/679). Aiemmin direktiivin noudattaminen oli sanktiojärjestelmän vähyyden tähden olematonta, koska noudattamatta jättämisen sanktiot olivat hyvin vähäiset. Eikä siitä käytännössä aiheutunut mitään organisaatiolle.

Perusperiaatteet direktiivin ja tietosuoja-asetuksen välillä ovat lähes samanlaiset, niinpä asetuksessa on voitukin yleissäännöksellä korvata viittaukset direktiivin ja asetuksen välillä. (Korpisaari, Pitkänen, Warma-Lehtinen 2018, 634-635.) Tietosuoja-asetuksen myötä koko EU:n alueelle muodostui yhtenäinen suoja ja yrityksille tasapuoliset toimintaedellytykset. Lisäksi mahdollistetaan henkilötietojen vapaa liikkuvuus ja kasvatetaan kuluttajien luottamusta. (Euroopan komissio 2018.)

3.1.1 Suomen oma tietosuojalaki

Tietosuoja-asetuksen voimaantulo edellytti henkilötietolainsäädännön tarkistamisen. Tarkastamisen tuloksena säädettiin uusi tietosuojalaki, henkilötietojen käsittelyn yleislaiksi. Hallituksen esitys annettiin eduskunnalle käsiteltäväksi 1.3.2018, se hyväksyttiin 13.11.2018. Tietosuoja-asetusta ei voida kokonaan

korvata kansallisella tietosuojalailla, mutta se antaa joissakin asioissa kansallista vapautta, tämän soveltaminen säädetään uudessa tietosuojalaissa. Tietosuojalaki (1050/2018) ja säädösmuutokset astuivat voimaan 1.1.2019. (Eduskunta 2018a.)

Uuden tietosuojadirektiivin käyttöönoton myötä korvautui 2008 annettu puitepäätös 2008/977/YOS rikosasioissa tehtävissä sekä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta (Euroopan unioni 2008). Eduskunta sai 5.4.2018 käsiteltäväksi hallitukselta lain henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä. Eduskunta hyväksyi esityksen 13.11.2018. Laki (1054/2018) ja muut siihen liittyvät säädökset astuivat voimaan 1.1.2019. (Eduskunta 2018a.; Finlex 2018a) EU:n tietosuoja-asetus rajaa henkilötietojen käsittelyn rikosasioissa asetuksen ulkopuolelle. (Finlex 2018b.) Lakiehdotukset hyväksyttiin hallintovaliokunnan mietintöjen HaVM 13/2018 ja HaVM 14/2018 mukaisina (Eduskunta 2018b; Eduskunta 2018c).

Eduskunnan hyväksymä uusi laki henkilötietojen käsittelystä panee täytäntöön rikosasioiden tietosuojadirektiivin, sisältäen säännökset rekisteröidyn oikeuksista sekä rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista. Rikosasioiden suojadirektiivin on tarkoitus helpottaa tietojen vapaata liikkuvuutta EU-maiden poliisi- ja oikeusviranomaisten välillä sekä varmistaa henkilötietojen suoja rikosasioita käsiteltäessä.

3.2 Asetuksen sisältö

Tietosuoja-asetus on muodostettu kahdesta eri osiosta: komission perustelut ja tausta asetukselle ja varsinainen lainsäädäntö. Asetus muodostuu luvuista, joissa on numeroituja artikloja. Artiklat on jaoteltu numeroituihin kohtiin, jotka voivat sisältää kirjaimin merkittyjä alakohtia.

3.3 Osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa

Osoitusvelvollisuus vaatii henkilötietojen säännösten mukaisen käsittelyn, lisäksi on kyettävä tarvittaessa osoittamaan sen noudattaminen. (Andreasson ym. 2019, 187) Tietoturvaloukkauksen sattuessa on kyettävä osoittamaan, että riskit on yritetty aktiivisesti tunnistamaan ja estämään. Säännösten noudatta-

matta jättäminen voi aiheuttaa maineen menettämisen lisäksi hallinnollisia seuraamuksia. Osoitusvelvollisuus edellyttää käytännössä myös dokumentointivelvollisuutta, toimenpiteiden toteutusta ja kirjaamista. (Andreasson ym. 2019, 176.)

Tietosuoja-asetuksessa mainittuja osoitusvelvollisuustoimenpiteitä ovat:

- seloste käsittelytoimista
- tietosuojan vaikutustenarviointi korkean riskin käsittelylle
- tietosuojavastaavan nimittäminen ainakin tiettyjen edellytysten täyttyessä
- oikeutettuun etuun perustuvan käsittelyn arviointi
- kyettävä osoittamaan rekisteröityneiden antamat suostumukset, kun käsittely perustuu suostumukseen
- henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle

(Tietosuojavaltuutetun toimisto 2018b)

Käsittelytoimien yhteydessä täytyy pystyä osoittamaan käsittelytoimien lainmukaisuus ja läpinäkyvyys, käyttötarkoituksenmukaisuus, tietojen minimointi, varmistuttava niiden säilytyksestä, täsmällisyydestä ja eheydestä ja varmistuttava tietojen luottamuksellisuudesta. Osoitusvelvollisuuden työkaluna voidaan käyttää tietotilinpäätöstä. (Tietosuojavaltuutetun toimisto 2018b.) Henkilötietojen käsittelyn prosessien määrittely kuuluu myös osana tietosuoja-asetuksen mukaista osoitusvelvollisuutta. Prosessien elinkaari muodostuu viidestä vaiheesta: tiedon luonnista, käytöstä, viittauksista, arkistoinnista ja tuhoamisesta. Systemaattisesti kuvattu elinkaari auttaa ymmärtämään milloin tieto on tarpeetonta ja se voidaan poistaa vaatimuksenmukaisesti. (Väre 2019, 51.)

3.3.1 Tietotilinpäätös

Tietosuoja-asetusta noudattaen organisaatioiden on tarvittaessa osoitettava vaatimuksien noudattaminen. Velvollisuudesta käytetään nimitystä osoitusvelvollisuus. Tietotilinpäätös toimii organisaation dynaamisena työkaluna ja lisää organisaation tehokkuutta, vaikuttavuutta ja kilpailukykyä. (Tietosuojavaltuutetun toimisto 2012.) Tietotilinpäätös on raportti, mikä syntyy organisaation sisäisen katselmuksen tuotoksena ja luo kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta ja tiedonhallinnan tilasta (Andreasson, Koivisto, Ylipartanen 2016, 145).

Tietotilinpäätös osoittaa EU:n tietosuoja-asetuksen mukaisen oikeaoppista tietojenkäsittelytavan noudattamista. Viranomaisten näkökulmasta se taas osoittaa viranomaisen toiminnan julkisuudesta annetun lain (621/1999) 18 §:ssä mukaisen tietohallintatavan noudattamista. Oikea tiedonhallintatapa vaatii, että käsiteltävän tiedon saatavuus, suoja ja sen laatu turvataan. Tietohallintalaissa (634/2011) tarkoitettua tietojärjestelmien yhteen toimivuutta voidaan myös tarkastella ja edistää tietotilinpäätöksen avulla. (Tietosuojavaltuutetun toimisto 2012.)

Tietotilinpäätöstä voidaan käyttää raportoitaessa organisaation sidosryhmille keskeisistä henkilötietojen käsittelyä koskevista asioista. (Andreasson ym. 2019, 57) Se toimii myös osana organisaation tietojohtamista sekä riskienhallintaa ja sisäistä valvontaa. (Tietosuojavaltuutetun toimisto 2012)

Tietotilinpäätöksen tarkoituksena on antaa kuvaus organisaation tietojen käsittelyn nykytilasta sekä arvio tietosuojan ja tietoturvan toteutumisesta. Tietotilinpäätöksessä arvioidaan myös tietojen käsittelyn kehittämistarpeet ja niiden vaatimat toimenpiteet. Johdolle tietotilinpäätös toimii niin toiminnan, tietosuojan suunnittelun, seurannan kuin kehittämisen työkaluna. (Tietosuojavaltuutetun toimisto 2012.)

Tietotilinpäätöksessä kuvataan organisaation tietovarannot, millainen on organisaation tietoarkkitehtuuri, hallittavien tietojen laatu ja niiden käytettävyys, millaisia menettelytapoja ja periaatteita tietojen käsittelyssä noudatetaan, miten hallittavat tiedot on suojattu ja miten niiden käyttöä valvotaan, kuinka rekisteröityjen oikeudet tietojen käsittelyssä toteutetaan. Tietotilinpäätös sisältää myös arvion organisaation tiedonhallinnan vahvuuksista ja heikkouksista. (Tietosuojavaltuutetun toimisto 2012.)

Tietotilinpäätös ohjaa organisaatiota systemaattisesti kriittisempään tietosuoja-asioiden tarkasteluun. Parhaimmillaan tietotilinpäätöksestä saa kuvan, että henkilötietojen käsittelyn valvonta on onnistunut niin lainsäädännön, määräysten kuin sisäisen ohjeistuksen mukaisesti. Tietotilinpäätös kuvaa myös tietojenkäsittelyn valvonnan kehittämiskohteet ja mahdolliset poikkeamat ja niihin reagoinnin. (Tietosuojavaltuutetun toimisto 2012.)

3.4 Tietosuoja-asetuksen tuomat muutokset

Tietosuoja-asetuksen lähestymistapa on riskiperusteinen, eli velvollisuudet kasvavat riskiasteen mukaisesti. (Andreasson ym. 2017, 30)

EU:n tietosuoja-asetuksen tuomat muutokset:

- Tietosuoja-asetuksen mukaiset käsitteet määritellään entistä tarkemmin, kuten suostumus.
- Henkilötietojen käsittelijöiden ja rekisterinpitäjien vastuut määritetään tarkemmin.
- Organisaation pitää pystyä noudattamisen lisäksi osoittamaan, että tietosuoja-asetuksen mukaiset säännökset on huomioitu rekisterinpitäjän toiminnassa.
- Organisaatioilla suurista tietoturvaloukkauksista ilmoitusvelvollisuus.
- Organisaatioilla tietyissä tilanteissa velvollisuus asettaa tietosuojavastaava.
- Rekisteröidyllä on oikeus saada itseään koskevat tiedot yleisesti käytössä olevassa koneluettavassa muodossa. Hänellä on oikeus siirtää kaikki antamansa tiedot toiseen järjestelmään, jos hän on itse antanut henkilötietonsa ja tietojen käsittely perustuu suostumukseen tai sopimukseen.
- Asetuksessa määritetään tietosuojaviranomaisen toimivallasta, tehtävistä ja valtuuksista. Jokaisen jäsenvaltion tietosuojaviranomainen on vastuussa oman jäsenvaltionsa alueella. Jäsenvaltioiden rajojen ylittävästä henkilötietojen käsittelystä on vastuussa yleensä rekisterinpitäjän päätoimipaikan tietosuojaviranomainen.
- EU:n jäsenvaltioiden tietosuojaviranomaisten yhteistyön apuna toimii yhdenmukaisuusmekanismi ja yhden luukun mekanismi. Tällä varmistetaan, että unionin tietosuojasääntelyä sovelletaan yhdenmukaisesti kaikissa jäsenvaltioissa ja että sen ratkaisukäytäntö säilyisi mahdollisimman yhdenmukaisena. Yhdenmukaisuusmekanismin keskeisenä toimijana on asetuksella perustettu Euroopan tietosuojaneuvosto (EDPB). Sen tehtävänä on antaa sitovia päätöksiä tietosuoja-asetuksen noudattamisesta.
- Valvontaviranomainen voi langettaa hallinnollisia seuraamuksia tietosuoja-asetuksessa säädetyistä teoista määräämällä sakkoja tiettyyn enimmäismäärään asti tapauksen olosuhteen huomioon ottaen. Sanktiot on jaettu kolmeen eri luokkaan.

(Andreasson ym. 2016, 33-34)

Tekniikan nopean kehittymisen takia muutoksia on myös tehty koneoppimisen osalta automaattiseen päätöksentekoon liittyen. Uutena asiana mukaan on tuotu vaatimus läpinäkyvyydestä henkilötietojen käsittelyssä (Korpisaari ym. 2018, 178). Myös asetuksen tuomat hallinnolliset sakot aikaisempaan oikeustilaan kuuluvat uusiin muutoksiin. Muutosten myötä valvontaviranomaisten valta kasvaa.

3.4.1 Rekisteröidyn oikeudet

Rekisteröityjen henkilöiden oikeuksia ovat:

- informoinnin läpinäkyvyys henkilötietojen käsittelystä,
- pääsy omiin henkilötietoihin,
- oikeus oikaista omia henkilötietojaan,
- oikeus omien henkilötietojen poistamiseen eli niin sanotusti tulla unohdetuksi,
- oikeus henkilötietojen käsittelyn rajoittamiseen,
- oikeus pyytää tiedot sellaisista henkilötietojen vastaanottajista, joille rekisterinpitäjän on ilmoitettava henkilötietojen oikaisuista, poistoista ja käsittelyn rajoituksista,
- oikeus siirtää henkilötiedot järjestelmästä toiseen
- vastustaa henkilötietojen käsittelyä sekä
- oikeus profiloinnin ja automaattisten päätöksien sijaan manuaaliseen ihmisen tekemiin päätöksiin.

(Hanninen ym. 2017, 56.)

Yrityksen täytyy toteuttaa yllä olevat oikeudet, joten on varmistettava, että tietojärjestelmät mahdollistavat oikeuksien toteutuksen, muuten tietojärjestelmiin on tehtävä muutoksia. Käsiteltäviin henkilötietoihin pitää aina olla laillinen peruste tai kohteen suostumus. Suostumus pitää voida todistaa ja suostumus on pyydettävä yksiselitteisesti ja painostamatta. Rekisteröidyn pyytäessä tietojensa siirtämistä rekisterinpitäjältä toiselle rekisteröidyn pitää saada tiedot vähintään jossain jäsennellyssä, yleisesti käytössä olevassa koneellisesti luettavassa muodossa kuten XML- tai JSON-tiedostona. (Hanninen ym. 2017, 64-65.)

Henkilön oikeuksiin sisältyy myös tiedonsaantioikeus. Vahti-raportti 1/2016 [s14] luetteloi asiat, joita rekisterinpitäjän tulee ilmoittaa rekisteröidylle tietoturvaloukkauksien ja muiden poikkeustilanteiden lisäksi.

Rekisteröidylle on tiedotettava:

- rekisterinpitäjän ja mahdollisen tietosuojavastaavan yhteystiedot
- käsittelyn tarkoitus, sen oikeusperusta ja henkilötietoryhmät
- kenelle tietoja on luovutettu
- mahdolliset kolmanteen maahan toteutetut siirrot ja siirtojen tietosuojan tilanne
- tietojensäilytysaika ja sen peruste

- rekisteröidyn oikeus tietojen oikaisuun sekä käsittelyn rajoittamiseen ja vastustamiseen.
- valitusoikeus valvontaviranomaiselle
- mahdollinen tieto tietojen perusteella tehtävästä automatisoidusta päätöksenteosta tai profiloinnista.
- mihin tietojen antamisen vaatimus perustuu, onko tietojen toimitus pakollinen ja seuraukset tietojen antamatta jättämisestä
- käytetyt oikeussuojakeinot
- tietojen alkuperä ja kerätyt tiedot, jos alkuperä muu kuin rekisteröity itse

(Valtiovarainministeriö 2016b)

Rekisteröidyllä on myös oikeus vaatia, että rekisteröityä koskevat päätökset tekee ihminen automaattisen profiloinnin sijaan (Tietosuojavaltuutetun toimisto 2018c).

3.4.2 Rekisterinpitäjä

Rekisterinpitäjä määrittää henkilötietojen käsittelyn tarkoitukset ja periaatteet. Rekisterinpitäjiä voi olla yksi tai useampia. (Korpisaari ym. 2018, 269.) Rekisterinpitäjä voi olla luonnollinen henkilö, oikeushenkilö tai julkishallinnon elin, jonka päätöksestä henkilötietoja käsitellään (Hanninen ym. 2017, 22). Rekisterinpitäjä on vastuussa tietosuojan vaatiman lainsäädännön noudattamisesta henkilötietoja käsiteltäessä. Rekisterinpitäjän täytyy varmistaa tietoturvan riittävä taso, organisaation henkilötietojen käsittelyn prosessien turvallisuus sekä rekisteröidyn mahdollisiin pyyntöihin vastaaminen, mikäli tietosuojavastaavaa ei ole organisaatiossa nimetty. (Korpisaari ym. 2018, 269.)

3.4.3 Henkilötietojen käsittelijä

Henkilötietojen käsittelijä on rekisterinpitäjän toimesta henkilötietoja käsittelevä taho. Tietosuoja-asetuksen artikla 28 mukaisesti henkilötietojen käsittelijän kuuluu noudattaa rekisterinpitäjän ohjeita ja dokumentaatiota henkilötietojen käsittelyssä. (Hanninen ym. 2017, 24.) Henkilötietojen käsittelijällä on kuitenkin oikeudellinen vastuu, joten käsittelijän täytyy myös itse varmistua, että käsittely vastaa EU:n tai jäsenvaltion lainsäädännön ehtoja. (Tietosuojavaltuutetun toimisto 2018d.)

Valtiovarainministeriön laatiman VAHTI-raportin mukaan tulisi lisäksi varmistaa, että henkilötietojen käsittelijä:

- Henkilötietojen käsittelijä käsittelee henkilötietoja vain rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti. Tähän kuuluu myös henkilötietojen käsittelyyn liittyvät sallitut tietojen siirrot ja sijainnit.
- Noudattaa tietosuoja-asetuksen mukaista salassapitovelvollisuutta.
- Noudattaa tietoturvallista henkilötietojen käsittelyä.
- Henkilötietojen käsittelyn ulkoistus vaatii rekisterinpitäjän kirjallisen ennakkosuostumuksen.
- Avustaa rekisterinpitäjää rekisteröidyn oikeuksien toteuttamisessa.
- Avustaa rekisterinpitäjää henkilötietojen käsittelyn tietoturvan toteuttamisessa, henkilötietojen tietoturvaloukkausten havaitsemisessa ja niistä ilmoittamisessa sekä vahinkojen minimoinnissa, vaikutustenarviointien tekemisessä ja valvontaviranomaisen ennakkokuulemisessa tietosuoja-asetuksen mukaisesti.

Tämä lisäksi organisaation tulee osana turvallisuussopimusta pohtia seuraavaa:

- Sitoutumista toimimaan niin että henkilötietojen käsittelyä toteuttavat vain sellaiset henkilöt, jotka ovat saaneet hyväksyttävän tuloksen turvallisuusselvityksessä, jos rekisterinpitäjällä on lainmukainen oikeus teettää turvallisuusselvityksiä ja jos rekisterinpitäjä selvitysten teettämistä käsittelijältä vaatii.

(Valtiovarainministeriö 2016b)

3.4.4 Henkilötietojen oikeudellinen peruste

Tietosuoja-asetuksen mukaisesti henkilötietojen käsittely on lainmukaista vain, jos käsittelylle on määritelty peruste. Henkilötietojen käsittelyyn voi soveltua samanaikaisesti useammat perusteet, yleisesti etu ja suostumus voivat tapahtua samanaikaisesti. Arkaluonteisten henkilötietojen käsittelyssä edellytetään myös jonkin erityisiä tietoryhmiä koskevan edellytyksen täyttymistä. (Hanninen ym. 2017, 29.)

Käsittelyedellytyksiä:

- rekisteröidyn suostumus
- rekisteröityä koskevan sopimuksen täyttyminen
- lakisääteinen velvoite
- yleinen etu
- julkisen vallan käyttö

- luonnollisen henkilön elintärkeiden etujen suojaaminen
- rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu

(Hanninen ym. 2017, 30-32)

Suostumuksessa rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn yhtä tai useampaa tarkoitusta varten. Suostumus on annettu vapaaehtoisesti, se on yksilöity ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy tietojensa käsittelyn ja jonka rekisterinpitäjän pitää pystyä myöhemminkin osoittamaan. Esimerkiksi verkkopalvelujen suostumuksen yhteydessä rekisteröityä on siis informoitava rekisterinpitäjän henkilöllisyydestä ja mihin henkilötietojen käsittelyn tarkoitukseen rekisteröity on myöntämässä suostumuksensa. (Hanninen ym. 2017, 30.)

Sopimusta käytetään tilanteissa, joissa rekisteröity on osapuolena sopimuksessa. Sopimuksen sisältö täytyy määritellä tarkasti koska sen pohjalta arvioidaan käsittelyn tarpeellisuus. Käsittely täytyy rajata välttämättömiin henkilötietoihin. Käsittelyperuste sisältää myös mahdolliset sopimusta edeltäneet henkilötietojen käsittelytoimet, jos ne on tehty rekisteröidyn omasta pyynnöstä, tilanne voi syntyä luottosopimuksen yhteydessä, kun luottokelpoisuutta arvioidaan. Sopimusta käytetään myös verkkokaupassa osoitteen käsittelyssä, työsopimusten yhteydessä ja palkan maksun yhteydessä. (Hanninen ym. 2017, 30.)

Lakisääteinen velvoite voi syntyä rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Lakisääteinen velvoite voi koskea yksityisellä tai julkisella sektorilla toimivaa rekisterinpitäjää. Lakisääteinen velvoite voi myös perustua Euroopan unionin tai jonkin sen jäsenvaltion lakiin. Lakisääteinen velvoite tulee vastaan esimerkiksi, kun työnantaja ilmoittaa työntekijänsä palkkatiedot veroviranomaisille tai kun osakeyhtiö pitää osakasluetteloa osakeyhtiölain perusteella. (Hanninen ym. 2017, 31.)

Kun yleinen etu tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen vaatii, henkilötietoja saa käsitellä ilman erillistä lupaa. Lupa perustuu lakiin tai muuhun oikeudellisiin säännöksiin. Myös näissä tilanteissa tietosuoja-asetuksen mukaiset rekisteröidyn oikeudet ovat voimassa, joten rekisteröidyllä olisi oikeus esimerkiksi poistaa tai vastustaa henkilötietojen käsittelyä. (Hanninen ym. 2017, 31.)

Kun kyse on elämästä ja kuolemasta tai uhkista, jotka voisivat aiheuttaa rekisteröidyn tai jonkun toisen loukkaantumiseen tai olla muutoin terveydelle vahingollisia voidaan käyttää käsittelyperusteena elintärkeiden etujen suojaamista. Tällaisia tilanteita ovat esimerkiksi humanitääriset hätätilanteet kuten luonnonkatastrofit tai epidemiat. (Hanninen ym. 2017, 31.)

Oikeutettujen etujen toteuttamiseksi voidaan myös sallia henkilötietojen käsittely, milloin etu katsotaan oikeutetuksi, selvitetään niin kutsutulla tasapainotestillä. Tällöin punnitaan rekisterinpitäjän tai kolmannen osapuolen intressiä rekisteröidyn intresseihin ja perusoikeuksia vasten. Oikeutetun edun täytyy myös olla lainmukainen, sen tulee olla selkeästi ilmaistu ja sen täytyy edustaa todellista ja välitöntä tarvetta eikä se saa olla spekulatiivinen.

Rekisteröidyn näkökulmasta käsittely ei saa olla ennakoimatonta ja odottamatonta. Rekisteröity voi myös vastustaa oikeudelliseen etuun perustuvaa henkilötietojen käsittelyä. Rekisteröidyn vastustaessa käsittelyä, täytyy käsittelyn tarve arvioida uudelleen. Tällöin oikeutetun edun nimissä henkilötietoja saa käsitellä vain, jos voidaan osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut ja oikeudet tai käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. (Hanninen ym. 2017, 32-33.)

Erityisen arkaluontoisen henkilötietoryhmien käsittely on lähtökohtaisesti kiellettyä, näitä voidaan käsitellä, jos perusteena on rekisteröidyn suostumus, rekisterinpitäjän velvoitteiden täyttäminen tai henkilöiden etujen suojelu (Hanninen ym. 2017, 40-41).

3.4.5 Tietosuojaperiaatteet

EU:n tietosuoja-asetus kattaa henkilötiedon koko elinkaaren.

EU:n yleisen tietosuoja-asetuksen 5 artiklan tietosuojaperiaatteita ovat:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus

(Tietosuoja-asetus 2016/679, artikla 5)

Rekisterinpitäjän velvollisuus on huolehdittava, että henkilötietojen käsittely noudattaa mainittuja tietosuojaperiaatteita. Rekisterinpitäjän täytyy siis ymmärtää mitä periaatteet tarkoittavat ja miten nämä toteutuvat yrityksen toiminnassa.

Yllä olevat 5 artiklan tietosuojaperiaatteet määrittävät yrityksen säilyttämälle henkilötiedoille ehtoja:

- Rekisteröidyllä on oikeus tietää hänestä tallennetut tiedot ja mitä seurauksia syntyy, jos hän ei halua luovuttaa kyseisiä tietoja.
- Yritys voi kerätä vain tietojenkäsittelyn toteuttamista varten tarpeelliset tiedot ja niiden säilytys vain, jos tietojenkäsittelyn toteuttaminen sen vaatii.
- Henkilötietoja kerätäkseen täytyy olla henkilön suostumus ja suostumus täytyy voida todentaa jälkikäteen.
- Virheelliset tiedot täytyy pystyä poistamaan nopeasti.
- Tiedot täytyy olla täsmällisiä ja niitä täytyy käsitellä luottamuksellisesti.

3.4.6 Tietosuojavastaava

Tietosuoja-asetuksessa on määritetty tietyt tilanteet, joissa rekisterinpitäjän ja henkilötietojen käsittelijän edellytetään nimeävän tietosuojavastaava. Konsernien kohdalla voidaan toimia niin että, nimetään vain yksi tietosuojavastaava, jos hän on helposti saatavilla jokaiselle toimipaikalle. Tietosuojavastaava voidaan nimetä organisaatiossa myös tilanteissa, joissa sitä ei edellytetä tietosuoja-asetuksen mukaisesti. (Hanninen ym. 2017, 121.)

Artikla 37 Tietosuojavastaavan nimittäminen:

1. Rekisterinpitäjän ja henkilötietojen käsittelijän on nimettävä tietosuojavastaava aina kun

a) tietojenkäsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään hoitava tuomioistuin;
b) rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka luonteensa, laajuutensa ja/tai tarkoituksensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa; tai
c) rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu artikla 9 mukaisiin erityisiin henkilötietoryhmiin ja artiklassa 10 tarkoitettuihin rikostuomiota tai rikkomuksia koskeviin tietoihin.

(Tietosuoja-asetus 2016/679, artikla 37)

Tietosuojavastaavalta oletetaan ammattipätevyyttä, asiantuntemusta tietosuojalainsäädännöstä ja -käytänteistä sekä valmiuksia selviytyä määrätyistä tehtävistä. Varsinaista tietosuojavastaavan koulutusta tai aiempaa kokemusta tehtävistä ei odoteta. (Hanninen ym. 2017, 121.) Tietosuojavastaavan tehtäviin kuuluvat: asetuksen noudattamisen seuraaminen ja puutteisiin reagointi, tiedonanto tietosuojasäännösten velvollisuuksista johdolle ja tietojenkäsittelijöille, antaa tietoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa vaikutustenarvioinnin toteutusta, toimia rekisteröityjen yhteyshenkilönä henkilötietojen käsittelyyn liittyen ja yhteistyö valvontaviranomaisten kanssa.

Myös rekisterinpitäjä voi antaa tietosuojavastaavalle tehtäviä kuten: avustaa täyttyykö vaikutustenarvioinnin tekemisen edellytykset ja mitä menetelmiä tämän toteuttamiseksi olisi noudatettava, tehdäänkö vaikutustenarviointi itse vai haetaanko toteutukseen apuja organisaation ulkopuolelta, riittävien suojatoimien ja tietoturvavaatimusten määrittely organisaatiolle, tarkistaa onko toteutettu vaikutustenarviointi ja sen tuottamat johtopäätökset asetuksen mukaiset. (Korpisaari ym. 2018, 367-368.)

Tietosuojavastaava on salassapitovelvollinen kaikissa tehtävissään ja hän ei ole vastuussa tietosuoja-asetuksen mukaisten velvollisuuksien noudattamisesta yrityksessä. Henkilötietojen käsittelijän ja rekisterinpitäjän vastuisiin kuuluu tietosuoja-asetuksen noudattaminen ja yrityksen johdon täytyy huolehtia, että yritys noudattaa tietosuoja-asetusta ja pystyä myös osoittamaan yrityksen näin toimivan. Kansallinen valvontaviranomainen ylläpitää keskitetty listaa asetuksen mukaisista tietosuojavastaavista. Tietosuojavastaavan kuuluukin ilmoittaa yhteystietonsa valvontaviranomaiselle, tietoja käytetään keskinäiseen tiedottamiseen ja asiointiin. (Korpisaari ym. 2018, 368.)

3.4.7 IT-järjestelmien muutokset

Tietosuoja-asetuksen noudattaminen saattaa aiheuttaa myös muutoksia organisaatioiden IT-järjestelmiin. Yrityksen verkkosivuilla käytetään erilaisia tapoja, joilla kerätään henkilötietoja mahdollisen sisäänkirjautumisen, verkkokauppaostosten ja postituslistojen myötä. Näistä muodostuu yritykselle henkilörekistereitä, jotka vaativat tietosuoja-asetuksen mukaisen toiminnan. Nämä vaativat yritykseltä asianmukaista henkilötietojen käsittelyä, tietoturvan tasoa ja dokumentointia. Henkilötietojen täytyy olla asianmukaisesti kerättyjä, joten sivusto vaatii riittävän informoinnin rekisteröityvälle.

Tietosuoja-asetus vaatii järjestelmän kehitysvaiheessa (Privacy by default and design) periaatteet noudattavaa suunnittelua, mikä tarkoittaa yksityisyyden suojaamisen oletusarvoa kehitysvaiheessa. Käytännössä tämä tarkoittaa tietosuojan ja yksityisyyden huomiointia ennakoivasti suunnittelu ja kehitysvaiheessa ja koko sovelluksen elinkaaren ajan. (Korpisaari ym. 2018, 277.)

Privacy by design – käsitteen seitsemän periaatetta:

1. *Proaktiivista, ei reaktiivista; ennaltaehkäisevää, ei hoitavaa*: tietosuoja tulee ottaa huomioon ennakoivasti, riskit pyritään tunnistamaan etukäteen ja vahinkojen jälkikäteisen korjailun sijaan yksityisyyden loukkaukset ja muut tietosuojariskit ennaltaehkäistään.
2. *Tietosuoja oletusasetuksena*: käyttäjän ei tarvitse tehdä mitään suojatakseen yksityisyytensä – yksityisyyden suoja on oletusarvona sisäänrakennettu järjestelmään. Sisäänrakennettu yksityisyys pyrkii tuottamaan mahdollisimman hyvän yksityisyyden suojan varmistamalla että henkilötiedot on automaattisesti suojattu missä tahansa tietojärjestelmässä ja millä tahansa toimintatavalla.
3. *Yksityisyys sisällytettynä suunnitteluun*: palvelut suunnitellaan niin, että tietosuoja on luonnollinen ja keskeinen osa järjestelmää heikentämättä sen toiminnallisuutta.
4. *Täysi toiminnallisuus; lisäarvoa eikä nollasummapeliä*: kaikki oikeutetut tavoitteet pyritään saavuttamaan ilman että tarpeettomia kompromisseja tarvitsee tehdä. Vältetään harhaanjohtavia vastakkainasetteluja, kuten yksityisyys vastaan turvallisuus, osoittamalla, että molemmat voidaan saavuttaa.
5. *Päästä-päähän-turvallisuus; koko elinkaaren suoja*: yksityisyyden suoja ja tietoturva varmistetaan koko henkilötietojen elinkaaren ajan alkaen ennen kuin ensimmäistäkään tiedon murusta on vielä tuotu järjestelmään ja jatkuen siihen asti, että tiedot varmasti tuhotaan, kun niitä ei enää tarvita.
6. *Näkyvyys, läpinäkyvyys ja avoimuus*: tietosuojaan liittyvien käytäntöjen ja prosessien tulla olla dokumentoituja, läpinäkyviä ja kaikkien osapuolten saatavilla tarvittaessa.
7. *Yksityisyyden kunnioitus ja käyttäjäkeskeisyys*: yksilön tarpeet on ennen kaikkea pidettävä päällimmäisinä. Tietosuoja on suunniteltava käyttäjälähtöisesti. Käyttäjillä on oltava riittävästi vaihtoehtoja tietosuoja-asetuksissa, oletusasetukset kunnioittavat yksityisyyttä, ja järjestelmä tarjoaa riittävästi tietoa käyttäjälle.

(Korpisaari ym. 2018, 277-278)

Tietosuojaa parantaakseen voidaan käyttää yksityisyyden suojaa edistäviä tekniikoita kuten pseudonymisointia ja erilaisia kryptografisia salausmenetelmiä (Korpisaari ym. 2018, 278). Lisäksi tietosuoja-asetuksen (2016/679) artikla 25 ja johdanto-osan kohta 78 mukaisesti tietosuojan periaatteet on huomioitava myös julkisten tarjouskilpailujen yhteydessä, ei siis riitä pelkästään, että tietosuoja periaatteet huomioidaan ohjelmistokehityksen eri vaiheissa.

Perus 78 EU yleinen tietosuoja-asetus:

> (78) Luonnollisten henkilöiden oikeuksien ja vapauksien suoja henkilötietojen käsittelyssä edellyttää, että toteutetaan asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että asetuksessa säädetyt vaatimukset täyttyvät. Jotta voidaan osoittaa, että asetusta on noudatettu, rekisterinpitäjän olisi hyväksyttävä sisäisiä menettelyjä ja toteutettava toimenpiteet, jotka vastaavat erityisesti sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita. Tällaisia toimenpiteitä voisivat olla muun muassa henkilötietojen käsittelyn minimointi, henkilötietojen pseudonymisointi mahdollisimman pian, tehtävien ja henkilötietojen käsittelyn läpinäkyvyys, sen mahdollistaminen, että rekisteröity voi valvoa tietojenkäsittelyä ja että rekisterinpitäjä voi luoda ja parantaa turvaominaisuuksia. Kehitettäessä, suunniteltaessa, valittaessa ja käytettäessä sovelluksia, palveluja ja tuotteita, jotka perustuvat henkilötietojen käsittelyyn tai käsittelevät henkilötietoja tehtävänsä täyttämiseksi, tuotteiden, palvelujen ja sovellusten tuottajia olisi kannustettava ottamaan huomioon oikeus tietosuojaan niiden kehittäessä ja suunnitellessa tällaisia tuotteita, palveluja ja sovelluksia ja varmistamaan uusin tekniikka asianmukaisesti huomioon ottaen, että rekisterinpitäjät ja henkilötietojen käsittelijät pystyvät täyttämään tietosuojavelvoitteensa. Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet olisi myös huomioitava julkisten tarjouskilpailujen yhteydessä.

(Tietosuoja-asetus 2016/679, kohta 78)

Rekisteröidyn oikeuksien mukaisesti rekisteröidyllä on myös oikeus pyytää ja saada rekisterinpitäjälle luovuttamansa henkilötiedot jäsennellyssä, koneellisesti luettavassa muodossa, tiedostojen siirtomahdollisuus olisi siis hyvä huomioida kehitettävässä järjestelmässä, kun henkilötietojen oikeus perustuu suostumukseen tai sopimuksen täytäntöönpanoon.

3.5 Pseudoanonymisointi ja anonymisointi

Pseudonymisoinnissa henkilötietoja käsitellään niin, että henkilötietoja ei voida yhdistää tiettyyn henkilöön ilman lisätietoja, kuitenkin yksilö voidaan erottaa tietojoukosta ja tarvittaessa yhdistää lisätietojen avulla henkilön muihin tietoihin. Pseudonymisoitujen henkilötietojen käsittelyssä sovelletaan henkilötietojen käsittelyn tietosuojasäännöksiä. Pseudonymisoinnilla voidaan vähentää rekisteröityihin kohdistuvia riskejä, jolloin se toimii suojausmenetelmänä ja auttaa noudattamaan tietosuojavelvoitetta. (Korpisaari ym. 2018, 64.)

Anonymisoinnissa henkilötietoja käsitellään niin, että henkilötietoja ei voida enää tunnistaa niistä eikä tunnistamista voida enää palauttaa hallussa olevilla tiedoilla tunnistettavaksi. Anonymisoituja tietoja ei tunnisteta henkilötiedoiksi eikä silloin myöskään sovelleta tietosuoja-asetuksen mukaisia tietosuojasäännöksiä. Aina henkilötietoja ei välttämättä voida anonymisoida kokonaan (yksilökohtaiset harvinaiset

henkilötiedot, kuten tietyt sairaudet) tällöin tietosuojasäännöksiä täytyy noudattaa. (Korpisaari ym. 2018, 612.) Anonymisoinnissa ei välttämättä riitä pelkästään tunnistetietojen poistaminen, koska henkilö ei saa olla tunnistettavissa edes saatavia tietoja yhdistelemällä (Pitkänen, Tiilikka, Warma 2013, 231).

3.6 Henkilötietojen siirto EU:n ulkopuolelle

Tietosuoja-asetuksessa (2016/679) määrittää henkilötietoja siirtäessä Euroopan talousalueen (ETA) ulkopuolelle, että kohdemaassa täytyy varmistaa asianmukainen ja turvallinen henkilötietojen käsittely. Ilman erillistä lupaa tietoja voidaan siirtää toiseen maahan vain, jos Euroopan komissio on arvioinut kyseisen maan pystyvän turvaamaan tietosuojan vaatiman tason lainsäädännöllisesti ja hallinnollisesti. (Tietosuoja-asetus 2016/679.)

Artikla 44 Siirtoja koskeva yleinen periaate:

> Sellaisten henkilötietojen siirto, joita käsitellään tai joita on tarkoitus käsitellä kolmanteen maahan tai kansainväliselle järjestölle siirtämisen jälkeen, toteutetaan vain jos rekisterinpitäjä ja henkilötietojen käsittelijä noudattavat tässä luvussa vahvistettuja edellytyksiä ja ellei tämän asetuksen muista säännöksistä muuta johdu; tämä koskee myös henkilötietojen siirtämistä edelleen kolmannesta maasta tai kansainvälisestä järjestöstä toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle. Kaikkia tämän luvun säännöksiä on sovellettava, jotta varmistetaan, että tällä asetuksella taattua luonnollisten henkilöiden henkilötietojen suojan tasoa ei vaaranneta.

(Tietosuoja-asetus 2016/679, artikla 44)

Vuonna 2016 Euroopan unioni ja Yhdysvallat sopivat Yhdysvaltojen kauppaministeriön valvomasta ohjelmasta nimeltä Privacy Shield. Henkilötietojen siirtäminen Yhdysvaltoihin on sallittua vain, jos tiedot vastaanottava yritys on Privacy Shield järjestelmässä mukana. Järjestelmässä on sovittu säännöistä, joilla unionista vastaanotettuja henkilötietoja täytyy käsitellä. Liittyessä järjestelmään yritys sitoutuu noudattamaan sovittuja ehtoja henkilötietojen käsittelyssä. (Korpisaari ym. 2018, 401-402.; Privacy Shield 2020.)

Kun kumppanin toiminta on riittävän suojattua ja rekisteröidylle tarjotaan tietosuojan mukainen riittävä oikeussuoja, voidaan henkilötiedot siirtää muihin maihin ilman erillistä lupaa. Käytännössä tämä, mahdollistuu kun rekisterinpitäjän ja ulkomaisen toimijan välisiin sopimuksiin sisällytetään Euroopan komission hyväksymät tietosuojaa koskevat vakiolausekkeet. Siirrot ovat mahdollisia ilman lupaa myös

monikansallisilla yrityksillä, kun yritys on laatinut tietyt vaatimukset täyttävät ja kaikkia yksiköitä sitovat säännöt. (Hanninen ym. 2017, 101-105.)

3.6.1 Pilvipalvelut

Pilvipalvelujen käyttö yrityksissä kasvaa, tällöin yrityksen käyttämät palvelut, ohjelmat ja tiedot sijaitsevat palveluntarjoajan palvelimella. Yleisimpiä pilvipalveluita ovat sähköiset kalenterit, sähköpostit, säilytys- ja jakopalvelut ja pikaviestimet kuten Google Calendar, Google Drive, Google Mail, Skype, Slack, Office 365, OneDrive ja muut vastaavat palvelut. Palvelut voivat sijaita eri maissa kuin niitä käyttävä yritys. Pilvipalveluiden käytetyimmät tyypit ovat IaaS, CaaS, PaaS, FaaS ja SaaS palvelut.

IaaS lyhenne muodostuu sanoista ”Infrastructure as a Service” ja tarkoittaa palveluna tarjottua infrastruktuuria. Palveluntarjoaja tarjoaa tyypillisesti asiakkaan käyttöön verkkoselaimen kautta hallintaliittymän, minkä kautta pystytään perustamaan halutut palvelimet sekä hallinnoida näiden kapasiteettia, verkkoyhteyksiä ja palomuurauksia. Palveluntarjoajan vastuulle jää vain alustat, joita käytetään kapasiteetin tarjoamiseen. Palvelunkäyttäjän vastuulla on palvelimet, niiden konfiguraatiot ja hallinnointi ja kaikki mitä näissä palvelimissa pyöritetään. (Watts, Raza 2019.; Planeetta 2016.)

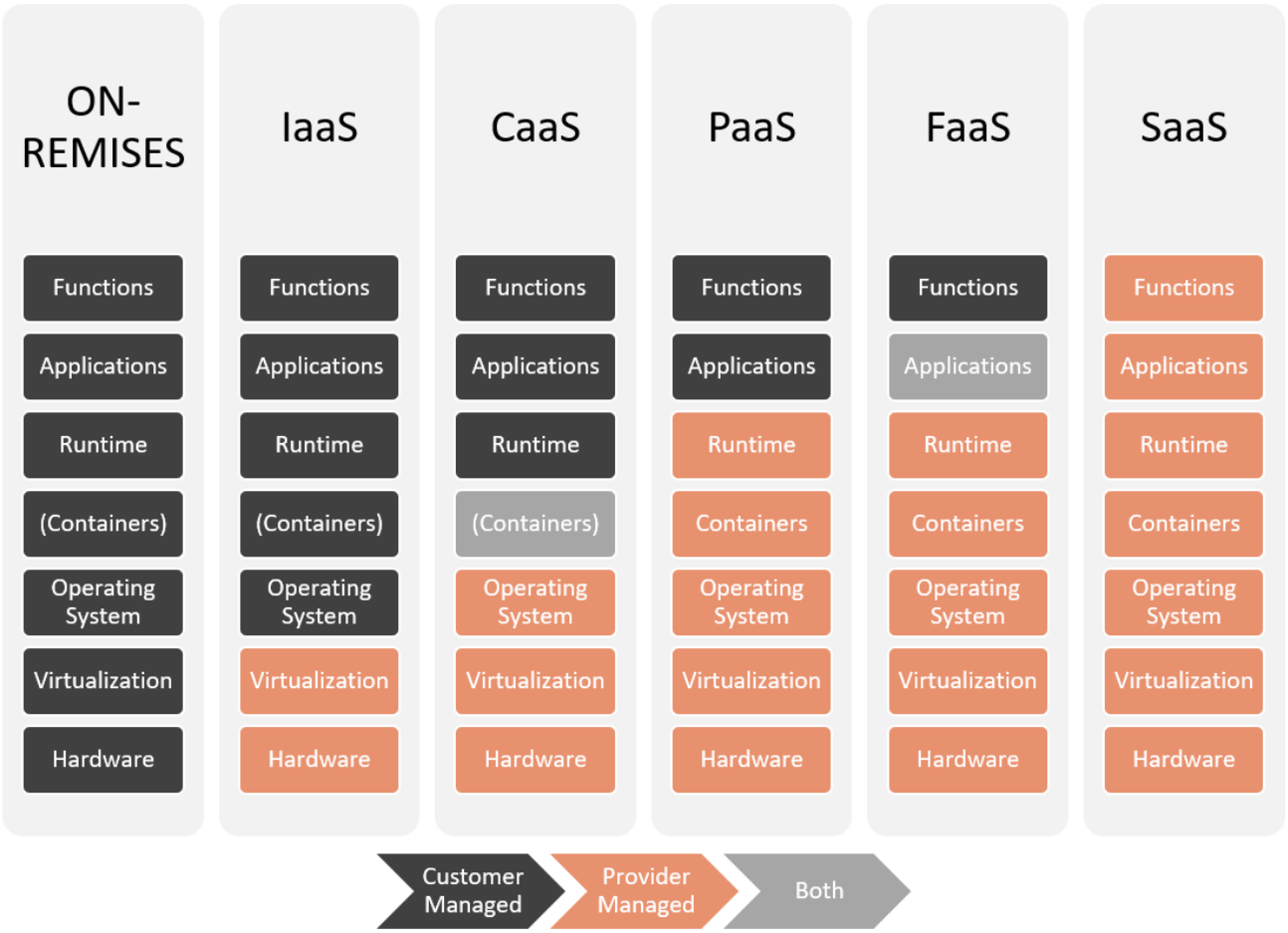
Caas lyhenne muodostuu sanoista ”Containers as a Service” ja tarkoittaa konttipalvelujen tarjoamista palveluna. Caas palvelut kuuluvat infrastruktuurin perusteella IaaS ja PaaS palveluiden väliin. Palveluntarjojan vastuulle kuuluu alustojen lisäksi käyttöjärjestelmän ja konttien hallinta. Palvelua käyttävän vastuulle jää konttien ja ajoympäristön hallinnan lisäksi oman ohjelmistonsa tietoturva. (Vento 2020.; Onrego oy.)

PaaS lyhenne muodostuu sanoista ”Platform as a Service” ja tarkoittaa palveluna tarjottua sovellusalustaa. Palveluntarjoaja tarjoaa usein verkkoselaimen kautta tapahtuvan yhteyden lisäksi muita tapoja muodostaa yhteyksiä palveluihin. Näitä voivat olla suorat yhteydet palvelimiin (FTP/SFTP, SSH), komentorivityökalut (CLI) ja API-rajapinta. Alustoja tarjotaan usein ohjelmistokehityksen tarpeisiin. Palveluntarjoajan vastuulle kuuluu käyttöjärjestelmä- ja perusasennettujen ohjelmistojen turvallisuus. Palvelua käyttävän yrityksen vastuulle jää oman asennetun ohjelmistonsa tietoturva. (Watts ym. 2019.; Planeetta 2016.)

FaaS lyhenne muodostuu sanoista ”Functions as a Service” ja tarkoittaa palveluna tarjottua funktioiden ajoalustaa. Yleisesti puhutaan tällöin serverless-arkkitehtuurista. Palveluntarjoajan vastuulla on resurssien allokointi. Palvelua käytetään yleisesti erilaisten ajastettujen skriptien suorittamiseen. Palvelunkäyttäjä maksaa vain käytetystä laskenta-ajasta. (Vento 2020.; Onrego oy.)

SaaS lyhenne muodostuu sanoista ”Software as a Service” ja tarkoittaa pilvessä sijaitsevaa ohjelmistoa kuten sähköpostia, mitä ylläpidetään palveluntarjoajan puolesta. Palvelun tarjonta voi tapahtua verkkoselaimen kautta, applikaationa tai näiden hybridinä. Palvelun vastuu on kokonaan palveluntuottajan vastuulla. (Watts, ym. 2019.; Planeetta 2016.)

Pilvipalveluita pidetäänkin tietoturvan suurimpina haasteina (Check Point Security Report 2019). Pilvipalvelujen osalta kannattaakin varmistaa voiko palvelussa määrätä tietojen maantieteellisen sijainnin.



KUVA 3. Asiakkaan ja palveluntarjoajan vastuut pilvipalveluissa. (Vento 2020.; Onrego oy.)

3.7 Tietomurtojen ja tietoturvaloukkausten käsittely

Tietosuojan tuoma ilmoitusvelvollisuus rajoittuu vain henkilötietoja koskeviin tietoturvaloukkauksiin, tämä vaikuttaa arviointiin onko organisaatiolla tarvetta tehdä ilmoitus tietosuojavaltuutetulle, mahdollisesti rekisteröidylle itselleen vai tehdäänkö mahdollinen ilmoitus Liikenne- ja viestintäviraston Traficomin Kyberturvallisuuskeskukselle ja rikostapauksessa poliisille. Mikäli tietoturvaloukkaus koskettaa henkilötietoja on tapahtunut tietosuojaloukkaus, tällöin on arvioitava loukkauksen mahdollisesti aiheuttaman vahingon suuruus ja tämän perusteella ilmoitettava tietosuojavaltuutetulle ja mahdollisesti rekisteröidyille. Tietosuojaloukkauksen tapahtuessa henkilötietoja häviää järjestelmästä, tiedot muuttuvat, niitä luovutetaan luvattomasti, tiedot tuhoutuvat kokonaan tai niihin pääsee käsiksi ulkopuolinen taho. (Andreasson ym. 2019, 171-172.; Korpisaari ym. 2018, 324-326.)

Tietosuojaloukkauksen havaintohetkestä on tietosuoja-asetuksen mukaisesti 72 tuntia aikaa ilmoittaa tietosuojavaltuutetulle. Jos tietoturvaloukkauksen arvioidaan aiheuttavan rekisteröidylle riskin henkilön oikeuksille ja vapauksille, ilmoitus täytyy aina tehdä. Rekisteröidylle aiheutuvasta riskistä on ilmoitettava myös rekisteröidylle viivyttelemättä. Ilmoituksen on tapahduttava selkeästi ja ymmärrettävästi. Samassa yhteydessä annetaan tietosuojavastaavan nimi, yhteystiedot mistä saa tapahtuneesta lisätietoja, mahdolliset seuraukset ja ehdotetut tai jo toteutetut toimenpiteet, joilla jatkossa estetään vastaava. Lisäksi mahdollisesti toimenpiteet, joilla voidaan lieventää tapahtuneen haittavaikutuksia. Epävarmoissa tilanteissa yritys saa neuvoja Tietosuojavaltuutetun toimistosta selvittääkseen miten loukkauksen kanssa toimitaan. (Andreasson ym. 2019, 171-172.; Korpisaari ym. 2018, 324-326.)

Tietosuoja-asetuksen 34 artiklan 3 kohdan alakohtien mukaisesti:

> 3. Edellä 1 kohdassa tarkoitettua ilmoitusta rekisteröidylle ei vaadita, jos jokin seuraavista edellytyksistä täyttyy:
> a) rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta;
> b) rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että 1 kohdassa tarkoitettu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu;
> c) se vaatisi kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla.

(Tietosuoja-asetus 2016/679, artikla 34)

Tietoturvaloukkauksen yhteydessä ei riitä, että tilanteesta on ilmoitettu vaan rekisterinpitäjän täytyy dokumentoida kaikki henkilötietojen tietoturvaloukkaukset. On myös pystyttävä osoittamaan niiden vaikutukset, analysoida tilanne, suunnitella ja toteuttaa korjaavat toimet, joilla vastaavat tilanteet estetään jatkossa. Dokumentoinnin perusteella valvontaviranomainen voi myös tarkistaa yrityksen noudattaneen tietosuoja-asetuksen velvollisuuksia. (Korpisaari ym. 2018, 321.)

3.8 Hallinnolliset sakot

Tietosuoja-asetus (EU 2016/679, artikla 83) määrittää hallinnollisten sakkojen enimmäismäärän, joka voi olla suurimmillaan perustavanlaatuisesta velvoitteiden rikkomuksesta 20 miljoonaa euroa tai neljä prosenttia yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta ja muiden tietosuoja-asetuksessa asetettujen velvoitteiden rikkomisesta hallinnollisten sakkojen enimmäismäärä on 10 miljoonaa euroa tai kaksi prosenttia yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta (Tietosuoja-asetus 2016/679, artikla 83). Ennakolta seuraamusten ankaruus sai asetuksen osalta eniten huomiota, toisaalta tämä toimi varmasti hyvänä liikkeellepanijana organisaatioissa. Jälkeenpäin on kuitenkin tarkentunut, että korkeita sanktioita ei käytetä kuin poikkeuksellisissa tilanteissa.

Hallinnollista sakkoa määrätessään viranomainen kiinnittää huomion seuraavien säännösten rikkomiseen:

- käsittelyn luonteeseen
- sen vakavuuteen ja kestoon
- säännösten rikkomisen tahallisuuteen
- aiheutuneen vahingon lieventämiseksi toteutettuihin toimiin
- vastuun tasoon
- mahdollisiin vastaavanlaisiin aiempiin rikkomisiin
- tapaan, kuinka säännösten rikkominen selvisi valvontaviranomaiselle (esimerkiksi, ilmoittiko rekisterinpitäjä tai henkilötietojen käsittelijä tapahtumasta ja sen laajuudesta)
- rekisterinpitäjälle tai henkilötietojen käsittelijälle annettujen toimenpiteiden noudattamiseen
- käytännesääntöjen noudattamiseen ja
- mahdollisiin muihin raskauttaviin tai lieventäviin tekijöihin.

(Korpisaari ym. 2018, 537-538)

Perustavanlaatuisiin velvoitteisiin kuuluvat: käsittelyn perusperiaatteet, rekisteröityjen oikeudet, tietojen siirto EU:n ulkopuolelle ja valvontaviranomaisen antaman määräyksen noudattamatta jättäminen tai valvontaviranomaisen pääsyn estäminen henkilötietoihin tai yrityksen tiloihin (Hanninen ym. 2017, 124). Tietosuoja-asetuksen mukaan vähäisestä rikkomuksesta riittää huomautus (Oikeusministeriö 2018).

4 EMPIIRISEN TUTKIMUKSEN TOTEUTUS

Luvussa käsitellään empiirisen tutkimuksen taustat ja tavoitteet. Tämän jälkeen tutustutaan toteutukseen ja kyselyyn osallistuvien valintaan. Lopuksi käsitellään tutkimusmenetelmät ja toimeksiantajayritys.

4.1 Tutkimuksen tavoite

Tutkimuksen tavoitteena oli kartoittaa kyselyllä ja haastatteluilla yrityksen työntekijöiden ymmärrystä EU:n tietosuoja-asetuksesta sen voimaantulon jälkeen. Asetus tuli voimaan 25.5.2018 ja tutkimus toteutettiin helmikuussa 2020 noin parin vuoden voimassaolon jälkeen. Lisäksi tutkimuksesta saatua tietoa on tarkoitus käyttää yrityksen jatkokehitystoimissa niin tietoturvan kuin asetuksen noudattamisen osalta. Tutkimuksessa selvitin myös työntekijöiden tuntemuksia tietosuoja-asetuksen tuomista mahdollisista muutoksista heidän omassa työssään ja yrityksen toiminnassa. Myös koulutustarvetta selvitettiin.

4.2 Tutkimusmenetelmän valinta

Tutkimusmenetelmäksi valikoitui laadullinen tapaustutkimus toimeksiantajayrityksen henkilöstön näkökulmasta. Laadullisen tutkimuksen pääpiirteisiin kuuluvat tutkittavien näkökulman tärkeys ja tutkijoiden omat havainnot määritetyssä kontekstissa ja haastattelun tärkeys ja tutkimukseen osallistuvien tarkoituksenmukainen valinta (Lappalainen, Auno 2018). Kyselynä tapahtuvan datan toteutustavaksi valikoitui kvalitatiivinen tutkimus, koska on tarkoitus vain kartoittaa aineistoa ja analysoida sitä. Kyselyn pääteemana oli tietosuoja-asetus. Kvalitatiivisessa tutkimuksessa pyritään selvittämään tutkittavan kohteen laatua ja ominaisuuksia, kuten tässä tapauksessa sitä miten tietosuoja-asetus ja siihen liittyvät asiat on sisäistetty kohdeyrityksessä. Kvalitatiivisen tutkimuksen piirteisiin kuuluu myös, että tutkimukseen osallistuvat henkilöt valitaan heidän kokemuksensa perusteella, kuten tässä tapauksessa eri tehtävissä toimimisen kautta.

Kyselyn materiaali hankittiin osin strukturoidulla lomakehaastattelulla osin puolistrukturoiduilla osioilla. Strukturoitu kysely sisältää samat kysymykset kaikille samassa järjestyksessä sisältäen vain valmiita vastausvaihtoehtoja. (Lappalainen ym. 2018) Näin toteutettiin osa kyselyn aiheista ja jokaisen aihealueen alkuosan kysymykset. Puolistrukturoidun kysely eroaa niin että kysymykset ovat kaikille samat

mutta valmiita vastausvaihtoehtoja ei ole kuten kyselyn aiheiden loppuosiot. Haastattelu toteutettiin teemahaastatteluna, eli haastattelun aihepiirit oli etukäteen määritelty ja haastatteluissa kysymysten järjestys ja laajuus vaihteli haastatteluiden välillä. Laadullisen datan analysointiin käytettiin määrällisiä menetelmiä (prosenttijakaumat).

4.3 Kysely tutkimuksen toteutus

Toimin yrityksessä tietoturvavastaavana ja yrityksen ”Tietoturva ja turvallisuuspalvelu (ASA)”-ryhmän toisena henkilönä, joten kysely auttaa jatkossa myös työtehtävissäni. Tutkimuksen toteutuksen aloitin miettimällä pääaiheet mistä tarvitsin lisätietoa muulta henkilökunnalta. Pääaiheiksi valikoitui: 1. Tietoturva, 2. Tietosuojakäytännöt, 3. Pilvipalvelut, 4. Sisäinen valvonta, 5. Riskienhallinta, 6. Tietosuojalaki. Seuraavaksi pohdin aihealueiden tiimoilta kysymyksiä mitkä antavat riittävästi informaatiota nykytilanteen selvittämiseksi ja mahdollisten jatkokehitystoimien aloittamiseksi.

Alfame Systems Oy on pieni ohjelmistoyritys. Yrityksessä on 3 heimoa (Java, Integraatiot ja .NET), myyntiryhmä ja johtoryhmä. Kyselyn osoitin henkilökunnalle niin että mahdollisimman monenlaisten tehtävien osalta tulisi näkemystä. Kysely lähetettiin joko sähköpostilla tai annettiin paikallisen toimiston väelle tulostettuna versiona. Kyselyn vastaanotti jokaisen heimon arkkitehti ja kehittäjä, myyntiryhmän työntekijä ja johtoryhmän jäsenet (Liite 1). Vastaajille annettiin reilu viikko vastausaikaa. Vastausajan lyhyys määritettiin tarkoituksella riittävän lyhyeksi, jotta kyselyn saaneet saataisiin toimimaan välittömästi sen saatuaan enkä uskonut pitemmän kyselyajan vaikuttavan vastausmäärän kasvuun aiempien yrityksessä toteutettujen kyselyiden perusteella. Kyselyyn tuli määräaikaan mennessä kymmenen vastausta.

4.4 Haastatteluiden toteutus

Tutkimukseen liittyvät haastattelut sovittiin etukäteen. Haastattelut toteutettiin niin että kävin haastateltavien kanssa lounaalla ja ohessa haastateltavat vastaili tutkimukseen liittyvään haastatteluun, haastattelut liittyivät kyselyn aihealueisiin. Osa kyselyyn vastaajista ei kerennyt lounaalle, joten he vastasivat vain kyselyyn. Haastateltavia oli 6 jotka täyttivät myös kyselyn ja pelkkään kyselyyn vastanneita oli lisäksi 4 henkeä. Haastattelut pidettiin rauhallisissa lounasravintoloissa Kokkolassa. Haastattelujen kestot olivat noin 30-45 minuuttia. Haastatteluja ennen haastateltaville kerrottiin tutkimuksen tarkoitus ja

tutkimusaihe. Haastattelun lähtökohtana oli saada kyselyä laajempi näkemys aihepiiristä tutkimuksen taustatiedoiksi.

4.5 Toimeksiantajayritys

Alfame Systems Oy on 2004 Kokkolassa alkunsa saanut IT-alan laajasti menestynyt yritys, joka tuottaa kokonaisvaltaisia digitaalisia integraatio ratkaisuja. Toimipisteitä yrityksellä on nykyään neljä: Kokkola, Helsinki, Tampere ja Rovaniemi. Kehittäjillä on keskimäärin yli kymmenen vuoden kokemus. Asiantuntijoita yrityksessä on hieman yli 50. Yritys on kasvanut vuosittain. Yritys on saanut useita tunnustuksia hyvin tehdystä työstä. Tuoreimpana näistä valinta Suomen parhaaksi yritykseksi Great Place To Work® -tutkimuksessa keskisuurten yritysten joukosta.

Taulukko 3. Kyselyyn valittujen taustatiedot.

Kyselyyn vastannut	Työtehtävä	Tietämys tietosuoja-asetuksesta
Vastaaja 1	Tuotantojohtaja	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Vastaaja 2	Ratkaisukonsultti	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Vastaaja 3	Ratkaisukonsultti	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa - Yrityksen tietosuojasivustoihin tutustuminen
Vastaaja 4	Ohjelmistoarkkitehti	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Vastaaja 5	Ohjelmistoarkkitehti	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Vastaaja 6	Ohjelmistosuunnittelija	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Vastaaja 7	Ohjelmistosuunnittelija	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Vastaaja 8	Ohjelmistosuunnittelija	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa

Vastaaja 9	Ohjelmistosuunnittelija	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Vastaaja 10	Ohjelmistosuunnittelija	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa

Kyselyssä kartoitettiin ensimmäisenä työtehtävä yrityksessä. Taulukossa 3 on kuvattu työntekijän työtehtävä ja mahdolliset tiedon hankinnat tietosuoja-asetuksesta. Mahdollinen yrityksen ulkopuolinen tietosuoja koulutus on laskettu taulukossa mukaan itsenäiseen tiedonhankintaan.

5 EMPIIRISEN TUTKIMUKSEN TULOKSET

Tutkimuksen tavoitteena oli selvittää yrityksen henkilöstön nykytilan tietämys tietosuojalaista ja tietosuojaosaamisesta yleisesti. Samalla tarkoitus arvioida henkilöstön tietämystä tietosuoja-asetuksen vaatimuksiin nähden ja arvioida tulevia tarpeita tietosuojaosaamisen parantamiseksi. Aluksi käydään läpi yrityksen nykytila ja miten siihen on päädytty. Tämän jälkeen käsitellään kyselyissä syntyneet vastaukset ja saatuja tuloksia laajennetaan haastattelujen perusteella.

5.1 Organisaation tietosuojan nykytila

Organisaatiossa aloitettiin EU:n tietosuoja-asetukseen valmistautuminen 2017. Perustettiin yrityksen ”Tietoturva ja turvallisuuspalvelu (ASA)”-ryhmä huolehtimaan yrityksen tietoturvaan ja tietosuojaan liittyvistä asioista. Tietoturvayksikkössä toimii lisäkseni yrityksen tuotantojohtaja. Tietosuoja-asetukseen tutustuin osallistumalla useisiin koulutuksiin aihepiiristä. Koulutusten kautta saamani tietopohjan auttamana aloitin varsinaisen valmistautumisen, osaamistani täydentelin aihepiirin teoksilla. Varsinainen tietosuoja-asetukseen valmistautuminen aloitettiin tekemällä nykytilanarviointi. Tämän perusteella selvitettiin puutteet ja aloitettiin toteuttamaan tarvittavat muutokset. Päivitettyäni tai luotuani dokumentaatiot kuten politiikat ja ohjeistukset ja mahdolliset muut muutokset toteutin tietosuoja-arvioinnin Opsec Oy:n tietosuojavastaavan kanssa.

Lisäksi myynti on käynyt toimitusjohtajan kanssa sopimukset läpi ja tehnyt tarvittavat muutokset. Tämän jälkeen tietoturvaan ja -suojaan liittyvät materiaalit on kerätty sisäiseen intraamme henkilöstömme luettavaksi. Perustettu tietoturvayksikkö toteuttaa jatkossa vähintään kerran vuodessa auditoinnin tietoturvan varmistamiseksi ja kehittämiseksi ja lisäksi ylläpitää säännöllisesti tietoturvaa. Yrityksen kotisivuille on päivitetty tietosuojaseloste ja tarvittavat muut dokumentaatiot. Lisäksi aihepiiriin liittyen on toteutettu yrityksen sivuille myös blogi: GDPR ja rekisteröidyn oikeudet – Korkea aika toimia on nyt! markkinoinnilliseen käyttöön. Yrityksen henkilöstöinfoissa on myös jaettu yrityksessä tarvittavaa tietosuojaan liittyvää informaatiota.

6 YHTEENVETO

Tietosuoja-asetuksen noudattaminen vaatii jatkuvaa seurantaa, reagointia ja dokumentoinnin ylläpitoa. Ilman säännöllistä hallittua seurantaa tietosuojauhkien hallinta ei pysy kasvavien tietoturvauhkien tasolla. Tämän tutkielman tulokset ovat hyvä pohja suunnitella seuraavia askeleita organisaatiomme ja henkilökuntamme tietoturvallisen toiminnan kehittämiseksi. Tutkimus kuvaa hyvin tilannetta keskimääräisessä organisaatiossa, jossa tietosuoja-asetukseen on valmistauduttu ja missä asetusta noudatetaan. Silti tietosuoja-asetuksen mukainen toiminta ja henkilöstön tietoturvatietoisuus on voinut epäonnistua tai jäädä kesken.

Tietoturva pitääkin saada osaksi yrityskulttuuria. Yrityskulttuuri muodostuukin henkilökunnan toiminnassaan omaksumista toimintavoista. Organisaation omat työntekijät nähdäänkin yritysten suurimpina tietoturvariskeinä. Tämän takia onkin tärkeää henkilökunnan onnistunut tietoisuuden lisääminen, ja yrityksessä sovittujen tietosuojakäytäntöjen motivoitunut noudattaminen. Esimiesten ja johdon onkin ensiarvoisen tärkeää toimia esimerkin mukaisesti ja korostaa omilla toimillaan tietoturvan tärkeyttä.

Tutkimuksen tuloksien osalta seuraavina toimenpiteinä pitääkin seuraavina vaiheina pohtia ratkaisuja, miten dokumentaatiosta tehdään löydettävämpi ja miten dokumentaatioiden sisällöt tuodaan osaksi arkipäiväistä toimintaa. Kyselyn voisikin toteuttaa organisaatiossa uudelleen isommalle joukolle, hieman kysymyksiä muokaten. Uudella kyselyllä saavuttaisin tiedon, kuinka tämän tutkimuksen tulosten perusteella toteuttavien muutosten jälkeen tietoturva olisi muodostunut osaksi kulttuuriamme.

Tutkimuksen tuloksena havaitaan myös henkilökunnan erilaiset tavat oppia asioita ja tämän takia tietoturvallisen toiminnan koulutusta täytyy toteuttaa useammallakin eri tavalla. Osalle riittää yleinen informointi asiasta mutta osa vaatii käytännön kokemusta sisäistääkseen asian. Tietosuoja-asetus on aihepiirinä laaja ja sisältää käytännössä kaiken tietoturvaan liittyvät toiminnan, joten koulutettavia asioita on laajasti ja sekin pakottaa pohtimaan mihin keskittyä koulutusmateriaalia pohtiessa ja millä tavoin eriasiat henkilökunnalle kouluttaisi. Tietosuoja-asetus velvoittaa myös riittävän henkilökunnan koulutuksen tietosuojasta ja -turvasta.

7 OPPIMINEN

Tietosuoja-asetuksen noudattaminen vaatii jatkuvaa säännönmukaista tietoturvan arviointia. Opinnäyteprosessin aikaan toteutettiin yrityksessä useampia muutoksia parempaan päin. Muutokset vaativat dokumentointiin muutoksia niin toimintatapojen kuin toimintaympäristön suhteen. Ilman säännönmukaista dokumentaatiota ohjeistukset vanhenevat liian nopeasti ja tulevat tarpeettomiksi tai pahimmillaan aiheuttavat tietoturvariskin organisaatiolle.

Tietosuoja-asetuksesta minulla ei ollut juuri lähtötietoja, joten opinnäytetyöprosessin ohessa tietoni tietosuoja-asetuksen osalta kasvoi valtavasti. Lisäksi sain myös paljon tietämystä toimintaani yrityksen ”Tietoturva ja turvallisuuspalvelu (ASA)”-ryhmän jäsenenä vastatakseni tietoturvan ylläpidosta. Kokonaisuutena toteutus oli melko raskas ja pitkä normaali työn päälle tapahtuvana prosessina.

Tutkimusosan tärkeimpinä anteina koin, että vaikka dokumentoinnit olisi toteutettu yrityksessä ja ulkopuolisella tietosuoja-asetuksen osalta validoitu se ei riitä, jos varsinaiset dokumentoinnit ovat henkilökunnan mielestä liian vaikeasti löydettävissä ja joiltakin osin hankalasti ymmärrettävissä. Näihin seikkoihin aion puuttua työssäni seuraavaksi ja tuoda toimintatavat osaksi yrityksemme kulttuuria.

Kokonaisuutena sain prosessista tulokseksi organisaation kannalta tulevaisuuteen hyödyntävän kokonaisuuden ja hyviä huomioita, joten tunnen tavoitteiden täyttyneen.

LÄHTEET

Andreasson, A., Koivisto, J. & Ylipartanen A. 2016. Tietosuojakäsikirja johdolle. Helsinki: TIETOSANOMA.

Andreasson, A., Riikonen, J. & Ylipartanen A. 2019. Osaava Tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Helsinki: TIETOSANOMA.

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2017. Osaava Tietosuojavastaava. Helsinki: TIETOSANOMA

Check Point Security Report 2019. Cyber Attack Trends Analysis. PDF-dokumentti. Saatavissa: http://snt.hr/boxcontent/CheckPointSecurityReport2019_vol01.pdf. Viitattu 13.1.2020.

Eduskunta 2018a. EU:n tietosuojauudistuksen kansallinen täytäntöönpano. Www-dokumentti. Saatavissa: https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx. Viitattu 13.1.2020.

Eduskunta 2018b. Valiokunnan mietintö HaVM 13/2018. Www-dokumentti. Saatavissa: https://www.eduskunta.fi/FI/vaski/Mietinto/Sivut/HaVM_13+2018.aspx. Viitattu 13.1.2020.

Eduskunta 2018c. Valiokunnan mietintö HaVM 14/2018. Www-dokumentti. Saatavissa: https://www.eduskunta.fi/FI/vaski/Mietinto/Sivut/HaVM_14+2018.aspx. Viitattu 13.1.2020.

Euroopan komissio 2018. Kysymyksiä ja vastauksia - yleinen tietosuoja-asetus. Www-dokumentti. Saatavissa: https://ec.europa.eu/commission/presscorner/detail/fi/MEMO_18_387. Viitattu 13.1.2020.

Euroopan unioni 2008. Euroopan unionista tehdyn sopimuksen VI osastoa soveltamalla annetut säädökset. Neuvoston puitepäätös 2008/977/YOS rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta. PDF-dokumentti. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32008F0977&from=FI. Viitattu 13.1.2020.

Finlex 2018a. Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018. Www-dokumentti. Saatavissa: https://www.finlex.fi/fi/laki/alkup/2018/20181054. Viitattu 13.1.2020.

Finlex 2018b. Tietosuojalaki 1050/2018. Www-dokumentti. Saatavissa: https://www.finlex.fi/fi/laki/alkup/2018/20181050. Viitattu 13.1.2020.

Hanninen, M., Laine, E., Rantala, K., Russi, M. & Varhela, M. 2017. Henkilötietojen käsittely - EU-tietosuoja-asetuksen vaatimukset. Helsinki: KAUPPAKAMARI

Korja, J. 2016. Biometrinen tunnistaminen ja henkilötietojen suoja. Turenki: Acta Universitatis Lapponiensis 325

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent Oy

Lappalainen, J., Auno, P. 2018. Laadullinen tutkimus (Qualitative research). Kajaanin Ammattikorkeakoulu

Oikeusministeriö 2018. Tietosuojalaki täydentäisi EU:n tietosuoja-asetusta. Www-dokumentti. Saatavissa: https://oikeusministerio.fi/artikkeli/-/asset_publisher/tietosuojalaki-taydentaisi-eu-n-tietosuoja-asetusta. Viitattu 13.1.2020.

Opitietosuojaa.fi Noviisista Mestariksi 2019a. Www-dokumentti. Saatavissa: https://opitietosuojaa.fi/index.php/fi/49-tyokalupakki/periaatteet-politiikat-ja-suunnitelmat. Viitattu 13.1.2020.

Opitietosuojaa.fi Noviisista Mestariksi 2019b. Yleistä Tietosuojasta. Www-dokumentti. Saatavissa: https://opitietosuojaa.fi/fi/aloitus/tietosuoja. Viitattu 13.1.2020.

Pitkänen, O., Tiilikka, P. & Warma, E. 2013. Henkilötieojen suoja. Helsinki: Talentum Media Oy

Planeetta 2016. IaaS, PaaS, SaaS? Mikä pilvipalvelu sopii yrityksellesi. Www-dokumentti. Saatavissa: https://www.planeetta.fi/2016/03/15/iaas-paas-saas-mika-pilvipalvelu-sopii-yrityksellesi/. Viitattu 13.1.2020.

Privacy Shield 2020. Privacy Shield Overview. Www-dokumentti. Saatavissa: https://www.privacyshield.gov/Program-Overview. Viitattu 13.1.2020.

Tietosuoja-asetus 2016/679, artikla 34. Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle. Www-dokumentti. Saatavissa: http://www.privacy-regulation.eu/fi/34.htm. Viitattu 13.1.2020.

Tietosuoja-asetus 2016/679, artikla 35. Tietosuojaa koskeva vaikutustenarviointi. Www-dokumentti. Saatavissa: http://www.privacy-regulation.eu/fi/35.htm. Viitattu 13.1.2020.

Tietosuoja-asetus 2016/679, artikla 36. Ennakkokuuleminen. Www-dokumentti. Saatavissa: http://www.privacy-regulation.eu/fi/36.htm. Viitattu 13.1.2020.

Tietosuoja-asetus 2016/679, artikla 37. Tietosuojavastaavan nimittäminen. Www-dokumentti. Saatavissa: http://www.privacy-regulation.eu/fi/37.htm. Viitattu 13.1.2020.

Tietosuoja-asetus 2016/679, artikla 5. Henkilötietojen käsittelyä koskevat periaatteet. Www-dokumentti. Saatavissa: http://www.privacy-regulation.eu/fi/5.htm. Viitattu 13.1.2020.

Tietosuoja-asetus 2016/679, artikla 83. Hallinnollisten sakkojen määräämisen yleiset edellytykset. Www-dokumentti. Saatavissa: http://www.privacy-regulation.eu/fi/83.htm. Viitattu 13.1.2020.

Tietosuoja-asetus 2016/679, kohta 78. Www-dokumentti. Saatavissa: http://www.privacy-regulation.eu/fi/r78.htm. Viitattu 13.1.2020.

Tietosuoja-asetus 2016/679. PDF-dokumentti. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Viitattu 13.1.2020.

Tietosuojaryhmä WP248 2017. Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”

PDF-dokumentti. Saatavissa: https://tietosuoja.fi/documents/6927448/8316711/Vaikutustenarviointi+fi.pdf/af51e999-5326-4223-9deb-e21bdd2e0a63/Vaikutustenarviointi+fi.pdf.pdf. Viitattu 13.1.2020.

Tietosuojavaltuutetun toimisto 2012. Laadi tietotilinpäätös. PDF-dokumentti. Saatavissa: https://tietosuoja.fi/documents/6927448/10594424/Laadi+tietotilinpäätös.pdf/4925bd9e-d07d-82fc-3f2d-71c5955310a0/Laadi+tietotilinpäätös.pdf. Viitattu 13.1.2020.

Tietosuojavaltuutetun toimisto 2018a. Tietosuojavaltuutetun päätös luetteloksi käsittelytoimista, joiden yhteydessä on tehtävä vaikutustenarviointi 21.12.2018. Www-dokumentti. Saatavissa: https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista. Viitattu 13.1.2020.

Tietosuojavaltuutetun toimisto 2018b. Osoita noudattavasi tietosuojasäännöksiä. Www-dokumentti. Saatavissa: https://tietosuoja.fi/osoitusvelvollisuus. Viitattu 13.1.2020.

Tietosuojavaltuutetun toimisto 2018c. Automaattinen päätöksenteko ja profilointi. Www-dokumentti. Saatavissa: https://tietosuoja.fi/automaattinen-paatoksenteko-profilointi. Viitattu 13.1.2020.

Tietosuojavaltuutetun toimisto 2018d. Henkilötietojen käsittelijän velvollisuudet. Www-dokumentti. Saatavissa: https://tietosuoja.fi/henkilotietojen-kasittelijan-velvollisuudet. Viitattu 13.1.2020.

Tietoturvariskien arviointi 2019. Www-dokumentti. Saatavissa: https://www.tietoturvariskienarviointi.fi. Viitattu 13.1.2020.

Valtiovarainministeriö 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 7/2003 PDF-dokumentti. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10229. Viitattu 13.1.2020.

Valtiovarainministeriö 2016a. Rekisterinpitäjän velvollisuudet. Www-dokumentti. Saatavissa: https://www.vahtiohje.fi/web/guest/rekisterinpitajan-velvollisuudet. Viitattu 13.1.2020.

Valtiovarainministeriö 2016b. Eu-tietosuojan kokonaisuudistus. VAHTI-raportti 1/2016. PDF-dokumentti. Saatavuus: https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128. Viitattu 13.1.2020.

Valtiovarainministeriö 2017. Ohje riskienhallintaan. Valtiovarainministeriön julkaisuja 22/2017. PDF-dokumentti. Saatavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf. Viitattu 13.1.2020.

Väre, T. 2019. Master Data. Helsinki: Alma Talent.

Vento, J. 2020. Onrego oy. IaaS, Caas, PaaS, Faas, SaaS - mitä mikäkin tarkoittaa? Www-dokumentti. Saatavissa: https://onrego.fi/julkisen-pilven-palvelumallit-avattuna. Viitattu 11.5.2020.

Watts, S. & Raza, M. 2019. Saas vs Paas vs Iaas: What's The Difference and How To Choose. PDF-dokumentti. Saatavissa: https://blogs.bmc.com/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/?print=pdf. Viitattu 13.1.2020.

Working Party WP168 2009. The Future of Privacy. PDF-dokumentti. Saatavissa: https://tzellis.gr/gdpr/wp29/list/wp168_The-Future-of-Privacy_12-2009.pdf. Viitattu 13.1.2020.

LIITE 1

Anonyymikysely tietoturvasta ja tietosuojalaista

Tietosuoja-asetuksen mukaisen tietämyksen selvitys Alfame Systems Oy:ssä. Seuraavan kyselyn tuloksia käytän jatkossa Alfame Systems Oy:n tietosuoja-asetuksen mukaisen toiminnan kehittämiseen ja YAMK Teknologiaosaamisen johtamisen opinnäytetyössäni. Tietoja käytetään molemmissa yhteyksissä anonyymisesti.

Työtehtäväsi : _____

1. Tietoturva

	Kyllä	Ei
1.1 Onko sinulle selvillä yrityksemme tietoturvalinjaukset ja toimintaohjeet?		
1.2 Onko ohjeet helposti saatavilla?		
1.3 Onko ohjeet riittävän selkeät?		
1.4 Kaipaatko lisäohjeita tietoturvasta?		
1.5 Auttaako tietoturvavaatimuksemme työtäsi?		
1.6 Haittaako tietoturvavaatimuksemme työtäsi?		
1.7 Koetko Tiiminne kehitystyössä tietoturvauhkien paikkoja?		
1.8 Pidetäänkö tietoturvallisuutta yrityksessämme riittävän tärkeänä mielestäsi?		
1.9 Koetko yrityksen tietoturvan nykytilanteen hyväksi?		
1.10 Saatko palautetta Tiimiltä tietoturvallisuudesta palveluissamme?		
1.11 Onko tietoa poikkeamista?		

1.5b/1.6b Jos tietoturvavaatimuksemme haittasi tai auttoi työtäsi niin miten?

1.7b Jos koit Tiiminne kehitystyössä tietoturvauhkien paikkoja, niin millaisia?

1.12 Mitkä tekijät koet pahimmiksi tietoturvauhkiksi yritykselle?

2. Tietosuojakäytännöt

	Kyllä	Ei
2.1 Lukitsen tietokoneen aina poistuessani työpisteeltä?		
2.2 Lukitsen myös muut päätelaitteet?		
2.3 En säilytä työpöydälläni/etäpisteellä mitään henkilötietoihin liittyvää materiaalia?		
2.4 Tunnen asianmukaiset suojaustoimenpiteet fyysisessä/digitaalisessa ympäristössä?		
2.5 Osaan ohjeistaa työkavereita oikeanlaiseen tietojen käsittelyyn parantaakseni yhteistä turvallisuutta?		

3. Pilvipalvelut

	Kyllä	Ei
3.1 Tarvitsetko tukea pilvipalveluiden käytössä?		
3.2 Pitäisikö yrityksemme huolestua pilvipalvelujen tietoturvasta?		
3.3 Tiedätkö mitä pilviratkaisuja yrityksellämme on käytössä?		
3.4 Tunnistatko erilaiset pilviratkaisut SaaS, PaaS, IaaS toisistaan?		
3.5 Erotatko erilaisissa pilviratkaisuissa Tilaajan ja Palveluntuottajan vastuut?		

3.6 Mitä seuraavista asioista koet pilvipalvelun eduksi?

__ tiedon saatavuus eri laitteilla __ helppokäyttöisyys __ etätyöskentely
__ tietoturva __ kilpailuetu __ järjestelmien ajantasaisuus
__ muu, mikä? _____

3.7 Miten kriittiseksi koet yrityksellemme käytössä olevien pilviratkaisujen katkokset?

3.8 Oletko ollut huolissasi tietoturvasta pilvipalveluiden vuoksi?

4 Sisäinen valvonta

	Kyllä	Ei
4.1 Tiedätkö mistä sisäisen valvonnan / riskienhallinnan dokumentaatiomme löytyvät?		
4.2 Onko yrityksellämme mielestäsi riittävän kattavat dokumentaatiot?		
4.3 Koetko että yrityksessämme huomioidaan riittävästi työtyytyväisyys kyselyn tulokset?		
4.4 Onko kyselyt mielestäsi riittävän anonyymisoituja?		

5 Riskienhallinta

	Kyllä	Ei
5.1 Tiedätkö onko meillä johtoryhmän hyväksymä riskienhallinta politiikka?		
5.2 Tiedätkö onko riskit määritelty mitenkään?		
5.3 Onko riskeille määritelty hallintatoimenpiteitä?		
5.4 Valvotaanko toteutumista?		

6 Tietosuojalaki

	Kyllä	Ei
6.1 Koetko ymmärtäväsi riittävästi tietosuoja-asetuksen vaikutuksista työhösi?		
6.2 Onko tietosuoja-asetuksella ollut vaikutuksia Tiimisi toimintaan?		
6.3 Onko tietosuoja-asetus aiheuttanut muutoksia kehitystyöhön?		
6.4 Tarvitsetko lisäkoulutusta tietosuoja-asetuksesta?		
6.5 Luuletko että Tiimi tarvitsisi lisäkoulutusta tietosuoja-asetuksesta?		
6.6 Käsitteletkö työssäsi henkilötietoja/tietosuojaan liittyviä asioita?		
6.7 Tiedätkö missä roolissa käsittelet tietosuoja-asetuksen alaista tietoa?		
6.8 Tiedätkö eri rooleissa (rekisterinpitäjä/henkilötietojen käsittelijä) toimimisen edellyttämät velvollisuudet?		
6.9 Osaatko toimia tietosuoja-asetuksen mukaisesti tietoturvarikkeen sattuessa?		
6.10 Oletko tietoinen yrityksen tietosuoja käytännöistä?		
6.11 Puuttuuko yritykseltä mielestäsi jotain mitä tarvitsemme uuden tietosuoja-asetuksen noudattamiseksi?		

6.12 Tiedätkö mitä seuraa uuden tietosuoja-asetuksen laiminlyönneistä?		
6.13 Osaan luokitella henkilötiedot eri suojausluokkien mukaisesti (julkinen/salassa pidettävät) ja tiedän miten niiden luokitus vaikuttaa niiden lainmukaiseen säilytykseen?		
6.14 Tiedätkö mitkä kaikki henkilötiedot vaativat erityistä suojausta eli ovat ns. arkaluontoisia tietoja?		
6.15 Olen tietoinen yrityksen tietosuojaohjesivuista ja olen tutustunut niiden sisältöön?		
6.16 Tiedätkö mitä tarkoittaa tietoturvariskien vaikutustenarviointi? ja milloin se on pakollista henkilötietojen käsittelyssä?		
6.17 Ymmärrätkö hallinnollisten sakkojen ja perustavanlaatuisten sakkojen eron?		

6.2b/6.3b Jos tietosuoja-asetuksella on ollut vaikutuksia Tiimisi toimintaan niin millaisia?

6.4b Jos tarvitsit lisäkoulutusta tietosuoja-asetuksen osalta, millaista?
__ tietosuoja-asetus yleisesti __ pilvipalvelujen suojaaminen __ eri rooleissa toiminta
__ toiminta tietosuojarikkeen tapahtuessa __ sisäiset ohjeet __ yrityksen tietoturva
__ muu, mikä? _____

6.11b Puuttuuko yritykseltä mielestäsi jotain uuden tietosuoja-asetuksen noudattamiseksi, mitä?

6.4c Jos tarvitsit lisäkoulutusta tietosuoja-asetuksen osalta, mikä koulutusmuoto palvelisi parhaiten?
__ lounasvalmennus __ yleisinfo __ verkkomateriaali __ tiimikohtainen koulutus

6.18 Yleinen mielipiteesi tietosuoja-asetuksesta?

Kiitos kyselyyn vastaamisesta!