Tietosuojalainsäädännön vaikutukset tietotur-vayrityksen toiminnassa

Heidi Kentala

2023 Laurea

LAUREA

Laurea-ammattikorkeakoulu

Tietosuojalainsäädännön vaikutukset tietoturvayrityksen toiminnassa

Heidi Kentala
Oikeudellinen erityisosaaminen ja oikeusmuotoilu
Opinnäytetyö
Maaliskuu, 2023

Laurea-ammattikorkeakoulu **Tiivistelmä**

Oikeudellinen erityisosaaminen ja oikeusmuotoilu

Tradenomi (Ylempi AMK)

Heidi Kentala

Tietosuojalainsäädännön vaikutukset tietoturvayrityksen toiminnassa

Vuosi 2023 Sivumäärä 77

Tutkielma on tutkimuksellinen kehittämistyö, jonka tavoitteena oli lainsäädäntöä tutkimalla kehittää toimeksiantajayritykselle oikeusmuotoiltu tarkistuslista tietosuojaan sekä tietoturvaan liittyvien toimintojen tueksi. Tutkielma toimii osana toimeksiantajayrityksen tietoturvan kehittämisprojektia.

Tutkielman lähdeaineisto koostuu tietosuojasta ja tietoturvasta sekä voimassa olevasta lainsäädännöstä niiden ympärillä. Siinä käsitellään myös osaltaan kyberturvallisuutta, joka muodostaa kokonaisuuden digitaalisen ympäristön turvallisuudesta. Tutkielman menetelmänä toimii ongelmakeskeinen lainoppi ja laadullinen tutkimus. Aineisto kerättiin kehitystyöpajojen kautta ja analysoitiin hyödyntäen aineistolähtöistä sisällönanalyysia. Koska tutkielma on osin lainopillinen, hyödynnettiin aineistona myös tietopohjaan syventyvää kirjallisuutta ja lainsäädäntöä.

Tutkielman tuotoksena on oikeusmuotoiltu tarkistuslista, jonka avulla toimeksiantajayrityksen henkilöstö tunnistaa tietosuojan oikeudellisen säätelyn sisällön ja vaatimukset. Listaus toimii henkilöstön toimintojen tukena ja kerää tärkeimmät tietosuojan ja tietoturvan asiakohdat selkeästi nähtäville.

Tutkielman kautta huomattiin tietosuojaosaamisen olevan vielä vähäistä sekä sen lainsäädännön velvoitteiden ja vaikutusten olevan vielä epäselvää. Esiinnousseita kehityskohtia tullaan jalostamaan tulosten kautta tarjoamalla henkilöstölle heidän kaipaamiaan osaamiskokonaisuuksia ja niitä tukevia sisäisiä ohjeistuksia.

Tutkielman tuloksia tullaan hyödyntämään toimeksiantajayrityksen tietoturvastrategian ja tietoturvallisen kulttuurin kehittämisessä. Tarkistuslistaa tullaan laajentamaan palvelemaan suurempaa henkilöstömäärää ja sen visuaalisia elementtejä tullaan implementoimaan myös muun dokumentaation joukkoon. Kehittämisehdotuksena ja jatkotoimenpiteenä voidaan tunnistaa tietosuojadokumentaation selkiyttäminen oikeusmuotoilun ja visuaalisuuden keinoin.

Asiasanat: tietosuoja, tietoturva, kyberturvallisuus, lainsäädäntö, oikeusmuotoilu

Laurea University of Applied Sciences

Legal Design and Expertise

Master of Business Administration

Heidi Kentala

Abstract

Effects of Data Protection Legislation on Security Company Operations

Year 2023 Pages 77

This thesis is a research-based development work the objective which was to develop a checklist by following the principles of legal design for the commissioning company to support activities related to data protection and data security by studying the legislation behind them. The thesis works as a part of the commissioning company's data protection development project.

The theoretical framework of the thesis consists of data protection and data security as well as the applicable legislation around them. This thesis also deals with cyber security which encompasses the whole security of the digital environment. The method of the thesis is problem-oriented jurisprudence and qualitive research. The material was collected through development workshops and was analyzed using data-driven content analysis. Since this thesis is partly juridical, literature and legislation that delve into the theoretical frameworks were also used as a material.

The result of the thesis is a checklist with which the personnel of the commissioning company can identify the content and requirements of the legislation of data protection. The checklist works to support the personnel's activities and collects the most important data protection and data security issues for easy viewing.

Through the thesis it was noticed that the data protection skills are still low and that the obligations and effects of the legislation are still unclear. The identified development points will be addressed through the thesis results by providing the personnel with the competences they need and the internal guidelines that support them.

The results of the thesis will be utilized in the development process of the commissioning company's data security strategy and security culture. The checklist will be expanded to serve a larger number of personnel and its visual elements will also be implemented among other documentation. Clarification of data protection documentation through legal design and visual methods can be identified as a development proposal and follow-up measure.

Keywords: data protection, data security, cyber security, legislation, legal design

Lainsäädäntö

Euroopan Unionin perusoikeuskirja (2000/C 364/01)

Euroopan Unionin yleinen tietosuoja-asetus (EU 2016/679)

Laki sähköisen viestinnän palveluista (917/2014)

Rikoslaki (39/1889)

Suomen perustuslaki (731/1999)

Tietosuojalaki (1050/2018)

Sisällys

1 Johdanto 9
2 Tutkielman tavoitteet ohjaavat sen toteutusta 10
2.1 Kehittämistehtävä 11
2.2 Tutkimuskysymykset 11
2.3 Tutkielman lähdeaineisto 12
2.4 Aikaisemmat tutkimukset 13
3 Tutkielman menetelmät kertovat tutkielman luonteen 13
3.1 Tutkimuksellinen kehittämistyö 15
3.2 Ongelmakeskeinen lainopillinen tutkimus 16
3.3 Laadullinen tutkimus 17
3.4 Oikeusmuotoilu 18
3.5 Aineistonkeruumenetelmä 18
3.6 Analysointimenetelmä 20
4 Tietosuojaa koskeva lainsäädäntö ohjaa sen sisältöä 27
4.1 Euroopan unionin perusoikeuskirja asettaa ihmisoikeudellisen viitekehyksen 27
4.2 Euroopan unionin yleinen tietosuoja-asetus asettaa tietosuojalainsäädännöllisen viitekehyksen 28
4.3 Laki sähköisen viestinnän palveluista velvoittaa tietoturvan noudattamiseen 29
4.4 Rikoslaki ohjaa Suomen rikosoikeudellista toteutusta 29
4.5 Suomen perustuslaki asettaa Suomen kansalaisten perusoikeudet 29
4.6 Tietosuojalaki ohjaa Suomen tietosuojalainsäädäntöä 30
5 Tietosuoja on henkilötietojen asiallista käsittelyä 30
5.1 Rekisterinpitäjä ja hänen velvollisuutensa 32
5.1.1 Käsittelyperuste velvoittaa henkilötietojen käsittelyn olevan perusteltua 33
5.1.2 Suunnitteluvelvoite velvoittaa henkilötietojen käsittelyn olevan suunniteltua 35
5.1.3 Huolellisuusvelvoite velvoittaa henkilötietojen suojaamisen ja tietoturvan riittävän käyttöönoton 35
5.1.4 Ilmoitusvelvollisuus velvoittaa tietoturvaloukkauksista ilmoittamisen viranomaisille 36
5.1.5 Osoitusvelvollisuus velvoittaa todentamaan tietosuojan ja tietoturvan eteen tehtävän työn 36
5.1.6 Tietosuojavastaava ohjaa organisaation tietosuojan toteutusta 37
5.2 Rekisteröity ja hänen oikeutensa 37
5.2.1 Oikeus saada tutustua tietoihin 38
5.2.2 Oikeus tietojen poistamiseen 39

5.2.3 Oikeus tietojen oikaisemiseen ... 41
5.2.4 Oikeus tietojen siirtämiseen ... 41
5.2.5 Oikeus tietojen käsittelyn rajoittamiseen ... 43
5.2.6 Oikeus vastustaa tietojen käsittelyä ... 44
5.3 Tietosuojariskit ovat henkilötietojen käsittelyn vaarantavia tekijöitä ... 45
5.4 Tietosuojaloukkaukset vaarantavat yksilön oikeudet ... 46
6 Tietoturva suojaa tietojärjestelmien sisältämää aineistoa ... 46
6.1 Tietosuojavastaava ja tietoturva ... 48
6.2 Tietoturvariskit ovat tietojen suojaamisen vaarantavia tekijöitä ... 49
6.3 Tietoturvaloukkaukset vaarantavat tietojen suojauksen ... 49
7 Kyberturvallisuus on digitaalisen maailman turvallisuutta ... 50
7.1 Kyberuhkat ovat digitaalisen maailman rikollisuutta ... 52
7.1.1 Tietomurto on luvatonta tunkeutumista toisen osapuolen tietojärjestelmiin 53
7.1.2 Tietojenkalastelu tavoittelee käyttäjän kirjautumistietojen kaappaamista 54
7.1.3 Identiteettivarkaus on toisen osapuolen henkilötietojen luvatonta käyttöä 54
7.1.4 Palvelunestohyökkäys pyrkii tahallisesti estämään tietojärjestelmien toimintaa ... 55
7.2 Riskienhallinta digitaalisessa ympäristössä ... 55
7.3 Tietoturvan merkitys strategian suunnittelussa ... 56
7.4 Tietoturvaloukkausten dokumentointiprosessi yrityksen toiminnassa ... 57
8 Tutkielman tulokset ... 61
9 Johtopäätökset ... 63
9.1 Eettisyys ... 63
9.2 Luotettavuus ... 64
9.3 Tavoitteiden saavutettavuus ... 65
Lähteet ... 68
Kuviot ... 72
Liitteet ... 73

1 Johdanto

Digitalisaation ja teknologistuvan yhteiskunnan myötä tietosuojalainsäädäntö ja sen velvoitteet muokkaavat kotimaisten organisaatioiden toimintaa henkilötietojen käsittelyn osalta entistä suoraviivaisemmaksi ja pyrkivät muokkaamaan koko prosessia eheämmäksi. Yrityksen toiminnasta halutaan läpinäkyvämpää ja asiakkaat antavat vaatimuksia, jotka yrityksen tulee täyttää. Euroopan unionin yleisen tietosuoja-asetuksen myötä tietosuojalainsäädäntö on siirtynyt tälle vuosikymmenelle ja siitä aiheutuu muutoksia sekä tarkentavia toimintamalleja yrityksille sekä heidän liiketoiminnoilleen.

Tietosuoja ja sen merkitys ovat kasvaneet runsaasti tietosuojalainsäädännön päivityksen sekä maailman nykytilanteen seurauksena. Yhä suurempi osa yhteiskunnan toiminnoista siirtyy verkkomaailmaan, josta aiheutuu riskejä ja uhkia niin organisaatioiden kuin yksityishenkilöiden toiminnalle. Yhteiskunta on riippuvainen teknologiasta ja sen kehitys on suurimmilta osin datakeskeistä digitaalisien toimintojen kietoutuessa yhä tiiviimmin yhteiskunnan toimintoihin. Yhteiskunnan toimintojen jatkuvuuden takaamiseksi kyberturvallisuuden kehittäminen on äärimmäisen tärkeää. Kyberturvallisuuden ohella tietosuoja ja tietoturva ovat ajankohtaisia käsitteitä, joiden merkitys tulee vain kasvamaan.[1]

Valtioneuvosto on tunnistanut tarpeen organisaatioiden tietoturvan kehittämiseksi ja antoi asetuksen sen kehittämiseksi tietoturvasetelin muodossa, joka tuli voimaan joulukuun alussa 2022. Tietoturvaseteli on suunnattu yhteiskunnan toiminnan kannalta kriittisten toimialojen yrityksille ja sitä tarjotaan kahdessa suuruusluokassa. Se haetaan kyberturvallisuuskeskukselta ja sen kautta pyritään nostamaan yhteiskunnan kykyä suojautua kasvavilta kyberuhkilta.[2]

Tutkielman aikana toimeksiantajayrityksen tarpeet ovat muuttuneet, jonka myötä tutkielman tavoitteet ovat muokkautuneet vastaamaan toimeksiantajayrityksen tarpeita. Tutkielman fokus on tietosuojalainsäädännössä ja sen vaikutuksissa organisaation toimintaan. Toimeksiantajayrityksellä on käynnissä tietoturvastrategian ja tietoturvakulttuurin kehittämisprojekti. Projektissa on tunnistettu puutetta tietosuojaosaamisen osalta, johon tämä tutkielma tuo lisäarvoa ja kasvattaa osaamista organisaation sisällä sen osalta.[3]

---

[1] Tarkoma 2021, 94
[2] Valtioneuvosto
[3] Toimeksiantajayrityksen tietoturvakehitys 2023

Toimeksiantajayritys toimii tietoturva-alalla keskittyen organisaatiovarmenteiden ja tiedonkalastelun ehkäisyyn. Koska yritys toimii tietoturva-alalla, ei tutkielmassa heidän nimeään tuoda suorasanaisesti esille. Toimeksiantajayritystä esitellään laajemmin kappaleessa 2.

2 Tutkielman tavoitteet ohjaavat sen toteutusta

Tämän tutkielman tarkoituksena on käsitellä tietosuojaan ja tietoturvaan liittyvää lainsäädäntöä sekä lisätä valveutta niiden ohjaavien määräysten osalta. Sen määränpäänä on laajentaa organisaation lakien velvoittamaa tietoutta ja päivittää osaltaan toimeksiantajayrityksen tietoturvastrategiaa. Tutkielman tavoitteena on luoda tarkistuslista, johon kootaan organisaation toiminnalle tärkeitä seikkoja tietosuojan osalta.[4]

Toimeksiantajayritys toimii tietoturvan ja kyberturvallisuuden parissa, pääsääntöisenä fokuksenaan digitaaliset SSL-/TLS-varmenteet. Organisaatiovarmenteet mahdollistavat vahvasti todennetut digitaaliset identiteetit, jotka tuovat luotettavuutta organisaation toimintaa kohtaan ja kertovat käyttäjälle heidän olevan oikealla ja luotettavalla sivustolla. PKI-pohjaiset, eli julkiseen avaininfrastruktuuriin Public Key Infrastructureen pohjautuvat allekirjoitusvarmenteet mahdollistavat asiakkaiden luvanmukaiset ja luotettavat sähköiset allekirjoitukset. Toimeksiantajayrityksen palvelutarjooma koostuu myös kalasteluviestien torjunta- ja koulutusratkaisuista, varmenteiden hallintapalvelusta sekä asiakkaiden konsultoinnista.[5]

Toimeksiantajayritys on perustettu vuonna 2015, mutta se on toiminut digitaalisten identiteettien parissa jo vuodesta 2011. Toimeksiantajayritys kilpailee ratkaisuillaan suurempia, kaupallisia kansainvälisiä toimijoita sekä avoimeen lähdekoodiin perustuvia maksuttomia itsepalvelun kautta toimivia ratkaisuja vastaan. Toimeksiantajayrityksen kilpailuetuna toimii kotimainen verifiointi eli organisaation identiteetin validoiminen sekä varmenneteknologian ajantasainen syväosaaminen ja sen mahdollistava asiakkaiden laaja tukeminen.[6]

Heinäkuussa 2022 toimeksiantajayrityksen koko osakekannan osti alalla toimiva suurempi toimija, tehden toimeksiantajayrityksestä näin osan suurempaa yhtiötä. Toimeksiantajayritys toimii vielä oman nimensä alaisuudessa, eikä muutoksia viralliseen toimintaan ole nähtävissä lähiaikoina. Toimeksiantajayrityksen osakekannan ostanut toimija on kotimainen riippumaton IT-integraattori, asiantuntijatalo ja ratkaisutoimittaja, joka toimii tietoturva- ja kyberturvallisuusratkaisuiden parissa. Heidän tavoitteenaan oli laajentua varmennemarkkinoille ja se oli pohja kahden tietoturva-alalla toimivan yrityksen yhdistymiselle.

---

[4] Toimeksiantajayrityksen tietoturvakehitys 2023
[5] Toimeksiantajayrityksen liiketoimintasuunnitelma 2022
[6] Ibid.

Tämä tutkielma pohjautuu yrityksen palvelutarjooman kokonaisuuteen ja pyrkii tavoittelemaan laajempaa implementointia tietosuojalainsäädännön osalta. Tutkielma pyrkii tuottamaan pitkäaikaista hyötyä ja käytettävyyttä toimeksiantajayritykselle sekä osaltaan kohottamaan toimeksiantajayrityksen toimintaa uudelle tasolle. Tutkielma tukee toimeksiantajayrityksen tietoturvan kehittämisprojektia ja toimii osana sen toteutusta.

2.1 Kehittämistehtävä

Kehittämistehtävän kautta määritellään tutkimuksen tavoitetila ja haluttu lopputulos. Usein sen tehtävänä on konkreettisen lopputuotteen eli ideoiden, konseptien, tuotteiden tai palveluiden kehittäminen. Kehittämistehtävän määrittäminen ja asettaminen voi olla yksi tutkimuksen vaikeimmista vaiheista. Määrittäminen tulee tehdä huolella ja syvällisen pohdinnan kautta, jotta tutkimus keskittyy oikeaan asiakokonaisuuteen ja etsii sille käytännössä toteutettavaa ratkaisua. On suotavaa huomata, että kehittämistehtävä voi muuntua ja uudelleensuuntautua tutkimuksen edetessä. Tällöin kokonaisuus tulee dokumentoida ja kirjata ylös täsmentynyt kehittämistehtävä.[7]

Tutkielman kehittämistehtävänä on kehittää toimeksiantajayrityksen tietosuojastrategiaa sekä muodostaa tarkistuslista helpottamaan henkilöstön työskentelyä tietosuojan ja tietoturvan osalta sekä kohottamaan valvelutta niiden osalta. Andreasson ja Ylipartanen korostavat organisaation oman henkilöstön tietoturva- ja tietosuojaoppaan tärkeyttä, sillä se tarjoaa henkilöstölle ohjeita ja tukea tietoturvaan ja tietosuojaan liittyvissä tärkeissä kysymyksissä.[8]

2.2 Tutkimuskysymykset

Tarkkaan harkitut ja selkeästi muotoillut tutkimuskysymykset aloittavat tutkimuksen ja luovat perustan aineiston keruulle. Tämä looginen järjestys kuitenkin saattaa muuttua tutkimuksen luonteen pohjalta. Esimerkiksi kvalitatiivisessa eli laadullisessa tutkimuksessa tutkimuskysymys saattaa muuttua tutkimuksen edetessä ja muotoutua lopulliseen muotoonsa vasta tutkimuksen myöhemmässä vaiheessa. Kvantitatiivisessa eli määrällisessä tutkimuksessa tutkimuskysymykset ovat selkeämmin nähtävissä sen numeerisen ja täsmällisen vaiheistuksen myötä.[9]

Jokaisen tutkimuksen taustalla on tutkimusongelma, josta tutkimuskysymykset ovat muotoutuneet. Tutkimusongelma on tutkimuksen ydin ja tutkimuskysymykset pyrkivät ratkaisemaan asetetun ongelman eli ohjaavat tutkimusta ja sen kulkua.[10]

---

[7] Ojasalo, Moilanen & Ritalahti 2015, 32-33
[8] Andreasson & Ylipartanen 2022, 134
[9] Hirsjärvi, Remes & Sajavaara 2009, 125-126
[10] Kananen 2017, 60-61

Tämän tutkielman tutkimusongelma pohjautuu sen kehittämistehtävään ja se voidaan tiivistää seuraavasti:

- Tietosuojalainsäädäntö ohjaa yrityksen tietoturvastrategiaa.

Tutkielma pyrkii tuottamaan vastaukset seuraaviin tutkimuskysymyksiin:

- Miten tietosuojalainsäädäntö vaikuttaa yrityksen tietosuojastrategiaan?
- Mitä vaatimuksia ja toimenpiteitä tietosuojalainsäädäntö asettaa yritykselle?

Tutkielman tavoitteena on lähdeaineiston ja oikeusnormien kautta kehittää toimeksiantajayrityksen tietoturvastrategiaa sekä luoda käytännöllinen ja henkilöstön käyttöön jalkautettava tarkistuslista tietoturvan ja tietosuojan tietouden kohottamiseen. Se keskittyy ymmärtämään voimassa olevaa lainsäädäntöä teoriapohjan takana ja luomaan niistä kattavan ohjeistuksen toimeksiantajayrityksen henkilöstölle ja mahdollisesti heidän asiakkailleen. Pyrkimyksenä on hyödyntää tutkielman tuloksia myös sisäisissä koulutuksissa ja luoda niiden pohjalta sisältöä toimeksiantajayrityksen ylläpitämälle blogille.

Kehittämiskysymykset voikin olla parempi sana kuvaamaan tämän opinnäytetyön taustaa kuin tutkimuskysymykset. Tutkielman olemusta kehittämistyönä kuvataan tarkemmin luvussa 3.1.

2.3 Tutkielman lähdeaineisto

Tässä tutkielmassa lähdeaineistolla tarkoitetaan tutkimuksen viitekehystä, sen teoreettista osuutta eli tietoperustaa. Tässä tutkielmassa viitekehys ja teoria voidaan mieltää samaa kokonaisuutta tarkoittavaksi, sillä molemmat muodostuvat käsitteistä sekä niiden välisistä merkityssuhteista.[11]

Tutkielman lähdeaineisto eli tietoperusta koostuu tietosuojasta ja tietoturvasta sekä voimassa olevasta lainsäädännöstä niiden ympärillä. Tutkielmassa hyödynnetään myös oikeusmuotoilun oppeja tarkistuslistan luomisessa ja tekstin elävöittämisessä kuten kuvio 1 tiivistää.

[11] Tuomi & Sarajärvi 2018, 23

Kuvio 1: Keskeiset käsitteet

2.4 Aikaisemmat tutkimukset

Tietosuoja on puhuttanut ja toiminut tutkimuksen kohteena jo useamman vuoden ajan. Tietosuoja lainsäädännön muutokset ovat kuitenkin antaneet tutkimuksen aiheelle uusia näkökulmia ja tuoreita tutkimuslähtökohtia. Euroopan unionin yleinen tietosuoja-asetus eli tuttavallisemmin GDPR on usean tutkielman aiheena. Sen implementointia yrityksen jokapäiväisiin toimenpiteisiin on tutkittu niin alemman kuin ylemmän ammattikorkeakoulututkinnon tasolla. Theseuksen järjestelmään on kirjattu tietosuoja avainsanan alle 158 tutkielmaa, joista suurin osa kuuluu alemman ammattikorkeakoulun tutkintoon. Järjestelmään on kyseisellä avainsanalla kirjautuneena vain 26 ylemmän ammattikorkeakoulututkinnon liittyvää tutkielmaa. Nämä tutkielmat keskittyvät pääsääntöisesti tietosuojaosaamisen kehittämiseen, uuden tietosuojalainsäädännön implementoimiseen yrityksen toimintoihin sekä tietosuojatoimintojen johtamiseen.[12]

Tämä tutkielma tukee aikaisempien tutkielmien sisältöä, mutta käsittelee tietosuojan lisäksi myös tietoturvaa sekä kyberturvallisuutta luoden kattavan kokonaisuuden digitaalisen turvallisuuden eri käsitteistä. Tämä tutkielma tarjoaa monipuolista tietoa tietosuojalainsäädännön osalta ja selkiyttää rekisterinpitäjän velvollisuuksia sekä rekisteröidyn oikeuksia.

3 Tutkielman menetelmät kertovat tutkielman luonteen

Tutkimuksella on aina jokin tarkoitus, tehtävä, tavoite tai päämäärä. Ne ohjaavat tutkimuksen toiminnallisia ja strategisia valintoja, joiden varaan koko tutkimus perustuu. Tutkimuksen tavoiteltava visio kertoo mikä on sen pohjimmainen syy olla olemassa. Tätä tutkimuksen

[12] Theseus

tarkoitusta voidaan kuvata ja luonnehtia neljän ominaisuuden perusteella: kartoittava, selittävä, kuvaileva tai ennustava. Huomioonotettavaa on, että tutkimusta ja sen tarkoitusta voi kuvata yksi tai useampi piirre sekä ne voivat muuntua tutkimuksen edetessä ja hahmottuessa muotoonsa.[13]

Mikäli tutkimuksen tarkoitus on kartoittava, vastaa se kysymykseen mitä tapahtuu ja miten tapahtumat liittyvät toisiinsa. Kartoittava tutkimus pyrkii katsomaan mitä tapahtuu, etsimään uusia näkökulmia, selvittämään hieman jo tunnettuja ilmiöitä ja mahdollisesti löytämään uusia sekä kehittämään hypoteeseja. Useimmiten tämä tutkimuksen piirre on laadullinen eli kvalitatiivinen.[14]

Selittävä tutkimus pyrkii vastaamaan kysymykseen, mitkä tapahtumat ovat vaikuttaneet tähän ilmiöön ja kuinka ne ovat vuorovaikutuksessa toisiinsa. Selittävä tutkimus etsii selitystä ja syytä tilanteelle, ongelmalle tai haasteelle sekä etsii syy-seuraussuhteita ja tunnistaa niiden potentiaalisia ketjuja. Tämä tutkimus voi olla niin laadullinen eli kvalitatiivinen kuin määrällinen eli kvantitatiivinen.[15]

Jos tutkimuksen tarkoitus on kuvaileva, etsii se vastausta kysymykseen, mitkä ovat kyseisessä ilmiössä näkyvimmät esiin tulevat tapahtumat ja prosessit. Kuvaileva tutkimus esittää detaljoituja kuvauksia niin henkilöistä kuin tapahtumista ja tilanteista sekä dokumentoi tapahtumista tai ilmiöistä niiden keskeisiä ja kiinnostavia ominaisuuksia. Tämän tutkimuksen piirre voi olla niin laadullinen eli kvalitatiivinen kuin määrällinen eli kvantitatiivinen.[16]

Ennustava tutkimus tavoittelee vastausta kysymykseen, mitä on tuloksena kyseisestä tapahtumasta tai ilmiöstä ja kehen vaikutukset ylettyvät. Ennustava tutkimus ennustaa ilmiöstä seurauksena olevia tapahtumia tai ihmisten tekoja. Tämä tutkimus on eksperimentaalinen strategia eli kokeellinen tutkimusmetodi.[17]

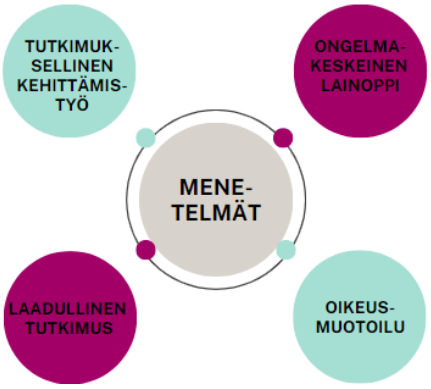
Tämän tutkielman tarkoitus ja päämäärä on piirteeltään kartoittava. Se pyrkii selvittämään lainsäädäntöä ja tietoperustaa tietosuojan sekä tietoturvan takana ja kehittämään niiden kautta toimeksiantajayrityksen tietoturvastrategiaa. Se pyrkii myös luomaan oikeusnormien ja teoriapohjan perusteella tarkistuslistan toimeksiantajayrityksen henkilöstölle tietosuojan lainsäädännöllisen toteutumisen osalta.

Seuraavissa alaluvuissa käydään läpi tutkimuksen menetelmät ja teoriat niiden takana. Itse tutkielman menetelmää voidaan luonnehtia yhdistelmämenetelmäksi, sillä siinä yhdistyy

---

[13] Hirsjärvi, Remes & Sajavaara 2009, 137-138
[14] Op.cit., 138
[15] Ibid.
[16] Supra note 13, s. 139
[17] Ibid.

laadullisen tutkimuksen menetelmät, oikeusmuotoilun opit sekä siitä voi tunnistaa osin klassisen lainopin sekä ongelmakeskeisen lainopin piirteitä. Tutkielman luonne on kuvattu myös kuviossa 2.



Kuvio 2: Käytetyt menetelmät

3.1 Tutkimuksellinen kehittämistyö

Tilastokeskus määrittelee tutkimus- ja kehittämistoiminnan luovaksi ja systemaattiseksi tiedon lisäämiseksi ja tiedon käyttämiseksi uusien sovellusten löytämisessä. Tutkimus- ja kehittämistoiminnan perimmäisenä tavoitteena on luoda jotain uutta.[18]

Tutkimuksellinen kehittämistyö saa usein alkunsa organisaation kehittämistarpeesta ja se koostuu pääsääntöisesti käytännön ongelmien ratkaisusta sekä uusien ja parhaimmillaan innovatiivisten ideoiden, konseptien, tuotteiden tai palveluiden kehittämisestä, toteuttamista ja käyttöönottoa. Kehittämistyön ideana on etsiä ja esittää parempia ratkaisuja sekä käytäntöjä ja viedä niitä käytännön tasolla eteenpäin. Suurin ero tieteellisen tutkimuksen ja tutkimuksellisen kehittämistyön välillä onkin, että tieteellinen tutkimus tuottaa uutta teoriaa ja tietopohjaa, kun taas tutkimuksellinen kehittämistyö tuottaa käytännön parannuksia ja uudenlaisia, innovatiivisia ratkaisuja. Siinä korostetaan ja kehotetaan tutkimuksen tarkkaa dokumentointia ja sen julkisuutta, jonka kautta on mahdollista luoda täysin uudenlaista ammatillista tietoa. Työstä syntynyttä uutta tietoa voidaan siten implementoida työelämän toteutukseen ja synnyttää sitä kautta uusia kehittämishankkeita.[19]

Kehittämistyötä tapahtuu organisaatioiden sisällä jatkuvasti ja huomaamatta. Tutkimukseksi se muuntuu muutostarpeen havainnosta sekä toimenpiteistä sen lopputuloksen tavoittelemiseksi. Kehittämistyö kehittyy tutkimukseksi, kun sen aikaiset toimenpiteet dokumentoidaan ja kehittämistehtävän ratkaisemiseksi käytetään tieteellisiä menetelmiä ja teoreettista

---

[18] Tilastokeskus
[19] Ojasalo, Moilanen & Ritalahti 2015, 19-20

tietoperustaa. Kehittämistutkimus on usein siis monimenetelmällinen kokonaisuus, jonka taustalla vaikuttaa aina teoreettinen tietoperusta, johon kehittämistehtävän ratkaisussa nojataan. Sen kohteena voi olla mikä tahansa toimenpide tai ilmiö, johon voidaan vaikuttaa, kuten organisaation prosessi, toiminto, tuote, palvelu tai asiantila.[20]

Tämä tutkielma on luonteeltaan tutkimuksellinen kehittämistyö, sillä sen tarkoituksena on toimeksiantajayrityksen tietoturvastrategian kehittäminen tietosuojan osalta. Sen tavoitteena on ymmärtää lainsäädäntöä tietosuojan ympärillä ja luoda käytännöllinen tarkistuslista helpottamaan henkilöstön ymmärrystä tietosuojan osalta. Tutkielmasta voi käyttää myös termiä ratkaisukeskeinen, sillä se pyrkii ratkaisemaan ongelman tai puutteen toimeksiantajayrityksen toiminnassa ja palvelukokonaisuudessa. Sen aikomuksena on tarjota toimeksiantajayrityksen tietosuoja- ja tietoturvakysymykseen ratkaisu ja täydentää tätä kautta heidän toimintaansa entistä selväpiirteisemmäksi.

3.2 Ongelmakeskeinen lainopillinen tutkimus

Tämän tutkielman tutkimusmenetelmänä toimii osaltaan ongelmakeskeinen lainopillinen tutkimus, sillä tutkielman tavoitteena on ratkaista ongelma. Lainopin eli oikeusdogmatiikan tutkimuskohteena on voimassa oleva oikeus. Sen tehtävänä on selvittää voimassa olevien oikeusnormien eli oikeussääntöjen ja oikeusperiaatteiden sisältöä sekä merkitystä. Lainoppi koostuu perinteisesti kahdesta eri tehtävästä: tulkinnasta ja systematisoinnista.[21]

Systematisointi on lainopin teoreettinen ulottuvuus ja sitä luonnehditaankin usein teoreettiseksi lainopiksi. Lainoppi systematisoi eli jäsentelee voimassa olevaa oikeutta sekä järjestää ja rakentaa tätä kautta koherenttia ja johdonmukaista oikeusjärjestelmää. Tulkinta on lainopin praktinen ulottuvuus ja sitä kutsutaan usein käytännölliseksi lainopiksi. Tähän kuuluu oikeussääntöjen ja oikeusperiaatteiden pohdinta, puntarointi ja tasapainottaminen. Tulkinta on lainopin keskeinen menetelmä.[22]

Lainoppia voidaan kuvata myös deskriptiiviseksi tieteeksi, sillä se antaa kuvauksen voimassa olevasta oikeudesta. Sen lauseet kuvaavat voimassa olevan oikeuden sisältöä ja sanomaa, mutta se ei ole puhdas kuvaus oikeudesta. Lainopin sisältöön kuuluu myös oikeusvertailu, joka on itsessään oikeustieteen itsenäinen osa-alue keskittyessään oikeusvertailuun ja sen teoreettisiin ja menetelmäopillisiin kysymyksiin. Lainopissa vertaillaan myös siis kotimaista oikeusjärjestystä ja lainsäädäntöä sekä sen sisältämiä normeja ja käytänteitä muiden maiden oikeusjärjestyksiin ja lakiteksteihin.[23]

---

[20] Kananen 2012, 19-21
[21] Hirvonen 2011, 21-24
[22] Op.cit., 25
[23] Op.cit., 25-26

Tutkielmasta voi käyttää myös käsitettä oikeusteoreettinen, sillä se käsittelee voimassa olevaa oikeutta sekä oikeudenaloille yhteisiä käsitteitä ja oikeusperiaatteita.[24] Sen tavoitteena on ymmärtää oikeusnormeja tietosuojan sekä tietoturvan ympärillä ja koota niistä henkilöstölle ymmärrettävä tarkistuslista.

3.3 Laadullinen tutkimus

Laadullisen eli kvalitatiivisen tutkimuksen tavoitteena on ilmiön, tapahtuman tai käsitteen eli tutkimuskohteen ymmärtäminen kohderyhmän kautta. Laadullinen tutkimus on usein aineistolähtöistä eli induktiivista ja sen sisältö on vuoropuhelua aineiston ja teorian välillä. Sen asetelma on joustava, joka mahdollistaa tutkimuksen sisällön muokkaamisen ja päivittämisen tutkimuksen edetessä.[25] Hirsjärvi, Remes ja Sajavaara luonnehtivat laadullista tutkimusta kertomukseksi etsimisestä[26].

Laadullisessa tutkimuksessa voidaan puhua teoreettisesta tutkimustyypistä ja empiirisestä tutkimustyypistä. Tutkimustyyppien suurin eroavaisuus on niiden havaintoaineiston tarkastelussa. Empiirisessä tutkimustyypissä korostuvat aineiston keräämis- ja analysointimenetelmät sekä niiden argumentointi ja dokumentointi koko tutkimuksen ajan. Teoreettisessa tutkimustyypissä ei ole virallisesti määritettyä analysointimenetelmää. Sen analysoinnissa on kyse kuvailevasta ongelmanratkaisusta, jonka raportoinnin tutkija määrittää itse. Empiirisessä tutkimustyypissä pyritään etiikan oppien mukaan suojaamaan havainnoidun henkilön henkilöllisyys ja huomioimaan tietosuoja, kun taas teoreettinen tutkimustyyppi turvautuu juuri yksittäiseen väitteeseen sekä väitteen antajan henkilöllisyyden tunnistamiseen.[27]

Laadullinen tutkimus on usein empiiristä, mikä tarkoittaa, että sen havaintoaineiston kerääminen, analysointi ja argumentointi tulkitaan empiiriseksi. Laadullinen tutkimus ei voi kuitenkaan koskaan olla täysin teoriatonta, mikäli sen kantaa tutkimuksen statusta, sillä jokaisen tutkimuksen tulee sisältää ihmisen suorittamaa tarkastelua eli olla luonteeltaan teoreettista.[28]

Tässä tutkielmassa hyödynnetään myös laadullisen tutkimuksen oppeja, sillä tarkoituksena on ymmärtää lainsäädäntöä ja teoriaa tutkittavan aiheen ympärillä yhteistyössä toimeksiantajayrityksen kanssa. Tutkielma ei sisällä määrällistä eli kvantitatiivista tietoa, vaan nojautuu lainsäädännön ja teorian kautta ilmiön ymmärtämiseen. Tutkielma ei tavoittele täysin

---

[24] Hirvonen 2011, 27
[25] Puusa & Juuti 2020, 9-12
[26] Hirsjärvi, Remes & Sajavaara 2009, 266
[27] Tuomi & Sarajärvi 2018, 24-27
[28] Op.cit., 25-27

ongelmakeskeistä oikeusdogmaattista tutkimusta, vaan sitä on täydennetty laadullisen tutkimuksen menetelmissä. Tutkielman luonnetta voi siis parhaiten kuvata termillä yhdistelmämenetelmä.

3.4 Oikeusmuotoilu

Oikeusmuotoilu on käyttäjälähtöistä suunnittelua oikeudellisten normien ja lainsäädännön muuntamiseksi selkeämpään ja ymmärrettävämpään muotoon. Oikeusmuotoilu yhdistää palvelumuotoilun ja käyttäjätutkimuksen vaikeaselkoisen lainsäädännön tulkitsemiseen ja muodostaa tätä kautta käytettäviä, käytännöllisiä, hyödynnettäviä ja puoleensavetäviä ratkaisuja tehden oikeudellisista palveluista käyttäjille mielekkäämpiä. Jotta tämä saavutetaan, tulee asianomaisten työskennellä yhteistyössä, yhdistäen tieto-taitonsa ja osaamisensa vuorovaikutukselliseksi kokonaisuudeksi. Tätä eri osaamistaustaisten ihmisten yhdistymää voidaan kutsua myös poikkitieteellisyydeksi, jossa eri alan ihmiset ryhtyvät yhteistyöhön kehittääkseen laajaalaisempia ratkaisuja.[29]

Muotoilu on innovaatioita luova lähestymistapa ongelmanratkaisuun. Käyttäjälähtöinen muotoilu keskittyy käyttäjien ongelmiin, haasteisiin ja tarpeisiin luoden ratkaisuja, jotka kehittävät käyttäjien kokemuksia ja tuovat heille arvoa. Arvon tuominen käyttäjälle ja heidän kokemuksiinsa keskittyminen on muotoilun ydin.[30]

Muotoilu on jäsennelty ja joustava lähestymistapa ongelmanratkaisuun, ideoiden synnyttämiseen ja niiden toteuttamiseen. Se tarjoaa laajemman ajattelutavan, jonka pohjalta haasteet nähdään suuremman oivalluskyvyn kautta. Tämä taas osaltaan avustaa innovatiivisten, käyttökelpoisten ja tehokkaampien ratkaisujen luomisessa. Muotoilua voi hyödyntää ja implementoida organisaation toimintoihin monin tavoin. Sitä voi käyttää nopeana ongelmanratkaisun työkaluna, pitkäjänteisenä kehittämistyönä sekä tutkimusmenetelmänä.[31]

3.5 Aineistonkeruumenetelmä

Koska tutkielma on osaltaan lainopillinen, perustuu sen aineiston kerääminen tietopohjaan syventyvään kirjallisuuteen ja voimassa olevaan lainsäädäntöön. Teoriapohjaista aineistoa on tuettu toimeksiantajayrityksen sisäisillä kehittämistyöpajoilla ja niiden tuotoksilla. Näiden avulla on pyritty tuomaan tutkielmaan toimeksiantajayrityksen omakohtaisia kokemuksia ja mielipiteitä aiheesta, jotka puolestaan rikastuttavat ja täydentävät teoriapohjaista aineistoa.

---

[29] Hagan 2017, What is Legal Design?
[30] Hagan 2017, What is design?
[31] Ibid.

Luova ongelmanratkaisu on tämän ajan suositelluin menetelmä kehittämistyössä, sillä sen työkalujen kautta luodaan innovatiivisia ja uudenlaisia näkökulmia, ideoita ja ratkaisuja. Menetelmiä tähän on lukuisia ja jokaisen kohdalla on hyvä muistaa, että ideoiden määrä synnyttää laatua ja tässä avaintekijänä on ryhmässä toimimisen taidot. Luova ongelmanratkaisu edellyttää myös avointa ja positiivista ilmapiiriä, kiireettömyyttä ja avoimuutta sekä tietynlaista kontrollia. Yhteistä kaikille ideointimenetelmille on tavoite eliminoida normaalin ajattelun rajoitteet, motivoida jakamaan toisten kanssa kaikki oivallukset ja mietteet sekä jatkokehittämään muiden ideoita ja pohdintoja. Ideoiden tuottaminen on edullista, mutta niiden toteuttaminen kallista. Tämän vuoksi luovan ongelmanratkaisun menetelmät pyrkivät etsimään ja löytämään niille määritettyjen työkalujen kautta parhaat ideat toteutettavaksi.[32]

Luovan ongelmanratkaisun keskeisenä tekijänä voidaan nähdä jo oikeusmuotoilussa mainittu poikkitieteellisyys ja sen tuomat hyödyt. Poikkitieteellisyys on mukaelma monitieteisyydestä sekä tieteidenvälisyydestä, jonka kautta voidaan saavuttaa uudenlaisia ratkaisuja. Monitieteellisyys yhdistää usean tieteenalan tutkimusmenetelmät, jotka yhdistyvät yleensä tutkimuksen loppuraportissa. Tieteidenvälisyys menee astetta pidemmälle yhdistäen eri tieteenalojen tutkimusmenetelmät jo itse tutkimustyönaikana. Sen kautta pyritään rikkomaan tieteiden rajoituksia ja niiden välisiä rajoja ja muodostamaan tutkimusprosessi, jossa hyödynnetään eri tieteiden sisältämää tietoa, käsitteitä, näkökulmia, teorioita ja menetelmiä. Poikkitieteellisyys yhdistää nämä kaksi toiminta- ja tutkimustapaa toisiinsa ja jo alkumetreinä unohtaa tieteiden väliset rajat. Poikkitieteellisyys edellyttää tutkimuksen yhtenäisyyttä niin käsitteiden kuin prosessin osalta ja tavoittelee yhteistä määränpäätä. Tieteiden välisten rajojen hämärtyessä voidaan keskittyä tutkimuksen olennaiseen ytimeen välittämättä tieteiden tai tutkijoiden eri taustoista. Osaamisen yhdistäminen tuo laaja-alaista ratkaisukyvykkyyttä, jonka kautta syntyy uudenlaisia ja innovatiivisia ratkaisuja. Poikkitieteellisyyden kautta syntyvä luova ajattelu mahdollistaa ennennäkemättömien ideoiden syntymisen ja niiden implementoimisen arjen toimintoihin.[33]

Tässä tutkielmassa luovaa ongelmanratkaisua hyödynnettiin kehittämistyöpajojen muodossa. Kehittämistyöpajoja voi kutsua myös ideointityöpajoiksi tai aivoriihiksi. Englanniksi siitä käytetään nimeä brainstorming. Kehittämistyöpajassa on usein 6-12 henkilöä ja heidän tavoitteenaan on pyrkiä tiettyyn tavoitteeseen. Tavoite voi olla muun muassa ratkaisu johonkin ongelmaan, uusi lähestymistapa johonkin asiakokonaisuuteen tai uuden toteutustavan ideoiminen.[34]

Tutkielman kehitystyöpajoja toteutettiin kaksi, joissa kartoitettiin toimeksiantajayrityksen henkilöstön ymmärrystä, osaamista ja odotuksia tietoturvastrategian, tietoturvan ja

---

[32] Ojasalo, Moilanen & Ritalahti 2015, 158-160
[33] Mikkeli & Pakkasvirta 2007, 63-66
[34] Supra note 32, s. 160-161

tietosuojan osalta. Kehitystyöpajojen välillä oli pari kuukautta, sillä toimeksiantajayrityksen vuoden 2022 heinäkuussa tapahtuneen liiketoimintakaupan ja siitä johtuvien tietoturvan yhtenäistämiseksi tehtävien toimenpiteiden vuoksi tutkielman aineistonkeruu viivästyi.

3.6 Analysointimenetelmä

Aineistoa voidaan analysoida monin eri tavoin, mutta tässä tutkielmassa keskitytään aineistolähtöiseen sisällönanalyysiin. Sisällönanalyysi on tutkimusaineiston kuvaamista sanallisesti, jonka vuoksi se mielletään enemmän laadullisen tutkimusmenetelmän metodiksi. Siinä etsitään merkityssuhteita- ja kokonaisuuksia, joiden tulokset voidaan esittää sanallisina tulkintoina.[35]

Aineistolähtöisen sisällönanalyysin tavoitteena on löytää tutkimusaineistosta eräänlainen toiminnan logiikka tai tyypillinen kertomus eli tyyppikertomus. Se koostuu kolmesta eri vaiheesta: pelkistämisestä, ryhmittelystä ja teoreettisten käsitteiden luomisesta. Pelkistämällä karsitaan tutkimusongelman osalta aiheeton tieto pois, säilyttäen tutkielman kannalta tärkeän informaation. Pelkistämiseen kuuluu myös aineiston tiivistäminen tutkimusongelman ja tutkimuskysymyksien ohjaamana. Ryhmittelyn kautta kootaan pelkistetty aineisto uudenlaiseksi ja johdonmukaiseksi kokonaisuudeksi sen mukaan mitä tutkimusaineistosta etsitään. Viimeisessä vaiheessa nimetään ryhmittelyssä luodut ryhmät niitä kuvaavalla käsitteellä. Tuloksia tarkastellaan teoreettisen lähdeaineiston avulla, jonka kautta tavoitellaan tutkittavan aiheen kuvaamaa merkityskokonaisuutta.[36]

Aineiston tiivistäminen ja pelkistäminen auttaa nostamaan esiin sen sisältämää olennaista tietoa ja jäsentelemään sitä. Tiedon tiivistämisen kautta myös sen informaatioarvo kasvaa. Ryhmittelyn avulla aineistosta etsitään toistuvia ja samankaltaisia käsitteitä tai aihealueen eroja kuvaavia käsitteitä. Samaan aihealueeseen kuuluvat käsitteet kootaan ryhmäksi ja ryhmä nimetään sen sisältöä kuvaavalla nimikkeellä.[37]

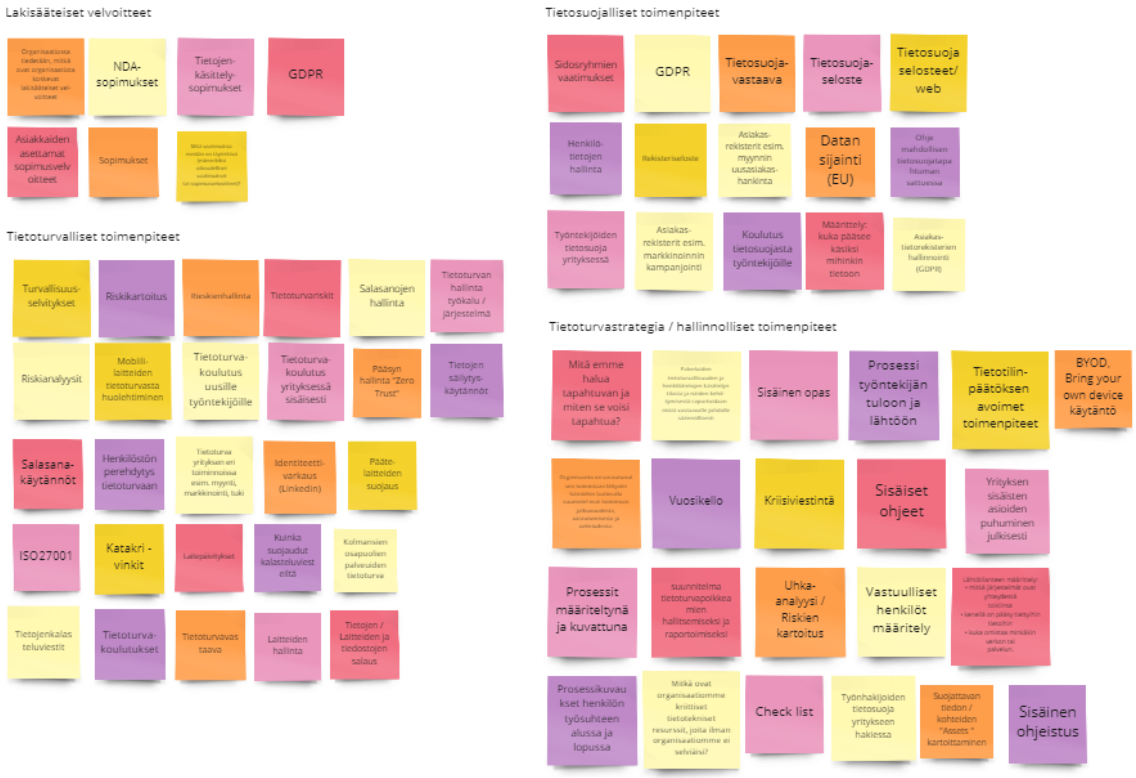
Aineistolähtöistä sisällönanalyysia voi viedä pidemmälle tyyppikertomusten eli narratiivien avulla. Tarina voidaan muodostaa kerätyn aineiston avulla tiivistäen kokemukset ja löydökset kertomuksen muotoon. Kertomukset voivat usein olla stereotyyppisiä ja yleistäviä, mutta ovat todellisia otteita ja signaaleja nykyelämästä.[38]

Tutkielman aineiston analysointi aloitettiin aineistolähtöisen sisällönanalyysin kautta tiivistämällä aineistoa pelkistetympään muotoon. Kehitystyöpajojen tuotoksista ja keskusteluista

---

[35] Vilkka 2021, 163
[36] Op.cit., 163-164, 170
[37] Ojasalo, Moilanen & Ritalahti 2015, 137-140
[38] Supra note 36, s. 170

poimittujen muistiinpanojen avulla saatiin muodostettua muistiinpanolappuja Miro-alustalle. Näistä muodostettiin selkeitä kokonaisuuksia, jotka ryhmiteltiin aihealueita kuvaavalla käsitteellä, kuten kuviosta 3 voidaan huomata.



Kuvio 3: Aineiston analysointi

Aineiston analysoinnin kautta nousi esille neljä selkeää asiakokonaisuutta: lakisääteiset velvoitteet, tietosuojalliset toimenpiteet, tietoturvalliset toimenpiteet ja hallinnolliset toimenpiteet eli tietoturvastrategiaan sisältyvät asiakokonaisuudet.

Lakisääteiset velvoitteet

- Organisaatiossa tiedetään, mitkä ovat organisaatiota koskevat lakisääteiset velvoitteet
- NDA-sopimukset
- Tietojenkäsittelysopimukset
- GDPR
- Asiakkaiden asettamat sopimusvelvoitteet
- Sopimukset
- Mitä vaatimuksia meidän on täytettävä (esimerkiksi oikeudelliset vaatimukset tai sopimusvelvoitteet)?

Tietosuojalliset toimenpiteet

- Sidosryhmien vaatimukset
- GDPR
- Tietosuojavastaava
- Tietosuojaseloste
- Tietosuojaselosteet/web
- Henkilötietojen hallinta
- Rekisteriseloste
- Asiakasrekisterit esim. myynnin uusasiakashankinta
- Datan sijainti (EU)
- Ohje mahdollisen tietosuojatapahtuman sattuessa
- Työntekijöiden tietosuoja yrityksessä
- Asiakasrekisterit esim. markkinoinnin kampanjointi
- Koulutus tietosuojasta työntekijöille
- Määrittely: kuka pääsee käsiksi mihinkin tietoon
- Asiakastietorekisterien hallinnointi (GDPR)

Tietoturvalliset toimenpiteet

- Turvallisuusselvitykset
- Riskikartoitus
- Riskienhallinta
- Tietoturvariskit
- Salasanojen hallinta
- Tietoturvan hallintatyökalu/-järjestelmä
- Riskianalyysit
- Mobiililaitteiden tietoturvasta huolehtiminen
- Tietoturvakoulutus uusille työntekijöille
- Tietoturvakoulutus yrityksessä sisäisesti
- Pääsyn hallinta ”Zero Trust”
- Tietojen säilytyskäytännöt
- Salasanakäytännöt
- Henkilöstön perehdytys tietoturvaan
- Tietoturva yrityksen eri toiminnoissa esim. myynti, markkinointi, tuki
- Identiteettivarkaus (LinkedIn)
- Päätelaitteiden suojaus
- ISO27001
- Katakri-vinkit
- Laitepäivitykset

- Kuinka suojaudut kalasteluviesteiltä
- Kolmansien osapuolien palveluiden tietoturva
- Tietojenkalasteluviestit
- Tietoturvakoulutukset
- Tietoturvavastaava
- Laitteiden hallinta
- Tietojen/laitteiden ja tiedostojen salaus

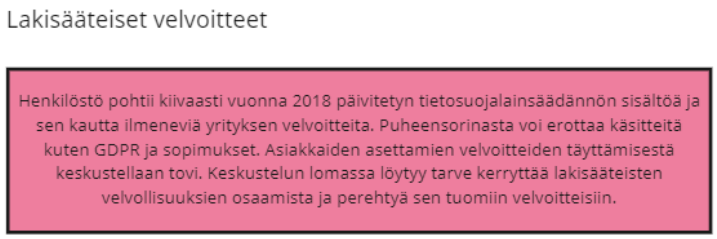
Hallinnolliset toimenpiteet / tietoturvastrategia

- Mitä emme halua tapahtuvat ja miten se voisi tapahtua?
- Palveluiden tietoturvallisuuden ja henkilötietojen käsittelyn tilasta ja näiden kehittymisestä raportoidaan niistä vastaavalle johdolle säännöllisesti
- Sisäinen opas
- Prosessi työntekijän tuloon ja lähtöön
- Tietotilinpäätöksen avoimet toimenpiteet
- BYOD Bring your own device käytäntö
- Organisaatio on varautunut sen toimintaan liittyviin häiriöihin laatimalla suunnitelmat toiminnan jatkuvuudesta, varautumisesta ja valmiudesta
- Vuosikello
- Kriisiviestintä
- Sisäiset ohjeet
- Yrityksen sisäisten asioiden puhuminen julkisesti
- Prosessit määriteltynä ja kuvattuna
- Suunnitelma tietoturvapoikkeamien hallitsemiseksi ja raportoimiseksi
- Uhka-analyysi/riskien kartoitus
- Vastuulliset henkilöt määritelty
- Lähtötilanteen määrittely: mitkä järjestelmät ovat yhteydessä toisiinsa, kenellä on pääsy tiettyihin tietoihin, kuka omistaa minkäkin verkon tai palvelun
- Prosessikuvaukset henkilön työsuhteen alussa ja lopussa
- Mitkä ovat organisaatiomme kriittiset tietotekniset resurssit, joita ilman organisaatiomme ei selviäisi?
- Check list
- Työnhakijoiden tietosuoja yritykseen hakiessa
- Suojattavan tiedon/kohteiden ”Assets” kartoittaminen
- Sisäinen ohjeistus

Aineiston ryhmittelyn jälkeen esille nousseista neljästä asiakokonaisuudesta muodostettiin tyyppikertomukset eli narratiivit, jotka ovat rakentuneet juonellisesti niihin sisältyvien teemojen ja teoreettisen lähdeaineiston kautta.

Ensimmäisessä tyyppikertomuksessa kuviossa 4, kuvataan kehittämistyöpajoissa esiin noussutta lakisääteisten velvoitteiden aihekokonaisuuden sisältöä. Tyyppikertomus tiivistää lainsäädäntöön liittyvät huomiot ja kehittämistyöpajoissa käydyn keskustelun sen ympäriltä.

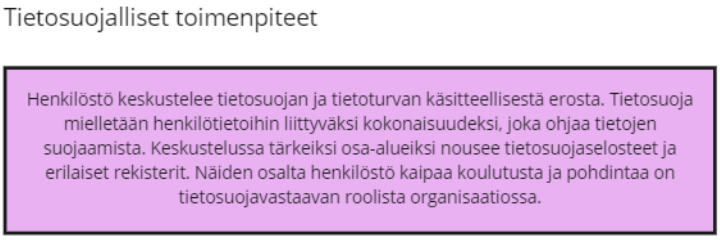
”Henkilöstö pohtii kiivaasti vuonna 2018 päivitetyn tietosuojalainsäädännön sisältöä ja sen kautta ilmeneviä yrityksen velvoitteita. Puheensorinasta voi erottaa käsitteitä kuten GDPR ja sopimukset. Asiakkaiden asettamien velvoitteiden täyttämisestä keskustellaan tovi. Keskustelun lomassa löytyy tarve kerryttää lakisääteisten velvollisuuksien osaamista ja perehtyä sen tuomiin velvoitteisiin.”



Kuvio 4: Tyyppikertomus 1, lakisääteiset velvoitteet

Toisessa tyyppikertomuksessa kuviossa 5 tiivistetään kehittämistyöpajojen sisältöä tietosuojallisten toimenpiteiden osalta. Kuvaus sisältää kehittämistyöpajoihin osallistuneiden pohdinnat ja huomiot tietosuojan käsitteen sekä kokonaisuuden ympärillä.

”Henkilöstö keskustelee tietosuojan ja tietoturvan käsitteellisestä erosta. Tietosuoja mielletään henkilötietoihin liittyväksi kokonaisuudeksi, joka ohjaa tietojen suojaamista. Keskustelussa tärkeiksi osa-alueiksi nousee tietosuojaselosteet ja erilaiset rekisterit. Näiden osalta henkilöstö kaipaa koulutusta ja pohdintaa on tietosuojavastaavan roolista organisaatiossa.”



Kuvio 5: Tyyppikertomus 2, tietosuojalliset toimenpiteet

Kolmas tyyppikertomus kuviossa 6 kuvaa kehittämistyöpajojen sisältämää keskustelua ja asiakohtia tietoturvallisten toimenpiteiden osalta. Kertomus tiivistää osallistuneiden huomiot tietoturvan ja sen toteutumisen kohdalta.

”Henkilöstö mieltää tietoturvan konkreettisiksi keinoiksi toteuttaa tietosuojaa. Keskustelu pyörii tiiviisti riskienhallinnan, suojauskäytäntöjen ja laitehallinnan ympärillä. Tietoturvakoulutus ja tietoturvavastaavan nimeäminen puhuttaa. Tietoturvan kehittämiseen mielletään suojautumiskeinot tietomurtojen varalta.”

Tietoturvalliset toimenpiteet

Henkilöstö mieltää tietoturvan konkreettisiksi keinoiksi toteuttaa tietosuojaa. Keskustelu pyörii tiiviisti riskienhallinnan, suojauskäytäntöjen ja laitehallinnan ympärillä. Tietoturvakoulutus ja tietoturvavastaavan nimeäminen puhuttaa. Tietoturvan kehittämiseen mielletään suojautumiskeinot tietomurtojen varalta.

Kuvio 6: Tyyppikertomus 3, tietoturvalliset toimenpiteet

Neljännessä tyyppikertomuksessa kuviossa 7 kuvataan kehittämistyöpajoissa käsiteltyä sisältöä hallinnollisten toimenpiteiden ja tietoturvastrategian osalta.

”Henkilöstön keskusteluiden pohjalta nousee esiin hallinnolliset toimenpiteet tietosuojan ja tietoturvan osalta. Keskusteluissa on useasti esillä prosessikuvaukset, sisäiset ohjeistukset ja koulutukset sekä toiminnan suunnittelu. Henkilöstö tunnistaa tarpeen tietoturvallisen kokonaisuuden johtamiselle ja valvonnalle.”

Tietoturvastrategia / hallinnolliset toimenpiteet

Henkilöstön keskusteluiden pohjalta nousee esiin hallinnolliset toimenpiteet tietosuojan ja tietoturvan osalta. Keskusteluissa on useasti esillä prosessikuvaukset, sisäiset ohjeistukset ja koulutukset sekä toiminnan suunnittelu. Henkilöstö tunnistaa tarpeen tietoturvallisen kokonaisuuden johtamiselle ja valvonnalle.

Kuvio 7: Tyyppikertomus 4, hallinnolliset toimenpiteet / tietoturvastrategia

Aineiston analysoinnin pohjalta muodostettiin kuviossa 8 esitetty hahmotelma tarkistuslistasta. Kehittämistyöpajojen sisällön analysoinnin tuloksia aseteltiin aihealueiksi tarkistuslistan luonnostelussa. Hahmotelma toimi prototyyppinä lopputuotoksen suunnittelussa. Sen kautta varmistettiin oikeiden asioiden nostaminen tarkistuslistaa kehittäessä.

Kuvio 8: Tarkistuslistan hahmotelma

Tietosuoja

- Tietosuojaseloste
- Rekisteriseloste
- Tietosuojavastaava
- Asiakasrekisterit
- Henkilötietojen hallinta
- Tietojenkäsittelysopimukset
- Sopimukset

Tietoturva

- Turvallisuusselvitykset
- Riskienhallinta
- Salasanakäytännöt

- Päätelaitteiden suojaus
- Tietojen säilytyskäytännöt
- Tietoturva yrityksen eri toiminnoissa esim. myynti, markkinointi, tuki
- Pääsyn hallinta ”Zero Trust”
- Tietoturvavastaava

Liittyvät dokumentit

- Sisäinen ohjeistus
- Uhka-analyysi / Riskien kartoitus
- Seloste käsittelytoimista
- Vuosikello
- Prosessikuvaukset

Lisätietoja

- Vastuuhenkilöt

Aineistosta esiin nousseita aiheita, huomioita ja toiveita tietoturvastrategian sekä hallinnollisten toimenpiteiden osalta viedään eteenpäin toimeksiantajayrityksen tietoturvastrategian ja turvallisuuspolitiikan kehittämisprojektissa. Huomiot toimivat henkilöstön näkemyksinä projektin sisällön ja toteutuksen tukena.

4 Tietosuojaa koskeva lainsäädäntö ohjaa sen sisältöä

Tietosuojaa ja tietoturvaa ohjaa niitä koskeva oikeudellinen säätely. Tähän säätelyyn kuuluvat lait velvoittavat tietosuojan ja tietoturvan sisällön oikeanmukaista toteutumista ja valvomista. Tässä kappaleessa käsitellään lainsäädäntöä opinnäytetyön aihealueen ympärillä.

4.1 Euroopan unionin perusoikeuskirja asettaa ihmisoikeudellisen viitekehyksen

Euroopan unionin perusoikeuskirja esiteltiin ensimmäistä kertaa joulukuussa vuonna 2000. Perusoikeuskirjan päivitetty versio julkaistiin kesäkuussa vuonna 2016 ja se on muutamaa maata lukuun ottamatta oikeudellisesti pätevä koko Euroopan unionissa. Se vahvistaa oikeudet, jotka pohjautuvat jäsenvaltiolle yhteisiin valtiosääntöperiaatteisiin, kansainvälisiin velvoitteisiin, ihmisoikeuksia ja perusvapauksia suojaavaan yleissopimukseen, hyväksyttyihin sosiaalisiin peruskirjoihin sekä Euroopan unionin ja Euroopan ihmisoikeustuomioistuimen

oikeuskäytäntöön. Euroopan unionin tuomioistuin sekä jäsenvaltioiden omat tuomioistuimet tulkitsevat ja toimeenpanevat tätä perusoikeuskirjaa. [39] [40]

Perusoikeuskirja asettaa ja määrittää EU:n sisällä vaikuttavat perusoikeudet. Näitä perusoikeuksia ovat ihmisarvo, vapaudet, tasa-arvo, yhteisvastuu ja kansalaisten oikeudet, esimerkiksi äänioikeus ja vaalikelpoisuus sekä liikkumis- ja oleskeluvapaus. Tähän tutkielmaan vaikuttaa erityisesti perusoikeuskirjan artiklat 7 ja 8. Artiklassa 7 säädetään, että jokaisella on oikeus yksityis- ja perhe-elämänsä, kotinsa sekä viestiensä kunnioittamiseen. Artiklassa 8 taas säädetään, että jokaisella on oikeus henkilötietojensa suojaan. Nämä kaksi artiklaa vaikuttavat suuresti myös Euroopan unionin yleisessä tietosuoja-asetuksessa.[41]

4.2 Euroopan unionin yleinen tietosuoja-asetus asettaa tietosuojalainsäädännöllisen viitekehyksen

Euroopan unionin yleinen tietosuoja-asetus eli GDPR (General Data Protection Regulation) astui voimaan toukokuussa 2016 ja sen kansallinen soveltaminen alkoi kaksi vuotta myöhemmin toukokuussa 2018. Uusi tietosuoja-asetus korvasi Euroopan parlamentin ja neuvoston vuonna 1995 asettaman tietosuojadirektiivin 95/46/EC ja henkilötietodirektiivin 95/46/EY. Päivitetty asetus EU 2016/679 päivittää ja yhtenäistää Euroopan unionin jäsenmaiden tietosuojaa koskevia käytänteitä ja lakeja sekä vahvistaa rekisteröidyn yksityishenkilön itsemääräämisoikeutta. Asetus tavoittelee yksilön oikeuksien vahvistamista, tietosuojasäännöstön täytäntöönpanon valvonnan tehostamista sekä tietosuojan tärkeyden maailmanlaajuista huomioimista. Sen tavoitteena on myös rakentaa Euroopan unionille relevantti, yhtenäinen ja perusteellinen alusta tietosuojalle sekä lisätä luottamusta verkkopalveluihin edistäen tätä kautta Euroopan digitaalisten sisämarkkinoiden kehitystä.[42] [43]

Tietosuoja-asetusta ei sovelleta rekisteröidyn yksityishenkilön henkilökohtaisessa ja kotitaloutta koskevassa toiminnassa tai prosessissa. Yksilön henkilökohtainen käyttö jää siis asetuksen ulkopuolelle.[44]

Päivitetyn tietosuoja-asetuksen taustalla vaikuttavat laajalti kansainväliset ihmisoikeussopimukset sekä Euroopan Unionin perusoikeuskirja. Euroopan Unionin perusoikeuskirjasta etenkin artikla 7 Yksityis- ja perhe-elämän kunnioittaminen ja artikla 8 Henkilötietojen suoja vaikuttavat suurelta osin tietosuoja-asetuksen sisällössä.[45]

---

[39] Euroopan unionin perusoikeuskirja 2000/C 364/01
[40] Euroopan unionin perusoikeuskirja 2016/C 202/02
[41] Op.cit., § 7-8
[42] Järvinen 2022, 132
[43] Andreasson & Ylipartanen 2022, 30
[44] Euroopan unionin yleinen tietosuoja-asetus 2016/679 § 2
[45] Supra note 41, § 7-8

4.3 Laki sähköisen viestinnän palveluista velvoittaa tietoturvan noudattamiseen

Laki sähköisen viestinnän palveluista (2014/917) säädettiin marraskuussa vuonna 2014 edistämään sähköisten ja digitaalisten viestintäpalveluiden tarjoomaa ja niiden käyttöä. Sen tavoitteena on myös varmistaa, että viestintäverkkoja on saatavilla koko maassa. Tämän tutkielman kannalta lain tärkein tavoite on kuitenkin sähköisen viestinnän luottamuksellisuuden, eheyden ja yksityisyyden suojan toteutuminen ja turvaaminen.[46]

Laissa säädetään sähköisen viestinnän tietoturvallisesta toiminnasta ja velvoitetaan niiden välittäjiä ryhtymään välittömiin toimenpiteisiin tietoturvan turvaamiseksi ja mahdollisten häiriöiden korjaamiseksi. Välittäjien on hetimiten ryhdyttävä häiriöiden korjaamiseen sekä välitettävä häiriöilmoitus käyttäjille ja Liikenne- ja viestintävirastolle, mikäli toimintaan epäillään kohdistuneen merkittävä tietomurto.[47]

Laki velvoittaa siis sähköisen viestinnän rekisterinpitäjiä noudattamaan tietoturvallisia menetelmiä koko maan viestintäpalveluiden jakelussa sekä toiminnallaan turvaamaan käyttäjiensä yksityisyyden suojaa.

4.4 Rikoslaki ohjaa Suomen rikosoikeudellista toteutusta

Rikoslaki (1889/39) säädettiin alun perin jo joulukuussa vuonna 1889 ja se ohjaa Suomen rikosoikeudellista lainsäädäntöä. Lakia on päivitetty useaan otteeseen sen jälkeen vastaamaan nykyajan vaatimuksia. Tämän vuoksi laista ei ole alkuperäisessä muodossaan kovinkaan montaa pykälää.[48]

Tämän tutkielman kannalta relevantein osa on luku 38, jossa käsitellään tieto- ja viestintärikoksia. Erityisesti artiklat 8 ja 9, joissa säädetään tietomurroista sekä tietosuojarikoksista vaikuttavat tämän tutkielman teeman sisällössä.[49]

4.5 Suomen perustuslaki asettaa Suomen kansalaisten perusoikeudet

Suomen perustuslaki (1999/731) säädettiin sellaiseen muotoonsa kesäkuussa vuonna 1999. Perustuslaki vahvistaa Suomen valtiosäännön, joka turvaa ihmisarvon koskemattomuuden sekä yksilön vapauden ja oikeudet edistäen oikeudenmukaisuutta Suomen täysivaltaisessa tasavallan yhteiskunnassa. Perustuslaki säätää Suomen kansalaisten perusoikeudet, kuten

---

[46] Laki sähköisen viestinnän palveluista 2014/917 § 1
[47] Op.cit., § 272-275
[48] Rikoslaki 1889/39
[49] Op.cit., § 8-9

yhdenvertaisuuden, oikeuden elämään sekä henkilökohtaiseen vapauteen ja koskemattomuuteen, yksityiselämän suojan, uskonnon ja omantunnon vapauden sekä sananvapauden ja julkisuuden.[50]

Tämän tutkielman teeman kannalta tarkastelluin kohta on artikla 10 Yksityiselämänsuoja, joka turvaa rekisteröidyn yksityishenkilön yksityiselämän, kunnian ja kotirauhan. Oikeudellisesti täydentävää lainsäädäntöä löytyy tietosuojalaista (2018/1050).[51]

4.6 Tietosuojalaki ohjaa Suomen tietosuojalainsäädäntöä

Tietosuojalaki (2018/1050) tuli voimaan joulukuussa 2018 kumoten aiemman vuonna 1999 voimaan tulleen henkilötietolain[52]. Tietosuojalain kautta selitetään Euroopan unionin yleistä tietosuoja-asetusta (EU 2016/679) sekä sen kansallista soveltamista. Se myös tarkentaa ja täydentää rekisteröidyn yksityishenkilön henkilötietojen suojaamista.[53]

Henkilötietolainsäädäntö eli nykyinen tietosuojalainsäädäntö määrittää rekisterinpitäjille rajat, joita tulee noudattaa ja joiden sisällä on oikeus käsitellä esimerkiksi rekisteröidyn yksityishenkilön arkaluontoisia henkilötietoja[54]. Arkaluontoisiksi tiedoiksi luetaan etnisyydestä, uskonnollisesta vakaumuksesta, terveydentilasta, poliittisesta kannasta sekä ammattiliiton jäsenyydestä. Näiden tietojen käsittely on alustavasi kielletty, mutta sallitaan tehtäväksi rekisteröidyn yksityishenkilön suostumuksella tai mikäli käsittelyyn on tärkeä yleinen etu.[55]

5 Tietosuoja on henkilötietojen asiallista käsittelyä

Tietosuoja eli englanniksi data protection on yleisen tietosuojalain ja sen erityislakien henkilötietojen käsittelyä koskevien oikeuksien ja velvollisuuksien huomioimista rekisterinpitäjän (yhteisö, yhdistys, yritys, yksityishenkilö tai julkisoikeudellinen taho, joka kerää tietoja jäsenistään tai asiakkaistaan) operatiivisessa toiminnassa sekä luonnollisten henkilöiden (rekisteröitynyt yksityishenkilö) yksityisyyden suojaamisessa ja oikeusturvan varmistamisessa[56].

Euroopan unionin yleinen tietosuoja-asetus (EU 2016/679) osoittaa artiklassa neljä henkilötietojen tarkoituksen seuraavasti:

---

[50] Suomen perustuslaki 1999/731
[51] Op.cit., § 10
[52] Henkilötietolaki 1999/523
[53] Tietosuojalaki 2018/1050 § 1,3
[54] Andreasson & Ylipartanen 2022, 23
[55] Järvinen 2022, 137
[56] Supra note 54, s. 23

--’henkilötiedoilla’ kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.--

Tietosuojavaltuutetun toimisto määrittää henkilötiedoiksi kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön eli rekisteröityyn yksityishenkilöön. Näitä tietoja voi löytyä tallennettuna muun muassa sähköisistä tiedostoista, tietokannoista, paperidokumenteista sekä ääni- ja kuvatallenteilta.[57]

Henkilötietoja ovat esimerkiksi:

- nimi
- kotiosoite
- puhelinnumero
- sähköpostiosoite
- henkilökortin numero
- auton rekisterinumero
- paikannustiedot
- IP-osoite
- potilas- ja terveystiedot
- lemmikin eläinlääkäritiedot
- suvussa olevia perinnöllisiä sairauksia koskevat tiedot.[58]

Henkilötietoja eivät ole esimerkiksi:

- yrityksen rekisteritunnus eli y-tunnus
- yleinen sähköpostiosoite
- anonymisoidut tiedot eli tiedot, joista henkilöä ei pystytä enää tunnistamaan.[59]

Andreassonin ja Ylipartasen mukaan tietosuojassa on kyse asiakkaan ja yrityksen välisestä luottamuksesta sekä henkilöstön kokonaisvaltaisesta tietosuojaosaamisesta[60]. Tietosuojaosaamisella tarkoitetaan asiakastietojen korrektia, oikeaoppista, perusteltua ja sujuvaa käsittelyä tiedon koko elinkaaren ajan. Tiedonkäsittelyn elinkaari koostuu eri vaiheista, jotka

---

[57] Tietosuojavaltuutetun toimisto
[58] Ibid.
[59] Ibid.
[60] Andreasson & Ylipartanen 2022, 21

kokonaisuudessaan muodostavat tietosuojan. Tiedonkäsittelyvaiheisiin lukeutuu muun muassa asiakastietojen kerääminen, tallentaminen, käyttö ja yhdistäminen sekä siirto, luovuttaminen, säilyttäminen, hävittäminen ja muu tiedon elinkaareen liittyvä käsittely.[61]

5.1 Rekisterinpitäjä ja hänen velvollisuutensa

Euroopan unionin yleinen tietosuoja-asetus (EU 2016/679) määrittelee artiklassa neljä rekisterinpitäjän seuraavasti:

--'rekisterinpitäjällä' luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot--

Tietosuojavaltuutetun toimisto tiivistää rekisterinpitäjän kuvauksen henkilöksi, yhteisöksi, yritykseksi tai viranomaiseksi, joka osoittaa henkilötietojen käsittelyn tarkoituksen ja toimenpiteet[62].

Tietosuojan piirissä rekisterinpitäjä on siis asianosainen, joka kerää ja käsittelee henkilötietoja. Rekisterinpitäjä voi olla esimerkiksi yhteisö, yhdistys, yritys, yksityishenkilö tai julkisoikeudellinen, jonka kuuluu määritellä henkilötietojen käsittelyn tarkoitus ja tavat sen toteuttamiseen ja valvomiseen. Rekisterinpitäjän ylläpitämään rekisteriin kerätään tiedot rekisteröidyiltä yksityishenkilöiltä, jonka myötä rekisteröidyllä on oikeuksia ja rekisterinpitäjällä velvollisuuksia.[63]

Rekisterinpitäjällä on useita velvollisuuksia ja ne alkavat jo toiminnan suunnitteluvaiheessa. Tietosuoja tulee huomioida alusta alkaen sekä täytyy tiedostaa, että toiminnan tulee olla asianmukaista ja rekisteröidyn suhteessa läpinäkyvää. Rekisterinpitäjä saa käsitellä ja kerätä vain toimintansa kannalta perusteltuja tietoja, joiden tulee olla relevantteja. Mikäli virheitä tiedoissa havaitaan, täytyy ne oikaista viipymättä. Tunnistettavassa muodossa olevia tietoja on oikeus käsitellä vain tietojenkäsittelyn tarkoituksen toteuttamisen ajan. Tiedot tulee tuhota turvallisesti, kun niitä ei enää tarvita.[64]

Työelämässä ja arkielämässä yksityisyyden suojan huomioiminen on paitsi rekisterinpitäjän laillinen velvollisuus, mutta myös osoitus ja vakuutus laadukkaasta henkilöstöasioiden hoidosta. Yksityisyyden kunnioittaminen ja luottamuksellisuus henkilötietoja käsitellessä ovat osa demokraattisen yhteiskunnan olennaisia arvoja.[65]

---

[61] Andreasson & Ylipartanen 2022, 21
[62] Tietosuojavaltuutetun toimisto
[63] Järvinen 2022, 136-137
[64] Op.cit., 139
[65] Kauhanen 2012, 211

Vastuullinen tietosuojatoiminta edellyttää avointa ja läpinäkyvää kommunikointia henkilötietojen käsittelyyn osallistuvien osapuolten kanssa. Avoin vuorovaikutus mahdollistaa rakentavan keskustelun uusista ratkaisuista, järjestelmistä ja tuotteista sekä niiden implementoimisesta organisaation toimintoihin. Tätä kautta tietosuoja muuntuu organisaation toimintoja rajoittavasta tekijästä liiketoimintaa ja sen mainetta kohottavaksi tekijäksi.[66]

Henkilötietojen käsittelijä

Kun rekisterinpitäjä määrittelee henkilötietojen käsittelyn, sen keinot ja tarkoitukset, toimii henkilötietojen käsittelijä rekisterinpitäjän ohjeistuksen mukaan ja heidän alaisuudessaan. Henkilötietojen käsittelijä on siis se osapuoli, joka konkreettisesti käsittelee henkilötietoja. Hänen ei tarvitse välttämättä olla rekisterinpitäjän sisäisessä palveluksessa, vaan henkilötietojen käsittelijän toimen voi ulkoistaa ulkopuoliselle palveluntarjoajalle. Henkilötietojen käsittelijän suorittamat toimenpiteet on määriteltävä erikseen sopimuksella tai oikeudellisella asiakirjalla ja hän voi käsitellä henkilötietoja vain rekisterinpitäjän määrittelemien tarkoitusten perusteella, ei omia tarkoituksiaan varten.[67]

Henkilötietojen käsittelijällä ei ole päätösvaltaa henkilötietojen käsittelyn elinkaaren eri vaiheiden suhteen, vaan kaikki päätäntävalta on rekisterinpitäjällä. Rekisterinpitäjä ohjeistaa henkilötietojen käsittelijää, kuinka tietojen käsittelyn eri vaiheissa toimitaan. Rekisterinpitäjä voi hyödyntää toimissaan vain sellaisia henkilötietojen käsittelijöitä, jotka ovat implementoineet tietosuoja-asetuksen mukaiset suojaustoimenpiteet käyttöönsä. Valittujen käsittelijöiden tulee pystyä todistamaan vaadittavien suojaustoimenpiteiden asianmukainen käyttö toiminnoissaan.[68]

Rekisterinpitäjä voi toimissaan käyttää useita henkilötietojen käsittelijöitä sekä määrittää heidän vastuualueensa joko suppeasti tai laajasti. Kaikki palveluntarjoajat eivät ole henkilötietojen käsittelijöitä, vaan heidän toimintansa luonne määrittelee, onko kyseessä rekisterinpitäjän nimissä tapahtuvaa käsittelyä.[69]

5.1.1 Käsittelyperuste velvoittaa henkilötietojen käsittelyn olevan perusteltua

Rekisterinpitäjällä täytyy olla aina perusteltu syy henkilötietojen käsittelyyn. Ilman pätevää syytä, on henkilötietojen käsittely laitonta.[70] Käsittelyn lainmukaisuuden perusteltuja syitä ovat rekisteröidyn suostumus, sopimuksen toteuttamiseen liittyvä tarve, lakisääteinen

---

[66] Andreasson & Ylipartanen 2022, 59
[67] Tietosuojavaltuutetun toimisto b
[68] Korpisaari, Pitkänen & Warma-Lehtinen 2022, 343-344
[69] Op.cit., 343
[70] Järvinen 2022, 139

velvoite, elintärkeiden etujen suojaaminen, yleinen etu tai julkiseen valtaan liittyvä peruste sekä oikeutettu etu[71].

Rekisterinpitäjän käsittelyperusteesta säädetään Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679) artiklassa 6, 7 ja 30.

Suostumus

Ensimmäinen hyväksyttävä peruste on rekisteröidyn suostumus. Suostumus tarkoittaa lupaa, mutta pään nyökkäys ei suinkaan riitä luvan muodostumiseksi. Luvan on oltava selkeä, kiistaton ja dokumentoitavissa sekä rekisteröidyn tulee ymmärtää mihin lupa liittyy. Rekisteröidyn suostumuksen ei kuitenkaan ole syytä olla ensisijainen perustelu, sillä rekisteröity voi peruuttaa suostumuksensa milloin tahansa.[72]

Sopimuksen toteuttamiseen liittyvä tarve

Sopimuksen toteuttamiseen liittyvä tarve on mahdollisesti eniten hyödynnetty perustelu, sillä yritykset ja yhteisöt käyttävät tätä hoitaakseen asiakkuuden tai jäsenyyden kannalta kriittisiä tehtäviä sekä täyttämään heille osoitetut omat velvollisuutensa. Tähän perusteeseen perustuu myös nettipalveluiden ja sosiaalisen median sisältämä rekisteröidyn henkilötietojen käsittely.[73]

Lakisääteinen velvoite

Lakisääteinen velvoite on yksi selkeimmistä perusteluista käsitellä henkilötietoja, sillä viranomaisilla on oikeus käsitellä rekisteröidyn kansalaisen henkilötietoja lainsäädännössä määriteltyjen tehtävien ja toimenpiteiden toteuttamiseksi[74].

Elintärkeiden etujen suojaaminen

Elintärkeiden etujen suojaaminen perusteluna kuuluu suurimmaksi osaksi poliisi- ja pelastustoiminnalle. He voivat käsitellä rekisteröidyn henkilötietoja suojatakseen ja varjellakseen elintärkeitä etuja tilanteissa, joissa muiden henkilöiden terveys, turvallisuus tai koskemattomuus on vaarassa.[75]

---

[71] Järvinen 2022, 140-141
[72] Op.cit., 140
[73] Ibid.
[74] Ibid.
[75] Supra note 71, s. 141

Yleinen etu tai julkiseen valtaan liittyvä peruste

Perusteluna yleinen etu tai julkiseen valtaan liittyvä peruste on käsitteenä jossain määrin tulkinnanvarainen. Tähän perusteeseen kuitenkin tukeutuvat muun muassa terveydenhuollon hallinto, kansanterveyteen liittyvät palvelut ja luottotietoja myyvät yritykset.[76]

Oikeutettu etu

Oikeutettu etu on perusteluna kaikista tulkinnanvaraisin. Suurimmaksi osaksi siksi, että Suomen aiemmassa henkilötietoja koskevassa laissa ei ollut vastaavaa pykälää. Tämä tekee oikeutetusta edusta rekisterinpitäjän mahdollisuuksia laajentavan säännöksen. Oikeutettua etua on usein hyödynnetty tilanteissa, joissa yrityksellä on tarve käsitellä henkilötietoja ilman erillistä asiakassuhdetta tai suostumusta kyseessä olevalta henkilöltä. Kyseinen perustelu voi olla käytössä muun muassa markkinoinnissa, tilastoinnissa, tieteellisessä tutkimuksessa, asiakaspalvelussa tai kameravalvonnassa.[77]

5.1.2 Suunnitteluvelvoite velvoittaa henkilötietojen käsittelyn olevan suunniteltua

Rekisterinpitäjän tulee aina suunnitella henkilötietojen käsittely ja siihen liittyvät toimenpiteet etukäteen ja ainoastaan toiminnan kannalta välttämättömiä tietoja on luvallista kerätä. Henkilötietoihin liittyy käyttötarkoitussidonnaisuus eli tietoja saa käyttää vain ja ainoastaan siihen tarkoitukseen, johon tiedot on alun perin kerätty.[78]

Rekisterinpitäjän suunnitteluvelvoitteesta säädetään Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679) artiklassa 5.

5.1.3 Huolellisuusvelvoite velvoittaa henkilötietojen suojaamisen ja tietoturvan riittävän käyttöönoton

Rekisterinpitäjällä on velvollisuus suojata henkilötiedot ja niiden käsittely koko niiden elinkaaren ajan. Toisin sanoen rekisterinpitäjällä on lakisääteinen velvoite huolehtia tietoturvan riittävästä käyttöönotosta. Henkilötietolainsäädännön perimmäisenä ja tärkeimpänä tavoitteena on lopettaa ja ehkäistä tietoturvaloukkausten ja niihin liittyvien vahinkojen tapahtuminen. Mikäli rekisterinpitäjä noudattaa tietosuoja-asetuksen määrittämiä ehtoja, ei vahinkoja pääse sattumaan. Tietosuoja ja tietoturva muodostavat täten yhdessä pitävän suojamuurin rekisterinpitäjän hallussa olevien henkilötietojen ympärille. On kuitenkin olemassa

---

[76] Järvinen 2022, 141
[77] Ibid.
[78] Supra note 76, s. 142

rekisterinpitäjästä riippumattomia syitä, jotka voivat itsessään luoda haavoittuvuutta järjestelmien ympärille. Näitä ovat muun muassa ulkoisten palveluiden ja tekniikan varassa toiminen.[79]

Rekisterinpitäjän huolellisuusvelvoitteesta säädetään Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679) artiklassa 5, 24, 25 ja 32.

5.1.4 Ilmoitusvelvollisuus velvoittaa tietoturvaloukkauksista ilmoittamisen viranomaisille

Rekisterinpitäjällä on velvollisuus ilmoittaa mahdollisesta tietoturvaloukkauksesta valvovalle viranomaiselle eli tässä tapauksessa tietosuojavaltuutetun toimistolle. Ilmoitus tulee tehdä mahdollisimman nopeasti sen havainnosta, mutta kuitenkin viimeistään 72 tunnin kuluessa. Tietoturvaloukkauksen tapahtuessa rekisterinpitäjän tulee arvioida tilannetta ja rekisteröidylle aiheutuvaa riskiä. Mikäli riski rekisteröidyn oikeuksille ja vapauksille arvioidaan korkeaksi ja kriittiseksi, rekisterinpitäjän tulee ilmoittaa tapahtuneesta viipymättä jokaiselle henkilölle tai taholle, jonka tietoihin tietoturvaloukkaus voi vaikuttaa.[80]

Rekisterinpitäjän ilmoitusvelvollisuudesta säädetään Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679) artiklassa 33.

5.1.5 Osoitusvelvollisuus velvoittaa todentamaan tietosuojan ja tietoturvan eteen tehtävän työn

Rekisterinpitäjällä on velvollisuus pystyä todentamaan tietosuojan ja tietoturvan eteen tehtävä työ. Tätä velvollisuutta kutsutaan osoitusvelvollisuudeksi.[81] Sen pääsääntöisenä tehtävänä on velvoittaa rekisterinpitäjää noudattamaan todistetusti tietosuojalainsäädäntöä ja se on yksi tietosuoja-asetuksen keskeisimmistä periaatteista. Rekisterinpitäjä näyttää osoitusvelvollisuuden kautta kunnioittavansa rekisteröityjen tietosuojaa ja kasvattaa tätä kautta rekisterinpitäjän toiminnan luotettavuutta.[82]

Rekisterinpitäjän tulee toteuttaa vaaditut tekniset ja organisatoriset toimenpiteet ja muutokset täyttääkseen osoitusvelvollisuuden sisältämät vaatimukset. Sen mukana tulee muun muassa dokumentointivelvollisuus, määrättyjen toimenpiteiden tekemistä ja kirjaamista. Tietosuoja-asetus sisältää myös osoitusvelvollisuutta koskevia vaatimuksia, joiden velvoittavuus käsitellään ja arvioidaan tapauskohtaisesti. Rekisterinpitäjän osoitusvelvollisuuden laajuus

---

[79] Järvinen 2022, 143-144
[80] Op.cit., 145
[81] Andreasson & Ylipartanen 2022, 152
[82] Tietosuojavaltuutetun toimisto c

riippuu muun muassa organisaation koosta, käsiteltävien henkilötietojen määrästä sekä niiden laadusta. Osoitusvelvollisuus on hyvä pitää mielessä henkilötietojen koko elinkaaren ajan.[83]

Rekisterinpitäjän osoitusvelvollisuudesta säädetään Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679) artiklassa 5 ja 24.

5.1.6 Tietosuojavastaava ohjaa organisaation tietosuojan toteutusta

Organisaatioissa, joissa henkilötietojen käsitteleminen on laajaa tai sisältää suuren määrän arkaluonteisten tietojen käsittelyä, tulee nimetä tietosuojavastaava. Tietosuojavastaava on asiantuntija, joka seuraa ja valvoo organisaation henkilötietojen käsittelyä sekä neuvoo ja ohjaa organisaation johtoa tietosuojaan liittyvissä kysymyksissä. Tietosuojavastaava toimii yhteistyössä viranomaisten kanssa sekä on ensisijainen yhteyshenkilö tietoturvaloukkauksen kohteeksi joutuneille yksityishenkilöille. Tietosuojavastaavalla ei ole viranomaisten määrittelemää koulutusvaatimusta, mutta tietosuojavastaavana toimivalla henkilöllä tulee olla tuntemusta tietojärjestelmien toiminnasta, tietoturvasta ja tietosuojaan liittyvästä lainsäädännöstä. Tietosuojavastaavan henkilöllisyys on julkista tietoa ja se yhteystietoineen tulee ilmoittaa Tietosuojavaltuutetun toimiston ylläpitämään rekisteriin.[84]

Tietosuojavastaavan tehtäviin kuuluu myös henkilötietojen käsittelyyn kuuluvien ohjeiden suunnittelu, laatiminen ja jalkauttaminen henkilöstölle. Tietosuojavastaava on vastuussa henkilöstön kouluttamisesta henkilötietojen oikeaoppiseen käsittelyyn sekä vastaa ohjeiden ajankohtaisesta päivittämisestä. Henkilöstön koulutus tulee aloittaa jo uuden henkilön perehdyttämisestä. Tietosuojavastaavan on hyvä pitää uudelle työntekijälle erillinen koulutus organisaation henkilötietojen käsittelystä, niiden sisällöstä ja periaatteista. Tällöin varmistetaan, että tieto jalkautuu uuden työntekijän tietouteen ja työntekijän on mahdollista implementoida ohjeet käytäntöön heti työuransa alussa.[85]

5.2 Rekisteröity ja hänen oikeutensa

Euroopan unionin yleinen tietosuoja-asetus (EU 2016/679) takaa rekisteröidylle, jonka tietoja käsitellään, erilaisia tietosuojallisia oikeuksia[86]. Tietosuoja-asetus määrittelee artiklassa neljä rekisteröidyn luonnolliseksi henkilöksi, jolla on henkilötietoihin liittyviä oikeuksia. Tietosuojavaltuutetun toimisto tiivistää rekisteröidyn määritelmän henkilöksi, jota kyseessä oleva henkilötieto koskee[87].

---

[83] Tietosuojavaltuutetun toimisto c
[84] Järvinen 2022, 145
[85] Andreasson & Ylipartanen 2022, 131-132
[86] Op.cit., 190-191
[87] Tietosuojavaltuutetun toimisto

Rekisteröity on luonnollinen henkilö eli ihminen ja tietosuoja-asetus koskee alustavasti kaikkien digitaalisessa muodossa olevien henkilötietojen käsittelyä, ei siis pelkästään henkilörekistereiden hallussa olevien tietojen käsittelyä. Tämän pohjalta tietosuoja-asetuksessa luonnollisesta henkilöstä käytetty käsite rekisteröity, voi olla harhaanjohtava.[88]

Rekisteröidyn yksityishenkilön yksityiselämän suoja on Suomen perustuslain sisältämä perustuslaillinen oikeus, joka takaa ihmisen oikeuden elää elämäänsä ilman kenenkään perusteetonta puuttumista[89].

Rekisteröidyn oikeudet juontavat juurensa perustuslaillisesta oikeudesta ihmisen yksityiselämän suojaamiseen ja turvaamiseen. Henkilötietojen suoja on yksi perustuslain yksityiselämän suojan osa-alue.[90]

5.2.1 Oikeus saada tutustua tietoihin

Rekisteröidyllä on oikeus tutustua omiin tietoihinsa ja saada tietää mitä tietoja rekisterinpitäjä on hänestä kerännyt. Tätä oikeutta kutsutaan myös tarkastamisoikeudeksi tai tarkastusoikeudeksi. Sen kautta rekisteröity voi tarkistaa ovatko kaikki kerätyt tiedot tarpeellisia ja paikkansapitäviä. Rekisterinpitäjä voi luovuttaa jäljennöksen paperilla, sähköisenä tiedostona tai jopa suullisesti.[91]

Tietosuojavaltuutetun toimisto kertoo, että pyyntö jäljennöksen toimittamisesta tulee osoittaa suoraan rekisterinpitäjälle, jonka täytyy vastata pyyntöön yhden kuukauden kuluessa tai ainakin ilmoittaa tarvitsevansa asiansa käsittelyyn enemmän aikaa. Mikäli rekisterinpitäjä tarvitsee asian käsittelyyn enemmän aikaa, on määräaika kolmen kuukauden kuluttua alkuperäisen pyynnön esittämisestä. Jos rekisterinpitäjän vastausta ei kuulu kolmen kuukauden määräajassa, kannattaa rekisteröidyn olla yhteydessä tietosuojavaltuutettuun tietosuojaoikeuksien loukkaamisesta. Hyvä on kuitenkin muistaa, että ilmoitus pidemmästä käsittelyajasta ei tarkoita, että pyynnöstä on kieltäydytty.[92]

Tarkastuspyyntöön tulee sisällyttää rekisteröidyn nimi, yhteystiedot, tieto siitä mitkä tiedot halutaan tarkistaa ja halutaanko tarkistaa kaikki tiedot vai tiedot vain tietyltä aikaväliltä sekä missä muodossa tiedot halutaan toimitettavan[93].

Rekisteröidyllä on oikeus saada tietoa seuraavista asioista:

---

[88] Korpisaari, Pitkänen & Warma-Lehtinen 2022, 34
[89] Andreasson & Ylipartanen 2022, 23
[90] Supra note 88, s. 8
[91] Järvinen 2022, 148
[92] Tietosuojavaltuutetun toimisto d
[93] Ibid.

- Mistä henkilötietoja on hankittu?
- Miksi henkilötietoja tarvitaan?
- Kuinka kauan henkilötietoja tarvitaan?
- Onko henkilötietoja luovutettu tai aiotaanko luovuttaa eteenpäin? Jos kyllä, kenelle niitä on luovutettu tai aiotaan luovuttaa?
- Onko henkilötietoja siirretty EU:n ulkopuolelle? Jos kyllä, miten ne on suojattu?
- Käsitelläänkö henkilötietoja automaattisen käsittelyn avulla? Jos kyllä, miten se toimii?
- Miten rekisteröity voi hyödyntää henkilötietoihin liittyviä oikeuksia?[94]

Rekisteröidyn tietojen tarkastuspyynnöstä ei lähtökohtaisesti saa periä maksua. Mikäli tarkastuspyyntö on perusteeton tai kohtuuton, voi rekisterinpitäjä periä kohtuullisen maksun tai kieltäytyä pyynnön toteuttamisesta. Rekisteröidyn pyytäessä useampia jäljennöksiä, voi rekisterinpitäjä periä maksun, joka kattaa toimenpiteen kustannukset.[95] [96]

Mikäli rekisterinpitäjä kieltäytyy tietojen antamisesta, tulee heidän kertoa rekisteröidylle kieltäytymisen syyt. Kieltäytymisen tulee aina perustua lakiin[97].

Rekisteröidyn tarkastusoikeudesta säädetään Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679) artiklassa 15.

5.2.2 Oikeus tietojen poistamiseen

Rekisteröidyllä on oikeus tietojensa poistamiseen yritysten ja muiden rekisterinpitäjänä toimivien tahojen järjestelmistä eli oikeus tulla unohdetuksi. Tämä oikeus on hyväksi muun muassa tietopalveluiden ja suoramarkkinoiden rekistereissä. Rekisterinpitäjän on poistettava tiedot, kun he vastaanottavat vaatimuksen. Useat viranomaiset ovat kuitenkin tämän unohdusoikeuden ulkopuolella ja esimerkiksi rikosrekisteriä ei saa tyhjennettyä tietosuojaan vetoamalla.[98]

Tietosuojavaltuutetun toimisto kertoo, että pyyntö tietojen poistamisesta tulee osoittaa suoraan rekisterinpitäjälle, jonka täytyy vastata pyyntöön yhden kuukauden kuluessa tai ainakin ilmoittaa tarvitsevansa asiansa käsittelyyn enemmän aikaa. Mikäli rekisterinpitäjä tarvitsee asian käsittelyyn enemmän aikaa, on määräaika kolmen kuukauden kuluttua alkuperäisen pyynnön esittämisestä. Jos rekisterinpitäjän vastausta ei kuulu kolmen kuukauden

---

[94] Tietosuojavaltuutetun toimisto d
[95] Järvinen 2022, 148
[96] Supra note 94
[97] Ibid.
[98] Supra note 95, s. 147

määräajassa, suositellaan rekisteröidyn olevan yhteydessä tietosuojavaltuutettuun tietosuojaoikeuksien loukkaamisesta.[99]

Rekisterinpitäjän täytyy poistaa rekisteröidyn henkilötiedot seuraavissa tapauksissa:

- Rekisterinpitäjä ei enää tarvitse rekisteröidyn henkilötietoja alkuperäiseen tarkoitukseen.
- Rekisteröity peruuttaa antamansa suostumuksen eikä täten henkilötietojen käsittelylle ole muuta laillista perustetta.
- Rekisteröity vastustaa henkilötietojen käsittelyä eikä käsittelylle ole perusteltua syytä.
- Rekisteröity vastustaa henkilötietojen käsittelyä suoramarkkinointiin.
- Rekisteröidyn henkilötietoja on käsitelty lainvastaisesti.
- Rekisteröidyn henkilötiedot on poistettava lainsäädännön perusteella.
- Rekisteröidyn henkilötiedot on kerätty huoltajan suostumuksella tietoyhteiskunnan palvelujen tarjoamisen yhteydessä. Tietoyhteiskunnan palveluita ovat muun muassa verkkokaupat ja sosiaalinen media.[100]

Rekisterinpitäjän mahdollisesti kieltäytyessä tietojen poistamisesta, tulee heidän myös ilmoittaa kieltäytymisen syyt rekisteröidylle. Kieltäytymisen tulee myös aina pohjautua lakiin. Rekisterinpitäjä voi esimerkiksi kieltäytyä tietojen poistamisesta, jos ne ovat perusteltavasti tarpeellisia seuraavia tarkoituksia ja toimenpiteitä varten: lain noudattaminen, sananvapaus ja tiedon välittäminen, oikeusvaade, yleinen etu (esimerkiksi arkistointi, tutkimus ja tilastointi) sekä itse rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen.[101]

Rekisteröidyn tietojen poistaminen on yleensä maksutonta. Poikkeuksena on perusteeton tai kohtuuton poistopyyntö, jolloin rekisterinpitäjän voi periä kohtuullisen maksun tai yksinkertaisesti kieltäytyä pyynnön toteuttamisesta.[102]

Rekisterinpitäjän poistaessa rekisteröidyn tiedot, tulee heidän ilmoittaa poistosta kaikille niille tahoille, joille rekisteröidyn tietoja on aikaisemmin luovutettu. Rekisteröidyn oikeutena on myös saada tietää ne tahot, joille tietoja on luovutettu.[103]

Rekisteröidyn tietojen poistamisoikeudesta säädetään Euroopan unionin yleisen tietosuojaasetuksen (EU 2016/679) artiklassa 17.

---

[99] Tietosuojavaltuutetun toimisto e
[100] Ibid.
[101] Ibid.
[102] Ibid.
[103] Ibid.

5.2.3 Oikeus tietojen oikaisemiseen

Rekisteröidyllä on oikeus tietojen oikaisuun eli oikeus vaatia virheellisten ja epätäsmällisten tietojen oikaisua ja puutteellisten tietojen viipymätöntä täydennystä. Rekisteröidyllä on lisäksi oikeus vaatia, että tarpeettomat tiedot poistetaan tässä yhteydessä.[104]

Tietosuojavaltuutetun toimiston mukaan henkilötietojen virheettömyys on osa rekisteröidyn oikeusturvaa ja jokaisella on oikeus tulla arvioiduksi oikeiden tietojen perusteella. Oikaisupyyntö osoitetaan suoraan rekisterinpitäjälle ja sen tulee sisältää rekisteröidyn nimi, yhteystiedot, sanatarkasti oikaistava tieto ja sen tilalle ehdotettava muutos sekä muutosehdotuksien perustelut. Rekisterinpitäjän täytyy vastata oikaisupyyntöön yhden kuukauden kuluessa tai ainakin ilmoittaa tarvitsevansa asiansa käsittelyyn enemmän aikaa. Mikäli rekisterinpitäjä tarvitsee asian käsittelyyn enemmän aikaa, on määräaika kolmen kuukauden kuluttua alkuperäisen pyynnön esittämisestä. Jos rekisterinpitäjän vastausta ei kuulu kolmen kuukauden määräajassa, kannattaa rekisteröidyn olla yhteydessä tietosuojavaltuutettuun tietosuojaoikeuksien loukkaamisesta.[105]

Rekisteröidyn tietojen oikaisu on usein maksutonta. Perusteettomasta tai kohtuuttomasta oikaisupyynnöstä rekisterinpitäjä voi periä kohtuullisen maksun tai selkeästi vain kieltäytyä pyynnön toteuttamisesta. Mikäli rekisterinpitäjä mahdollisesti kieltäytyy tietojen oikaisemisesta, tulee heidän ilmoittaa kieltäytymisen syyt rekisteröidylle. Kieltäytymisen tulee myös aina pohjautua lakiin.[106]

Rekisterinpitäjän oikaistaessa rekisteröidyn tietoja, tulee heidän ilmoittaa oikaisusta kaikille niille tahoille, joille rekisteröidyn tietoja on aikaisemmin luovutettu. Rekisteröidyn oikeutena on myös saada tietää ne tahot, joille tietoja on luovutettu.[107]

Rekisteröidyn tietojen oikaisemisoikeudesta säädetään Euroopan unionin yleisen tietosuojaasetuksen (EU 2016/679) artiklassa 16.

5.2.4 Oikeus tietojen siirtämiseen

Rekisteröidyllä on oikeus tietojen siirtämiseen rekisterinpitäjän järjestelmästä toisen palveluntarjoajan järjestelmään. Tiedot tulee saada yleisesti käytetyssä ja sujuvasti koneellisesti luettavassa muodossa, jotta siirtäminen on vaivatonta. Oikeus tietojen siirtämiseen koskee vain rekisteröidyn itse tuottamaa tai järjestelmään luovuttamaa sisältöä. Tämä helpottaa palveluntarjoajan vaihtamista, sillä tiedot on mahdollista saada kulkeutumaan sujuvasti ilman

---

[104] Andreasson & Ylipartanen 2022, 192
[105] Tietosuojavaltuutetun toimisto f
[106] Ibid.
[107] Ibid.

rekisteröidyn omia ponnisteluja.[108] Siirtäminen onnistuu rekisteröidyn itse toimittamana tai rekisteröity voi pyytää aiempaa rekisterinpitäjää toimittamaan tiedot uudelle palveluntarjoajalle[109].

Tietosuojavaltuutetun toimisto kertoo, että pyyntö tietojen siirtämisestä toiselle palveluntarjoajalle tulee osoittaa suoraan rekisterinpitäjälle. Siirtopyyntöön tulee sisältää rekisteröidyn nimen, yhteystiedot, yksilöidysti mistä tiedosta on kyse sekä haluaako rekisteröity siirtää tiedot itse vai onko toiveissa, että rekisterinpitäjä siirtää tiedot suoraan uudelle palveluntarjoajalle.[110]

Henkilötietojen siirtäminen tulee olla perusteltua ja edellytyksiä niiden siirtämiselle on, että:

- Henkilötietojen käsittely on perustunut joko rekisteröidyn suostumukseen tai rekisteröidyn ja rekisterinpitäjän väliseen sopimukseen.
- Henkilötietoja on käsitelty automaattisen tietojenkäsittelyn avulla.
- Henkilötiedot koskevat rekisteröityä ja ovat heidän toimittamiaan.
- Henkilötietojen siirto ei vaikuta negatiivisesti kolmansien osapuolien oikeuksiin tai vapauksiin.[111]

Kaikkien edellä mainittujen edellytysten on täytyttävä, jotta henkilötietojen on perusteltua ja sallittua. Vain tällöin rekisteröity voi hyödyntää oikeuttaan tietojen siirtoon. Tämä oikeus ei sisällä tietoja, jotka rekisterinpitäjä on itse luonut rekisteröidyn toimittamien tietojen pohjalta, kuten terveyttä koskevat arviot, tai tietoja, jotka on koostettu rekisteröidyn tarkkailusta ja datansyötöstä muodostuneiden tietojen analysoinnista, kuten profilointi.[112]

Rekisterinpitäjän täytyy vastata pyyntöön yhden kuukauden kuluessa tai ainakin ilmoittaa tarvitsevansa asiansa käsittelyyn enemmän aikaa. Mikäli rekisterinpitäjä tarvitsee asian käsittelyyn enemmän aikaa, on määräaika kolmen kuukauden kuluttua alkuperäisen pyynnön esittämisestä. Jos rekisterinpitäjän vastausta ei kuulu kolmen kuukauden määräajassa, kannattaa rekisteröidyn olla yhteydessä tietosuojavaltuutettuun tietosuojaoikeuksien loukkaamisesta. Mikäli rekisterinpitäjä kieltäytyy tietojen siirtämisestä, tulee heidän kertoa rekisteröidylle kieltäytymisen syyt. Kieltäytymisen tulee aina perustua lakiin.[113]

Rekisteröidyn siirtäessä henkilötietonsa rekisterinpitäjältä toiselle, ei hänen henkilötietonsa välttämättä poistu alkuperäisen rekisterinpitäjän rekisteristä ja järjestelmistä.

---

[108] Järvinen 2022, 147
[109] Tietosuojavaltuutetun toimisto g
[110] Ibid.
[111] Ibid.
[112] Ibid.
[113] Ibid.

Rekisteröidyllä on kuitenkin oikeus pyytää tietojen poistoa alkuperäiseltä rekisterinpitäjältä siirtäessään tietoja toiselle palveluntarjoajalle. Rekisteröidyn tietojen siirtäminen on usein maksutonta. Poikkeuksena on perusteeton tai kohtuuton pyyntö, jolloin rekisterinpitäjän voi periä kohtuullisen maksun tai yksinkertaisesti kieltäytyä pyynnön toteuttamisesta.[114]

Järvisen mukaan siirto-oikeuden taustalla on tavoite lisätä verkkopalveluiden välistä kilpailua[115]. Tämä ei kuitenkaan ole niin yksikertaista ja yksiselitteistä, sillä useimmat palvelut ovat niin erilaisia, että tietojen siirto niiden välillä ei onnistu sellaisenaan.

Rekisteröidyn tietojen siirto-oikeudesta säädetään Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679) artiklassa 20.

5.2.5 Oikeus tietojen käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus rajoittaa henkilötietojensa käsittelyä tietyissä tapauksissa siksi aikaa, kunnes hänen tietonsa on hyväksyttävästi tarkistettu ja oikaistu tai täydennetty. Rajoittaminen tarkoittaa tässä tapauksessa sitä, että rekisterinpitäjä saa käsitellä tietoja vain rekisteröidyn suostumuksella, oikeusvaateessa, toisen henkilön oikeuksien suojaamisessa tai yleisen edun vuoksi.[116] [117]

Rekisteröity voi rajoittaa henkilötietojen käsittelyä seuraavissa tilanteissa:

- Henkilötiedot ovat virheellisiä.
- Henkilötietoja käsitellään lainvastaisesti, mutta niitä ei haluta poistettavan kokonaan.
- Rekisterinpitäjä ei tarvitse henkilötietoja alkuperäiseen tarkoitukseen, mutta rekisteröity tarvitsee tietoja oikeusvaateeseen.
- Rekisteröity on vastustanut tietojen käsittelyä eli hyödyntänyt vastustamisoikeutta, mutta lopullinen päätös on vielä harkinnassa.[118]

Pyyntö tietojen käsittelyn rajoittamisesta tulee osoittaa suoraan rekisterinpitäjälle ja sen täytyy sisältää rekisteröidyn nimi, yhteystiedot, tieto mitä tietoa halutaan rajoittaa sekä perustelut rajoittamiselle, poikkeuksena suoramarkkinointi, jonka rajoittamista ei tarvitse perustella. Rekisterinpitäjän täytyy vastata pyyntöön yhden kuukauden kuluessa tai ainakin ilmoittaa tarvitsevansa asiansa käsittelyyn enemmän aikaa. Mikäli rekisterinpitäjä tarvitsee asian käsittelyyn enemmän aikaa, on määräaika kolmen kuukauden kuluttua alkuperäisen

---

[114] Tietosuojavaltuutetun toimisto g
[115] Järvinen 2022, 147
[116] Andreasson & Ylipartanen 2022, 192-193
[117] Tietosuojavaltuutetun toimisto h
[118] Ibid.

pyynnön esittämisestä. Jos rekisterinpitäjän vastausta ei kuulu kolmen kuukauden määräajassa, kannattaa rekisteröidyn olla yhteydessä tietosuojavaltuutettuun tietosuojaoikeuksien loukkaamisesta. Mikäli rekisterinpitäjä kieltäytyy tietojen rajoittamisesta, tulee heidän kertoa rekisteröidylle kieltäytymisen syyt, joiden tulee aina perustua lakiin.[119]

Rekisterinpitäjän rajoittaessa rekisteröidyn tietoja, tulee heidän ilmoittaa rajoittamisesta kaikille niille tahoille, joille rekisteröidyn tietoja on aikaisemmin luovutettu. Rekisteröidyn oikeutena on myös saada tietää ne tahot, joille tietoja on luovutettu.[120]

Rekisteröidyn tietojen rajoittamisoikeudesta säädetään Euroopan unionin yleisen tietosuojaasetuksen (EU 2016/679) artiklassa 18.

5.2.6 Oikeus vastustaa tietojen käsittelyä

Rekisteröidyllä on oikeus vastustaa henkilötietojen käsittelyä henkilökohtaiseen tilanteeseen liittyvän erityisen syyn perusteella. Tätä oikeutta kutsutaan vastustamisoikeudeksi tai kielto-oikeudeksi ja se tarkoittaa, että tietoja ei käsitellä ollenkaan. Oikeus on voimassa myös silloin, kun tietojen käsitteleminen perustuu yleistä etua koskevan tehtävän tai toimenpiteen suorittamiseen, rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseen tai oikeutetun edun hyödyntämiseen, esimerkiksi rekisteröidyn tietojen käyttämisessä suoramarkkinointiin.[121] [122]

Vastustamispyyntö tulee osoittaa suoraan rekisterinpitäjälle ja sen täytyy sisältää rekisteröidyn nimi, yhteystiedot sekä perustelut tietojen käsittelyn vastustamiselle, poikkeuksena suoramarkkinointi, jonka vastustamista ei tarvitse perustella. Rekisterinpitäjän täytyy vastata pyyntöön yhden kuukauden kuluessa tai ainakin ilmoittaa tarvitsevansa asiansa käsittelyyn enemmän aikaa. Mikäli rekisterinpitäjä tarvitsee asian käsittelyyn enemmän aikaa, on määräaika kolmen kuukauden kuluttua alkuperäisen pyynnön esittämisestä. Jos rekisterinpitäjän vastausta ei kuulu kolmen kuukauden määräajassa, kannattaa rekisteröidyn olla yhteydessä tietosuojavaltuutettuun tietosuojaoikeuksien loukkaamisesta. Mikäli rekisterinpitäjä kieltäytyy tietojen käsittelyn vastustamispyynnöstä, tulee heidän kertoa rekisteröidylle kieltäytymisen syyt, joiden tulee aina perustua lakiin.[123]

Vastustamisoikeudesta eli kielto-oikeudesta voi olla rekisteröidylle peräti päivittäistä hyötyä suoramarkkinoinnin vähentämisessä. Eri rekistereistä voi laittaa voimaan yhteystietojen

---

[119] Tietosuojavaltuutetun toimisto h
[120] Ibid.
[121] Andreasson & Ylipartanen 2022, 193-194
[122] Supra note 119
[123] Ibid.

luovutuskiellon, kieltää tietojenluovutuksen tai rajoittaa muun muassa puhelinmarkkinointia. Kaikki nämä pohjautuvat rekisteröidyn oikeuteen vastustaa henkilötietojen käsittelyä.[124]

Rekisteröidyn tietojen vastustamisoikeudesta säädetään Euroopan unionin yleisen tietosuojaasetuksen (EU 2016/679) artiklassa 21.

5.3 Tietosuojariskit ovat henkilötietojen käsittelyn vaarantavia tekijöitä

Tietosuojariskejä ovat asiat ja toimenpiteet, jotka osaltaan vaarantavat organisaation henkilötietojen käsittelyn eheyden ja luotettavuuden. Näitä ovat muun muassa vääränlaiset tietojärjestelmien käyttöoikeuksien valtuudet sekä turhat tietojärjestelmien voimassa olevat käyttöoikeudet, joista esimerkkinä toimii poislähteneet työntekijät ja heidän käytössään olleet eri järjestelmien käyttöoikeudet. Tietosuojariskit kasvavat kehittyvän digitalisaation ja teknologistuvan yhteiskunnan myötä ja uusia tunnistetaan jatkuvasti. Uusia tunnistettuja tietosuojariskejä ovat muun muassa ohjelmistorobotiikka, tekoäly, esineiden internet (Internet of Things) ja data-analytiikka.[125]

Henkilötietoja käsitellessä tietosuojaan kohdistuvat riskit realisoituvat radikaalisti, minkä vuoksi organisaation riskienhallinta on äärimmäisen tärkeää. Riskienhallinta on osa yrityksen toiminnan ja johtamisen prosesseja, suunnittelua ja seurantaa. Riskienhallinta tavoittelee tulevien riskien kartoittamista, niihin varautumista sekä aiemmista virheistä oppimista. Riskejä kuvatessa tulee kyetä tuomaan niitä myös käytännön ja praktisuuden tasolle. Näin ollen kyseisiin riskeihin voidaan varautua systemaattisesti ja asettaa niille vastuuhenkilöt valvomaan niiden kehittymistä. Tämä helpottaa ja suoraviivaistaa riskienhallinnan johtamista ja riskien seurantaa tehden myös riskienhallinnan raportoinnista yksinkertaisempaa.[126]

Vaikutuksenarviointi

Korkeariskinen henkilötietojen käsittely vaatii käyttäjien tietosuojan, oikeuksien ja vapauksien vaikutustenarvioinnin eli englanniksi data protection impact assesment tai DPIA suorittamista. Sen tarkoituksena on tunnistaa, arvioida ja minimoida henkilötietojen käsittelyyn sidoksissa olevia riskejä. Sen tehtävä on myös synnyttää aineistoa, jolla tietosuojalainsäädännön noudattaminen voidaan todistaa.[127]

---

[124] Rousku 2014, 134-135
[125] Andreasson & Ylipartanen 2022, 63, 67
[126] Op.cit., 60-62
[127] Op.cit., 59, 70

5.4 Tietosuojaloukkaukset vaarantavat yksilön oikeudet

Tietosuojaloukkaukset ovat tietosuojalainsäädännön rikkomisesta johtuvia rangaistavia tekoja. Se on tapahtuma, jonka seurauksena henkilötietoja tuhoutuu, ne häviävät tai muuttuvat tai niihin pääsee luvattomasti käsiksi niihin oikeudeton taho. Tietosuojaloukkaukset vaarantavat yksilön oikeudet ja vapaudet sekä johtavat pahimmassa tapauksessa tietomurtoihin, kun arkaluontoisia ja toiminnalle kriittisiä tietoja joutuu haitallisten tahojen ulottuville.[128]

Tietosuojalainsäädännön rikkomisesta säädetään rikoslain 1889/39 luvussa 38. Henkilötietojen käsittelyn eheyttä rikkova rikos tai väärinkäyttö voi johtaa rikosoikeudellisten seuraamusten lisäksi myös työoikeudellisiin ja vahingonkorvausoikeudellisiin seuraamuksiin. Työoikeudellinen seuraamus voi olla varoitus tai jopa työsuhteen irtisanominen.[129] Myös tietosuojavaltuutetun toimisto eli tietosuojaviranomaiset voivat määrätä tietosuojalainsäädäntöä rikkoville osapuolille seuraamusmaksuja. Seuraamusmaksut voivat olla erittäin suuria, sillä niiden yläraja on säädetty kansainvälisen liikevaihdon mukaan. Se voi olla jopa neljä prosenttia yrityksen kansainvälisestä liikevaihdosta.[130]

Tietosuojaloukkauksia voidaan ehkäistä järjestelmällisen ja tehokkaan tietoturvan kautta.

6 Tietoturva suojaa tietojärjestelmien sisältämää aineistoa

Tietoturvalla pyritään turvaamaan järjestelmien sisältämä tieto ulkopuolisilta tahoilta[131]. Tietosuojavaltuutetun toimisto määrittelee sen yhdeksi tietosuojan toteuttamisen keinoksi, sillä sen kautta suojataan tietojärjestelmiä ja tietoaineistoa niiden sisällä. Tietoturvalla tarkoitetaan esimerkiksi teknisiä toimenpiteitä, joiden kautta varmistetaan ja taataan tiedon luottamuksellisuus, järjestelmien toimivuus sekä tärkeimpänä rekisteröidyn yksityishenkilön oikeuksien toteutuminen.[132] Tietoturva on kokonaisuudessaan tietosuojan toteutumisen edellytys[133].

Tietoturva eli englanniksi data security käsittää tietosuojan näkökulmasta ne tekniset ja hallinnolliset toimenpiteet, joilla pyritään suojaamaan ja turvaamaan rekisteröidyn yksityishenkilön elämää, etuja, oikeuksia ja vapauksia. Näihin lukeutuu muun muassa tiedon laadun, rehtiyden ja luottamuksellisuuden ylläpitäminen ja suojaaminen teknisten ja hallinnollisten keinojen kautta. Tietoturva sisältää käytännön toimenpiteet, joiden kautta pyritään

---

[128] Andreasson & Ylipartanen 2022, 197
[129] Op.cit., 147
[130] Järvinen 2022, 146
[131] Niemi 2021, 118
[132] Tietosuojavaltuutetun toimisto
[133] Supra note 128, s. 175

toteuttamaan rekisteröidyn yksityishenkilön tietosuojan sisältämät vaatimukset. Koska tietoturva keskittyy käytännön toimenpiteisiin, on sen pääasiallisena tehtävänä turvata kriittisten tietojärjestelmien ja tietoverkkojen jatkuva toiminta, ehkäistä tietojärjestelmien luvatonta käyttöä ja tietojen tahatonta tai tahallista tuhoutumista tai vääristymistä sekä minimoida näistä mahdollisesti aiheutuvia vahinkoja. Tietoturvaa on hyödynnettävä kaikissa tiedonkäsittelyn elinkaaren vaiheissa asiakastietojen keräämisestä niiden hävittämiseen saakka.[134]

Tietoturva keskittyy tietojen, tiedostojen ja laitteiden suojaamiseen. Siinä on siis kyse datan suojaamisesta ja tietojärjestelmien toimivuuden jatkuvuudesta ja niiden toiminnan varmistamisesta.[135]

Tietoturva tavoittelee kolmea tavoitetta, jotka muodostavat englanninkielisen kirjainyhdistelmän CIA. Luottamuksellisuus eli confidentiality, eheys eli integrity ja saatavuus eli availability. Luottamuksellisuus tuo tietoturvaan uskoa ja arvostusta, sillä luottamus tietojen suojaamiseen on yksi tietoturvan avaintekijöistä. Tietojen tekninen salaaminen erilaisten algoritmien kautta on helppoa. Vaikeampaa on organisaation henkilöstön luottamuksellisuuden varmistaminen niin, etteivät he vuoda organisaatiolle kriittistä tietoa eteenpäin ulkoisille osapuolille. Tietojen eheys tietoturvan kannalta tarkoittaa tietojen loogista oikeudellisuutta ja niihin kohdistuvia oikeutettuja muutoksia. Tämä voi olla uhattuna, mikäli organisaation henkilöstöllä on käyttöoikeuksia järjestelmiin ja toimintoihin, joita he eivät työssään tarvitse. Eheys voi pettää myös hakkereiden murtautuessa organisaation verkkosivuille ja heidän sekoittaessaan niiden sisältämät tiedot tai syöttäessään sinne virheellistä tietoa. Tietoturvan kannalta saatavuus voi olla suurikin ongelma laitteiden ja palveluiden osalta: tietokone ei käynnisty, verkkoyhteydessä on häiriöitä, tietokoneen komponentti on rikki tai tiedostoja ei löydy. Saatavuus on suurimmaksi osaksi tekninen ongelma ja sitä yritetään hallita muun muassa hankkimalla vikasietoisia koneita sekä langattomia verkkoyhteyksiä. Langaton verkkoyhteyskin, kuten organisaation muutkin toiminnot voivat kuitenkin vaarantua ulkoisten ilmiöiden vuoksi. Näitä ovat muun muassa tulipalon runtelema konesali, pakkasen halkaisema vesiputki laitehuoneessa tai huoltokoneen katkaisema valokuitukaapeli. Tavoitteiden saavuttaminen saattaa siis kuulostaa yksinkertaiselta, mutta tekniset ja käytännölliset syyt tekevät niistä hankalia hallita.[136]

Kananen vertaa verkkojärjestelmissä ja sosiaalisessa mediassa tapahtuvaa toimintaa mustekalaksi, joka kietoo lonkeronsa käyttäjän ympärille ja kiskoo hänet osaksi verkossa sijaitsevaa maailmaa. Käyttäjän liikkeistä ja verkkovierailuista jää yksilöity jalanjälki, joiden kautta käyttäjästä voidaan rakentaa profiili. Verkossa sijaitseva maailma voi olla monin tavoin

---

[134] Andreasson & Ylipartanen 2022, 23
[135] Järvinen 2018, 14
[136] Järvinen 2022b, 13-15

riskialtista ja varomaton käyttäytyminen voi aiheuttaa pitkällekin kantautuvia seurauksia. Tietoturva ja sen noudattaminen yhdessä varovaisuuden kanssa suojaa ja terävöittää käyttäjää olemaan valppaana asioidessaan verkossa.[137]

Suomessa digitaalista turvallisuutta kehittää Digi- ja väestötietoviraston alaisuudessa toimiva VAHTI-verkosto. Verkosto koostuu julkisen hallinnon digitaalisen turvallisuuden johtoryhmästä, valtionhallinnon tietoturvan vastuuhenkilöiden verkostosta sekä laajasta digitaalisen turvallisuuden asiantuntijoiden verkostosta. Henkilöstöä VAHTI-verkostossa on noin 70 henkilöä lähes 40 kotimaisesta organisaatiosta. Verkosto kokoontuu viisi kertaa vuodessa ja sen tehtävänä on jakaa digiturvallisuuden tilannekuvaa ja parhaita käytäntöjä digitaalisen turvallisuuden kehittämiseksi sekä koordinoida ja kehittää yhteistyötä ja toimintatapoja. Verkosto itsessään koostuu viidestä erilaisesta työryhmästä, josta jokainen pyrkii kehittämään ja valvomaan oman osa-alueensa hyviä käytäntöjä. Näitä osa-alueita on riskienhallinnan kehittäminen, tietosuojan kehittäminen, digiturvaosaamisen kehittäminen, ICT-palveluiden digitaalisen turvallisuuden kehittäminen sekä toiminnan jatkuvuuden ja varautumisen kehittäminen.[138]

6.1 Tietosuojavastaava ja tietoturva

Tietosuojavastaavan avaintehtävä on varmistaa, että organisaatio noudattaa toiminnassaan tietosuojaan liittyvää lainsäädäntöä. Sen toteuttamiseksi tietosuojavastaava valvoo ja ohjaa organisaation henkilötietojen käsittelyä, neuvoo ja ohjaa organisaation johtoa ja henkilöstöä tietosuojaan liittyvissä kysymyksissä, välittää tietoa tietosuojalainsäädännöstä henkilöstölle, neuvoo ja osallistuu vaikutuksenarviointiin sekä toimii yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä kysymyksissä ja toimenpiteissä rekisteröityjen ja viranomaisten suuntaan.[139]

Tietosuojan lisäksi tietosuojavastaavan tulee ymmärtää kokonaisuutta tietoturvan ympärillä. Tietosuojavastaavan tulee hallita vähintään tietoturvan perusteet sen molemmista osa-alueista: niin hallinnollisesta kuin teknisestä tietoturvasta. Tämän kautta organisaatiossa pystytään valvomaan ja minimoimaan riskejä toimintamenettelyiden, tietojärjestelmien ja sopimusten mahdollisten puutteiden osalta.[140]

Andreasson ja Ylipartanen tunnistavat seuraavat aiheet tietoturvallisuuden tärkeiksi aihealueiksi, jotka alalla työskentelevän olisi hyvä sisäistää:

- Organisaation identiteetti- ja käyttövaltuushallinnon toteutus
- Verkkoliikenne, työasema- ja palvelinympäristön lokienhallinta

---

[137] Kananen 2013, 165-166
[138] Digi- ja väestötietovirasto
[139] Korpisaari, Pitkänen, Warma-Lehtinen 2022, 441
[140] Andreasson ja Ylipartanen 2022, 149

- Tietoturva- ja tietosuojavaatimusten tunnistaminen ja tulkinta toiminnan eri vaiheissa
- Palvelinten tietoturvapäivitysten toteutus ja valvonta
- Tietojärjestelmien tekniset suojaustoimenpiteet
- Tietoturvan tilannekuva, suoritus- ja reagointikyky
- Häiriötilanteiden selvittämisprosessi ja kyky toimintojen toipumiseen.[141]

6.2 Tietoturvariskit ovat tietojen suojaamisen vaarantavia tekijöitä

Tietoturvan riskit ja uhkakuvat liittyvät usein fyysisiin vahinkoihin tai rikolliseen toimintaan verkossa. Fyysinen vahinko voi olla esimerkiksi laitteen hajoaminen tai tiedoston häviäminen ja rikollista toimintaa verkossa voi olla muun muassa tietojen ja salasanojen kalastelu tai järjestelmämurto.[142]

Tietoturvan suurin riskitekijä on tietojärjestelmien käyttäjä. Ihminen on inhimillinen, tekee virheitä väsyneenä ja on kiireisenä usein huolimaton. He ovat helposti erehdytettävissä ja huijattavissa erilaisten hakkereiden hyödyntämien keinojen kautta. Tämän vuoksi tietoturvan avaintehtävä on saada käyttäjät noudattamaan asianmukaisia ohjeita ja toimimaan niiden mukaisesti. Tällöin voidaan osaltaan minimoida tietoturvariskejä ja rakentaa kestävämpää tietoturvapolitiikkaa.[143]

6.3 Tietoturvaloukkaukset vaarantavat tietojen suojauksen

Tietoturvaloukkaukset ovat seuraamuksia teknisen tietoturvan pettämisestä. Tietoturvassa korostuu organisaation oman toimintaympäristön tunteminen, ulkoisten uhkien tunnistaminen ja trendien seuraaminen tietoturvaloukkausten ehkäisemistä ja minimoimista varten. Vaikka suurin osa tietoturvaloukkauksista tapahtuu verkossa, ei tule sen ulkopuolista toimintaa laiminlyödä ja unohtaa. Myös organisaation suojattuihin tilojen murtautuminen voi johtaa tietoturvaloukkaukseen, kuten tietovuotoon.[144]

Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta puhutaan silloin, kun organisaation vastuulla olevien henkilötietojen saatavuus ja salassapito vaarantuvat. Sillä tarkoitetaan tapahtumaa, jonka lopputuloksena henkilötietoja häviää tai tuhoutuu, niitä luovutetaan oikeudettomasti tai niihin pääsee luvattomasti käsiksi taho, jolla ei ole tietojen käsittelyoikeutta. Henkilötietojen tietoturvaloukkaus vaarantaa rekisteröidyn henkilön perustuslailliset oikeudet ja vapaudet. Tämän luonteinen loukkaus voi koskea niin yhtä henkilöä kuin suurempaakin henkilöstöryhmää.[145]

---

[141] Andreasson ja Ylipartanen 2022, 149-150
[142] Järvinen 2018, 15
[143] Järvinen 2022b, 32
[144] Supra note 141, s. 151-153
[145] Op.cit., 196-197

Tietoturvaloukkauksista tulee aina ilmoittaa valvovalle viranomaiselle viipymättä, mutta viimeistään 72 tunnin kuluessa tietoturvaloukkauksen havaitsemisesta. Laskenta 72 tunnin määräajalle alkaa, kun tietoturvaloukkaus on tullut rekisterinpitäjän tietoon. Mikäli tietoturvaloukkaus aiheuttaa kriittisen riskin ja haitan rekisteröidylle henkilölle, tulee myös heille ilmoittaa asiasta. Jos on aihetta epäillä, että tietoturvaloukkauksessa on kyseessä rikollinen teko, tulee siitä tehdä rikosilmoitus poliisille. Tietojen kalastelusta ja palvelunestohyökkäyksistä sekä niiden yrityksistä tehdään ilmoitus Kyberturvallisuuskeskukselle.[146]

Tietoturva yhdistetään usein kyberturvallisuuteen, jota käsitellään seuraavassa kappaleessa. Tietoturvaloukkauksen takana olevia tietoturvauhkia ja sen eri muotoja määritellään kyberturvallisuuden alakappaleissa.

7 Kyberturvallisuus on digitaalisen maailman turvallisuutta

Kyberturvallisuus eli englanniksi cyber security on digitaalisen maailman turvallisuutta. Se on turvallisuuden alue, joka käsittää ihmiskunnan luoman digitaalisen maailman ympärillämme. Tähän digitaaliseen maailmaan kuuluvat esimerkiksi internet, sosiaalinen media, tietojärjestelmät ja ohjelmistot. Sanaa kyber käytetään yhdyssanan etuliitteenä kuvaamaan digitaalista maailmaa ja liittämään käsitteitä sen suuntaan. Tällaisia käsitteitä ovat muun muassa kuten kyberturvallisuus, kyberuhka tai kyberrikollisuus.[147]

Limnéllin, Majewskin ja Salmisen mukaan kyberturvallisuus tarkoittaa digitaalisen maailman tilaa, jossa on olemassa niin ymmärryksen myötä kasvatettu luottamuksen tunne kuin käytännöin toimenpiteiden kautta saavutettu kyky hallita kyberuhkia ennakoidusti sekä kestää niiden vaikutuksia.[148]

Rousku kertoo kyberturvallisuuden keskittyvän voimakkaasti tietojärjestelmien turvaamiseen. Kyberturvallisuuden kautta varmistetaan, että kybertoimintaympäristö on luotettava ja sen asianmukaisesta ja jatkuvasta toiminnasta huolehditaan. Kybertoimintaympäristö muodostuu yhteiskunnan kriittisistä toiminnoista, joiden varassa meidän nykyisyytemme toimii. Se on digitaalisessa muodossa oleva tietojärjestelmistä koostuva ympäristö, jonka tarkoituksena on mahdollistaa tietojenkäsittely.[149]

Kyberturvallisuus liitetään usein tietoturvaan ja käsitteitä käytetään yleensä ristiin, sillä kummassakin on kyse datan suojaamisesta ja tietojärjestelmien toimivuuden jatkuvuudesta sekä

---

[146] Andreasson & Ylipartanen 2022, 197-199
[147] Limnéll, Majewski & Salminen 2014, 29
[148] Op.cit., 39
[149] Rousku 2014, 55-57

niiden toiminnan varmistamisesta. Näiden toimintojen tavoitteet kuitenkin eroavat toisistaan. Kun tietoturvalla suojataan tietoja, tiedostoja sekä laitteita, ulottuu kyberturvallisuudessa tietoturva koko yhteiskunnan perustavanlaatuisiin ja kriittisiin palveluihin. Kyberturvallisuus kuuluu myös suurelta osin maanpuolustukseen tietotekniikan levitessä sotilaalliseen käyttöön ja informaatiosodanteon kasvattaessa suosiotaan. Kyberturvallisuudella siis viitataan usein arjen infrastruktuurin ja maanpuolustuksen tietoturvaan.[150] [151]

Suomessa kyberturvallisuutta valvoo Liikenne- ja viestintävirasto Traficomin alaisuudessa toimiva Kyberturvallisuuskeskus. Kyberturvallisuuskeskus määrittelee kyberturvallisuuden käsitteeksi, jolla viitataan yhteiskunnan ja organisaatioiden digitalisoitumisen aiheuttamiin ennennäkemättömiin turvallisuushaasteisiin. Kyberturvallisuus siis usein kuvaa niitä toimenpiteitä, joiden avulla organisaatio suojaa liiketoiminnassaan hyödynnettävät tietojärjestelmät, tietoliikenneyhteydet, ohjelmistot ja laitteet.[152]

Kyberturvallisuuskeskus julkaisee kuukausittain tiedotteita kuluneen kuukauden tietoturvapoikkeamista ja tietoturvaan liittyvistä ilmiöistä. Tätä kuukausittaista uutiskirjettä kutsutaan Kybersääkoosteeksi ja se antaa lukijalleen lyhyen kokonaiskuvan kyberturvallisuuden tapahtumista. Kybersää koostuu seuraavista osa-alueista: tietomurrot- ja vuodot, huijaukset ja kalastelut, haittaohjelmat ja haavoittuvuudet, automaatiot ja IoT, verkkojen toimivuus sekä vakoilu. Näitä mitataan kolmen tilannestatuksen kautta: rauhallinen, huolestuttava sekä vakava. Vuonna 2022 suurin osa osa-alueista on ollut jatkuvasti statuksessa huolestuttava. Tammikuussa Ukrainan ja Venäjän kiristyvät välit näkyivät myös Suomessa, jonka kautta vakoilun status nousi vakavan tasolle kyberhyökkäysten yleistyessä ja suomalaisdiplomaattien mobiililaitteiden vakoilun kasvaessa. Huhtikuussa ja toukokuussa huijausten ja kalasteluiden status nousi vakavan tasolle valheellisten työtarjousten, pyramidihuijausten ja verottajan nimissä tietojen kalastelun seurauksena.[153]

Euroopan unionin tasolla on tunnistettu kyberturvallisuuden korostunut merkitys maailman nykytilanteen ja teknologian kehittymisen osalta. Kyberrikollisuus on kasvanut vuoteen 2021 mennessä 5,5 triljoonaan euroon maailmanlaajuisesti. Nykyinen lainsäädäntö soveltuu tiettyihin digitaalisia elementtejä sisältäviin tuotteisiin. Useimmat laitteisto- ja ohjelmistotuotteet eivät kuitenkaan sisälly minkään kyberturvallisuutta koskevan EU:n lainsäädännön piiriin. Nykyinen lainsäädäntö ei käsittele sulautettujen ohjelmistojen kyberturvallisuutta, vaikka yhä

---

[150] Järvinen 2018, 14
[151] Järvinen 2022b, 16
[152] Traficom 2020, 4
[153] Kybersää: tammikuu, huhtikuu, toukokuu

useammin kyberhyökkäykset kohdistuvat näiden tuotteiden haavoittuvuuksiin. Tämä osaltaan aiheuttaa merkittäviä yhteiskunnallisia ja taloudellisia kustannuksia.[154]

Tällä hetkellä Euroopan komissiolla on valmistelussa merkittäviä säätelyhankkeita kyberturvallisuuden ja sen osa-alueiden kehittämiseksi. Yksi merkittävä valmistelussa oleva asetus on Cyber Resilience Act eli kyberkestävyyteen keskittyvä asetus. Asetus pyrkii luomaan edellytykset turvallisten digitaalisia elementtejä sisältävien tuotteiden kehittämiselle varmistamalla, että laitteisto- ja ohjelmistotuotteet tuodaan markkinoille vähentynein haavoittuvuuksin sekä varmistamalla, että tuotevalmistajat huolehtivat tuotteen tietoturvasta riittävällä tasolla koko sen elinkaaren ajan. Asetus tavoittelee myös luomaan olosuhteet, jossa käyttäjät voivat huomioida kyberturvallisuuden valitessaan ja käyttäessään digitaalisia elementtejä sisältäviä tuotteita.[155]

Kyberkestävyyden asetus tavoittelee konkreettisesti neljää tunnistettua aihekokonaisuutta: laitteisto- ja ohjelmistovalmistajien digitaalisia elementtejä sisältävien tuotteiden turvallisuuden parantaminen niiden koko elinkaaren ajan; johdonmukaisen kyberturvallisuuskehyksen varmistamista, joka helpottaa laitteisto- ja ohjelmistotuottajien vaatimusten noudattamista; digitaalisia elementtejä sisältävien tuotteiden turvallisuusominaisuuksien läpinäkyvyyden parantamista sekä organisaatioiden ja kuluttajien digitaalisia elementtejä sisältävien tuotteiden turvallisen käytön mahdollistamista.[156]

Kyberturvallisuuteen keskittyvät säädöshankkeet tulevat kehittämään ja ohjaamaan kyberympäristöön liittyvien aihekokonaisuuksien toimintaa sekä sitä kautta ehkäisemään kasvavaa kybermaailmaan kohdistuvaa rikollista toimintaa.

7.1 Kyberuhkat ovat digitaalisen maailman rikollisuutta

Kyberturvallisuuskeskus määrittelee kyberuhkat haitallisiksi tapahtumiksi tai ilmiöiksi, jotka voivat vaikuttaa haitallisesti organisaation toimintaan sekä sen talouteen ja tietohallintoon. Kyberuhkia ovat muun muassa tietojenkalastelu, palvelunestohyökkäykset ja haittaohjelmat.[157]

Kyberuhkat ovat kybertoimintaympäristöön eli digitaaliseen ympäristöön kohdistuvia uhkakuvia- ja tilanteita, jotka pääasiassa heikentävät yhteiskunnan toimintojen tietoturvallisuutta tai jatkuvuutta. Ne ovat vaikutuksiltaan mittavia ja niiden seuraamukset vaikuttavat koko yhteiskuntarakenteeseen. Uhka voi itsessään lamauttaa yhteiskunnan tai organisaation

---

[154] European Comission
[155] Ibid.
[156] Ibid.
[157] Traficom 2020, 4-8

toiminnan kannalta olevia kriittisiä toimintoja ja pahimmillaan aiheuttaa pysyviä sekä laajamittaisia vahinkoja.[158] [159]

Kyberuhkien yleistyessä vakuutusyhtiöt ovat lisänneet palvelutarjoomaansa myös tieto- ja kyberturvavakuutukset. Organisaatioiden ensisijaisena tehtävänä on varautua ja ennaltaehkäistä tietoturvaan liittyviä vahinkoja, mutta vakuutusten avulla voidaan minimoida mahdollisia haittoja ja vahinkoja sekä keskustella asiantuntijan kanssa niistä selviämisestä.[160]

Kyberturvallisuuskeskus auttaa kaikkia kotimaisia organisaatioita, jotka ovat joutuneet kyberuhkan eli tietoturvaloukkauksen kohteeksi. Heidän verkkosivuillaan on ohjeita erilaisiin skenaarioihin niin yksityishenkilölle, organisaatioille kuin tietoturva-alalla työskenteleville.

7.1.1 Tietomurto on luvatonta tunkeutumista toisen osapuolen tietojärjestelmiin

Kyberturvallisuuskeskus määrittelee tietomurron luvattomaksi tunkeutumiseksi tietojärjestelmään, sovellukseen tai laitteeseen. Esimerkiksi sähköpostin asiaton haltuunotto saatujen tunnusten kautta. Tietomurtojen kautta pyritään hankkimaan taloudellista ja rahanarvoista hyötyä, kuten esimerkiksi järjestelmissä elävät suojatut tiedot. Tietomurron kohteeksi joutunutta ympäristöä voidaan myös hyväksikäyttää haitallisen materiaalin jakamiseen, ympäristön toiminta voidaan jopa kokonaan lamauttaa haittaohjelman avulla tai ympäristöä voidaan käyttää muiden hyökkäysten osana, kuten esimerkiksi osana palvelunestohyökkäystä.[161]

Tietomurtojen kautta tavoitellaan hyödynnettävää tietoa, jonka avulla aiheuttaa taloudellista ja maineellista tappiota kohteena olevalle organisaatiolle. Tietomurtoja käytetään hyväksi myös kilpailevan organisaation toiminnan sabotoimiseksi ja tappion aiheuttamiseksi sekä niiden kautta voi päämääränä olla myös vakoilu- tai kiristysohjelman asentaminen ja ujuttaminen kohteena olevan organisaation järjestelmiin. Tietomurto johtaa usein tietovuotoon, joka johtaa muun muassa identiteettivarkauksiin.[162]

Rikoslaki profiloi tietomurron toiminnaksi, jossa tietojärjestelmän käyttäjätunnusta käytetään oikeudettomasti tai sen turvajärjestelyt ohitetaan ja järjestelmään murtaudutaan. Tietomurto ja sen yritys ovat joka kerta rikoksia ja niistä tulee tehdä rikosilmoitus poliisille.[163]

Tietomurroista säädetään rikoslain luvun 38 pykälässä 8.

---

[158] Rousku 2014, 55
[159] Järvinen 2018, 15
[160] Andreasson & Ylipartanen 2022, 179-180
[161] Kyberturvallisuuskeskus
[162] Järvinen 2022b, 104
[163] Poliisi

7.1.2 Tietojenkalastelu tavoittelee käyttäjän kirjautumistietojen kaappaamista

Tietojenkalastelu eli englanniksi phishing, on yksi yleisin ja tunnetuin tietomurtojen toteuttamistapa. Se tarkoittaa käyttäjän huijaamista kirjautumaan väärennetylle sivustolle. Tätä kautta hakkeri kaappaa käyttäjän kirjautumistiedot ja aloittaa tietomurron järjestelmiin. Hakkeri saattaa ohjata käyttäjän oikealle sivustolle tämän syötettyä kirjautumistiedot väärennetylle sivustolle, jonka vuoksi käyttäjä ei edes huomaa tulleensa huijatuksi. Tietojenkalastelussa hyödynnettäviä huijausviestejä kutsutaan kalasteluviesteiksi. Tietojenkalastelun vaarallisin ja kriittisin osa-alue on keihäskalastelu eli englanniksi spear phishing, jossa kohteet valitaan tarkasti ja heille lähetetyt viestit muotoillaan ja laaditaan niin, että ne näyttävät tulevan käyttäjän oman organisaation sisältä. Tätä muotoa voidaan sanoa myös kohdennetuksi tietojen kalasteluksi. Viestien sisältämä tieto on kuitenkin väärennettyä ja ohjaa käyttäjän huijaussivustolle.[164]

Kyberturvallisuuskeskuksen mukaan tietojenkalastelun tavoitteena on saattaa käyttäjien kirjautumistietoja ja muita heille tai organisaatiolle kriittisiä tietoja rikollisen haltuun. Tästä hyvänä esimerkkinä toimii muun muassa maksukortit.[165]

7.1.3 Identiteettivarkaus on toisen osapuolen henkilötietojen luvatonta käyttöä

Järvinen kertoo identiteettivarkauden tarkoittavan sitä, että joku käyttää luvattomasti toisen henkilötietoja tuottaen tätä kautta vahinkoa ja haittaa uhrille. Se voi toimia myös rikollisen keinona piilottaa hänen oma henkilöllisyytensä rikosta tehdessä.[166]

Identiteettivarkauksissa esiinnytään ja profiloidutaan toisen henkilöllisyyden kautta. Rikollinen hyödyntää jonkun toisen henkilötietoja tai tunnistautumistietoja, kuten henkilötunnusta, osoitetietoja tai pankkitunnuksia. Rikolliset keräävät näitä yksilötietoja muun muassa tietovuodon tai tietojenkalastelun kautta. Identiteettivarkaus esiintyy käytännössä esimerkiksi toisena ihmisenä esiintymisenä, toisen ihmisen nimissä tehdyn verkkokauppatilauksen ja sen pohjalta tulevan laskun kautta.[167]

Usein identiteettivarkaus kohdistuu yksityishenkilöön, mutta myös organisaation identiteetti voidaan kaapata tekemällä luvattomia ja valheellisia ilmoituksia esimerkiksi kaupparekisteriin. Yhden väärennetyn asiakirjan kautta rikollinen pystyy nimittämään itsensä muun muassa organisaation puheenjohtajaksi. Tämän jälkeen hän pystyy tilaamaan tavaraa ja tekemään sopimuksia organisaation nimissä. Mikäli huijaus ehtii tarpeeksi pitkälle, voi rikollinen muuttaa

---

[164] Järvinen 2022b, 54
[165] Kyberturvallisuuskeskus b
[166] Järvinen 2022, 166, 175
[167] Kyberturvallisuuskeskus c

organisaation osoitetiedot ja tilinumerot ja todella tehdä suurta vahinkoa organisaation toiminnalle ja maineelle.[168]

Identiteettivarkauksista säädetään rikoslain luvun 38 pykälässä 9 a.

7.1.4 Palvelunestohyökkäys pyrkii tahallisesti estämään tietojärjestelmien toimintaa

Palvelunestohyökkäys eli englanniksi Denial of Service tai DoS, on turhan tai tahallisesti virheellisen verkkoliikenteen kohdistamista kohdeorganisaatioon, jonka kautta palvelu menee tukkoon ja kaatuu. Hyökkääjä siis ylikuormittaa palvelua suunnitellusti ja estää sen toimintojen normaalia toimintaa. Hyökkäyksiä tehostetaan hajauttamalla se satoihin tai tuhansiin tietokoneisiin ja ip-osoitteisiin ympäri maailman haittaohjelmien avulla.[169]

Poliisin mukaan palvelunestohyökkäykset tietoliikenneverkossa ovat vallitseva ja tavanomainen kyberrikollisuuden osa[170]. Palvelunesto itsessään voi olla myös tahatonta. Esimerkiksi suosittujen konserttien lipunmyynti voi aiheuttaa palveluun ylikuormituksen, kun suuri massa ihmisiä yrittää ostaa liput samanaikaisesti ensimmäisten minuuttien aikana. Tähän voi varautua palvelintehoa ja verkkoyhteyden nopeutta kasvattamalla, mutta silloin kustannukset voivat nousta nopeasti korkeiksi.[171]

Palvelunestohyökkäyksestä säädetään rikoslain luvun 38 pykälässä 7.

7.2 Riskienhallinta digitaalisessa ympäristössä

Yrityksen riskienhallinta tulee ulottua vaatimusten noudattamista pidemmälle ja todella yhdistää riskienhallinta turvallisuuskulttuurin kanssa. Koska digitaalinen maailma tuo mukanaan aiemmin tunnistamattomia riskejä, tulee kyberturvallisuus ja kyberriskit sisällyttää osaksi yrityksen riskienhallintaprosesseja. Digitaalisen ympäristön sisältämiä riskejä on hyvä tarkastella useammin kuin riskienhallintaan sisältyviä muita riskejä, sillä teknologia ja sen tuomat haavoittuvuudet kehittyvät koko ajan. Muut riskienhallinnan osa-alueet, kuten taloudelliset riskit, ovat ymmärrettävyydeltään vielä nykyaikana yksinkertaisempia kuin alati kehittyvät digitaaliset riskit.[172]

Rousku kirjoittaa Digi- ja väestötietoviraston artikkelissaan digitaalisen ympäristön tuomien riskien, kuten esimerkiksi tietojenkalastelun ja palvelunestohyökkäyksien, olevan myös osaltaan taloudellisia sekä henkilöstöön kohdistuvia riskejä. Riskienhallintaa tulee käsitellä

---

[168] Järvinen 2022b, 244
[169] Op.cit., 153
[170] Poliisi b
[171] Järvinen 2018, 340
[172] Kyberturvallisuus ja yrityksen hallituksen vastuu 2020, 14-15

kokonaisuutena ja jalkauttaa sitä johtamisen kautta koko organisaation tietouteen. Sen tulisi olla jatkuvaa ja muodostaa kokonaisvaltainen riskienhallinnan prosessi, joka ei pääty riskien tunnistamiseen ja niiden seurantaan. Ennakoiva riskienhallintaprosessi varautuu mahdollisiin tuleviin riskeihin ja niistä johtuviin seurauksiin.[173]

Ennakoivan riskienhallinnan kautta voidaan varautua mahdollisiin toiminnan häiriöihin. Suunnitelmallisuus, roolitus ja harjoittelu vaikuttavat suuresti organisaation toimintakykyyn häiriöiden sattuessa. Riskien käydessä toteen niihin varautuminen voi pelastaa organisaation suuremmilta haitoilta. Riskien tunnistamisen yhteydessä muodostettu suunnitelma ja sen sisältämät toimenpiteet ohjaavat henkilöstöä toiminnassa, sillä usein häiriöiden sattuessa henkilöstön ja organisaation päätöksentekokyky heikkenee. Ennakointiin kuuluu myös häiriöistä oppiminen, niiden arviointi ja niistä saatujen kokemuksien jakaminen. Tuleviin riskeihin varautuminen on aina kattavampaa, kun niihin yhdistetään aiemmin toteutuneiden riskien opit. Toiminnan jatkuva kehittäminen tulee huomioida jo strategiassa.[174]

7.3 Tietoturvan merkitys strategian suunnittelussa

Tietoturvan johtaminen on prosessi, jonka kautta huolehditaan tiedon suojauksesta sekä riskienhallinnasta kustannustehokkaasti. Sen kautta tavoitellaan ja ylläpidetään organisaation luottamuksellisuutta, yhtenäisyyttä ja eheyttä, saatavuutta, vastuullisuutta, oikeellisuutta ja luotettavuutta. Se perustuu organisaation tietoturvatavoitteisiin ja riskienarviointiin. Tietoturvan johtamisen tulee tämän vuoksi olla tärkeä aihealue organisaation johtamissuunnitelmassa sekä sen riskienarviointi tulee yhdistää osaksi organisaation kokonaisvaltaista riskienhallinnan kokonaisuutta.[175]

Strategia ohjaa organisaation toimintaa tehden siitä johdonmukaista ja tavoitteellista. Sen kautta organisaatio keskittyy toimintansa kannalta oikeisiin aihealueisiin. Tietoturvastrategia tunnistaa organisaation toiminnan kannalta kriittiset tietoturvalliset tavoitteet ja dokumentoi kuinka nämä tavoitteet voidaan saavuttaa. Strategiaa tulee päivittää säännöllisesti vastaamaan organisaation visiota, missiota ja toimintaympäristöä sekä jatkuvasti kehittyviä teknologia- ja riskiympäristöjä. Digitalisaation ja teknologistuvan yhteiskunnan myötä tietoturvastrategian kriittisyys kasvaa ja sen riskejä tunnistetaan päivä päivältä enemmän. Riskienhallinta ja strategia muodostavat turvallisuuspolitiikan kokonaisuuden, joka kuvaa organisaation nykytilaa, tavoitteita ja niiden saavuttamisen toimenpiteitä.[176]

---

[173] Rousku 2018
[174] Kyberturvallisuus ja yrityksen hallituksen vastuu 2020, 36-38
[175] Stallings & Brown 2015, 486-488
[176] Op.cit., 489-490

Tietoturvastrategia eli tietoturvasuunnitelma ylläpitää ja kehittää kokonaisuutta organisaation tietosuojan ja tietoturvan ympärillä. Se dokumentoi organisaation tietoturvallisen kulttuurin toteutumista ja täyttymistä sekä velvoittaa tietosuojaan, tietoturvaan ja tietojärjestelmiin kohdistuvan käytön ja ylläpidon asianmukaista toteutumista. Tietoturvastrategia yhdenmukaistaa ja kokoaa yhteen ohjeistukset, tukee osaltaan organisaation tavoitteiden toteutumista, selkeyttää roolituksia, ohjaa vaatimusten täyttymistä sekä seuraa koko tietoturvallisen kokonaisuuden toteutumista. Sen seurannan toteutus voidaan aikatauluttaa organisaation toiminnan vuosikelloon ja oikein toteutettuna se toimii tarpeellisena dokumentaationa osoitusvelvollisuuden täyttämiseksi.[177]

Tietoturvastrategian jalkauttaminen henkilöstölle kehittää henkilöstön tietosuojaosaamista sekä tekee organisaation toiminnasta joustavaa ja lainmukaista. Tietosuojaosaamisen kautta saavutetaan vaikuttavia etuja ja hyötyjä niin organisaatiolle ja sen henkilöstölle kuin asiakaskunnallekin. Henkilöstön kouluttaminen tietoturvalliseen toimintaan ja tietosuojaosaamiseen on kannattava investointi organisaation toiminnan menestyksekkääseen kehittämiseen. Andreasson ja Ylipartanen tiivistävät Suomen kansallisen tuottavuuden kehittämisen osa-alueiksi seuraavat kohdat: tietoturvallisen digitalisaation lisääminen, tietojärjestelmien kehittäminen, yhteistyökumppaneiden valintaprosessiin panostaminen, henkilötietojen käsittelysopimuksen sisällön määrittäminen sekä henkilöstön tietosuojaosaamisen kehittäminen.[178]

Tietosuojaosaamista ja tietoturvallista toimintaa kehittämällä saadaan luotua kokonaisvaltaisesti selkeä ja oikeudellisesti pätevä toimintakulttuuri, joka kehittää koko Suomen kansallisen tietoturvastrategian toteutumista.

7.4 Tietoturvaloukkausten dokumentointiprosessi yrityksen toiminnassa

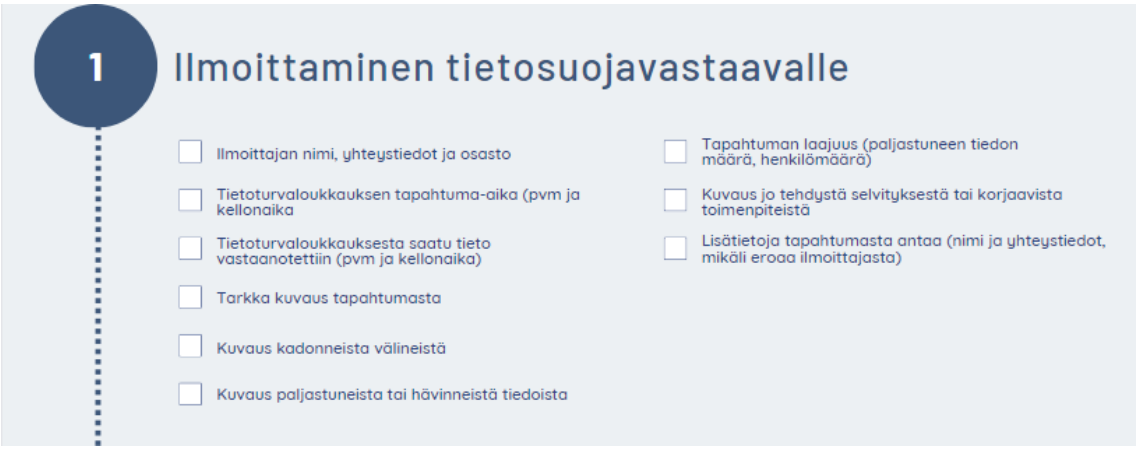
Kyberrikollisuuden lisääntyessä tulee organisaatiolla olla kuvattuna toimenpiteet ja prosessi mahdollisen tietoturvaloukkauksen tapahtuessa. Dokumentti ohjaa henkilöstön toimintaa häiriön sattuessa, sillä usein poikkeaman edessä henkilöstön sekä koko organisaation päätöksentekokyky ja suorituskyky heikkenevät. Prosessikuvauksesta tulee käydä ilmi toimenpiteet koko tietoturvaloukkauksen elinkaaren ajalle, sen havaitsemisesta sen raportointiin saakka.[179]

Poikkeaman löytyessä tulee sen havainneen henkilön ilmoittaa siitä välittömästi organisaation sisäisesti sille osoitetulle taholle. Tämä taho voi olla esimerkiksi tietosuojavastaava tai tietohallinto. Henkilöstön velvollisuuksiin kuuluu ilmoittaa jokaisesta havaitusta poikkeamasta, häiriöstä tai uhkasta, joka vaarantaa rekisteröidyn oikeudet tai organisaation toiminnan. Poikkeaman syöte voi tulla myös palveluntarjoajalta tai asiakkaalta. Näitä ilmoituksia varten

---

[177] Andreasson & Ylipartanen 2022, 115-118
[178] Op.cit., 51-53
[179] Op.cit., 197

kannattaa olla luotuna valmis lomake, jotta kaikki vaaditut tiedot tulee kirjattua. Kuviosta 9 voidaan huomata vaiheen 1 kohdat, jotka on hyvä sisällyttää lomakkeelle.[180]



Kuvio 9: Vaihe 1, ilmoittaminen tietosuojavastaavalle

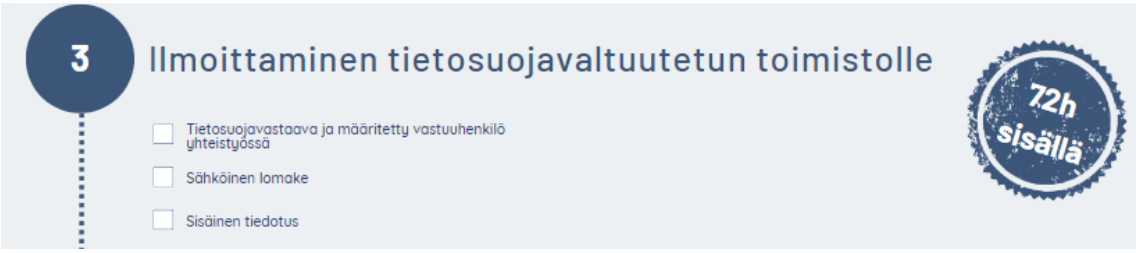
Organisaation määrittämä vastuuhenkilö koordinoi tietoturvaloukkauksen selvittämisprosessia yhteistyössä tietosuojavastaavan kanssa. Prosessin avuksi kerätään asiantuntijatiimi, joka koostuu usein tietohallinnon asiantuntijoista, palveluntarjoajasta, toimialasta ja asianajajasta. Tietoturvaloukkausten sattuessa on suositeltavaa hyödyntää ammattilaisia, esimerkiksi asianajajaa, jotka ovat asiantuntijoita sillä alalla. Mikäli kyseessä on laaja ja vakava tietoturvaloukkaus, perustetaan selkeästi roolitettu koordinointiryhmä. Asiantuntijatiimi tekee tapahtuneesta riskienarvioinnin, jonka pohjalta lähdetään korjaaviin toimenpiteisiin. Kuvio 10 koostaa vaiheessa kaksi tehtävät toimenpiteet.[181]

Kuvio 10: Vaihe 2, loukkauksen selvittäminen ja korjaavat toimenpiteet

Tietoturvaloukkauksesta tulee tehdä ilmoitus tietosuojavaltuutetun toimistolle, joka on valvova viranomainen tietosuojaan liittyvissä asioissa. Ilmoitus tulee tehdä viivästymättä, mutta

[180] Andreasson & Ylipartanen 2022, 198
[181] Op.cit., 198-199

vähintään 72 tunnin kuluessa poikkeaman havaitsemisesta. Tässä vaiheessa on hyvä pohtia myös organisaation sisäistä tiedottamista. Kuviosta 11 selviää vaiheen 3 sisältämät toimenpiteet.[182]



Kuvio 11: Vaihe 3, ilmoittaminen tietosuojavaltuutetun toimistolle

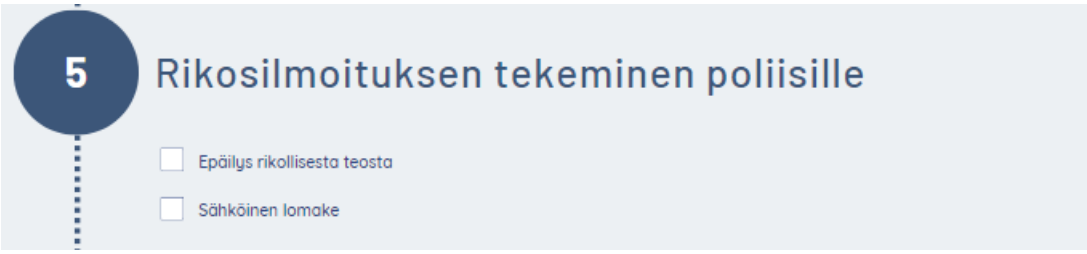
Tietosuojavastaavan ja organisaation johdon yhteistyössä tulee ilmoittaa tietoturvaloukkauksesta rekisteröidylle, jonka tietoja loukkaus koskee. Organisaation toimiala osallistuu usein ilmoitusprosessiin laatimalla asiakkaille lähetettävän kirjelmän. Vaiheen 4 toimenpiteet on kuvattu kuviossa 12.[183]

Kuvio 12: Vaihe 4, ilmoittaminen rekisteröidylle

Mikäli on syytä epäillä, että tietoturvaloukkauksen takana on rikollinen taso, tulee loukkauksesta tehdä rikosilmoitus poliisille. Rikoslain luku 38 käsittelee tieto- ja viestintärikoksia. Kuvio 13 tiivistää vaiheen 5 sisältämät toimenpiteet.[184]

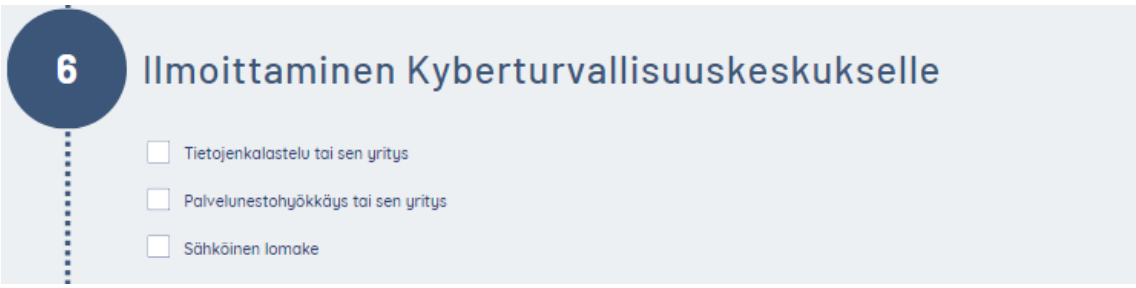
---

[182] Andreasson & Ylipartanen 2022, 199
[183] Ibid.
[184] Ibid.



Kuvio 13: Vaihe 5, rikosilmoituksen tekeminen poliisille

Mikäli tietoturvaloukkauksen aiheuttajana on tietojenkalastelu tai palvelunestohyökkäys, tulee loukkauksesta ilmoittaa Liikenne- ja viestintävirasto Traficomin alaiselle Kyberturvallisuuskeskukselle. Kuviossa 14 esitellään vaiheen 6 toimenpiteet.[185]



Kuvio 14: Vaihe 6, ilmoittaminen Kyberturvallisuuskeskukselle

Organisaation jatkuvan oppimisen ja kehittymisen kannalta on kriittistä tutkia tietoturvaloukkauksen syitä ja seurauksia sekä tarkastella sen kautta dokumentoitu aineisto. Toiminnan kannalta on myös usein kannattavaa tarkastella loukkauksen aiheuttamat työmäärät ja kustannukset. Kuvio 7 sisältää toimenpiteet vaiheen 7 osalta.[186]

Kuvio 15: Vaihe 7, loukkauksen jälkiarviointi

Organisaation tulee tilastoida kaikki henkilötietoihin kohdistuvat tietoturvaloukkaukset. Näistä tehdään organisaation johdolle yhteenveto kaksi kertaa vuodessa. Raportoinnin

---

[185] Andreasson & Ylipartanen 2022, 199
[186] Op.cit., 200

pohjalta voidaan tehdä riskienarviointia ja kehittää organisaation toiminnan eri osa-alueita. Kuviossa 16 kuvataan vaiheen 8 sisältämiä toimenpiteitä.[187]

Kuvio 16: Vaihe 8, loukkauksen raportointi ja tilastointi

Organisaation tietoturvaloukkauksen dokumentointiprosessin sisältämät kuviot ovat otteita tutkielman lähdeaineiston pohjalta luodusta ohjeesta, joka löytyy tutkielman liitteestä 1.

8 Tutkielman tulokset

Kehittämistyöpajoista aineistolähtöisen sisällönanalyysin kautta havaittiin, että tietosuojan kokonaisuuden ymmärrys on vähäistä. Lainsäädännön tuomat velvoitteet ja merkitykset liiketoimintoihin ovat epäselviä. Lainsäädäntö ja oikeusnormit ovat hankalalukuisia sekä tulkinnanvaraisia, joka osaltaan vaikeuttaa käytännönymmärtämistä. Analyysin kautta esille nousseiden huomioiden kautta on koottu esityslistaa toimeksiantajan tietoturvastrategian ja turvallisuuspolitiikan kehittämisprojektille, jonka kautta pyritään tuomaan henkilöstön huomioita ja toiveita toimenpiteiden sekä ohjeistuksien osalta projektin johdolle.

Tutkielman lähdeaineiston lainopillisen menetelmän ja syvällisen perehtymisen kautta huomattiin, että tietosuojalainsäädäntö ohjaa yrityksen tietoturvastrategian sisältöä laajasti. Tietoturva on yksi tietosuojan toteuttamisen muoto, minkä vuoksi tietosuojan voidaan ymmärtää ohjaavan koko tietoturvastrategian sisältöä ja toteutusta.[188] Tietosuojalainsäädäntö velvoittaa organisaatiota käsittelemään tietoa perustellusti, suunnittelemaan tietojen käsittelyn prosessikokonaisuuden ja siihen liittyvät toimenpiteet, huolehtimaan tietoturvan riittävästä käyttöönotosta ja suojaamaan tiedot niiden koko elinkaaren ajan, ilmoittamaan mahdollisista tietoturvaloukkauksista valvoville viranomaisille ja jokaiselle taholle, jonka tietoihin tietoturvaloukkaus vaikuttaa sekä todentamaan ja osoittamaan tietosuojan ja tietoturvan eteen tehtävä työ muun muassa määrättyjen dokumenttien kautta. Yksi tunnetuimmista tietosuojadokumentaatiosta on seloste käsittelytoimista, joka on korvannut EU:n yleisen

[187] Andreasson & Ylipartanen 2022, 200
[188] Tietosuojavaltuutetun toimisto

tietosuoja-asetusta edeltävän henkilötietolain vaatiman rekisteri- tai tietosuojaselosteen. Se on organisaation sisäinen asiakirja mistä ilmenee henkilötietojen lainmukainen käsittely. Organisaatiolla on myös velvollisuus informoida yksityishenkilöä henkilötietojen käsittelystä, jonka apuna voi käyttää osia käsittelytoimien selosteesta.[189]

Organisaation tulee myös dokumentoida kaikki henkilötietojen käsittelyyn liittyvät sopimukset, suostumukset ja tarkastukset. Sopimusten kattavuus ja rakenne on syytä käydä läpi poikkitieteellisesti yhteistyössä siihen liittyvien eri aihealueiden asiantuntijoiden kanssa. Sopimuksia tulee myös tarkastella ja päivittää säännöllisin väliajoin, jotta niiden ajantasaisuus voidaan taata. Yhtä tärkeää on muistaa neuvotella ja päivittää sopimusten sisältöä säännöllisesti siihen liittyvien osapuolien kanssa. Sopimusten laadinta suositellaan tehtäväksi niin, että ne koostuvat pääosin liitteistä. Yksittäisten liitteiden päivittäminen on helpompaa ja vähemmän työllistävää kuin koko sopimuksen uusiminen. Liitteissä voidaan määritellä pääsopimuksen mukaisen toiminnan yksityiskohdat, joita voidaan päivittää tilanteen muuttuessa. Tietosuojaa ja tietoturvaa koskevat asiat voidaan upottaa myös yhteiseen liitteeseen, joka kantaa usein nimeä turvallisuusliite.[190]

Tutkielman kehittämistyöpajoista kerätyn ja aineistolähtöisen sisällönanalyysin kautta tarkastellut tulokset auttoivat yhteistyössä valikoidun lähdeaineiston kanssa luomaan toimeksiantajayrityksen toimintoja helpottavan tarkistuslistan. Tarkistuslista pitää sisällään tietosuojassa ja tietoturvassa huomioitavia asioita sekä selkiyttää tietosuojan ja tietoturvan eroja, jotka molemmat liittyvät sähköisen tiedon ja datan suojaamiseen, mutta suojaamisen kohde ja tarkoitus eroavat toisistaan. Tietoturva suojaa organisaation omia tietoja ja tavoittelee organisaation toiminnan turvaamista. Tietosuoja taas on yksilön henkilötietojen suojaamista ja tavoittelee yksilön perusoikeudellista yksityisyyden suojan turvaamista.[191]

Tarkistuslista tulee toimimaan toimeksiantajayrityksen tietoturvan kehittämisprojektin tukena ja sitä tullaan kehittämään projektin edetessä. Tarkistuslistasta ei saatu halutun laajuista, sillä toimeksiantajayrityksen yhdistyminen suurempaan toimialalla toimivaan yritykseen sekä sen kautta laajemmaksi kasvanut tietoturvan kehittämisprojekti aiheutti omalta osaltaan haasteita sen toteutuksen suhteen. Mikäli kehittämistyöpajoihin olisi otettu mukaan osallistujia suuremmasta yrityksestä, johon toimeksiantajayritys yhdistyi, olisi kehittämistyöpajat tulleet toteuttaa hybriditoteutuksena. Tämä olisi osaltaan vaikeuttanut kehittämistyöpajojen toteutusta ja tehnyt nyt tiiviistä ja intiimistä toteutuksesta laajempaa ja passiivisempaa. Tilanteihin mukautuminen on kuitenkin suuri osa työelämää, jonka vuoksi tutkielman prosessi on relevantti kuvaus työelämän projektien elinkaaresta. Tutkielman kautta luotu

---

[189] Andreasson & Ylipartanen 2022, 187, 189-190
[190] Op.cit., 167-168
[191] Järvinen 2022b, 25

tarkistuslista toimii kuitenkin erinomaisena pohjana projektin edetessä tulevien huomioiden keräämiseen ja muotoilemiseen. Kehittämistyöpajojen ja lähdeaineiston pohjalta luotu tarkistuslista löytyy liitteestä 2.

Tutkielman tuotokset ovat tehty Canva-työkalua hyödyntäen ja niiden käyttöoikeudet ovat toimeksiantajayrityksellä.

9 Johtopäätökset

Tietosuojalainsäädäntö ohjaa organisaation tietoturvallista toimintaa ja sen toteutusta. Se velvoittaa organisaatiota käsittelemään tietoa perustetullusti, suunnittelemaan tietojen käsittelyn prosessin, huolehtimaan riittävästä tietoturvan käyttöönotosta, ilmoittamaan viipymättä mahdollisista tietoturvaloukkauksista sekä osoittamaan tietosuojan ja tietoturvan eteen tehtävää työtä määrättyjen dokumentaatioiden kautta.[192]

Käytäntö on asettanut teorian tietosuojan implementoimisen helppoudesta organisaation arkisiin toimenpiteisiin ristiriitaan. Tietosuojalainsäädäntö aiheuttaa organisatorisiin ja sopimushallinnollisiin toimenpiteisiin lukuisia haasteita, sillä sen täydellinen hyödyntäminen ja upottaminen yhteiskuntaan on vielä alkutekijöissä. Oppimisprosessi on vielä alussa ja tietoisuus tietosuojalainsäädännöstä ja sen vaatimista toimenpiteistä kasvaa jatkuvasti. Andreassonin ja Ylipartasen kuvailemaa tulevaisuutta, jossa tietosuojatyö muuttuu esteestä ja haasteesta menestystekijäksi ja luo edellytyksiä toimivalle ja tehokkaalle toiminnalle, saamme siis hetken vielä odottaa.[193]

Tutkielman aihe on ajankohtainen ja kriittinen nykyajan teknologistumisen ja digitalisaation kiihtyvän kehityksen alla. Kattava tietosuoja ja tietoturva voidaan tunnistaa olevan kasvavan digitalisaation ja teknologistumisen edellytys. Digitaalinen turvallisuus mahdollistaa digitalisoitumisen ja teknologian hyötyjen vastaanottamisen täysimääräisesti ja onnistuneesti. Tämän vuoksi jokaisen organisaation tulisi kiinnittää huomiota tietosuojalainsäädännön noudattamiseen ja henkilötietojen turvalliseen ja eheään käsittelyyn.[194]

9.1 Eettisyys

Eettisyydellä eli etiikalla tarkoitetaan yleisesti pohdintoja oikean ja väärän välillä. Tutkimuseettinen neuvottelukunta TENK määrittää tutkimusetiikan tarkoittavan kaikkia tutkimukseen

---

[192] Andreasson & Ylipartanen 2022, 189-190
[193] Op.cit., 22
[194] Op.cit., 54

ja tieteeseen liittyviä eettisiä näkökulmia ja arviointeja.[195] Jo tutkimusetiikan nimestä voi päätellä, että tutkimuksella ja etiikalla on vuorovaikutuksellinen suhde: tutkimuksen tulokset vaikuttavat eettisiin ratkaisuihin ja eettiset näkemykset vaikuttavat tutkimuksessa tehtyihin ratkaisuihin. Eettisyys on tutkimuksen luotettavuuden toinen puoli, kuten kolikollakin on kaksi puolta, niin on myös luottamuksella. Eettisyys kytkeytyy tiukasti myös laatuun, sillä hyvää tutkimusta ohjaa eettiset käytännöt ja niihin sitoutuminen. Yksi tärkeimmistä eettisistä kysymyksistä tutkimusta tehdessä, on sen aiheen valinta, jossa tulee pohtia, kenen ehdoilla aihe on valittu ja miksi sen tutkimiseen ryhdytään.[196]

Kehittämistyössä eettisyys korostuu, sillä kyse on aina inhimillisestä toiminnasta, jossa osallisten haasteet ja rajoitteet ovat automaattisesti myös kehittämistyön haasteita ja rajoitteita. Kehittämistyön tavoitteiden ja päämäärän tulee olla hyvän moraalin mukaisia sekä työ tulee tehdä rehellisesti ja huolellisesti pitäen mielessä lopputuloksen hyödynnettävyyden. Myös kehittämistyön aiheen valinnassa tulee pohtia, kenen ehdoilla kehittämiskohde valitaan ja miksi sen tutkimiseen ja kehittämiseen ryhdytään.[197]

Tässä tutkielmassa etiikan käytänteitä noudatettiin koko tutkimuksen elinkaaren ajan. Tutkielmaa tehdessä noudatettiin rehellisyyttä ja läpinäkyvyyttä sekä tiedotettiin toimeksiantajayritystä ja sen henkilöstöä tutkielman luonteesta, tavoitteista ja etenemisestä. Kehitystyöpajoihin osallistuneita henkilöitä ei pysty tunnistamaan tuotoksesta eikä heitä ole käsitelty tutkielmassa erikseen millään tavalla.

Tutkimuksen eettisyyttä valvottiin niin tekijän kuin toimeksiantajayrityksen toimesta. Toimeksiantajayrityksen kanssa pidettiin tarkastelupalavereita, joiden kautta tiedotettiin tutkielman etenemisestä ja vaiheista. Tutkielman aihe valikoitui tekijän mielenkiinnon ja aiheen ajankohtaisuuden vuoksi. Toimeksiantajayrityksen tietoturvastrategian ja turvallisuuspolitiikan kehittämisprojekti on käynnissä parhaillaan ja tutkielman aihe tukee projektia sujuvasti. Toimeksiantajayrityksen toiminnan luonne keskittyy eritoten tietoturvallisien palveluratkaisujen tuottamiseen, jonka toimituksessa tietosuojallinen osaaminen nousee keskiöön.

9.2 Luotettavuus

Tutkimusmenetelmien luotettavuutta käsitellään usein reliabiliteetin eli reliaabeliuksen ja validiteetin eli validiuksen kautta. Reliabiliteetti kuvaa tutkimustulosten toistettavuutta eli reliaabelius tarkoittaa tutkimuksen kykyä tuottaa ei-sattumanvaraisia, vaan jäsennettyjä tuloksia. Tutkimuksen reliaabelius voidaan todeta muun muassa, mikäli kaksi tutkijaa päätyy samaan tulokseen tai tutkimuksen kohteesta saadaan kahdella eri kerralla sama tulos.

---

[195] Tutkimuseettinen neuvottelukunta 2012, 4
[196] Tuomi & Sarajärvi 2018, 147, 149-150, 153-154
[197] Ojasalo, Moilanen & Ritalahti 2015, 48-49

Validiteetti tarkoittaa, että tutkimuksessa on tutkittu sitä, mitä on luvattu eli validius kuvaa tutkimuksen pätevyyttä.[198] [199]

Validiteetti saa usein laadullisesta tutkimuksesta puhuttaessa enemmän huomiota kuin reliabiliteetti. Laadullisen tutkimusmenetelmän kautta tehty tutkimus voidaan sanoa olevan luotettava tutkimuskohteen ja lähdeaineiston ollessa yhteensopivia. Laadullisen tutkimuksen luotettavuus perustuu suurimmilta osin tekijän rehellisyyteen ja avoimuuteen. Prosessin vaiheiden dokumentointi ja valintojen perustelu kasvattaa tutkimuksen luotettavuutta.[200] [201]

Tutkielman koko elinkaaren aikana harjoitettiin läpinäkyvyyttä tiedottaen toimeksiantajayrityksen henkilöstöä sen aiheesta ja sisällöstä sekä sen edistymisestä ja etenemisestä. Henkilöstön viikkopalavereiden kautta tiedotettiin tutkielman sisällön tärkeydestä ja seuraavista askeleista. Kehittämistyöpajojen kautta henkilöstö pääsi vaikuttamaan tarkistuslistan sisältöön ja kertomaan omia ajatuksiaan sen osalta. Osallistujien määrä oli pieni, sillä tutkielman alkaessa, toimeksiantajayritys ei ollut vielä yhdistynyt suuremman toimijan kanssa. Osallistuja määrä päätettiin pitää muuttumattomana kahden yrityksen yhdistymisestä johtuvien haasteiden vuoksi. Tämä ei tuottanut tutkielmalle haasteita, sillä prosessi oli jo aloitettu pienen ryhmän kanssa ja sen kautta kehittämistyöpajojen toteutus oli selkeää ja tuloksellista. Aineisto on kerätty kehittämistyöpajojen muistiinpanoista sekä niiden tuotoksista pyrkien objektiivisesti tuomaan esille niissä muotoutuneet keskustelut, mielipiteet ja ehdotukset. Kehittämistyöpajoista kerätty aineisto tuki tutkielman tavoitteiden saavuttamista.

9.3 Tavoitteiden saavutettavuus

Tutkielma oli tutkimuksellinen kehittämistyö, jonka tavoitteena oli kehittää toimeksiantajayrityksen osaamista tietosuojan osalta sekä kehittää heidän tietoturvastrategiansa ja turvallisuuspolitiikan toteutumista. Tutkielman toteutuksessa hyödynnettiin ongelmakeskeistä lainoppia sekä laadullista tutkimusta. Lisäksi lopputuotoksen muotoilussa hyödynnettiin oikeusmuotoilun oppeja. Lainopillinen tutkimus sopi tutkielman toteutukseen erittäin hyvin, sillä sen kautta pyrittiin ymmärtämään tietosuojalainsäädännön vaikutuksia organisaation toimintaan ja tietoturvastrategian ohjaukseen. Laadullisen tutkimuksen avulla saatiin henkilöstöltä arvokasta tietoa aiheen ympäriltä sekä kuvauksia nykytilasta ja kehityskohteita tulevaisuudelle.

Tutkielma antoi vastaukset sen asettamiin tutkimuskysymyksiin, jotka olivat seuraavat: miten tietosuojalainsäädäntö vaikuttaa yrityksen tietosuojastrategiaan ja mitä vaatimuksia ja

---

[198] Hirsjärvi, Remes & Sajavaara 2009, 231-232
[199] Tuomi & Sarajärvi 2018, 160
[200] Vilkka 2021, 196-197
[201] Supra note 198, s. 232

toimenpiteitä tietosuojalainsäädäntö asettaa yritykselle. Ymmärrys näihin syntyi lähdeaineiston kautta ja tarve tarkistuslistalle syntyi toimeksiantajayrityksen kanssa pidetyistä kehittämistyöpajoista. Kehittämistyöpajat olisivat voineet olla sisällöltään ja toteutukseltaan laajempia, mutta koska tietosuojaosaaminen ja sen lainsäädännön tunteminen on vielä vähäistä eikä sen implementoiminen toimintoihin ole vielä selkeää, ei kehittämistyöpajojen sisältökään voinut olla tarkempaa. Tämä tukee osaltaan tämän tutkielman toteutusta, aihetta ja sisältöä.

Visuaalisuuden implementointi tarkistuslistaan osoittautui jokseenkin haastavaksi, sillä tuotosta ei haluttu viedä liian pitkälle ennen kuin toimeksiantajayrityksen tietoturvan kehittämisprojektin kautta saadut dokumentoinnit ovat valmiina, mutta sitä ei myöskään haluttu tehdä liian vajaaksi. Tuotosta tullaan kuitenkin projektin kautta hyödyntämään ja kehittämään toimeksiantajayrityksen tarpeiden mukaisesti. Toimeksiantajayrityksen tietosuojadokumentaatiota ja sisäisiä ohjeistuksia on mahdollista kehittää oikeusmuotoilun ja visuaalisuuden keinoin tulevaisuudessa.

Tutkielman tulokset tulevat toimimaan osana toimeksiantajayrityksen tietosuoja- ja tietoturvastrategian kehittämistä. Tutkielma toi mukanaan arvokasta tietoa tietosuojalainsäädännön osalta, joka on sellaisenaan hyödynnettävissä organisaation toimintojen kehittämisessä. Tutkielman lähdeaineiston pohjalta tullaan pitämään sisäisiä koulutuksia sekä kirjoittamaan toimeksiantajayrityksen kotisivuilla ylläpitämään blogiin tietoiskuja tietosuojan ja tietoturvan osalta. Tutkielman pohjalta luotu ensimmäinen blogiteksti löytyy tutkielman liitteestä 3.

Tekijä ei ollut pohjakoulutukseltaan oikeustieteen kandidaatti tai maisteri, joten oikeudellisten lähteiden ja lainsäädännön tutkiminen ei ollut tuttua. Tämän vuoksi oikeudellisten lähteiden käyttö jää hieman vajaaksi niiden syvällisestä ja monipuolisesta käytöstä. Tutkielma itsessään antoi tekijälle tilaisuuden kehittyä tietosuojaosaamisessa sekä mahdollisuuden toimia organisaationsa tietosuoja-asiantuntijana. Työskentely kyseisen uuden osa-alueen parissa alkaa tämän kevään aikana. Tutkielma pyrkii ennen kaikkea tuomaan lisäarvoa niin yritykselle kuin tekijälle ja sen voidaan todeta toteutuneen kiitettävästi. Kokonaisuudessaan voidaan siis todeta tutkielman täyttäneen sille asetetut tavoitteet.

Toimeksiantajayritys tutustui tutkielmaan ja antoi palautetta sen kehittämistehtävän toteutumisesta seuraavasti:

”Heidi Kentalan tutkielman aihe oli yritykselle ajankohtainen ja tärkeä osa yrityksen käynnissä olevaa kehitystyötä. Yrityksessä oli tiedostettu tietosuojaan liittyvät lainsäädännölliset vaatimukset ja ymmärretty, että niiden osalta ei vielä ollut riittävän laajaa osaamista.

Opinnäytetyössä on keskitytty yrityksen kannalta tärkeisiin tietosuojan osa-alueisiin ja nostettu esiin olennaiset tietosuojaan liittyvät vaatimukset. Opinnäytetyön tekemisen yhteydessä

pidetyt työpajat lisäsivät yrityksen henkilöstön kesken ymmärrystä tietosuojan merkityksestä osana tietoturvaa ja saimme työpajojen myötä koostettuna esiinnousseet kohdat ja opinnäytetyön jälkeiseen kehittämistyöhön saatiin paljon konkreettisia ajatuksia ja tehtäviä. Opinnäytetyön myötä yrityksessä lainsäädännöllinen tietämys on lisääntynyt tietosuojan osalta ja pystymmekin käyttämään tätä tietämystä päivittäisessä työssä.

Opinnäytetyön tavoitteena oli kehittää yrityksen tietosuojastrategiaa ja luoda tarkistuslista tietosuojan ja tietoturvan osalta sekä vahvistaa henkilöstön osaamista näiden asioiden ympärillä. Näissä tavoitteissa koemme Heidin onnistuneen opinnäytetyötä tehdessään ja erityisesti tietosuojan ja tietoturvan tarkistuslista tullaan käyttämään pohjana edelleen jatkuvassa kehityksessä.

Opinnäytetyön myötä Heidin tehtävänkuva laajenee tietosuoja-asiantuntijan rooliin ja tämä opinnäytetyö toimii erinomaisena pohjana tietosuoja- ja tietoturvastrategian kehitystyössä. Kiitos Heidille opinnäytetyön tekemisestä, työpajoista ja tietämyksen lisäämisestä yrityksessämme.”

Lähteet

Painetut

Andreasson, A. & Ylipartanen, A. 2022. Osaava tietosuojavastaava ja EU:n yleinen tietosuojaasetus (GDPR). 2. uudistettu painos. Tietosanoma: Helsinki.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. Kustannusosakeyhtiö Tammi: Helsinki. 15. uudistettu painos. Kariston Kirjapaino Oy: Hämeenlinna.

Järvinen, P. 2022. Digiajan tietosuoja. Turvaa henkilötietosi, torju identiteettivarkaudet, suojaudu urkinnalta. Tammi: Helsinki.

Järvinen, P. 2022b. Yrityksen tietoturvaopas. Helsingin Kamari Oy.

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Digiaikana sinäkin olet etulinjassa. Docendo Oy: Jyväskylä.

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylän ammattikorkeakoulun julkaisuja -sarja. Suomen Yliopistopaino Oy – Juvenes Print: Jyväskylä.

Kananen, J. 2013. Digimarkkinointi ja sosiaalinen media liiketoiminnassa. Miten yritykset voivat saavuttaa tuloksia digimarkkinoinnilla ja sosiaalisella medialla? Jyväskylän ammattikorkeakoulun julkaisuja -sarja. Suomen Yliopistopaino Oy – Juvenes Print: Jyväskylä.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä. Kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylän ammattikorkeakoulun julkaisuja -sarja. Tampereen Yliopistopaino Oy – Juvenes Print: Tampere.

Kauhanen, J. 2012. Henkilöstövoimavarojen johtaminen. 10.-11. painos. Sanoma Pro Oy: Helsinki.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2022. Tietosuoja. 2. uudistettu painos. Alma Talent Oy. Otavan Kirjapaino Oy: Keuruu.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Docendo Oy: Jyväskylä.

Mikkeli, H. & Pakkasvirta, J. 2007. Tieteiden välissä? Johdatus monitieteisyyteen, tieteidenvälisyyteen ja poikkitieteellisyyteen. WSOY Oppimateriaalit Oy: Helsinki.

Niemi, V. 2021. Yksityisyys tekoälyn aikakaudella. Teoksessa Älykäs huominen – Miten tekoäly ja digitalisaatio muuttavat maailmaa? Gaudeamus: Helsinki.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyönmenetelmät. Uudenlaista osaamista liiketoimintaan. 3.-4. painos. Sanoma Pro Oy: Helsinki.

Puusa, A. & Juuti, P. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. Gaudeamus. Printon Trükikoda: Tallinna.

Rousku, K. 2014. Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Talentum Media Oy.

Tarkoma, S. 2021. Miten tekoäly vaikuttaa kokonaisturvallisuuteen? Teoksessa Älykäs huominen – Miten tekoäly ja digitalisaatio muuttavat maailmaa? Gaudeamus: Helsinki.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu painos. Kustannusosakeyhtiö Tammi: Helsinki.

Vilkka, H. 2021. Tutki ja kehitä. 5. päivitetty painos. PS-kustannus: Jyväskylä.

Sähköiset

Digi- ja väestotietovirasto. VAHTI-verkosto kehittää digitaalista turvallisuutta. Viitattu 19.9.2022. https://dvv.fi/vahti

European Comission. Cyber Resilience Act. Viitattu 24.2.2023. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Euroopan unionin perusoikeuskirja. Euroopan yhteisöjen virallinen lehti. 2000/C 364/01. Viitattu 20.9.2022. https://www.europarl.europa.eu/charter/pdf/text_fi.pdf

Euroopan unionin perusoikeuskirja. Euroopan yhteisöjen virallinen lehti. 2016/C 202/389. Viitattu 25.1.2023. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN

Euroopan unionin yleinen tietosuoja-asetus 2016/679. Euroopan unionin virallinen lehti. L 119/1. Viitattu 25.1.2023. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI

Hagan, M. 2017. Law by Design. 1. Legal Design. Viitattu 24.9.2022. https://lawbydesign.co/legal-design/

Henkilötietolaki 1999/523. Annettu Helsingissä 22.4.1999. Viitattu 25.1.2023. https://www.finlex.fi/fi/laki/ajantasa/kumotut/1999/19990523

Hirvonen, A. 2011. Mitkä metodit? Opas oikeustieteen metodologiaan. Helsinki: Yleisen oikeustieteen julkaisuja 17. Viitattu 13.4.2022. https://www2.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf

Kybersää. Kybersäätiedotteet 2022. Viitattu 10.1.2023. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa?toggle=Kybers%C3%A4%C3%A4tiedotteet%202022

Kyberturvallisuuskeskus. Näin suojaudut tietomurroilta. Viitattu 21.9.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta

Kyberturvallisuuskeskus b. Kyberturvallisuuden perussanasto. Tietojenkalastelu. Viitattu 22.9.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kyberturvallisuuden-perussanasto?toggle=Tietojenkalastelu

Kyberturvallisuuskeskus c. Neuvoja identiteettivarkauden tai tietovuodon uhrille. Viitattu 23.9.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-identiteettivarkauden-tai-tietovuodon-uhrille.

Kyberturvallisuus ja yrityksen hallituksen vastuu. 2020. Viitattu 20.2.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Poliisi. Tietomurrot. Viitattu 21.9.2022. https://poliisi.fi/tietomurrot

Poliisi b. Palvelunestohyökkäys. Viitattu 8.10.2022. https://poliisi.fi/palvelunestohyokkays

Rousku, Kimmo. 2018. Digitaalinen toimintaympäristö tuo mukanaan uusia uhkia – hallittu riskinotto on avain onnistumiseen. Viitattu 20.2.2023. https://dvv.fi/-/digitaalinen-toimintaymparisto-tuo-mukanaan-uusia-uhkia-hallittu-riskinotto-on-avain-onnistumise-2

Stallings, W. & Brown, L. 2015. Computer Security Principles and Practice. 3. uudistettu painos. Pearson Education Inc: New Jersey. http://www.cs.unibo.it/babaoglu/courses/security/resources/documents/Computer_Security_Principles_and_Practice_(3rd_Edition).pdf

Theseus. Ammattikorkeakoulujen opinnäytetyöt ja julkaisut. Haku. Tietosuoja. Viitattu 20.2.2023. https://www.theseus.fi/discover?field=subjects&query=tietosuoja&filtertype=subjects&filter_relational_operator=equals&filter=tietosuoja

Tietosuojalaki 2018/1050. Annettu Helsingissä 5.12.2018. Viitattu 25.1.2023. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Tietosuojavaltuutetun toimisto. Tietosuoja. Viitattu 15.7.2022. https://tietosuoja.fi/tietosuoja

Tietosuojavaltuutetun toimisto b. Organisaatiot. Henkilötietojen käsittelijät. Viitattu 23.9.2022. https://tietosuoja.fi/henkilotietojen-kasittelijat

Tietosuojavaltuutetun toimisto c. Organisaatiot. Osoita noudattavasti tietosuojasäännöksiä. Viitattu 15.7.2022. https://tietosuoja.fi/osoitusvelvollisuus

Tietosuojavaltuutetun toimisto d. Yksityishenkilöt. Kun haluat tarkastaa tietosi. Viitattu 19.8.2022. https://tietosuoja.fi/kun-haluat-tarkastaa-tietosi

Tietosuojavaltuutetun toimisto e. Yksityishenkilöt. Kun haluat poistaa tietojasi. Viitattu 15.7.2022. https://tietosuoja.fi/kun-haluat-poistaa-tietosi

Tietosuojavaltuutetun toimisto f. Yksityishenkilöt. Kun haluat oikaista tietojasi. Viitattu 19.8.2022. https://tietosuoja.fi/kun-haluat-oikaista-tietojasi

Tietosuojavaltuutetun toimisto g. Yksityishenkilöt. Kun haluat siirtää tietosi toiselle rekisterinpitäjälle. Viitattu 18.8.2022. https://tietosuoja.fi/kun-haluat-siirtaa-tietosi

Tietosuojavaltuutetun toimisto h. Yksityishenkilöt. Kun et halua, että tietojasi käsitellään. Viitattu 19.8.2022. https://tietosuoja.fi/kun-et-halua-etta-tietojasi-kasitellaan

Tilastokeskus. Tietoa tilastoista. Käsitteet. Tutkimus- ja kehittämistoiminta. Viitattu 11.8.2022. https://www.stat.fi/meta/kas/t_ktoiminta.html

Traficom. 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. Tarficomin julkaisuja 2/2020. Viitattu 23.9.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Tutkimuseettinen neuvottelukunta. 2012. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Viitattu 22.2.2023. https://tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf

Rikoslaki 1889/39. Annettu Helsingissä 19.12.1889. Viitattu 26.1.2023. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Valtioneuvosto. 2022. Valtioneuvostolta tukea yritysten tietoturvan kehittämiseen. Viitattu 23.2.2023. https://valtioneuvosto.fi/-/valtioneuvostolta-tukea-yritysten-tietoturvan-kehittamiseen

Julkaisemattomat

Toimeksiantajayrityksen liiketoimintasuunnitelma 2022

Toimeksiantajayrityksen tietoturvakehitys 2023

Kuviot

Kuvio 1: Keskeiset käsitteet 13
Kuvio 2: Käytetyt menetelmät 15
Kuvio 3: Aineiston analysointi 21
Kuvio 4: Tyyppikertomus 1, lakisääteiset velvoitteet 24
Kuvio 5: Tyyppikertomus 2, tietosuojalliset toimenpiteet 24
Kuvio 6: Tyyppikertomus 3, tietoturvalliset toimenpiteet 25
Kuvio 7: Tyyppikertomus 4, hallinnolliset toimenpiteet / tietoturvastrategia 25
Kuvio 8: Tarkistuslistan hahmotelma 26
Kuvio 9: Vaihe 1, ilmoittaminen tietosuojavastaavalle 58
Kuvio 10: Vaihe 2, loukkauksen selvittäminen ja korjaavat toimenpiteet 58
Kuvio 11: Vaihe 3, ilmoittaminen tietosuojavaltuutetun toimistolle 59
Kuvio 12: Vaihe 4, ilmoittaminen rekisteröidylle 59
Kuvio 13: Vaihe 5, rikosilmoituksen tekeminen poliisille 60
Kuvio 14: Vaihe 6, ilmoittaminen Kyberturvallisuuskeskukselle 60
Kuvio 15: Vaihe 7, loukkauksen jälkiarviointi 60
Kuvio 16: Vaihe 8, loukkauksen raportointi ja tilastointi 61

Liitteet

Liite 1: Yrityksen toimintaohje tietoturvaloukkauksen sattuessa..... 74
Liite 2: Tietosuojan ja tietoturvan tarkistuslista..... 75
Liite 3: Blogiteksti toimeksiantajayrityksen kotisivuilla 76

Liite 1: Yrityksen toimintaohje tietoturvaloukkauksen sattuessa

TIETOTURVALOUKKAUKSEN SATTUESSA

1 Ilmoittaminen tietosuojavastaavalle

- [ ] Ilmoittajan nimi, yhteystiedot ja osasto
- [ ] Tietoturvaloukkauksen tapahtuma-aika (pvm ja kellonaika
- [ ] Tietoturvaloukkauksesta saatu tieto vastaanotettiin (pvm ja kellonaika)
- [ ] Tarkka kuvaus tapahtumasta
- [ ] Kuvaus kadonneista välineistä
- [ ] Kuvaus paljastuneista tai hävinneistä tiedoista
- [ ] Tapahtuman laajuus (paljastuneen tiedon määrä, henkilömäärä)
- [ ] Kuvaus jo tehdystä selvityksestä tai korjaavista toimenpiteistä
- [ ] Lisätietoja tapahtumasta antaa (nimi ja yhteystiedot, mikäli eroaa ilmoittajasta)

2 Loukkauksen selvittäminen ja korjaavat toimenpiteet

- [ ] Vastuuhenkilön määritys
- [ ] Asiantuntijaverkon kasaaminen: tietohallinto, palveluntarjoaja, toimiala, asianajaja
- [ ] Riskienarviointi
- [ ] Koordinointiryhmän muodostus

3 Ilmoittaminen tietosuojavaltuutetun toimistolle

72h sisällä

- [ ] Tietosuojavastaava ja määritetty vastuuhenkilö yhteistyössä
- [ ] Sähköinen lomake
- [ ] Sisäinen tiedotus

4 Ilmoittaminen rekisteröidylle

- [ ] Tietosuojavastaava koordinoi yhteistyössä organisaation johdon kanssa
- [ ] Toimiala osallistuu ilmoitusprosessiin esimerkiksi tiedotuskirjeen lähettämisen muodossa

5 Rikosilmoituksen tekeminen poliisille

- [ ] Epäilys rikollisesta teosta
- [ ] Sähköinen lomake

6 Ilmoittaminen Kyberturvallisuuskeskukselle

- [ ] Tietojenkalastelu tai sen yritys
- [ ] Palvelunestohyökkäys tai sen yritys
- [ ] Sähköinen lomake

7 Loukkauksen jälkiarviointi

- [ ] Dokumentaation läpikäynti
- [ ] Jatkuva oppiminen ja kehittäminen
- [ ] Kustannusten arviointi

8 Loukkauksen raportointi ja tilastointi

- [ ] Loukkausten tilastoiminen organisaatiossa
- [ ] Yhteenveto johdolle kaksi kertaa vuodessa
- [ ] Riskienarviointi ja tarpeelliset toimenpiteet

9 Hyödyllisiä verkkosivuja

- [ ] www.tietosuoja.fi
- [ ] www.kyberturvallisuuskeskus.fi
- [ ] www.poliisi.fi

Liite 2: Tietosuojan ja tietoturvan tarkistuslista

1

Tietosuoja

- [ ] Rekisterinpitäjän velvoitteet
  - [ ] Käsittelyperuste
  - [ ] Huolellisuusvelvoite
  - [ ] Osoitusvelvollisuus
  - [ ] Suunnitteluvelvoite
  - [ ] Ilmoitusvelvollisuus
- [ ] Rekisteröidyn oikeudet
  - [ ] Oikeus saada tutustua tietoihin
  - [ ] Oikeus tietojen oikaisemiseen
  - [ ] Oikeus tietojen käsittelyn rajoittamiseen
  - [ ] Oikeus tietojen poistamiseen
  - [ ] Oikeus tietojen siirtämiseen
  - [ ] Oikeus tietojen käsittelyn vastustamiseen
- [ ] Asiakasrekisterit ja vastuuhenkilöt
- [ ] Henkilötietojen hallinta
- [ ] Vaikutuksenarviointi
- [ ] Oikeudellinen säätely

2

Tietoturva

- [ ] Tietoturvajärjestelmät
- [ ] Ohjelmistolistaus ja vastuuhenkilöt
- [ ] Laitehallinta ja vastuuhenkilöt
- [ ] Turvallisuusselvitykset
- [ ] Salasanakäytännöt
- [ ] Laitteiden suojaus
- [ ] Tietojen säilytyskäytännöt
- [ ] Pääsynhallinta / käyttäjätunnuksien hallinnointi

3

Liittyvät dokumentit

- [ ] Seloste käsittelytoimista
- [ ] Tietojenkäsittelysopimukset
- [ ] Turvallisuusopimukset
- [ ] Riskienarviointi
- [ ] Suostumukset
- [ ] Tietoturvastrategia ja tietoturvasuunnitelma
- [ ] Toimintaohje tietoturvaloukkausten varalta
- [ ] Sisäiset ohjeet
- [ ] Prosessikuvaukset
- [ ] Vuosikello

4

Lisätietoja

- [ ] Tietosuojavastaavan nimi ja yhteystiedot
- [ ] Tietoturvavastaavan nimi ja yhteystiedot
- [ ] Tietohallinnon yhteystiedot

Liite 3: Blogiteksti toimeksiantajayrityksen kotisivuilla

Blogi

Tietosuojalainsäädännön sisältämät velvoitteet ja oikeudet

24.2.2023
Kirjoittaja: Heidi Kentala | Ajankohtaista , Data , Identiteetti

Tietosuojan lainsäädäntö mullistui vuonna 2018, kun Euroopan unionin yleisen tietosuoja-asetuksen kansallinen soveltaminen alkoi. Päivitetty lainsäädäntö tuo mukanaan yrityksille suunnattuja velvoitteita, joiden tehtävänä on turvata rekisteröidyn oikeudet ja vapaudet sekä osaltaan kehittää kansallista kyberturvallisuutta.

Tietosuoja ja tietoturva ovat kyberturvallisuuden osa-alueita, jotka molemmat liittyvät sähköisen datan suojaamiseen. Ne ovat saman kolikon eri puolia, joiden suojaamisen kohde ja tarkoitus eroavat toisistaan. Tietosuoja on henkilötietojen suojaamista ja rekisteröidyn perusoikeudellisen yksityisyyden suojan turvaamista, kun tietoturva suojaa yrityksen sisältämiä tietoja ja tavoittelee yrityksen toiminnan turvaamista.

Tietosuoja on henkilötietojen oikeanmukaista käsittelyä

Henkilötietojen käsittelyä Suomessa ohjaa tietosuojalaki 2018/1050. Tietosuojalaki tuli voimaan joulukuussa 2018 kumoten vuonna 1999 voimaan tulleen henkilölain. Sen sisältöä ohjaa Euroopan unionin yleinen tietosuoja-asetus EU 2016/679, jonka sanomaa tietosuojalaki selittää ja tarkentaa.

Henkilötiedoiksi luetaan kaikki tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot kuten nimi, henkilötunnus, potilas- ja terveystiedot, kotiosoite, puhelinnumero, sähköpostiosoite, auton rekisterinumero, sijaintitieto ja verkkotunnistetiedot sekä fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen ja sosiaalinen tekijä, jonka kautta luonnollisen henkilön voi tunnistaa.

Tietosuojalainsäädäntö määrittelee rekisterinpitäjälle useita velvollisuuksia, joiden pohjalta tietosuoja tulee rakentaa ja suunnitella. Rekisterinpitäjällä tarkoitetaan henkilöä, yhteisöä, yritystä tai viranomaista, joka ohjaa henkilötietojen käsittelyn tarkoitusta ja toimenpiteitä sekä kerää ja käsittelee henkilötietoja. Näitä velvollisuuksia ovat käsittelyperuste, joka velvoittaa henkilötietojen käsittelyn olevan perusteltua; suunnitteluvelvoite, joka velvoittaa henkilötietojen käsittelyn olevan suunniteltua; ilmoitusvelvollisuus, joka velvoittaa tietoturvaloukkauksista ilmoittamisen valvoville viranomaisille sekä osoitusvelvollisuus, joka velvoittaa todentamaan tietosuojan ja tietoturvan eteen tehtävän työn.

Rekisteröidylle eli luonnolliselle henkilölle tietosuojalainsäädäntö määrittelee erilaisia oikeuksia, jotka juontavat juurensa Euroopan unionin perusoikeuskirjan ihmisoikeudellisesta viitekehyksestä sekä Suomen perustuslain perusoikeuksien määrityksestä. Rekisteröidyllä on oikeus saada tutustua omiin tietoihinsa, oikeus omien tietojen poistamiseen, oikeus omien tietojen oikaisemiseen, oikeus omien tietojen siirtämiseen, oikeus omien tietojen käsittelyn rajoittamiseen sekä oikeus vastustaa omien tietojen käsittelyä.

Tietoturva suojaa tietojärjestelmiä ja niiden sisältämää tietoa

Tietoturva on yksi tietosuojan toteuttamisen keino, joka pyrkii turvaamaan järjestelmien sisältämää tietoa ulkopuolisilta tahoilta. Tietoturva pitää sisällään tekniset toimenpiteet, joiden kautta pyritään varmistamaan tiedon luottamuksellisuus ja eheys, järjestelmien toimivuus ja jatkuvuus sekä rekisteröidyn oikeuksien oikeanmukainen toteutuminen.

Tietoturvassa on kyse datan suojaamisesta sekä tietojärjestelmien toiminnan varmistamisesta ja niiden toimivuudet takaamisesta. Se sisältää käytännön toimenpiteet, jotka pyrkivät toteuttamaan tietosuojalainsäädännön määrittämiä rekisteröidyn oikeuksia. Sen pääasiallinen tehtävä on turvata kriittisten tietojärjestelmien -ja verkkojen katkeamaton toiminta, ehkäistä niiden luvatonta käyttöä ja tietojen tahallista tuhoutumista sekä minimoida näistä aiheutuvia vahinkoja.

Tietoturvassa on kyse datan suojaamisesta sekä tietojärjestelmien toiminnan varmistamisesta ja niiden toimivuudet takaamisesta. Se sisältää käytännön toimenpiteet, jotka pyrkivät toteuttamaan tietosuojalainsäädännön määrittämiä rekisteröidyn oikeuksia. Sen pääasiallinen tehtävä on turvata kriittisten tietojärjestelmien -ja verkkojen katkeamaton toiminta, ehkäistä niiden luvatonta käyttöä ja tietojen tahallista tuhoutumista sekä minimoida näistä aiheutuvia vahinkoja.

Yrityksen osoitusvelvollisuuden todentavat dokumentit

Tietosuojalainsäädäntö velvoittaa yritystä todentamaan ja osoittamaan tietosuojan ja tietoturvan eteen tehtävän työn. Osoitusvelvollisuuden täyttämisen tueksi on luotu erilaisia tietosuojadokumentteja. Yksi tunnetuimmista tietosuojadokumenteista on seloste käsittelytoimista, joka on korvannut EU:n yleisen tietosuoja-asetusta edeltävän henkilötietolain vaatiman rekisteri- tai tietosuojaselosteen. Seloste käsittelytoimista on yrityksen sisäinen asiakirja, joka todentaa henkilötietojen lainmukaisen käsittelyn.

Yrityksen velvollisuutena on myös dokumentoida kaikki henkilötietojen käsittelyyn liittyvät sopimukset ja suostumukset. Sopimuksia tulee tarkastella ja päivittää tasaisin väliajoin, jotta niiden sisältö pysyy ajan tasalla. Yhtä tärkeää on säännöllisin väliajoin sopimusten sisällöstä neuvottelevien siihen liittyvien osapuolien kanssa. Asiantuntijat suosittelevat laatimaan sopimukset niin, että ne koostuvat pääosin erillisistä liitteistä. Liitteiden päivittäminen on helpompaa ja vähemmän kuormittavaa kuin koko pääsopimuksen uusiminen. Liitteissä määritellään pääsopimuksen sisältämät yksityiskohdat, joiden päivittäminen tilanteen muuttuessa on mutkatonta. Tietosuojaa ja tietoturvaa koskevat asiat voidaan upottaa yhteiseen liitteeseen, joka on usein nimetty turvallisuusliitteeksi.