Opinnäytetyö (AMK)

Tieto- ja viestintätekniikan koulutus

2019

Johanna Nyberg

EU:N YLEINEN TIETOSUOJA-ASETUS (GDPR) JA HENKILÖTIETOJEN KÄSITTELYN TIETOTURVALLISUUS

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikan koulutus

2019 | 48 sivua, 1 liitesivu

Johanna Nyberg

EU:N YLEINEN TIETOSUOJA-ASETUS (GDPR) JA HENKILÖTIETOJEN KÄSITTELYN TIETOTURVALLISUUS

Opinnäytetyössä tutkitaan Euroopan parlamentin ja Euroopan unionin neuvoston antamaa yleistä tietosuoja-asetusta 2016/679, joka yksinkertaistaa ja yhtenäistää henkilötietojen käsittelyä koskevaa lainsäädäntöä EU:n alueella sekä tarkentaa henkilöiden oikeuksia käsittelytoimissa. Asetus on tuonut mukanaan runsaasti epäselvyyttä siitä, miten henkilötiedot tulee suojata ja miten tulee menetellä, mikäli asetuksen noudattaminen epäonnistuu tai kun tietoihin kohdistuu tietoturvaloukkauksia.

Asetus velvoittaa kaikkia henkilötietoa käsitteleviä yrityksiä implementoimaan teknisiä ja organisatorisia toimenpiteitä henkilötietojen riittävän suojan takaamiseksi, mutta ei määrittele tarkkoja teknisiä vaatimuksia tämän toteuttamiseen. Tästä syystä työn tavoitteena oli tutkia tietosuoja-asetusta tietoturvallisuuden näkökulmasta ja selvittää, mitä toimenpiteitä yrityksien on toteutettava, jotta ne täyttäisivät asetuksen asettamat velvoitteet henkilötietojen tietosuojasta ja tietoturvasta. Tutkimalla tietoturvakäytäntöjä voitiin todeta, että dokumentoinnilla, henkilötietojen salauksella, päätelaitteiden suojauksella, henkilöstön koulutuksella sekä sisäverkon turvaamisella yritykset voivat huomattavasti vähentää henkilötietoihin kohdistuvia uhkia.

Pilvipalveluteknologian yleistymisen ja siihen kohdistuvien uhkien lisääntymisen takia tutkittiin myös henkilötietojen tietosuojaa pilvipalveluissa. Pilvipalveluissa sijaitsevan henkilötiedon tietosuoja on edelleen yrityksen vastuulla, joten yrityksen tulee valita tarjoaja, joka toiminnallaan noudattaa tietosuoja-asetusta.

Pilvipalveluteknologian kehittyessä ja käsiteltävien henkilötietojen määrän lisääntyessä myös mahdollisten uhkien määrät kasvavat ja muuttuvat. Yrityksien tulee jatkuvasti päivittää tietoturvakäytäntönsä ja uudelleenarvioida henkilötietoihin kohdistuvia riskejä.

ASIASANAT:

GDPR, tietoturva, tietosuoja-asetus, henkilötieto, pilvipalvelu, tietovirta

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2019 | 48 pages, 1 page in appendices

Johanna Nyberg

GENERAL DATA PROTECTION REGULATION (GDPR) AND THE SECURITY OF PERSONAL DATA IN PROCESSING OPERATIONS

This thesis examines the General Data Protection Regulation 2016/679 (GDPR) given by the European Parliament and the Council of the European Union. The regulation simplifies and unifies the legislation of processing personal data in the EU and specifies the rights of individuals in data processing operations. The regulation has brought a lot of confusion as to how personal data should be protected and how to proceed if companies fail to comply with the regulation or if personal information is subject to security breaches.

The Regulation mandates that all companies dealing with personal data need to implement technical and organizational measures to ensure adequate protection of personal data, but does not specify the exact technical procedures on how to achieve this. For this reason, the goal of this thesis was to study the data protection regulation from an information security perspective and to find out what measures companies should take to meet the data protection and data security obligations. By researching security practices, it was found that by encrypting personal data, protecting end devices, training personnel, making proper documentations and securing their intranet, companies can significantly reduce possible threats to personal data.

Because of the fast growth of cloud computing and the increased threats to it, the security of personal data in cloud services was also researched. The company is still responsible of the personal data after it is stored in a cloud. Therefore companies must choose a cloud service provider that is GDPR compliant.

As cloud service technology evolves and the amount of personal data processed increases, the number of potential threats increase and change. Companies must constantly update their security practices and reassess the risks to personal data.

KEYWORDS:

GDPR, information security, data protection regulation, personal data, cloud service, data flow

SISÄLTÖ

KÄYTETYT LYHENTEET **7**

1 JOHDANTO **8**

2 EU:N TIETOSUOJA-ASETUS YLEISESTI **9**
2.1 Tietosuoja ja tietoturva 10
2.2 Rekisteröity, rekisterinpitäjä ja henkilötietojen käsittelijä 10
2.3 Henkilötietojen käsittely 11
2.4 Suostumus 13
2.5 Valvontaviranomainen 14
2.6 Tietosuojavastaava 14
2.7 Tietojen käsittely EU:n ulkopuolella ja Privacy Shield -järjestelmä 15
2.8 Sanktiot 16

3 REKISTERÖIDYN OIKEUDET **18**
3.1 Pääsy tietoihin 18
3.2 Tietojen oikaisu- ja poisto-oikeus 18
3.3 Vastustamisoikeus 19
3.4 Siirto-oikeus 19
3.5 Automatisoidut yksittäispäätökset 20
3.6 Käsittelyn rajoitus 20

4 REKISTERINPITÄJÄN VELVOLLISUUDET **22**
4.1 Seloste käsittelytoimista 22
4.2 Tietoturvallisuus 22
4.2.1 Sisäänrakennettu ja oletusarvoinen tietosuoja 23
4.2.2 Sertifiointi 23
4.2.3 Tietosuojan vaikutuksenarviointi 24
4.3 Osoitusvelvollisuus 24
4.4 Tietoturvaloukkaus ja ilmoitusvelvollisuus 25

5 HENKILÖTIETOJEN KÄSITTELIJÄN VELVOLLISUUDET **28**

6 TIETOVIRTAKUVAUS **30**

7 TIETOSUOJAN JA TIETOTURVAN TOTEUTTAMINEN 33
7.1 Kenttätason suojaus 33
7.1.1 Päätelaitteiden suojaus 34
7.1.2 Internet of things -konsepti 35
7.2 Vikasietoisuus ja varmuuskopiointi 35
7.3 Sisäverkon turvaaminen 36
7.4 Pseudonymisointi 38
7.5 Henkilötietojen salaus 38
7.6 Tietosuoja sovellus- ja järjestelmäkehityksessä 39

8 PILVIPALVELUTEKNOLOGIA 41
8.1 Tietojen tallentaminen pilvipalvelussa 42
8.2 Tietoturvaloukkaus pilvipalvelussa 43

9 YHTEENVETO 44

LÄHTEET 45

LIITTEET

Liite 1. Vuokaavio tietoturvaloukkauksen ilmoitusvaatimuksista (Tietosuojatyöryhmä 2017).

KUVAT

Kuva 1. Esimerkki tietovirtakuvauksesta. 32
Kuva 2. Sisäverkon VPN-yhteys päätelaitteeseen. 37
Kuva 3. Tietoturva kehitysprosessissa. 40

KUVIOT

Kuvio 1. Julkisten pilvipalveluiden markkinaosuuden arvioitu kasvu 2008–2020 (Statista 2018). 41

TAULUKOT

Taulukko 1. Tietovirtakuvauksen symbolit. 31

KÄYTETYT LYHENTEET

AAA	Authentication, Authorization, Accounting. Protokolla, jolla voidaan hallita käyttäjien pääsy- ja toimintaoikeuksia päätelaitteistossa ja verkkoympäristössä.
ACL	Access List. Reitittimiin asetettava pääsylista, jonka avulla voidaan hallinnoida ulkoverkon ja yrityksen sisäverkon välistä liikennettä.
GDPR	General Data Protection Regulation. EU:n yleinen tietosuoja-asetus.
IoT	Internet of Things. Käsite, jossa jokapäiväsillä esineillä on yhteys internettiin.
LAN	Local Area Network. Rajatulla ja pienellä maantieteellisellä alueella toimiva verkko eli lähiverkko.
VPN	Virtual Private Network. Julkisen verkon yli kulkeva yksityinen verkkoyhteys, jolla voidaan piilottaa käyttäjän sijainti ja salata yhteyden välityksellä kulkeva tieto.

1 JOHDANTO

EU:n tietosuoja-asetus 2016/679 eli GDPR (General Data Protection Regulation) on Euroopan parlamentin ja Euroopan unionin neuvoston antama henkilötietojen käsittelyä koskeva yleinen tietosuoja-asetus. [1, artikla 99]. Asetuksen myötä luonnollisten henkilöiden on helpompi saada tieto häntä koskevista henkilötietojen käsittelytoimista ja seurata käsittelytoimien lainmukaisuutta [1, artikla 12 kohta 1]. Käsittelytoimia suorittaville osapuolille on asetettu tarkkoja velvoitteita, joiden avulla suojellaan luonnollisten henkilöiden vapauksia ja yksinkertaistetaan yleistä henkilötietojen käsittelyä koskevaa lainsäädäntöä koko EU:n alueella ja tilanteissa, joissa henkilötietoa siirtyy EU:n alueen ulkopuolelle [1, kohta 3 & 101].

Tämän opinnäytetyön tarkoituksena on selvittää, miten tietosuoja-asetus vaikuttaa yrityksiin ja mitä toimenpiteitä yrityksien tulee vähintään toteuttaa, jotta se täyttää tietosuoja-asetuksen asettamat tietosuojan ja tietoturvan vaatimukset. Työssä käsitellään myös, miten yrityksien tulee vastata henkilöiden oikeuksiin käsittelytoimissa. Tietosuoja-asetus määrää, että käsiteltäviä henkilötietoja on suojeltava ja yrityksien on implementoitava riittävät organisatoriset ja tekniset hallintatoimenpiteet tämän toteuttamiseen. Asetus ei kuitenkaan määrittele tarkkoja teknisiä vaatimuksia hallintatoimenpiteiden toteutukselle, joten yrityksien vastuulle jää näiden menetelmien arviointi ja valinta. Hallintamenetelmien riittävyyden arviointi on kuitenkin haasteellista. Pilvipalveluteknologian käytön yleistymisen takia tietosuoja-asetus on tuonut myös paljon epävarmuutta siitä, miten tietoja saa käsitellä pilvipalveluiden kautta EU:n alueen ulkopuolella.

Tämän opinnäytetyön tutkimuskysymykset ovat:

- mitä konkreettisia tietosuojan ja tietoturvan varmistavia toimenpiteitä yrityksen tulee toteuttaa,
- miten yrityksen tulee menetellä, kun henkilötietoihin kohdistuu uhkia, sekä
- miten yrityksen tulee valita pilvipalvelun tarjoaja ja kuka on vastuussa pilvipalveluissa sijaitsevista henkilötiedoista.

Opinnäytetyön toimeksiantaja on mikroyritys, joka kehittää asiakkailleen työkaluja henkilötietojen keräämiseen ja käsittelyyn.

2 EU:N TIETOSUOJA-ASETUS YLEISESTI

Euroopan parlamentti ja Euroopan unionin neuvosto antoivat 27. huhtikuuta 2016 uuden tietosuoja-asetuksen 2016/679, joka tunnetaan yleisemmin nimellä GDPR (General Data Protection Regulation, GDPR). Asetus koskee kaikkia Euroopan unionin maita sekä kaikkia maita, joissa henkilötietojen käsittely kohdistuu Euroopan unionin kansalaisiin [1, artikla 1 kohta 1 & 2], [1, artikla 3 kohta 1 & 2]. Asetuksen varsinainen soveltaminen alkoi kahden vuoden siirtymäajan jälkeen 25. toukokuuta 2018 [1, artikla 99].

Uuden tietosuoja-asetuksen tarkoituksena on yhtenäistää sekä yksinkertaistaa henkilötietoa koskevaa lainsäädäntöä kaikissa Euroopan unionin maissa. Tämä asettaa luonnollisten henkilöiden henkilötietojen käsittelylle uudet velvoitteet ja suojelee tietojen vapaata liikkuvuutta sekä luonnollisen henkilön oikeuksia henkilötietojen käsittelyssä. Asetus vaikuttaa kaikkiin yrityksiin ja organisaatioihin, jotka käsittelevät EU:n kansalaisten henkilötietoa, eli lähes kaikkiin EU:n alueella toimiviin yrityksiin ja organisaatioihin. Asetus myös velvoittaa niitä tarkistamaan sekä uudistamaan tietosuojakäytäntönsä varmistaakseen niiden lainmukaisuuden. [2]

EU:n uusi tietosuoja-asetus kumosi vuonna 1995 voimaan astuneen direktiivin 95/46/EY henkilötietojen käsittelystä ja tiedon vapaasta liikkuvuudesta. Uusi asetus tarkentaa ja lisää luonnollisen henkilön oikeuksia sekä helpottaa tiedon liikkuvuutta esimerkiksi eri järjestelmien välillä. [3]

Eduskunta tiedotti 13. marraskuuta 2018 uudesta tietosuoja-asetusta täydentävästä ja täsmentävästä tietosuojalaista sekä lain henkilötietojen käsittelystä rikosasioissa, jotka kumosivat aiemman voimassa olleen henkilötietolain sekä lain tietosuojalautakunnasta ja tietosuojavaltuutetusta [3]. Uusia lakeja sovelletaan tietosuoja-asetuksen rinnalla ja niiden tarkoituksena on tietosuoja-asetuksen täsmennyksen ja poikkeustilanteiden säätämisen lisäksi helpottaa jäsenvaltioiden viranomaisten välistä työtä ja tiedonvaihtoa. Ne myös suojelevat luonnollisten henkilöiden oikeuksia ja vapauksia takaamalla johdonmukaista sekä korkeatasoista henkilötietojen käsittelyä rikosasioihin liittyvissä käsittelytoimissa. [4]

2.1 Tietosuoja ja tietoturva

Käsitteitä tietosuoja ja tietoturva käytetään usein toistensa synonyymeinä, mutta niillä on eri merkitys. Tietosuojalla tarkoitetaan luonnollisen henkilön oikeuksia itseään koskevaan tietoon. Kaikilla yksilöillä on oikeus yksityisyyden suojaan sekä henkilötietojensa lainmukaiseen käsittelyyn ja niiden turvaamiseen luvattomalta käytöltä. [2] Oikeaoppinen tietosuojan toteuttaminen takaa, että luonnollisen henkilön oikeuksiin on vastattu.

Tietoturvalla puolestaan tarkoitetaan tiedon eheyttä, saatavuutta, käytettävyyttä ja luottamuksellisuutta, joiden ylläpitämisestä yritys huolehtii suojaamalla omat tietojärjestelmänsä ja -aineistonsa [5]. Tietoa voidaan kutsua eheäksi silloin, kun se ei ole vääristynyt eikä valtuuttamaton henkilö ole sitä päässyt muokkaamaan. Valtuuttamaton on henkilö, jolla ei ole lupaa päästä käsiksi henkilötietoihin. Saatavuudella tarkoitetaan, että valtuutetuilla henkilöillä on tietoon esteetön pääsy ja he voivat hyödyntää tietoa aina kun se on tarpeellista [6]. Tiedon luottamuksellisuus tarkoittaa, että ainoastaan siihen valtuutetuilla henkilöillä on mahdollisuus lukea tai muokata tietoa. Jos esimerkiksi järjestelmään kirjautumiseen käytettävä salasana vuotaa valtuuttamattomille osapuolille, tietoa ei enää pidetä luottamuksellisena.

2.2 Rekisteröity, rekisterinpitäjä ja henkilötietojen käsittelijä

Rekisteröity on luonnollinen henkilö, johon henkilötietojen käsittely kohdistuu ja jonka perusoikeuksia ja -vapauksia tietosuoja-asetus suojelee henkilötietojen käsittelytoimissa [1, artikla 4 kohta 1]. Henkilötiedot sijaitsevat henkilörekisterissä, jolla tarkoitetaan mitä tahansa digitaalista tai fyysistä tietojoukkoa, joka sisältää henkilötietoja [1, artikla 4 kohta 6].

Rekisterinpitäjä määrää henkilötietojen käsittelyn tarkoituksen sekä käsittelyssä käytettävistä menetelmistä. Rekisterinpitäjänä voi toimia luonnollinen henkilö, virasto, viranomainen, oikeushenkilö tai jokin muu elin, jonka velvollisuutena on vastata rekisteröidyn oikeuksiin ja noudattaa tietosuoja-asetusta. [1, artikla 4 kohta 7]

Henkilötietojen käsittelijä voi olla yrityksen työntekijä tai ulkoinen taho, joka toimii rekisterinpitäjän toimeksiannon ja ohjeiden mukaisesti henkilötietojen käsittelytoimissa.

Käsittelijänä voi toimia luonnollinen henkilö, virasto, viranomainen, oikeushenkilö tai jokin muu elin. [1, artikla 4 kohta 8]

2.3 Henkilötietojen käsittely

Henkilötiedolla tarkoitetaan kaikkea tietoa, jonka avulla luonnollinen henkilö voidaan tunnistaa joko suoraan tai yhdistämällä eri tietoaineistoista henkilöön liittyviä tietoja. Henkilötietoa on esimerkiksi nimi, puhelinnumero, henkilötunnus, kuva, ikä, sähköpostiosoite sekä IP-osoite. Kaikki toiminta, joka kohdistuu henkilötietoihin, on henkilötietojen käsittelyä. Toiminta voi olla esimerkiksi tiedon tallentamista, järjestelyä, muokkaamista ja keräämistä joko manuaalisesti tai automaattisesti. [7] Manuaalisella henkilötietojen käsittelyllä tarkoitetaan henkilörekisterin tai siihen tarkoitetuksi kuuluvan osan käsittelyä, joka tapahtuu luonnollisen henkilön toimesta ilman esimerkiksi järjestelmän suorittamaa automaattista prosessointia. Henkilötietojen automaattista käsittelyä tapahtuu esimerkiksi profiloinnissa, jossa henkilötietojen perusteella tehdään arviota tai analyysia luonnollisen henkilön henkilökohtaisista piirteistä, taloudellisesta tilanteesta, käytöksestä tai muista ominaisuuksista. [8] Henkilötietojen käsittely tulee aina suorittaa asianmukaisesti, lainmukaisesti ja käsittelyssä tulee soveltaa läpinäkyvyysperiaatetta. Käsittelyn läpinäkyvyys tarkoittaa, että rekisteröidyllä on aina oikeus tietää miten ja mihin häntä koskevaa tietoa on käytetty tai tullaan käyttämään, ja rekisterinpitäjä tai henkilötietojen käsittelijä tarjoaa tämän tiedon selkeästi ja avoimesti. [1, artikla 5 kohta 1a]

Yrityksen tulee myös henkilötietojen käsittelyssä huomioida tietojen käyttötarkoitussidonnaisuus. Henkilötiedot on kerättävä ainoastaan tietylle niille ilmoitettuun, lailliseen käyttötarkoitukseen. Niitä ei saa käyttää tavalla, joka on ilmoitetun tarkoituksen kanssa yhteensopimaton eikä niitä saa käyttää uudestaan myöhemmissä käsittelytoimissa ilman uutta, erillistä ilmoitusta rekisteröidylle. Mikäli rekisterinpitäjä käyttää henkilötietoja uuteen alkuperäisestä poikkeavaan käyttötarkoitukseen ja tekee käsittelystä ilmoituksen, tulee hänellä lisäksi olla tähän rekisteröidyn suostumus. [1, artikla 5 kohta 1b]

Rekisterinpitäjän on toiminnallaan suojattava rekisteröidyn henkilötiedot lainvastaiselta ja luvattomalta käytöltä, vääristymiseltä, häviämiseltä ja tuhoutumiselta [1, artikla 5 kohta 1f]. Tällainen toiminta voi olla esimerkiksi varmuuskopioiden teko ja huolellinen säilytys

sekä teknisten ja organisatoristen menetelmien toteuttaminen, joiden avulla voidaan estää pääsy tietoihin henkilöiltä, joilla ei ole lupaa käsitellä niitä.

Rekisterinpitäjän tulee säilyttää henkilötietoja ainoastaan niin kauan kuin se on tarpeellista, eli säilytysaika ei saa ylittää käsittelytoimien kestoa. Tietojen säilytyksestä tulee asettaa määräaika, jonka kuluessa rekisterinpitäjä tarkistaa tai poistaa ne. Jos säilytysaika umpeutuu tai rekisteröity vaatii henkilötietojensa poistoa, poisto koskee sen hetkisiä aktiivisia järjestelmiä ja käsittelytoimia. [9] Mikäli rekisteröidyn tietoja on tallentunut varmuuskopioituihin tietoihin, rekisterinpitäjän ei tarvitse poistaa tietoja varmuuskopioista välittömästi, mikäli tämä aiheuttaisi rekisterinpitäjälle kohtuutonta vaivaa. Rekisterinpitäjä on kuitenkin vastuussa henkilötiedoista esimerkiksi tietoturvaloukkauksen tapahtuessa ja niihin pätee edelleen rekisteröidyn oikeudet. Jos varmuuskopioituja tietoja ei voida poistaa välittömästi rekisteröidyn pyynnöstä, rekisterinpitäjän tulee ilmoittaa tästä rekisteröidylle ja asettaa määräaika, johon mennessä tiedot poistetaan. [1, kohta 39]

Henkilötiedot ovat erityisen arkaluonteisia, jos niistä ilmenee luonnollisen henkilön uskonnollinen tai filosofinen vakaumus, terveystietoja, etninen alkuperä, poliittinen kanta tai mielipide, ammattiliiton jäsenyys, biometrisia tai geneettisiä tietoja henkilön tunnistamiseksi tai henkilön seksuaaliseen suuntautumiseen tai käyttäytymiseen liittyvää tietoa. Tällaisten henkilötietojen käsittely on lähtökohtaisesti kielletty, ellei niitä käsitellä tietosuoja-asetuksessa määritellyissä erityistapauksissa. Erityistapaukseksi katsotaan esimerkiksi se, että luonnollisen henkilö on antanut suostumuksensa rekisterinpitäjälle käsitellä näitä nimenomaisia tietoja tai henkilö on saattanut tiedot julkisesti saataville. [1, artikla 9] Tietojen käsittely saattaa niiden arkaluonteisuuden takia aiheuttaa henkilön oikeuksille ja vapauksille merkittäviä riskejä, joten tietojen suojelemiseen käsittelytoimissa on käytettävä erityistä tarkkuutta ja huolellisuutta.

Rekisterinpitäjän tulee lainmukaisesti laatia henkilötietojen käsittelijälle dokumentoidut ohjeet henkilötietojen käsittelystä, sen kestosta luonteesta sekö tarkoituksesta. Henkilötietojen käsittelijä ei saa tietojen käsittelyssä poiketa rekisterinpitäjän ohjeista, ellei EU:n oikeudessa tai jäsenvaltion lainsäädännössä toisin määrätä. [1, artikla 28 kohta 3]

2.4 Suostumus

Rekisterinpitäjän tulee aina saada rekisteröidyltä suostumus henkilötietojen käsittelyyn. Suostumus voidaan antaa suullisesti tai kirjallisesti ja rekisterinpitäjän on kyettävä todistamaan, että hänellä on rekisteröidyn suostumus käsittelytoimiin. Suostumuksen antaminen tulee olla selkeää ja helppoa ja sen täytyy perustua rekisteröidyn vapaaehtoisuuteen. [1, artikla 7] Esimerkiksi valmiiksi valittua valintaruutua lomakkeessa ei tunnisteta suostumuksen antamiseksi, vaan valintaruudun tulee lähtökohtaisesti olla tyhjä ja rekisteröidyn tulee vapaaehtoisesti painaa valintaruutua, jolla suostumus annetaan. Suostumuksen antamatta jättäminen ei kuitenkaan saa olla este palveluiden tarjoamiselle. Eli jos henkilö päättää olla painamatta valintaruutua, se ei saa estää lomakkeen edelleenlähetystä. Asetus ei velvoita käyttämään valintaruutuja [7].

Mikäli henkilötietojen käsittelyyn kohdistuu useita toimia, rekisteröidyn on annettava suostumuksensa kaikkia näitä toimia varten, vaikka ne toteutetaan samaa tarkoitusta varten. Mikäli rekisteröity päättää peruuttaa suostumuksensa, on hänen ilmoitettava tästä rekisterinpitäjälle. Suostumuksen peruuttaminen tulee olla rekisteröidylle helppoa. [7]

Alle 16-vuotiaiden rekisteröityjen henkilötietojen käsittelyyn vaaditaan rekisteröidyn vanhemman suostumus. EU:n jäsenvaltiot voivat tästä poiketen soveltaa lainsäädännössään alimmillaan 13 vuoden ikärajaa. [1, artikla 8]

Evästeiden tallentamiseen liittyvät suostumusvaatimukset eivät ole asetuksen myötä muuttuneet. Suomessa sovelletaan edelleen Euroopan parlamentin ja neuvoston antamaa direktiiviä 2002/58/EY, jonka mukaan evästeiden tallentamiseen tarvitaan käyttäjän suostumus ja niiden tallentamisesta sekä käyttötarkoituksesta on ilmoitettava käyttäjälle selkeästi. Evästeistä ei poikkeuksellisesti tarvitse ilmoittaa, mikäli käyttäjä on pyytänyt palvelua, joka perustuu evästeiden käyttöön tai jos niitä käytetään ainoastaan palvelun käytön helpottamiseen tai viestin välittämiseen teknisesti. Evästeiden ilmoittamisesta tai niiden käytön hyväksymisestä ei Suomessa vaadita ponnahdusikkunaa, mutta sivustolla tulee olla tieto evästeiden käytöstä käyttäjälle selkeällä tavalla ja mahdollisuus lukea niiden käytöstä lisätietoa. [10]

2.5 Valvontaviranomainen

Valvontaviranomainen valvoo tietosuoja-asetuksen toteutumista ja täyteenpanoa yhteistyössä muiden jäsenvaltioiden valvontaviranomaisten sekä EU:n komission kanssa tietosuoja-asetuksen johdonmukaisen soveltamisen takaamiseksi sekä luonnollisten henkilöiden oikeuksien ja vapauksien suojelemiseksi [1, artikla 51].

Valvontaviranomainen tiedottaa rekisterinpitäjiä ja henkilötietojen käsittelijöitä asetuksen velvoitteista, sanktioista sekä oikeuksista. Rekisteröity voi myös halutessaan pyytää valvontaviranomaiselta tietoa asetuksen määräämistä luonnollista henkilöä koskevista oikeuksista. Rekisteröidyn oikeuksiin ja henkilötietojen yleiseen suojaan vaikuttaa tietoja viestintätekniikassa tapahtuva kehitys, jonka erityinen seuraaminen on valvontaviranomaisen vastuu. [1, artikla 57]

2.6 Tietosuojavastaava

Yrityksen on nimitettävä tietosuojavastaava, jos se käsittelee arkaluontoisia henkilötietoja EU:n alueella tai toteuttaa henkilötietojen järjestelmällistä ja säännöllistä seurantaa. Rekisterinpitäjä tai henkilötietojen käsittelijä nimittää tietosuojavastaavan rooliin henkilön, joka toimii yrityksen tietosuojan asiantuntijana ja neuvonantajana. Yrityksen tulee ottaa tietosuojavastaava mukaan kaikkiin henkilötietojen käsittelyyn liittyviin tietosuojakysymyksiin, mutta vastuu asetuksen tietosuoja- ja tietoturvavaatimusten noudattamisesta käsittelyssä on rekisterinpitäjällä. Rooliin nimitetyn henkilön yhteystiedot tulee julkaista ja ilmoittaa valvontaviranomaiselle. [1, artikla 37 kohta 1]

Tietosuojavastaava valvoo asetuksen vaatimuksien täyttymistä ja tarpeen tullen neuvoo sekä kouluttaa yrityksen henkilökuntaa käsittelyyn liittyvistä toimintamenettelyistä ja tietosuojaperiaatteista. Tietosuojavastaava toimii myös rekisteröityjen yhteyshenkilönä kaikkiin henkilötietojen käsittelyyn liittyvissä kysymyksissä. Nimitetty henkilö voi kuulua rekisterinpitäjän tai henkilötietojen käsittelijän henkilöstöön tai olla organisaation ulkopuolinen palveluntarjoaja. [7]

Rekisterinpitäjä ja henkilötietojen käsittelijä varmistavat, että tietosuojavastaavalla on kaikki tarvittavat tiedot sekä resurssit, jotka ovat tehtävien suorittamisen kannalta välttämättömiä ja että häntä ei rangaista tietosuojavastaavan tehtäviin kuuluvien toimien

hoitamisesta. [7] Jos yritys tai organisaatio päättää olla noudattamatta tietosuojavastaavan neuvoja esimerkiksi tietoturvapoikkeuksen tapahtuessa, rekisterinpitäjän on suotavaa laatia kirjallinen dokumentaatio syistä, joiden takia neuvoja päätettiin olla noudattamatta.

2.7 Tietojen käsittely EU:n ulkopuolella ja Privacy Shield -järjestelmä

Henkilötietoja siirtyy usein EU:n ulkopuolelle käsiteltäväksi eri palveluiden kautta. Esimerkiksi verkkokaupassa tapahtuvassa kaupankäynnissä tarvitaan usein luonnollisen henkilön nimi, puhelinnumero, osoite, syntymäaika, sähköpostiosoite sekä luottokorttitietoja. Jos henkilötietoa siirtyy EU:n alueen ulkopuolelle, tulee kohdemaan, -alueen, -sektorin tai -järjestön olla Euroopan komission hyväksymä sekä täyttää riittävän tietosuojan vaatimukset [11]. Vuoteen 2019 mennessä Euroopan komissio on todennut Andorran, Kanadan, Argentiinan, Färsaarien, Islannin, Norjan, Israelin, Japanin, Jerseyn, Mansaarien, Sveitsin, Uruguayn, Uuden-Seelannin sekä Guernseyn täyttävän vaaditun tietosuojan tason. Euroopan komissio on todennut myös Yhdysvalloissa sijaitsevien yritysten, jotka kuuluvat Privacy Shield -järjestelmään, täyttävän riittävän tietosuojan tason. [12]

Yhdysvaltojen liittovaltion kauppakomissio ja Euroopan komissio suunnittelivat Privacy Shield -järjestelmän turvatakseen EU:n alueen kansalaisten perusoikeuksia ja -vapauksia sekä helpottaakseen kaupankäyntiä ja tietosuoja-asetuksen noudattamista, kun EU:n kansalaisen henkilötietoa siirtyy Yhdysvaltoihin. EU:n kansalaisten henkilötietojen käsittely Yhdysvalloissa on sallittu ainoastaan niissä yrityksissä, jotka kuuluvat järjestelmään. Järjestelmä koostuu viitekehyksestä, jossa on määritelty yrityksiin kohdistuvat vaatimukset sekä luonnollisiin henkilöihin kohdistuvat oikeudet. [13]

Järjestelmään kuuluvia yrityksiä velvoitetaan muun muassa suojaamaan EU:n alueelta vastaanotettuja henkilötietoja, noudattamaan EU:n tietosuojaviranomaisten ohjeita, vastaamaan mahdollisiin valituksiin viivyttelemättä, näyttämään tietosuojakäytäntönsä verkkosivuillaan sekä uusimaan Privacy Shield -sertifikaattinsa vuosittain. Tietojen salauksesta ei ole asetettu yksityiskohtaisia vaatimuksia, mutta tietoturvariskien vähentämiseksi yrityksen on riittäviä teknisiä toimenpiteitä hyödyntäen suojattava henkilötiedot. Toimenpiteiden riittävyys voidaan arvioida esimerkiksi riskianalyysin

avulla. Privacy Shield -järjestelmän kautta käsiteltäviin henkilötietoihin pätee tietosuoja-asetuksen määrittämät velvoitteet ja oikeudet. [14]

2.8 Sanktiot

Valvontaviranomaisella on oikeus soveltaa yritykseen tai organisaatioon kohdistuvia tutkintavaltuuksia, kuten määrätä kaikki käsittelytoimiin liittyvät henkilötiedot luovutettavaksi ja saada pääsy kaikkiin tarvittaviin tietoihin ja laitteisiin, suorittaa tutkimuksia tarkastusten muodossa sekä määrätä sertifioinnin uudelleentarkastelusta [1, artikla 58 kohta 1]. Mikäli yrityksen tai organisaation katsotaan rikkoneen tietosuoja-asetusta tai rekisteröity tekee valituksen, valvontaviranomainen voi soveltaa korjaavia toimivaltuuksia. Asetuksen mukaan kaikilla valvontaviranomaisilla on seuraavat korjaavat toimivaltuudet:

- Antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle varoitus sekä huomauttaa asetuksen säännösten vastaisista käsittelytoimista,
- Määrätä vastaamaan rekisteröidyn pyyntöjä,
- Määrätä käsittelytoimien saattaminen asetuksen säännösten mukaisiksi,
- Määrätä rekisterinpitäjä ilmoittamaan tietoturvaloukkauksesta rekisteröidylle, jonka henkilötietoihin loukkaus on kohdistunut,
- Asettaa käsittelykielto tai käsittelyn rajoitus,
- Määrätä henkilötietojen oikaisusta, poistosta tai käsittelyn rajoituksesta sekä velvoittaa näistä muutoksista kaikille tahoille, joille kyseiset henkilötiedot on luovutettu,
- Peruuttaa sertifiointi tai kieltää sertifiointielintä antamasta sertifiointia, mikäli sitä koskevia vaatimuksia ei enää täytetä, sekä
- Määrätä kielto henkilötietojen siirtämiselle kolmansiin maihin EU:n alueen ulkopuolelle, [1, artikla 58 kohta 2].

Valvontaviranomaisilla on lisäksi valtuudet määrätä hallinnollisista sakoista, jotka voidaan määrätä valvontaviranomaisen toimenpiteiden lisäksi tai sijasta. Hallinnollisten sakkojen määräämisessä otetaan huomioon muun muassa rikkeen luonne, laajuus, tahallisuus, rekisterinpitäjän aiemmat asetuksen rikkomukset, kaikkien tahojen oikeudet ja velvollisuudet sekä henkilöryhmät, joihin rike kohdistuu. Sakon määrään vaikuttaa lisäksi rekisterinpitäjän menettely rikkomuksen vahinkojen minimoimiseksi ja rekisteröidyn oikeuksien suojelemiseksi, kuten yhteistyö valvontaviranomaisen kanssa

sekä välittömien toimenpiteiden toteuttaminen tietoturvaloukkauksen tapahtuessa. Lieventävänä tekijänä voidaan katsoa se, että rikkominen tuli valvontaviranomaisen tietoon rekisterinpitäjän toimesta. [1, artikla 83 kohta 2]

Hallinnollisten sakkojen enimmäismäärä on yritykselle joko neljä prosenttia sen vuosittaisesta maailmanlaajuisesta kokonaisliikevaihdosta tai 20 000 000 euroa, mikäli tämä summa on suurempi. Sakko määräytyy aina suuremman summan mukaan. [1, artikla 83 kohta 4 & 5] Kyseisten sakkojen saaminen edellyttää kuitenkin laajaa ja usein toistuvaa tietosuoja-asetuksen rikkomista ja sen asettamien velvollisuuksien laiminlyömistä. Hallinnollisia sakkoja ei määrätä ensimmäisenä sanktiona, vaan valvontaviranomainen soveltaa ensin tutkintavaltuuksiaan ja korjaavia toimivaltuuksiaan. [1, artikla 83 kohta 1 & 2]

Usein hallinnollisia sakkoja merkittävämmäksi sanktioksi voidaan katsoa valvontaviranomaisen määräys tietojenkäsittelyn väliaikaisesta tai pysyvästä rajoituksesta, kaikkien henkilötietojen käsittelytoimien kieltämisestä tai henkilörekisterien poistamisesta [1, artikla 58 kohta 1f & 1g]. Tämä voi joidenkin yritysten tai organisaatioiden kohdalla tarkoittaa esimerkiksi koko asiakasrekisterin tai muiden henkilörekisterien poistoa, jotka ovat usein välttämättömiä niiden toiminnan kannalta.

3 REKISTERÖIDYN OIKEUDET

Luonnollisesta henkilöstä tulee rekisteröity, kun hänen henkilötietoja käytetään jossakin käsittelytoimissa. Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus saada tietoa häneen kohdistuvista käsittelytoimista joko sähköisesti luettavassa tai kirjallisessa muodossa rekisterinpitäjältä. Rekisteröidyllä tulee aina olla oikeus tietoihin, joiden avulla hän voi varmistaa itseensä kohdistuvien käsittelytoimien lainmukaisuus [1, artikla 12 kohta 1]. Rekisteröidyn oikeuksien toteuttaminen ei kuitenkaan saa aiheuttaa riskiä tai vahinkoa muiden luonnollisten henkilöiden perusoikeuksille ja -vapauksille [1, kohta 63], kuten esimerkiksi ohjelmistojen tekijänoikeuksille.

3.1 Pääsy tietoihin

Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, käsitelläänkö häntä koskevia henkilötietoja. Rekisteröidyllä on lisäksi oikeus saada tietää, mitä häntä koskevia henkilötietoja rekisterinpitäjällä on, mikä niiden käyttötarkoitus on, kauanko tietoja säilytetään, mille tahoille tietoa on mahdollisesti luovutettu, mistä rekisterinpitäjä on tiedot saanut sekä oikeus tehdä valitus valvontaviranomaiselle. [1, artikla 13] Mikäli mahdollista ilman kohtuutonta vaivaa tai lainmukaisuutta loukkaamatta, rekisteröidyllä tulee olla etäpääsy omiin käsiteltäviin tietoihinsa, joiden tulee sijaita turvatussa järjestelmässä [1, kohta 63].

Rekisterinpitäjän on viimeistään kuukauden kuluessa vastattava rekisteröidyn pyyntöön sähköisesti, ellei rekisteröity toisin pyydä. Rekisterinpitäjä vastaa joko toimittamalla pyydetyt tiedot tai kieltäytymällä pyynnöstä. Mikäli rekisterinpitäjä kieltäytyy rekisteröidyn pyynnöstä, on kieltäytyminen perusteltava. Jos pyyntö on monimutkainen tai niitä on useita, pyynnön toimittamisen määräaikaa voidaan jatkaa kahdella kuukaudella. Rekisterinpitäjän on toimitettava määräajan jatkamisesta perustelu rekisteröidylle. [15]

3.2 Tietojen oikaisu- ja poisto-oikeus

Mikäli rekisteröidyn henkilötiedot ovat virheelliset tai puutteelliset, hänellä on oikeus saada virheelliset tiedot oikaistua tai täydennettyä esimerkiksi toimittamalla

rekisterinpitäjälle lisäselvitys. Rekisterinpitäjän on ilman aiheetonta viivytystä oikaistava tai täydennettävä tiedot. [1, artikla 19], [15]

Rekisteröidyllä on oikeus vaatia rekisterinpitäjältä henkilötietojensa poistamista, mikäli käyttötarkoitussidonnaisuus ei enää täyty, rekisteröity kumoaa suostumuksensa, käsittely ei ole tapahtunut lainmukaisesti, tietojen käsittelyyn ei ole perusteltua syytä, rekisteröity vastustaa henkilötietojensa käsittelyä tai jos rekisterinpitäjään kohdistuu lakisääteinen velvoite, joka perustuu EU:n oikeuteen tai jäsenvaltion lainsäädäntöön. Rekisterinpitäjän on vastattava vaatimukseen ilman aiheetonta viivytystä. Tietojen poistoa varten rekisterinpitäjän tulee tietää tarkkaan mitä kaikkea henkilöön liittyvää tietoa käsitellään, missä tieto sijaitsee ja tunnistaa, onko tiedon poistoa varten laadittu automatisoitua prosessia. [16]

3.3 Vastustamisoikeus

Tietosuoja-asetuksessa määrätään rekisteröidyn oikeudesta vastustaa henkilötietojensa käsittelyä. Mikäli rekisteröity vastustaa käsittelyä, rekisterinpitäjä ei saa käsitellä kyseiseen henkilöön liittyviä henkilötietoja ilman erityisen tärkeää ja perusteltua syytä, joka kumoaa rekisteröidyn vastustamisoikeuden. Rekisteröidyllä ei ole vastustamisoikeutta, jos käsittelytoimet koskevat tehtävää, joka ajaa yleistä etua. Rekisterinpitäjän on ilmoitettava rekisteröidylle 30 päivän kuluessa, mikäli rekisteröidyn pyynnöstä kieltäydytään sekä tarjottava rekisteröidylle kirjallinen perustelu kieltäytymisestä. Jos rekisterinpitäjä osoittaa pyyntöjen olevan kohtuuttomia tai perusteettomia, on hänellä oikeus kieltäytyä tai periä rekisteröidyltä maksu pyynnön toteuttamisesta. [16]

3.4 Siirto-oikeus

Kun rekisterinpitäjä soveltaa käsittelytoimissa automaattista käsittelyä, rekisteröidyllä on oikeus häntä koskevien henkilötietojen siirtoon nykyisen rekisterinpitäjän järjestelmien välillä tai toisen rekisterinpitäjän järjestelmään sekä oikeus saada häntä koskevat tiedot rekisterinpitäjältä. Oikeus koskee kuitenkin ainoastaan tietoja, jotka rekisteröity henkilö on tietoisesti itse toimittanut rekisterinpitäjälle sekä tietoa, jota rekisteröity on tietoisesti tuottanut esimerkiksi kyselyiden kautta. Oikeutta ei sovelleta esimerkiksi rekisterinpitäjän tekemiin analyyseihin, päätelmiin tai arvioihin, jotka pohjautuvat rekisteröidyn

toimittamiin tietoihin tai tietoa, joka on syntynyt automaattisen prosessoinnin, kuten profiloinnin kautta. Siirto-oikeus mahdollistaa rekisteröityjen helpon vaihdon palvelusta toiseen. Rekisterinpitäjän tulee vastata siirtopyyntöön ilman aiheetonta viivytystä 30 päivän kuluessa. Rekisteröidyn siirto-oikeuteen vastaaminen ei saa aiheuttaa kielteisiä vaikutuksia muiden rekisteröityjen oikeuksiin ja vapauksiin tai rikkoa säädöksiä henkilötietojen käsittelystä EU:n ulkopuolella. [17]

Rekisterinpitäjän tulee toimittaa rekisteröidyn pyytämät henkilötiedot yleisesti käytetyssä ja koneellisesti luettavassa muodossa. Tiedostomuodon tulee siis olla sellainen, että ohjelmistot voivat lukea siitä tietoa automaattisesti. Henkilötiedot toimitetaan suoraan rekisteröidylle myös tilanteissa, joissa suora siirto toiseen järjestelmään ei ole teknisesti toteutettavissa. Tällöin rekisteröity voi halutessaan toimittaa tiedot toisen järjestelmän ylläpitäjälle itse. Rekisterinpitäjät eivät ole velvollisia eri järjestelmien yhteensopivuuden varmistamisesta. [1, kohta 68]

3.5 Automatisoidut yksittäispäätökset

Automatisoitu yksittäispäätös on automaattista henkilötietojen käsittelyä, jossa sovellus tai ohjelmisto tekee päätöksen rekisteröidystä luonnollisen henkilön puolesta. Rekisteröidyllä on oikeus vastustaa automaattista käsittelyä ja vaatia, että luonnollinen henkilö toimii päätöksentekijänä tai arvioi sovelluksen tekemät päätökset. [7] Päätös voi tapahtua esimerkiksi automaattisen käsittelyn johdosta, jossa automatisoitu prosessi järjestelmässä hyväksyy tai hylkää käyttäjän tekemän pyynnön hänen täyttämän lomakkeen perusteella. Prosessi voi esimerkiksi hylätä automaattisesti työnhakijoita heidän iän perusteella. Rekisteröity voi riitauttaa automatisoidun yksittäispäätöksen [7].

3.6 Käsittelyn rajoitus

Rekisteröidyllä on tietyissä tilanteissa oikeus vaatia rekisterinpitäjältä omien henkilötietojensa käsittelyn rajoittamista. Mikäli rekisterinpitäjä on käsitellyt henkilötietoja lainvastaisesti, rekisteröity voi vaatia käsittelyn rajoittamista, mutta samanaikaisesti vastustaa tietojensa poistoa rekisteristä. Rekisterinpitäjän tulee aina ilmoittaa rekisteröidylle käsittelyn rajoituksen poistosta. [15]

Käsittelyä voidaan rajoittaa väliaikaisesti, jos rekisteröity kiistää tietojensa totuudenmukaisuuden. Tällöin rekisterinpitäjän tulee varmistaa tietojen totuudenmukaisuus ja keskeyttää henkilötietojen käsittely rajoituksen ajaksi. Mikäli rekisteröity tarvitsee henkilötietoja oikeudellisesti perustellun vaatimuksen laatimiseen, esittämiseen tai puolustamiseen, voidaan rajoitettua käsittelyä soveltaa väliaikaisesti, vaikka rekisterinpitäjä ei enää tarvitse tietoja käsittelyyn. Jos rekisteröity vastustaa henkilötietojensa käsittelyä henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella, tulee rekisterinpitäjän keskeyttää tietojen käsittely tai olla perusteltu syy tietojen käsittelyn jatkamiselle, joka kumoaa rekisteröidyn oikeudet ja vapaudet. Rajoitettua käsittelyä sovelletaan sen ajan, kun rekisteröity odottaa päätöksen todentamista. [1, artikla 21 kohta 1]

4 REKISTERINPITÄJÄN VELVOLLISUUDET

Rekisterinpitäjän tulee kaikissa käsittelytoimissa noudattaa tietosuoja-asetuksessa määriteltyjä velvollisuuksia lainmukaisesti ja vastata rekisteröidyn oikeuksiin. Yrityksen on tärkeää tunnistaa, toimiiko se rekisterinpitäjänä vai henkilötietojen käsittelijänä kussakin käsittelytoimia vaativassa projektissa. Molempien osapuolien tulee tutustua tietosuoja-asetukseen perusteellisesti ja osattava kaikissa käsittelytoimissa huomioida käsittelyn lainmukaisuus sekä rekisteröidyn oikeudet. Rekisterinpitäjän on myös pystyttävä auttamaan ja neuvomaan henkilötietojen käsittelijöitä sekä varmistamaan heidän käsittelytoimien lainmukaisuus. [1, artikla 28 kohta 1 & 3].

Rekisterinpitäjinä voi joissakin tilanteissa toimia yrityksen tai organisaation asiakas, jonka kanssa on laadittu sopimus henkilötietojen käsittelystä ja rekisterinpitäjän roolista. Tällainen tilanne voi syntyä esimerkiksi, jos yritys tarjoaa asiakkaalleen työkalun henkilötietojen keräämiseen ja tallentamiseen, mutta asiakas määrää henkilötietojen käsittelyn tarkoituksesta ja toimii tällöin rekisterinpitäjänä. Mikäli yritys osallistuu käsittelytoimiin, se toimii henkilötietojen käsittelijänä. Yrityksen ja asiakkaan välinen sopimus on oltava lainmukainen [1, artikla 28 kohta 3].

4.1 Seloste käsittelytoimista

Rekisterinpitäjän tulee laatia kirjallinen seloste organisaation toteuttamista käsittelytoimista. Selosteessa tulee olla kuvattuna kaikki henkilötietoihin kohdistuva toiminta sekä niitä koskevat henkilöryhmät. Seloste toimii ohjeena organisaation rekisterinpitäjille ja henkilötietojen käsittelijöille sisäisenä asiakirjana. Henkilötietolaki, joka kumottiin 5.12.2018 velvoitti rekisterinpitäjiä laatimaan rekisteri- ja tietosuojaselosteen jokaisesta organisaation rekisteristä, jonka avulla rekisteröidyt saivat tietoa heihin kohdistuvista käsittelytoimista. Uusi tietosuoja-asetus ei rekisterinpitäjiä kuitenkaan tähän velvoita. [7]

4.2 Tietoturvallisuus

Asetus velvoittaa rekisterinpitäjän arvioimaan henkilötietojen käsittelyyn liittyviä riskejä ja valitsemaan riskitason mukaiset hallintatoimenpiteet, joilla tietoturvaloukkauksen

mahdollisuutta vähennetään ja sen mahdollinen vahinko minimoidaan [1, artikla 32 kohta 1]. Toimenpiteiden suunnittelussa tulee ottaa huomioon mahdollisten riskien ja niiden vakavuuden sekä todennäköisyyden lisäksi mahdolliset kustannukset, toimenpiteiden tekniikan uutuus sekä käsittelyn laajuus, luonne, asiayhteys ja tarkoitus [1, artikla 25]. Riskit on hyvä asettaa numerojärjestykseen niiden todennäköisyyden ja mahdollisten vaikutusten mukaan sekä priorisoida uhkia tai hallintamenetelmiä niiden kiireellisyyden perusteella. Uhkien ja menetelmien prioriteettiin vaikuttaa usein niihin liittyvät kustannukset. Organisaatio voi mahdollisuuksiensa mukaan työstää yleisen riskitason alentamista käyttämällä analyysistä johdettua kokonaisarvoa, joka koostuu uhkien arvojen yhteenlasketusta määrästä. [18]

4.2.1 Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuoja-asetuksessa määrätään sisäänrakennetusta ja oletusarvoisesta tietosuojasta. Sisäänrakennetulla tietosuojalla tarkoitetaan, että yritys tai organisaatio ottaa käyttöön riittävät tietosuojan ja -turvan varmistavat hallintatoimenpiteet käsittelyn suunnittelun alkuvaiheissa ennen varsinaisten käsittelytoimien alkamista. Tällöin riittävien tietosuojaperiaatteiden käyttö varmistetaan koko käsittelyn keston ajaksi. Tietosuojan riittävyyttä on hyvä arvioida käsittelytoimien edetessä ja mikäli tarpeellista, tietosuojan hallintamenetelmät tulee päivittää. Oletusarvoinen tietosuoja tarkoittaa, että yritys tai organisaatio toteuttaa kaikissa käsittelytoimissa korkeaa yksityisyydensuojaa kuten henkilötietoihin pääsyn rajoittamista, tietojen säilyttämistä mahdollisimman vähän aikaa sekä käsittelyn rajausta ainoastaan välttämättömiin tietoihin. [8] Tietosuoja-asetuksessa ei määrätä tietosuojan teknisistä minimivaatimuksista.

4.2.2 Sertifiointi

Yritys tai organisaatio voi osoittaa täyttävänsä tietosuojavaatimukset sekä muut asetuksen velvoitteet sertifioinnin avulla. Sertifiointielin voi myöntää enintään kolmeksi vuodeksi sertifikaatin, mikäli yritys tai organisaatio pystyy osoittamaan noudattavansa tietosuoja-asetusta; kun tämä toimittaa käsittelynsä sertifiointimekanismille; toimittaa valvontaviranomaiselle tai sertifiointielimelle sertifiointimenettelyn suorittamiseen tarvittavat tiedot sekä myöntää pääsyn käsittelyssä käytettäviin järjestelmiin ja

dokumentaatioihin. Sertifioidun yrityksen tai organisaation tulee edelleen noudattaa kaikkia tietosuoja-asetuksessa asetettuja velvoitteita. [1, artikla 42], [14]

4.2.3 Tietosuojan vaikutuksenarviointi

Mikäli yritys arvioi henkilötietoihin kohdistuvan riskitason olevan korkea, tulee yrityksen tehdä tietosuojan vaikutustenarviointi. Vaikutustenarviointi tulee suorittaa myös tilanteissa, joissa käsittelytoimet koskevat huomattavaa määrää henkilötietoa, voivat vaikuttaa huomattavaan määrään rekisteröityjä tai voivat vaikeuttaa rekisteröidyn oikeuksien toteutumista tai niihin vastaamista. Myös erityisen arkaluonteisten henkilötietojen käsittelyssä on suositeltavaa suorittaa arviointi. [1, 35 artikla], [19]

Vaikutustenarviointi suoritetaan ohjelmiston, järjestelmän tai palvelun suunnitteluvaiheessa ja siinä tulee kuvata järjestelmällisesti henkilötietojen käsittelyn käyttötarkoitus, niiden tietovirta tietovirtakuvauksella (ks. luku 6) sekä niihin kohdistuvat mahdolliset riskit [1, artikla 30]. Arvioinnissa otetaan huomioon yrityksen tai organisaation nykyinen tietosuojan taso ja sen riittävyys tulevissa käsittelytoimissa. Vaikutustenarviointidokumentaatiota tulee päivittää käsittelytoimien edetessä, mikäli arvioidut riskitasot muuttuvat, käsiteltävien henkilötietojen määrä kasvaa huomattavasti tai jos käsittelytoimissa tapahtuu muita merkittäviä muutoksia. Samaa vaikutustenarviointia ei tule käyttää eri käsittelytoimissa, joiden käyttötarkoitukset eroavat toisistaan. [1, artikla 35] Vaikutustenarvioinnin avulla voidaan tunnistaa puutteita yrityksen nykyisessä tietosuojassa ja vahvistaa tietosuojaperiaatteita sekä hallintatoimia, täten pienentäen henkilötietoihin kohdistuvaa riskitasoa. Mikäli riskitason pienennys ei onnistu vaikutustenarvioinnin laatimisen jälkeen eivätkä tietosuoja-asetuksen asettamat vaatimukset täyty, tulee rekisterinpitäjän ottaa yhteyttä valvontaviranomaiseen ja tehdä tästä kirjallinen ilmoitus [1, kohta 84].

4.3 Osoitusvelvollisuus

Osoitusvelvollisuudella tarkoitetaan rekisterinpitäjän velvollisuutta pystyä osoittamaan, että henkilötietojen käsittelyyn on saatu rekisteröidyn suostumus ja että kaikkia henkilötietojen käsittelyyn kohdistuvia velvoitteita on noudatettu lainmukaisesti ja rekisteröidyn oikeuksiin on vastattu jokaisessa käsittelyn vaiheessa. Rekisterinpitäjän on pystyttävä esittämään dokumentaatio käsittelyn lainmukaisuudesta,

käyttötarkoitussidonnaisuudesta, velvollisuuksien noudattamisesta, rekisteröidyn suostumuksesta, käytetyistä tietosuojan organisatorisista ja teknisistä menetelmistä sekä rekisteröidyn oikeuksiin vastaamisesta. Suullinen osoitus ei ole pätevä. [19]

4.4 Tietoturvaloukkaus ja ilmoitusvelvollisuus

Tietoturvaloukkaus voi aiheuttaa aineellista, aineetonta tai fyysistä vahinkoa luonnollisen henkilön oikeuksille ja vapauksille. Aineellisella vahingolla tarkoitetaan vahinkoa, jonka arvoa voidaan mitata ja määrittää varallisuusarvona, kuten taloudellista menetystä tai tekijänoikeuksien vaarantumista. Aineettomalla vahingolla tarkoitetaan vahinkoa, jonka arvoa ei suoraan voida määrittää minkään objektiivisen mittapuun mukaan. [20] Aineetonta vahinkoa on esimerkiksi maineen vahingoittuminen tai kärsimys. Fyysistä vahinkoa voi olla esimerkiksi fyysinen turvattomuus.

Henkilötietoihin kohdistuva tietoturvaloukkaus määritellään tietosuoja-asetuksessa tapahtumana, jossa käsiteltävät henkilötiedot häviävät, tuhoutuvat, muuttuvat tai niitä käsitellään lainvastaisesti joko tahattomasti tai tahallisesti. Tietosuoja-asetusta ei sovelleta tapauksissa, joissa tietoturvaloukkaus ei kohdistu henkilötietoihin. [1, artikla 4 kohta 12]

Henkilötietojen lainvastaista käsittelyä tapahtuu esimerkiksi tilanteissa, joissa henkilötietoja käsittelee osapuoli, jolla ei ole lupaa päästä tietoihin. Luvatonta pääsyä tietoihin voi tapahtua organisaation sisäisen henkilökunnan toimesta tai esimerkiksi tietomurron johdosta. Luvaton pääsy tietoihin voi johtaa tietojen häviämiseen, jos tiedot sisältävä laitteisto varastetaan, järjestelmän salasana vaihdetaan tai tiedot salataan tavalla, joka estää rekisterinpitäjän pääsyn niihin. Tietojen häviämisellä tarkoitetaan, että rekisterinpitäjällä ei ole enää pääsyä henkilötietoihin tai ne eivät enää ole tämän valvonnassa tai hallussa. Vahingossa tapahtuvaa häviämistä on esimerkiksi tietojen tahaton poisto tai salattujen tietojen salausavaimen katoaminen, eli käytettävyys häviää. Tahallista häviämistä tapahtuu esimerkiksi silloin, kun haittaohjelmat sieppaavat ja salaavat henkilötietoja. Mikäli henkilötiedot voidaan palauttaa esimerkiksi varmuuskopiosta tai salauksen purkamalla, käytettävyyden häviäminen on väliaikaista. Pysyvä käytettävyyden häviäminen tarkoittaa, että rekisterinpitäjän pääsyä tietoihin ei voida palauttaa. [21]

Tietoturvaloukkauksen todennäköisyyttä voidaan vähentää suorittamalla henkilötietojen riskianalyysi ja soveltamalla riskitasoa vastaavat hallintamenetelmät. Rekisterinpitäjän tulee soveltaa sisäisiä prosesseja, joiden avulla voidaan havaita tietoturvapoikkeamia sekä -loukkauksia ja vastata niihin nopeasti. Tietovuon seurantatyökalut hälyttävät epätavallisista tapahtumista järjestelmissä tai verkossa. Hälytyksiä voidaan tutkia yhdessä tapahtumalokien analysointivälineiden kanssa, jotta voidaan määritellä tapahtumia ja tunnistaa mahdollisia tietoturvaloukkauksia. [21] Tietoturvapoikkeamat on tutkittava mahdollisimman pian niiden havaitsemisten jälkeen. Kun tietoturvaloukkausta epäillään, hallintamenetelmistä laadittua dokumenttia voidaan käyttää apuna selvittämään, onko henkilötietoihin kohdistuva loukkaus todella tapahtunut ja ovatko henkilötiedot vaarantuneet. Yrityksessä tietoturvasta vastaava henkilö tutkii tietoturvapoikkeamia, toteaa tietoturvaloukkaukset, soveltaa tarvittavat toimenpiteet sekä suorittaa riskiarvioinnin yhdessä rekisterinpitäjän kanssa.

Mikäli tietoturvaloukkaus todetaan tapahtuneen, yrityksen on välittömästi sovellettava vahingonhallintatoimenpiteitä ja arvioitava rekisteröidyille aiheutuva todennäköinen riski. Vaikutusarvioinnissa tehty riskianalyysi on usein yleisluonteisempi kuin tietoturvaloukkauksen aiheuttaman todelliset riskit, joten arviointi harvoin vastaa täysin tietoihin kohdistuvaa todellista uhkaa. Jos rekisterinpitäjä toteaa rekisteröityjen oikeuksiin ja vapauksiin kohdistuvan merkittäviä riskejä on tietoturvaloukkauksesta ilmoitettava valvontaviranomaiselle 72 tunnin kuluessa loukkauksen havaitsemisesta. Mikäli ilmoituksen antaminen ylittää 72 tunnin määräajan, tulee rekisterinpitäjän toimittaa perusteltu syy ilmoitusajan ylittämisestä. Rekisterinpitäjän katsotaan laiminlyöneen tietosuoja-asetuksen ilmoitusvelvollisuutta, jos tietoturvaloukkaus on tapahtunut eikä ilmoitusta ole annettu. [21]

Tietoturvaloukkauksen ilmoituksessa tulee kuvata loukkauksen luonne ja laajuus, tietosuojavastaavan nimi sekä yhteystiedot tai yhteyspiste, arvioidut seuraukset sekä toimenpiteet, jotka on suoritettu tai aiotaan suorittaa tietoturvaloukkauksen aikana ja sen jälkeen henkilötietoihin kohdistuvan vahingon lieventämiseksi. Mikäli mahdollista, rekisterinpitäjän tulee ilmoittaa arvioitu lukumäärä rekisteröidyistä, joihin loukkaus on kohdistunut. Rekisterinpitäjän tulee myös osoittaa, että henkilötietojen suojeluun vaadittavia toimenpiteitä on noudatettu ja että rekisterinpitäjä on suorittanut riskianalyysin ennen käsittelytoimien aloittamista. [1, artikla 34 kohta 2], [22]

Rekisterinpitäjällä ei aina ole tarpeeksi tietoa tietoturvaloukkauksesta 72 tunnin kuluessa sen havaitsemisesta tehdäkseen tarpeeksi kattavan ilmoituksen valvontaviranomaiselle.

Tällöin rekisterinpitäjä voi tehdä vaiheittain tapahtuvan ilmoituksen. Vaiheittain tapahtuvassa ilmoituksessa rekisterinpitäjä tekee alustavan ilmoituksen ja luovuttaa siihen asti keräämänsä tiedot. Täydentävät tiedot voidaan toimittaa valvontaviranomaiselle myöhemmin. Mikäli rekisterinpitäjä toimittaa tietoturvaloukkauksen tiedot vaihteittain, tulee hänen erikseen tiedottaa tästä ja tarjota perusteltu syy. Rekisterinpitäjä ja valvontaviranomainen tekevät sopimuksen lisätietojen toimittamisen tavasta sekä ajankohdasta. Esimerkiksi rikosteknistä tutkimusta vaativissa tapauksissa sovelletaan usein vaiheittaista ilmoitusta. [21]

Rekisterinpitäjän ei tarvitse lainkaan tehdä ilmoitusta tietoturvaloukkauksesta valvontaviranomaiselle, mikäli loukkauksesta ei aiheudu riskiä luonnollisen henkilön oikeuksille ja vapauksille. Tällaisissa tapauksissa riskitaso saattaa kuitenkin muuttua ajan kuluessa, joten rekisterinpitäjän on suotavaa arvioida tietoturvaluokkauksen luonnetta uudestaan myöhemmässä vaiheessa. Jos esimerkiksi henkilötietoa siirtyy henkilölle, jolla ei ole lupaa päästä tietoihin, mutta tiedot ovat salattuja eivätkä täten luettavassa muodossa, loukkaus ei välttämättä aiheuta riskiä rekisteröidyille. [21] Kyseinen henkilö voi kuitenkin pystyä saattamaan tiedot luettavaan muotoon, jos hän esimerkiksi saa haltuunsa salauksenpurkuavaimen, jolloin luonnolliseen henkilöön kohdistuvat riskit kasvavat huomattavasti.

Tietoturvaloukkauksen tapahtuessa rekisterinpitäjän tulee myös ilmoittaa loukkauksesta rekisteröidylle, paitsi jos loukkauksesta ei aiheudu riskiä hänen oikeuksille ja vapauksille tai ilmoituksen teko vaatisi kohtuutonta vaivaa. Ilmoituksen yhteydessä on suotavaa tarjota rekisteröidylle ohjeita, joilla hän voi suojautua mahdollisilta vaikutuksilta tai lisävahingoilta. [1, artikla 34 kohta 3], [21]

Jos rekisteröity vaatii tietojensa oikaisua, täydentämistä tai poistoa, peruuttaa suostumuksensa henkilötietojen käsittelystä, vastustaa käsittelyä tai jos käsittely on suoritettu lainvastaisesti, tulee rekisterinpitäjän ilmoittaa muutoksista kaikille osapuolille, joille henkilötietoja on luovutettu. Ilmoitusta ei tarvitse tehdä, jos se on mahdotonta tai vaatii kohtuutonta vaivaa [1, artikla 19].

5 HENKILÖTIETOJEN KÄSITTELIJÄN VELVOLLISUUDET

Henkilötietojen käsittelijä toimii rekisterinpitäjän apuna ja varmistaa, että käsittelytoimissa noudatetaan tietosuoja-asetuksessa säädettyjä velvollisuuksia käsittelyn turvallisuudesta ja yleisestä tietosuojasta [1, artikla 32 kohta 1]. Rekisterinpitäjä tekee henkilötietojen käsittelijän kanssa lainsäädännön mukaisen kirjallisen ja sähköisen oikeudellisen asiakirjan käsittelytoimien tarkoituksesta, kestosta, kohteesta, luonteesta sekä käsiteltävien henkilötietojen tyypeistä ja rekisteröityjen ryhmistä. Rekisteröityjen ryhmiä voivat olla esimerkiksi työntekijät, työnhakijat tai asiakkaat. Asiakirjassa tulee lisäksi ilmetä rekisterinpitäjän velvollisuudet ja oikeudet. Henkilötietojen käsittelijä sitoutuu noudattamaan asiakirjan ohjeiden mukaisia käsittelyperiaatteita, eikä poikkea kirjatuista ohjeista, ellei käsittelijään sovelleta EU:n oikeudessa tai jäsenvaltion lainsäädännössä määräystä, joka kumoaa asiakirjan ohjeen. Käsittelijä ei saa ulkoistaa tehtäviään tai tehdä muutoksia käsiteltäviin henkilötietoihin ilman kirjallista ennakkolupaa rekisterinpitäjältä. [1, artikla 28] Mikäli henkilötietojen käsittelijä rekisterinpitäjän luvalla käyttää toisen käsittelijän palveluita, molempiin käsittelijöihin kohdistuu rekisterinpitäjän kanssa laaditun oikeudellisen asiakirjan mukaiset vaatimukset. Yrityksen henkilötietojen käsittelijän vastuulla on varmistaa, että palvelun tarjoava käsittelijä noudattaa asiakirjan ohjeita. [1, artikla 32 kohta 4]

Mikäli henkilötietojen käsittelijä määrää tietojen käsittelyn tarkoituksesta tai sen menetelmistä, tulee käsittelijästä rekisterinpitäjä. Henkilötietojen käsittelijä voi toimia yksittäisten käsittelyiden rekisterinpitäjänä, jolloin käsittelijään kohdistuu rekisterinpitäjän velvoitteet käsittelyn ajaksi. Mikäli henkilötietojen käsittelijä määrää rekisterinpitäjän kanssa yhdessä henkilötietojen käsittelyn tarkoituksesta tai menetelmistä, heistä tulee yhteisrekisterinpitäjiä. [1, artikla 26]

Henkilötietojen käsittelijän tulee noudattaa vaikutustenarvioinnin mukaisia tietosuojatoimenpiteitä ja sitoutuu täyttämään asetuksen tietosuojavaatimuksia. Mikäli henkilötietojen käsittelijä havaitsee tietoturvapoikkeaman, hänen tulee selvittää, onko tietoturvaloukkausta tapahtunut ja viipymättä ilmoittaa tästä rekisterinpitäjälle. Tietosuoja-asetuksessa ei kuitenkaan ole säädetty tarkkaa määräaikaa, jonka kuluessa henkilötietojen käsittelijän tulee ilmoittaa rekisterinpitäjälle tietoturvaloukkauksesta. Henkilötietojen käsittelijä voi ilmoituksen tehtyään suorittaa riskiarviointia yhdessä

rekisterinpitäjän kanssa, mutta häntä ei velvoiteta arvioimaan tietoturvaloukkauksen todennäköisiä riskejä ennen rekisterinpitäjälle ilmoittamista. Henkilötietojen käsittelijä voi myös tehdä ilmoituksen loukkauksesta valvontaviranomaiselle, mikäli hänellä on ilmoituksen tekoon tarvittavat tiedot ja rekisterinpitäjä on myöntänyt hänelle valtuudet siihen. Ennen valvontaviranomaiselle ilmoittamista henkilötietojen käsittelijän on kuitenkin tiedotettava tästä rekisterinpitäjälle. Rekisterinpitäjän toimittamat lisätiedot tai esimerkiksi varmuuskopiot saattavat kumota ilmoituksen tekemisen tarpeellisuuden**.** Oikeudellinen vastuu tietoturvaloukkauksen ilmoituksesta ja varmistus siitä, että se saapuu valvontaviranomaisen tietoon 72 tunnin kuluessa on kuitenkin rekisterinpitäjällä, vaikka henkilötietojen käsittelijä tekee ilmoituksen tämän puolesta. [21]

6 TIETOVIRTAKUVAUS

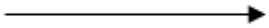
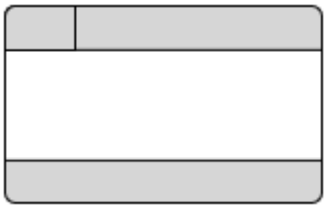
Tietosuoja-asetus velvoittaa kaikkia yrityksiä ja organisaatioita, jotka käsittelevät EU:n kansalaisten henkilötietoja laatimaan tietovirtakuvauksen [1, artikla 30]. Tietovirtakuvaus on työkalu, jonka avulla voidaan luoda graafinen kuvaus tiedon kulusta järjestelmissä, eri järjestelmien välillä ja niiden ympäristössä. Kuvauksen avulla selviää kaikki tiedonkulkuun liittyvät prosessit niiden vastaanottohetkestä alkaen. [23]

Tietovirtakuvaus voi olla looginen tai fyysinen. Loogista tietovirtakuvausta käytetään kuvaamaan mitä tiedonkulussa tapahtuu, eli miten henkilötiedot liikkuvat organisaation sisällä ja mitkä tahot käsittelevät tietoa. Tietotyypin, yleisen prosessin sekä entiteettien kuvaus ovat osa loogista tietovirtakuvausta. Sillä ei ole tarkoitus kuvata prosessien teknistä taustaa vaan selittää yrityksen tai organisaation toimintaa. Fyysisen tietovirtakuvauksen avulla voidaan kuvata esimerkiksi järjestelmien rakennetta ja muita käsittelyyn osallistuvia laitteita sekä ohjelmistoja ja niiden teknisiä ominaisuuksia [24]. Tässä luvussa on sovellettu tietovirtakuvauksen luomiseen yleisimmin tunnettua Ganen ja Sarsonin menetelmää.

Yrityksen tai organisaation laatimassa tietovirtakuvauksessa tulee kuvata kaikkien käsiteltävien henkilötietojen kulkua käsittelytoimien eri vaiheissa. Kuvauksesta tulee selvitä kuka tietoa käsittelee ja kenellä on siihen pääsy, mitä prosesseja käsittelytoimiin kuuluu sekä minne tietoa siirretään ja tallennetaan [24]. Tietosuoja-asetus velvoittaa yritystä tai organisaatiota ainoastaan loogisen tietovirtakuvauksen tekoon.

Käsittelyyn osallistuvia henkilöitä, organisaatioita ja järjestelmiä merkitään ulkoisen entiteetin (engl. external entity) symbolilla. Ulkoiset entiteetit ovat järjestelmän ulkopuolella, mutta ovat siihen vuorovaikutuksessa. Kuvauksessa tulee olla kuvattuna rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijät sekä mahdolliset muut entiteetit. Prosessisymbolia (engl. process) käytetään kuvaamaan käsittelytoimiin liittyviä tapahtumia, kuten suostumuksen antaminen, henkilötietojen käsittelijän nimittäminen tai tiedon kerääminen. Datavarastosymbolilla (engl. data store) kuvataan tallennettua tietoa ja tietojoukkoja, jotka sijaitsevat esimerkiksi organisaation sisäisessä tallennusjärjestelmässä tai pilvipalvelussa. Entiteettien, prosessien ja datavarastojen välillä kulkevaa tietoa merkitään nuolella (engl. data flow), joka kuvaa yksittäisen henkilötiedon tai yksittäisistä tiedoista koostuvan tietojoukon kulkua (Taulukko 1.). [23]

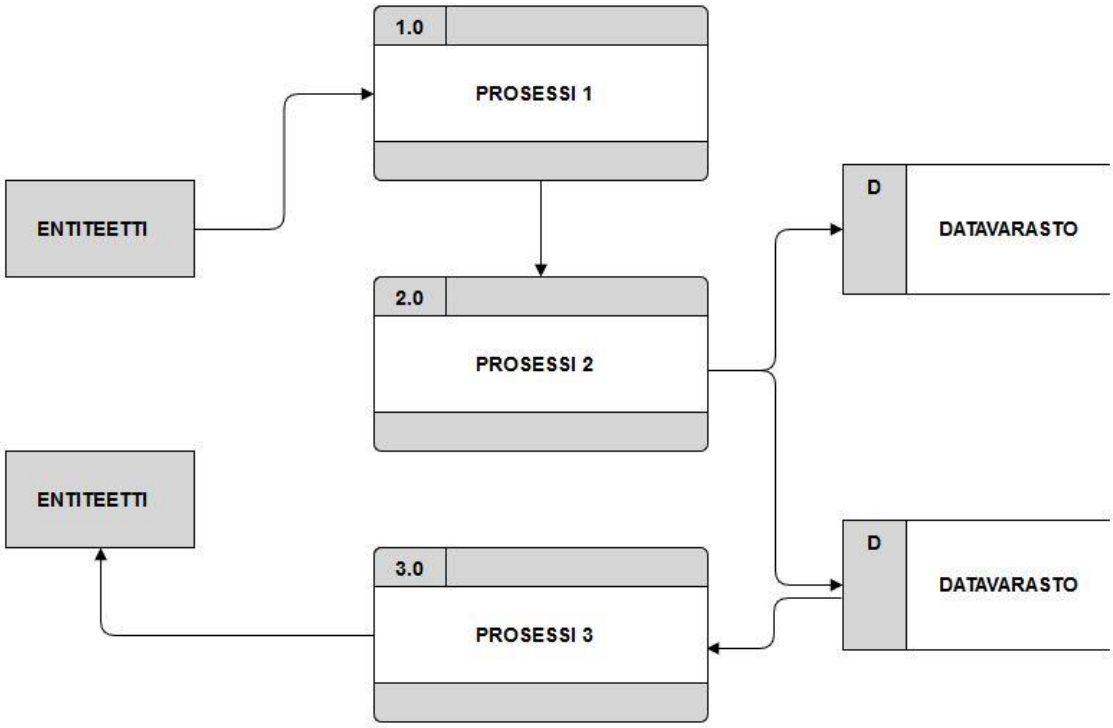
Taulukko 1. Tietovirtakuvauksen symbolit.

Symboli	Nimi
	Ulkoinen entiteetti (external entity)
	Tiedon kulku (data flow)
	Prosessi (process)
	Datavarasto (data store)

Jokaiseen tietovirtakuvaukseen merkittyyn ulkoiseen entiteettiin on merkittävä ainakin yksi tiedon kulkua kuvastava nuolisymboli. Nuoli voi osoittaa tiedon kulkua joko entiteetistä prosessiin tai prosessista entiteettiin. Jokaisesta yksittäisestä henkilötiedosta tai yksittäisistä tiedoista koostuvasta tietojoukosta tulee merkitä erillinen nuolisymboli. [23]

Jokaisesta prosessista sekä datavarastosta on myös merkittävä ainakin yksi tiedon kulkua kuvastava nuolisymboli. Prosesseista voi kulkea tietoa molempiin suuntiin toisiin prosesseihin, entiteetteihin tai datavarastoon. Tiedon kulkua ei saa merkitä suoraan entiteetistä toiseen tai suoraan datavarastosta toiseen. Kun tietoa kulkee entiteetiltä toiselle tai datavarastosta toiseen, niiden välillä tapahtuu aina prosessointia, joka tulee merkitä prosessisymbolilla. Jokaiselle prosessille annetaan oma järjestysnumero, jotta niiden tapahtumajärjestystä on helpompi seurata. Datavarastot on myös hyvä erotella

joko numeroinnilla tai nimillä, jotta henkilötietojen tarkka tallennuspaikka on aina rekisterinpitäjän tiedossa (Kuva 1.). [23]



Kuva 1. Esimerkki tietovirtakuvauksesta.

7 TIETOSUOJAN JA TIETOTURVAN TOTEUTTAMINEN

Vaikka tietosuoja-asetuksessa ei ole säädetty tietoturvan teknisistä minimivaatimuksista tai salausvaatimuksista, rekisterinpitäjiä velvoitetaan soveltamaan riittävää tietosuojaa ja -turvaa teknisillä ja organisatorisilla toimenpiteillä henkilötietojen suojelemiseksi. Tietosuojan ja tietoturvan riittävyyttä voi kuitenkin olla vaikea arvioida. Rekisterinpitäjän tulee tehdä arviointi käsittelytoimistaan ja soveltaa riittäviä suojatoimia tapauskohtaisesti. Asetuksessa säädetyt tekniset ja organisatoriset toimenpiteet, jotka rekisterinpitäjän tulee vähintään toteuttaa ovat seuraavat:

- Henkilötietojen pseudonymisointi ja salaus
- Käsittelyjärjestelmien ja palveluiden vikasietoisuuden, käytettävyyden, eheyden ja luottamuksellisuuden takaus
- Tietojen saatavuuden ja niihin pääsyn nopea palautus fyysisen tai teknisen vian sattuessa sekä
- Teknisten ja organisatoristen menetelmien säännöllinen testaus, tutkimus ja arviointi, [1, artikla 32 kohta 1]

7.1 Kenttätason suojaus

Organisaation tietosuojan ja tietoturvan toteuttaminen alkaa kenttätasosta. Kenttätason suojaus sisältää organisaation toimitilojen sekä siellä sijaitsevien päätelaitteiden ja järjestelmien suojaamisen. Organisaation tulee harjoittaa pääsyn rajoittamista tiloihinsa, minkä avulla voidaan estää valtuuttamattomien henkilöiden pääsy henkilöstön työpisteille ja mahdollisesti henkilötietoihin. Jokaisen työntekijän ja vierailijan henkilöllisyys on myös syytä todentaa ja heidän toimintansa kirjata esimerkiksi lokeihin. Työntekijöiden käyttämät laitteet henkilötietojen käsittelyssä tulee turvata vähintään vahvalla salasanalla, niiden sisältämät henkilötiedot salattava ja ne on suotavaa kiinnittää työpisteisiin siihen tarkoitetulla kaapelilla varkauden estämiseksi. [18] Myös serverilaitteisto on hyvä kiinnittää paikoilleen kaapeleiden avulla ja sijoittaa lukittuun huoneeseen. Kaikki käsittelytoimissa käytettävät liikutettavat laitteet kuten ulkoiset kovalevyt, kannettavat tietokoneet ja USB-laitteet tulee suojata salauksella ja mahdollisuuksien mukaan kiinnitettävä työpisteille. Organisaatio voi käyttää esimerkiksi henkilötietojen keruuseen lukijoita tai kannettavia tietokoneita, joita on usein liikuteltava

työn sujuvuuden kannalta, eikä niiden kiinnitys työpisteille siksi ole edullista. Tällöin laitteet voidaan sijoittaa käytön jälkeen lukollisiin kaappeihin tai niihin tarkoitettuihin telakointiasemiin [18]. Laitteisiin voidaan asentaa hälytys- ja seurantaohjelmistoja varkauden varalta. Liikuteltavien laitteiden käytöstä on suotavaa pitää lokia, jotta tietoturvapoikkeamien tapahtuessa voidaan varmistua siitä, kenen hallussa laite on ollut.

7.1.1 Päätelaitteiden suojaus

Päätelaitteissa tai organisaation käyttämissä ohjelmistoissa ja palveluissa saattaa olla tietoturvaa vaarantavia puutteita tai haavoittuvuuksia, jotka rekisterinpitäjän on otettava huomioon riskianalyysiä ja vaikutustenarviointia tehdessään sekä toteuttaessaan riskitasoa vastaavia tietosuojan ja -turvan hallintatoimenpiteitä. Haavoittuvuuksista johtuvien tietoturvaloukkausten todennäköisyyttä voidaan usein pienentää suorittamalla säännöllisiä ohjelmisto- ja järjestelmäpäivityksiä sekä asentamalla haittaohjelmia ja hyökkäyksiä havaitsevia ja ehkäiseviä ohjelmistoja. Laitteiden, järjestelmien ja ohjelmistojen suorittaminen on suotavaa mahdollisuuksien mukaan eriyttää toisistaan, jotta mahdollisten tietoturvaloukkausten vahinko olisi mahdollisimman pieni. [25] Organisaation on myös hyvä poistaa verkkoympäristöstään laitteet, joilla ei ole käyttöä hyökkäyspinta-alan pienentämiseksi.

Jokaisella henkilöllä, jolla on valtuudet päästä käsiksi päätelaitteisiin ja järjestelmiin, tulee olla ainoastaan käsittelytoimissa tarvittavat välttämättömät oikeudet ja pääsy tietoihin. Kaikkien päätelaitteiden ja niitä käyttävien henkilöiden toimintaa organisaation verkkoympäristössä ja järjestelmissä on myös suotavaa seurata ja kirjata, eli organisaation kannattaa soveltaa AAA-protokollaa. AAA tulee sanoista authentication, authorization ja accounting eli käyttäjien todennus, heidän oikeuksien hallinta ja toiminnan seuraus. Todennuksella voidaan varmistaa, etteivät valtuuttamattomat henkilöt pääse kirjautumaan laitteille tai järjestelmiin. Oikeuksien hallinnalla määrätään tietyt oikeudet käyttäjälle tai käyttäjäryhmille, jolloin he eivät voi suorittaa oikeuksiaan ylittäviä toimia. Toiminnan seurauksella voidaan kerätä tietoa sekä seurata ja kirjata lokeihin käyttäjien, ohjelmistojen ja järjestelmien toimintaa sekä käytettyjä verkkoresursseja. [26]

Päätelaitteissa ja järjestelmissä käytettävien salasanan vahvuus riippuu sen pituudesta ja siinä käytetyistä erikoismerkkien määrästä. Salasanan minimipituuden suositus on kahdeksan merkkiä, mutta järjestelmän pääkäyttäjä voi asettaa salasanojen pituudesta

eri vaatimuksia. Pääkäyttäjän tai ylläpitäjän on myös kannattavaa asettaa rajoituksia siitä, kuinka usein työntekijöiden on vaihdettava salasanansa ja kuinka usein entisiä käytössä olleita salasanoja voidaan ottaa uudelleen käyttöön. Mahdollisia tietoturvaloukkauksia voidaan ehkäistä asettamalla raja sisäänkirjautumisyrityksille, jonka ylittäessä käyttäjä lukitaan ulos järjestelmästä, eikä hän voi yrittää kirjautua järjestelmään ennen tietyn määräajan päättymistä. Yrityksen tai organisaation henkilöstön tulee olla tietoinen tietojen kalastelusta, jonka avulla hyökkääjä voi pyrkiä saamaan haltuunsa esimerkiksi salasanoja. [27]

7.1.2 Internet of things -konsepti

IoT eli internet of things tarkoittaa konseptia, jossa laitteet tai melkein mikä tahansa esine on yhteydessä internetiin ja lähettää tietoa, vastaanottaa sitä tai tekee molempia verkon yli. Organisaatio voi esimerkiksi käyttää käsilukijoita tai mobiililaitteita henkilötietojen keräämiseen ja kerätyt tiedot lähetetään automaattisella prosessoinnilla henkilörekisteriin. Jos esimerkiksi henkilö ilmoittautuu tapahtumaan tai ostaa pääsylipun ennakkoon, hänelle voidaan lähettää QR-koodi, joka luetaan itse paikalla. Koodin lukeva laite lähettää automaattisesti tiedot henkilöstä verkon yli järjestelmään, jossa henkilön todennetaan saapuneen paikalle tai käyttäneen pääsylippunsa. Organisaation ulkopuolinen henkilö voi itse käyttää lukijaa tai työntekijä voi suorittaa QR-koodin luvun. Mikäli organisaation ulkopuolinen henkilö käyttää lukijaa, tulee rekisterinpitäjän varmistaa, ettei laite joudu ulkopuolisen henkilön haltuun. Rekisterinpitäjän tulee myös varmistaa, että lukija lähettää tiedot järjestelmään suojatun verkon yli.

7.2 Vikasietoisuus ja varmuuskopiointi

Järjestelmän, verkon, ohjelmiston tai laitteen vikasietoisuuden taso voidaan määrittää sen mukaan, miten onnistuneesti se pystyy muutoksesta tai viasta huolimatta toipumaan ja jatkamaan normaalia toimintaansa [28]. Vikasietoisuutta määritettäessä muutoksen tai vian odotetaan tapahtuvan ja sen todennäköisyys arvioidaan. Mikäli esimerkiksi järjestelmälle ei ole arvioitu tapahtuvan mitään normaalitoiminnasta poikkeavaa, vian sattuessa järjestelmä voi käyttäytyä odottamattomasti, eikä rekisterinpitäjä ole onnistunut takaamaan sen vikasietoisuutta. Järjestelmän sisältämät henkilötiedot voivat täten olla haavoittuvaisia ja tietoturvaloukkauksen sattuessa rekisterinpitäjä on rikkonut

asetusta. Jos järjestelmä, verkko, ohjelmisto tai laite pystyy vikatilanteessa varmistamaan, etteivät sen sisältämät tai käsittelemät tiedot vahingoitu, vääristy, häviä tai tuhoudu, sitä voidaan kutsua vikaturvalliseksi. Vikaturvallisuudella voidaan varmistaa henkilötietojen suoja poikkeustilanteissa, mutta palvelun tai järjestelmän palauttamista ei voida taata. [29] Vian tai muutoksen aiheuttaja on yleensä odottamaton tapahtuma, kuten hyökkäys tai sähkökatko.

Vikasietoisuutta ja vikaturvallisuutta voidaan lisätä suorittamalla vian todennäköisyyden tapahtumakohtainen arvio ennen järjestelmän, verkon, ohjelmiston tai laitteen käyttöönottoa ja tuntemalla sen haavoittuvuudet. Tällöin voidaan suunnitella ja soveltaa sopivat toimintamenetelmät ja tehdä esimerkiksi riittävät varmuuskopiot tarpeeksi ajoissa, jotta henkilötietojen käytettävyys saadaan palautettua poikkeustilanteessa. Varmuuskopioitavat tiedot kannattaa järjestää ja jäsennellä, jotta voidaan helposti varmistua siitä, että kaikki tarvittava tieto on varmuuskopioitu ja tarvittaviin tietoihin päästään käsiksi nopeasti. Varmuuskopioita on suotavaa mahdollisuuksien mukaan ja kustannukset huomioon ottaen tallentaa useampaan paikkaan. Organisaatio voi esimerkiksi hyödyntää pilvipalveluiden tarjoamaa tallennusta tai tallentaa tiedot paikallisesti. Mikäli henkilötietojen varmuuskopiointi tehdään paikallisesti organisaation laitteistolle, sen tulee olla irrallinen muusta laitteistosta, jota käytetään käsittelytoimissa. Jos käsittelytoimissa käytettyyn laitteistoon kohdistuu tietoturvapoikkeama, sen aiheuttamat riskit eivät tällöin vaikuta varmuuskopioutuihin tietoihin.

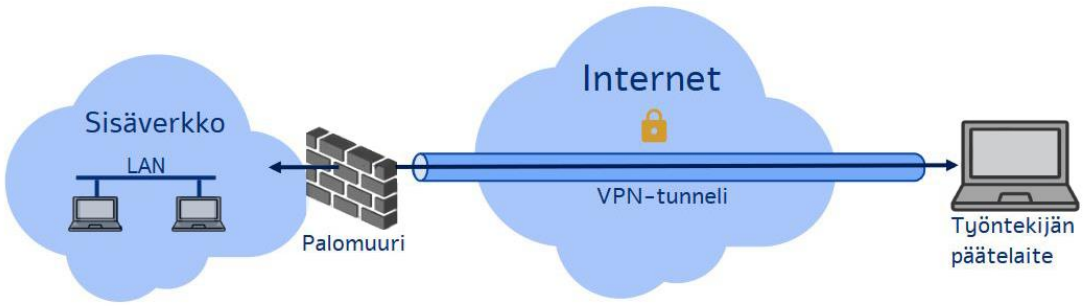
7.3 Sisäverkon turvaaminen

Sisäverkolla tarkoitetaan organisaation sisäistä, yksityistä verkkoympäristöä, johon ainoastaan organisaation henkilökunnalla on pääsy. Sisäverkko käsittää organisaation lähiverkot (engl. local area network, LAN), niiden ylläpitämiseen käytetyn laitteiston sekä siihen liittyvät palvelimet ja palvelut. Lähiverkko on ympäristö, jossa tietyllä rajatulla alueella sijaitsevat päätelaitteet ovat yhteydessä toisiinsa. Sisäverkko voi maantieteellisestä sijainnista riippumatta koostua useasta lähiverkosta. Organisaation sisäverkon lähiverkot on jaettu eri alueisiin, jotka tavallisesti toimivat eri toimipisteissä ja toimipisteiden verkkoympäristöt voidaan puolestaan jakaa toimintatarkoitusten perusteella eri aliverkkoihin. Mikäli mahdollista, organisaation kehitystoimet ovat suotavaa suorittaa aliverkossa, joka on tarkoitettu testiympäristöksi ja käsittelytoimet siihen tarkoitetussa erillisessä aliverkossa. Aliverkkoja käyttämällä organisaatio voi

hallinnoida resursseja tehokkaammin ja esimerkiksi haittaohjelmien vaikutuksen leviäminen organisaation koko sisäverkkoon voidaan ehkäistä. [25]

Sisäverkon yhteys ulkoverkkoon, kuten internetiin, sekä lähiverkkojen välinen yhteys on syytä turvata palomuureilla tai reitittimen pääsylistoilla (engl. access list, ACL). Palomuurille asetetaan tietyt säännöt, joiden perusteella se hallinnoi liikennettä sisäverkon ja ulkoverkon välillä ja monitoroi sitä. Palomuurin avulla voidaan siis ehkäistä hyökkäyksiä ja ulkopuolisten pääsyä organisaation sisäverkkoon ja minimoida hyökkäysten vaikutus verkkoympäristössä. Organisaation on suotavaa määrittää palomuuri sallimaan ainoastaan välttämätön tietoliikenne sisäverkon ja ulkoverkon välillä. Pääsylistojen tarkoituksena on suodattaa paketteja ja hallinnoida liikennettä tietyltä päätelaitteelta tai osoitteesta listasääntöjen avulla.

Usein suuri osa työskentelystä tapahtuu organisaation sisäverkon ulkopuolella etätyön kautta. Kun työntekijä ottaa etäyhteyden organisaation sisäverkkoon, työntekijän päätelaitteiden tietoturvallisuutta ei aina voida määrittää. Työntekijän päätelaitteen ja sisäverkon välillä kulkeva tietoliikenne tulee tällöin suojata käyttämällä VPN-yhteyttä (Kuva 2). VPN-yhteys salaa työntekijän päätelaitteen ja organisaation välillä kulkevan liikenteen ja voidaan naamioi työntekijän IP-osoitteen sekä sijainnin. Organisaation eri toimipisteiden välinen yhteys on myös hyvä suojata VPN-yhteydellä.



Kuva 2. Päätelaitteen VPN-yhteys organisaation sisäverkkoon.

7.4 Pseudonymisointi

Henkilötietojen pseudonymisoinnilla tarkoitetaan prosessia, jossa tiedot saatetaan sellaiseen muotoon, jossa niitä ei yksinään voida käyttää tietyn luonnollisen henkilön tunnistamiseen. Prosessissa henkilöön liittyviä tietoja erotetaan ja niitä säilytetään erillään toisistaan tai ne korvataan peitetiedoilla. Henkilön tunnistaminen tietojen perusteella tulee vaatia viittausta toisiin erotettuihin tietoaineistoihin. Siksi on tärkeää, että tietoihin sovelletaan suojaustoimenpiteitä, kuten salausmenetelmiä, joiden avulla voidaan estää tietojen yhdistäminen tunnistettavissa olevaan luonnolliseen henkilöön sekä luvaton pääsy tietoihin. Pseudonymisoidut tiedot ovat edelleen henkilötietoa ja niihin sovelletaan kaikkia asetuksen tietosuojasäännöksiä. [1, artikla 4 kohta 5]

7.5 Henkilötietojen salaus

Henkilötietojen salauksella tarkoitetaan niiden saattamista sellaiseen muotoon, jossa ne eivät ole luettavissa ilman niiden lukuun tarvittavia valtuuksia. Tietojen salaus ei ehkäise tietojen sieppausta, mutta tietojen joutuessa kolmannen osapuolen haltuun salauksen avulla voidaan estää mahdollinen tietoturvaloukkaus. Salaukseen käytetään algoritmeja, joiden avulla tiedot saatetaan salakirjoitukseksi joko symmetrisellä tai epäsymmetrisellä salauksella, jolloin tietoja ei voida lukea ilman avaimen käyttöä [30]. Salauksen vahvuuteen vaikuttaa muun muassa avaimen pituus. Vahvan salauksen avulla henkilötiedot voidaan muuttaa salakirjoitukseksi, joka ei ole murrettavissa millään tunnetulla hyökkäysmenetelmällä [31].

Symmetrisessä salauksessa käytetään yhtä yksityistä avainta tietojen salaukseen sekä purkuun. Koska tietoihin ei päästä käsiksi ilman salausavainta, tulee kaikilla valtuutetuilla käsittelytoimiin osallistuvilla osapuolilla olla avain hallussaan, jotta tietojen saavutettavuus ja käytettävyys säilyy. Kun avain luovutetaan valtuutetuille osapuolille, tulee sen luovutus tehdä suojatun yhteyden välityksellä. [32] Jos kolmas osapuoli saa avaimen haltuunsa, hän voi purkaa ja lukea salatut henkilötiedot.

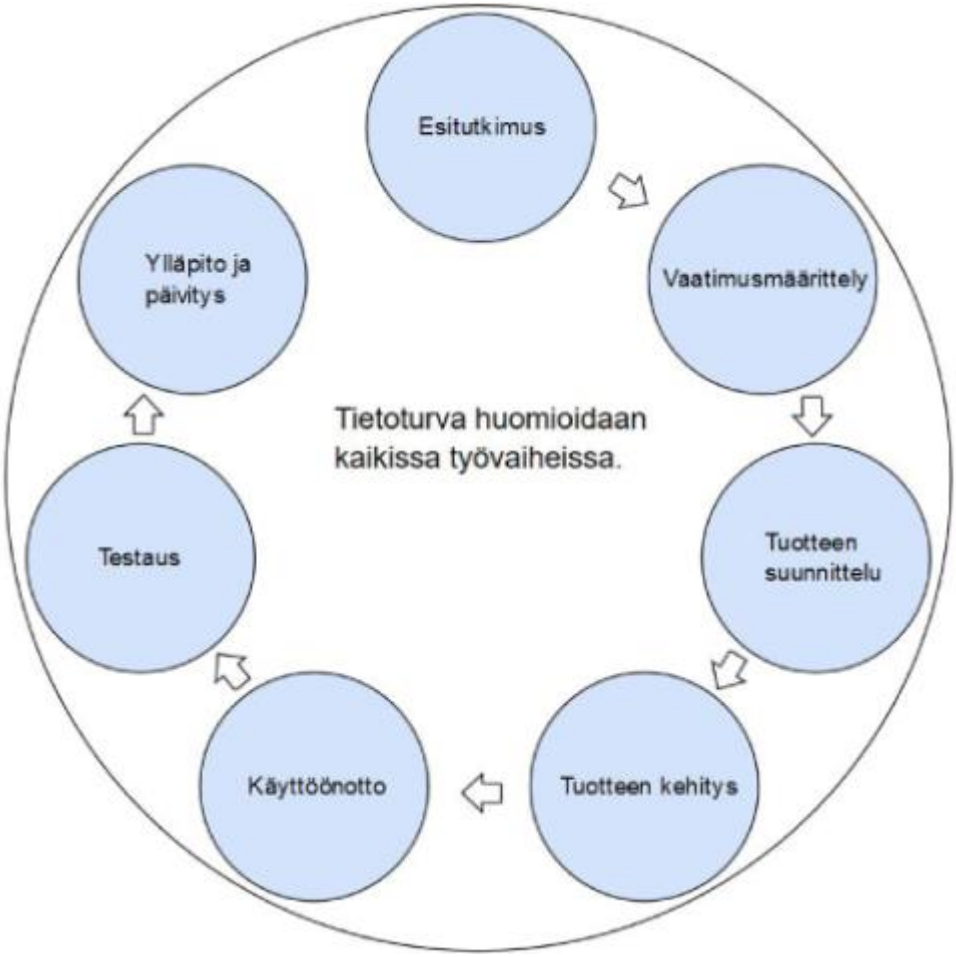
Epäsymmetrisessä salauksessa käytetään kahta avainta: yksityistä ja julkista. Julkista avainta käytetään tietojen salaamiseen ja ainoastaan siihen sopivaa yksityistä avainta voidaan käyttää niiden purkamiseen. Jos esimerkiksi tietoja halutaan lähettää verkon yli, lähettäjä salaa tiedot julkisella avaimella ja tiedot säilyvät salakirjoituksena, kunnes

niiden vastaanottaja purkaa ne omalla yksityisellä avaimellaan. Yksityistä avainta ei voida päätellä julkisesta avaimesta. Epäsymmetrinen salaus on selvästi symmetristä salausta yleisempi. [32]

Yrityksen tai organisaation tulee suorittaa avaintenhallintaa, jolla estetään salaisen avaimen vuotaminen valtuuttamattomille osapuolille. Vahvatkin salaukset voivat mitätöityä, jos hyökkääjä saa haltuunsa salaisen avaimen. Jos esimerkiksi avaimia säilytetään siirrettävällä medialla, laitteet tulee säilyttää turvallisessa paikassa, jossa valtuuttamattomilla henkilöillä ei ole niihin pääsyä. Kun henkilötietojen salausta ja avaimenhallintaa sovelletaan yhdessä, varmistetaan tietojen eheys ja luottamuksellisuus. Suomen julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, VAHTI, on julkaissut ohjeen salauskäytännöistä, jota yritys tai organisaatio voi henkilötietojen salausta toteuttaessaan hyödyntää. [31]

7.6 Tietosuoja sovellus- ja järjestelmäkehityksessä

Henkilötietojen käsittelyn tietosuoja ja tietoturva tulee huomioida sovellus- ja järjestelmäkehityksessä jokaisessa työvaiheessa (Kuva 3). Vaikutustenarviointi on hyvä ottaa osaksi kehitystä, jotta toteutuksen tietosuojan hallintamenetelmät vastaavat henkilötietoihin kohdistuvaa arvioitua riskitasoa. Sovellus- ja järjestelmäkehityksen aikana tietosuojavaatimuksia ja mahdollisia riskejä voidaan uudelleenarvioida ja tarvittaessa kirjata ne aikaisemmin laadittuun vaikutustenarviointiin. Tietoturvakäytännöt sisällytetään osaksi sovellusten ja järjestelmien ominaisuuksia. Myös mahdolliset tulevat muutokset tuotteessa tai tietoturvakäytännöissä tulee huomioida kehitysvaiheessa. Tietoturvan sisällyttäminen kehitysprosesseihin katsotaan usein hidastavan sovellus- ja järjestelmänkehitystä ja aiheuttavan tarpeettomia lisäkustannuksia, mutta tietoturvan huomioiminen projektin alussa tulee usein huomattavasti edullisemmaksi kuin sen toteuttaminen valmiissa tuotteessa. [19]



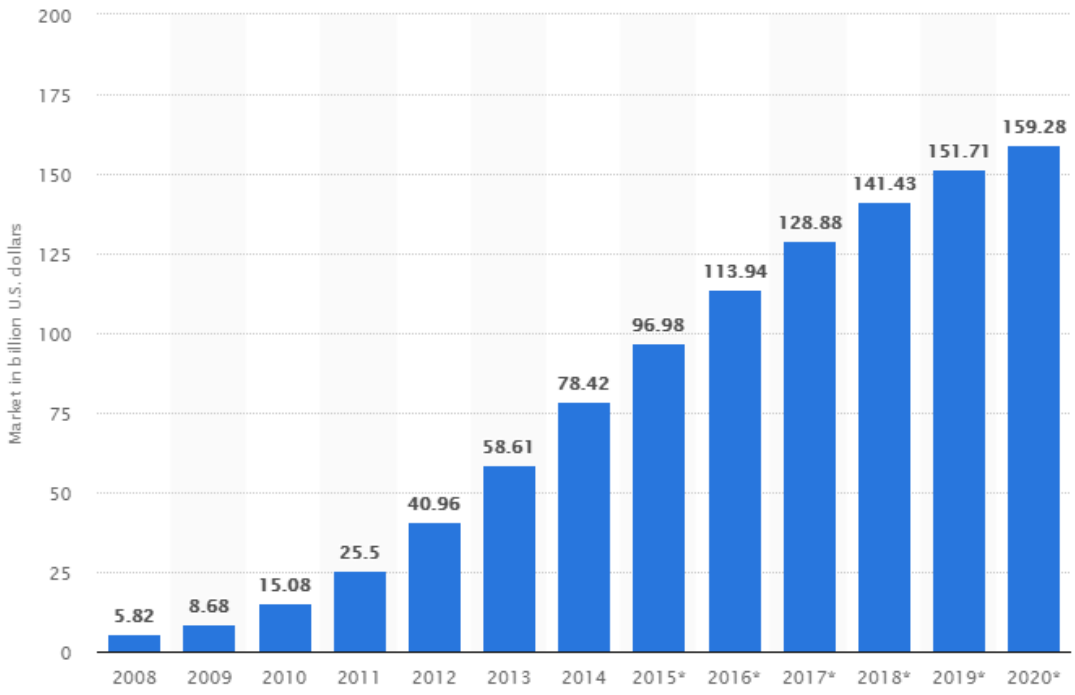
Kuva 3. Tietoturva kehitysprosessissa.

Riskitason pienentämiseksi yrityksen sovellus- ja järjestelmäkehityksestä vastaavien asiantuntijoiden tulee tietää parhaista voimassa olevista tietoturvakäytännöistä ja valittava tapauskohtaisesti soveltuvimmat hallintamenetelmät. Sovellus- ja järjestelmätestauksen avulla voidaan havaita hallintamenetelmien puutteellisuus tai virheellisyys. [33]

Jos sovellus- tai järjestelmäkehitys on ulkoistettu, rekisterinpitäjän tulee tehdä kehityksestä vastaavan osapuolen kanssa sopimus, jossa on määritelty tietosuojavaatimukset kehitysprosesseissa, joissa käsitellään henkilötietoja. Määritelmän tulee yksilöidä vaatimuksia sekä mahdollisuuksien mukaan hallintamenetelmiä, eikä se saa olla luonteeltaan liian suuripiirteinen. Mikäli rekisterinpitäjä hankkii tai ostaa henkilötietojen käsittelyssä käytettäviä ohjelmistoja, sovelluksia tai järjestelmiä ulkoiselta taholta, tulee tietosuojavaatimukset ottaa huomioon hankintavaiheessa tarjouspyynnössä. [19]

8 PILVIPALVELUTEKNOLOGIA

Pilvipalveluteknologia on yksi nopeimmin kasvavista IT-alan osa-alueista. Julkisten pilvipalveluiden käyttö on noussut tasaisesti vuodesta 2008 lähtien ja sen arvioitu markkinaosuus vuoteen 2020 mennessä on jopa 159,28 miljardia dollaria (Kuvio 1.). [34] Pilvipalveluteknologia tarjoaa yrityksille mahdollisuuden hyödyntää palveluita kuten tiedon tallennusta, verkkoympäristöjä, infrastruktuureja ja arkkitehtuuria sekä kehitysalustoja ilman merkittäviä rahallisia sijoituksia tai organisaation fyysisiä infrastruktuurin muutoksia. [35] Alkusijoitukset ja laajennukset kuten tallennustilan lisäys, uusien laitteiden hankita tai serverien ylläpito on usein kallista ja hidastaa etenkin pienten IT-alan yrityksien kasvua.



Kuvio 1. Julkisten pilvipalveluiden markkinaosuuden arvioitu kasvu 2008-2020. (Statista, 2018)

Uusi tietosuoja-asetus on kuitenkin tuonut mukanaan myös runsaasti haasteita yrityksille, jotka käyttävät pilvipalveluita henkilötietojen käsittelyyn. Rekisterinpitäjän on suositeltavaa tehdä pilvipalvelun tarjoajista kartoitus ja valita tarjoaja, joka toiminnallaan noudattaa tietosuoja-asetuksen asettamia velvoitteita. Pilvipalvelun tarjoajan valinta tulee ottaa huomioon organisaation arkkitehtuurisuunnittelussa ja -toteutuksessa sekä

tulevien projektien suunnitteluvaiheissa. Koska rekisterinpitäjän on vaikeampi hallita pilvipalveluissa sijaitsevia tietoja, rekisteröidyn luottamus tietojen turvallisuuteen saattaa olla heikko. Rekisteröidyillä on oikeus vastustaa henkilötietojensa käsittelyä pilvipalveluissa [1, artikla 15 kohta 1 & 2].

8.1 Tietojen tallentaminen pilvipalvelussa

Koska tietosuoja-asetus määrittää, että käsiteltävien henkilötietojen sijainti sekä käsittelytavat tulevat olla rekisterinpitäjän ja henkilötietojen käsittelijän tiedossa [1, artikla 30], [1, artikla 32], yksi suurimmista haasteista yrityksille on tietää henkilötietojen tarkka maantieteellinen sijainti pilvipalvelussa ja niiden tietosuojan takaaminen. Henkilötietoja siirtyy usein pilvipalveluiden kautta toiseen maahan, eikä niiden olinpaikka ole aina selkeä. Pilvipalveluita käytetään verkon yli ja kun esimerkiksi henkilötietoja tallennetaan pilvipalvelussa, se tallentuu organisaation ulkopuolisiin datakeskuksiin. Yksi pilvipalvelutarjoaja ei pysty tarjoamaan kaikkia palveluita, joten tarjoajat tekevät usein yhteistyötä ja jakavat resursseja keskenään [36]. Tällöin keskukset ovat usein joko yhden tai useamman palveluntarjoajan omistuksessa [36]. Varmuus siitä, missä tai kuinka monessa datakeskuksessa henkilötiedot sijaitsevat, voi tällöin olla erittäin haastavaa tai joissakin tilanteissa mahdotonta. Jotkin pilvipalveluiden ylläpitäjät tarjoavat kuitenkin mahdollisuuden asiakkaalle valita EU:n sisällä sijaitsevan datakeskuksen, jossa tietoja säilytetään. Ne voivat myös tarjota työkaluja, joiden avulla henkilötietojen sijaintia voidaan seurata. Mikäli pilvipalvelun tarjoaja ei kuulu Privacy Shield -järjestelmään tai Euroopan komission hyväksymiin maihin, on EU:n kansalaisen henkilötietojen käsittely näiden palveluiden kautta kielletty [1, artikla 45 kohta 1]. Kun henkilötiedot sijaitsevat organisaation ulkopuolella, vastuu tietosuoja-asetuksen noudattamisesta ja henkilötietojen suojauksesta on ensisijaisesti rekisterinpitäjällä ja henkilötietojen käsittelijällä [37]. Organisaation rekisterinpitäjän ja henkilötietojen käsittelijän on valittava pilvipalvelun tarjoaja, joka pystyy osoittamaan noudattavansa tietosuoja-asetuksen velvoitteita ja toteuttaa läpinäkyvyysperiaatetta. Kun henkilötietoa käsitellään asetusta noudattavassa palvelussa, palvelun tarjoaja toimii myös henkilötietojen käsittelijänä [37].

8.2 Tietoturvaloukkaus pilvipalvelussa

Pilvipalveluteknologian kasvavan markkinaosuuden myötä myös siihen kohdistuvien hyökkäyksien riskit kasvavat. Kun uusia palveluita kehitetään, niihin liittyvät hyökkäyspinta-alat ja haavoittuvuuksien mahdollisuudet suurenevat. Pilvipalveluiden ylläpitoon käytettävän arkkitehtuurin monimutkaisuudesta ja jatkuvasta yhteydestä ulkoverkkoon johtuen hyökkäyksien hallinta ja niiden leviämisen estäminen palvelussa ovat suuria haasteita pilvipalveluteknologiassa. Rekisterinpitäjällä ei ole merkittäviä toimintavaltuuksia hyökkäysten hallintaan, eikä hän usein saa läpinäkyvästi tietoa pilvipalvelun tarjoajalta tietoturvaloukkauksen tapahtuessa ilman erillistä sopimusta. Useat pilvipalvelun tarjoajat tekevät yhteistyötä varmistaakseen henkilötietojen eheyden, saatavuuden, käytettävyyden ja luottamuksellisuuden.

Rekisterinpitäjän on suositeltavaa laatia pilvipalvelun tarjoajan kanssa sopimus, jossa on määritelty mitä tietoturvaloukkauksella tarkoitetaan, miten loukkauksen tapahtuessa menetellään ja mitä menetelmiä palvelun tarjoaja soveltaa ehkäistäkseen mahdollisia loukkauksia. Tietoturvaloukkauksen tapahtuessa valvontaviranomainen tutkii rekisterinpitäjän toimia ja voi vaatia henkilötietojen käsittelystä selosteen sekä tietovirtakuvauksen. [37] Rekisterinpitäjä on siis suotavaa seurata ja dokumentoida henkilötietojen sijainti säännöllisesti. Rekisterinpitäjää tai pilvipalvelun tarjoajaa ei rangaista tietoturvapoikkeamista tai -loukkauksista, jos he voivat osoittaa noudattaneensa asetusta ja toteuttaneensa toimenpiteitä henkilötietojen suojaamiseksi välittömästi sekä ilmoittavat poikkeamasta tai loukkauksesta valvontaviranomaiselle ilman aiheetonta viivytystä. Jos rekisterinpitäjä on käsitellyt henkilötietoja pilvipalvelussa, joka sijaitsee EU:n alueen ulkopuolella, eikä kuulu Euroopan komission hyväksymiin maihin tai Privacy Shield -järjestelmään tai ei noudata tietosuoja- asetuksen velvoitteita, on rekisterinpitäjä rikkonut asetusta. [1, artikla 45 kohta 1]

9 YHTEENVETO

Opinnäytetyön tavoite oli selvittää, miten EU:n yleisen tietosuoja-asetuksen asettamat tietoturvan ja tietosuojan velvoitteet vaikuttavat yrityksiin sekä miten rekisteröidyn oikeudet toteutetaan käytännössä. Työssä selvitettiin myös, mitä seurauksia tietosuojan ja tietoturvan laiminlyönnillä voi olla sekä rekisterinpitäjälle että rekisteröidylle.

Tietosuoja-asetuksen tulkinta oli sen yleisluonteisuuden takia haastavaa. Asetuksen asettamista tietoturvan ja tietosuojan velvoitteista onnistuttiin kuitenkin määrittelemään konkreettisia teknisiä ja organisatorisia menetelmiä, jotka toteuttamalla rekisterinpitäjät noudattavat asetuksen vähimmäisvaatimuksia henkilötietojen tietosuojasta ja tietoturvasta. Menetelmien tärkein tarkoitus on ehkäistä henkilötietoihin kohdistuvia tietoturvaloukkauksia. Tietoturvakäytäntöjä tutkimalla selvitettiin, että dokumentoinnilla, henkilötietojen salauksella, päätelaitteiden suojauksella, henkilöstön koulutuksella sekä sisäverkon turvaamisella voidaan huomattavasti vähentää henkilötietoihin kohdistuvien uhkien määrää. Yrityksien tulee arvioida henkilötietoihin kohdistuvat riskit tapauskohtaisesti ja toteuttaa riskejä vastaavat toimenpiteet. Koska tietosuoja-asetuksessa määrätään, että rekisterinpitäjän on aina taattava henkilötietojen suoja, voitiin todeta, että myös pilvipalvelussa sijaitsevat tiedot ovat rekisterinpitäjän vastuulla. Huomattiin, että henkilötietojen siirtymistä voidaan selvittää tietovirtakuvauksilla.

Tietoturvapoikkeamien ja tietoturvaloukkausten ehkäisemistä ja hallintaa ei aina oteta huomioon verkkoympäristön suunnittelussa kustannussyistä, mutta tietosuoja-asetuksen myötä henkilötietoa käsittelevät yritykset ja organisaatiot eivät voi enää sivuuttaa näiden laiminlyömisestä johtuvia mahdollisia seurauksia. Mediassa selvästi keskustelluin seuraus on yritykselle tai organisaatiolle mahdollisesti määrättävien sakkojen suuruus, mutta tietosuoja-asetusta tutkimalla huomattiin, että maksimisakkojen saaminen on erittäin epätodennäköistä ja esimerkiksi käsittelytoimien keskeyttäminen on usein yrityksen tai organisaation toiminnalle tuhoisampaa.

Yrityksien on jatkuvasti tarkistettava ja päivitettävä tietosuojakäytäntönsä. Pilvipalveluteknologian kehittyessä ja käsiteltävien henkilötietojen määrän lisääntyessä myös mahdollisten uhkien määrät kasvavat ja muuttuvat. Jatkotutkimuksena voitaisiin selvittää, miten yrityksen sisäisiin järjestelmiin voidaan implementoida tietoturvakäytäntöjä ja miten henkilötietoja suojataan, kun yritys käyttää pilvipalvelussa sijaitsevaa kehitysalustaa.

LÄHTEET

[1] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Annettu 27.4.2016. Saatavilla https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL

[2] Pauliina Hirvonen, Citrus Oy, ICT Tietoturvapäivä 7.3.2017

[3] Oikeusministeriö, Uusi tietosuojalaki voimaan vuoden 2019 alusta, 2018. Viitattu 8.4.2019. https://oikeusministerio.fi/artikkeli/-/asset_publisher/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta

[4] Eduskunta, EU:n tietosuojadirektiivin täytäntöönpano, 2018. Viitattu 8.4.2019. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/EUn-tietosuojauudistus/Sivut/EUn-tietosuojadirektiivi.aspx

[5] Valtiovarainministeriö, Henkilöstön tietoturvaohje, 2013. S.17. ISSN 1798-0860 (sähköinen). https://www.vahtiohje.fi/c/document_library/get_file?uuid=ce1ccede-8669-4166-b084-9cafbe6e1e60&groupId=10229

[6] Sanastokeskus TSK, TEPA Term Bank. Viitattu 12.4.2019. http://www.tsk.fi/tepa/en/search/tietoturva

[7] Tietosuojavaltuutetun toimisto, Organisaatioille. Viitattu 23.8.2018. https://tietosuoja.fi/organisaatiot

[8] Elinkeinoelämän keskusliitto EK, Tietopaketti yrityksille: EU:n yleinen tietosuoja-asetus ja tietosuojalaki. Viitattu 2.4.2019. https://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen/

[9] Euroopan komissio, Kuinka kauan tietoja voidaan säilyttää ja pitääkö niitä päivittää?. Viitattu 9.4.2019.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_fi

[10] Viestintäviraston kyberturvallisuuskeskus, Evästeiden turvallinen käyttö, 2018. Viitattu 2.9.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet/palveluidenturvallinenkaytto/evasteet.html

[11] Euroopan komissio. Lehdistötiedote Bryssel 12. heinäkuuta 2016, 2016. Viitattu 8.2.2019. http://europa.eu/rapid/press-release_IP-16-2461_fi.htm

[12] Euroopan komissio. Adequacy decisions. Viitattu 13.2.2019. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

[13] Privacy Shield Framework, Privacy Shield Overview. Viitattu 14.3.2019. https://www.privacyshield.gov/Program-Overview

[14] Euroopan komissio, EU-U.S. Privacy Shield, 2016. Viitattu 20.3.2019. https://ec.europa.eu/info/sites/info/files/factsheet_eu-us_privacy_shield_en.pdf

[15] Tietosuojamalli, Rekisteröidyn oikeudet. Viitattu 8.11.2018. https://fakta.tietosuojamalli.fi/kategoria/rekisteroidyn-oikeudet

[16] Tietosuojavaltuutetun toimisto, Yksityishenkilöille. Viitattu 8.12.2018. https://tietosuoja.fi/yksityishenkilot

[17] Iablogi, Tietosuoja-asetuksen mukainen siirto-oikeus – mitä se tarkoittaa?, 2017. Viitattu 4.4.2019. https://www.iab.fi/iablogi/2017-postaukset/iablogi/tietosuoja-asetuksen-mukainen-siirto-oikeus-mita-se-tarkoittaa.html

[18] Gambrel, B. (toim.), *Microsoft Official Academic Course, Security Fundamentals*. USA: John Wiley & Sons, Inc., 2012. S. 4-12, ISBN 978-0-470-90184-7 (sähköinen).

[19] Valtiovarainministeriö, EU-tietosuojan kokonaisuudistus, 2016. S. 19, 21, 23. ISSN 1798-0860 (sähköinen). https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

[20] Minilex, Aineellinen ja aineeton vahinko. Viitattu 12.4.2019.
https://www.minilex.fi/a/aineellinen-ja-aineeton-vahinko

[21] Tietosuojatyöryhmä, Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta, 2017. S. 7, 12-13, 21. Viitattu 6.4.2019.
https://tietosuoja.fi/documents/6927448/8316711/Tietoturvaloukkauksen+ilmoittaminen+fi/9c0f2f46-33b1-4b01-9a50-9320d59bd605/Tietoturvaloukkauksen+ilmoittaminen+fi.pdf

[22] Asianajotoimisto Lukander Ruohola HTO, EU:n tietosuoja-asetus. Viitattu 6.4.2019.
https://tietosuoja.info/

[23] Ibrahim, R. & Yen Yen, S. A Formal Model for Data Flow Diagram Rules, 2011. vol. 1:2. S. 60-63. Viitattu 2.4.2019.
http://scientific-journals.org/archive/vol1no2/vol1no2_3.pdf

[24] Bangerter, J. Data Flow Diagram Symbols, Types and Tips, 2017. Viitattu 2.4.2019.
https://www.lucidchart.com/blog/data-flow-diagram-tutorial

[25] Valtiovarainministeriö, Päätelaitteiden tietoturvaohje, 2013. S. 21, 35. ISSN 1798-0860 (sähköinen)
https://www.vahtiohje.fi/c/document_library/get_file?uuid=b1064d7a-83e5-4246-be9a-a8a84c8caaa0&groupId=10229

[26] Cisco, Cisco IOS Security Configuration Guide. Viitattu 16.4.2019.
https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfaaa.pdf

[27] Cisco, Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS Release 15SY, 2015. Viitattu 15.4.2019.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-aaa-comm-criteria-pwd.html

[28] Tieteen termipankki. Viitattu 15.4.2019.
http://tieteentermipankki.fi/wiki/Nimitys:vikasietoisuus

[29] Gegick, M & Barnum, S., *Failing Securely*, 2005. Viitattu 16.4.2019. https://www.us-cert.gov/bsi/articles/knowledge/principles/failing-securely

[30] Goldreich, O., *Foundations of Cryptography: Volume 2, Basic Applications,* US: Cambridge University Press, 2004. vol. 2. S. 375, ISBN 0-521-83084-2 (sähköinen).

[31] Valtiovarainministeriö, Ohje salauskäytännöistä, 2015. S. 22. ISSN 1797-9714 (sähköinen). https://www.vahtiohje.fi/c/document_library/get_file?uuid=8e28cd10-2e1e-4bd5-b6f1-f75a1fec2f5d&groupId=10229

[32] IBM Knowledge Center, Security Concepts. Viitattu 13.4.2019. https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/seccon.html

[33] Valtiovarainministeriö, Sovelluskehityksen tietoturvaohje, 2013 S. 57. ISSN 1798-0860 (sähköinen). https://www.vahtiohje.fi/c/document_library/get_file?uuid=03c32520-f3f8-4621-b0d4-ec4ca8edafb3&groupId=10128&groupId=10229

[34] Statista, Total size of the public cloud computing market from 2008 to 2020 (in billion U.S. dollars). Viitattu 29.4.2019.

[35] Kuyoro, S.O, Ibikunle, F. & Awodele, O. Cloud Computing Security Issues and Challenges, 2011. S. 247. vol.3:5. http://eprints.lmu.edu.ng/1390/1/Cloud%20Computing%20Security%20Issues%20and%20Challenges.pdf

[36] Frahim, J., Josyula, V., Morrow, M.J. & Owens, K. *Intercloud: Solving Interoperability and Communication in a Cloud of Clouds.* USA: Cisco Press, 2016. S.30-31, ISBN-13: 978-1-58714-445-5.

[37] The Duke Perspective, Compliance for Cloud Computing following the GDPR in 2018, 2018. Viitattu 2.3.2019. https://sites.duke.edu/perspective/2018/10/03/compliance-for-cloud-computing-following-the-gdpr-in-2018/

LIITTEET

Liite 1. Vuokaavio tietoturvaloukkauksen ilmoitusvaatimuksista (Tietosuojatyöryhmä 2017).