Aleksi Jylhä

TIETOTURVAKOULUTUKSEN SUUNNITTELU TOIMEKSIANTAJALLE

Opinnäytetyö

Tradenomi (AMK)

Liiketalouden koulutus

2023

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Tradenomi (AMK)
Tekijä/Tekijät	Aleksi Jylhä
Työn nimi	Tietoturvakoulutuksen suunnittelu toimeksiantajalle
Toimeksiantaja	Digia Oy
Vuosi	2023
Sivut	52 sivua, liitteitä 1 sivu
Työn ohjaaja(t)	Mirka Loponen

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli auttaa toimeksiantajaa laatimaan kaupallisesti painottuvaa tietoturvakoulutusohjelmaa suunnittelemalla sisältöä, jossa painotetaan tietosuojaa ja siihen liittyvää lainsäädäntöä. Toimeksiantaja ei ollut aiemmin tarjonnut verkkokoulutusta asiakkailleen, ja opinnäytetyön tarkoituksena oli laatia suunnitelma tällaisen koulutuksen suunnittelua varten.

Produktiivinen tutkimus koostuu kahdesta osasta. Ensimmäinen osa on teoriapohja ja toinen osa on produktio, joka on käytännön työn tulos, tässä tapauksessa tietoturvakoulutussuunnitelma.

Opinnäytetyössä keskityttiin erityisesti lainsäädännölliseen näkökulmaan, mutta suunnitelmaan sisällytettiin paljon tietoturvaa koskevaa materiaalia, jotta se olisi mahdollisimman toimiva.

Toimeksiantajan tavoitteena on hyödyntää opinnäytetyön sisältöä sähköisen koulutusalustan toteuttamisessa. Tässä työssä esitettyä alustavaa koulutussuunnitelmaa pidettiin hyvänä lähtökohtana kohti kaupallista versiota. Suunnitelman keskeneräisyyden vuoksi opinnäytetyössä esitetään kuitenkin vain sen sisällysluettelo.

Asiasanat: tietosuoja, GDPR, tietosuojakoulutus, tietoturvakoulutus, lakisääntö

South-Eastern Finland University of Applied Sciences

Degree	Bachelor of Business Administration
Author (authors)	Aleksi Jylhä
Thesis title	Designing security training for the commissioner
Commissioned by	Digia Oy
Time	2023
Pages	52 pages, 1 appendix page
Supervisor	Mirka Loponen

ABSTRACT

The aim of the thesis was to help the commissioner to prepare a commercially oriented information security training program by designing content with an emphasis on data protection and related legislation. The commissioner had not previously offered online training to its customers, and the purpose of the thesis was to provide a plan for the design of such training.

This practice-based study consists of two parts. The first part is the theoretical basis, and the second part is the security training plan.

The thesis focused particularly on the legislative aspect, but a great deal of material on information security was included for the plan to be effective.

The commissioner aims to utilize the content of the thesis to implement the e-learning platform. The preliminary training plan presented in this study was considered a good starting point towards a commercial version. However, due to its unfinished status, only the table of contents of the plan will be presented in the thesis.

Keywords: data protection, GDPR, data security training, legislation

SISÄLLYS

1 JOHDANTO

Nykypäivänä digitaalisessa muodossa olevaa tietoa on saatavilla valtava määrä. Tietosuojalainsäädännön implementoinnilla organisaatiot kykenevät luomaan enemmän varmuutta organisaatiotasolla palvellakseen asiakkaitansa laadukkaammin. Suurten tietoaineistomäärien säilyttäminen ja hallinta kuitenkin vaatii organisaatioilta paljon resursseja suojatoimenpiteisiin, jonka takia tarvitaan myös paljon intoa jatkuvalle lainsäädännön omaksumiselle. (Keller 2023, 23–24, 78.) Kyberhyökkäyksiä vastaan organisaatioiden on osattava tarjota aktiivisesti henkilökunnallensa tietoturvakoulutuksia ja -ohjeistuksia, joiden avulla he ovat kykeneväisiä estämään tietoturvaloukkauksia. Ilman toimivaa ohjeistusta ja koulutusta on vaarana inhimillinen virhe, jota ei voida edes estää teknisin ratkaisuin. Organisaatioiden tuleekin ohjata työntekijöitä toimimaan turvallisesti käsitellessään valtavia määriä tietoja. (Pulkkanen 2021.)

Tämä opinnäytetyö käsittelee tietoturvakoulutuksen suunnittelua ja toteutusta toimeksiantajalle Digia Oyj -yhtiölle. Vaikka kyseessä on ohjelmisto- ja palveluyritys, joka tarjoaa asiakkaillensa konsultointia ja tukea eri tavoin liiketoiminnassa, puuttuu kuitenkin yhtiöltä verkkokoulutusmahdollisuudet. Joten yhteistyössä Digian ja verkkokoulutusalustan valmistajan kanssa on asetettu tavoitteeksi toteuttaa kaupalliseen käyttöön tarkoitettu tietoturvakoulutus tietoturvakoulutussuunnitelman avulla.

Toukokuussa 2018 voimaan astunut EU:n yleinen tietosuoja-asetus (GDPR) on tänä päivänäkin vahvasti läsnä oleva tekijä sekä organisaation että luonnollisten henkilöiden toiminnassa. Asetuksella pyritään suojaamaan ihmisten yksityisyyden suojaa määrittelemällä henkilötiedon ja ohjeistetaan organisaatiot toimimaan oikeaoppisesti lain puitteissa mahdollisten sanktioiden uhan avulla. Viiden vuoden sisään mahtuu jo suurehko määrä esimerkkitapauksia, joista viimeisin on tietosuojavaltuutetun toimiston seuraamuskollegion antama 440 000 euron suuruinen hallinnollinen seuraamusmaksu yritykselle seurauksena siitä, että laiminlyötiin tietoisesti määräystä korjaavista toimenpiteistä (Suomen Asiakastiedolle seuraamusmaksu… 2023).

Koulutussuunnitelman tavoitteena on luoda Digian asiakkaille helppolukuinen tietoturvakoulutus. Oppimisen helpottamiseksi koulutusta suunnitellaan koulutusmoduulin muodossa. Koulutusmoduuli toimii kantaluokkana tietoturvaopintorakenteen eri osille, joissa opintokokonaisuus koostuu pääopintojaksojen lisäksi pienemmistä opintokokonaisuuksista. Moduulin avulla saadaan Digian asiakkaille siten paloiteltua GDPR-asetuksen, Suomen lainsäädännön ja ISO 27001 -standardin sisältö pienempiin helppolukuisiin koulutusosioihin.

Opinnäytetyön tietoperusta koostuu Digian sisäisistä koulutuksista ja ohjeistuksista, valtionvarainministeriön VAHTI-ohjeista, Suomen lainsäädännön, EU:n yleisen tietosuoja-asetuksen, NIS2-direktiivin sekä ISO 27001-standardin materiaalista. Koulutustaustan takia koulutussuunnitelman näkökulmana on lainsäädäntö, asetukset, direktiivit ja niitä koskevat eri standardit ja käytännöt opinnäytetyön toteuttamiseksi.

Kiinnostus kyseiseen opinnäytetyöaiheeseen syntyi edellisen toimeksiantajan harjoitteluajanjakson aikana. Harjoittelussa työstettiin samanaikaisesti useampaa projektia, sillä tietosuoja ja -turvakoulutuksen suunnittelu oli osa toteutetuista projekteista, joten opinnäytetyön valinta on ollut helppo, kun kyseistä projektia tarjoava toimeksiantaja tulee vastaan.

1.1 Toimeksiantajan esittely

Toimeksiantajana toimii Digia Oyj, joka on ohjelmisto- ja palveluyritys. Yhtiön jatkuvana tavoitteena on yhdistää teknologian mahdollisuudet ja ihmisten kyvykkyydet älykkäämmän liiketoiminnan ja yhteiskunnan sekä kestävän tulevaisuuden rakentamiseksi. Atk-laitteiston ja ohjelmistokonsultoinnin toimialalla toimivan yhtiön keskeisenä vahvuutena on kattava osaaminen, joka ulottuu konsultoinnista digitaalisiin palveluihin, liiketoiminnan ydinjärjestelmiin ja datan hyödyntämisen ratkaisuihin. (Digia Oyj 2023.)

Yhtiön pääkonttori sijaitsee Helsingissä, ja muut toimisteet ovat Tampereella, Jyväskylässä, Turussa, Joensuussa, Raumalla, Oulussa, Vaasassa, Lahdessa ja Kuopiossa sekä Tukholmassa. Yhtiön tytäryhtiön toimintaa löytyy Ruotsin ja Suomen lisäksi myös Alankomaissa. Jatkuvasti kehittyvälle yhtiölle

työskentelee nykyään ympäri Suomea yli tuhat neljäsataa (1400) ”digialaista”. (Digia Oyj 2023.)

Nykyinen Digia Oyj sai alkunsa 1990 perustetusta SysOpen Oyj nimisestä yrityksestä, sekä vuonna 1997 perustetusta Digia Oy:stä. Nämä yhdistyivät 2005 SysOpen Digia Oyj:ksi. Vuosina 2005–2006 yhdistyneeseen yritykseen liitettiin yrityskaupoilla Yomi Software Oy, Samstock Oy sekä Sentera Oyj. SysOpen Digia muutti nimensä jälleen vuonna 2008 Digiaksi. Jatkuvasti kehittyvä yritys koki voimakkaita murroksia vuosina 2011–2012, kun silloinen yhteistyökumppani Nokia uudisti liiketoiminstrategiansa ja myi Digialle Qt-liiketoiminnan. Digia jakautui vuonna 2016 siten, että kaikki sen Qt-liiketoimintaan liittyvät varat, velat ja vastuut siirtyvät jakautumisesta syntyvälle Qt Group Oyj yhtiölle. Qt-jakautumisen jälkeen yhtiö uudisti strategiansa ja koki jatkuvaa uudistusta sen myötä. Jatkuvasti maailmanmarkkinoilla kehittyvä Digia Oyj on laajentanut toimintaa useaan eri maahan. (Digia Oyj 2023.) Yhtiö on listattuna Nasdaq Helsingissä (Nasdaq 2023). Digia Oyj tuotti vuonna 2022 liikevaihtoa 170,8 miljoonaa, liikevoittoa 12,7 miljoonaa euroa ja tilikauden tulos oli 9,5 prosenttia (Kauppalehti 2023).

1.2 Tutkimusmenetelmän valinta

Koulutussuunnitelmaa ajatellen vain toiminnallinen opinnäytetyö oli vaihtoehtona. Toiminnallinen opinnäytetyö keskittyy enemmän käytännön näkökulmasta työelämän kehitykseen, kun vertaa muihin tarjolla oleviin tutkimusmenetelmiin. Toiminnalliseen opinnäytetyöhön sisältyy teoriaosuuden lisäksi produktiosuus, joka syntyi toimeksiantajan toiveesta toteuttaa kyseinen projekti. Toiminnallisessa opinnäytetyössä tutkimuksellinen osio toimii tiedonhankinnan yhtenä tärkeimpänä apuvälineenä ja on tukena produktiosuudelle. (Vilkka & Airaksinen 2003, 9, 56–60.)

2 TIETOSUOJA YLEISESTI

Euroopan unionin perusoikeuskirjan 8. artikla määrittelee jokaisen oikeutetuksi henkilötietojensa suojaan. Perusoikeussuojaa vahvistetaan lainsäädännöllä, jotta voidaan turvata rekisteröityjen oikeuksien ja vapauksien toteutuminen henkilötietojen käsittelyssä. (Euroopan unionin perusoikeuskirja 2000.) Tietosuojan avulla tarkennetaan, milloin ja millä edellytyksin henkilötietoja voidaan

käsitellä. Tiedonkäsittelyä on toteutettava asianmukaisella tavalla niin, että toiminta perustuu lainmukaiseen tarkoitukseen, ja sen on suoritettava asianomaisen suostumuksen tai muun laissa säädetyn oikeuttavan perusteen pohjalta. Jokaisella on oikeus tutustua itseään koskeviin tietoihin, ja hänellä on oikeus vaatia tietojen muuttamista, poistamista ja oikaisemista. (Tietosuojavaltuutetun toimisto s.a.) Lainsäädännöllä määritellään, kuinka tietosuojaa voidaan toteuttaa, ja tietoturvalla tavoitellaan tapoja, joilla turvataan jokaisen yksilön henkilötiedot. Kun maailma verkottuu ja yritysten toiminta digitalisoituu, tieto on merkitykseltään raaka-aine yrityksille ja organisaatioille. Lainsäädännön myötä jokaisella yrityksellä ja organisaatiolla on yhä suurempi vastuu tiedonkäsittelyssä. (Data ja analytiikka 2023.)

2.1 EU:n tietosuoja-asetus ja muu lainsäädäntö

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, toisin sanoen Euroopan unionin yleinen tietosuoja-asetus astui voimaan 25. päivä toukokuuta 2018, ja se määritteli uuden alun tietosuojauksen toteutumiselle. Asetusta voidaan soveltaa sellaisenaan, ja siksi kyseessä ei ole maakohtainen lakipakko. Asetuksella pyritään varjelemaan luonnollisten henkilöiden henkilötietojen käsittelyä sekä määritellään asetuksen koskevan 2. sekä 3. artiklan nojalla kaikkia unionin alueella lainsäädäntöä koskevia tahoja riippumatta siitä, missä päin maailmaa unionin olevia henkilötietoja käsitellään. Asetusta ei sovelleta luonnollisten henkilöiden kohdalla, kun kyseessä on yksinomaan henkilökohtainen tai kotitalouttaan koskeva toiminta, eikä sitä sovelleta rikostoiminnan ennaltaehkäisevien viranomaisten toiminnassa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 2.–3. artikla.)

Suomessa jo 1990-luvulta lähtien on pyritty huolehtimaan yksityisyyden suojasta ja niitä koskevista perusoikeuksista. Vuonna 2019 astui voimaan uusi tietosuojalaki, joka kumosi tietosuojalain 37. §:n nojalla henkilötietolain sekä tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain. (Tietosuojalaki 5.12.2018/1050, 6. luku 37. §.) Tietosuojalaki spesifioi vuonna 2018 julkaistua Euroopan unionin yleistä tietosuoja-asetusta ja täydentää asetuksen kansallista soveltamista. (Tietosuojalaki, 1. luku 2. § mom. 1.) Lisäksi tietosuojalaissa säädetään viranomaisen nimittämisestä ja organisaatiosta sekä sen toimivaltuuksista. (Tietosuojalaki s.a.)

Tietosuojalainsäädännön ja tietosuoja-asetuksen lisäksi Suomessa on voimassa henkilötietojen käsittelyä koskeva erityislainsäädäntö. Erityislainsäädännöllä rajataan viranomaisten henkilötietojen käsittelyä sääntelemällä tarkemmaksi käsittelyä jossakin toiminnassa tai määrittelemällä, miten henkilötietoja on sallittu käsitellä yleislaista poiketen. Erityislainsäädäntö on jaettu useampiin säädöksiin, jotka käsittelevät yhteiskunnan henkilörekistereitä sekä säädöksiä tiettyyn toimialaan liittyvistä henkilötietojen käsittelyistä, kuten luottotietolaki ja työelämän tietosuojalaki. (Erityislainsäädäntö s.a.) Erikoistietosuojalainsäädännöstä poiketaan hieman keskusteltaessa rikosasioiden tietosuojasta koskevasta tietosuojadirektiivistä ja -laista. Rikosasioiden tietosuojalaissa sovelletaan Euroopan unionin direktiiviä ja sovelletaan muutoin Suomen muuta lainsäädäntöä. (Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018, 1. luku 1. § mom. 5, 1. luku 2. § mom. 1.)

2.2 Tietosuoja-asetuksen ja muun lainsäädännön keskeiset termit

Tässä luvussa käsitellään Euroopan unionin ja Suomen lainsäädännön erikoissanaston termejä. Kyseisten termien tarkoituksena on varmistaa, että lukija ymmärtää opinnäytetyön sisällön ja osaa yhdistää eri termien käyttöyhteydet toisiinsa sekä eri aihepiireihin.

Anonymisoimisella tarkoitetaan henkilötietojen käsittelytoimenpidettä, jossa karkeistetaan tiedot yleiselle tasolle ja estetään niiden tunnistettavuus peruuttamattomaan muotoon, ettei tietoja käsittelevä taho voi muuttaa hallussa olevia tietoja takaisin tunnistettavaan olemukseen. (Pseudonymisoidut ja anonymisoidut tiedot s.a.)

Asianmukaisilla suojatoimenpiteillä tarkoitetaan sellaisia toimenpiteitä, joilla taataan henkilötietojen lainmukaisuus huomioiden käsittelyn luonne, laajuus, asiayhteys, tarkoitukset ja rekisteröityjen oikeuksiin viittaavat riskit (Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä, 1. luku 3. § mom. 1 10. kohta).

Biometrisillä henkilötiedoilla tarkoitetaan kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin tunnuspiirteisiin liittyviä henkilötietoja, kuten kasvokuvat tai sormenjäljet, joiden pohjalta voidaan hänet tunnistaa tai varmistaa tunnistautuminen (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 14. kohta).

Erityisiksi henkilötiedoiksi, eli arkaluontoisiksi henkilötiedoiksi luokitellaan ne tiedot, joista ilmenee rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettiset, biometriset, terveyttä, seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot (Euroopan parlamentin ja neuvoston asetus (EU), 9. artikla 1. kohta).

Geneettisillä henkilötiedoilla tarkoitetaan luonnollisen henkilön perittyjä tai hankittuja geneettisiä tunnusmerkillisyyksiä, joista ilmenee yksilöllistä tietoa luonnollisen henkilön fysiologiasta tai terveydentilasta analysoimalla kyseisen luonnollisen henkilön biologista näytettä (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 13. kohta.).

Hallinnollisella sakolla tarkoitetaan valvontaviranomaisen antamaa sakkoa rekisterinpitäjälle tai henkilötietojen käsittelijälle tietosuoja-asetuksen vaatimusten laiminlyönnistä. Rikkomuksen luonteen perusteella sakko voi olla enimmäismäärältään 20 miljoonaa euroa tai 4 % yrityksen edeltävän tilikauden globaalista kokonaisliikevaihdosta. (Euroopan parlamentin ja neuvoston asetus (EU), 83. artikla.)

Hallinnollisella seuraamuksella tarkoitetaan valvontaviranomaisen määräämiä seuraamuksia tietosuoja-asetuksen laiminlyönnistä (Euroopan parlamentin ja neuvoston asetus (EU), 84. artikla).

Henkilötiedolla tarkoitetaan niitä tietoja, joiden pohjalta voidaan tunnistaa suoraan tai epäsuorasti luonnollinen henkilö. Henkilötietoja voidaan kerätä henkilön sosiaalisesta mediasta, henkilöllisyyttä koskevista yksilötiedoista tai fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen tekijän perusteella. (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 1. kohta.)

Henkilötietojen käsittelijällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa, organisaatiota tai muuta tahoa, joka käsittelee henkilötietoja rekisterinpitäjän alaisuudessa (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 8. kohta).

Johtavalla valvontaviranomaisella tarkoitetaan rekisterinpitäjää, joka toimii useassa EU:n jäsenvaltiossa ja joka voi asetuksen nojalla asioida päätoimipaikkansa johtavana valvontaviranomaisena poistaen tarpeen asioida eri jäsenvaltioiden valvontaviranomaisten kanssa (Euroopan parlamentin ja neuvoston asetus (EU), 56. artikla).

Kansainvälisellä järjestöllä tarkoitetaan kahden tai useamman maan välisen sopimuksen perusteella perustettua järjestöä tai sen alaisia tahoja, joihin sovelletaan kansainvälistä julkisoikeutta. (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 26. kohta).

Kolmannella osapuolella tarkoitetaan sellaisia henkilötietojen käsittelijöitä, jotka ovat oikeutettuja käsittelemään henkilötietoja suoraan rekisterinpitäjän tai käsittelijän vastuunalaisuudessa (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 10. kohta).

Kolmannella maalla tarkoitetaan muita valtioita kuin Euroopan unioniin ja talousalueeseen kuuluvia valtioita taikka Sveitsiä (Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä, 1. luku 3. § mom. 1 15. kohta).

Käsittelyllä tarkoitetaan henkilötietojen käsittelyyn kohdistuvia automaattisia taikka manuaalisia toimintoja, joilla on vaikutusta tietojen olemukseen. Käsittelyllä tarkoitetaan kaikkea henkilötietojen keruusta käsittelyyn ja tallentamisesta siirtoon sekä luovutukseen ja jopa käsittelyn suunnittelu ja niiden poistaminen luokitellaan henkilötietojen käsittelyksi. (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 2. kohta; Henkilötietojen käsittely s.a.)

Käsittelyn rajoittamisella tarkoitetaan merkittyjen henkilötietojen rajoittamista myöhempää käsittelyä varten (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 3. kohta).

Lapsen henkilötietojen käsittelyllä tarkoitetaan tietosuoja-asetuksen nojalla määriteltyä 16 vuoden ikärajaa. Jäsenvaltioilla on oikeus laskea ikäraja 13 vuoteen. Suomen tietosuojalaissa katsotaan lainmukaiseksi kerätä henkilötietoja vähintään 13-vuotiailta. (Euroopan parlamentin ja neuvoston asetus (EU), 8. artikla; Tietosuojalaki, 2. luku 5. §.)

Osallistuvalla valvontaviranomaisella tarkoitetaan henkilökäsittelyä koskevaa valvontaviranomaista, kun kyse on valvontaviranomaisen jäsenvaltion alueella toimivasta rekisterinpitäjästä tai henkilötietojen käsittelijästä, jossa käsittely vaikuttaa merkittävällä tavalla jäsenvaltiossa asuviin rekisteröityihin tai käsittelystä on tehty valitus valvontaviranomaiselle (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 22. kohta).

Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai viranomaista, virastoa, organisaatiota tai muuta tahoa, jotka yksinään tai yhteistyössä määrittelevät henkilötietojen käsittelyn tarkoitukset ja keinot (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 7. kohta).

Profiloinnilla tarkoitetaan henkilötietojen automaattista käsittelyä, jossa hyödynnetään yksilöllisiä henkilötietoja analysoimalla tai ennakoimalla niiden piirteitä, jotka liittyvät rekisteröidyn työskentelyyn, taloudelliseen tilanteeseen, hyvinvointiin taikka sijaintiin. (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 4. kohta.)

Pseudonymisoimisella tarkoitetaan rekisteröidyn tunnistettavuuden rajoittamista niin, että hänet voidaan silti tunnistaa lisätietojen avulla. Tietojen saatavuus ja säilytys on toteutettava erillään pseudonymisoiduista tiedoista ja niihin on sovellettava asianmukaiset toimenpiteet, joilla varmistetaan, ettei henkilötietojen yhdistäminen rekisteröityyn ole mahdollista. (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 5. kohta.)

Rekisterillä tarkoitetaan henkilötietojen muodostavaa tietojoukkoa, josta tiedot ovat saatavilla rekisterinpitäjälle, henkilötietojen käsittelijälle tai rekisteröidylle tietyin perustein (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 6. kohta).

Suostumuksella tarkoitetaan hyväksyntää henkilötietojen käsittelyyn, jolloin annetaan selkeä lausunto suostumuksesta. Hyväksyttäväksi suostumukseksi luokitellaan sellainen yksilöity tahdonilmaisu, joka on tehty vapaaehtoisesti ja tietoisesti. (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 11. kohta.)

Terveystiedoilla tarkoitetaan luonnollisen henkilön terveyteen tai terveydentilaan liittyviä henkilötietoja mukaan lukien terveyspalveluiden tiedot, joista ilmenee hänen terveydentilansa. (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 15. kohta).

Tietoturvaloukkauksella tarkoitetaan tilannetta, jossa henkilötietojen siirron, tallennuksen tai käsittelyn yhteydessä tiedot vahingossa tai lainvastaisesti tuhoutuu, häviää, muuttuu, siirtyy tai niihin pääsee ulkopuoliset käsiksi. (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 12. kohta.).

Toimivaltaisella viranomaisella tarkoitetaan asetuksen mukaisesti ”viranomaisia, joiden toimivalta kattaa rikoksen ennalta estämisen, paljastamisen, selvittämisen tai syyteharkintaan saattamisen, syyteharkinnan tai muun rikoksesta syyttämiseen liittyvän toiminnan, rikosoikeudellisiin seuraamuksiin tuomitsemisen tai rikosoikeudellisten seuraamusten täytäntöönpanon, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy” (Euroopan parlamentin ja neuvoston asetus (EU), 1. luku 3. § mom. 1 5. kohta).

Valvontaviranomaisella tarkoitetaan jäsenvaltion 51. artiklan nojalla perustamaa riippumatonta viranomaista (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 21. kohta).

Vastaanottajalla tarkoitetaan yhtä tai useampaa luonnollista henkilöä tai viranomaista, virastoa, organisaatiota tai muuta tahoa, joille voidaan tarvittaessa luovuttaa henkilötietoja (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 9. kohta.).

Yhteisrekisterinpitäjällä tarkoitetaan vähintään kahden tai useamman rekisterinpitäjien yhteisesti määrittämiä käsittelyn tarkoituksia ja keinoja. Rekisterinpitäjien vastuualueiden järjestelyllä voidaan vahvistaa asetuksen velvoitteiden noudattamisen. (Euroopan parlamentin ja neuvoston asetus (EU), 26. artikla.)

2.3 Henkilötiedot ja niiden käsittely

Kaikki luonnolliseen henkilöön liittyvät tiedot, joiden avulla hänet tunnistetaan, luokitellaan aina henkilötiedoiksi (Euroopan parlamentin ja neuvoston asetus (EU), 4. artikla 1. kohta). Saatavilla olevilla tiedoilla voidaan tunnistaa henkilö suoraan tai välillisesti yhdistämällä useat eri yksilötiedot, kuten nimi ja henkilötunnus, jotka sitten mahdollistavat tunnistamisen. (Mikä on henkilötieto s.a.) Anonymisoidut ja pseudonymisoidut henkilötiedot lasketaan edelleen henkilötiedoiksi niin pitkään, kunnes niiden tietojen perusteella ei voida tunnistaa luonnollista henkilöä eikä tietoja voida palauttaa takaisin alkuperäiseen muotoon. (Pseudonymisoidut ja anonymisoidut tiedot s.a)

Lainmukainen henkilötietojen käsittely edellyttää tietosuoja-asetuksen 6. artiklan 1. kohdan toteutumista. Lainmukaisuuden toteutumiseksi on määriteltävä vähintään yksi käsittelyperuste ennen henkilötietojen käsittelyä. Peruste on sitova, eikä sitä voi vaihtaa enää toiseen. Valitulla käsittelyperusteella on merkittävä vaikutus rekisteröidyn oikeuksiin suhteessa rekisterin pitäjään. (Milloin henkilötietoja saa käsitellä? s.a.) Henkilötietojen käsittely on lainmukaista, kun

- käsittelyyn annetaan nimenomainen suostumus.
- käsittely on tarpeellista sopimuksen täytäntöön panemiseksi.
- rekisteröity pyytää sopimuksessa kirjattujen toimenpiteiden toteuttamista.
- rekisterinpitäjän on noudatettava lakisääteistä velvoitetta.
- kyse on rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamisesta.
- suoritetaan yleistä etua koskevia tehtäviä.
- kyse on rekisterinpitäjälle kuuluvan julkisen vallan käytöstä.
- pyritään toteuttamaan rekisterinpitäjän tai kolmannen osapuolen oikeutettuja etuja.

Lapseen kohdistuvassa käsittelyssä on otettava huomioon 8. artiklan 1. kohta, jossa määritellään lainmukaisuuden rajan menevän 16-vuotiaan kohdalla. Alle 16-vuotiaiden kohdalla käsittely on lainmukaista silloin, kun huoltaja suostuu

tai antaa valtuudet käsittelyyn. (Euroopan parlamentin ja neuvoston asetus (EU), 8. artikla 1.–2. kohta). Tietosuojalain 6. § poikkeaa asetuksen 6. artiklan 1. kohdan e alakohdan kohdalla siten, että se määrittelee viranomaistoiminnalle omat käsittelyperusteet (Tietosuojalaki, 2. luku 6. §).

Lähtökohtaisesti erityisiä henkilötietoryhmiä koskeva tietojen käsittely tietosuoja-asetuksen 9. artiklan 1. kohdan nojalla on kiellettyä. Erityisiä henkilötietoryhmiä voidaan kuitenkin käsitellä 9. artiklan 2. kohdan perusteella, jos

- rekisteröitynyt on antanut siihen nimenomaisen suostumuksensa.
- käsittely on tarpeen rekisterinpitäjän tai rekisteröidyn velvoitteiden ja erityisten oikeuksien noudattamiseksi työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla lainsäädännön puitteissa.
- kyseessä on rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaaminen, jossa rekisteröity fyysisesti tai juridisesti estynyt antamasta suostumusta.
- henkilötietoja käsitellään yhteisön laillisen toiminnan yhteydessä.
- rekisteröitynyt henkilökohtaisesti julkaisee henkilötietoa julkiseksi.
- kyse on oikeusvaateen laatimisesta, esittämisestä tai puolustamisesta, kun tuomioistuimet suorittavat lainkäyttötehtäviään.
- asia koskee yleistä etua unionin oikeudella tai jäsenvaltion lainsäädännön nojalla.
- salassapitovelvollisuuden sitomalla viranomaisella tai ammattilaisella on tarkoitus käsitellä erityisiä henkilötietoryhmiä, kun käsittely koskee ennalta ehkäisevää tai terveydenhuoltoa koskevia tarkoituksia sekä kansanterveyteen liittyvää yleistä etua.
- käsittelyn tarve on yleisen edun mukaista arkistointitarkoituksia taikka tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten.

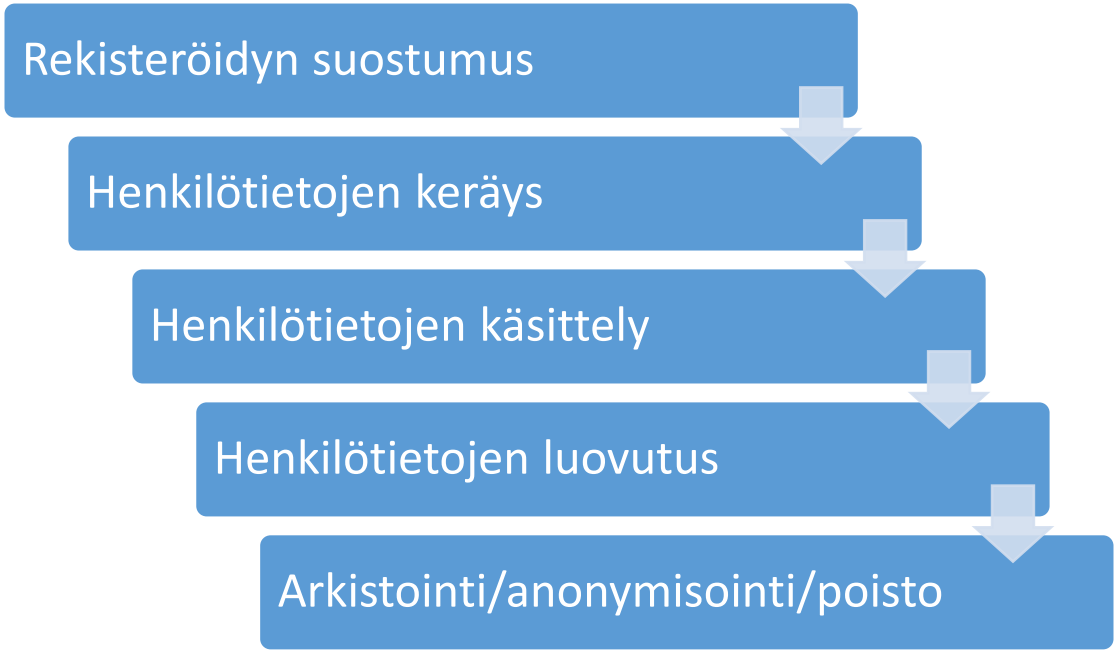
Tietosuojalain 2. luvun 6. §:ssä säädetään tarkemmin erityisten henkilötietoryhmien käsittelystä.

Tietosuoja-asetuksen 5. artiklan sisältö määrittelee henkilötietojen käsittelylle seuraavat tietosuojaperiaatteet, joiden mukaan henkilötietoja on käsiteltävä ” lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi”. Tiedon keruun ja käsittelyn on noudatettava tiettyjen ja nimenomaisten lain tarkoituksia. Tietomateriaalin on oltava asianmukaista, olennaista ja rajoitettua tarpeelliseen määrään käsittelyä varten. Kerätty tieto täytyy olla täsmällistä ja tarvittaessa päivitettyä, ja lisäksi epäselvät ja epäkohdalliset tiedot on oikaistava tai poistettava heti. Tiedot on säilytettävä tunnistettavassa muodossa ainoastaan niin kauan, kuin on tarpeen. Jos tietoja käsitellään yleisen edun vuoksi,

sovelletaan 89. artiklan 1. kohtaa edellyttäen, että asetuksessa on tehty asianmukaiset toimenpiteet rekisteröityjen oikeuksien ja vapauksien turvaamiseksi. Rekisterinpitäjän vastuuna on varmistaa henkilötietojen asianmukainen turvallisuus sekä käyttää asianmukaisia teknisiä ja organisatorisia toimia suojatakseen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Rekisterinpitäjällä on vastuu ja osoitusvelvollisuus 6. artiklan 1. kohdan toteutumisesta koko henkilötiedon elinkaaren ajan. (Euroopan parlamentin ja neuvoston asetus (EU), 6. artikla 1.–2. kohta.)

Henkilötietojen käsittely edellyttää aina vähintään yhtä tietosuoja-asetuksen 6. artiklan 1. kohdan käsittelyperusteen toteutumista. Kun henkilötietojen käsittely sidotaan valittuun käsittelyperusteeseen, on peruste sitova, eikä sitä voida vaihtaa toiseen (Milloin henkilötietoja saa käsitellä? s.a.). Käsittelyn on noudatettava kaikkia tietosuoja-asetuksen 5. artiklan 1. kohdassa lueteltuja tietosuojaperiaatteita. Rekisterinpitäjän on käsiteltävä henkilötietoja niin, että rekisteröidyn kysyessä osoitusvelvollisuuden määräämänä osataan läpinäkyvästi kertoa henkilötiedon elinkaari kokonaisuudessaan ja kyetään mahdollistamaan rekisteröidyn oikeuksien käyttö.

Henkilötiedon elinkaarella tarkoitetaan tiedon kokonaisvaltaista olemassaoloa keruusta tiedon poistamiseen saakka, ja siinä käsittelyn elinkaari on suunniteltava alusta loppuun (Henkilötietojen käsittelyn elinkaari, tietosuojaperiaatteet ja tietojen suojaaminen tieteellisessä tutkimuksessa s.a.). Lainsäädännön sekä liiketoiminnan vaatimusten perusteella määritellään henkilötiedoille tarpeellinen säilytysaika (EU-tietosuojan kokonaisuudistus 2016, 24).



Kuva 1. Henkilötietojen elinkaari (EU-tietosuojan kokonaisuudistus 2016, 24)

Kuva 1. kuvastaa edellä mainitun sisällön pohjalta elinkaarimallia, joka on referoitu EU-tietosuojan kokonaisuudistuksen PDF-dokumentista. Tiedon kerääminen alkaa luonnollisen henkilön suostumuksesta, jonka jälkeen henkilötietoja käsitellään vain erikseen tarkoitettuun käyttöön. Tietosuoja-asetuksen 5. artiklaa on noudettava, tiedon keruussa ja käsittelyssä on oltava tarkat tavoitteet, säilytysajat ja tarvittavat rajaukset on määriteltävä, sekä tiedot on luokiteltava ja käsiteltävä luottamuksellisesti. Henkilötiedon elinkaari on päätöksessään, kun tiedon käyttötarkoitus, -oikeus tai säilytysaika loppuu. Tarpeettomille henkilötiedoille on oltava valmiina asianmukaiset toimenpiteet, kuten tietojen poisto, anonymisointi, pseudonymisointi tai arkistointi, ja tiedon käsittelyn päättymisestä on ilmoitettava rekisteröidylle. (Vartiainen 2016; Euroopan parlamentin ja neuvoston asetus (EU), 19. artikla.) Henkilötiedot, jotka sisältävät taloudellista tietoa, kuten esimerkiksi tilinpäätökset ja toimintakertomukset, on kirjanpitolain 10. §:n mukaan säilytettävä vähintään 10 vuotta tilikauden päättymisestä siten, että 6., 7. ja 9. §:n vaatimukset täyttyvät (Kirjanpitolaki 30.12.1997/1336, 10. § mom. 1.).

2.4 Rekisteröidyn oikeudet

Tietosuojalla suojataan ihmisten yksityiselämää, johon kuuluu oikeus henkilötietoihin. Perusperiaatteena on suojata henkilötiedot valtuudettomalta tai hen-

kilöä vahingoittavalta tietojen käytöltä. Suomessa tietosuoja-asetuksen määrittelemät rekisteröidyn oikeudet on rajoitettu tietyissä tapauksissa Suomen lainsäädännön viranomaistoiminnassa. (EU-tietosuojan kokonaisuudistus 2016, 13; Tietosuojalaki, 5. luku 34. §.)

Rekisteröidyn oikeuksien toteuttaminen on kuitenkin yksi rekisterinpitäjän päävelvollisuuksista. Tietosuoja-asetuksen 19. ja 34. artiklan nojalla rekisterinpitäjällä on ilmoitusvelvollisuus. Ilmoitusvelvollisuuden velvoittamana rekisteröidyllä on oikeus saada tietää luvattomasta tietoturvaloukkauksesta sekä mahdollisista henkilötietojen oikaisua, poistoa tai käsittelyn rajoittamista koskevista asioista. (EU-tietosuojan kokonaisuudistus 2016, 13; Yleinen tietosuoja-asetus, 19., 34. artikla.) Rekisteröity on tunnistettava, kun hän käyttää oikeuksiaan saadakseen pääsyn tietoihin tai pyytääkseen oikaisua, poistoa tai siirtoa eri rekisteriin. Pyyntöihin on vastattava kuukauden sisään. Ainoastaan monimutkaisen tai laajan pyynnön kohdalla voidaan vastata kahden kuukauden viiveellä. Toimitettavat tiedot tulee esittää pääsääntöisesti sähköisenä ja niiden tulee olla pääsääntöisesti maksuttomia. Kohtuuttomista, jatkuvasti toistuvista tai ilmeisen perusteettomista pyynnöistä rekisterinpitäjällä on oikeus periä kohtuullinen maksu aiheutuneista hallinnollisista kustannuksista tai kieltäytyä suorittamasta pyydettyä toimenpidettä. (Euroopan parlamentin ja neuvoston asetus (EU), 12. artikla, 2.–7. kohta.)

Tietosuoja-asetuksen 12. artiklan velvoittamana rekisterinpitäjää sitoo tiedonantovelvoite. Jo ennen käsittelytoimien alkua, rekisterinpitäjällä on velvollisuus tiedottaa henkilötietojen käsittelystä. Rekisterinpitäjän on toimitettava rekisteröidylle

- rekisterinpitäjän tai edustajan sekä mahdollisen tietosuojavastaavan yhteystiedot.
- selvitys henkilötietojen käsittelyn tarkoituksista ja oikeusperusteista.
- rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut ja mahdolliset tiedot henkilötietojen vastaanottajista tai -ryhmistä.
- mahdolliset henkilötietojen siirrot kolmanteen maahan tai kansainväliselle järjestölle.
- henkilötietojen säilyttämisajat tai tämän ajan määrittämiskriteerit.
- ilmoitus rekisteröidyn oikeuksien käyttömahdollisuuksista, vastustamisoikeudesta sekä valittamisoikeudesta.

Ilmoittaminen on toteutettava läpinäkyvästi, helposti ymmärrettävässä, selkeällä kielellä niin, että jokaisen ikäluokan henkilö kykenee lukemaan ilmoituksen. Toimitettavat tiedot on oltava kirjallisessa muodossa tai rekisteröidyn pyytäessä sähköisessä muodossa. Rekisteröidyn pyytäessä tietoja suullisesti, on rekisterinpitäjän varmistettava henkilöllisyys. (Euroopan parlamentin ja neuvoston asetus (EU), 12. artikla, 1. kohta; 13.–22. artikla.)

Rekisteröidylle on ilmoitettava 12. artiklan sisällön lisäksi hänen kaikista mahdollisista oikeuksistaan, joihin kuuluu mahdollisuus pyytää henkilötietojen käsittelyä koskevat tiedot ja tietojen oikaisua, poistoa, rajoittamista, tietojen siirtoa järjestelmästä toiseen, valittaa halutessaan valvontaviranomaiselle tai vastustaa tietojen käsittelyä ja kieltäytyä automaattisen käsittelyn kohteeksi joutumisen. Rekisterinpitäjän on ilmoitettava läpinäkyvästi henkilötietojen säilytysaika, oikeus peruuttaa suostumus milloin tahansa, se onko henkilötietojen antaminen lakisääteistä tai sopimukseen perustuvaa tai kohdistuuko rekisteröityyn automaattista päätöksentekoa mukaan lukien profilointia ja käsittelystä johtuvat mahdolliset seuraukset. (Euroopan parlamentin ja neuvoston asetus (EU), 13. artikla.)

Henkilötietojen keruun jälkeen rekisterinpitäjä on velvoitettu välittämään rekisteröidylle jäljenne käsiteltävistä henkilötiedoista. Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus henkilötietojensa käsittelystä, ja jos tietoja käsitellään, rekisteröidyllä on oikeus tutustua tietoihinsa ja oikaista ne tarvittaessa. Rekisteröidyllä on mahdollisuus tarkistaa, ovatko kerätyt tiedot oikeita ja oikeutettuja, pyytää tarvittaessa oikaisua virheellisten tietojen kohdalla ja halutessaan tehdä valitus valvontaviranomaiselle tai pyytää selvitystä tietojen alkuperästä ja säilytysajan pituudesta. Rekisterinpitäjän on vastattava rekisteröidylle ilman aiheetonta viivästystä, kuitenkin kuukauden kuluessa pyynnön vastaanottamisesta. Lähtökohtaisesti oikeuden käyttö on maksutonta, mutta aiheutuvista hallinnollisista kustannuksista voidaan periä kohtuullinen summa. Pyynnön vastaamisesta voidaan periä maksua myös silloin, kun pyyntö on perusteeton tai kohtuuton. Vaihtoehtoisesti voidaan pyynnön toteuttamisesta kieltäytyä. (Oikeus saada tietoa henkilötietojen käsittelystä s.a.; Euroopan parlamentin ja neuvoston asetus (EU), 15.–16. artikla.)

Rekisteröidyllä on oikeus tulla unohdetuksi, eli käytännössä rekisteröidyllä on oikeus pyytää häntä koskevien tietojen poistoa ilman viivästyksiä. Rekisterinpitäjällä on velvollisuus poistaa henkilötiedot ilman viivästystä, kun

- kerätyillä henkilötiedoilla ei enää ole käyttötarkoitusta, eikä niiden käsittelylle ole perustetta.
- rekisteröity peruu suostumuksen.
- rekisteröity vastustaa käsittelyä tai henkilötietoja on käsitelty lainvastaisesti.
- noudatetaan lakisääteisiä velvoitteita.

Henkilötietojen poistamista voidaan rajoittaa tai estää, kun käsittely koskee sananvapautta ja tiedonvälityksen vapautta koskevaa oikeuden käyttöä tai unionin oikeutta tai jäsenvaltion lainsäädäntöä, edellyttäen lakisääteisten velvoitteiden noudattamista tai yleisen edun suorittamista, rekisterinpitäjän julkisen vallan käyttöä sekä kansaterveyteen liittyviä yleisiä etuuksia ja yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai tutkimustarkoituksia. Käsittelyä voidaan rajoittaa myös oikeudellisen vaateen laatimista, esittämistä tai puolustamista koskevissa tilanteissa. (Euroopan parlamentin ja neuvoston asetus (EU), 18. artikla.)

Rekisteröidyllä on oikeus käsittelyn rajoittamiseen. Rekisterinpitäjän on rajoitettava käsittelyä, kun

- rekisteröity kieltää henkilötietojen todenmukaisuuden, jolloin tietojen käsittelyä rajoitetaan, kunnes tietojen todenmukaisuus varmistuu.
- käsittely on lainvastaista ja rekisteröity edellyttää henkilötietojen rajoittamista tietojen poistamisen sijaan.
- rekisterinpitäjällä ei ole henkilötiedoille tarvetta, mutta rekisteröity tarvitsee tietoja oikeudellisiin toimenpiteisiin.
- rekisteröity vastustaa henkilötietojen käsittelyä todentaakseen syrjivätkö rekisterinpitäjän oikeutetut perusteet rekisteröidyn perusteita.

Rajoittamisen aikana henkilötietoja voidaan käsitellä vain rekisteröidyn suostumuksella taikka oikeudellisten toimenpiteiden toteuttamiseksi, tai toisen yksilön oikeuksien suojaamiseksi tai yleistä etua koskevista syistä. Rekisterinpitäjällä on velvollisuus ilmoittaa rekisteröidylle 18. artiklan 3. kohdan mukaisesti rajoittamisen päättymisestä. (Euroopan parlamentin ja neuvoston asetus (EU), 18. artikla.)

Rekisteröidyllä on oikeus tietonsa siirtää rekisterinpitäjältä toiselle. Toimitettavat henkilötiedot on oltava jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa niiden siirtyessä toiselle rekisterinpitäjälle. Siirto on mahdollista toteuttaa, kun käsittely perustuu lainmukaiseen suostumukseen ja sopimukseen, ja käsittely suoritetaan automaattisesti. Henkilötietojen siirto-oikeutta voidaan rajoittaa, kun kyseessä on yleistä etua koskevan tehtävän suorittaminen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttö, eikä siirto-oikeudella saa olla negatiivista vaikutusta muiden oikeuksiin ja vapauksiin. (Euroopan parlamentin ja neuvoston asetus (EU), 20. artikla.)

Rekisteröidyllä on 21. artiklan mukaan vastustamisoikeus. Toisin sanoen rekisteröidyllä on oikeus vastustaa milloin tahansa häntä koskevien henkilötietojen käsittelyä. Rekisterinpitäjä menettää oikeuden käsitellä henkilötietoja, ellei osoiteta, että käsittelylle on tärkeä ja perusteltu syy, joka kumoaa rekisteröidyn edut ja oikeudet. Rekisteröity voi vastustaa henkilötietojen käsittelyä suoramarkkinointia ja profilointia, kun se liittyy suoramarkkinointiin sekä automaattiseen käsittelyyn ja päätöksentekoon. (Euroopan parlamentin ja neuvoston asetus (EU), 21.–22. artikla.)

Tietosuojalain 4.luvun 21. §:n mukaan rekisteröidyllä on oikeus viedä asia tietosuojavaltuutetulle käsiteltäväksi, jos koetaan häntä koskevien henkilötietojen käsittelyn rikkovan sitä koskevaa lainsäädäntöä. Asian käsittely voidaan valtuutetun toimesta keskeyttää, jos käsittely jo on vireillä tuomioistuimessa.

2.5 Rekisterinpitäjän velvollisuudet

Tietosuoja-asetus asettaa henkilötietoja käsitteleville tahoille velvollisuudet noudattavat tietosuojaperiaatteiden toteutumista henkilötietojen käsittelyssä. Rekisterinpitäjän vastuuna on määrittää henkilötietojen käsittelylle perusteet ja hänen tulee huolehtia, että henkilötietoja käsitellään vain lainmukaisen, asianmukaisen ja tarkoituksen mukaisin edellytyksin. Henkilötietojen käsittelyn aikana rekisterinpitäjää sitoo osoitusvelvollisuus, ja hänen on pystyttävä osoittamaan, miten on varmistettu tietosuojaperiaatteiden toteutuminen toiminnassaan tarvittavin teknisin ja organisatorisin toimenpitein. (EU-tietosuojan kokonaisuudistus 2016, 18.)

Rekisterinpitäjä voi halutessaan siirtää osan henkilötietojen käsittelystä henkilötietojen käsittelijälle. Kahden osapuolen välillä on oltava sopimus, jossa määritellään tietosuoja-asetuksen mukaisesti henkilötietojen käsittelyn päämäärä, aikeet ja ajanjakso sekä käsiteltävät henkilötiedot. Valitun henkilötietojen käsittelijän on sopimuksen mukaisesti noudatettava henkilötietojen käsittelytapoja annettujen asianmukaisten toimenpiteiden avulla, sekä täytettävä tietosuoja-asetuksen vaatimukset ja huolehdittava rekisteröityjen oikeuksien toteutumisesta. Sopimuksessa on määritettävä käsittelijän salassapitovelvollisuus, oikeudet ja yhteistyövelvoitteet rekisterinpitäjän kanssa. Sopimuksen voimassaolon aikana on suositeltavaa määritellä tietosuojan ja tietoturvan säännölliset raportoinnin käytännöt ja järjestää osapuolten väliset palaverit, joissa seurataan tietosuoja ja -turvan toteutumista henkilötietojen käsittelyssä. (EU-tietosuojan kokonaisuudistus 2016, 28–29; Euroopan parlamentin ja neuvoston asetus (EU), 28.–29. artikla.)

Jotta voidaan huolehtia tietosuojasta organisaation laajuisessa toiminnassa, tietosuojan hallinnoinnin vastuuta on jaettava organisaatiossa. Hallinnointiin on varattava riittävä määrä resursseja koko organisaation tietosuojatehtävien toteuttamiseen. Asetus velvoittaa tiettyjä rekisterinpitäjiä nimeämään tietosuojavastaavan, kun

- tietojen käsittelyä suorittaa viranomainen tai muu julkishallinnon elin.
- organisaation ydintehtävät muodostavat luonteeltaan sellaisia käsittelytoimia, jotka edellyttävät säännöllistä ja järjestelmällistä seurantaa laajassa mittakaavassa.
- organisaation ydintehtävät muodostavat sellaisia käsittelytoimia, jotka kohdistuvat 9. artiklan määritelmiin erityisiin henkilötietoryhmiin tai 10. artiklassa tarkoitettuihin rikoksiin liittyviin henkilötietoihin.

Organisaatiot voivat myös vapaaehtoisesti nimetä yhden tietosuojavastaavan, jonka toimenkuvaan kuuluu huolehtia henkilötietojen käsittelyn lainmukaisuudesta ja lain toteutumisesta. (EU-tietosuojan kokonaisuudistus 2016, 18–19; Euroopan parlamentin ja neuvoston asetus (EU), 37. artikla.)

Rekisteröidyn ja henkilötietojen käsittelijän on taattava, että organisaatiossa nimetty tietosuojavastaava toimii riippumattomassa asemassa sekä hänet otetaan asiaankuuluvasti ja kohtuullisen aikaisin mukaan kaikkiin henkilötietojen suojaa käsittelevien asioiden käsittelyyn. Rekisteröidyt voivat ottaa yhteyttä

tietosuojavastaavaan kaikissa henkilötietojen käsittelyä ja asetukseen perustuviin oikeuksiensa käyttöä koskevissa asioissa. Tietosuojavastaavalle on annettava tueksi tarvittavat resurssit toimenkuvaan kuuluvien tehtävien toteuttamiseksi, samoin pääsy henkilötietoihin, käsittelytoimiin sekä on tarjottava mahdollisuuksia asiantuntemuksen ylläpitämiseksi. Salassapitoon velvoitettu tietosuojavastaava voi olla rekisterinpitäjän, käsittelijän tai ulkoistetun palveluntarjoajan palkkalistoilla. Tietosuojavastaava raportoi suoraan rekisterinpitäjälle tai henkilötietojen käsittelijän ylimmälle johdolle. Tietosuojavastaavalla on oikeus tehdä muita työtehtäviä oman toimenkuvan lisäksi niin, ettei niistä aiheudu eturistiriitoja eikä häntä voida erottaa tai rangaista tietosuojatehtävien hoitamisen vuoksi. (EU-tietosuojan kokonaisuudistus 2016, 19; Euroopan parlamentin ja neuvoston asetus (EU), 38. artikla.)

Tietosuojavastaavan toimenkuvaan kuuluu neuvoa sekä informoida rekisterinpitäjää tai henkilötietojen käsittelijää sekä henkilötietoja käsitteleville työntekijöille asioista, jotka koskevat asetuksen ja valtion tietosuojalainsäädännön mukaisia velvollisuuksia. Vastaava seuraa tietosuoja-asetuksen ja -lainsäädännön noudattamista, ohjeistaa toimintamenettelyissä, jotka liittyvät henkilötietojen suojaan. Tietosuojavastaava huolehtii vastuunjaosta, dokumentaatiosta ja tiedon lisäyksestä ja käsittelyyn osallistuvan henkilöstön kouluttamisesta. Pyydettäessä tietosuojavastaavan on annettava neuvoja vaikutusten arviointien tekemiseen. Hänen on valvottava arvioinnin toteutusta tietosuojasäännöksen mukaisesti. Tietosuojavastaavan velvollisuuksiin kuuluu myös työskennellä yhteistyössä valvontaviranomaisen kanssa ja toimia yhteyshenkilönä käsittelyyn liittyvissä kysymyksissä mukaan lukien ennakkokuulemisessa. (EU-tietosuojan kokonaisuudistus 2016, 19; Euroopan parlamentin ja neuvoston asetus (EU), 39. artikla.)

2.6 Riippumaton asema

Tietosuoja-asetuksen 51. artiklan mukaan jokaisen jäsenvaltion on varmistettava, että yksi tai useampi riippumaton valvontaviranomainen on vastuussa asetuksen valvonnasta, oikeuksien ja vapauksien suojaamisesta henkilötietojen käsittelyssä sekä unionissa vapaan liikkuvuuden varmistamisesta. (Euroopan parlamentin ja neuvoston asetus (EU) 51. artikla). Suomen tietosuojalain-

säädännön 3. luvun 8. §:ssä määritellään valvontaviranomainen tietosuojavaltuutetuksi. Tietosuojavaltuutettu on toiminnassaan itsenäinen ja riippumaton. Hänen henkilöstöönsä kuuluu vähintään kaksi apulaistietosuojavaltuutettua sekä tarpeelliseksi koettu määrä tietosuojavaltuutetun tehtävänalaan perehtyneitä asiantuntijoita. (Tietosuojalaki, 3. luku 8. §.)

Tietosuojavaltuutetun toimenkuvaan kuuluu huolehtia ja valvoa tietosuojalainsäädännön ja muiden henkilötietojen käsittelyä koskevien lakien noudattamista. Tietosuojavaltuutettu käsittelee vastaanotettuja pyyntöjä, valituksia ja ilmoituksia tietosuojavastaavista tai tietoturvaloukkauksista. Hän tekee tarvittavat selvitykset ja tarkastukset sekä tarvittaessa määrää tietosuoja-asetuksen rikkomisesta hallinnollisin seuraamuksin. Tietosuojavaltuutetulla on määräysoikeus saada kaikki henkilötietoihin liittyvät tiedot ja ilmoittaa mahdollisista asetuksen rikkeistä rekisterinpitäjälle tai henkilötietojen käsittelijälle. Rikkeistä voidaan antaa varoituksia, huomautuksia tai määrätä korjaaviin toimenpiteisiin. Käsittely voidaan rajoittaa väliaikaisesti tai pysyvästi ja tarvittaessa asetetaan rekisterinpitäjä suoraan käsittelykieltoon. Rekisterinpitäjä tai henkilötietojen käsittelijä voidaan määrätä 83. artiklan nojalla hallinnollisiin seuraamusmaksuihin riippuen tapauksen olosuhteista. (Tietosuojavaltuutetun tehtävät s.a.; Euroopan parlamentin ja neuvoston asetus (EU), 57.–58. artikla.)

2.7 Oikeussuojakeinot, vastuu ja seuraamukset

Tietosuoja-asetuksen mukaan rekisteröity on oikeutettu kanteen tekoon valvontaviranomaiselle, jos hän kokee, että hänen tietosuoja-asetukseensa perustuvia oikeuksia on loukattu. Kantelun vastaanottaneen valvontaviranomaisen on ilmoitettava asianomaiselle edistymisestä ja päätöksestä sekä oikeussuojakeinojen mahdollisuuksista. (Korpisaari ym. 2022, 604; Euroopan parlamentin ja neuvoston asetus (EU), 77. artikla.)

Jokainen on oikeutettu tekemään valitus valvontaviranomaisen päätöksestä. Kyse voi olla valvontaviranomaisen päätös seuraamusmaksusta. Rekisteröidyllä on oikeus tehokkaisiin oikeussuojakeinoihin, eli oikeus saattaa tuomioistuimen käsiteltäväksi asia 3 kuukauden kuluessa siitä, kun valvontaviranomainen ei ole käsitellyt kannetta tai tiedottanut sen kulusta tai päätöksestä.

Suomessa tietosuojavaltuutetun ja apulaistietosuojavaltuutettujen sekä seuraamuskollegion päätöksistä valitetaan hallinto-oikeuteen. Kyseisten tapausten kohdalla säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa. (Korpisaari ym. 2022, 604–605; Euroopan parlamentin ja neuvoston asetus (EU), 78. artikla.)

Jokainen on oikeutettu tehokkaisiin oikeussuojakeinoihin, jos voidaan katsoa, että heidän henkilötietojensa käsittelyssä ei ole noudatettu tietosuoja-asetuksen säännöksiä. Kanteen nostaminen edellyttää selkeää ja tutkittua tiedon oikeudenmukaisuutta, eikä oikeuden käytön tule estyä hinnan, käsittelyn keston tai prosessuaalisten esteiden vuoksi. (Korpisaari ym. 2022, 607–609; Euroopan parlamentin ja neuvoston asetus (EU), 79. artikla.)

Rekisteröity voi hakea tukea 77.–79. artiklan läpivientiin valtuuttamalla tahon hoitamaan tapaukset rekisteröidyn puolesta. Hän voi halutessaan hakea apua tietosuojavaltuutetun neuvontapalvelun kautta. Rekisteröity voi valtuuttaa halutessaan kuluttajajärjestön, joka ryhtyy ajamaan kannetta, jos loukattu ei kykene edustamaan itseään tai kyseessä on suuri määrä pieniä loukkauksia. Rekisteröidyn on kyettävä tunnistamaan mahdollinen oikeudenloukkaus ja ryhdyttävä asian käsittelyyn. (Korpisaari ym. 2022, 611–609; Euroopan parlamentin ja neuvoston asetus (EU), 80. artikla.)

Rekisterinpitäjä on vastuussa kaikista mahdollisista vahingoista, jotka ovat aiheutuneet tietosuoja-asetuksen laiminlyönnistä henkilötietojen käsittelyn aikana. Henkilötietojen käsittelijä on vastuussa laiminlyödessään rekisterinpitäjän osoittamia velvoitteita tai ohjeistuksia. Rekisteröityneellä on 82. artiklan mukaan oikeus hakea korvauksia, jos tietosuoja-asetuksen rikkomisesta on seurannut aineellista tai aineetonta vahinkoa. Korvausvelvollisuudesta vapaudutaan ainoastaan, jos kyetään todistamaan, ettei rekisterinpitäjä tai henkilötietojen käsittelijä ole vastuussa millään tavalla vahingon aiheuttaneesta tapahtumasta. Osoitusvelvollisuuden ja vaikutustenarvioinnin asiamukaisella toteuttamisella sekä osoitettujen riskien pienentävillä toimenpiteiden suorittamisella on suuri merkitys syyttömyyden todistamisessa. (Korpisaari ym. 2022, 618–620; Euroopan parlamentin ja neuvoston asetus (EU), 82. artikla.)

Tietosuoja-asetuksessa säädetään jokaisen valvontaviranomaisen velvoitteeksi varmistaa, että asetuksen periaatteita noudatetaan ja yksilöiden oikeudet toteutetaan. Jos rekisterinpitäjälle tai henkilötietojen käsittelijälle ei varoitus tai huomautus tunnu riittävän, valvontaviranomaisella on oikeus siirtyä järeämpiin puutumiskeinoihin. Viranomainen voi määrätä henkilötietojen käsittelyn lopetettavaksi tai määrätä rikkeestä hallinnollisen seuraamusmaksun. Seuraamusmaksun suuruus vaihtelee rikoksen vakavuuden ja luonteen perusteella. Säännösten rikkomisesta voidaan asettaa seuraamusmaksu, joka on enimmillään 20 miljoonaa euroa tai 4 % yrityksen edeltävän tilikauden vuotuisesta kansainvälisestä liikevaihdosta. Seuraamusmaksun suuruus riippuu siitä, kumpi summa on suurempi. (Korpisaari ym. 2022, 631–633; Euroopan parlamentin ja neuvoston asetus (EU), 82. artikla.)

Yksilön oikeutta omiin tietoihin suojataan myös Suomen lainsäädännön rikosoikeudellisin keinoin. Rikoslain 24. luvussa käsitellään rikokset kotirauhan, viestintärauhan, kotirauhan ja julkisrauhan rikkomisesta sekä salakuuntelusta, yksityiselämää loukkaavan tiedon levittämisestä ja kunnian loukkauksesta. (Korpisaari ym. 2022, 22; Rikoslaki 1889/39, 24. luku 1.–10. §.) Suojaa antaa myös 38. luvussa käsiteltävät aiheet salassapitorikoksesta ja -rikkomuksesta, viestintäsalaisuuden loukkauksesta, tietoliikenteen ja -järjestelmän häirinnästä, tietomurrosta, suojauksen purkujärjestelmärikoksesta ja tietosuojarikoksesta sekä identiteettivarkaudesta (Rikoslaki, 38. luku 1.–9. §).

3 TIETOTURVA YLEISESTI

Tietoturva on osa tietosuojan toteutumisen keinoista. Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joiden avulla pyritään varmistamaan tietoaineistojen ja palveluiden asianmukainen suojaus keskittämällä huomio luottamuksellisuuteen, eheyteen ja saatavuuteen liittyviin riskeihin. (Järvinen 2022, 13–15.) Tämä merkitsee sitä, että valvotaan tietojärjestelmien käytettävyyttä ja tarjotaan jatkuvaa tiedon saatavuutta vain niitä omistaville henkilöille. Vain tiedon omistajalla on oikeus käsitellä, muuttaa tai poistaa henkilökohtaisia tietoja niiden koko elinkaaren ajan. Yritystoiminnassa henkilötietoja käsittelevät tahot ovat oikeutettuja käsittelemään rekisteröityjen henkilötietoja vain lainmukaisissa työtehtävissään. (Henkilöstön tietoturva ohje 2013, 17.) Tiedon eheyden

varmistamiseksi käsittelijöiden on dokumentoitava kaikki tiedon käsittely mahdollista tiedon palauttamista varten.

Organisaation henkilöstöllä on velvollisuus huolehtia aktiivisesti tietoturvallisuuden tasosta. Yleisimmät tietoturvallisuuteen liittyvät ongelmat ovat usein huolimattomuudesta, osaamattomuudesta tai kiireestä johtuvia virheitä, jotka vaikuttavat tietojärjestelmien toteutukseen sekä käytön laadullisiin tekijöihin. (Henkilöstön tietoturva ohje 2013, 18.) Teknologian kehittyessä jatkuvasti myös toimintatavat muuttuvat. Muutoksen rinnalla tietoturvan on pysyttävä kehityksessä mukana. Parantaakseen tietoturvallisuutta työnantajan on hyvä arvioida riskit, tunnistaa uhat ja antaa työhön tarvittavat ajantasaiset toimintaohjeet sekä suorittaa säännöllisesti koulutuksia henkilöstölleen (Järvinen & Rousku 2017, 6. luku).

3.1 NIS2-direktiivi

NIS2-direktiivi eli verkko- ja tietoturvadirektiivi on 2023 voimaan astuva EU:n laajuinen kyberturvallisuutta koskeva lainsäädäntö. Direktiivin tavoitteena on parantaa kyberturvallisuuden yleistä tasoa oikeudellisilla toimenpiteillä. Aikaisempaan NIS-direktiiviin nähden uuden direktiivin avulla nykyaikaistetaan nykyistä oikeudellista kehystä, jotta voidaan pysyä perässä digitalisaation kehityksessä sekä kyberturvallisuuden uhkaympäristön kehittymisen tasalla. (Euroopan komissio 2023.) Direktiivin soveltamisalaa on laajennettu esimerkiksi energia- ja terveydenhuoltosektorilla toimiville tahoille sekä digitaalisen infrastruktuurin palveluntarjoajille. Direktiiviin soveltamisala koskee nyt myös uusia sektoreita ja toimijoita. (Valtioneuvosto 2023.)

Direktiivissä säädetään yhteiskunnan kriittisille sektoreille tietoturvallisuutta vahvistavia riskienhallinta- ja raportointivelvoitteita tietoturvaloukkauksista. Direktiivissä on kirjattuna vähimmäistoimenpiteet, jotka on toteutettava kyberturvallisuusriskien minimoimiseksi. Toimijoilla on direktiivin velvoittamana tietosuojalain tavoin ilmoitusvelvollisuus viranomaisille sekä tarvittaessa palvelujensa vastaanottajille mahdollisista poikkeamista. (Valtioneuvosto 2023.)

Direktiivin perustama Euroopan kyberkriisien yhteysorganisaatioiden verkosto tukee laajamittaisten tietoturvaloukkausten hallinnointia. Tavoitteena on parantaa jäsenvaltioiden olemassa olevia yhteistyömekanismeja ja tiivistää viranomaisten välistä yhteistyötä. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii Suomen edustajana. (Valtioneuvosto 2023.)

3.2 Tietoturvan osa-alueet

Tietosuoja-asetus velvoittaa rekisterinpitäjää toteuttamaan tarpeelliset toimenpiteet henkilötietojen käsittelyn turvaamiseksi. Organisaation on osattava tunnistaa toimintaansa kohdistuvat tietoturvallisuuteen liittyvät vaatimukset, jotka koskevat myös tietojenkäsittelyä. (EU-tietosuojan kokonaisuudistus 2016, 24.) Tämä tarkoittaa sitä, että laitteistot, ohjelmistot, tietoliikenneyhteydet ja tiedot ovat suojattuna fyysisesti, teknisesti ja toiminnallisesti (Railas 2006, 2).

Tietoturvallisuuden avulla voidaan tataa organisaation käsiteltävän tiedon eheys, käytettävyys ja luottamuksellisuus. Tietoturvallisuuden laajan käsitteen takia on helpompi jakaa aihe eri osa-alueeseen, kuten fyysinen turvallisuus, hallinnollinen turvallisuus, henkilöstö-, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus. Kokonaisuus kattavasti dokumentoituna sekä hyvin johdettuna toimii vahvana perustana organisaation toiminnan jatkuvuudelle, luotettavuudelle, tehokkuudelle ja tuloksellisuudelle. (Tietoturvallisuus ja tulosohjaus 2004, 5.)

Hallinnollisella turvallisuudella tarkoitetaan tietoturvallisuuden johtamista, jonka avulla suunnitellaan ja asetetaan tarvittavat vaatimukset ja tavoitteet organisaation tietoturvallisuudelle kiinnittäen huomiota tasavertaisesti niin fyysiseen kuin tekniseen tietoturvallisuuteen. Hallinnollisella tietoturvallisuudella pyritään varmistamaan tiedon suojaaminen noudattamalla organisaation valmistamaa tietoturvapolitiikkaa. Politiikalla määritellään tietoturvallisuuden vaatimukset voimassa olevan lainsäädännön ja organisaation tarpeiden mukaan. Hyvin toteutetulla tietoturvallisuudella mahdollistetaan organisaation tietojen oikeaoppinen suojaaminen, mikä sitten kasvattaa luottamusta ja lisäarvoa asiakkaiden silmin. (Mitä on hallinnollinen tietoturvallisuus 2020.)

Henkilöstöturvallisuus koostuu henkilöstöstä johtuvasta riskien hallinnasta. Turvallisuuden perustana on ammattitaitoinen henkilöstö, jolle tietoturvavastuut ja -tehtävät ovat selkeästi kirjattuna toimenkuvassa. Tärkeänä osa-alueena ovat siis prosessit, jotka käsittelevät työhönottoa, toimenkuvien muutoksia sekä työsuhteen päättymistä, ja näistä eri osa-alueista on tarpeellista olla käytössä niihin sopivat toimintamallit. (Tietoturvallisuudella tuloksia 2007, 57.)

Fyysisellä turvallisuudella pyritään turvaamaan organisaatioiden häiriötön toiminta kaikissa olosuhteissa ottaen huomioon erilaiset tarpeet sekä mahdolliset riskit. Kyseiseen tietoturvallisuusosa-alueeseen sisältyy kulun- ja kameravalvonta, sekä muut tekniset valvontametodit ja vartiointi sekä muiden fyysisten vahinkojen torjunta, kuten palo-, vesi-, sähkö-, ilmastointi- tai murtovahinko. (Tietoturvallisuudella tuloksia 2007, 59.)

Tietoliikenneturvallisuudella pyritään huolehtimaan tiedonsiirron häiriöttömästä toiminnasta kaikissa olosuhteissa. Organisaation tavoitteena on suunnitella ja toteuttaa verkkojärjestelmät hyvien tiedonhallintatapojen mukaisesti niin, että osataan varautua erilaisia uhkia varten. (Tietoturvallisuudella tuloksia 2007, 61.)

Käyttöturvallisuudella pyritään luomaan sekä ylläpitämään tietotekniikan turvalliset käytön vaatimat toimintaolosuhteet työpaikalla sekä etätöissä. Turvallisuuden toteuttamisesta huolehditaan toimintojen, käytön ja lokien valvonnalla, käyttöoikeuksien hallinnoimisella, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvillä turvallisuustoimenpiteillä sekä varmuuskopioinnilla ja häiriöraporteilla. (Tietoturvallisuudella tuloksia 2007, 66.)

Ohjelmistoturvallisuudella viitataan turvallisuustoimenpiteisiin, jotka kohdistetaan käyttöjärjestelmien, työkaluohjelmien sekä muiden ohjelmistojen kehitykseen, ylläpitoon sekä päivityksiin. Ohjelmistojen turvallisuuteen vaikuttaa vahvasti henkilöstön saama koulutus ja ohjeistus ohjelmistokehityksen prosesseista, ohjelmistojen käytönaikaisten asetusten sekä palvelualustojen asetusten käytöstä. Turvallisuutta voidaan myös parantaa käyttäen muita teknisiä turvakeinoja, kuten asentamalla ajantasaiset turvapäivitysajurit ja -ohjelmat ja aktivoimalla järjestelmien kaikki turvaominaisuudet. (Tietoturvallisuudella tuloksia 2007, 70.)

Laitteistoturvallisuudella viitataan laitteistojen suojaukseen, asennukseen, ylläpitoon ja poistoon liittyviin hallinnollisiin toimenpiteisiin, joissa määritellään omistaja ja hänen turvaluokituksensa sekä laitteiden valvonnan tarve. Laitteistoturvallisuudella pyritään turvaamaan laitteiston elinkaarta, ja tähän sisältyvät asennukset, takuut ja muut tukipalvelut laitteiston elinkaaren loppuun saakka. (Tietoturvallisuudella tuloksia 2007, 63.)

Tietoaineistoturvallisuus käsittelee tietojen eri tallennusmuotojen suojausta, säilytystä, varmuuskopiointia, palauttamista ja tuhoamista. Kyseessä olevat tiedot voivat olla paperiasiakirjoja, optisia ja magneettisia muisti- tai lukuvälineitä, mikrofilmejä, äänitteitä ja muita teknisiä laitteita. Organisaatiolla on vastuu henkilöstön perehdyttämisestä tietoaineistojen käsittelyohjeisiin. (Tietoturvallisuudella tuloksia 2007, 55.)

3.3 Riskienhallinta

Tietosuoja-asetuksessa yhtenä keskeisenä periaatteena on riskilähtöinen lähestyminen, joka sisältää riskien arviointia ja ongelmien ennaltaehkäisemistä. 25. artiklan mukaan on oltava kriittinen ja on otettava huomioon mahdolliset riskit sisäänrakennettua ja oletusarvoista tietosuojaa toteutettaessa. Vaikutustenarvioinnilla pyritään 35. artiklan mukaan rekisterinpitäjän on ennen käsittelyn aloittamista toteutettava arviointi tulevien käsittelytoimien vaikutuksista rekisteröidyn henkilötietojen suojalle, jos koetaan todennäköiseksi käsittelyn aiheuttavan korkeaa riskiä henkilön oikeuksille ja vapauksille. Vaikutustenarviointi on siis oleellinen osa riskienhallinnan kokonaisuutta, koska arvioinnissa suunnitellaan tarvittavat toimenpiteet riskien minimoimiseksi. (Korpisaari ym. 2022, 31; Euroopan parlamentin ja neuvoston asetus (EU), 25., 32., 35. artikla.)

Tietosuoja-asetuksen 24. artikla asettaa velvollisuuden rekisterinpitäjälle huomioida käsittely kokonaislaajuisesti arvioiden sen luonnetta, asiayhteyksiä ja tarkoituksia sekä observoida luonnollisen henkilön oikeuksiin ja vapauksiin suuntautuvat vaihtelevat riskit. Rekisterinpitäjän on identifioitava riskit ja suoritettava tarpeelliset toimenpiteet riskien minimoimiseksi (Euroopan parlamentin ja neuvoston asetus (EU), 25. artikla).

Rekisterinpitäjät ja henkilötietojen käsittelijät ovat velvoitettuja analysoimaan säännöllisesti henkilötietojen käsittelyyn kytkeytyviä riskejä ja valikoimaan riskitason mukaiset hallintatoimenpiteet. Tietosuojariskien hallinta on erinomaista yhdistää osaksi riskienhallintaprosessia, jolloin korkeamman tason riskit voidaan suoraan raportoida johdolle. Nimetty tietosuojavastaava tukee eri yksiköitä, jotta tietosuojariskejä tunnistettaisiin pienemmällä ponnistelulla. (EU-tietosuojan kokonaisuudistus, 21.) Tarpeellisten suojatoimien hahmottamiseksi on tunnistettava, millaisessa ympäristössä tietoa käsitellään ja ketkä kaikki osallistuvat aineiston käsittelyyn (Henkilötietojen käsittelyn elinkaari… s.a.).

Riskitasojen vaihtelevuus riippuu haitan vakavuudesta. Haitta voi olla vakavuudeltaan vähäistä, rajattua, merkittävää tai korkeaa. Vähäisen haittaluokituksen sisällöllä voidaan rekisteröityneelle aiheuttaa ajanhukkaa tai muuta mielipahaa. Rajattu haittaluokitukseen kuuluvat haitat voivat aiheuttaa yksityisyyden loukkauksen tunteen ilman peruuttamatonta vahinkoa. Merkittävä haittaluokituksen sisältyvät haitat voivat pahimmillaan aiheuttaa rekisteröityneelle tunteen perusoikeuksien loukkaamisesta. Korkealla haittaluokituksella tarkoitetaan rekisteröityneelle pitkäaikaista, pysyvää fyysistä tai psykologista aiheutettua haittaa. (Henkilötietojen käsittelyn elinkaari, tietosuojaperiaatteet ja tietojen suojaaminen tieteellisessä tutkimuksessa s.a.) Rekisterinpitäjän on pyrittävä huolehtimaan jatkuvasti riskien pienentämisestä, ettei riskienarvioinnin jälkeen jouduta ottamaan yhteyttä valvontaviranomaiseen. (EU-tietosuoja kokonaisuudistus, 21).

3.4 Tietoturvapolitiikka

Organisaatioiden toiminnan pelisäännöt ovat tyypillisesti kuvattu politiikoiksi. Yhdessä nämä politiikat muodostavat organisaation pelikirjan, jonka avulla ohjataan organisaation kokonaisvaltaista toimintaa. Yhtenä keskeisenä osapuolena organisaation konsernitasolla on määriteltynä tietoturvapolitiikka, joka läpikäydään ja hyväksytään organisaation ylemmän johtoryhmän toimesta. (Sihvonen & Uusi-hautamaa 2019, 105.) Tietoturvapolitiikka määrittelee organisaatiossa tietoturvallisuuden päämäärät, tavoitteet, vastuut ja toteutuskeinot.

Tietoturvapolitiikkaan voi myös kuulua useita eri ohjesäätöjä, kuten tietojärjestelmien käyttöoikeuksien hallinta, joka antaa käytännönläheisiä menettelytapoja järjestelmien käyttöoikeuksien hallitsemisesta. (Ratsula 2016, luku 5.4.)

Tietoturvasuunnittelulla voidaan välittää eri toimintapolitiikoista ja strategioista niihin kirjatut turvallisuustoimenpiteet koko organisaation tavoitteiksi. Organisaation on määritettävä käsittelemänsä tietoaineiston luottamuksellisuuden taso, tiedon käsittelytavat sekä käyttöoikeudet, arkistointi, tiedon poistamisen käytänteet ja menettelytavat normaalioloista poikkeavissa häiriötilanteissa sekä valmiuslaissa määrätyissä poikkeusolosuhteissa. (Tietoturvallisuussuunnitelman laatiminen… 2007, 17.)

Suunnitelman yhteydessä kuuluu laatia kuvaus tiedonkäsittelyn prosesseista, riskien arvioinnista ja riskien poistoon tai minimoimiseen vaadittavat toimenpiteet. Lisäksi suunnitelmaan tulee sisällyttää kuvaus henkilöstön koulutuksesta. Kuvauksen sisältöä käytetään hyväksi suunnitelman laadinnassa sekä siihen perustuvan toimenpide- ja investointiohjelmien valmisteluissa. (Tietoturvallisuussuunnitelman laatiminen… 2007, 17.)

Tietoturvasuunnitelman jatkuvuussuunnitelmassa kuvataan toimenpiteet sellaisissa tilanteissa, jossa estyvät normaalit tietojen käsittelyn mahdollisuudet, eikä tietojen käsittelyä voida toteuttaa tavallisia menetelmiä käyttäen. Edellä mainittujen tilanteiden varalle on arvioitava tiedonkäsittelyn tärkeysjärjestys sekä tarvittavat menettelytavat tiedon tallentamiseksi ja palauttamiseksi ongelmatilanteen poistuessa. (Tietoturvallisuussuunnitelman laatiminen… 2007, 17.)

3.5 Sertifiointi

Rekisterinpitäjä voi halutessaan hakea omalle tietoturvalliselle toiminnalle sertifiointia. Sertifikaatin tarkoituksena on auttaa rekisterinpitäjää ja osoittaa rekisteröidyille asetuksen mukaisen toiminnan toteutumista henkilötietojen käsittelyssä. (Korpisaari ym. 2022, 457–458.)

Sertifikaatin määritelmää ei käsitellä suoranaisesti tietosuoja-asetuksessa, vaan viitataan kansainvälisen standardoimisjärjestön yleistävään määritelmään. Sertifikaatin saavuttaminen vaatii ulkopuolisen tai riippumattoman tahon hyväksyntää tuotteen, palvelun tai järjestelmän kriteerien täyttämisestä. (Korpisaari ym. 2022, 458.) Kansainvälinen standardisoimisjärjestö ISO, eli International Organization for Standardization, täydentää tietosuoja-asetuksen sertifioinnin kriteerit ISO-standardien avulla. Standardit sisältävät sertifiointielinten akkreditointisääntöjä ja toimivaltaisen valvontaviranomaisen tai tietosuojaneuvoston hyväksymiä sertifiointikriteerejä. (Sertifiointia ja sertifiointikriteerien… 2019, 9.)

Tietoturvallisuuden hallintajärjestelmien ISO 27001 -standardin mukaisen sertifioimisen suorittaa akkreditoitu ISO/IEC 17021- ja ISO/IEC 27006 -standardien mukainen sertifiointielin. Sertifioimisen suorittamiseksi rekisterinpitäjän on osallistuttava sertifiointiauditointeihin, jossa suoritetaan tietoturvan johtamisjärjestelmän analyysi sekä arviointi sertifiointia varten. Sertifikaatti on voimassa enintään 3 vuotta, mutta voimassaoloa voidaan jatkaa suorittamalla uudelleensertifioinnilla. (Siivonen 2022.)

4 TIETOTURVAKOULUTUKSEN SUUNNITTELU

Koulutuksen toteutussuunnitelma lähti liikkeelle toimeksiantajan toiveesta valmistaa kaupalliseen käyttöön tarkoitettu verkkokoulutus tietoturvallisuudesta. Alustava suunnittelu toteutettiin yhteistyössä toimeksiantajan tietoturvatiimin kanssa, jonka jälkeen työ toteutettiin pääosin itsenäisesti. Laajan saatavuuden ansiosta koettiin parhaaksi toteuttaa koulutussuunnitelma alustavasti yleisellä tasolla, mikä voisi palvella kaikkia toimeksiantajan asiakkaita.

Toimeksiantajalla oli tarjota käytettäväksi valmis pohja sisäisen henkilöstön turvallisuuskoulutuksesta. Koulutuksen runkoa muokattiin ja laajennettiin käsittelemään tietoturvallisuutta avoimemmin. Yhtenä koulutuksen tavoitteena oli kirjoittaa koulutuksen sisältö mahdollisimman yksinkertaisena ja selkeänä. Sisältö koottiin hyödyntäen Euroopan unionin standardeja, direktiivejä ja Suomen lainsäädäntöä. Lisäksi tietoturvaa koskevia osa-alueita täydennettiin tietoturvallisuuden kirjallisuudella.

4.1 Työpaikalla työskentely

Organisaation toimitiloissa työskentelevä henkilöstö usein tavalla tai toisella käsittelee luottamuksellisia ja salassa pidettäviä tietoja, keskustelee ja analysoi niitä keskenään. Tietosuoja-asetuksella sekä eri tietoturvapolitiikoilla ohjeistetaan henkilöstöä toimimaan tietoturvallisella tavalla niin, ettei organisaatiolle luottamuksellista tietoa vuodateta julkisuuteen.

Organisaation henkilöstö työskentelee työympäristössä, jota valvotaan kulunvalvonnan avulla. Kulunvalvonnalla estetään korkean suojaustason tiloihin kulku ilman myönnettyä oikeutta. Esimerkiksi toimitiloissa liikkuvalla huolto- ja siivoushenkilöstöllä on oltava kulkuluvat, joiden avulla kontrolloidaan pääsyä eri toimitiloihin. Jos työtiloihin saapuu asiattomia henkilöitä, heidät on ohjattava pois paikalta ja suoraan vastaanottopisteelle tunnistautumaan. Henkilöstö tunnistetaan kuvallisesta henkilötunnisteesta ja toimitiloihin saapuessa käytetään henkilökohtaisia kulkutunnisteita tai avaimia. (Toimitilojen tietoturvaohje 2013, 23.)

Luokitellun tietoaineiston käsittely toteutetaan suojatussa työympäristössä. Tiedonkäsittelyn päättyessä tietoaineistoa on säilytettävä salasanalla suojatussa päätelaitteessa, lukitussa kaapissa tai laatikossa. Korkeamman suojaustason tietoaineisto on säilytettävä esimerkiksi kassakaapissa tai holvissa. (Toimitilojen tietoturvaohje 2013, 23.)

Työpisteellä on huolehdittava tietoaineiston näkyvyydestä. Tarpeetonta luokiteltua tietoaineistoa on säilytettävä läsnäolosta riippumatta poissa ulkopuolisten näkökentästä. Puhtaan pöydän periaate koskee luokitellun tietoaineiston lisäksi muita teknisiä laitteita sekä fyysisiä muistilappuja, jotka voivat heikentää organisaation sekä työntekijän tietoturvallisuutta. (Henkilöstön tietoturvaohje 2013, 34.)

4.2 Työskentely organisaation ulkopuolella

Yleisesti etätyöllä tarkoitetaan paikkariippumatonta työntekoa, eli organisaation ulkopuolella tehtävää toimistotyötä (Mönkkönen & Roos 2023, 108, 122).

Etätyötä voidaan tehdä myös matkoilla tai organisaation järjestämissä etätyöpisteissä, jolloin työympäristöt vaihtelevat ja työntekijän on kiinnitettävä huomiota turvallisuuteen. (Henkilöstön tietoturvaohje 2013, 39.)

Työnantajan on järjestettävä etätyöntekijälle työhön tarvittavat laitteet, ohjelmistot sekä tietoliikenneyhteydet. Useat organisaatiot sallivat myös työntekijöiden henkilökohtaisten päätelaitteiden käytön edellyttäen sen, että käytetään esimerkiksi TeamViewer-ohjelmistoa, joka hyödyntää VPN-tunnelointia yhteyden turvaamiseksi. Työhön tarkoitetut työ- ja tunnistusvälineet, laitteistot, ohjelmistot ja erilaiset työaineistot ovat henkilökohtaisia, eikä niiden jakaminen ole sallittua työkavereille tai ulkopuolisille. Etätyössä käytettävät laitteiden ja ohjelmistojen, kuten haittaohjelmien torjuntaohjelmistojen on oltava päivitettynä, jotta ne välttyvät päätelaitteistojen haavoittumiselta. (Henkilöstön tietoturvaohje 2013, 39.)

Etätyöskentely matkoilla tai muutoin julkisella paikalla vaatii erityistä tarkkaavaisuutta ympäristöön. Julkisella paikalla on vältettävä luottamuksellisten tietoaineistoja koskevia keskusteluja sekä huolehdittava päätelaitteiden näköturvallisuudesta asentamalla näytöille turvakalvot, joiden avulla voidaan pienentää kurkistelijoiden määrää ja tietoturvallisuutta koskevia riskejä. Nettikahviloissa ja muissa wlan-yhteyksiä tarjoavissa paikoissa kannattaa vältellä niiden käyttöä. Suositeltavaa on käyttää henkilökohtaista mobiiliverkkoa, mutta jos sellaista mahdollisuutta ole, niin kannattaa käyttää VPN-tunnelointia wlan-yhteyksiä käyttäessään tietoliikenteen suojaamiseksi. Muuten päätelaitteistot alistuvat mahdollisille vakoilu- ja haittaohjelmille. (Järvinen 2022, 219–220.)

4.3 Päätelaitteiden käyttö

Päätelaitteella tarkoitetaan työtehtävien hoitamiseen tarkoitettua elektronista laitetta, joka voi olla työntekijän aseman mukaan älypuhelin, kannettava-, pöytätietokone tai jokin muu vastaavanlainen laite (ICT-ala, ilmasto ja ympäristö 2020, 75). Työkäyttöön annettu päätelaite on henkilökohtainen työväline ja sen turvallisuudesta vastaa työntekijä itse. (Henkilöstön tietoturva ohje 2013, 29.)

Päätelaitteiden tietojenkäsittely voi tapahtua laitteella ja siihen asennetulla ohjelmistolla tai laitteeseen liitetyllä ulkoisella tallennusvälineellä, kuten CD/DVD-levyillä, USB-muisteilla tai kiintolevyillä. Päätelaitteiden käyttöönoton yhteydessä annetaan tarvittavat ohjeet päätelaitteiston tietoturvallisuuden ylläpitoon. Työntekijöiden on kuitenkin oltava jatkuvasti tietoisia kytkettävien tallennusvälineiden alkuperästä, sillä tuntemattomien välineiden käyttö on kiellettyä mahdollisten haittaohjelmien ja virusten takia. (Päätelaitteiden tietoturvaohje 2013, 14; Järvinen 2022, 61–65.)

Laitteiden käyttöä arvioidaan riskienarvioinnin avulla, jonka perusteella määritellään tarkoituksenmukaiset turva-asetukset ja kovennukset eri käyttötilanteille, päätelaitteille ja palveluille sekä päätetään, miten ja minkä suojaustason tietoja voidaan käsitellä eri päätelaitteissa ja palveluissa. (Päätelaitteiden tietoturvaohje 2013, 22.)

Organisaation antamien älypuhelimien yleisasetukset määritellään käyttöönotettaessa. Työpuhelimien tietoturvallisuutta edistetään poistamalla ylimääräiset sovellukset ja palvelut, jotta vältetään luottamuksellisten tietojen vaarantuminen. (Ohjeita viestinnän suojaamiseen s.a., 13.)

Ennen kuin voidaan käsitellä salassa pidettäviä tietoja, tulee varmistaa päätelaitteen tietyn suojaustason vaatimusten täyttyminen. Organisaation tulee asettaa ja lukita päätelaitteiden turva-asetukset haluamalleen suojaustasolle, sekä ottaa käyttöön päätelaitteet keskitettyyn hallintaan, jonka kautta voidaan koventaa ja valvoa laitteiden käyttöä. (Päätelaitteiden tietoturvaohje 2013, 44.)

Päätelaitteiden keskitetyssä hallinnassa organisaation tulee varmistua siitä, että käytetyt hallintapalvelimet ja hallintaan käytettävät päätelaitteet täyttävät turvallisuuden vähimmäiskriteerit. Palvelimien ja laitteiston on oltava valitun suojaustason käsittelykyvyn mukaisia ja teknisesti kovennettuja. Organisaatiot voivat halutessaan tarkentaa ohjeistuksiaan hyödyntämällä kansainvälisiä kovennusohjeita, joita julkaisevat esimerkiksi NIST (National Institute of Standards and Technology) sekä CIS (Center of Internet Security). (Päätelaitteiden tietoturvaohje 2013, 44, 46.)

Päätelaitteiden elinkaari päättyy uudelleenkäyttöönottoon tai käytöstä poistoon. Yhteisenä tekijänä ovat laitteistojen tehdasasetuksiin palautus ennen niiden luovuttamista. Työntekijän on huolehdittava ensi kädessä tietoaineiston tallentamisesta organisaation sisäisiin palvelimiin tai hyväksyttyihin pilvipalvelimiin, jonka jälkeen suojaustason mukaan päätelaitteiden muistit alustetaan, yli kirjoitetaan tai tuhotaan fyysisesti. (Päätelaitteiden tietoturvaohje 2013, 54–55.)

4.4 Salasanat ja tunnistautuminen

Työntekijä voi tunnistautua organisaation ja julkisen palvelun tietojärjestelmiin tai päätelaitteisiin kirjautumalla sisään käyttäjätunnuksella sekä vaihtoehtoisella tunnistautumistavalla. Tietoturvallisuuden tunne koostuu hänen asettamastaan salasanan vahvuudesta, tunnistautumismuodosta sekä tietojärjestelmän toimintavarmuudesta. Vahvistamalla salasanan rakennetta ja hyödyntämällä erilaisia tunnistautumismuotoja voidaan edistää tietoturvaa tietojärjestelmissä.

Vahvan salasanan tunnuspiirteinä on vähintään 15 merkin pituus, pienet sekä isot kirjaimet ja erikoismerkkejä sisältävä kokonaisuus. Salasana voidaan muodostaa myös useista sanoista tai lauseesta, joka on myös helpompi muistaa ja kirjoittaa verrattuna merkkisarjaan. (Järvinen 2022, 94–96.)

Samanlaisten salasanojen käyttöä eri tietojärjestelmissä tulee välttää. Työntekijän on tehtävä yksilölliset salasanat suojatakseen muiden järjestelmien käyttäjätunnukset. Organisaation tietojärjestelmät voivat vaatia säännöllisesti salasanojen vaihtoa, jolla pyritään estämään mahdollisten tietovuotojen aiheuttamia vahinkoja. (Järvinen 2022, 96.)

Salasanojen kirjoittaminen muistiin ja säilyttäminen on sallittua, kun ne eivät ole helposti löydettävissä. Työntekijä ei saa myöskään luovuttaa käyttäjätunnuksia, salasanoja tai muita tunnistautumisvälineitä toisen henkilön käyttöön. Yhteiskäyttöön tarkoitettuja tunnuksia voidaan jakaa toisten kanssa vain silloin, kun siihen annetaan omistajan perusteltu lupa. (Henkilöstön tietoturvaohje 2013, 31.)

Päätelaitteisiin voidaan asentaa organisaation luvalla salasanojen hallintaohjelma, joka muodostaa valittuihin palveluihin salasanat ja tallentaa ne automaattisesti suojattuun tietojärjestelmään. Työntekijän vastuuna on luoda yksilöllinen vahva pääsalasana hallintaohjelman käyttöä varten. Hallintaohjelman käyttö toimii kaksivaiheisen tunnistautumisen tavoin, jossa käyttäjä tunnistautuu käyttäjätililleen käyttäen toista tunnistautumismuotoa. (Kyberturvallisuuskeskus 2020.)

Tunnistautumisella tarkoitetaan digitaalista pääsyä fyysisen pääsyn tueksi. Tunnistautuminen perustuu vähintään yhteen seuraavista tiedoista

- tieto, kuten salasanat, PIN-koodit
- omistus, kuten turva-avaimet (FIDO2), kulkukortit (RFID) tai Tokenit
- biometrinen tunniste, kuten sormenjäljet tai kasvotunnisteet.

Yhden tai useamman tunnistetiedon käyttö lisää merkittävästi turvallisuutta, mutta niiden käyttö ei kuitenkaan takaa käyttäjälle vedenpitävää turvaa. (Tunnistautumistavat s.a.)

4.5 Haittaohjelmat

Tietoturvaongelmat syntyvät uusien toimintamallien, palveluiden sekä tietoturvauhkien yhdistelmästä. Merkittävimmät tietoturvauhat perustuvat käyttäjän omaan toimintaan ja rikollisten, ääriryhmien tai valtioiden pyrkimyksistä saada haltuunsa tietoja tai vaikuttaa negatiivisesti organisaation toimintaan, talouteen ja liiketoiminnan jatkuvuuteen. (Kyberturvallisuus ja yrityksen hallituksen vastuu 2020, 4.)

Rikolliset hyödyntävät usein sosiaalisen median palveluita, pilvipalveluita ja muita viestintäjärjestelmiä levittämällä niiden kautta erilaisia haittaohjelmia, jotka ottavat haltuunsa päätelaitteen sekä sen sisällön (Kyberturvallisuus ja yrityksen hallituksen vastuu 2020, 6). Rikollisjärjestöt halutessaan hyödyntävät kaapattuja päätelaitteita botnet-verkkona erilaisiin käyttötarkoituksiin, kuten palvelinestohyökkäyksiin, tietomurtoihin tai salasanayhdistelmien paljastamiseen. (Sosiaalisen median tietoturvaohje 2010, 13.)

Ikävimmät haittaohjelmat kuuluvat kiristysohjelmien joukkoon. Saastuttaessaan käyttäjän päätelaitteen, ohjelma lukitsee tai salaa luottamuksellisia tietoja ja vaatii niistä lunnaita. Ohjelmaan usein integroidaan ajastin, joka määrätyn ajan jälkeen tuhoaa tai vuodattaa tiedot julkisuuteen. Lunnaita pyydetään usein kryptovaluutan muodossa, koska niiden siirtäminen on helppoa ja pitkälti jäljittelemätöntä. Lunnaita maksavalla uhrilla ei ole muuta vaihtoehtoa kuin luottaa rikollisen sanaan. Huonoimmassa tapauksessa uhrille ilmoitetaan jatkokiristyksestä, jossa uhataan tietojen julkaisua maksusta huolimatta. (Järvinen & Rousku. 2017, 3. luku.)

Ohjelmien levittäminen perustuu massajakeluun luottaen ihmisten uteliaisuuteen. Useita kiristysohjelmia levitetään sähköpostin Word -tiedostoliitteissä, koska niitä on vaikeampi havaita virustarkistuksissa. Word -tiedostoon kirjoitetaan makrokielellä koodisarja, joka aktivoituu dokumentin avautuessa. Aktivoituessaan rikollinen saa pääsyn järjestelmään ja siten salaa haluamansa tiedostot. (Järvinen & Rousku. 2017, 3. luku.)

4.6 Sosiaalinen media ja viestintä

Sosiaalisen median palveluiden käyttö asettaa organisaatiolle ja työntekijöille lisävastuuta. Työnantajan on ohjeistettava työntekijälle verkkoyhteyksien käytöstä päätelaitteistolla työpaikalla niin myös organisaation ulkopuolella. Organisaation verkkoyhteyksien käyttö työntekijän omiin tarpeisiin on oltava pääsääntöisesti kiellettyä, poikkeuksena ammattiinsa liittyvää tiedonhankinta tai omien sähköpostien lukeminen. Mobiililaitteiden käyttö voi olla perusteltua esimerkiksi työnantajan luvalla tai toimenkuvan toimesta. (Järvinen & Rousku. 2017, 5. luku.)

Monet sosiaalisen median palveluita käyttävät organisaatiot hyödyntävät mediaa markkinoinnin ja organisaatiokuvan luomisessa. Mediaa hyödynnetään myös myynnin ja asiakaspalvelun kanavana. Organisaatioiden linjaukset sosiaalisen median käytöstä ovat usein rajoittavia varmistaakseen työtehtävien toteutuminen tai organisaation imagon säilyttäminen. (Järvinen & Rousku. 2017, 5. luku.)

Kommunikoidessa organisaatiota koskevista asioista henkilökohtaisella tai työpaikan käyttäjätunnuksilla, työntekijän on muistettava, että hän edustaa organisaatiota. Kaikki sosiaalinen kanssakäynti vaikuttaa epäsuorasti organisaation imagoon. Jokainen vastaanottaja lukee ja tulkitsee viestit kirjaimellisesti, joten huolimattomasti kirjoitetut viestit voivat aiheuttaa väärinkäsityksiä ja ongelmia. (Järvinen & Rousku. 2017, 5. luku.)

Työntekijän olisi hyvä pitää erossa henkilökohtaisen ja työpaikan sähköpostiosoitteiden käytön, jottei käy niin, että työsuhteen päättyessä työhön sekä vapaa-aikaan liittyvät tiedot poistetaan ja palveluiden tai palautusosoitteiden käyttö estyy osoitteen de-aktivoituessa. Organisaatiossa voidaan seurata työntekijöiden toimintaa työnantajan tai palveluntarjoajan toimesta, joten työntekijän yksityisyyden kunnioittamiseksi on parempi pitää henkilökohtainen elämä erossa työhön liittyvistä osoitteista. (Järvinen & Rousku. 2017, 5. luku.)

Luottamuksellisten tietojen välittäminen sähköpostipalveluiden välillä vaatii yhteyden suojaamista. Suojattu yhteys määritellään sähköpostipalvelun yhteysasetuksessa, jonka jälkeen tietokoneen ja palvelimen välinen yhteys voidaan salata mahdollisilta salakuunteluilta. Selainsähköpostia käyttäessä on varmistettava selaimen SSL-suojaus, joka salaa päätelaitteen ja palvelimen välisen verkkoliikenteen ja varmentaa sivuston aitouden. (Ohjeita viestinnän suojaamiseen s.a. 9.)

4.7 Tiedon luokittelu ja käsittely

Organisaatiolla tulee olla selkeät ohjeet tiedon käsittelylle ja luokittelulle, sillä luottamuksellisen tiedon oikeaoppinen käsittely on yksi osa tietoturvallista työskentelyä. Työskentelyssä on huolehdittava julkisten tietojen eheydestä, luotettavuudesta sekä niiden saatavuudesta. (Järvinen & Rousku. 2017, 2. luku.)

Tietoturvallisuuden näkökulmasta on suositeltavaa jakaa tietoaineisto julkiseen ja salassa pidettävään tietoon. Salassa pidettävä tieto katsotaan joko luokittelemattomaksi tai luokitelluksi. Luokiteltu tietoaineisto voidaan jakaa kuva 2. ohjeistuksen mukaan sisäiseksi, luottamukselliseksi, salaiseksi tai erittäin salaiseksi. (Tietoturvallisuudella tuloksia 2007, 84.)

Kuva 2. Tietoaineiston luokitustaulukko (Tietoturvallisuudella tuloksia 2007, 84)

Henkilötietojen käsittelijät ovat henkilökohtaisesti vastuussa dokumenttien luokittelusta ja salassapidosta kertovan tunnisteen merkitsemisestä. Salassa pidettäviä tietoja on käsiteltävä organisaation ohjeistuksien mukaisesti. (Henkilöstön tietoturvaohje 2013, 26.) Luokitus voi kuitenkin muuttua, kun henkilötietojen säilytysaika tai käsittelyn tarve loppuu ja kyseisille tiedoille on tehtävä organisaation ohjeistuksen mukaiset toimenpiteet. Tarve muutokselle syntyy myös sisällön muuttuessa arkaluontaiseksi tai sisältöä tarkennetaan tunnistamisen helpottamiseksi. Markkinointia varten voidaan muuttaa luokitus julkiseksi, jolloin organisaatio voi vapaasti käyttää tiettyjä asiakasprojekteja koskevia tietoja kuten asiakaskokemuksia. Luokituksen poistamisesta tai muuttamisesta on tehtävä asianmukaiset merkinnät alkuperäiseen dokumenttiin. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010, 3. luku 10. §.)

Tietojen käsittelijällä on oikeus käsitellä tietoja niitä vaativiin työtehtäviin. Käsittelyn lainmukaisuutta valvotaan tieto- ja käyttöoikeusjärjestelmien avulla. (Henkilöstön tietoturvaohje 2013, 26.)

4.8 Tallentaminen ja varmuuskopiointi

Organisaation henkilöstölle tulee olla ohjeistettuna luottamuksellisten tietojen käsittelystä ja niiden tallentamisesta sekä varmuuskopioinnista. Tiedot on luokiteltava ja siten tallennettava eri suojaustason palvelimiin, jotta pääsy korkeamman suojatason tietoaineistoihin estetään sivullisilta. (Katakri 2020, 29.)

Salassa pidettävien tietojen tallentaminen, siirtäminen ja arkistoiminen voidaan toteuttaa eri tallennusvälineillä ja tavoilla, kuitenkin vain organisaation antamien ohjeiden mukaisesti. Organisaation on tehtävä riskianalyysin pohjalta päätös tallennusvälineiden ja palveluiden käytöstä sekä tietojen tallennuksesta valittuihin muotoihin. Tiedot tallennetaan pääsääntöisesti organisaation sisäisiin palvelimiin tai erikseen määriteltyihin pilvitallennuspalveluihin, kuten Microsoft 365- (OneDrive) tai Teams -palveluohjelmistoihin. Tallennettaessa luottamuksellista tietoa ulkoisiin tallennusvälineihin työntekijän on salattava tietoaineisto ja tallennusvälineet, sekä huolehdittava fyysisestä turvallisuudesta säilyttämällä välineet suojatussa tilassa. (Henkilöstön tietoturvaohje 2013, 12, 26.)

Varmuuskopioinnilla tarkoitetaan tietoaineiston turvaamista kopioimalla ja varastoimalla ne myöhempää käyttöä varten. Varmuuskopiointia tarvitaan tietoaineiston korruptoituessa tai hävitessä. Varmistaakseen tietoaineiston eheys on hyvä varmuuskopioida aineisto säännöllisin ajoin, jotta voidaan vähentää menetetyn tiedon määrän. Kopioitu aineisto on suojattava asianmukaisilla suojaustason menetelmillä ja tallennettava organisaation määrittelemiin sisäisiin palvelimiin. (Katakri 2020, 104.)

Tarpeettomaksi tulleet tietoaineistot on arkistoitava tai tuhottava organisaation ohjeistuksien mukaisesti. Arkistoitavat tiedot sijoitetaan tietoturvallisella tavalla elektroniseen muotoon, jotta voidaan varmistaa tiedon säilyvyyden myöhempää käyttöä varten. Tietoaineisto on muutettava helposti luettavaan ja saatavaan muotoon huomioiden tiedon säilytysajan, -paikan ja -tavan. (Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta 2020, 24.)

Tuhottavien tietoaineistojen menetelmät riippuvat siitä, minne ja miten tiedot on tallennettu. Tuhoamisella estetään tietojen kokoaminen alkuperäiseen luettavaan muotoon. Salassa pidettävä aineiston tuhoaminen onnistuu silppurilla, polttamisella tai tuhoamisella. Sähköisessä muodossa olevien tietoaineistojen tuhoaminen tapahtuu salaamalla tiedot ja poistamalla ne lopullisesti organisaation ohjeiden mukaisesti. (Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta 2020, 25.)

4.9 Poikkeamat, loukkaukset ja niistä palautuminen

Poikkeamalla tarkoitetaan tilannetta, jossa tapahtuu inhimillinen tai tarkoituksellinen virhe, joka aiheuttaa potentiaalista vaaraa rekisteröidyille. Tietoturvaloukkaus käsitettä käytetään, kun poikkeamasta aiheutuu ongelmia organisaatiolle sekä rekisteröidyille. Tietoturvaloukkauksen sattuessa organisaation määrittämä rekisterinpitäjä on velvoitettu ilmoittamaan valvontaviranomaiselle tapahtuneesta 72 tunnin kuluessa siitä, kun loukkaus havaittiin. (EU-tietosuojan kokonaisuudistus 2016, 26.)

Välttyäkseen tietoturvaloukkauksilta organisaation on osattava havaitsemaan poikkeamat ympäristöstään. Yhdessä rekisterinpitäjän ja tietosuojavastaavan kanssa organisaation on luotava havainnollistavat dokumentaatiot erilaisista poikkeuksista ja teetettävä niiden pohjalta ohjeistuksia, joiden avulla henkilöstöä koulutetaan tunnistamaan ongelmakohdat sekä toimimaan ja ilmoittamaan niistä ohjeiden mukaisesti. (EU-tietosuojan kokonaisuudistus 2016, 26–27.)

Tietoturvallisuussyistä kaikista työvälineiden, tunnistusesineiden tai päätelaitteiden katoamisista ja rikkoutumisista on ilmoitettava esimiehelle tai IT-tuelle, jotta voidaan rajoittaa tilapäisesti käyttöoikeuksia ja siten pienennetään tietoturvariskejä. Tapaukset loukkauksista tai haittaohjelmientartunnoista on dokumentoitava alusta loppuun ja toimittava ohjeistuksien mukaisesti ongelman pysäyttämiseksi tai rajoittamiseksi. (Henkilöstön tietoturvaohje 2013, 43–44.)

Tietoturvaloukkausten varalta organisaatiot toteuttavat erilaisia varautumistoimenpiteitä. Toimenpiteillä tarkoitetaan esimerkiksi riskienarviointia, jatkuvuus- ja valmiussuunnittelua, koulutuksia ja harjoituksia, joiden avulla varmistetaan

organisaation mahdollisimman häiriötön toiminta, sekä jatkuminen häiriötilanteiden aikana sekä niiden jälkeen. Tilanteen sattuessa työntekijän on adaptoiduttava tilanteeseen toimimalla ohjeistuksien mukaisesti, usein tällä tarkoitetaan siirtymistä sähköisestä fyysiseen työskentelyyn. Hyvin toteutetuilla suunnitelmilla organisaatiolla on hyvät mahdollisuudet toipua häiriötilanteista lyhyellä aikavälillä ja pienellä taloudellisella menetyksellä. (Toiminnan jatkuvuuden hallinta 2016, 23–26, 36.)

5 TOTEUTUS JA POHDINTA

Tämän opinnäytetyön tarkoituksena oli toteuttaa Digia Oyj:n tietoturvatiimille tietoturvallisuuskoulutuksen suunnitelma, joka palvelisi heitä verkkokoulutuksen toteutuksessa. Digialla ei siis ole omaa kaupalliseen käyttöön tarkoitettua verkkokoulutusjärjestelmää, jonka vuoksi suunnitelman toteutuksen toivottiin sisältävän laajalti tietoaineistoa eri tietoturvallisuuden osa-alueista voidakseen palvella jokaisen toimialan asiakasta.

Opinnäytetyön alkuvaiheessa tarkoituksena oli toteuttaa tietosuojaa sekä -turvallisuutta koskeva koulutussuunnitelma. Opinnäytetyö toteutettiin syventävän harjoittelun ohella ja harjoittelun ohjaajan kanssa käytiin säännöllisin ajoin Teams-palaverien välityksellä keskustelua työn toteutumisesta. Työnteon helpottamiseksi annettiin koulutusrungon raakaversio, johon tarkoituksena oli lisätä puutteellisuudet ja omat ideat koulutuksen kehittämiseksi. Koulutussuunnitelman tekoon koettiin tarpeelliseksi tuoda esille opinnäytetyön teoria- ja produktio-osion sisältö, lisäksi toivottiin organisaation tarjoamien lähteiden ja esimerkkien hyödyntämistä.

Koulutussuunnitelman keskivaiheessa osallistuin muutamiin Digian sekä kolmannen osapuolen välisiin palavereihin, joissa keskusteltiin verkkokoulutusalustan suunnittelusta sekä toteutuksesta. Koulutussisältöön toivottiin monipuolisuutta koskien eri toimialoja sekä syventävää oppimateriaalia. Verkkoalustaan suunniteltiin moduulipohjaista kouluttamista, jossa hyödynnettäisiin nano oppimisen periaatteita. Yhteistyökumppanuudelle ei kuitenkaan saatu jatkoa tarjouspyynnön summan takia. Digialla ollaan siitä huolimatta itsevarmoja projektin toteutumisesta, koska siihen varattiin toteutumisaikaa yli puoli vuotta. Etukäteen varattu toteutumisaika omalta osalta tarkoittikin sitä, että

työni jää kesken ja sitä jatketaan eteenpäin harjoittelun päätyttyä. Opinnäytetyöhön liitettiinkin tästä syystä vain suunnitelman sisällysluettelo.

Koulutustaustan takia opinnäytetyötä käsittelin mahdollisimman paljon juridiikan näkökulmasta. Valitun näkökulman ansiosta opinnäytetyön teoreettinen osuus saatiin täydennettyä lyhyellä aikavälillä, mutta kirjoittaessa tuli huomattua monien eri lähteiden lainanneen suoraan tietosuoja-asetuksen ja eri lainsäädännön sisältöä. Välttyäkseen lainsäädännön tahattomalta muokkaamiselta päädyin käyttämään alkuperäistä lakitekstiä tukena teoreettisen osan teossa. Lisäksi tutkiessani eri lainsäädännön kytköksiä toisiinsa, jouduin tekemään vaikean päätöksen, eli työn määrää oli rajoitettava, jotta opinnäytetyön tekeminen määräaikaan mennessä olisi mahdollista.

Kirjallisuuden sekä monien eri verkkolähteiden ansiosta produktio-osuuden teko onnistui suhteellisen vaivattomasti. Useasti esille tulleet lähteet olivat valtionvarainministeriön julkaisemia VAHTI-ohjeita. Julkaisupäivämäärästä huolimatta useat eri ohjeet voidaan todeta edelleen ajankohtaisiksi suurimmalta osalta, sillä nykypäivänä nettirikollisuuden kasvaessa syntyy myös erilaisia haittaohjelmia. Produktio-osuudessa ei käsitellä kaikkea koulutussuunnitelmaan kirjatuista asioista, sillä ne käydään jo teoriaosuuksissa läpi. Tämän lisäksi osa produktio-osuuden sisältöä on hieman supistettu välttyäkseen opinnäytetyön liialliselta kasvulta.

Tietoturvallisuutta koskevan koulutuksen suunnittelussa ja toteutuksessa huomasin oppivan jatkuvasti jotain uutta itsestäni, lainsäädännöstä, tietosuoja-asetuksesta ja tietoturvallisuudesta. Koin suurta apua säännöllisistä Teams-palavereista ja sain aina tarvittaessa ohjeita tiedonsaantiin sekä lähteisiin. Uskon jatkavan tästä eteenpäin kohti tietoturvallisuuden alaa, sillä kyseessä on erittäin mielenkiintoinen kokonaisuus ja tällä kyseisellä alalla on jatkuva tarve asiantuntijoille.

LÄHTEET

Data ja analytiikka. 2023. Digia Oyj. WWW-dokumentti. Saatavissa: https://digia.com/palvelumme/data-ja-analytiikka/ [viitattu 14.3.2023].

Digia Oyj. 2023. Digia yrityksenä. WWW-dokumentti. Saatavissa: https://digia.com/yritys/#digia-yrityksena [viitattu 7.3.2023].

EU-tietosuojan kokonaisuudistus. 2016. Valtiovarainministeriön julkaisu. PDF-dokumentti. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI-raportti_1_2016_pdf.pdf [viitattu 16.3.2023].

Euroopan komissio. 2023. Direktiivi toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa (NIS2-direktiivi). WWW-dokumentti. Päivitetty 16.1.2023. Saatavissa: https://digital-strategy.ec.europa.eu/fi/policies/nis2-directive [viitattu 23.3.2023].

Euroopan unionin perusoikeuskirja. 2000. Euroopan yhteisöjen virallinen lehden julkaisu. PDF-dokumentti. Saatavissa: text_fi.pdf (europa.eu) [viitattu 14.3.2023].

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.

Erityislainsäädäntö s.a. Tietosuojavaltuutetun toimisto. WWW-sivusto. Saatavissa: https://tietosuoja.fi/erityislainsaadanto [viitattu 14.3.2023].

Henkilöstön tietoturva ohje. 2013. Valtionhallinnon tietoturvallisuuden johtoryhmän julkaisuja 2013:4. Helsinki: Valtiovarainministeriö. PDF-dokumentti. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/Vahti_4_2013_pdf.pdf [viitattu 14.3.2023].

Henkilötietojen käsittely s.a. Tietosuojavaltuutetun toimisto. WWW-sivusto. Saatavissa: https://tietosuoja.fi/henkilotietojen-kasittely [viitattu 15.3.2023].

Henkilötietojen käsittelyn elinkaari, tietosuojaperiaatteet ja tietojen suojaaminen tieteellisessä tutkimuksessa s.a. Tietosuojavaltuutetun toimisto. WWW-sivusto. Saatavissa: https://tietosuoja.fi/henkilotietojen-kasittelyn-elinkaari-tietosuojaperiaatteet-ja-tietojen-suojaaminen [viitattu 16.3.2023].

ICT-ala, ilmasto ja ympäristö. 2020. Liikenne- ja viestintäministeriön julkaisuja 2020:9. Helsinki: Liikenne- ja viestintäministeriö. PDF-dokumentti. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162307/LVM_2020_9.pdf?sequence=1&isAllowed=y [viitattu 13.5.2023].

Järvinen, P. 2022. Yrityksen tietoturvaopas. Viro: Meedia OU. E-kirja. Saatavissa: https://ezproxy.xamk.fi/login?url=https://kauppakamaritieto.fi/ammattik...rvaopas-2022 [viitattu 12.5.2023].

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas. Helsinki: Alma Talent. E-kirja. Saatavissa: https://bisneskirjasto-almatalent-fi.ezproxy.xamk.fi/teos/BAFBBXXTBBAED#piste:b0 [viitattu 14.3.2023].

Katakri. 2020. Tietoturvallisuuden auditointityökalu viranomaisille. PDF-dokumentti. Saatavissa: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246 [viitattu 19.4.2023].

Kauppalehti. 2023. Digia Oyj. WWW-dokumentti. Saatavissa: https://www.kauppalehti.fi/yritykset/yritys/digia+oyj/0831312-4 [viitattu 7.3.2023].

Keller, M. 2023. Mitä on tietosuoja. Helsinki: Alma Talent. E-kirja. Saatavissa: https://verkkokirjahylly-almatalent-fi.ezproxy.xamk.fi/teos/23ju123456 [viitattu 12.5.2023].

Kirjanpitolaki 30.12.1997/1336.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2022. Tietosuoja. Helsinki: Alma Talent. E-kirja. Saatavissa: https://verkkokirjahylly-almatalent-fi.ezproxy.xamk.fi/teos/CAIBCXETEB#kohta:Tietosuoja [viitattu 21.3.2023].

Kyberturvallisuus ja yrityksen hallituksen vastuu. 2020. Traficomin julkaisuja 2020:2. Helsinki: Liikenne- ja viestintävirasto Traficom. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf [viitattu 13.5.2023].

Kyberturvallisuuskeskus. 2020. Neuvoja salasanan hallintasovelluksen käyttöönottoon. Päivitetty 25.01.2023. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon [viitattu 13.4.2023].

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

Mikä on henkilötieto s.a. Tietosuojavaltuutetun toimisto. WWW-sivusto. Saatavissa: https://tietosuoja.fi/mika-on-henkilotieto [viitattu 16.3.2023].

Milloin henkilötietoja saa käsitellä? s.a. Tietosuojavaltuutetun toimisto. WWW-sivusto. Saatavissa: https://tietosuoja.fi/kasittelyperusteet [viitattu 15.3.2023].

Mitä on hallinnollinen tietoturvallisuus. 2020. Seclion. Blogi. Saatavissa: https://blog.seclion.fi/turvallisuus/hallinnollinen-tietoturvallisuus [viitattu 22.3.2023].

Mönkkönen, K. & Roos, S. 2023. Työyhteisötaidot digiajassa. Helsinki: Gaudeamus. E-kirja. Saatavissa: https://www.ellibslibrary.com/xamk/9789523458321 [viitattu 13.5.2023].

Nasdaq. 2023. Digia, Digia Oyj. WWW-dokumentti. Saatavissa: https://www.nasdaqomxnordic.com/aktier/microsite?Instrument=HEX24367&name=Digia%20Oyj&ISIN=FI0009007983 [viitattu 7.3.2023].

Ohjeita viestinnän suojaamiseen s.a. Viestintävirasto. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_viestinnan_suojaamiseen.pdf [viitattu 16.4.2023].

Oikeus saada tietoa henkilötietojen käsittelystä s.a. Tietosuojavaltuutetun toimisto. WWW-sivusto. Saatavissa: https://tietosuoja.fi/oikeus-saada-tietoa-kasittelysta [viitattu 18.3.2023].

Pulkkanen, A. 2021. Henkilöstön tietoturvakoulutus ja tietoturvaohjeistus digiturvamallissa. Blogi. Saatavissa: https://www.digiturvamalli.fi/blogi/henkiloston-tietoturvakoulutus-ja-tietoturvaohjeistus-digiturvamallissa [viitattu 7.3.2023].

Pseudonymisoidut ja anonymisoidut tiedot s.a. Tietosuojavaltuutetun toimisto. WWW-sivusto. Saatavissa: https://tietosuoja.fi/pseudonymisointi-anonymisointi [viitattu 16.3.2023].

Päätelaitteiden tietoturvaohje. 2013. Valtionministeriön julkaisuja 5/2013. Helsinki: Valtionvarainministeriö. PDF-dokumentti. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_5_2013_pdf.pdf [viitattu 11.4.2023].

Railas, L. 2006. Tietoturvallisuuslainsäädäntö: Kansainvälinen vertailututkimus. Luoti- julkaisuja 4/2006. Helsinki: Liikenne- ja viestintäministeriö. PDF-dokumentti. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78507/4_2006.pdf?sequence=1 [viitattu 22.3.2023].

Ratsula, N. 2016. Compliance – Eettinen ja vastuullinen liiketoiminta. Helsinki: Alma Talent. E-kirja. Saatavissa: https://verkkokirjahylly-almatalent-fi.ezproxy.xamk.fi/teos/FAIBEXCTEB#kohta:COMPLIANCE((20 [viitattu 22.3.2023].

Rikoslaki 19.12.1889/39.

Sertifiointia ja sertifiointikriteerien määrittelemistä asetuksen 42 ja 43 artiklan mukaisesti koskevat suuntaviivat 1/2018. 2019. European Data Protection Board julkaisuja 2019:4. Euroopan Unioni: European Data Protection Board. PDF-dokumentti. Saatavissa: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_fi.pdf [viitattu 23.3.2023].

Sihvonen, J. & Uusi-hautamaa, L. 2019. Väärinkäytökset yrityksessä – Estä, havaitse, korjaa. Helsinki: Alma Talent. E-kirja. Saatavissa: https://verkkokirjahylly-almatalent-fi.ezproxy.xamk.fi/teos/FABBXXBTAB-DED#kohta:((2013)((20)Est((e4),((20)havaitse,((20)korjaa((20)/piste:b7 [viitattu 22.3.2023].

Siivonen, M. 2022. ISO 27001 -sertifiointi. DQS Finland Oy. WWW-sivusto. Saatavissa: https://www.dqsglobal.com/fi-fi/sertifioi/iso-27001-sertifiointi [viitattu 22.3.2023].

Sosiaalisen median tietoturvaohje. 2010. Valtionvarainministeriön julkaisuja 4/2010. Helsinki: Valtionvarainministeriö. PDF-dokumentti. Saatavissa:

https://www.suomidigi.fi/sites/default/files/2020-06/Ohje_4_2010_etusivu_ohjepdf.pdf [viitattu 16.4.2023].

Suomen Asiakastiedolle seuraamusmaksu tietosuojavaltuutetun määräyksen noudattamatta jättämisestä. 2023. Tietosuojavaltuutetun toimisto. WWW-dokumentti. Päivitetty 2.3.2023. Saatavissa: https://tietosuoja.fi/-/suomen-asiakastiedolle-seuraamusmaksu-tietosuojavaltuutetun-maarayksen-noudattamatta-jattamisesta [viitattu 12.5.2023].

Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta. 2020. Valtiovarainministeriön julkaisuja 2020:21. Helsinki: Valtionvarainministeriö. PDF-dokumentti. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162150/VM_2020_21.pdf?sequence=1&isAllowed=y [viitattu 19.4.2023].

Tietosuojalaki 5.12.2018/1050.

Tietosuojalaki s.a. Tietosuojavaltuutetun toimisto. WWW-sivusto. Saatavissa: https://tietosuoja.fi/tietosuojalaki [viitattu 14.3.2023].

Tietosuojavaltuutetun toimisto s.a. Tietosuoja. WWW-sivusto. Saatavissa: https://tietosuoja.fi/tietosuoja [viitattu 14.3.2023].

Tietosuojavaltuutetun tehtävät s.a. Tietosuojavaltuutetun toimisto. WWW-sivusto. Saatavissa https://tietosuoja.fi/tehtavat [viitattu 21.3.2023].

Tietoturvallisuudella tuloksia. 2007. Valtionvarainministeriön julkaisuja 3/2007. Helsinki: Valtionvarainministeriö. PDF-dokumentti. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_3_2007.pdf [viitattu 22.3.2023].

Tietoturvallisuus ja tulosohjaus. 2004. Valtionvarainministeriön julkaisuja 2/2004. Helsinki: Valtionvarainministeriö. PDF-dokumentti. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_2_2004.pdf [viitattu 22.3.2023].

Tietoturvallisuussuunnitelman laatiminen: Opas sosiaali- ja terveydenhuollon toimintayksiköille. 2007. Sosiaali- ja terveysministeriön julkaisuja 2007:19. Helsinki: Sosiaali- ja terveysministeriön julkaisuja 2007:19. PDF-dokumentti. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/71714/julkaisuja_2007_19_tietoturvallisuussuunnitelma_verkko.pdf?sequence=1 [viitattu 22.3.2023].

Toimitilojen tietoturvaohje. 2013. Valtionvarainministeriön julkaisuja 2/2013. Helsinki: Valtionvarainministeriö. PDF-dokumentti. Saatavissa: https://www.finlex.fi/data/normit/41654/Toimitilojen_tietoturvaohje_VAHTI_2_2013_netti.pdf [viitattu 17.4.2023].

Tunnistautumistavat s.a. Digiturvamalli. WWW-dokumentti. Saatavissa: https://www.digiturvamalli.fi/konsepti/tunnistautumistavat [viitattu 13.4.2023].

Työelämän tietosuojan käsikirja. 2020. Tietosuojavaltuutetun toimiston julkaisuja. PDF-dokumentti. Saatavissa: https://tietosuoja.fi/documents/6927448/8214540/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+2020-+Tietosuojavaltuutetun+toimisto.pdf [viitattu 14.3.2023].

Valtioneuvosto. 2023. Kyberturvallisuusdirektiivi vahvistaa koko EU:n kyberturvallisuustasoa – kansallinen toimeenpanohanke käynnistyi. WWW-dokumentti. Päivitetty 9.1.2023. Saatavissa: https://valtioneuvosto.fi/-/kyberturvallisuusdirektiivi-vahvistaa-koko-eu-n-kyberturvallisuustasoa-kansallinen-toimeenpanohanke-kaynnistyi [viitattu 23.3.2023].

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010.

Vartiainen, S. 2016. Henkilötiedon elinkaari ja tietosuoja yritystoiminnassa. PWC. WWW-dokumentti. Saatavissa: https://uutishuone.pwc.fi/undefined/henkilotiedon-elinkaari-ja-tietosuoja-yritystoiminnassa [viitattu 16.3.2023].

Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Jyväskylä: Tammi.

Kuvaluettelo

Liite 1

Tietoturvakoulutuksen sisällysluettelo