LAPIN AMK
Lapland University of Applied Sciences

# TIETOTURVAOPPAAN JA -KOULUTUKSEN SUUNNITTELU JA TOTEUTUS

CASE: Eduro-säätiö

Collins Johannes

Opinnäytetyö
Tietojenkäsittely ja tieto- ja viestintätekniikka
Tietojenkäsittelyn koulutus
Tradenomi (AMK)

2019

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tietojenkäsittely ja tieto- ja viestintätekniikka
Tietojenkäsittelyn koulutus
Tradenomi (AMK)


| | | | |
|---|---|---|---|
| **Tekijä** | Johannes Collins | Vuosi | 2019 |
| **Ohjaaja(t)** | Jari Sarja | | |
| **Toimeksiantaja** | Eduro-säätiö | | |
| **Työn nimi** | Tietoturvaoppaan ja -koulutuksen suunnittelu ja toteutus CASE: Eduro-säätiö | | |
| **Sivu- ja liitesivumäärä** | 64 + 5 | | |



Opinnäytetyön tarkoituksena oli toteuttaa Eduro-säätiön henkilökunnalle tietoturvaopas sekä suunnitella ja pitää koulutus, jonka pääpainona on tietosuoja. Opinnäytetyössä tarkastellaan kokonaisvaltaisesti tietoturvaa, johon tärkeänä osana kuuluu tietosuoja. Oppaan tarkoitus on toimia työkaluna nykyiselle ja tuleville työntekijöille. Opas on suunniteltu siten, että se on helppolukuinen ja siihen on yksinkertaista tehdä muutoksia ja lisäyksiä aina tarpeen vaatiessa.

Opinnäytetyössä tietoturvaa ja erityisesti tietosuojaa tarkastellaan sellaisten työntekijöiden näkökulmasta, jotka käsittelevät päivittäisessä työnteossa salassa pidettäviä ja luottamuksellisia tietoa sekä asiakkaiden ja työntekijöiden henkilötietoja.

Nykyisessä tietoyhteiskunnassa tietojen määrä on valtava ja tiedon suojeleminen on erityisen tärkeää. Tietoturvassa on useita asioita, joista voi koitua suuriakin tietoturvariskejä, ja pienillä toimintatapamuutoksilla pystytään karsimaan tai vähentämään mahdollisia riskejä. Opinnäytetyössä selvitettiin, mitä tietoja henkilökunnan on osattava, jotta voidaan toimia mahdollisimman tietoturvallisesti ja jouhevasti. Lähtökohtana oli säätiön riskianalyysi, johon kuului eri osa-alueiden riskiluokitukset.

Raporttiosuus jakaantuu kahteen osaan, jossa syvennytään tutkimaan käytännön tietoturvaa ja perehdytään EU:n yleiseen tietoturva-asetukseen, joka voi vaikuttaa säätiön toimintaan. Näiden lisäksi yhtenä osana opinnäytetyötä oli tehdä kysely, jossa selviää työntekijöiden tarvittavat tiedot sekä olemassa olevat taidot. Kyselyn perusteella selvisi, että henkilökunnan kouluttamiselle on tarvetta. Henkilökunnan osaaminen tulee saada yhteneväiselle tasolle, sillä se on keskeinen osa tietoturvariskien hallinnassa.



| | |
|---|---|
| Avainsanat | Tietoturva, tietosuoja, tietoturvaopas, tietosuojakoulutus |
| Muita tietoja | Opinnäytetyöhön kuuluu tietoturvaopas ja tietosuojakoulutus. |

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

Degree Program in Business
Information Technology
Bachelor of Business Administration

| | | | |
|---|---|---|---|
| **Author** | Collins Johannes | Year | 2019 |
| **Supervisor** | Jari Sarja | | |
| **Commissioned by** | Eduro-säätiö | | |
| **Subject of thesis** | Planning and Implementing an Information Security Guide and Data Privacy Training Course: CASE: Eduro-säätiö | | |
| **Number of pages** | 64 + 5 | | |

The purpose of this thesis was to implement an information security guide and to plan and give a training course focusing on data protection for the Eduro foundation staff members. The thesis comprehensively examined information security that includes data protection as an important part. The purpose of the guide is to serve as a tool for current and future employees. The guide is designed to be easy to read and simple to make changes and additions whenever necessary.

In the thesis, information security and especially data protection where examined from the employees' point of view. They process customers' and employees' secret, confidential information and personal data. In the current information society, the amount of information is huge and protecting this information is especially important. In information security there are several things that can pose as a major security risk, and minor policy changes can eliminate or reduce these potential risks. This thesis clarified what information the staff must know in order to operate in the most secure and efficient way possible. The baseline was the foundation's risk analysis, which included risk classifications in different areas.

The thesis report is divided into two parts, practical information security in more depth and the EU's General Data Protection Regulation which can affect the foundation's operations. In addition, one part of the thesis was to conduct a questionnaire that examined the necessary and existing knowledge of the employees. The survey revealed that there is a need for staff training. The staff's knowledge should be consistent as it is a key part of managing information security.

| | |
|---|---|
| Key words | data security, data privacy, security guide, data privacy training |
| Special remarks | The thesis includes an Information Security Guide and Data Privacy Training Course. |

SISÄLLYS

# 1 JOHDANTO

Tänä päivänä tiedon määrä on valtava, jota ilman yhteiskunnan olisi vaikea toimia. Etenkin suurissa organisaatioissa tallennettu tietoaineistomäärä on massiivinen ja sen hallinta on merkittävässä asemassa, mikä jatkuvasti tuottaa heille haasteita (Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008, 12). Yksityisyys kuuluu länsimaissa ihmisen perusoikeuksiin, jotka on määritelty useissa erilaisissa lainsäädännöissä (Tikkinen-Piri, Rohunen & Markkula 2017, 3). Tämän myötä myös tietoturva ja tietosuoja ovat yhä merkittävämmässä roolissa organisaatioiden toiminnassa. Perinteisesti on ajateltu, että tietoturva kuuluu vain IT-osaston vastuulle, mutta todellisuudessa se kuuluu koko organisaation henkilökunnalle. Tiedon suojaus kuuluukin nykyään organisaation perustoimintaan. Organisaation johto hyväksyy tietoturvastrategian, ja he ovat loppukädessä vastuussa organisaation tietoturvasta. IT-henkilöstö toimii asiantuntijana, laittaa käytäntöön sekä huolehtii teknisestä toteutuksesta, ja muu henkilöstö huolehtii tietoturvasta omalla toiminnallaan. (International Chamber of Commerce 2016, 8.)

Tämä opinnäytetyö käsittelee tietoturvaoppaan ja koulutuksen suunnittelua ja toteutusta Eduro-säätiön henkilöstölle. Koulutuksella pyritään kouluttamaan ja opastamaan työtekijöitä parempiin ja tietoturvallisiin toimintatapoihin. Säätiöllä ei ole aikaisemmin ollut käytössä varsinaista opasta tietoturvasta, vaan on ollut erillisiä toimintaohjeita tai menettelyjä. Tämän lisäksi henkilökunnalla on ollut omaa hiljaista tietoa, mikä ei ole kantautunut ohjeistuksiin. Lisäksi tietoturvan kehityksen myötä nykyiset mallit on tarkastettu ja päivitetty. Tähän opinnäytetyöhön kuuluu raporttiosuuden lisäksi kaksi osaa, tietoturvan perehdyttämisopas sekä tietoturvakoulutus. Tämä ratkaisu tuntui parhaimmalta, jotta tietoturvakäytännöt jäisivät mahdollisimman hyvin henkilökunnan mieleen.

Tietoturva on tutkimuksen kohteena erittäin mielenkiintoinen muutamasta syystä. Ensinnäkin, tietosuoja on tällä hetkellä hyvinkin pinnalla oleva asia koko EU:n alueella uuden Euroopan parlamentin ja neuvoston asetuksen 2016/679 (myöhemmin tietosuoja-asetus tai asetus) vuoksi. Lisäksi jokainen meistä haluaa omalla kohdallaan, että omia henkilötietoja osataan käsitellä oikein ja tietoturvallisesti kaikissa tilanteissa.

Tietoturvan perehdyttämisopas on suunniteltu koko Eduron henkilökunnalle ja toimii konkreettisena apuvälineenä, jotta he osaavat toimia säätiön toimintatapojen mukaisesti. Opas antaa käytännön toimintamalleja ja neuvoja jokapäiväiseen toimintaan. Oppaan lisäksi materiaalina toimii tietoturvakoulutus, jossa pääpainona on viime vuonna voimaan tullut yleinen tietosuoja-asetus. Myöhemmissä koulutuksissa tullaan käymään läpi myös oppaassa olevia sisältöjä, jotka rajautuivat opinnäytetyön ulkopuolelle.

Tietoturva on tällä hetkellä ajankohtainen ja tärkeä aihe. Toukokuussa 2018 astui voimaan EU:n uusi tietosuoja-asetus, joten säätiölle tuli hyvä tilaisuus tarkastella kokonaisvaltaista riskien hallintaa, johon kuului myös tietoturvan kehittäminen. Tietoturvasuunnitelma ei saisi jäädä ainoastaan dokumentiksi arkistoon, vaan se pitäisi ottaa käyttöön ja henkilökuntaa tulisi kouluttaa turvallisempaan tietojen käsittelyyn, jolloin pystytään minimoimaan mahdolliset tietoturvariskit. Tietoturvan merkitys ei tule tulevaisuudessa vähentymään, vaan sen tarpeellisuus tulee kasvamaan entisestään uusien uhkien myötä. Toimenpiteitä ei siis tehdä ainoastaan EU:n lainsäädännön takia, vaan säätiön henkilökunnan ja asiakkaiden vuoksi.

Opinnäytetyön tietoperusta pohjautuu pääasiallisesti kolmeen eri tietokanavaan: lainsäädännöt, johon kuuluvat sekä EU:n uusi tietosuoja-asetus että myös Suomen lainsäädäntö, Eduro-säätiön tieturvastrategia ja talon omat toimintatavat sekä lisäksi yleiset teoriapohjaiset tiedot tietoturvasta.

## 1.1 Taustaa

Toimeksiantajana toimii Eduro-säätiö, joka toimii Rovaniemellä hyvinvoinnin ja työllisyyden sektorilla. Säätiö toimii sosiaalialalla, ja se tarjoaa tuen ja ohjauksen palveluja työhön kuntoutumiseen, osaamisen vahvistamiseen sekä työllistymiseen. (Eduro-säätiö 2019.) Säätiö työllistää noin 50 henkilöä, ja säätiöllä on vuosittain yli 600 asiakasta. Asiakaskuntaan kuuluu osatyökykyisiä, nuoria ja pitkäaikaistyöttömiä.

Suurin osa henkilökunnasta käsittelee luottamuksellista tietoa, henkilötietoja sekä arkaluontoisia henkilötietoja, joten hyvien ja tietoturvallisten toimintatapojen noudattaminen on erityisen tärkeää. Eduro-säätiö kuuluu Rovaniemen kaupungin konsernille, joten moni toimintatapa on linjassa kaupungin tietoturvan kanssa. Säätiöllä on siitä huolimatta omat järjestelmät ja toimintamenettelyt. Eduron digikoordinaattori toimii myös Eduron tietosuojavastaavana, ja säätiön rekisterinpitäjänä toimii Rovaniemen kaupunki.

## 1.2 Tutkimusongelma ja -menetelmä

Koulutuksen ja oppaan suunnittelun myötä opinnäytetyön tutkimusongelmaksi muodostui seuraava kysymys: *Miten tietoturvaa koulutetaan Eduro-säätiön henkilökunnalle?* Tutkimusongelman avuksi muodostui kaksi apukysymystä: *Miten tietoturva otetaan huomioon Eduro-säätiössä, ja miten voidaan varmistaa tietoturvan jatkuvuus?*

Koska tietoturva on aiheena erittäin laaja ja monimutkainen, oli tärkeää rajata opinnäytetyötä niin, että siitä saataisiin hallittu ja järkevä kokonaisuus. Työn laajuus onkin rajattu koskemaan ainoastaan Eduro-säätiön näkökulmaa. Opinnäytetyö toteutettiin laadullisena tutkimuksena eli kvalitatiivisena tutkimuksena, jossa kuvataan todellisia tilanteita, jotka ovat toisistaan hyvinkin vaihtelevia (Hirsjärvi, Remes & Sajavaara 1997, 161).

Lisäksi tehdyssä henkilökunnan kyselyssä joudutaan käyttämään induktiivista päättelyä, jolloin tuloksien analyysissä ja havainnoissa tapahtuu yleistyksiä, kuten esimerkiksi ajatus, jonka mukaan jos yksi ei osaa, moni muukaan ei osaa. Tämä ei kuitenkaan ole välttämättä huono asia, sillä vaikka asiat olisivatkin jo entuudestaan tuttuja, voi niiden kertaaminen olla silti hyväksi, jotta koko henkilökunnan osaaminen saadaan päivitettyä samalle tasolle. Tämä auttaa koulutuksen toteuttamisessa. Yleistyksissä mennään kuitenkin aina heikoimman mukaan.

Opinnäytetyössä käytetään viittä erilaista aineistohankintamenetelmää: valmiit teoriapohjaiset tietolähteet, eli kirja- ja verkkolähteet, säätiön omat dokumentaatiot, muun muassa tietoturvastrategia, lainsäädäntö, sisältäen sekä Suomen lainsäädännön että EU:n asetukset, tietoturvakysely sekä näiden kaikkien me-

netelmien pohjalta rakentuvat käytännön ohjeistukset. Erilaisten hankintamenetelmien avulla varmistetaan se, että aineistopohja on tarpeeksi laaja tutkimusongelman ratkaisun löytämiseksi.

# 2 TIETOTURVA YLEISESTI

Uusien haasteiden mukana on tullut uusia ajattelutapoja. On helppo vastuuttaa IT-osastoa huolehtimaan hyvästä tietoturvasta tekniikan avulla, mutta tällainen ajattelutapa on kuitenkin vanhanaikaista. Tietoturva koostuu ihmisistä, tekniikasta ja prosesseista. Noin 35 prosenttia yrityksen turvallisuuteen kohdistuvista häiriöistä aiheutuu ihmisten huolimattomuudesta johtuvista virheistä. Jäljelle jääneistäkin häiriöistä yli puolet olisi voitu estää jo etukäteen turvallisemman käsittelyn avulla. Tietojen ennaltaehkäisevä toimenpide tulee pidemmällä aikavälillä halvemmaksi kuin jälkikäteen tehty, puhumattakaan imagon menetyksestä. Tärkeä osa ennaltaehkäisevässä tietoturvassa on riskien hallinta, jota pitää jatkuvasti tarkastella. (International Chamber of Commerce 2016, 8–9.) Vakava tietovuoto ei ole ainoastaan vahinko tai rikkomus, vaan myös taloudellinen ja imagollinen uhka, joka voi estää myös toiminnan jatkuvuuden (Andreasson, Koivisto & Ylipartanen 2016, 119–120). On työnantajan velvollisuus tunnistaa uhat, arvioida riskit sekä antaa tarvittavat toimintaohjeistukset henkilöstölle (Järvinen & Rousku 2017, 31).

Tehokkain tapa toimia tietoturvallisesti on kiinnittää eniten huomiota ja resursseja suurimpaan riskiluokkaan kuuluvien tietojen suojaukseen. Siksi organisaatiossa onkin tärkeää tehdä riskianalyysi. Ennen riskianalyysiä on tehtävä riskien kartoitus, jossa määritellään riskitekijät, mihin ja millä lailla riskit vaikuttavat sekä niiden syyt. Tarkoituksena on saada riskeistä mahdollisimman ajantasaista ja kattavaa tietoa. Tekemällä riskianalyysejä voidaan kartoittaa, mitä uhkia ylipäänsä on, mitä toimenpiteitä tulee tehdä riskien minimoimiseksi ja kuinka suurista uhista voi olla kyse. Lisäksi riskejä täytyy priorisoida. Kaikkia riskejä ei kannata kohdella tasapuolisesti, jotta voidaan keskittyä uhkaavampiin ja haitallisimpiin riskeihin. Tämän pohjalta voidaan lähteä tekemään toimintasuunnitelmia riskien toteutumisen varalle. Suunnitelmaan kuuluu myös suunnitelma riskin poistamista tai minimoimista varten. Riskinhallintaan voidaan käyttää erilaisia käytäntöjä tai standardeja kuten ISO 31000 Riskinhallintastandardi. (Andreasson ym. 2016, 118–120.)

Teknologia kehittyy jatkuvasti, ja sen myötä myös toimintatavat muuttuvat. Tämän muutoksen rinnalla myös tietoturvan on pysyttävä kehityksessä ja muutok-

sissa mukana. Näissä muutoksissa tietoturvan tulee olla integroituna, eikä erillisinä palveluina tai toimenpiteinä. Mikäli tietoturva vaikuttaa merkittävästi organisaation henkilöstön toimintaan, on syytä arvioida uudelleen organisaation tietoturvamekanismit. Täytyy muistaa, että teknologian tarkoituksena on nimenomaan helpottaa ja tehostaa toimintaa. Jokaisella tiedolla on oma elinkaarensa. Ensimmäisenä tieto tuotetaan tai kerätään, jonka jälkeen tietoa käytetään eli käsitellään. Tämän jälkeen tieto joko arkistoidaan tai tuhotaan lopullisesti. Jokaisessa näissä vaiheissa on tiedettävä aina, kuka tehtävän hoitaa ja milloin. (Järvinen & Rousku 2017, 31–32, 47.)

Tietoturvassa on huolehdittava seuraavista osa-alueista; saatavuus, luottamuksellisuus ja eheys. Tiedon saatavuuden puute tarkoittaa sitä, että tarvittava tieto ei ole saatavilla silloin, kun tietoa tarvitaan. Tämä voi johtua esimerkiksi toimivan verkon puutteesta tai palvelunestohyökkäyksestä. Mikäli organisaatiolla on kymmeniä työntekijöitä, jotka ovat riippuvaisia tiedon saannista, ja työ pysähtyy tiedon saatavuuden puutteen vuoksi, voi haitan hinta olla yllättävänkin suuri. Luottamuksellisuudella tarkoitetaan sitä, että tietoon pääsevät käsiksi ainoastaan sellaiset henkilöt, joilla on siihen perusteltu oikeus. Luottamuksellisuuden puutteessa kyseessä voi olla, että tietoa ei rajoiteta tarpeeksi, jolloin tietoihin pääsee käsiksi sellaisia henkilöitä, joille se ei ole välttämätöntä. Lisäksi tietoturvan pettäessä tieto voi joutua vääriin käsiin ja julkisuuteen. Riskin haitan vakavuus ja suuruus määräytyvät suoraan vuodetun tiedon määrästä ja sisällöstä, vaikka on tapauksia, joissa yksittäisen tiedon vuotaminen on voinut aiheuttaa suurta haittaa. Tällöin on yleensä ollut kyseessä julkisuuden henkilö. Tietojen eheyden puuttumisella tarkoitetaan sitä, että tietoja voidaan muuttaa, jolloin tiedon oikeellisuutta ei voida varmistaa. Tämä on erityisen vakavaa silloin, kun ei tiedetä, että tietoa on muutettu ja vääristetty, muussa tapauksessa kyseiset tiedot voidaan aina palauttaa. (Järvinen & Rousku 2017, 40.) Vaikka säätiön kannalta suurin tietoturvariski on henkilöstön omat inhimilliset erehdykset, niin muita uhkia ei voida sulkea pois. Muita uhkatekijöitä ovat harrastelijat ja kokeilijat, haktivistit, tietoverkkorikolliset, kyberterroristit ja valtiollinen tai kansallinen tiedustelu.

Harrastelijat tai kokeilijat eivät välttämättä tiedosta itse, kuinka suurta haittaa he saattavat oikeasti todellisuudessa tehdä. He saattavat tehdä haittaa mielenkiin-

non vuoksi, jännityksen kaipuun tai näyttämisen halun takia. Haktivistit ovat astetta ammattilaisempia, ja he yleensä tekevät haittaa oman tarkoituksensa edistämiseksi. Tällainen keino voi olla esimerkiksi palvelunestohyökkäys. He saattavat tehdä myös haittaa huonon kokemuksensa vuoksi tai organisaation maineen huonontamiseksi. Tietoturvarikolliset ovat suurin yksittäinen ryhmä, jonka tarkoituksena on yleensä saada rahallista hyötyä joko suoranaisesti tai epäsuorasti. Tällaisia ovat esimerkiksi varastettujen tietojen, kuten luottokorttitietojen myyminen, erilaiset nettihuijauspalvelut, lunastus- tai uhkailukeinot, palvelunestohyökkäykset sekä huijaussähköpostit. Monesti tämän ryhmän keinot ovat luovia ja kohdistuvat yleensä massaväestöön. (Järvinen & Rousku 2017, 35–36.)

Kyberterrorismi on samankaltaista kuin perinteinen terrorismi, mutta kohteena ovat ICT-järjestelmät tai -palvelut. Tarkoituksena on saada aikaan mahdollisimman paljon haittaa. Tällaisen terrorismin kohteena ovat yleensä viranomaiset, suuret organisaatiot tai palvelut, kuten pankkitoiminta, sähkönjakelu ja internetoperaattorit. Toistaiseksi Suomessa on suurelta osin vältytty näiltä uhkatekijöiltä. Valtiollinen tai kansallinen tiedustelu pyritään pitämään mahdollisimman huomaamattomana. Kohteena ovat yleensä valtionjohto tai maiden puolustusvoimat tai armeijat. (Järvinen & Rousku 2017, 37.)

## 2.1 Tietoturvan roolit

Organisaatiossa jokaisella työntekijällä on oma vastuualue tietoturvan saralla, ja se kuuluu luonnollisena osana työkuvaan. Tietosuoja-asetuksessa on määritelty rekisterinpitäjän tehtävät melko tarkasti. *Rekisterinpitäjäksi* kutsutaan oikeushenkilöä, virastoa, viranomaista tai muuta tahoa, jonka vastuulla on määritellä ne toimet, joilla henkilötietoja käsitellään, ja perusteet käsittelylle. Rekisterinpitäjä on vastuussa myös siitä, että henkilötietoja käsitellään lakien vaatimalla tavalla. Tämä vastuu kuuluu myös *henkilötietojen käsittelijälle*, eli taholle, joka rekisterinpitäjän määräämänä huolehtii henkilötietojen käsittelystä. Rekisterinpito ja tietosuoja kuuluvat *organisaation johdon* vastuisiin samoin kuin huolehtiminen siitä, että tietosuojaa kehitetään. Johdon kuuluu myös varata tarpeeksi resursseja tietosuojan toteutumista ja kehittämistä varten. Käytännössä vastuiden osa-alueet jakautuvat johdolle riippuen muun muassa ohjeistuksista, säännöistä tai määritellyistä työjärjestyksistä. Organisaatiossa esimiesten on varmistettava,

että henkilöstöllä on tarvittavat tiedot ja työkalut henkilötietojen käsittelyyn. Heidän vastuullaan on myös varmistaa, että tarvittavat ohjeistukset ja kouluttautumisvalmiudet ovat henkilöstön saatavilla. Esimiehet toimivat valvovassa roolissa, jolloin he pystyvät varmistamaan tietosuojan toteutumista, ja tarvittaessa heidän kuuluu raportoida mahdollisten poikkeamien ja vaarantumisien sattuessa. Organisaatiolla kuuluu olla ennalta määrätyt toimintamallit näitä tilanteita varten. *Henkilöstön* velvollisuuksiin kuuluu toimia annettujen tietosuoja- ja tietoturvaohjeistusten sekä muiden ohjeistusten ja lainsäädännön määrittelemien toimintaperiaatteiden mukaisesti. Mahdollisten poikkeamien tai vaaratilanteiden sattuessa jokaisella henkilöstöön kuuluvalla on vastuu raportoida havainnoistaan. Varta vasten luodut toimintamallit helpottavat ja ohjaavat toimintaa näiden tilanteiden varalta. (Andreasson, Riikonen & Ylipartanen 2017, 80, 113–114, 124.)

Eduro-säätiössä on käytössä tietoturvapoikkeamaraportti, josta käy ilmi poikkeaman havaittu aika ja sen luonne mahdollisimman tarkasti. Tietoturvaavastaava käsittelee poikkeaman, josta käydään läpi seuraavat toimenpiteet. Todetaan, että poikkeama on todella sattunut. Ensin pitää hallita vahingot ja mahdollisesti estää haitan paheneminen tai leviäminen. Näiden kiireellisten toimenpiteiden jälkeen on kerättävä todisteet. Nämä voivat olla palvelimen ja järjestelmän lokit tai valvontakameramateriaalit. Vasta näiden jälkeen pyritään korjaamaan vahingot esimerkiksi tekemällä varmuuskopioinnin palautukset tai tiukentamalla tietoturva-asetuksia. Lopuksi tiedotetaan kaikille tarvittaville tahoille tai henkilöille. Mikäli henkilötietojen osalta on tapahtunut vakava luvaton tietojen käsittely, tietosuoja-asetuksen mukaan on ilmoitettava kyseisille rekisteröidyille. Jokaisesta poikkeamasta on annettava arvio sen vakavuudesta ja raportoitava siitä, miten poikkeama on hoidettu, ja tietoturvavastaava antaa johdolle omat ehdotuksensa siitä, mitä toimenpiteitä on tehtävä, jotta riskiltä voitaisiin välttyä seuraavalla kerralla. Tietoturvapoikkeaman lisäksi tietosuojavastaavan on tehtävä henkilötietojen tietoturvaloukkauksia koskeva ilmoitus, jossa selviää, mihin tietoihin rike on kohdistunut, onko mukana erityisiin henkilötietoryhmiin kuuluvaa tietoa sekä kuinka montaa henkilöä tietoturvaloukkaus koskee ja onko heille ilmoitettu loukkauksesta. (Eduro-säätiö 2018d; Eduro-säätiö 2018b.)

Tietosuoja-asetuksessa on tietyssä tilanteessa nimettävä *tietosuojavastaava*. Nimike on hieman harhaanjohtava, sillä voisi olettaa, että sen myötä vastuu kattaisi koko tietosuojan. Vastaavan tehtävänä on kuitenkin toimia tarvittaessa neuvonnan lähteenä sekä auttaa kehittämään tietosuojaa eteenpäin. Tietosuojavastaava raportoi suoraan organisaation johdolle, eikä saa johdolta ottaa vastaan toimintaohjeita. Roolin myötä vastuuseen kuuluu myös pitää huoli siitä, että tietosuojan seuranta on vaatimusten tasolla. Organisaatio voi nimetä vain yhden tietosuojavastaavan, jolta vaaditaan riippumattomuutta, eli organisaation johto ei voi määrätä häntä ottamaan tietynlaista kantaa, eikä häntä voida sen perusteella irtisanoa. Tehtävän luonteen vuoksi vastaavaan rooliin ei voi määrätä sellaisia henkilöä, joka päättää henkilötietojen käsittelystä. Tällainen voisi esimerkiksi olla organisaation oma IT-johtaja tai markkinointijohtaja. Tehtäväkuvaan kuuluu, että rekisteröidyt voivat olla tietosuojavastaavaan yhteydessä kaikissa tietosuojaan liittyvissä asioissa, ja hän toimii yhteyshenkilönä valvontaviranomaisten kanssa. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 121–122.)

## 2.2 Tietoturvan osa-alueet

Tietoturvassa voidaan pilkkoa tietoturvan kokonaisuus erilaisiin osa-alueisiin. Nämä osa-alueet ovat hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, laitteisto-, ohjelmisto- ja tietoliikenneturvallisuus, tietoaineisto- ja käyttöturvallisuus sekä fyysinen turvallisuus. Jokaisella osa-alueella on oman roolinsa, ja ne on otettava huomioon suunnitteluvaiheessa. (Hakala, Vainio & Vuorinen 2006, 10.)

*Hallinnollinen tietoturvallisuus* on yksi organisaation prosesseista. Hallinto on sitoutettava huolehtimaan siitä, että se johtaa ja kehittää koko organisaation tietoturvallisuutta. Sen on myös koulutettava henkilöstöä tarvittaessa. Hallinto tunnistaa riskit ja varmistaa, että tietoturva on riittävällä tasolla ja että toimitaan laillisesti oikein. Hallinto luo organisaatiolle tietoturvapolitiikkaa ja määrittelee toimintalinjaukset sekä erilaiset dokumentit ja ohjeet. Jotta saadaan toimiva ja tehokas kokonaisuus, on hallinnon osattava jakaa vastuualueita. (Laakso 2018.)

*Henkilöstöturvallisuuteen* kuuluu se, että henkilökunnan pitää tunnistaa organisaatioon liittyvät uhat ja miten nämä riskit vaikuttavat toimintaan käytännössä. Jokaisella henkilöllä on oma riskinottokyky, ja tunnistamme ja käsittelemme riskejä eri tavoin. Kouluttamalla henkilökuntaa voidaan yhdenmukaistaa henkilöiden riskintunnistuskyvyt. Henkilöstöturvallisuus on tärkeässä roolissa tietoturvallisuudessa, sillä henkilöstö on se, joka käsittelee tietoa. (Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008, 11–12.)

Usein organisaatiossa ajatellaan uhkina ainoastaan henkilöstön tuottamia vahinkoja, olivat ne sitten tahattomia tai tahallisia. Täytyy kuitenkin muistaa, että organisaation omalla panostamisella tietotekniikkaan ja rakenteeseen voi vaikuttaa merkittävästi uhkien todennäköisyyksiin. Kehittämällä henkilöstöturvallisuustyötä, kuten kouluttamalla, työmenetelmien suunnittelulla, asenteiden rikkomisella sekä ohjeistuksilla, on mahdollista pienentää henkilöstön aiheuttamien uhkien riskejä. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2008, 19.)

*Laitteistoturvallisuudella* tarkoitetaan erilaisia tietoteknisten järjestelmien suojaamisia. Tähän voi kuulua reitittimet, palomuurit, kopiokoneet, tietokoneet ja puhelimet. *Ohjelmistoturvallisuudella* tarkoitetaan tietokoneohjelmistojen suojaamista ja lisenssien ylläpitoa. Esimerkkinä tähän kuuluvat muun muassa käyttöjärjestelmät, palvelinohjelmistot, virusturvat ja toimisto-ohjelmat. *Tietoliikenneturvallisuudella* taas tarkoitetaan tietoliikenneyhteyksien suojaamista erilaisilla ratkaisuilla. Tähän kuuluvat VPN-yhteydet, erilaiset yhteyksien salaukset ja lisäksi myös palomuurit. (Ruohonen 2002, 4–5.)

Perinteisesti ajatellaan, että tietoturva tarkoittaa pelkästään tietoaineiston turvaa, mutta todellisuudessa se on vain yksi tietoturvan osa-alueista. *Tietoaineistoturvallisuudella* suojataan tietojärjestelmien sisältämiä tietoja. Kyseessä voi olla joko henkilötietoja tai muuta tietoa, jota halutaan suojata. Tietoaineistoturvallisuus käsittelee kokonaisuudessaan tietojen käsittelyä, eli siihen kuuluvat tiedon saannin lisäksi sen muuttaminen, kirjoittaminen, käyttöoikeuksien varmentaminen sekä tiedon saatavuuden takaaminen. *Käyttöturvallisuudella* taas turvataan tietolaitteiden ja -järjestelmien turvallista käyttöä. Tämä osa-alue on suoraan sidoksissa henkilöstöturvallisuuteen. (Ruohonen 2002, 4–5.)

*Fyysinen turvallisuus* suojaa organisaatiota fyysisesti esimerkiksi tilojen, rakennuksen tai muun omaisuuden osalta. Osana tähän kuuluvat kulku- ja kamera- tai muu tekninen valvonta, erinäiset palo-, räjähdys-, sähkö- tai vesivahinkojen torjumiset sekä muut luonnonkatastrofien huomioimiset. Fyysiseen turvallisuuteen liittyvät myös ihmisten aiheuttamat haitat, kuten sodat, ilkivallat, murrot tai vandalismit. Pääsääntöisesti tilojen fyysisestä turvallisuudesta vastaa kiinteistöhallinta tai omistajataho, mutta varsinkin tietoteknillisiä ratkaisuja on hyvä laatia organisaatiotasolla. On otettava huomioon erilaiset uhat, riippumatta niiden todennäköisyydestä. (Krutz & Vines 2003, 326–327.)

## 2.3 Riskien hallinta

Riskienhallinta on tietoturvallisuuden keskeisin osa, ja se on oleellinen osa EU:n tietosuoja-asetusta. Ainoa tapa eliminoida riskit kokonaan olisi lopettaa kyseinen toiminta tai palvelu, joka riskin aiheuttaa, mutta tämä voi olla monesti huonoin ratkaisu tai ääritapauksessa organisaatio ei voisi toimia ollenkaan. On sisäisesti pohdittava organisaation todelliset uhat, niiden todennäköisyydet sekä seuraamukset ja kuinka usein uhat toistuvat. (Krutz & Vines 2003, 15.)

Tietoturvaan liittyvät riskit ovat monesti näkymättömiä, jolloin niiden vaikutusta ei välttämättä nähdä tarpeeksi suurena uhkana. Uudessa asetuksessa on useampi kohta, joka keskittyy nimenomaan riskienhallintaan. Nämä asetukset ovat artikla 25, 32, 34 ja 35. Artikla 25 muistuttaa, että riskien hallinnan kuuluu olla integroituna organisaation toimintatapoihin tai toimintamalleihin. Artiklassa 32 vaaditaan, että rekisterinpitäjän ja henkilötietojenkäsittelijöiden on muistettava ottaa huomioon työssään tarvittavat toimenpiteet pitääkseen turvallisuuden riskiluokituksen mukaisesti vaadittavalla tasolla. Artiklassa 34 määrätään ilmoittamaan rekisteröidyille viivyttelemättä, jos heidän tietojaan on voinut päätyä ulkopuolisten käsiin tai jos riski siihen on noussut tapahtuneen loukkauksen vuoksi. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 25.)

Taulukossa 1 näkyy riskin seurauksen arvio ja sen todennäköisyydet. Asteikolla 1–5 yksi on todennäköisyydeltään erittäin heikko ja seurauksiltaan vähäinen. Viisi taas on erittäin todennäköinen ja seurauksiltaan kaikista vakavin. Näistä saadaan riskin vakavuusluokat. (Korpisaari ym. 2018, 26.)

Taulukko 1. Riskien vakavuusluokat (mukaillen Korpisaari ym. 2018, 27)

| | Todennäköisyys | | | | |
|---|---|---|---|---|---|
| **seuraukset** | **1** | **2** | **3** | **4** | **5** |
| **1** | 1 | 2 | 3 | 4 | 5 |
| **2** | 2 | 4 | 6 | 8 | 10 |
| **3** | 3 | 6 | 9 | 12 | 15 |
| **4** | 4 | 8 | 12 | 16 | 20 |
| **5** | 5 | 10 | 15 | 20 | 25 |

On vaikea arvioida, kuinka paljon organisaation tulee budjetoida riskien hallintaa varten. Aina löytyy parempia ratkaisuja ja tekniikoita turvallisuuden parantamiseen, mutta käytettävien resurssien raja on vedettävä johonkin. Jos riskit käyvät liian suuriksi, eikä resursseja niiden hallintaan ole, tulee pohtia, voidaanko riskejä vähentää tietoturvakeinoilla vai poistetaanko riskien mahdollisuus kokonaan. Tästä esimerkkinä on organisaation sähköinen varausjärjestelmä. Jos ei ole mahdollista suojata järjestelmää riittävästi, järjestelmän käyttöä ja tarpeellisuutta on arvioitava uudelleen.

Tietoturvan riskit kuuluvat liiketoimintariskien hallintaan, ja niiden hallintaan tarvitaan sekä osaamista että myös toimintamenetelmiä. Yksi tällainen on portfoliolähestymistapa, jossa riskit luokitellaan kahdeksaan eri osaan: projektit, IT-palvelujen jatkuvuus, tieto-omaisuus, palvelun tarjoajat, sovellukset, infrastruktuuri sekä strategiset riskit ja tulevaisuuden uhat. Vaikka riskialueet kuuluvat perinteiseen IT-riskien hallintaan, voidaan riskejä pohtia myös tietoturvan näkökulmasta. Näiden eri osien riskit käydään läpi osa kerrallaan. Kun riski ilmenee, on pohdittava, mitä riskille tulee tehdä. Voidaan poistaa riskit, minimoida riskien todennäköisyydet tai minimoida riskien vaikutukset. Toiminnallisessa mielessä riskejä voidaan ulkoistaa, jolloin palveluntarjoaja kantaa vastuun. Tämä itsestään ei poista riskejä, mutta se voi vähentää niiden seuraamuksia, varsinkin taloudellisessa mielessä. (Jordan & Silcock 2006, 55–73.)

## 2.4 Tietoturvapolitiikka ja -suunnitelma

Tietoturvapolitiikka on konkreettinen dokumentti ja tärkeä osa organisaation prosesseja, johon ylin johto sitoutuu ja hyväksyy. Loppukädessä johto on aina vastuussa yrityksen tietoturvasta. Politiikka tehdään yleensä keskipitkälle tai pitkälle aikavälille. Hyvä tietoturvapolitiikka on luotu yleisellä tasolla, muttei kuitenkaan liian yleisellä tasolla, jolloin politiikasta tulee vain joukko kauniita ja koristeltuja sanoja. On koettu, että toimiva tietoturvapolitiikka sisältää tietoturvan määritelmät ja kohteet, tietoturvan laajuuden ja tärkeyden, johdon sitoumuksen tukea tietoturvan toteuttamista, tietoturvan rakenteen ja käytännöt, lainsäädännöt ja sopimukset, turvallisuuskoulutukset, tietoturvan ja tietosuojan vastuualueet ja henkilöt, käytännöt ja seuraamukset sekä lisäksi tarkennukset käytettävistä ohjeista ja standardeista. Tietoturvapolitiikan dokumentti on tarkoitettu organisaation koko henkilökunnalle, ja se on luonteeltaan julkinen, joten siihen ei kannata dokumentoida sellaista tietoa, joka voi vaarantaa organisaation tietoturvallisuutta. (Hakala ym. 2006, 7–9.)

Tietoturvasuunnitelma on huomattavasti konkreettisempi ja yksityiskohtaisempi kuin tietoturvapolitiikka, ja se sisältää erittäin paljon teknisiä ratkaisuja. Suunnitelmassa käydään läpi keskipitkällä aikavälillä olevia käytäntöjä. Suunnitelmaa voidaan ja pitääkin tarvittaessa päivittää säännöllisesti, myös suunnitelman aikavälin sisällä. Organisaation toimintaprosessit ja järjestelmät voivat muuttua, joten on hyvä pitää tarkastelujakso vuosittain. Suunnitelma noudattaa tietoturvapolitiikan reunaehtoja. Tietoturvasuunnitelman asiakirja luokitellaan usein salaiseksi tai luottamukselliseksi, sillä se sisältää yksityiskohtaisia tietoja tietoturvaratkaisuista ja menetelmistä. Hyvä tietoturvasuunnitelma voi toimia suoraan ohjeena, mutta tällöin asiakirja ei motivoi tietojärjestelmien käyttäjiä, jolloin ohjeet voivat jäädä noudattamatta. Tällöin on tärkeä kertoa suunnitelman merkitys sekä käyttäjälle itselleen että myös organisaatiolle. (Hakala ym. 2006, 9–10.)

# 3 TIETOSUOJA YLEISESTI

Henkilötietojen käsittely ja prosessointi on nopeasti kasvanut 1960-luvulta saakka, ja tämän myötä tietosuojalainsäädännöt ovat kehittyneet. Teknologian kehittyminen on mahdollistanut tietojen yhdistämisen ja prosessoinnin hyvin laajasti esimerkiksi henkilökohtaisiin palveluihin ja markkinointiin. Vaikka uudet teknologiat palvelevat sekä yrityksiä että myös kuluttajia, kerätyt tiedot aiheuttavat suuria ja kasvavia henkilötietoriskejä. Tämän vuoksi henkilöt eivät välttämättä luota sellaisiin yrityksiin tai palveluihin, jotka keräävät paljon tietoja. Tämä voi osaltaan taas hidastaa uusien teknologioiden hyödyntämistä. (Tikkinen-Piri ym. 2017, 135.)

Tietosuoja on yksi tärkeimmistä tietoturvan osa-alueista. Henkilökunnan on osattava käsitellä henkilötietoja luotettavasti ja turvallisesti. On erityisen tärkeää tietää, miten näitä tietoja käsitellään oikeaoppisesti. Tämä on tärkeää sekä tietojen käsittelijälle että myös käsiteltävälle henkilölle, hänen oman oikeusturvansa vuoksi. Aikaisemmin tietojenkäsittelijän työ ei ole vaatinut suurempaa tarkkuutta tietojen käsittelemiseen, vaan työnkuva on rajoittunut suurimmaksi osaksi tietoturvaan. Tietosuoja-asetuksen myötä tietojenkäsittelijän rooli on saanut entistä enemmän vastuuta, ja nyt onkin huomioitava tarkemmin tietojenkäsittelyn rajat ja oikeudet. (Hanninen ym. 2017, 27.) Tietosuoja on luonnollisten henkilöiden perusoikeus, jonka tarkoituksena on suojata henkilötietojen käsittelyä. Tietoturva on toiminnallinen keino turvata kaikenlaista tietoa, esimerkiksi tietoaineistoa tai tietojärjestelmää, kun taas tietosuoja on lakiin perustuva henkilösuoja. (Tietosuojavaltuutetun toimisto 2018a.)

## 3.1 EU:n yleinen tietosuoja-asetus

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 tai useasti myös käytetty Euroopan unionin yleinen tietosuoja-asetus, tunnetaan myös nimellä GDPR, joka tulee sanoista *General Data Protection Regulation*, astui voimaan 25. toukokuuta 2018. Asetus tuli suoraan sovellettavaksi, ja se korvasi 1995 annetun henkilötietodirektiivin (Direktiivi 95/46/EC) ja kumoaa myös kaikki sen kanssa ristiriidassa olevat lait. Asetuksesta ei siis tarvitse tehdä maakohtaisia lakeja, vaan se on suoraan sovellettavissa. Asetus koskee nimenomaan luon-

nollisten henkilötietojen käsittelyä ja koskee lähes kaikkia tahoja, yrityksiä, yhdistyksiä ja yhteisöjä, mutta ei yksityisiä henkilöitä. Henkilötiedot voidaan kerätä henkilökohtaiseen tai kotitalouden käyttöön. Lain lähtökohtana on yhdenmukaistaa Euroopan unionin alueen tietosuojalakeja, helpottaa palvelujen tarjoamista yli valtion rajoja ja ennen kaikkea antaa henkilöille parempia oikeuksia tietojensa suojaamista varten. Myös EU-alueen ulkopuoliset tahot joutuvat noudattamaan asetusta, mikäli he käsittelevät EU-kansalaisten henkilötietoja. (Tikkinen-Piri ym. 2017, 135.)

Yleinen tietosuoja-asetus antaa maakohtaisia vapauksia määritellä täydentäviä lakeja. Suomessa vastikään otettiin käyttöön tietosuojalaki (1050/2018), joka hyväksyttiin viides päivä joulukuuta vuonna 2018 ja astui voimaan ensimmäinen päivä tammikuuta 2019. (Tietosuojalaki 1050/2018 1 §, 37 §.) Näiden lakien lisäksi työpaikkojen on otettava huomioon myös muita lakeja, kuten laki yksityisyyden suojasta työelämässä.

Tietosuoja-asetuksen lisäksi asetettiin EU-maiden tietosuojaviranomaisista koostuva WP29-niminen tietosuojatyöryhmä, jonka tarkoituksena on tuottaa ohjeita ja tarkennuksia sekä antaa neuvoa lain soveltamisesta. Tarkennuksia tehtiin muun muassa läpinäkyvyyteen ja ohjeistuksia tietosuojaselosteeseen. Työryhmä antoi myös konkreettisen esimerkin, jossa oli sekä hyvä että myös huono toimintamenettely. Huonona menettelynä pidettiin sellaista tapaa, jossa tietosuojaselosteessa lukee, että rekisteröityjen tulee ottaa yhteyttä asiakaspalveluun pyytääkseen pääsyä henkilötietoihinsa. Hyvänä tapana pidettiin sähköistä tai tulostettua lomaketta, joka voidaan helposti täyttää. (Agendium 2018.)

### 3.1.1 Henkilötieto ja arkaluontoinen henkilötieto

Henkilötietojen käsittelyn tulee olla tarkoituksenmukaista, suunnitelmallista ja dokumentoitua. Kaikelle kerättävälle tiedolle tulee olla perusteet, eli mitään epäolennaista tietoa ei saa kerätä ja käsitellä. (Hanninen ym. 2017, 16.)

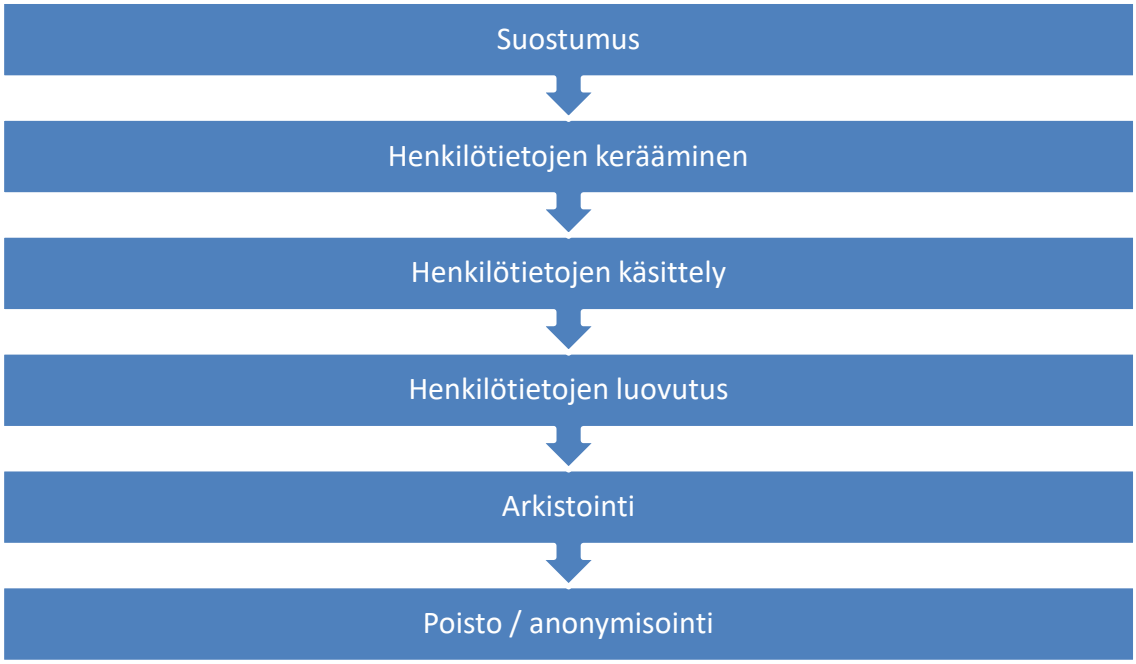
Tietosuoja-asetus pitää ottaa huomioon aina, kun käsitellään henkilötietoja, oli kyseessä sitten automaattinen tai manuaalinen käsittely. Henkilötiedoiksi lasketaan kaikki luonnolliseen, tunnistettuun tai tunnistettavissa olevaan ihmiseen liittyvät tiedot. Tähän kuuluu myös erillään olevat tiedot, jotka yhdistämällä pys-

tytään tunnistamaan kyseinen henkilö. Henkilötiedoiksi lasketaan myös ne tiedot, joita voidaan käyttää tunnistamiseen, vaikka ne on käsitelty niin, että ne ovat salattuja, anonymisoituja tai pseudonymisoituja. Tästä huolimatta näihinkin tietoihin kuuluu soveltaa yleistä tietosuoja-asetusta. Jos henkilötiedot anonymisoidaan peruuttamattomasti niin, että kohdehenkilöä ei enää pysty niiden avulla tunnistamaan, ei tietoja enää lasketa henkilötiedoiksi. (Euroopan komissio 2018.)

### 3.1.2 Henkilötiedon elinkaari

Henkilötietojen elinkaari on otettava huomioon koko prosessin aikana. Elinkaarella tarkoitetaan tietojen keräämistä, tietojen käyttöä sekä tiedon hävittämistä tai arkistointia. Henkilörekisteriin tallennetaan vain rekisterin käyttötarkoituksen kannalta tarpeellisia tietoja, jotka on määritelty tietosuojaselosteessa, ja tietoja saa käyttää ainoastaan siihen tarkoitukseen, mitä varten ne on kerätty. Tietoja kerättäessä on käytettävä tarpeeksi luotettavia tietolähteitä, eikä henkilörekisteriin saa tallettaa puutteellisia, tarpeettomia tai vanhentuneita henkilötietoja. Tällaiset tiedot on poistettava rekisteristä. Kun henkilötietoja ei enää tarvita, ne on poistettava, anonymisoitava tai arkistoitava, mikäli siihen on asianmukainen peruste. (Korpisaari ym. 2018, 113.)

Henkilötietojen elinkaaresta tulee tehdä suunnitelma, jonka mukaan voidaan tarvittaessa toimia. Rekisterinpitäjällä on velvollisuus määritellä henkilötietojen säilytysaika ja kriteerit, jonka pohjalta määritelty säilymisaika perustuu. On myös pidettävä huoli, että poistettu tieto ei enää palaudu esimerkiksi varmuuskopion palauttaessa. Kuviossa 1 näkyy henkilötietojen elinkaarimalli. Tietoja pitää vielä säilyttää, mikäli laki niin vaatii, esimerkiksi kirjanpitolakia varten. Henkilötietojen säilytysaika tulee ilmoittaa myös rekisteröidylle. (EU-tietosuojan kokonaisuudistus 2016, 24.)




Kuvio 1. Henkilötietojen elinkaarimalli (mukaillen EU-tietosuojan kokonaisuudistus 2016, 24)

### 3.1.3 Tietosuojatermistö ja käsitteet

*Anonymisoinnilla* tarkoitetaan henkilötietojen tunnistettavuuden poistamista. Tämä tarkoittaa käytännössä sitä, että vastaisuudessa tietojen perusteella ei voida päätellä, kehen ne kohdistuvat. Toimenpide on peruuttamaton, eikä anonymisoituja tietoja voida palauttaa. Anonymisoinnin jälkeen tiedot eivät kuulu tietosuoja-asetuksen alaisuuteen. (Hanninen ym. 2017, 21.)

*Pseudonymisoinnilla* tarkoitetaan tietojen hajauttamista niin, että itsestään tietoa ei pystytä yhdistämään tiettyyn henkilöön, vaan sitä varten tarvitaan yhdistävä tunnistetieto tai koodi. Pseudonymisoitu tieto kuuluu edelleen tietosuoja-asetuksen piiriin, sillä tieto voidaan vielä tarvittaessa kohdentaa tiettyyn henkilöön. Yhdistävä henkilötieto on säilytettävä erillään pseudonymisoidusta henkilötiedosta. (Hanninen ym. 2017, 21.) Pseudonymisointi on hyvä tapa käsitellä henkilötietoja esimerkiksi tietokannoissa, sillä vuodon tai hakkeroinnin sattuessa vuodettu tieto ei yhdisty tiettyyn henkilöön.

*Rekisterillä* tarkoitetaan mitä tahansa käsiteltyä ja jäsenneltyä henkilötietojoukkoa. Asetus ei määrittele sen muotoa tai kokoa, vaan kyse on kerätyn henkilö-

tiedon käyttötarkoituksesta. Rekisteri voi olla hajautettu toiminnallisesti tai maantieteellisesti. (Hanninen ym. 2017, 21.)

*Profiloinnilla* tarkoitetaan mitä tahansa henkilötietojen automaattista käsittelyä, jossa arvioidaan henkilön tiettyjä ominaisuuksia. Nämä voivat olla henkilön ostotottumukset, taloudellinen tilanne tai henkilön muu mahdollinen käyttäytyminen. (Hanninen ym. 2017, 21.) Profilointia tapahtuu hyvin paljon muun muassa pankeissa ja vakuutusyhtiöissä, mutta myös internetissä, esimerkiksi sosiaalisessa mediassa tai hakujen yhteydessä.

*Rekisterinpitäjä* on luonnollinen henkilö, oikeushenkilö, organisaatio, viranomainen tai muu taho taikka elin, joka määrää rekisterin. Rekisterinpitäjä määrittelee, mitä henkilötietoja kerätään ja mitä tiedolla tehdään. (Hanninen ym. 2017, 22.)

*Henkilötietojen käsittelijä* on luonnollinen henkilö, oikeushenkilö, organisaatio, viranomainen tai muu taho tai elin, joka käsittelee henkilötietoja rekisteripitäjän lukuun. Henkilötietojen käsittelijä on ulkopuolinen alihankkija, palveluntarjoaja tai muu yhteistyökumppani, jolla on oikeudet käsitellä henkilötietoja. Henkilötietojen käsittelijä ei ole päätösvaltainen tietojen keräämisen, säilytyksen, käyttämisen tai käsittelyn suhteen. Käsittelijä toimii aina rekisterinpitäjän vaatimusten mukaan. (Korpisaari ym. 2018, 68.)

*Tietosuojavaltuutettu* on viranomainen, joka valvoo tietosuojalainsäädännön sekä henkilötietojen käsittelyn lakien noudattamista. Tietosuojavaltuutettu antaa muun muassa ohjeita rekisterinpitäjille, antaa lausuntoja mahdollisista lakien rikkomuksista sekä määrää hallinnollisia sanktioita tietosuoja-asetuksen rikkomisesta. Uuden henkilötietolain (1050/2018) myötä tietosuojalautakunta lakkautui 1.1.2019 lähtien ja tehtävät siirtyivät kokonaisuudessaan tietosuojavaltuutetun toimistoon. (Tietosuojavaltuutetun toimisto 2018b; Tietosuojalaki 1050/2018 6.38 §.)

*Tietoturvaloukkaus* on joko tahallista tai vahingossa lainvastaista henkilötietojen käsittelyä. Tähän kuuluu henkilötietojen luovuttaminen, tuhoaminen, muuttaminen, lisääminen tai muu tietoon käsiksi pääsy. (Hanninen ym. 2017, 22.)

*Suostumus* on henkilön vapaaehtoinen tahdonilmaisu tietojen käsittelyyn. Suostumus pitää olla yksilöity ja yksiselitteinen. Suostumuksessa on oltava kaikki käsittelyperiaatteet, ymmärrettävässä ja tarpeeksi tiiviissä muodossa. Rekisterinpitäjällä on velvollisuus osoittaa suostumuksen olemassaolo. (Korpisaari ym. 2018, 70–71.)

*Vastaanottaja* on luonnollinen henkilö, oikeushenkilö, organisaatio, viranomainen tai muu taho tai elin, jolle henkilötiedot luovutetaan. Tämä käytännössä tarkoittaa sitä, että henkilötiedot luovutetaan ulkopuoliselle taholle tai toiselle rekisterinpitäjälle, jolloin syntyy uusi henkilötietorekisteri. Esimerkkinä tällaisesta voi olla muun muassa työpaikan ja palkanlaskentatoimiston välinen sopimus. (Korpisaari ym. 2018, 69.)

*Käsittely* tarkoittaa mitä tahansa henkilötietojen automaattista tai manuaalista käsittelyä. Tämä tarkoittaa tietojen käyttöä, hakua, luovuttamista, tallentamista, poistamista, muuttamista, keräämistä, järjestämistä tai säilyttämistä. Eli henkilötietojen käsittely koskee kaikkia toimenpiteitä, jotka kohdistuvat henkilötietoihin. (Hanninen ym. 2017, 20–21.)

*Rekisteröity* on luonnollinen henkilö, josta käsitellään tunnistettavia henkilötietoja. Uudessa tietosuoja-asetuksessa rekisteröity on keskeisessä asemassa, jolla on useita oikeuksia. (Hanninen ym. 2017, 20.)

*Henkilötieto* tarkoittaa kaikenlaista tietoa, jonka perusteella voidaan tunnistaa tietty henkilö. Tunnistettavan tiedon avulla voidaan tunnistaa henkilö joko suoraan tai epäsuoraan. (Euroopan komissio 2018.)

*Arkaluontoisilla tiedoilla* eli erityisillä henkilötietoryhmillä tarkoitetaan tietoja, joista selviää henkilön rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettiset tai biometriset tiedot, joita käsitellään yksiselitteisesti henkilön tunnistamista varten, terveyttä käsittelevät tiedot tai seksuaalinen käyttäytyminen ja suuntautuminen. Lähtökohtaisesti näiden tietojen kerääminen ja käsittely on kiellettyä, mutta tähän on kuitenkin säädelty tiettyjä poikkeuksia. Tietoja voidaan käsitellä, jos henkilö on antanut nimenomaisen suostumuksensa vähintään yhtä käyttötarkoitusta varten. Lisäksi käsittelylle on peruste, jos työlainsäädäntö sallii käsittelyn tai jos se on

tarpeen oikeusvaateen laatimisen, esittämisen tai puolustamisen takia. Jos suostumusta arkaluontoisten tietojen käsittelyyn ei ole pyydetty, tulee suostumus pyytää jälkikäteen. Mikäli suostumusta ei anneta tai saada, tulee tiedot poistaa. Arkaluontoisten tietojen kanssa tulee huomioida muun muassa se, että muiden tietojen perusteella voi ilmetä arkaluontoisia tietoja. Tästä esimerkkinä erityisruokavaliot, joiden perusteella voi käydä ilmi henkilön terveydentila tai uskonnollinen vakaumus. (Hanninen ym. 2017, 40–42.)

Tietoja, jotka käsittelevät henkilön rikostuomioita tai rikkomuksia, saa käsitellä ainoastaan viranomaisten valvonnassa tai silloin, kun lainsäädäntö niin vaatii. Organisaatiolla tulisi siis olla erityinen peruste käsitellä näitä tietoja, jos niihin halutaan päästä käsiksi. Tällainen peruste tulee esimerkiksi silloin, kun henkilö hakee töitä, joissa hän on tekemisissä lasten kanssa. (Hanninen ym. 2017, 44.)

*Henkilötunnus* on myös sellainen tieto, jonka käsittelylle on säädelty tiettyjä edellytyksiä. Sen avulla voidaan tunnistaa henkilö muiden samannimisten joukosta. Tunnusta saa käsitellä ainoastaan henkilön nimenomaisella suostumuksella tai jos sille on lainmukainen peruste. Henkilötunnusta voidaan myös käsitellä, jos käsitellään jotakin seuraavista toimista: luotonanto, perintä, vakuustoimet, luottolaitos-, luottotieto- tai maksupalvelutoimet, vuokraus- tai lainaustoimet, terveydenhuolto, sosiaalihuolto tai sosiaaliturvan toteuttaminen sekä silloin, kun asia koskee virka-, työ- tai muita palvelussuhteita ja niiden etuja. Näihin edellä mainittuihin ei tarvita erikseen rekisteröidyn suostumusta, sillä toimien yksilöimistarpeen vuoksi käsittelylle on perusteet. On kuitenkin huolehdittava siitä, että henkilötunnusta ei kirjata tarpeettomasti rekisterin perusteella laadittuihin asiakirjoihin tai tulosteisiin. Jos asiakkaalle tarvitaan jokin toinen yksilöinti nimen lisäksi, on suositeltavaa käyttää henkilötunnuksen sijaan esimerkiksi yksilöityä asiakasnumeroa. (Hanninen ym. 2017, 44–46.) Vaikka henkilötunnuksesta ei ole suoraan säädelty EU:n tietosuoja-asetuksessa, niin se kuuluu erityiseen henkilötietoryhmään, joita käsitellään pitkälti samankaltaisesti kuin arkaluonteisia henkilötietoja (Lahtinen 2017).

### 3.1.4 Rekisteröidyn oikeudet

Yhtenä suurena kokonaisuutena GDPR:ssä on rekisteröidyn erilaiset oikeudet. Tässä luvussa käsitellään oikeudet ja mitä ne käytännössä tarkoittaa. Näitä oikeuksia on määritelty asetuksessa III-luvussa artikloissa 12–23. Yhtenä isona osana uudessa EU:n tietosuoja-asetuksessa on tiedon läpinäkyvyys, joka käydään läpi artiklassa 12. Rekisteröidyn on tiedettävä tarkalleen, mihin hänen tietojansa käytetään. Kerättävästä henkilötiedosta on ilmoitettava selkeästi ja läpinäkyvästi. Lisäksi lapsiin kohdistuvassa viestinnässä on oltava erityisen tarkkana ja kielenkäyttö on oltava erityisen helposti ymmärrettävää. Nämä tiedot on ilmoitettava kirjallisesti. Laki antaa mahdollisuuden ilmoittaa tiedot sähköisesti, mikäli se on tarkoitettu laajemmalle joukolle, ns. yleisölle. Esimerkiksi verkkosivustolla riittää, että tiedot ovat selkeästi saatavilla. Erikoistapauksissa rekisteröidyn tiedot voidaan hänen pyynnöstään antaa suullisesti. Tiedonannosta ei voida veloittaa maksua. Henkilön on tarkkaan tiedettävä, mihin hänen tietojansa käytetään ja kenelle niitä mahdollisesti luovutetaan. Myöskin liian epämääräisesti tai ympäripyöreästi muotoillut lauseet ovat kiellettyjä. Tällainen voisi olla esimerkiksi seuraavanlainen lause: ”tietoja kerätään erilaisiin käyttötarkoituksiin” tai ”keräämme tarpeellista tietoa markkinointia varten”. (Korpisaari ym. 2018, 176–177.)

Rekisterinpitäjän on toimitettava rekisteröidylle keräämisen aikana rekisterinpitäjän tai sen edustajan yhteystiedot sekä tietosuojaajavastaavan yhteistiedot. Tämän lisäksi tulee toimittaa syy henkilötietojen käsittelylle ja perusteet sille, miksi tietoja on oikeus käsitellä. Jos rekisterinpitäjällä tai kolmannella osapuolella on oikeutettu etu tietojen käsittelyyn, rekisteröidylle tulee ilmoittaa näiden etujen sisältö sekä henkilötietojen vastaanottajat tai vastaanottajaryhmät. Rekisteröidylle täytyy myös antaa tieto siitä, mikäli rekisterinpitäjä aikoo siirtää tietoja EU-alueen ulkopuolelle tai kansainväliselle taholle. Näiden tietojen lisäksi rekisterinpitäjällä on velvollisuus kertoa henkilötietojen säilytysaika tai säilytyksen kriteerit läpinäkyvyyden takaamiseksi. (Korpisaari ym. 2018, 173.)

Rekisteröidylle on ilmoitettava hänen oikeuksistaan, joihin kuuluu mahdollisuus pyytää hänestä kerätyt tiedot, pyytää tietojen oikaisemista tai poistamista, tietojen käsittelyn rajoittamista tai vastustaa tietojen käsittelyä sekä oikeutta siirtää tiedot

järjestelmästä toiseen, mikäli tämä on teknisesti ja taloudellisesti mahdollista. Henkilölle on myös tiedotettava hänen oikeuksistaan peruuttaa suostumuksensa koska tahansa sekä oikeudesta tehdä valitus valvontaviranomaisille. Rekisteröidylle on myös kerrottava, onko henkilötietojen antaminen lakisääteistä tai sopimukseen perustuvaa, sekä on tiedotettava, mikäli hänestä tehdään automaattinen päätöksenteko. Rekisterinpitäjän tulee ilmoittaa kaikille henkilötietojen vastaanottajille, jos heidän saamiinsa henkilötietoihin kohdistuu oikaisu- tai poistovaatimuksia tai jos tietojen käsittelyyn muodostuu uusia rajoituksia. Poikkeuksena toimivat sellaiset tilanteet, jolloin tämän ilmoituksen suorittaminen koituu kohtuuttoman vaikeaksi tai mahdottomaksi. (Europan parlamentin ja neuvoston asetus 679/2016, Artikla 13, 19.)

Artiklassa 14 muistutetaan rekisterinpitäjän velvollisuudesta toimittaa henkilötiedot myös sellaisissa tapauksissa, jolloin henkilötietoja ei ole saatu suoraan rekisteröidyltä. Tämä artikla on pääosin samalainen kuin artikla 13, jossa henkilötiedot on saatu rekisteröidyltä, mutta suurimpana erona on artikla 14:ssä listattujen poikkeustilanteiden määrä. Esimerkiksi, jos rekisterinpitäjiä on useampia, riittää että vain yksi rekisterinpitäjä informoi rekisteröityä, mutta ilmoittaa kaikki tiedot toistenkin rekisterinpitäjien puolesta. Rekisteröidylle on selkeyden kannalta parempi, jos hän saa tarvittavat tiedot yhden rekisterinpitäjän kautta. Muut poikkeukset liittyvät pääosin tieteelliseen tai historialliseen tutkimukseen ja tilastollisiin tai arkistointitarkoituksiin. Poikkeukset on käsitelty asetuksessa melko suppeasti. (Korpisaari ym. 2018, 199.)

Asetuksessa kerrotaan, että rekisteröidyllä on oikeus nähdä hänestä tallennetut tiedot. Tämä parantaa huomattavasti läpinäkyvyyttä sekä varmistaa paremmin rekisterin lainmukaisuuden. Rekisteröidyllä on mahdollisuus tarkistaa, ovatko hänestä itsestään kaikki kerätyt tiedot oikeita ja oikeutettuja, jolloin hänellä on mahdollisuus pyytää virheellisistä tiedoista oikaisua tai tehdä valitus valvontaviranomaisille. Rekisteröidyllä on mahdollisuus saada tietää tiedon alkuperä, mikäli tietoa ei ole saatu suoraan häneltä, sekä tiedon säilyttämisaika tai sen määrittelemiskriteerit. Mikäli tiedot lähetetään sähköisesti rekisteröidylle, tiedot ovat lähetettävä suojattuna. Oikeus tietoihin on oltava pääosin maksuton, mutta tähänkin on tiettyjä poikkeuksia. Mikäli rekisteröity on juuri antanut tietojaan rekisterinpitäjälle tai rekisteröity pyytää tarkistusta useampaan kertaan lyhyen ajan

sisällä, jolloin rekisteriin ei ole ehtinyt tulla suuria muutoksia, tai jos rekisteröity pyytää useampia jäljennöksiä tiedoista, on rekisterinpitäjällä mahdollisuus pyytää tiedonannosta kohtuullinen korvaus. Rekisterinpitäjällä on myös tällöin mahdollisuus kieltäytyä toimesta, jolloin rekisterinpitäjän on osoitettava rekisteröidyn pyynnön perusteettomuus tai kohtuuttomuus. Mikäli rekisteröity pyytää tietojaan, rekisterinpitäjän on oltava varma rekisteröidyn henkilöllisyydestä, etenkin jos kyseiset tiedot sisältävät arkaluontoisia tai erityisryhmään kuuluvia tietoja. Rekisterinpitäjän on vastattava rekisteröidyn pyyntöön kuukauden kuluessa ja tiedot on annettava kolmen kuukauden sisällä. Mikäli pyyntö on monimutkainen ja vaatii pidempää käsittelyaikaa, on tästä ilmoitettava rekisteröidylle kuukauden sisällä. Käytännön esimerkissä henkilötiedot on hajautettuina useissa eri rekistereissä. Rekisteröidyllä on myös oikeus saada häntä koskevat henkilötiedot jäsennellyssä ja yleisesti käytetyssä muodossa, jolloin ne on mahdollista siirtää toiselle rekisterinpitäjälle ja toiseen järjestelmään. Tätä sovelletaan ainoastaan digitaalisissa rekistereissä. Artiklan tarkoituksena on kannustaa omadata- eli My Data -tyyppiseen tietojen hallintamalliin, jossa henkilö on itse keskiössä ja pääsee paremmin hallitsemaan häntä itseään koskevia tietoja. (Korpisaari ym. 2018, 209–215, 241–242, 247.)

Rekisteröidyllä on aina oikeus omien tietojensa oikaisemiseen, jolloin hänellä on mahdollisuus pyytää virheellisistä tiedoista oikaisua tai poistamista ja puutteelliset tiedot voidaan täydentää. Mikäli näin ei tehdä, hänellä on oikeus valittaa valvontaviranomaisille. Tämä tukee viidennen artiklan kohtaa, jossa määritellään, että henkilötietojen tulee olla täsmällisiä ja ajantasaisia. Tietojen täsmällisyys tai tarkkuus ovat asetuksessa tulkinnanvaraisia, mutta voidaan olettaa esimerkiksi, että jos rekisteriin tallennetaan ulkomailla syntyneet luokkaan ”ulkomaat”, rekisteröity ei voi vaatia täsmennytystä esimerkiksi luokkaan ”ruotsi”. Rekisteröity ei siis voi itse sanella, mitä rekisteriin tallennetaan. Tietojen oikaisemisesta ei myöskään saa periä maksua, mutta mikäli rekisterinpitäjä katsoo muutosta kohtuuttomaksi, voi rekisterinpitäjä periä kohtuullisen maksun muutoksen tekemisestä. (Korpisaari ym. 2018, 216–220.)

Oikeus tietojen poistamiseen eli ”oikeus tulle unohdetuksi” on saanut asetuksen myötä paljon huomiota. Rekisteröidyllä on oikeus saada tietonsa poistetuksi ilman viivästystä tietyn ehtoin. Nämä ehdot voivat olla sopimukseen perustuvia,

esimerkiksi laskutustiedot ja jäsenyydet. Tietojen lopullinen poistaminen tuo erilaisia haastavia kysymyksiä esimerkiksi siitä, millä lailla tiedot tulee poistaa. Voidaan kysyä myös, lasketaanko tietojen poistamiseksi sitä, että siirretään tiedot roskikseen, tai pitääkö tiedot poistaa siten, että tietoja on mahdotonta saada enää palautettua. Vaikka tiedot poistetaan tietojärjestelmistä, kone ainoastaan merkitsee sen, että tieto on poistettu, ja täten tieto on mahdollista palauttaa. Käytännössä tietojen täydellinen poistaminen on liki mahdotonta, sillä ainoa tapa varmistaa tietojen lopullinen poistuminen on kirjoittaa uudelleen tiedon päälle. Toinen suuri huolenaihe on, tuleeko tiedot poistaa myös erilaisista varmuuskopioista, koska yksittäisten tietojen poistaminen arkistoista tai varmuuskopioista voi olla hyvinkin haastavaa tai jopa mahdotonta. Tiedon poistaminen saattaa myös vaarantaa muiden rekisteröityjen oikeuksia, jolloin on tulkittu, ettei tietoja näistä varmuuskopioinneista ole tarpeellista poistaa, mutta on varmistettava, että tiedot eivät koskaan palaudu takaisin tietojärjestelmään. Henkilötiedot on poistettava silloin, kun henkilötietoja ei enää tarvita alkuperäiseen käyttötarkoitukseensa. Henkilötiedot tulee myös poistaa silloin, kun rekisteröity peruuttaa suostumuksensa. (Korpisaari ym. 2018, 222–234.)

Rekisteröidyllä on oikeus rajoittaa tietojensa käsittelyä. Tällainen tapaus on, kun rekisteröity kiistää tietojensa oikeinmukaisuuden, jolloin henkilötietojen käsittelyä rajoitetaan tietojen tarkastamisen ajaksi. Tällöin tiedot voidaan säilyttää, mutta muu käsittely vaatii rekisteröidyn luvan. Henkilötietojen käsittely on myös voinut tapahtua lainvastaisesti, eikä rekisteröity halua, että henkilötietoja poistetaan, jolloin niitä voidaan tilapäisesti rajoittaa. Tietoja voidaan myös rajoittaa, jos rekisterinpitäjä ei enää tarvitse kyseisiä henkilötietoja, mutta rekisteröity tarvitsee tietoja oikeudellisiin toimenpiteisiin. (Europan parlamentin ja neuvoston asetus (EU) 679/2016, Artikla 18.)

Rekisteröidyllä on oikeus kieltää täysin häntä koskevien henkilötietojen käsittely. Asetuksessa tätä käsitellään vastustamisoikeutena. Tällöin rekisterinpitäjä ei enää saa käsitellä rekisteröidyn tietoja. Poikkeuksena tähän on se, mikäli rekisterinpitäjällä on tärkeä ja perusteltu syy, joka ajaa rekisteröidyn omien etujen edelle. Henkilö voi aina kieltää henkilötietojensa käsittelyn suoramarkkinointia varten, tähän liittyy myös rekisteröidyn profilointi. Vastustamisoikeutta sovelletaan sellaisiin tapauksiin, jolloin tietojen kerääminen on laillista, mutta rekisteröi-

ty vastustaa tätä. (Europan parlamentin ja neuvoston asetus 2016/679 Artikla 21.) Rekisteröidyllä on myös oikeus kieltää automaattiset päätöksenteot ja profiloinnit, jotka haittaavat tai vaikuttavat hänen oikeuksiinsa merkittävällä tavalla. Automaattiset päätökset ovat jo jonkin verran käytössä ja tulevat lähitulevaisuudessa lisääntymään huomattavasti. (Korpisaari ym. 2018, 257–259.)

### 3.1.5 Sanktiot ja seuraamukset

Toiminnan varmistamiseksi asetuksessa on myös määritelty huomattavat seuraamukset, mikäli asetusta ei noudateta. Pahimmillaan rikkeistä voidaan tuomita maksettavaksi sanktioita, jotka voivat olla jopa 20 miljoonaa euroa tai 4 % yrityksen edellisen tilikauden maailmanlaajuisesta liikevaihdosta, riippuen siitä, kumpi summa on suurempi. Mikäli henkilörekisteriä pitävä organisaatio on aiheuttanut aineellista tai aineetonta vahinkoa rekisteröidylle, on organisaatio velvollinen korvaamaan vahingot, mikäli se on tarkoituksellisesti laiminlyönyt tietosuoja-asetusta. (Hanninen ym. 2017, 129–130.)

Useita sakkoja on jo ehditty kirjoittaa lainsäädännön voimaantulon jälkeen, josta vuonna 2018 mittavin sakkorangaistus määrättiin portugalilaiselle Centro Hospitalar Barreiro Montijo -sairaalalle, joka tuomittiin yhteensä 400 000 euron sakkoihin. Sairaalan potilastietojärjestelmää pääsi käsittelemään sellaisia henkilökuntaan kuuluvia, joilla ei ollut siihen syytä. Tästä määrättiin 300 000 euron sanktiot. Loput 100 000 euroa tulivat sairaalan kykenemättömyydestä varmistaa järjestelmien ja palvelujen luottamuksellisuus, eheys ja saatavuus. (LaCroix 2018.) Lisäksi puolalaiselle yritykselle määrättiin mittavat sakot artikla 14 kohdan rikkomisesta, kun yritys keräsi yli kuuden miljoonan yrittäjän henkilötiedot vapaista lähteistä eikä ilmoittanut rekisteröidylle tietojen lähdettä, tietojenkäsittelyn tarkoitusta eikä rekisteröidyn oikeuksia, jolloin rekisteröidyillä ei ollut mahdollisuutta vastustaa tietojen käsittelyä, korjausta tai poistamista. (European Data Protection Board 2019.)

# 4 TIETOTURVAOPPAAN JA -KOULUTUKSEN SUUNNITTELU

Alkuperäisenä ideana oli pitää pelkästään tietoturvakoulutus, mutta pian kävi ilmi, että myös fyysiselle oppaalle oli suuri tarve ja se auttaisi myös tukemaan koulutusta. Säätiöllä oli joitakin toimintaohjeita valmiina, mutta oli selkeää, että yhtenäinen opas olisi tarpeen, jotta henkilökunta osaisi löytää aiheesta tarvittavat tiedot helposti ja ymmärrettävästi. Tämän takia opinnäytetyö koostuu raportin lisäksi tietoturvaoppaasta sekä tietosuojaan kohdistuvasta täsmäkoulutuksesta.

Osa ihmisistä ei piittaa tietosuoja-asetuksesta, kun taas osa saattaa ylireagoida voimakkaasti. On tärkeää ymmärtää, mitä asetus edellyttää, jotta voitaisiin toimia joustavasti, mutta oikeaoppisesti. On myös tärkeää kouluttaa koko henkilöstö tietoturvan perustietoihin, jotta he ymmärtävät vastuunsa ja jokapäiväiset riskit ja uhat.

## 4.1 Tietoturvakysely

Ennen suunnitteluvaihetta päätin tehdä pienimuotoisen kyselyn (Liite 1), jossa kartoitettiin henkilökunnan osaamista ja tietämystä tietoturvasta. Kysely toteutettiin Google Formsin avulla ja se lähetettiin niille 46:lle Eduro-säätiön henkilökunnan jäsenille, jotka käsittelevät henkilötietoja päivittäisessä työssään. Kyselyyn vastasi 21 henkilöä, joten vastausprosentti oli noin 46 %. Google Formsin kautta sain muodostettua vastauksista suoraan kysymyskohtaiset diagrammit, joiden perusteella vastauksia oli helppo analysoida. Kyselyn avulla sain tietoa koulutusaiheiden tarpeista ja selvisi, mistä aihealueista henkilökunnalla oli puutteita, jonka takia taas kysely helpotti oppaan sekä koulutuksen suunnittelua.

Kysely oli jaettu kahteen osaan: ”Mitä ja miten tietoja käsittelen”, jossa kysyttiin millä lailla henkilökunta käsittelee tietoja, ja ”Tietämys tietoturvasta”, jossa testattiin tietoturva- ja tietosuojaosaamista. Kyselyssä kävi ilmi jonkin verran ongelmia. Henkilökunnan tuntemuksessa oli paljon kehitettävää. Esimerkiksi 95 % henkilökunnasta vastasi, että henkilötunnus on arkaluontoinen henkilötieto, vaikka kyseessä on erityinen henkilötietoryhmä. Verkko-osoitteessa oleva *https* oli henkilökunnalle hankala aihe, johon suurin osa vastasi myös väärin.

Alussa kysyttiin, mihin järjestelmiin vastanneilla oli käyttöoikeudet ja oliko käytössä peruskäyttöoikeudet tai laajennetut oikeudet. Tämän kysymyksen tarkoituksena oli varmistaa, että laajennettujen oikeuksien omaavilla henkilöillä olisi vaativuutta vastaavasti paremmat käsitykset tietoturvasta ja tietosuojasta. Tämän perusteella voitaisiin mahdollistaa heille tulevaisuudessa syventäviä koulutuksia. Kyselyyn vastanneista vain yhdellä henkilöllä oli laajennetut oikeudet, joten suurta johtopäätöstä vastauksista oli lähes mahdoton tehdä. Henkilökunnalta kysyttiin myös varmuuskopioinnista. Tällä tarkasteltiin, kuinka säännöllisesti näitä tehdään. Vaikka kyselyssä jopa 60 % vastasi, ettei tee varmuuskopiointia, niin se ei välttämättä ole niin suuri huolenaihe, sillä monen henkilön työn luonteen takia heidän ei tarvitsekaan tehdä niitä.

Kyselyyn vastanneista 81 % kertoi, että he käsittelevät päivittäin arkaluontoisia henkilötietoja. Todennäköisesti luvun suuruus johtuu pitkälti siitä, että isolle osalle henkilökunnasta on epäselvää, mitkä tiedot kuuluvat arkaluontoisiin henkilötietoihin. Tämä kävi myös ilmi myöhemmin kyselyssä.

Vastanneista 47 % vastasi kyselyssä, etteivät he käsittele luottamuksellista tietoa etänä. Luku oli yllättävän pieni organisaation toimenkuvaan nähden, ja hyvin todennäköisesti luku on paljon tätä suurempi, sillä vastanneet eivät välttämättä ymmärrä, mitä asioita lasketaan luottamuksellisiin tietoihin.

Kyselyssä kysyttiin myös salasanojen käytöstä. Vajaat 62 % vastanneista kertoi, että osa heidän käyttämistään salasanoista on samankaltaisia, ja jopa yli 14 % vastasi, että suurin osa salasanoista on samanlaisia. Tämä on erittäin huolestuttavaa, sillä se aiheuttaa huomattavia tietoturvariskejä, jos yksikin salasana pääsee ulkopuolisen käsiin.

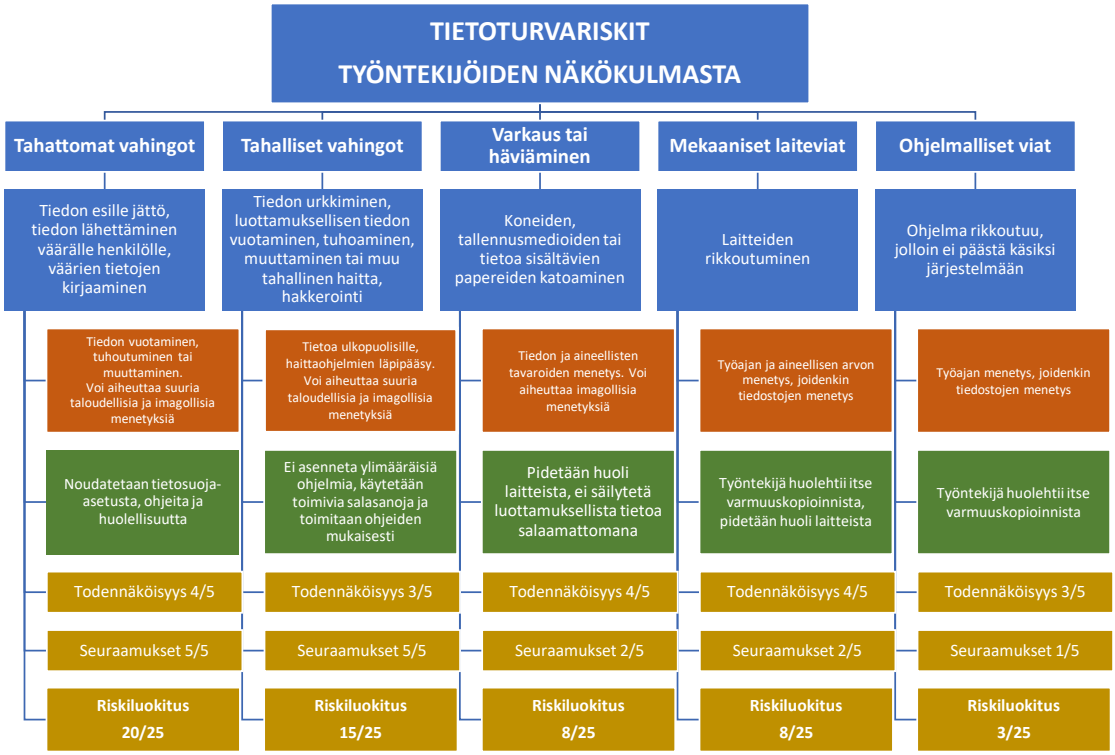
Suurin osa kyselyyn vastanneista kaipasi apua internetin ja laitteiden turvallisen käytön kanssa, henkilötietojen keräämisessä (ARVI[1] kirjaukset) sekä EU:n tietosuoja-asetuksen kanssa. Vähiten apua kaivattiin salasanojen käytössä, mikä on osaltaan ristiriidassa sen kanssa, että samanlaisia tai samankaltaisia sala-

[1] ARVI on Eduron oma arviointijärjestelmä, johon tehdään toimenpiteitä ja kirjauksia asiakkaista.

sanoja käytti yli puolet vastanneista. Tämä voi johtua joko siitä, että henkilöt eivät tiedä salasanojen merkityksestä, tai sitten siitä, ettei heillä ole tarpeeksi kiinnostusta keksiä eri salasanoja jokaiseen järjestelmään. Tämä kysymys auttoikin suuresti koulutuksen suunnittelussa.

Suurin osa henkilökunnasta piti itseään huolellisena tai erittäin huolellisena henkilötietojen käsittelyssä. Kyselyssä pyydettiin arvioimaan, onko henkilö mielestään käsitellyt tietoja epäturvallisesti työnteon helpottamiseksi. Vaihtoehdot jakautuivat asteikolla 1–5, jossa 1 tarkoitti, että käsittelyä ei ole koskaan tehty epäturvallisesti työnteon helpottamiseksi, ja 5 tarkoitti, että tätä tapahtuu usein. Vastaukset jakautuivat tasaisesti 1:n ja 4:n välille, ainoastaan yksi henkilö vastasi tekevänsä näin usein. Tässä täytyy kuitenkin muistaa, että vika ei kuitenkaan välttämättä ole kokonaan henkilössä, vaan organisaation tulee tarkastella omia järjestelmiä, onko ne tehty niin kankeaksi, että työnteon helppoutta ja tietoturvan takaamista ei ole helppo yhdistää. Kyselyn toisessa osassa testattiin henkilökunnan osaamista. Tarkoitus ei ollut selvittää laajasti henkilökunnan osaamista, vaan saada jonkinlainen käsitys aiheesta. Ensimmäisessä kysymyksessä piti vastata kymmeneen kohtaan, jotka liittyivät tietosuojaan.

Henkilöstön näkökulmasta (kuvio 2) tehdyn uhkapuun avulla pystytään selvittämään mahdollisia riskejä, joita voi ilmetä työntekijöiden roolissa. Tämän avulla saatiin selvennettyä uhkia, jotka ovat nimenomaan työntekijöiden kannalta suurimmat. Sinisellä taustalla olevat kertovat yleisimmistä riskeistä, joita Eduron työntekijät voivat kohdata, punaisella taustalla näkyy riskien vaikutukset, vihreällä taustalla näkyy riskejä ennaltaehkäiseviä toimia ja keltaisella taustalla kuvataan riskien todennäköisyys asteikolla 1–5, riskien seuraamukset asteikolla 1–5 sekä riskiluokitusta asteikolla 1–25. Uhkapuussa on otettu huomioon riskien todennäköisyydet sekä haittavaikutukset. Riskiluokitus määräytyy kertaamalla todennäköisyydet seuraamuksella. Suurimpana riskinä on ihmisten aiheuttamat tahattomat vahingot, näihin sisältyy esimerkiksi tietoja sisältävien papereiden jättäminen työpöydälle muiden ihmisten nähtäville. Tahattomat vahingot aiheutuvat yleensä ajattelemattomuudesta ja huolimattomuudesta, ja niitä on vaikea ennakoida.




Kuvio 2. Uhkapuussa havainnollistetaan riskit ja riskiluokitukset

Uhkapuusta rajattiin pois muun muassa ne aiheet, jotka koskevat esimerkiksi hallinnon työnkuvaan kuuluvia ohjelmistoja, esimerkiksi taloushallinnon ohjelmistoja. Nämä kohdistuvat vain pieneen osaan työntekijöitä, eikä niitä näin ollen ollut aiheellista ottaa mukaan koko henkilökunnan yleiseen kouluttamiseen.

Henkilöstön on tunnistettava mahdolliset riskit ja osattava tehdä kohdistuvista riskeistä poikkeamia. Organisaatiossa tyypilliset tietoturvariskit ovat päätelaitteen häviäminen, jossa on salassa pidettävää tietoa tai kyseisen laitteen avulla päästään käsiksi sellaiseen tietoon. Salassa pidettävään tietoon voi myös päästä käsiksi sellainen henkilö, jolla ei ole siihen asianmukaista oikeutta. Tyypillisiä riskejä ovat myös, jos käyttäjätunnus tai salasana päätyvät ulkopuolisille, päätelaite on saastunut esimerkiksi jollakin haittaohjelmalla tai viruksella tai jos tietoja menetetään laiterikkoutuman takia. Inhimilliset erehdykset voivat sattua hyvinkin helposti, voidaan esimerkiksi tulostaa väärälle tulostimelle, lähetetään viesti väärälle henkilölle tai unohdetaan jokin tärkeä paperi johonkin. Nämä erehdykset voidaan minimoida, mutta ne ovat hyvin hankalia poissulkea kokonaan. Organisaatiossa voi myös käydä niin, että tiloissa liikkuu sellaisia henkilöitä, joilla ei ole asianmukaisia lupia tai jos organisaatiossa ei ole toimittu ohjeiden tai pro-

sessien mukaisella tavalla. Henkilökunnan on omaksuttava prosessit, ja siitä on tultava osa rutiinia. Tämä edellyttää sitä, että henkilöstön on hallittava organisaation toimintatavat ja käytännöt. (Järvinen & Rousku 2017, 42.) Henkilöstöltä vaaditaan nopeaa ja aktiivista reagointia mahdollisiin uhkiin, ja niistä on välittömästi ilmoitettava esimiehelle ja/tai tietosuojavastaavalle.

Aina ennen uuden palvelun käyttöönottoa on syytä pohtia palvelun riskit eri näkökulmista ja tehtävä jonkinlainen riskianalyysi. On syytä pohtia, mitä tietoja palvelulla käsitellään, ja pitää tarkistaa, millainen tietosuojaseloste palvelulla on. Ei voida olettaa, että vaikka kyseessä olisi iso luotettava organisaatio, niin käyttäjäehdot olisivat välttämättä organisaation toiminnalle sopivia.

## 4.2 Tietoturvaopas

Eduro-säätiöllä on jonkin verran ohjeistuksia, mutta osa niistä on vanhoja, osa taas hieman epäselkeästi kirjoitettuja. Lisäksi ne ovat hajautettuja, jonka vuoksi näin tarpeelliseksi niiden yhteen kokoamisen. Lähdin tekemään opasta, jonka tavoitteena on olla mahdollisimman yksinkertainen ja selkeä. Kävin läpi säätiön kriittiset järjestelmät ja loin niiden pohjalta yhtenäiset toimintalinjaukset. Käytettävänä materiaalina minulla oli Eduro-säätiön jo valmiit ohjeistukset ja linjaukset, joiden avulla pystyin määrittelemään työskentelyohjeita yhtenäiseksi kokonaisuudeksi. Kaikista osa-alueista valmiita ohjeistuksia ei ollut, joten jouduin tekemään niitä itse tietoturvan ja tietosuojan teoriapohjaa apuna käyttäen. Tekemäni ohjeistukset hyväksytetään säätiön johtoportaassa.

Tietoturvaopas on suunniteltu aloittaville työntekijöille sekä niille, jotka tarvitsevat nopeasti tiedon jokapäiväiseen työskentelyyn. Koin tärkeäksi myös sen, että opas olisi sellaisessa muodossa, jotta tiedot olisivat nopeasti päivitettävissä. Siksi suunnittelin oppaan siten, että se on helposti muokattavissa, mutta silti visuaalisesti miellyttävä. Tällä tavoin oppaan voi päivittää ilman taitto-ohjelmaa. Tietoturvaopas tulee olemaan sekä digitaalisessa muodossa säätiön sisäisessä järjestelmässä että vihkona henkilöstön yleisen perehdyttämisoppaan liitteenä. Opasvihkot painetaan Eduro-säätiön omissa tiloissa pienissä määrissä tarpeen mukaan.

### 4.2.1 Salassapito ja vaitiolositoumus

Henkilökunta ja kolmannen osapuolen tahot ja henkilöt, jotka ovat tekemisissä Eduro-säätiön henkilötietojen, luottamuksellisten ja salassa pidettävien tietojen kanssa, ovat velvoitettuja allekirjoittamaan salassapitosopimuksen tai vaitiolositoumuksen. Tämän sitoumuksen tarkoituksena on varmistaa, että henkilöt ymmärtävät salassapitovelvoitteensa. Kahden tai useamman organisaation väliset salassapitosopimukset voidaan liittää osaksi yleissopimusta. Organisaation salassa pidettävät tiedot saa luovuttaa ainoastaan erikseen määrätyille henkilöille tai henkilöryhmille. Vaitiolovelvollisuus jatkuu myös sopimuksen päättymisen jälkeen. (Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008, 44–45.)

EU:n tietosuoja-asetusten lisäksi sosiaalialalla asiakastietojen salassapito ja luottamuksellisuus on laissa määritelty ja sen noudattaminen on välttämätöntä. Säätiössä jokainen tuotannollinen työntekijä, kuntoutuja ja työvoimapoliittisessa valmennustoimenpiteessä oleva henkilö on velvollinen allekirjoittamaan henkilökohtaisen salassapitositoumuksen. Tämän lisäksi kaikki säätiön yhteistyökumppanit, jotka ovat tekemisissä Eduro-säätiön henkilötietojen tai luottamuksellisen tietojen kanssa, joutuvat hyväksymään ja allekirjoittamaan säätiön salassapitositoumuksen. Eduron salassapidon piiriin kuuluvia tietoja ovat esimerkiksi liike- ja ammattisalaisuudet, henkilötiedot, asiakassuhteessa olevia henkilöitä koskevat tiedot ja turvallisuusjärjestelyihin liittyvät tiedot. Tieto on salassa pidettävää tietoa riippumatta siitä, onko se suullisessa, kirjallisessa, sähköisessä tai muussa vastaavassa muodossa. (Eduro-säätiö 2018a.) Sosiaalihuollon asiakirjat, jotka sisältävät tietoja sosiaalihuollon asiakkaasta tai muusta yksityisestä henkilöstä, ovat myös salassa pidettäviä (Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista 812/2000, 3 §). Keskustelutilanteessa tulee myös huolehtia siitä, ketkä voisivat mahdollisesti olla kuuloetäisyyden päästä, tai on pyrittävä löytämään sellainen tila, jossa keskustelua voidaan vapaasti käydä, sillä muutoin keskustelut tulee anonymisoida (Järvinen & Rousku 2017, 58).

Työntekijöillä voi olla hankaluuksia tunnistaa, mitkä organisaation asiakirjoista ovat salassa pidettäviä. Voi olla, että henkilöillä on pääsy joihinkin luottamuksellisiin tai salassa pidettäviin tietoihin eikä hän tiedä niiden luottamuksellisuudes-

ta, vaan kokee, että tiedot ovat yleisessä tiedossa tai julkisia. Henkilötietojen tai salassa pidettävien tietojen luovuttamisen kanssa pitää olla erityisen tarkka, sillä henkilötietojen välittäminen esimerkiksi työtovereille tai jopa esimiehelle voi olla lainvastaista, ellei se ole perusteltua. (Järvinen & Rousku 2017, 52.)

### 4.2.2 Salasanan määritteleminen ja tallentaminen

Oppaassa käydään läpi säätiön salasanakäytäntöjä. Päätin lisätä aiheen kyselyyn, sillä säätiön riskienhallinnassa on arvioitu, että henkilökunnan salasanakäytänteet ja ohjeistukset puuttuvat ja monella voi olla hyvinkin vanhanaikaiset ymmärrykset käytäntöjen suhteen. Säätiön riskienhallinnassa on määritelty, että asteikolla yhdestä viiteen heikoista salasanoista johtuvien riskien todennäköisyys kuuluu luokkaan kolme ja riskin seuraamukset ovat luokassa neljä. (Edurosäätiö 2018c.) Erilaisilla järjestelmillä on erilaiset tavat määritellä hyvä salasana. Joissakin pitää olla vähintään kahdeksan merkkiä, joissakin numeroita, suuria ja pieniä merkkejä tai jopa erikoismerkkejä. Tämän takia on ymmärrettävää, että käyttäjät ovat menneet hiukan sekaisin hyvistä ja toimivista salasanoista. Kyselyn perusteella suurella osalla työntekijöistä salasanat olivat monissa järjestelmissä samat tai samankaltaisia. Tämä johtaa siihen, että mikäli edes yhteenkään järjestelmään tapahtuu tietomurto, niin salasanat ovat tiedossa myös muihinkin järjestelmiin.

Yhdysvaltojen kansallinen standardien ja teknologian instituutti (NIST) on julkaissut ohjeistuksen, jossa todetaan, ettei monimutkainen salasana ole välttämättä huomattavasti turvallisempi vaihtoehto kuin pitkä ”helposti muistettava” salasana. Esimerkiksi ”talvenkylminilta” on käytännössä turvallisempi vaihtoehto kuin J#We”0. Pakollinen salasanan ”monimutkaistaminen” voi pahimmillaan tarkoittaa sitä, että samaa salasanaa käytetään useissa paikoissa ja salasanakuviot toistuvat. Lisäksi jos pakotetaan käyttämään erikoismerkkejä tai isoja kirjaimia, voidaan mahdollisesti päätellä tai ohjelmoida yleisimmin käytettävät merkintätavat. Tästä esimerkkinä ”salasana”, jos tähän on pakko lisätä vähintään yksi numero, suuri kirjain ja erikoismerkki, on uusi muodostettu salasana mahdollisesti ”Salasana1!”. Lisäksi nämä muutokset lisäävät käyttäjän turhautuneisuutta salasanan muodostamiseen. Näiden lisäksi salasanassa ei saa toistua samat kirjaimet liian usein esimerkiksi aaaaaa, ei saa olla kuviollisia esimer-

kiksi a1a1a1 tai peräkkäisiä esimerkiksi qwerty tai abc123. (Grassi, Fenton & Newton 2017, 68, 14.)

Väsytyshyökkäys, eli Brute-force attack, on yksinkertainen kryptoanalyysihyökkäyksen menetelmä, jossa käydään läpi systemaattisesti kaikki salasanavaihtoehdot läpi nollan ja äärettömän väliltä siinä toivossa, että salasanan murtuminen onnistuisi (Shankdhar 2018). Eduro-säätiössä tätä menetelmää ei pidetä suurimpana uhkana. Tässä hyökkäystavassa ei ole suurta riskiä säätiön toimintaan ja menetelmän riskiarvio on hyvinkin pieni.

Suunnittelin opasta varten matriisin, jonka avulla työntekijät osaavat käyttää salasanojansa oikein. Taulukko 2:ssa näkyy, miten eri tasoisissa järjestelmissä tulee valita oikean vahvuinen salasana.

Taulukko 2. Salasanamatriisi Eduron käyttämistä palveluista

| TASO 1 | TASO 2 | TASO 3 |
|---|---|---|
| Suuren riskiluokan järjestelmät, joissa käsitellään henkilötietoja ym. salassa pidettäviä tietoja | Sivustot, joissa ei aiheudu suuria riskejä | Järjestelmät, joista voi aiheutua vain hyvin pieniä riskejä. |
| • ARVI-järjestelmä<br>• Sähköposti<br>• Muut järjestelmät, joissa käsitellään salassapidettäviä tietoja | • Luotettavammat sivustot<br>• Sometilit<br>• Peruskäyttäjätason tilit; Heeros ja C&Q<br>• Vanha ARVI<br>• Tunnukset voidaan säilyttää koneella, mutta salasanojen on oltava uniikkeja | • Tyypilliset sivustot, esim. tilausten seurantasivu<br>• Salasanat ja käyttäjätunnukset voidaan tallentaa koneelle. |
| • Ei suositella käyttää salasanan hallintaohjelmaa | • Voidaan käyttää salasanan hallintaohjelmaa | • Voidaan käyttää salasanan hallintaohjelmaa |

Salasanan säännöllinen vaihtaminen ei luo käytännössä lisää tietoturvaa, sillä useiden salasanojen muistaminen on lähes mahdotonta. Salasanojen vaihtaminen johti siihen, että ihmiset laittoivat vain numeroita perään, esimerkiksi salasana1, salasana2 ja niin edelleen. (Komanduri ym. 2011, 7.)

Salasanan hallintaohjelmien käyttö on joissakin tapauksessa suositeltua varsinkin, jos palveluja tarjoava yritys on luotettava ja he kiinnittävät erityisen paljon huomiota tietoturvallisuuteen. IT-tuki määrittelee käytettävät ohjelmat, mutta tämän lisäksi IT-tuki seuraa ulkopuolisten järjestelmien käyttöön kohdistuvia mahdollisia tietoturvaloukkauksia, jolloin pystytään nopeasti reagoimaan tilanteisiin. Mikäli käyttäjätunnuksella on järjestelmäylläpitäjän oikeudet, niin salasanojen tulee olla erityisen hyvin suojattu.

### 4.2.3 Järjestelmien etäkäyttö

Järjestelmien etäkäyttö yleisesti työpaikoilla on lisääntymässä, ja Eduron tulee pysyä kehityksen mukana. Tuoreessa Työ- ja elinkeinoministeriön tekemässä julkaisussa kerrotaan, kuinka etäkäyttö on yleistynyt 2012 ja 2017 välisenä aikana. Vuonna 2012 etätyötä teki vähintään satunnaisesti 21 % työntekijöistä, ja vuonna 2017 luku oli jo 35 %. Suurin muutos on tapahtunut viikoittaisen etätyön lisääntymisessä. (Lyly-Yrjänäinen 2018, 69.) Myös vähäisten työtehtävien tekeminen vapaa-ajalla on lisääntynyt. Voidaan vastata puhelimeen, päivittää organisaation some-tilejä tai vastata sähköposteihin. Tällöin on myös muistettava noudattaa organisaation ohjeita. Henkilökohtaisten asioiden hoitaminen organisaation sähköpostilla ei ole suotavaa. (Järvinen & Rousku 2017, 62.)

Salassa pidettäviin tietoihin liittyvä käsittely ja toiminta on turvallisinta organisaation omissa tiloissa. Tämä johtuu siitä, että yleensä organisaatiolla on selkeät toimintaohjeet, joita tulee noudattaa. Ohjeiden on kuitenkin oltava yksiselitteiset ja selkeät toimivuuden varmistamiseksi. Muualla kuin organisaation tiloissa toimiminen on yleensä turvattomampaa, sillä riskitekijöitä voi olla vaikeampi hallita. Usein sopimukset voivat estää etätyömahdollisuudet tai käytön henkilökohtaisilla laitteilla. ICT-alalla on yleistä, että ylläpitotöitä saadaan käsitellä ainoastaan organisaation määräämissä työpisteissä. (Järvinen & Rousku 2017, 48.)

Edurossa on laadittu ohje, joka kattaa työasemien ja mobiililaitteiden käytön. Ohjeessa on todettu, että esimerkiksi varkauden yhteydessä menetetty tieto voi olla huomattavasti suurempi haitta organisaatiolle kuin tietokoneen aineellinen hinta. Ohje kehottaa myös erityiseen huolellisuuteen ja varovaisuuteen aina, kun laitteita ja järjestelmiä käytetään etänä. (Eduro-säätiö 2018e.) Oppaassa

läpikäyty etäkäyttö perustuu Eduron laadittuihin olemassa oleviin linjauksiin sekä yksinkertaiseen matriisiin (taulukko 3), jonka tavoitteena on selventää, mitä järjestelmiä voidaan käyttää etänä ja mitä ei. Lähtökohtaisesti etäkäyttökielto koskee kaikkia niitä järjestelmiä, joissa käsitellään henkilötietoja. Tällaisella etätyön rajoittamisella pyritään minimoimaan tietojen leviämistä ulkopuolisille. On suositeltavaa käyttää 3G- tai 4G-yhteyttä WIFI-verkon sijasta, sillä WIFI-verkkoa on lähes aina turvattomampi käyttää ja tieto voi kulkeutua huonosti suojatun laitteen läpi (Järvinen & Rousku 2017, 69).

Taulukko 3. Matriisi Eduron järjestelmien etäkäyttöoikeuksista

| Järjestelmä | Rajatut käyttäjäoikeudet | Laajennetut käyttäjäoikeudet | Järjestelmävalvoja |
|---|---|---|---|
| **ARVI** | SAA | SAA | EI |
| **ARVI2** | EI | EI | EI |
| **Sähköposti** | SAA | SAA | SAA |
| **IMS** | SAA | SAA | EI |
| **C&Q** | SAA | EI | EI |
| **Telia VIP** | - | - | |

### 4.2.4 Tallentaminen ja varmuuskopiointi

Eduron linjauksen mukaan tiedostojen henkilökohtaiseen varmuuskopioon käytetään Microsoft OneDriveä ja jokainen työntekijä varmistaa itse, että kaikki tiedot varmuuskopioidaan tasaisin väliajoin. Jos varmuuskopiointi on automatisoitu, täytyy varmuuskopiot varmistaa säännöllisesti, eli että tiedot on varmuuskopioitu oikein ja että palautusprosessi toimii. Myös pilvipalvelujen varmuuskopiointien onnistuminen on varmistettava. (International Chamber of Commerce 2016, 9.) CSC-tieteen tietotekniikan keskuksen ylläpitämässä Eduuni-palvelussa todetaan, että ”palvelun käyttö sisältää merkittäviä riskejä omistajuuteen, tietosuojaan tai tietoturvaan liittyen”, ja se on luokittanut palvelun huonoimpaan luokkaan. Vaikka käyttäjien tallentamat tiedostot säilyvät tekijöille, niin ”Microsoft pidättää oikeuden valvoa ja tarkistaa tiedostoja laittoman sisällön varalta”. Lisäksi palvelu ei sijaitse kokonaan EU- tai ETA-alueen sisällä. (Tikkanen & Kommonen 2017.) Vaikka palveluun liittyy omat riskinsä, Eduro on tehnyt

oman riskianalyysinsä, jonka mukaan ulkoisten tallennuslaitteiden käyttö aiheuttaa huomattavasti suuremman uhan verrattuna muihin vastaaviin palveluihin. Tämän lisäksi palvelun luotettavuus ja käytettävyys on parempaa verrattuna muihin ratkaisuihin, ja palvelun eduiksi katsotaan myös sen helppokäyttöisyys sekä tuotteen edullisuus.

NIST:n IT-tietoturvatietoisuuteen ohjelmistopäällikkö Carolyn Schmidt totesi haastattelussa, että ulkoiset mediat ovat siirrettäviä, käteviä ja helppokäyttöisiä ja niiden kieltäminen olisi kohtuuton ja niiden käyttö riippuu vahvasti käyttäjän omasta harkinnasta (TechTarget: SearchSecurity 2010). Edurossa on linjattu, että henkilötietojen tallentamista ulkoisiin tallennusmedioihin kuten USB-tikkuihin tai mukana kulkeviin ulkoisiin kovalevyihin on kielletty ja salassa pidettävien tietojen tallentamista näihin on vältettävä. Epämääräisistä tai tunnistamattomista lähteistä tulevien USB-laitteiden kytkeminen Eduron laitteisiin on kiellettyä, sillä niiden avulla järjestelmiin voidaan ujuttaa haittaohjelmia. Tämän takia Eduron koneissa ulkoisten laitteiden automaattinen sovellusten ajo on poistettu käytöstä.

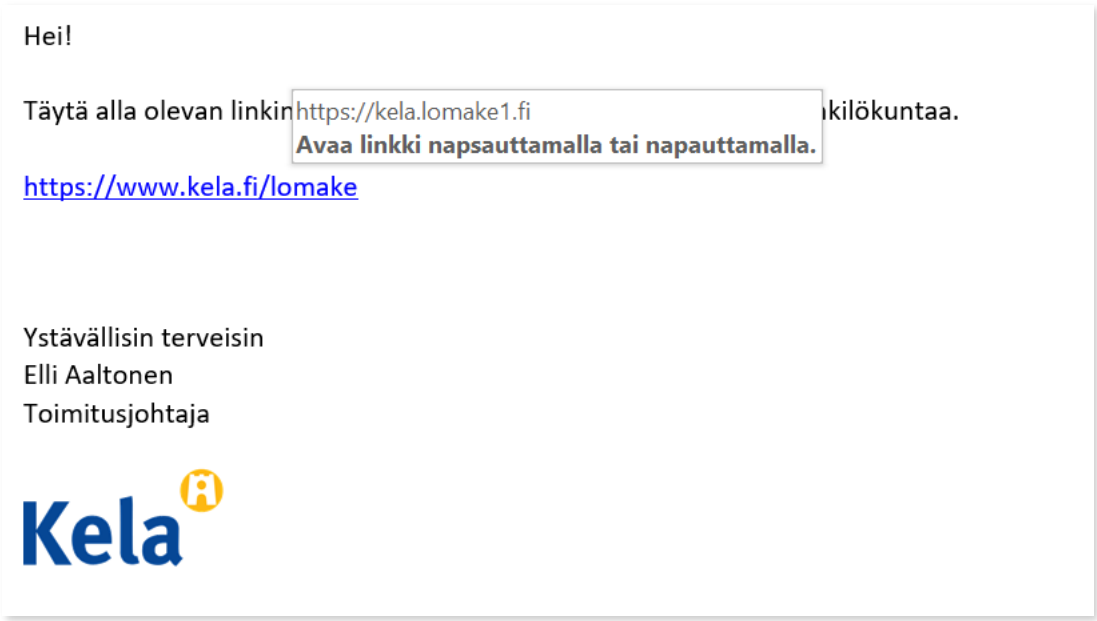
### 4.2.5 Tietoturvallinen internetin käyttö

Kyselyssä kävi ilmi myös se, että monelle henkilölle oli vierasta, miten tunnistetaan turvallisia linkkejä tai mitä suojattu sivu tarkoittaa. Kysymykseen vastasi 20 ihmistä, joista tasan puolet vastasivat, että sähköpostissa oleva linkki on turvallinen, vaikka niin ei ollut. Sähköposteja on erittäin helppo väärentää, eikä siihen tarvita osaamista. On olemassa web-palveluita, joilla on erittäin helppo lähettää sähköposteja kenen tahansa nimellä. (Ruohonen 2002, 358.)

Kuva 1 näyttää oikealta viestiltä, joka olisi tullut Kelan toimitusjohtajalta, mutta todellisuudessa viesti on lähetetty anonyymisti sähköpostigeneraattorin avulla. Roskapostisuodattimet saattavat suodattaa viestit pois tai siirtää sen roskakoriin, kuten tässä kokeilussa kävi.

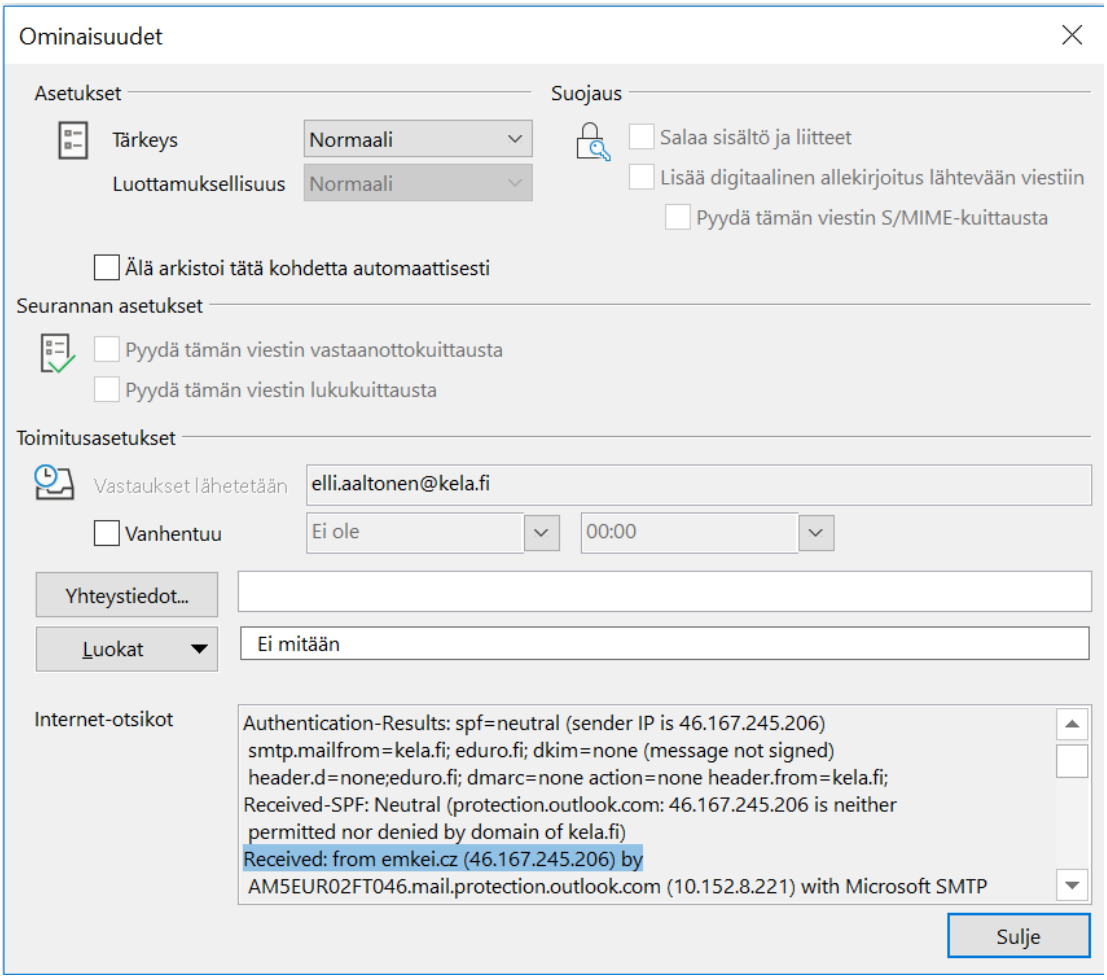

Kuva 1. Viesti vaikuttaa nopeasti katsottuna autenttiselta

Viestissä näkyvä linkki näyttää siltä, että osoite on aito, mutta kuva 2 osoittaa linkin olevan väärä. Linkki on aina syytä tarkistaa. Tämän lisäksi kaikki eivät ymmärrä domain-osoitteen rakennetta. Tässä tapauksessa alidomain on kela ja päädomain on lomake1.fi. Tässäkin on oltava tarkkana, että päädomain ohjautuu luotettavalle sivustolle. Mikä tekee asiasta entistä vaikeampaa havaita, on se, että osoitteessa voi käyttää kirjaimien lisäksi numeroita sekä muita kirjaimia hämäystarkoituksessa. Tästä esimerkkinä Kela, jossa L-kirjain on oikeasti iso i-kirjain.




Kuva 2. Linkit saattavat johtaa joskus harhaan

Mobiililaitteita käyttäessä on vaikeampi havaita näitä harhaanjohtavia linkkejä, sillä mobiilisähköpostiohjelmat eivät aina näytä oikeaa linkkiosoitetta. Tämä esimerkki ei rajoitu pelkästään sähköpostikäyttöön, vaan linkkiä voidaan käyttää mihin tahansa www-sivustoon. Voi olla mahdollista päätellä sähköpostiviestin otsikkotiedostoista viestin aitoutta, mutta tämä vaatii erityisen paljon osaamista, ja jopa asiantuntija ei pysty jokaista viestiä tarkastamaan. (Ruohonen 2002, 358.) Kuvassa 3 on Microsoft Outlook ominaisuudet -ikkuna, josta näkee otsikkotiedot. Tässä tapauksessa näkyy osoite ja IP-numero. RIPE:n tai WHOIS-palvelun avulla saadaan vielä varmistus, että kyseinen IP-numero on Tšekeistä.




Kuva 3. Ominaisuudet-ikkunasta näkee, että alkuperäinen lähettäjä on Tšekeistä

Selaimeen asennettavissa ohjelmissa voi myös olla haittaohjelmia tai haavoittuvuuksia, jotka voivat lisätä riskejä. Vuonna 2010 Firefox-selaimeen oli saatavilla Firesheep-niminen haittaohjelma, jonka tarkoituksena oli kuunnella verkkoliikennettä sekä kaapata erilaisten sosiaalisen median palveluiden käyttämiä evästeitä, jotka mahdollistavat henkilötietojen varastamisen tai identiteettivarkaudet. (Sosiaalisen median tietoturvaohje 2010, 17.)

URL-lyhenteet tuovat huomattavia vaaroja, sillä linkin avaaja ei tiedä, mihin linkki oikeasti ohjautuu. Vasta avaamisen jälkeen mahdollisesti selviää todellinen osoite, mutta sekin on helposti estettävissä. Kuka tahansa voi ohjata minkä tahansa linkin esimerkiksi Bitlyn tai tinyurln kaltaisen palvelun kautta. Palvelun ideana on tehdä pitkistä ja hankalista linkeistä lyhyempiä ja siistimpiä. Palvelu oli aikoinaan suunniteltu Twitter-viesteille, joihin sai kirjoitettua vain 160 merk-

kiä. (Valtiovarainministeriö 2010, 17–18.) Oppaassa on kehotettu henkilökuntaa olemaan tarkkana lyhennettyjen osoitteiden kanssa.

Mikäli viestissä, sivustossa tai muussa palvelussa esiintyy huomattava määrä kirjoitus- ja kielioppivirheitä, on syytä olla epäileväinen. Monesti huijausviestit käännetään automaattikääntäjän avulla, mutta taitavimmat saattavat käyttää oikeita kääntäjiä apunaan. Suomen etuina on se, että suomen kieli on hankalaa automaattikääntäjille, ja se, että suomen kielen osaajien määrä on sen verran vähäinen, ettei huijareiden kannata tuhlata siihen resursseja. (Järvinen & Rousku 2017, 74.) Tämän lisäksi suomalaiset ovat isolta osalta koulutettuja ja osaavat varautua kriittisesti asioihin. Näistä huolimatta joka vuosi useat menevät silti huijareiden lankaan.

Verkkosivustoilla on käytössä monenlaisia huijauskeinoja. Vaikka sivusto olisi luotettava, saattaa siellä silti olla mainoksia, jotka ohjautuvat huijaussivustoille. Tämä joutuu siitä, että mainoksia tarjoavat kansainväliset palvelut, joilla voi olla vaikeuksia todeta kaikkien mainostensa luotettavuutta. (Järvinen & Rousku 2017, 75.) Suomen ulkoministeriöltä onnistuttiin huijaamaan 400 000 euroa kehitysapurahoja. Rahat oli onnistuttu haalimaan nimenomaan väärennettyjen sähköpostien avulla. Tässä tapauksessa isoa osaa rahoista ei onneksi ollut ehditty siirtää, jolloin ne saatiin palautettua. Voisi ajatella, että huijaukset tapahtuvat ainoastaan pienille ja tietämättömille toimijoille, mutta tässäkin tapauksessa kyseessä oli ministeriötasoinen taho, jolla on jo käytössä laajat tietoturvamenetelmät, ja huijaus onnistui silti. (Paajanen 2019.)

### 4.2.6 Viestittäminen

Yhteydenoton helppous ja ryhmäviestittely on tärkeässä roolissa tänä päivänä. Viestittämistä varten on tullut useita eri menetelmiä ja palveluita. Eduro on tutkinut asiaa ja päättänyt joissakin tilanteissa sallia WhatsApp-sovelluksen käytön. Palvelu luokitellaan Eduunin mukaan myös huonoimpaan C-luokkaan, sillä palvelu sijaitsee myös EU- ja Eta-alueen ulkopuolella ja edellyttää kontaktitietojen tallentamista. Lisäksi pidetään huolestuttavana sitä, että käyttöehtojen muutokset ilmoitetaan ainoastaan palveluntarjoajan internetsivustolla. (Tikkanen & Kommonen 2017.) WhatsApp-sovelluksen käyttäjäehtojen mukaan viestit tallen-

tuvat yrityksen palvelimelle vain silloin, kun viesti toimitetaan, ja viesti poistetaan palvelimelta heti sen toimituksen jälkeen. Säätiön toiminnassa WhatsAppista koetaan olevan suurta hyötyä etenkin nuorten asiakkaiden kanssa. Palvelu käyttää nykyään Open Whisper Systemsin kehittämää end-to-end-salausta, jota pidetään erittäin hyvänä (Burrell 2017). Viestittäminen on myös erittäin hyödyllistä asiakkaiden, yksilövalmentajien, työvalmentajien sekä sidosryhmien välillä. Täytyy kuitenkin muistaa, että palvelun kautta ei silti saa lähettää luottamuksellista tai henkilötietoja.

Sähköpostin lähettämistä voidaan verrata postikorttiin. Vaikka viesti lähetetään ja vastaanotetaan samasta maasta, voi viesti kulkea silti ulkomaan kautta. Edurossa on kiellettyä käyttää ulkopuolisia sähköpostipalveluita työkäytössä. Sähköpostiohjelmat tuovat myös omat haittansa. Tällainen voisi olla sähköpostiohjelman tietoturva-aukot tai epäluotettavat laajennukset. Haittaohjelmat ovat myös mahdollista asentaa sähköpostipalvelimeen, johon loppukäyttäjä ei voi suoranaisesti vaikuttaa. On tästä syystä suositeltavaa käyttää luotettavampia palveluntarjoajia, joilla on resursseja suojata järjestelmää. Nykyään onkin suositumpaa hoitaa järjestelmä SaaS-palveluna, eli palveluntuottaja tarjoaa koko infrastruktuurin, ja näin ollen ulkoistetaan riskit. Tämä on suotavaa etenkin pienemmässä organisaatiossa, jolla voi olla haasteita hoitaa tietoturvaa. (Hållfast 2016.)

Mikäli joudutaan lähettämään henkilötietoja tai muuta luottamuksellista tietoa, on Eduron henkilökunnan käytettävissä ulkopuolisen tarjoama Turvapostipalvelu. Vaihtoehtoisia ratkaisuja olisivat olleet esimerkiksi PGP-kryptatut viestit, jotka käyttävät end-to-end-tyylistä salausmenetelmää, mutta tämä olisi voinut osoittautua hankalaksi varsinkin heille, jotka eivät käytä kyseistä ohjelmaa, sillä se perustuu julkisiin ja yksityisiin avaimiin (Cobb 2015). Tällöin lähettäjän on saatava vastaanottajan avain, jotta viesti voidaan salata ja lähettää turvallisesti. Ainoastaan omalla henkilökohtaisella avaimella viestit saadaan auki. Mikäli yksityinen avain hukkuu tai unohtuu, viestejä on käytännössä mahdotonta saada auki.

On hyvä erottaa henkilökohtaisen ja työsähköpostin käyttö. Työsähköpostin käyttöoikeus loppuu siihen, kun työsuhde päättyy, jonka jälkeen niihin tietoihin

ei enää päästä käsiksi. Esimerkiksi jos avaa jonkin henkilökohtaisen palvelun yrityssähköpostiosoitteella ja unohtaa salasanan työnsuhteen päättymisen jälkeen, salasanan palauttaminen on mahdotonta.

Eduro-säätiö on ottanut viime vuoden puolella koekäyttöön Microsoft Teams -ryhmäkeskusteluohjelmiston. Tätä palvelua käytetään sisäiseen ryhmäviestittämiseen siten, ettei henkilötietoja lähetetä sen kautta. Järjestelmä on suunniteltu ideoimiseen ja toiminnan kehittämiseen.

### 4.2.7 Markkinointi

Tietosuoja-asetuksessa on mainittu, että henkilötietojen käsittely suoramarkkinoinnissa voidaan katsoa oikeutetun edun piiriin kuuluvaksi. Suoramarkkinointia voidaan lähettää henkilöille, mikäli heille kerrotaan mahdollisuudesta kieltää suoramarkkinointi. Rekisteröidyllä on oikeus kieltää henkilötietojensa käsittely suoramarkkinointia varten, mukaan lukien profilointi, mikäli se liittyy suoramarkkinointiin. Tämä oikeus ei koske julkisen sektorin toimintaa. On edellytettävä, että käytetään ”opt-in”-ominaisuutta, eli rekisteröidyn on aktiivisesti hyväksyttävä suostumus. Käytännössä tämä tarkoittaa sitä, että esimerkiksi sähköisissä järjestelmissä valintaruutu pitää hyväksyä itse, eli se ei saa olla automaattisesti valmiiksi hyväksytty (opt-out). (Hanninen ym. 2017, 35.)

### 4.2.8 Haittaohjelmat

Niissä palveluissa, missä käyttäjämäärät lisääntyvät, lisääntyvät myös kyseisten alustojen haittaohjelmat. Haittaohjelmat leviävät nopeasti ja houkuttelevat käyttäjiään asentamaan ohjelmia. Riskit kohdistuvat juuri salaisiin sivustoihin tai palveluihin, jossa ulkopuoliset palveluntarjoajat voivat lisätä alustaan omia sovelluksia tai koodinpätkiä. Etenkin sosiaalisissa medioissa haittaohjelmien lisääminen on vaarallisempaa, sillä haittaohjelmat voivat levitä kavereiden kautta, jolloin uhri kokee, että lähde on luotettava. Lisäksi sosiaalinen media kehittyy ja muuttuu nopeasti ja palveluntarjoajat haluavat olla alansa edelläkävijöitä tai ainakin kehityksessä mukana. Tämä kannustaa lisäämään uusia ominaisuuksia tai rajapintoja, jolloin ei ehditä huolehtimaan tarpeeksi tietoturvasta. Palveluntarjoajille syntyy paineita tuottaa käyttäjille tai rahoittajille uusia palveluita. (Sosiaalisen median tietoturvaohje 2010, 13.)

Erilaiset haittaohjelmat ovat iso riesa uhreilleen. Niitä on lukemattomasti, ja niiden määrä on jatkuvassa kasvussa. Haittaohjelman elinikä on yleensä vain muutamia tunteja, jolloin torjuntaohjelmat eivät pysy kehityksessä mukana. Yksi ikävimmistä haittaohjelmatyypeistä on kiristysohjelmat, jolloin haittaohjelma salaa taustalla tiedostot huomaamattomasti, jonka jälkeen omistajalle ilmestyy ilmoitus siitä, että tietyn ajan kuluessa pitää maksaa lunnaita tietyn summan verran, jotta saa purkuavaimen, jolla tiedostot saa takaisin auki. Yleensä maksamalla tiedostot saadaan palautettua, mutta tätä ei suositella, sillä se kannustaa kiristäjiä jatkamaan keinon käyttöä. Maksut tapahtuvat yleensä Bitcoinien avulla. Useat kiristysohjelmat leviävät erilaisten Office-tiedostojen välityksellä, makrotiedostoina, jolloin viruksentorjuntaohjelmilla on vaikeuksia havaita näitä haittaohjelmia. Nykyään Office-tiedostoista on helpompi tunnistaa, mikäli tiedosto sisältää makroja. Vanhan Officen versiot, kuten .doc, .xls. ja .ppt, saattavat sisältää makroja, mutta Office versio 2007 ja uudemmissa versioissa makrotiedostot näkyvät tiedoston päätteissä. Tiedostotyypit .docm, .xlsm ja .pptm sisältävät makroja, ja tiedostotyypit .docx, .xlsx ja .pptx eivät sisällä makroja. Windows-käyttöjärjestelmässä tämä voi olla hankalampaa tunnistaa, sillä tiedostomuodot piilotetaan. Tällöin makroja sisältävä ”asiakirja.docx.docm” näyttää käyttöjärjestelmässä turvalliselta ”asiakirja.docx”-tiedostolta. (Järvinen & Rousku 2017, 91–95.)

### 4.2.9 Sosiaalinen media

Sosiaalinen media eli some on usein keskeisessä roolissa organisaation ulkopuolisessa viestinnässä ja markkinoinnissa. Tästä huolimatta harva organisaatio on kuitenkaan laatinut ohjeistuksia somen käyttöä varten, jolloin somepäivitykset ja postauksien sisältö jää usein henkilöiden omaan harkintaan, ja tämä voi aiheuttaa riskejä. Sosiaalisen median käyttöä ei kuitenkaan kannata lähteä rajoittamaan, vaan päinvastoin siitä kannattaa pyrkiä ottamaan kaikki irti. On kuitenkin hyvä miettiä etukäteen, mitä ja mistä aiheista voidaan julkaista päivityksiä. (Andreasson & Koivisto 2013, 151.) Vaikka harvemmin suoraan henkilötietoja, kuten nimiä, julkaistaan esimerkiksi Facebook-päivityksessä, voi valokuvan julkaiseminen olla konkreettinen tapaus henkilön tietosuojan loukkaamisesta. Täytyy myös muistaa, että vaikka organisaation julkaisut sosiaalisessa mediassa tehdään henkilökohtaisella profiililla tai yrityksen profiiliin linkitetyllä

omalla profiililla, tulkitaan päivitykset useimmiten yrityksen virallisiksi kannoiksi. Ja vaikka henkilökohtainen profiili olisi nähtävillä vain rajoitetulle määrälle ihmisiä, määrä voi kuitenkin olla huomattava, joten tehtyä julkaisua voi verrata kaikille nähtävillä olevaan julkiseen päivitykseen. On myös ymmärrettävä sosiaalisen median käyttöehdot, jotka voivat vaihdella riippuen palvelualustasta. On tiedettävä, kuka esimerkiksi omistaa julkaisun sisällön julkaisemisen jälkeen. Vertaillessa on yllättävää, että sosiaalinen media on suurempi uhka kuin sähköposti, sillä erilaiset pelit, visat ja linkit houkuttelevat todennäköisemmin klikkaamaan huolettomammin linkit auki kuin sähköpostiin saapuvia linkkejä. Sähköpostin uhista on ollut paljon keskustelua, mutta koska sosiaalinen media on vielä sen verran tuore yritysten viestinnän välineenä, sen aiheuttamat uhat eivät ole niin selkeästi nähtävillä. Sosiaalisen median palvelut pyrkivät poistamaan näitä uhkia, mutta ennen kuin näin tapahtuu, haitta voi olla jo tehty. Tämän lisäksi somen eri palvelut ovat erittäin suosittuja, joten myös niihin kohdistuvien uhkaajien määrä on laaja. Sosiaalisen median palveluita on paljon ja uusia ilmestyy jatkuvasti ja olemassa olevatkin voivat muuttua. Lisäksi jokaisella palvelulla on erilaiset tietoturvakäytännöt. Tämän vuoksi tietoturvan hallinta on haasteellista. (Andreasson & Koivisto 2013, 153–154.) Sosiaalinen media on kehittynyt huomattavasti lähiaikoina, mutta tätä myötä verkkorikolliset ovat keksineet luovia ideoita hyödyntää tietoturvan puutteita (Irshad & Soomro 2018, 43).

Henkilökohtaisella sometilillä, joka on yhdistetty organisaation tiliin, on pidettävä erityisen hyvää huolta salasanojen valinnasta ja tilin käytöstä. Vaikka kyseessä on henkilökohtainen tili, toimii se kuitenkin porttina organisaation tiliin, joten on käyttäjästä kiinni, kuinka vahva portti on kyseessä. Tällainen esimerkki voi olla, kun henkilökohtainen sometili jää auki toiseen laitteeseen tai jos salasana on käytössä myös sellaisessa paikassa, jossa on tapahtunut tietomurto, jonka vuoksi ulkopuoliset voivat päästä käsiksi organisaation sometiliin. Henkilökohtaiselle profiilille voi myös hyvin helposti julkaista tahattomasti postauksia yrityksen nimissä.

Tietoturvauhat voivat aiheutua henkilön omasta toimesta tai ammattimaisesta toiminnasta kuten rikolliset, ääriryhmät taikka valtiot, jossa pyritään saamaan henkilötietoja tai muita salassa pidettäviä tietoa haltuunsa, muuttamaan tietoa tai tekemään muuta haittaa haitatakseen organisaation toimintaa (Sosiaalisen

median tietoturvaohje 2010, 13). Edurolla ei ole käytössä erillistä sosiaalisen median käytön ohjeistusta, joten opasta varten täytyi laatia selkeät linjaukset ja tuli pohtia, kenen vastuulla sosiaalinen media on ja kuka tai ketkä luovat siihen sisältöä ja millä tavalla.

Sosiaalisen median identiteettivarkaudet ovat yleistymässä. Identiteettivarkaus voi käytännöissä tarkoittaa sitä, että luodaan profiili toisten henkilön nimiin. Tämä on hyvin helppoa toteuttaa, ja väärennetty profiili voi olla mahdoton tunnistaa oikeasta. Väärennetyllä profiililla voidaan jakaa esimerkiksi väärää tietoa ja tehdä tahallisesti haittaa organisaation maineelle. Kiinni jäämisen riski voi olla myös hyvin alhainen, varsinkin jos profiilin luoja on käyttänyt VPN-yhteyttä, julkista tietokonetta tai prepaid-liittymää, jolloin ei tiedetä, kuka on todellisuudessa IP-osoitteen takana.

### 4.2.10 Puhelimen käyttö

Puhelin on suojattava puhelimen PIN-koodilla ja suojakoodilla tai vaihtoehtoisesti sormenjälkitunnistautumisella. Puhelin- tai PIN-koodit 1234, 0000 tai muut vastaavat ovat yleensä operaattoreiden tai puhelimien oletuskoodeja, joten nämä koodit on vaihdettava. Myöskään syntymävuotta ei saa käyttää. PIN-koodi tai sormenjäljen tunnistin ovat turvallisempia vaihtoehtoja verrattuna kuvioon perustuvaan koodiin, sillä urkkija voi nähdä ja muistaa kuviokoodin paremmin.

Arkaluontoisten ja luottamuksellisten asiakastietojen käsittely puhelimessa on kielletty. Myöskään luottamuksellisia tietoja ei saa tallentaa puhelimeen. Tulee myös muistaa, että bluetooth-yhteys pitää olla poiskytketty silloin, kun sitä ei tarvita. (Järvinen & Rousku 2017, 69.) Salasanoja, luottamuksellisia tekstiviestejä tai muita luottamuksellisia tietoja tai tiedostoja ei tule säilyttää puhelimessa. Puhelimen asetukset tulee laittaa niin, että viimeistään viiden minuutin käyttämättömyyden jälkeen se lukkiutuu automaattisesti.

Luovuttaessa puhelimen tai SIM-kortin pois käytöstä on hyvä huolehtia siitä, että puhelimen ja SIM-kortin muistit tyhjennetään ja puhelin palautetaan tehdasasetuksiin. Myös mahdolliselta muistikortilta tulee poistaa tiedot. IT-osasto varmistaa, että puhelimeen tai SIM-korttiin ei jää mitään tietoja, ja tarvittaessa kirjoittaa muistikortin päälle, jotta mitään tiedostoja ei voi saada enää palautet-

tua. Tämä toimenpide on tarpeellinen vain silloin, jos muistikortti ei ole ollut salattu ja jos muistikortti ei jää yrityksen sisäiseen käyttöön. Henkilöstö voi tarvittaessa saada lisätietoa puhelimen käytöstä Eduron sisäisestä toiminnanohjaus- ja dokumenttienhallintajärjestelmästä.

Puhelimeen kannattaa ladata mahdollisimman vähän sovelluksia, ja niistä sovelluksista, joita asennetaan, pitää tarkastaa, mitä oikeuksia sovelluksella on. Esimerkiksi jotkut sovellukset saattavat lukea käyttäjien osoitekirjaa ja lähettää tiedot eteenpäin. Puhelimen omat päivitykset on suositeltava asentaa mahdollisimman pian, jotta puhelin ja sovellukset ovat ajan tasalla. (Järvinen & Rousku 2017, 124.)

### 4.2.11 Ulkoisen muistin käyttö

Ulkoisten USB-tikkujen tai laitteiden käyttö on monesti helppoa ja käytännöllistä, mutta näiden välineiden käyttöön liittyy aina yllättävän monenlaisia riskejä. Pienet USB-tikut on helppo unohtaa johonkin, ja USB-tallennuslaitteiden kautta koneelle voidaan ujuttaa erilaisia haittaohjelmia. USB-tikkuihin voidaan laittaa automaattisesti käynnistyvä ohjelma, tai ovelammissa tapauksissa haittaohjelma on ujutettu suoraan USB-tikun sisäiseen elektroniikkaan. Tällöin torjuntaohjelmat eivät havaitse sovellusta tai koodinpätkää. (Järvinen & Rousku 2017, 106–107.) Vaikka tiedostot poistettaisiin tallennusmediasta ja se alustettaisiin, on tiedostojen palauttaminen siitä huolimatta erittäin helppoa. Oppaassa ohjeistetaan välttämään vieraiden USB-laitteiden käyttöä ja kielletään henkilötietojen ja salassa pidettävien tietojen tallentaminen näihin tallennusmedioihin. On myös olemassa näppäimistöjen tallennusohjelmia ja laitteita, joita tavallisen käyttäjän on hyvin vaikea huomata. Ohjelmallisella kaappaajalla voidaan tallentaa kaikki, mitä näytössä tapahtuu tai kaikki mitä näppäimistöllä kirjoitetaan. Näppäimistön tallennuskaappaajalaite asennetaan näppäimistön ja tietokoneen väliin, ja se tallentaa kaiken, mitä näppäimistöllä kirjoitetaan. Tiedot tallentuvat laitteen omaan muistiin. Laite on pieni ja huomaamaton, helposti saatavissa sekä hyvin edullinen. Tämä toimii ainoastaan koneissa, joissa on erillinen näppäimistö. (Järvinen & Rousku 2017, 113.) Eduro-säätiön riskien hallinnassa ulkoisiin tallennuslaitteisiin liittyvien riskien todennäköisyys ja riskin seuraamus ovat asteikolla yhdestä viiteen molemmat luokkaa kolme (Eduro-säätiö 2018c).

### 4.2.12 Tulostimen käyttö

Monessa organisaatiossa tulostetaan edelleen mittavia määriä tulosteita, ja niissä voi hyvinkin olla salassa pidettäviä materiaaleja tai henkilötietoja. Kopiokoneisiin liittyviä riskejä saatetaan helposti vähätellä tai pitää mitättöminä, mutta riskit ovat suurempia kuin mitä voisi kuvitella. Tällä hetkellä Eduro-säätiöllä ei ole käytössä turvatulostin-ominaisuutta, joten kun asiakirja laitetaan tulostumaan, kopiokone tulostaa sen välittömästi. Pahimmassa tapauksessa tulostin sijaitsee rakennuksen toisessa päässä ja tulostuksien hakemiseen kuluva aika on huomattava. Tänä aikana on hyvinkin helppo vilkaista tulostettuja papereita tai jopa viedä ne mukanaan, jolloin tulostaja saattaa luulla, ettei tulostus onnistunutkaan. Lisäksi Eduron kopiokone on tällä hetkellä sijoitettu vessoja vastapäätä, jolloin siihen jää henkilöitä odottelemaan omaa vuoroaan. Toinen riskitilanne on se, että useampi henkilö tulostaa yhtä aikaa, jolloin toinen henkilö ottaa vahingossa toisenkin henkilön tiedostot mukaansa tai lukee niitä vahingossa. Joissakin tapauksissa tällaisia tilanteita välttääkseen voidaan myös tulostaa omalle paikalliselle tulostimelle tai harkita sellaisen hankkimista, vaikka kustannukset olisivat suuremmat. (Järvinen & Rousku 2017, 51.) Tällaisten riskien välttämistä käsitellään oppaan luvussa ”kopiokoneen käyttö.”

### 4.2.13 Verkkolaskut ja kirjeposti

Yrityksille lähetetään monesti valelaskuja, jotka näyttävät oikeilta laskuilta, mutta todellisuudessa kyseessä on esimerkiksi tarjous, joka lukee pienellä präntillä. Tarkoituksena on hämmentää laskun saajaa ja pakottaa heitä maksamaan lasku. Tämä on yleistä varsinkin kesällä, sillä lasku saattaa kohdistua sellaiselle henkilölle, joka on juuri silloin lomalla, ja lasku saatetaan hyväksyä helpommin tai laskua käsittelee sijainen. Fyysiset kirjeet kulkevat useampien tahojen kautta ja ovat helposti muokattavissa, sillä avaamattoman näköinen kirje ei takaa sitä, että sisältö olisi autenttinen. Esimerkiksi on helppo tulostaa tavalliseen kirjekuoreen mikä tahansa logo tai teksti, eikä kirjeen saaja huomaa sitä. Verkkolaskut poistavat tämän ongelman. (Järvinen & Rousku 2017, 82.)

## 4.3 Tietoturvakoulutus

Tietoturvakoulutus on painotettu EU:n yleiseen tietosuoja-asetukseen, sillä tämä aihe oli monelle työntekijöille hyvinkin vieras ja vaikeasti sisäistettävä asia. Lisäksi säädös on tuonut monia muutoksia säätiön toimintaan. Tavoitteenani oli se, ettei koulutuksesta tulisi liian raskaat kalvosulkeiset, jossa asetus käsitellään läpikotaisin, vaan tarkoituksena oli antaa tarvittavaa tietoa vastuulliseen ja lailliseen tietojen käsittelyyn. Koulutuksen tukena toimi esitysgrafiikka, joka helpottaa ja tukee asian sisäistämistä.

Ennen koulutuksen suunnittelua oli tärkeää kartoittaa säätiön nykyiset toimintatavat sekä ohjeistukset. Eduro-säätiössä toimii hallinto ja hallinnon alaisuudessa toimivat työntekijät, apu- sekä työvalmentajat, yksilö- sekä ryhmävalmentajat sekä oppisopimuslaiset. Tämän takia minun täytyi selvittää, mitä tietoturvariskejä liittyy kunkin työntekijän työnkuvaan. Suunnittelun alustana toimi miellekartta, johon kirjasin mahdollisia riskejä, mitä eteen voisi sattua ja joita varten työntekijöiden olisi hyvä saada käyttöönsä toimivat toimintatavat. Koulutuksen suunnitteluvaiheessa olin tiivisti tekemisissä säätiön digikoordinaattorin kanssa, joka vastaa säätiön tietoturvasta.

Suunnittelin tietoturvakoulutuksen, joka on tarkoitus järjestää säännöllisesti koko henkilökunnalle. Tämä koetaan tärkeäksi työtehtävien vuoksi, sillä lähes kaikki säätiön työntekijät käsittelevät henkilötietoja. Suunnitellun koulutuksen kesto on puoli tuntia. Puolessa tunnissa asia pystytään käymään tehokkaasti läpi ja pystytään keskittymään nimenomaisesti olennaiseen tietoon. Tietoa pystytään omaksumaan paremmin useassa pienessä erässä kuin yhdessä suuressa. Pääosin henkilökunta on jaettu noin 20 hengen tiimeihin, joten tämän vuoksi myös koulutus pidetään tiimien jaon mukaisesti tiimipalavereiden yhteydessä. Tämä helpottaa myös koulutuksen säännöllistä järjestämistä, sillä myös palavereita järjestetään tasaisin väliajoin.

Koulutuksessa on otettu huomioon myös kohderyhmä. Koulutettavista noin 70 % ovat naispuolisia, ja ikäjakauma ulottuu noin 28-vuotiaista jopa lähelle eläkeikää. Koko henkilöstön keski-ikä on noin 47 vuotta. (Eduro-säätiö 2017.) Ikäjakauma toi haastetta koulutuksen suunnitteluun, sillä sen tuli olla kaikkien sisäis-

tettävissä. Jokainen ihminen on erilainen, ja jokaisella on oma yksilöitynyt tapansa oppia ja sisäistää asioita. Nuorempien on helpompi ottaa käyttöön uusia työskentelytapoja ja he ovat kasvaneet digitalisaation mukana, joten heille asiat saattavat olla tutumpia. Kokemuksen myötä ihmisille muodostuu pysyviä tapoja toimia ja ajatella, joten onkin tärkeää, että uuden oppimisen lisäksi pystytään opettelemaan ulos tietyistä, huonoista tavoista. Tämä on mahdollista, sillä oppiminen ei lopu koskaan ja uutta tietotaitoa pystytään kartuttamaan vanhan pohjan päälle, kunhan uusi asia on vain pystytty kytkemään käytäntöön. Näin pystytään ohjailemaan sitä, miten oppija tulkitsee tietoa, ja hän pystyy saamaan hyvän syyn omaksua uutta tietoa. (Tietoturvakouluttajan opas 2006, 13.)

Gender, Risk and Security -tutkimuksen mukaan miehet tiedostavat riskit naisia paremmin, mutta naispuoliset ovat yleisellä tasolla varovaisempia ja huolellisempia tietoturvan suhteen. Lisäksi raportin mukaan miehet voivat olla välinpitämättömämpiä tietoturvan asiallisen hoitamisen kanssa ja saattavat ottaa turhia riskejä. (Roger & Petric 2017, 15–19.) Tämä tulee ottaa huomioon koulutuksessa.

Ryhmän koko voi myös vaikuttaa koulutukseen. Valtionvarainministeriön Tietoturvakouluttajan oppaassa (2006 kerrotaan, kuinka ryhmäkoko voi vaikuttaa merkittävästi muun muassa siihen, minkälaiset opetustavat ovat toimivimpia. Mitä isompi koko, sitä rajatummat menetelmätavat on käytettävissä. Taulukosta 4 näkyy, kuinka ryhmäkoko vaikuttaa myös oppijoiden aktiivisuuteen koulutustilanteessa. Pienessä ryhmässä on helpompi tuoda omia ajatuksia esille, mutta mitä suurempi ryhmä on kyseessä, sitä harvempi uskaltautuu käyttämään ääntään. (Tietoturvakouluttajan opas 2006, 28.)

Taulukko 4. Ryhmäkoon vaikutus läsnäolijoiden aktiivisuuteen ja käytettäviin menetelmiin (mukaillen Valtionvarainministeriö 2006, 29)

| Ryhmäkoko | Aktiivisuus | Soveltuva menetelmä |
|---|---|---|
| 3-6 | Kaikki puhuvat | Vuoropuheinen opetus<br>Ryhmätyö kaikissa muodoissaan<br>Demonstraatio<br>Harjoitus |
| 7-10 | Lähes kaikki puhuvat<br>Hiljaisemmat äänessä vähemmän<br>Yksi tai kaksi ei puhu lainkaan | |
| 11-18 | Viisi tai kuusi henkilöä puhuu paljon<br>Muista kolme tai neljä liittyy mukaan silloin tällöin | Luento<br>Kyselevä opetus<br>Vuoropuheinen opetus<br>Ryhmätyö kaikissa muodoissaan<br>Demonstraatio<br>Harjoitus |
| 19-30 | Kolme tai neljä ryhmää dominoivaa jäsentä | |
| Yli 30 | Pieni osallistumismahdollisuus | Luento<br>Paneelikeskustelu |

Koulutus on suunniteltu jo olemassa olevien tiimien myötä noin 20 hengen kokonaisuuksille. Tiimien tuttu kokoonpano voi kuitenkin helpottaa koulutuksen toteuttamista. Tuntemattomien henkilöiden kokoonpanossa taulukon mukaiset aktiivisuudet voivat korostua herkemmin kuin tutuista ihmisistä koostuvassa tiimissä. Tietoturvallisuus kuuluu omaan osaamisalueeseensa, ja sitä ei voi opetella kerralla täydelliseksi. Jatkuvalla oppimisella varmistetaan se, että asiantuntemus pysyy ajankohtaisella tasolla, jolloin myös tietoturvaa pystytään kehittämään paremmaksi. (Tietoturvakouluttajan opas 2006, 18.) Taulukko 5 kuvaa organisaation eri työrooleja tietoturvan kannalta. Taulukossa näkyy IT-puolen, hallinnon ja johdon sekä kaikkien työntekijöiden osa-alueet.

Taulukko 5. Tietoturvan työroolit organisaation eri tasoissa

| Kaikki | Johto | IT |
|---|---|---|
| Tietoturvatoiminnan tavoitteet | Tietoturvallisuuden hallintajärjestelmä | Tekninen tietoturvallisuus |
| Tietoturvatoiminnan organisointi, vastuut ja tehtäväjako | Tietoturvapolitiikka ohjauskeinona | Tietoturvatuotteet |
| Noudatettava ohjeisto ja sen sijainti | Suojattavien kohteiden määrittely | Erikoistumisalueen mukainen lisäkoulutus |
| Peruskäsitteet | Riskien arviointi ja hallinta | Toipumissuunnittelu |
| Viranomaisen toiminnan julkisuus ja salassapitovelvoitteet | Henkilöstöturvallisuus | Lokien seuranta ja hallinta |
| Asianhallinnan turvallisuus | Työturvallisuus ja työsuojelu | Tekninen valvonta ja auditointi |
| Asiakirjojen luokittelu ja käsittely | Tiedottaminen | |
| Henkilötietojen käsittely | Hankinnat ja tietoturvallisuus | |
| Tietokoneen käyttö | Palvelujen valvonta | |
| Internetin ja sähköpostin käyttö | (Liike)toiminnan jatkuvuussuunnittelu | |
| Toimitilaturvallisuuden perusteet | Resurssien hallinta | |
| Vierailijakäytäntö | Arviointien ja auditointien hyödyntäminen | |
| Etätyö ja etäkäyttö | Mittarit ja jatkuva parantaminen | |
| Matkatyö ja mobiililaitteiden käyttö | Johdon katselmus | |
| Aloitetoiminta | | |
| Toiminta ongelmatilanteissa ja ilmoitusvelvollisuus | | |
| Seuraamukset | | |

## 4.4 Koulutuksen onnistumisen arviointi

Koulutusta tulee arvioida, jotta selviäisi, oliko siitä hyötyä ja mitä toimia vastaisuudessa tulee tehdä. Arvioinnissa käytettävien mittareiden kanssa tulee olla tarkkana, sillä niiden tulee mitata haluttua arvioitavaa kohdetta. Se ei myöskään ole yksiselitteistä, vaan arviointi voi jakautua eri osa-alueille. On hyvä tehdä erilaisia mittauksia, esimerkiksi millaiset tavoitteet koulutuksen onnistumiselle alussa asetettiin ja kuinka hyvin ne loppujen lopuksi saavutettiin. Myöhemmin tulee arvioida, miten opetus on mennyt perille ja kuinka paljon koulutuksesta on omaksuttu omiin työskentelytapoihin.

Paras keino nähdä koulutuksen onnistuminen onkin tarkastella, kuinka koulutuksessa läpikäydyt asiat tulevat esille tavallisessa työympäristössä. Työyhteisössä kannattaa myös tilastoida mahdolliset tietoturvavahingot ja niiden selvitykset, jotta myöhemmin voidaan tarkastella, ovatko toimet olleet oikeita vai onko aihetta lisäkoulutuksille. Parhaimmassa tapauksessa tietoturvaongelmia saadaan vähenemään ja virheiden määrä pienenee.

Heti koulutuksen jälkeen voidaan myös kerätä palautetta kaikilta koulutukseen osallistuneilta. Palautelomakkeella kerättävä arviointi kertoo suoraan sen, miten osallistujat suhtautuivat koulutukseen ja miten he kokivat koulutuksen onnistumisen. Lomakkeen avulla he voivat myös kertoa, jos heillä ilmeni parannusehdotuksia seuraavaa koulutusta varten.

# 5 POHDINTA

Tämän opinnäytetyön perimmäisenä tarkoituksena oli saada Eduro-säätiön henkilökunta tunnistamaan tietoturvariskit sekä toimimaan mahdollisimman tietoturvallisesti. Huomasin, että teknisesti paras ratkaisu ei ole aina paras ratkaisu toiminnan kannalta. Koin, että tietoturva on kuin vaaka, jossa yhdellä puolella on erittäin hyvää tietoturvaa ja toisella puolella toimivuutta. Mitä tietoturvallisempaa on, sitä vaikeammaksi asiat monesti muuttuvat. Liian tiukka tietoturva aiheuttaa toiminnassa jäykkyyttä ja siten aiheuttaa tehottomuutta toimintaan. Lisäksi liian jäykät tietoturvatoimet, jotka haittaavat työntekoa, voivat toimia myös tietoturvariskinä itsessään. Kaikki eivät välttämättä noudata ohjeistuksia jäykkyyden vuoksi, jolloin toimitaan omin päin. Onkin tärkeä löytää tietoturvalle tasapaino kouluttamalla ja tiedottamalla henkilökuntaa, mutta myös kuuntelemalla heitä, jolloin tietoturvan haasteet tulevat esiin.

Kun aloitin opinnäytetyön prosessin, tarkoituksenani oli pitää pelkästään koulutustilaisuus. Huomasin kuitenkin pian, että olisi tarpeellista tehdä lisäksi kirjallinen käytännön opas, jotta henkilökunnalla olisi aina käytettävissään selkeät ohjenuorat käytännön tietoturvan toteuttamista varten. Kaikki tarvittava tieto löytyisi yhdestä paikasta ja nopeasti. Oppaan ja koulutuksen suunnittelussa tuli huomioida henkilökunnan jo olemassa olevat tiedot ja osaaminen. Näitä ominaisuuksia kartoittaakseni tein kyselyn, jonka avulla pystyin hahmottamaan tämän hetkisen tilanteen. Tutkiessani vastauksia huomasin, että henkilökunnan tarpeet vaihtelivat hyvin paljon ja oli tärkeää, että heikoimpien osaamisen taidot ovat riittävällä tasolla ja että heidät saadaan sitoutumaan toimimaan tietoturvallisesti. Päätin, ettei liian yksinkertaisia asioita ole, eikä saa olettaa, että kaikki tietävät näitä asioita. Näistä yksinkertaisista asioista syntyy suurempia riskejä. Sanotaan, että organisaation tietoturva on yhtä vahva kuin sen heikoin lenkki. Hyvä tietosuojaosaaminen on sekä säätiön etu, henkilötietojen käsittelijän etu, mutta nimenomaan myös rekisteröidyn henkilön etu.

Opasta tehdessä säätiön omat toimintatavat ehtivät muuttua, joka vahvisti päätöstä tehdä helposti muokattava opas. Oppaan selkeys oli myös alusta asti vahvasti mukana. Opinnäytetyön koulutuksen suunnittelin teknisessä mielessä, mutta nopeasti huomasin, että jokainen henkilö sisäistää tietoa eri tavoin. Aina

ei riitä, että ihmisille annetaan vain teknisiä ratkaisuja, joita heidän tulee noudattaa. Koulutuksen kuuluu myös innostaa, jolloin tieto välittyy paremmin. Jotta koulutus olisi mahdollisimman toimiva, niin suunnittelussa on hyvä ottaa huomioon erilaisia koulutusmenetelmiä sekä koulutuksen sisältö ja kohderyhmä.

EU-tietosuoja-asetukseen perehtyessä tuli eteen paljon kysymyksiä, sillä ensimmäisenä asiana oli asetuksen kielen kankeus ja tietynlainen ympäripyöreys. Toisena asiana oli lain tuoreus, jonka vuoksi opinnäytetyötä aloittaessa ei ollut vielä syntynyt ennakkotapauksia, mutta työtä tehdessä niitä alkoi hiljalleen tulemaan. Kolmantena asiana oli EU-asetusten tarkennukset, jotka olivat toistaiseksi osittain vielä tekemättä.

Kun päätin tutkia erilaisia lakeja, jotka vaikuttavat henkilötietojen käsittelyyn, huomasin asian olevan kuin Pandoran lipas, eli työn määrä olisi moninkertaistunut. Esimerkkinä Laki yksityisyyden suojasta työelämässä (759/2004), joka määrittelee, mitä tietoja työnantaja saa kerätä työntekijöistä. Tällöin päätin rajata muut asiaa koskevat lait pois. Lisäksi rajasin pois tiettyjä henkilökunnan erikoisryhmiä, joilla on omat ohjeistukset, jotta koulutus ja opas olisivat koko henkilökunnan käytettävissä.

Vaikka oppaassa ja koulutuksessa pyrin olemaan menemättä kovin syvälle teoriaosuuteen koulutettavan kohderyhmän ja sisällön ymmärrettävyyden takia, niin tutkiessani aihetta opin paljon ja itsellenikin syntyi uusia toimintatapoja. Huomasin myös sen, että vaikka asiat olisivat kuinka yksinkertaisia ja helppoja, kaikki eivät silti tiedä niitä. Uskon, että aihe on ja tulee olemaan relevantti vielä pitkään, sillä tietojenkäsittelyn merkitys on jatkuvassa nousussa myöskin tulevaisuudessa. Etenkin tietojen automaattinen käsittely on vasta alkutekijöissään. Täytyy myös muistaa, että jo yksikin tietoturvaloukkaus on liikaa.

LÄHTEET

Agendium 2018. Tietosuojamalli: WP29-kooste: Läpinäkyvyys. Viitattu 4.5.2019 https://fakta.tietosuojamalli.fi/artikkelit/wp29-kooste-lapinakyvyys.

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2016. Tietosuojakäsikirja johdolle. 3. painos. Helsinki: Tietosanoma.

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2017. Osaava tietosuojavastaava. Helsinki: Tietosanoma.

Burrell, H. 2017. How secure is WhatsApp? WhatsApp security and encryption explained. Tech Advisor. Viitattu 18.10.2018 https://www.techadvisor.co.uk/feature/internet/how-secure-is-whatsapp-whatsapp-security-encryption-explained-3637780/.

Cobb, M. 2015. How does OpenPGP encryption improve messaging security?. TechTarget. Viitattu 18.10.2018 https://searchsecurity.techtarget.com/answer/How-does-OpenPGP-encryption-improve-messaging-security.

Eduro-säätiö 2017. Tasa-arvo- ja yhdenvertaisuussuunnitelma. Viitattu 9.12.2018. Eduron sisäiset asiakirjat.

– 2018a. Henkilökunnan salassapitositoumus. Viitattu 9.12.2018. Eduron sisäiset asiakirjat.

– 2018b. Henkilötietojen tietoturvaloukkauksia koskeva ilmoitus. Viitattu 5.5.2019. Eduron sisäiset asiakirjat.

– 2018c. Riskianalyysi. Viitattu 9.12.2018. Eduron sisäiset asiakirjat.

– 2018d. Tietoturvapoikkeamaraportti. Viitattu 5.5.2019. Eduron sisäiset asiakirjat.

– 2018e. Työasemien ja mobiililaitteiden käyttö. Viitattu 9.12.2018. Eduron sisäiset asiakirjat.

– 2019. Työelämän tiennäyttäjä. Viitattu 20.5.2019 https://www.eduro.fi/.

Euroopan komissio 2018. Mitkä tiedot ovat henkilötietoja?. Viitattu 20.11.2018 https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_fi.

Euroopan parlamentin ja neuvoston asetus 2016/679.

European Data Protection Board 2019. First fine imposed by the President of the Personal Data Protection Office. Viitattu 4.5.2019

https://edpb.europa.eu/news/national-news/2019/first-fine-imposed-president-personal-data-protection-office_fi.

EU-tietosuojan kokonaisuudistus 2016. Helsinki: Valtiovarainministeriö. Viitattu 10.4.2018 Valtionhallinnon tietoturvallisuuden johtoryhmä.

Grassi, P., Fenton, J. & Newton, E. 2017. Digital Identity Guidelines. Authentication and Lifecycle Management. National Institute of Standards and Technology Special Publication 800-63B. Viitattu 17.10.2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely. Vantaa: Helsingin Kamari Oy.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 1997. Tutki ja kirjoita. 3. painos. Helsinki: Kirjayhtymä.

Hållfast, M. 2016. Kyberturvallinen pilvi - Uhka vai mahdollisuus? Viitattu 10.2.2019 https://www.cgi.fi/fi/blogi/kyberturvallinen-pilvi-uhka-vai-mahdollisuus.

International Chamber of Commerce 2016. Tietoturvaopas yrityksille: ICC Cyber security guide for business. Viitattu 18.10.2018 https://kauppakamari.fi/wp-content/uploads/2016/11/tietoturvaopas-yrityksille.pdf.

Irshad, S. & Soomro, T. R. 2018. Identity Theft and Social Media.

International Journal of Computer Science and Network Security 1.1.2018. Viitattu 5.11.2018 http://paper.ijcsns.org/07_book/201801/20180106.pdf.

Jordan, E. & Silcock, L. 2006. Strateginen IT-riskien Hallinta. Helsinki: Edita.

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas. Helsinki: Alma Talent.

Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Faith Cranor, L. & Egelman, S. 2011. Of Passwords and People: Measuring the Effect of Password-Composition Policies. Pittsburgh: Carnegie Mellon University. Viitattu 17.10.2018 https://www.archive.ece.cmu.edu/~lbauer/papers/2011/chi2011-passwords.pdf¨.

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

Krutz, R. & Vines, R. 2003. Tietoturva sertifikaatti. Helsinki: IT-Press.

Laakso, M. 2018. Tietojesi turvaksi. Viitattu 20.11.2018 https://tietojesiturvaksi.fi/tietoturvasuunnitelma/hallinnollinen-tietoturva.

LaCroix, K. 2018. Guest Post: What Can the First GDPR Fines Tell Us? The D&O Diary. Viitattu 6.2.2019.

https://www.dandodiary.com/2018/12/articles/regulatory-enforcement-2/guest-post-can-first-gdpr-fines-tell-us/.

Lahtinen, M. 2017. 10 kysymystä tietosuoja-asetuksesta. Kauppakamari. Helsingin seudun kauppakamari. Viitattu 6.2.2019 https://www.kauppakamarilehti.fi/index.php/neuvontapalvelut/10-kysymysta-tietosuoja-asetuksesta/.

Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista 22.9.2000/812.

Laki yksityisyyden suojasta työelämässä 759/2004.

Lyly-Yrjänäinen, M. 2018. Työolobarometri 2017 Ennakkotiedot. Työ- ja elinkeinoministeriön julkaisuja 2018:3.

Paajanen, O. 2019 Ulkoministeriö maksoi noin 400 000 euroa kehitysapurahoja väärälle tilille – poliisi epäilee, että ministeriötä huijattiin sähköposteilla. Aamulehti 24.1.2019. Viitattu 5.5.2019 https://www.aamulehti.fi/a/201422115.

Roger, K. & Petric, G. 2017. Gender, Risk and Security. Yhdysvallat: CLTRe. E-kirja.

Ruohonen, M. 2002. Tietoturva. Docendo: Jyväskylä.

Shankdhar, P. 2018. Popular Tools for Brute-force Attacks. InfoSec Institute. Viitattu 8.11.2018 https://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref.

Sosiaalisen median tietoturvaohje 2010. Helsinki: Valtiovarainministeriö. Viitattu 10.4.2018 Valtionhallinnon tietoturvallisuuden johtoryhmä.

TechTarget: SearchSecurity 2010. Viitattu 18.10.2018 https://searchsecurity.techtarget.com/USB-thumb-drive-security-best-practices-spelled-out-by-NIST.

Tietosuojalaki 1050/2018.

Tietosuojavaltuutetun toimisto 2018a. Tietosuoja turvaa oikeutesi henkilötietoja käsiteltäessä. Viitattu 6.2.2018 https://tietosuoja.fi/tietosuoja.

– 2018b. Tietosuoja on menestystekijä. Viitattu 10.4.2018 https://tietosuoja.fi/tietosuojavaltuutetun-toimisto.

Tietoturvakouluttajan opas 2006. Helsinki: Valtiovarainministeriö. Viitattu 10.4.2018 Valtionhallinnon tietoturvallisuuden johtoryhmä.

Tikkanen, M. & Kommonen, M. 2017. Eduuni Wiki. Microsoft OneDrive. Viitattu 18.10.2018 https://wiki.eduuni.fi/display/pilviohje/Microsoft+OneDrive#space-menu-link-content.

Tikkinen-Piri, C., Rohunen, A. & Markkula, J. 2017. EU General Data Protection Regulation: Changes and implications for personal data collecting companies.

Computer Law & Security Review: The International Journal of Technology Law and Practice.

Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008. Helsinki: Valtiovarainministeriö. Viitattu 10.4.2018 Valtionhallinnon tietoturvallisuuden johtoryhmä.

LIITTEET

# Henkilökunnan kysely

## Mitä seuraavista järjestelmistä käytän Eduro-säätiön tilojen ulkopuolella?

| | Tavalliset oikeudet | Laajennetut oikeudet |
|---|---|---|
| ARVI | ○ | ○ |
| ARVI2 | ○ | ○ |
| IMS | ○ | ○ |
| C&Q | ○ | ○ |
| Sähköposti tai OneDrive | ○ | ○ |
| Telia VIP | ○ | ○ |
| Heeros | ○ | ○ |
| Eduron hallinnassa olevien www-sivujen päivittämistä kuten eduro.fi tai rakka.fi | ○ | ○ |

## Kuinka usein teet varmuuskopioita?

- ○ Päivittäin
- ○ Viikottain
- ○ Kuukausittain
- ○ Harvemmin
- ○ En tee varmuuskopioita
- ○ Minun ei tarvi tehdä varmuuskopioita
- ○ Muu: _____

Kuinka usein käsittelet arkaluontoisia henkilötietoja?

- ◯ Päivittäin
- ◯ Viikottain
- ◯ Kuukausittain
- ◯ Harvemmin
- ◯ En käsittele
- ◯ Muu: _____

Kuinka usein käsittelet luottamuksellista tietoa etänä?

Tämä koskee salassapidettäviä asiakirjoja sekä henkilötietoja.

- ◯ Päivittäin
- ◯ Viikottain
- ◯ Kuukausittain
- ◯ Harvemmin
- ◯ En käsittele
- ◯ Muu: _____

Käytätkö töissä samoja tai lähes samanlaisia salasanoja eri järjestelmissä tai www-sivustoissa?

- ◯ Kaikki salasanat ovat täysin erilaisia
- ◯ Osa salasanoista on samankaltaisia
- ◯ Suurin osa käyttämistäni salasanoista on toistensa kaltaisia tai täysin samoja

Tarvitsen lisäkoulutusta seuraaviin osa-alueisiin
(Voit valita useamman vaihtoehdon)

- [ ] EU:n tietosuoja-asetus
- [ ] Salasanojen käyttö
- [ ] Asiakirjojen käsittely
- [ ] Internetin ja laitteiden turvallinen käyttö
- [ ] Henkilötietojen kerääminen (ARVI kirjaukset)

Kuinka huolellinen olet mielestäsi henkilötietojen käsittelyssä?

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Epähuolellinen | ○ | ○ | ○ | ○ | ○ | Huolellinen |

Käsitteletkö arkaluontoisia tai salassapidettäviä tietoja mielestäsi epäturvallisesti helpottaaksesi työntekoa?

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| En koskaan | ○ | ○ | ○ | ○ | ○ | Usein |

Mitä seuraavista väitteistä pitää paikkaansa?

- [ ] Henkilötunnus on arkaluontoinen henkilötieto
- [ ] Asiakkaan henkilötiedot on poistettava välittömästi, mikäli hän näin vaatii
- [ ] Mitä tahansa henkilötietoja saa kerätä, kunhan on henkilön suostumus
- [ ] Tietosuoja-asetus määrää henkilötietojen käsittelyn suostumuksen myös sopimusasiakirjoissa
- [ ] Minun on välittömästi näytettävä mitä kirjauksia olen asiakkaasta kirjoittanut, mikäli asiakas näin vaatii
- [ ] Saan kerätä vain oleellisia tai tarpeellisia henkilötietoja
- [ ] Tietosuoja kuuluu pääsääntöisesti tietosuojavastaavalle
- [ ] Henkilötietojen luovuttamisen suostumus voidaan peruuttaa
- [ ] Sähköpostiosoite voi olla henkilötieto
- [ ] Suomen tietosuojalaki tulee täydentämään EU:n yleistä tietosuoja-asetusta

Saapuneet -viestikansiossa näkyy alla oleva viesti. Onko viesti autenttinen ja onko viestissä oleva linkki turvallinen?

Vastaa Vastaa kaikille Lähetä edelleen

Wed 10/17/2018 20:04

EA Elli Aaltonen <elli.aaltonen@kela.fi>

**Kela tiedottaa**

Vastaanottaja Johannes Collins

Hei!

Täytä alla olevan linkin kautta lomake, tämä koskee koko Kelan henkilökuntaa.

https://www.kela.fi/lomake

Ystävällisin terveisin
Elli Aaltonen
Toimitusjohtaja

Kela

- ○ Viesti on autenttinen. Linkki on salattu (https) ja viesti on tullut Kelan sähköpostiosoitteesta.
- ○ Viesti ei ole välttämättä autenttinen ja tätä myötä ei ole turvallinen.

Mitä verkko-osoitteessa oleva https tarkoittaa?


- ☐ Sivusto on todettu luotettavaksi
- ☐ Sivuston yhteys on salattu
- ☐ Sivuston sisältö on suojattu
- ☐ Sivu on autenttinen
- ☐ Ei mikään näistä