SAVONIA

OPINNÄYTETYÖ - AMMATTIKORKEAKOULUTUTKINTO
LIIKETALOUDEN ALA

TIETOSUOJA

ja sen turvaamat oikeudet henkilötietojen käsittelyssä

TEKIJÄ Anne Lappalainen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Yhteiskuntatieteiden, liiketalouden ja hallinnon ala	
Tutkinto-ohjelma Liiketalouden tutkinto-ohjelma	
Työn tekijä Anne Lappalainen	
Työn nimi Tietosuoja ja sen turvaamat oikeudet henkilötietojen käsittelyssä	
Päiväys 28.2.2025	35
Yhteistyötaho	

EU:n yleinen tietosuoja-asetus (GDPR) astui voimaan toukokuussa 2018 (Asetus 2016/679/EU. Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)). Tuolloin sen käytännön toteuttaminen tuli pakolliseksi kaikissa EU:n jäsenvaltioissa. EU:n tietosuoja-asetusta täsmennetään ja täydennetään kansallisella tietosuojalailla aina maakohtaisesti. Tietosuoja-asetuksen tärkeimpänä lähtökohtana on ollut oikeus henkilötietojen suojaan, joka on jokaisen henkilön perusoikeus. Yleinen tietosuoja-asetus asettaa reunaehdot henkilötietojen käsittelylle, ja sen tarkoituksena on säätää rekisteröidyn oikeuksista ja käsittelyn periaatteista. Asetuksen mukaan henkilötietoja on aina käsiteltävä lain- ja asianmukaisesti sekä rekisteröidyn kannalta läpinäkyvästi (Asetus 2016/679/EU, 5 artikla.) Tämän opinnäytetyön tavoitteena on ollut tutkia ja koostaa tietopakettia oikeuksista, velvollisuuksista sekä ohjeistuksista, joiden avulla tietosuojaa toteutetaan yrityksissä, yhteisöissä ja organisaatioissa. Tarkoituksena on ollut selvittää, *mitä riittävä tietosuoja toteuttamisen taso vaatii,* ja mitä aihealueesta täytyy jokaisen tietää työelämää ajatellen.

Tämä opinnäytetyö on toteutettu laadullisena- eli kvalitatiivisena tutkimuksena, pohjautuen empiirisiin aineistoihin, sekä niiden analysointiin. Tutkimuskysymyksenä oli selvittää se, mitä tarvitsee tietää riittävän tietosuoja tason toteuttamiseksi? Käsiteltävä aihealue on melko laaja, mutta suuresta tietomäärästä on pyritty keräämään vain oleellisin riittävän tietotason kannalta. Käsiteltävää aineistoa on rajattu vain uusimpaan käytössä olevaan materiaaliin, koska aihepiiriin liittyvät lait ja asetukset ovat muuttuneet paljonkin viimeisen kymmenen vuoden aikana. Käytössä on ollut useampi perusteos, sekä syvemmälle menevää kapeampaa aihealuetta käsitteleviä tietokirjoja. Näiden teosten rinnalla on ollut käytettävissä virallisia *internet lähteitä*, sekä *asiatuntija artikkeleita* verkosta. Internet lähteissä on usein saatavissa kaikkein virallisin ja ajantasaisin tieto, sekä voimassa olevat lait ja asetukset. *Asiantuntija artikkeleiden* hyötynä on se, että niissä usein pureudutaan aihealueen ongelmakohtiin etsimällä niihin ratkaisuja. Kyseessä on aineistolähtöinen tutkimus, jossa tietoa on rajattu ja analysoitu tutkijan tarpeiden ja lähtökohtien mukaisesti. Lähestymistapa aihealueeseen tässä opinnäytetyössä on tullut työntekijän näkökulman kautta, mutta yleisellä tasolla tieto koskee meistä jokaista rekisteröityä henkilöä.

Tutkimuksen tavoitteet täyttyivät. Laajasta tutkimusmateriaalista ja saatavissa olevasta tiedosta on pystytty laatimaan aihealueen peruskysymyksiin vastaava kirjallinen yleiskatsaus tiivistetyssä muodossa. Tämän tutkimuksen tärkein merkitys on ollut, että tutkija sai luotua käyttöönsä kattavan tietopohjan, sekä hyvät tiedonhakuvalmiudet aihealueeseen liittyen.

Avainsanat
tietosuoja, EU:n yleinen tietosuoja-asetus, GDPR, julkisuusperiaate, henkilötieto, tietosuojalaki, laki julkisen hallinnon tiedonhallinnasta

SISÄLTÖ

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on tutkia ja koostaa tietoa oikeuksista, velvollisuuksista ja ohjeistuksista, joiden avulla tietosuojaa toteutetaan yrityksissä, yhteisöissä ja organisaatioissa. Kaikkea tietosuojaan liittyvää ohjaa koko Euroopassa EU:n yleinen tietosuoja-asetus (GDPR), jota täydennetään useiden lakien, kuten tietosuoja- ja julkisuuslain säännöksillä Suomessa.

Tietosuojalaki ja siihen läheisesti liittyvät asetukset ovat hyvin laaja kokonaisuus, ja termit usein hyvin samankaltaisia. Materiaalia, lainsäädäntöä, kirjallisuutta ja verkkojulkaisuja aihepiiriin liittyen on valtava määrä saatavilla. Isoin osa tässä opinnäytetyössä on ollut kerätä kaikesta saatavilla olevasta materiaalista tietämyksen kannalta vain olennaisin tieto, sekä koostaa siitä riittävän tietosuojatason täyttävä tiivis kokonaisuus. Lähestymistapa aihealueeseen tässä opinnäytetyössä on tullut työntekijän näkökulman kautta, mutta yleisellä tasolla tieto koskee meistä jokaista rekisteröityä henkilöä.

Tiedon ajantasaisuuden tarkastaminen on ollut suuressa roolissa tätä opinnäytetyötä kirjoittaessa. EU:n yleinen tietosuoja-asetus on useamman vuoden voimassa oltuaankin vielä melko tuntematon asia, ja oikeiden tietolähteiden sekä niiden ajantasaisuuden tunnistaminen varsinkin verkossa on välillä haastavaa asiaan enemmän perehtyneillekin henkilöille.

Tietotosuojaan läheisesti liittyvien lakien kanssa eletään usein siirtymävaiheessa. Voimassa oleva lainsäädäntö alkaa olla jo vanhentunutta, mutta lakien uudistaminen vie aikaa useita vuosia. Prosessit ovat aina pitkiä ja vaativat oman aikansa niiden käsittelyyn ja vahvistamiseen. Esimerkkinä tästä läheisesti tietosuoja-asetukseen liittyvä julkisuuslaki, joka on säädetty vuonna 1999. Julkisuuslakia alettiin ajantasaistamaan vuonna 2021, mietintö luovutettiin vuonna 2023, ja laki odottaa parhaillaan päätöstä mahdollisista jatkovalmisteluista. (Oikeusministeriö.fi 2025.) Kun ajatellaan kaikkea sitä, mitä varsinkin digitaalisessa maailmassa on tuona aikana tapahtunut, voidaan päätellä, ettei lainsäädäntö varmastikaan ole enää riittävän ajantasaista.

Työelämässä on viimeisen kymmenen vuoden aikana päästy seuraamaan EU:n tietosuoja-asetuksen valmistelua, käyttöönottoa sekä saatavissa olevan tiedon viemistä käytäntöön. EU:n tietosuoja-asetuksen käyttöönottamisessa on usein tullut yllätyksenä sen monimutkaisuus, sekä sen tulkinnan vaikeus käytännön työtehtävissä ja työyhteisöissä. Työelämän kannalta on tärkeää myös oppia tunnistamaan rajat, minkä puitteissa tietosuojaa työssä toteutetaan sen riittävän tason turvaamiseksi.

2 EU:N TIETOSUOJA- ASETUS, JA SEN KESKEISET KÄSITTEET HENKILÖTIETOJEN KÄSITTELYSSÄ

Tietosuojan tarkoituksena on aina ensisijaisesti pyrkiä ohjaamaan rekisterinpitäjää hyviin henkilötietojen käsittely – ja tietosuojakäytäntöihin. Tietosuojan toteuttamisessa tarkoituksena on samalla turvata myös riittävästi tiedon kohteen yksityiselämää ja etuja koskevia oikeuksia sekä vapauksia. Jokaisella rekisteröidyllä yksityiselämän suoja on perustuslaillinen oikeus. Yksityiselämän suojan tarkoituksena on taata jokaiselle ihmiselle oikeus elää elämäänsä, niin kuin hän itse tahtoo sitä elävän. Ilman, että kukaan siihen perusteettomasti puuttuu. Henkilötietolainsäädännön tehtävänä on asettaa rekisterinpitäjälle ne rajat, joiden puitteissa hänellä on oikeus käsitellä muun muassa rekisteröityä koskevia arkaluonteisia tietoja. (Andreasson & Ylipartanen 2022, 23.)

Tietosuojaan liittyen on ensiarvoisen tärkeää tuntea ja erottaa toisistaan siihen keskeisesti liittyvät käsitteet. Käsitteiden tuntemus auttaa tietosuojalain tulkinnassa ja sekä hahmottamaan siihen liittyvää kokonaisuutta paremmin.

Tähän lukuun on kerätty keskeisiä termejä eri tietolähteitä hyödyntäen, sekä avattu avainasioita niihin liittyen.

2.1 Henkilötieto

Henkilötiedon määrittely virallisen Tietosuojavaltuutetun toimiston mukaan on, että niitä ovat kaikki ne tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Niitä voi olla tallennettuna esimerkiksi sähköisissä tiedostoissa, tietokannoissa, paperilla, kortistossa, mapeissa tai ääni- tai kuvatallenteella. (Tietosuojavaltuutetun toimisto 2024.)

Asetuksen mukaan henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (ihmiseen) liittyviä tietoja, ja niitä ovat esimerkiksi nimi, sijaintitiedot tai puhelinnumero (Asetus 2016/679/EU, 4 artikla). Kirjassa Henkilötietojen käsittely 2017, EU-tietosuoja asetuksen vaatimukset henkilötieto määritellään seuraavasti: *”kaikki, jotka pystytään suoraan tai epäsuorasti tunnistamaan erityisten tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon (kuten kännykän), verkkotunnistetietojen (ID) taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella”.* (Hanninen, Laine, Ranta, Rusi & Varhela 2017, 19.)

2.2 Arkaluonteiset henkilötiedot

Arkaluonteisiksi henkilötiedoiksi katsotaan tiedot, joka käsittelevät esimerkiksi poliittista, filosofista tai uskonnollista vakaumusta, seksuaalista suuntautuneisuutta tai etnistä alkuperää. Myös terveyttä koskevat tiedot luetaan arkaluonteisiksi. Lähtökohtaisesti näitä erityisiä henkilötietoryhmiä ei saa käsitellä, kuin vain ainoastaan siinä tapauksessa, että rekisteröidyltä on saatu nimenomaisesti suostumus siihen, tai jos käsittelyn katsotaan olevan tarpeen yleistä etua koskevasta syystä. (Asetus 2016/679/EU, 9 artikla.)

2.3 Henkilötietojen käsittely

Henkilötietojen käsittelyllä tarkoitetaan kaikenlaisia toimintoja, jotka kohdistuvat henkilötietojen keräämiseen, säilyttämiseen, käyttöön, siirtämiseen sekä niiden luovuttamiseen (Asetus 2016/679/EU,

4 artikla). Myös henkilötietoihin kohdistuvan katselun, muuttamisen ja tietojen yhdistämisen sekä poistamisen katsotaan olevan tiedon käsittelyä.

2.4 Rekisterinpitäjä

Rekisterinpitäjäksi kutsutaan ihmistä tai organisaatiota, jonka tehtävänä on määritellä henkilötietojen käsittelyn tarkoitus ja tavat (Minilex 2024). Rekisterinpitäjä voi joko yksin, tai yhdessä toisten kanssa määritellä keinot ja tarkoitukset, miten tietoja käsitellään. (Tietosuojavaltuutetun toimisto 2024.)

2.5 Henkilötietojen käsittelijä

Henkilötietojen käsittelijäksi on määritelty ihminen tai organisaatio, jonka henkilötietojen käsittely tapahtuu rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi olla luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai joku muu elin. (Hanninen ym. 2017, 23.) EU:n tietosuoja-asetuksen mukaan *”rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimine täytäntöönpanemiseksi niin, että käsittely täyttää tämän asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu”*. (Asetus 2016/679/EU, 28 artikla.)

Rekisterinpitäjä voi ulkoistaa henkilötiedon käsittelyn, jolloin kyseessä on alihankinta- tai toimeksiantosuhde. Kyseessä voi olla esimerkiksi palkanmaksu. Rekisteripitäjällä ja henkilötietojen käsittelijällä on oltava aina voimassa oleva kirjallinen sopimus, jossa on määritelty sen vähimmäissisältö. (Alapuranen, Lehtonen, Koskinen & Wiberg 2020, 43–44.)

Rekisterinpitäjällä on aina vastuu tiedon keräyksestä ja käytöstä, eli käsittelijä ei päätä siitä mitä tiedoilla tehdään. Rekisterinpitäjän on pidettävä yllä dokumentoituja ohjeita, joiden mukaisesti henkilötietojen käsittelijä toimii. (Hanninen ym. 2017, 23.)

2.6 Henkilörekisteri

Rekisteri sisältää jäsenneltyä henkilötietoa tietojoukon perusteella, ja siinä sijaitsevat tiedot ovat saatavilla tietyin perustein. Tietomassa voidaan jakaa, keskittää tai hajauttaa tietyin perustein ja näistä esimerkkeinä voidaan käyttää esimerkiksi jäsen- ja käyttäjärekistereitä. (Asetus 2016/679/EU, 4 artikla.)

2.7 Rekisteröity

Rekisteröidyksi kutsutaan henkilöä, jonka henkilötietoja käsitellään ja jota käsiteltävät tiedot koskevat (Hanninen ym. 2017, 20).

2.8 Tietojen vastaanottaja

Tietojen vastaanottaja on usein eri kuin henkilötietojen käsittelijä, jolle henkilötietoja luovutetaan. Tällöin kyseessä on rekisterinpitäjän tietojen luovuttaminen ulkopuoliselle taholle, joka ei ole henkilötietojen käsittelijä. Tietojen vastaanottajasta tulee tuolloin luovutettavien tietojen rekisterinpitäjä. (Hanninen ym. 2017, 22.)

2.9 Suostumus

Suostumuksen katsotaan olevan mikä tahansa vapaaehtoinen, yksilöity ja tietoisesti tehty tahdonilmaisu, jonka avulla rekisteröity hyväksyy henkilötietojensa käsittelyn. Suostumuksen avulla rekisteröity saa mahdollisuuden valvoa omien henkilötietojen käsittelemistä sekä peruuttaa suostumuksensa.

Suostumuksen katsotaan olevan pätevä, kun se on:

- yksilöity
- tietoinen
- aidosti vapaaehtoinen ja yksiselitteinen tahdonilmaisu. (Euroopan komissio 2025.)

Jos henkilötietojen käsittelyn tarkoitus muuttuu, on pyydettävä aina uusi suostumus ennen käsittelyn aloittamista. (Euroopan komissio 2025).

Rekisterinpitäjän on tarvittaessa tehtävä aina uudelleen arviointi siitä, vastaako aikaisemmin annettu suostumus enää tietosuoja-asetuksen vaatimuksia. Tuossa tapauksessa suostumus on pyydettävä uudelleen, jos tietosuoja-asetuksen vaatimukset eivät enää toteudu. Henkilötietojen käsittely on tuossa tapauksessa lopetettava, koska käsittelyperustetta ei voi enää vaihtaa toiseen. Tässä tapauksessa henkilötietojen käsittely on lopetettava, jos uutta tietosuoja-asetuksen vaatimukset täyttävää suostumusta ei saada tai käsittelyä ei voi perustaa toiseen oikeusperusteeseen. (Hanninen ym. 2017, 37.)

2.10 Luonnollinen- ja oikeushenkilö

Lainsäädännössä on käytössä termi ”luonnollinen henkilö”, jolla viitataan ihmiseen, sekä termi ”oikeushenkilö”, jolloin kyseessä on yritys/yhteisö (Valtioneuvoston kanslia 2017).

2.11 WP 29

EU:n tietosuojatyöryhmää on kutsuttu nimillä WP 29 tai Working Party 29. EU:n tietosuojatyöryhmä toimii riippumattomana neuvoa-antavana työryhmänä (Aalto-Setälä & Viitala 2018.)

Säädös tästä työryhmästä on henkilötietodirektiivin 29 artiklassa. Työryhmä koostui jäsenvaltioiden- sekä komission edustajista sekä Euroopan tietosuojavaltuutetuista. Tämän työryhmän työtä jatkaa Euroopan tietosuojaneuvosto. (Aalto-Setälä & Viitala 2018.)

2.12 Valvontaviranomainen

Tietosuoja-asetuksessa on säädetty asetus valvovan kansallisen valvontaviranomaisen tehtävistä ja toimivaltuuksista (Virkkala 2019, 18). Tämän EU:n tietosuoja-asetuksen mukaan *”kunkin jäsenvaltion on varmistettava, että yksi tai useampi riippumaton viranomainen on vastuussa tämän asetuksen soveltamisen valvonnasta luonnollisten henkilöiden perusoikeuksien- ja vapauksien suojaamiseksi käsittelyssä ja henkilötietojen vapaan liikkuvuuden helpottamiseksi unionissa”*. (Asetus 2016/679/EU, 51 artikla.) Tietosuojavaltuutetun toimisto on Suomessa kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista. Sen henkilökunta on valtioneuvoston nimittämää, ja toimikausi on aina 5 vuotta. (Tietosuojavaltuutetun toimisto 2024.) Tietosuojavaltuutetun toimiston tarkoituksena on turvata ihmisten oikeudet ja vapaudet henkilötietojen käsittelyssä sekä lisätä tietoisuutta aiheeseen liittyen.

3 TIETOSUOJA-ASETUKSEN TAUSTAA

3.1 EU:n tietosuoja-asetus

EU:n tietosuoja-asetus koskee tietosuojaa eli henkilötietojen käsittelyä (Asetus 2016/679/EU, 1 artikla). GDPR lyhenne muodostuu sanoista General Data Protection Regulation (Your Europe 2025), ja se on yleisesti käytössä myös suomen kielessä tarkoittaen yleistä tietosuoja-asetusta.

Tietosuoja-asetusta edelsi EU:n henkilötietodirektiivi, johon myös Suomen henkilötietolaki perustui. (Virkkala 2019,14). Nämä kumoutuivat asetuksen astuttua voimaan toukokuun 25. päivänä 2018. Tietosuoja-asetusta sovelletaan suoraan automaattisesti kaikissa EU-maissa. Asetuksen voimassa ololla automaattisesti sovellettavana tarkoitetaan sitä, että siitä ei erikseen tarvitse enää säätää eri maissa. Tietosuoja-asetuksen keskeinen tavoite on yhdenmukaistaa EU:n valtioiden tietosuojalakeja sekä siihen liittyviä muita sääntelyjä. Tietosuoja-asetuksen yhtenä tärkeänä tavoitteena on ollut helpottaa palvelujen tarjoamista yli kansallisrajojen. Se toi tullessaan myös yrityksille ja yhteisöille uusia velvoitteita henkilötietojen käsittelyyn liittyen. Toisaalta asetus antoi lisää uusia oikeuksia rekisteröidyille henkilöille. Oikeudet lisääntyivät esimerkiksi asiakkailla ja työntekijöillä. Tietotosuoja-asetuksen rinnalla Suomessa on käytössä myös joukko erityislakeja, joissa on tietosuojaan liittyviä säännöksiä. (Hanninen, Laine, Ranta, Rusi & Varhela 2017, 9–14.)

Tietosuoja-asetuksen tarkoituksena on antaa parempaa suojaa henkilötiedoille. Asetus antaa myös lisää keinoja hallita niiden käsittelyä. Yleisen tietosuoja-asetuksen tarkoituksena on asettaa yrityksille ja organisaatioille tarkat vaatimukset, jotka koskevat henkilötietojen keräämistä, säilytystä ja hallinnointia. Vaatimuksia sovelletaan ihmisten henkilötietoja käsitteleviin eurooppalaisiin organisaatioihin, jotka käsittelevät niitä EU:n sisällä. Vaatimukset ovat voimassa myös koskien EU:n ulkopuolisia organisaatioita, joiden suorittama tietojen käsittely kohdistuu EU:n alueella asuviin ihmisiin. (Your Europe 2025.)

3.2 Tietosuoja ja sen uudistamisen historia Euroopassa

Tietosuoja-asetuksen edeltäjä, vuonna 1948 yhdistyneiden kansakuntien eli YK:n laatima ihmisoikeuksien yleismaallinen julistus loi pohjan eurooppalaiselle tietosuojalle. Tämän julistuksen jälkeen Euroopan neuvosto laati oman yleissopimuksensa vuonna 1950, ja se koski ihmisoikeuksien ja perusvapauksien suojaamista. Vuonna 1980 OECD, eli taloudellisen yhteistyön ja kehityksen järjestö antoi ensimmäisen ohjeistuksensa yksityisyyden suojasta, sekä henkilötietojen rajaylittävästä siirtämisestä. Tämä ohjeistus luotiin yhteistyössä Euroopan neuvoston ja Euroopan yhteisöjen kanssa. (Korpisaari, Pitkänen, & Warma-Lehtinen 2022, 5.)

Nykyisen voimassa olevan tietosuojan uudistamisen EU:n tietosuojalainsäädännön osalta katsotaan lähteneeksi liikkeelle vuonna 2012. Euroopan Unionin tietosuoja lainsäädäntö ei enää pysynyt mukana kehityksen kulussa. Myöskään sen vastaavuus globaalissa tietoympäristössä ei toteutunut enää riittävällä tasaolla olosuhteisiin nähden. Tavoitteena tietosuoja uudistuksella oli turvata henkilötietojen suojaa jokaisen henkilön perusoikeutena. EU:n tietosuojauudistuksen kansallisen täytäntöön panon seurauksena syntyivät yleinen tietosuoja-asetus (GDPR) sekä tietosuojadirektiivi. Vanha henkilötietolaki kumottiin uudella tietosuojalailla. (Eduskunta 2017.)

Eduskunta.fi sivustolla uudistuksen historiaa käsiteellään seuraavasti; *”yleinen tietosuoja-asetus korvasi vuoden 1995 henkilötietodirektiivin. Uusi tietosuoja-asetus on yleissäädös, joka koskee lähtökohtaisesti kaikenlaista henkilötietojen käsittelyä. Asetukseen sisältyy säännökset rekisteröidyn oikeuksista sekä rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista. Yleinen tietosuoja-asetus on tullut voimaan 25.5.2016, ja sen soveltaminen on aloitettu jäsenvaltioissa 25.5.2018*”. (Eduskunta 2024.) Tietosuoja-asetusta sovelletaan suoraan kaikissa EU-maissa, mutta jokaisessa maassa voidaan käyttää asetuksen sallimaa liikkumavaraa täydentämällä sitä maakohtaisilla asetuksilla. Käytännössä tämä vaati Suomessa henkilötietolainsäädännön tarkistamista, uuden tietosuojalain käyttöönottoa sekä sen toteuttamista henkilötietojen käsittelyä koskevana yleislakina. (Eduskunta 2024.)

3.3 Tietosuoja ja sen toteuttaminen kansallisella tasolla Suomessa

Tietosuojalain tarkoituksena on täydentää ja täsmentää EU:n yleistä tietosuoja-asetusta, sekä sen soveltamista kansallisella tasolla (Tietosuojalaki 1050 /2018, 1 luku 1 §).

Lähtökohtana tietosuojalain säätämiseen, sekä sen noudattamiseen on aina jokaisen oikeus henkilötietojen suojaan. Henkilötietojen suojan katsotaan aina olevan perusoikeus, joka kuuluu meistä jokaiselle. Viranomaisilla on valvontavelvollisuus laadittujen sääntöjen noudattamisessa. (Eduskunta.fi 2024.)

Viranomaistoimintaa varten on säädetty laki julkisen hallinnon tiedonhallinnasta, ja sen tarkoituksena on täsmentää ja täydentää EU:n yleistä tietosuoja-asetusta. Lakia kutsutaan tiedonhallintalaiksi, ja se astui voimaan 1.1.2020. Tiedonhallintalain tarkoituksena on säännellä viranomaisten toiminnan julkisuudesta asiakirjojen ja muiden tietoaineistojen kohdalla. Laki koskee asiakirjojen julkisuutta ja salassapitoa, sekä tiedon antamista asiakirjasta ja siihen liittyvää menettelyä. Lisäksi tällä lailla määrätään säännöksillä viranomaisten velvollisuudesta edistää tiedonsaantia. (Laki julkisen hallinnan tiedonhallinnasta 906/2019, 1 luku 1–3 §.)

3.4 Tietosuoja-asetuksen tarkoitus

Tietosuoja-asetuksella on paljon myös muita tarkoituksia, kuin vain henkilötietojen suoja. Näitä ovat esimerkiksi seuraavat:

- *”Tukea vapauden ja turvallisuuden kehittämistä.*
- *Tukea oikeusalueen ja talousunionin kehittämistä.*
- *Tukea taloudellista ja sosiaalista edistystä EU:n alueella.*
- *Tukea talouksien lujittamista ja lähentämistä sisämarkkinoilla.*
- *Turvata luonnollisten henkilöiden hyvinvointia”.* (Asetus 2016/679/EU.)

Tietosuojan riittävä toteuttamisen taso on tärkeä kilpailuetu nykypäivän organisaatioissa ja yrityksissä. Tietosuojasta hyvin huolehtiminen korostuu myös jatkuvasti kasvavien tietosuojavaatimusten myötä. Asiakkailla on koko ajan kiinnostusta ja tietoisuutta enemmän siitä, miten heidän henkilötiedoistaan huolehditaan. Yrityksen tai organisaation laadukas ja riittävä tietosuoja osaaminen on aina hyvän luottamuksen perustana yhteistyölle. Sen avulla pystytään arvioimaan luotettavuuden tasoa, ja luomaan pohjaa myös yritystoiminnan jatkuvuutta ajatellen. (Aalto-Setälä & Viitala 2018, 4–6.)

3.5 Riittävän tietosuojatason toteuttaminen ja sen päivittäminen

Organisaatioiden on ollut välttämätöntä tarkistaa omaa tietosuojan tasoaan EU:n yleisen tietosuoja-asetuksen astuttua voimaan. Tarkistettavana ja päivitettävänä on esimerkiksi tietosuojakäytäntöjen lainmukaisuus eli henkilötietojen käsittelyn nykytila sekä se, vastaavatko käsittely- ja tietosuojakäytänteet lainsäädännön vaatimuksia. Myös tietoturvan riittävyydellä ja ongelmatilanteisiin varautumisella on merkitystä tietosuojan toteuttamisen kannalta. (Andreasson & Ylipartanen 2022, 47.)

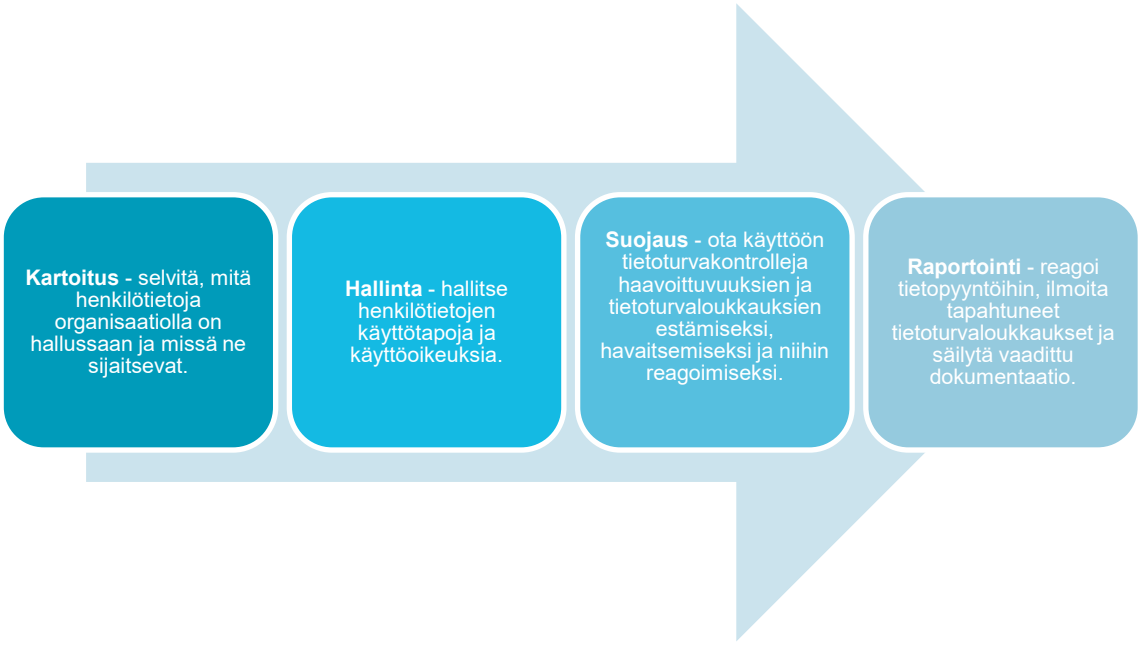
Tietosuojan tason oikea mitoittaminen, sekä sen hallittu ja suunnitelmallinen toteuttaminen ovat tärkeässä asemassa organisaatioissa. Jos yrityksissä/yhteisöissä taso on määritetty liian korkealle, tulee siitä usein liian vaikeasti tulkittavaa ja hankalaa hallita. Jos suojaustaso taas on liian matala tai se ei reagoi muutoksiin riittävästi, on tietosuojan toteuttaminen silloin riittämätöntä lain vaatimaan tasoon nähden. EU:n yleisen tietosuoja-asetuksen myötä, organisaatioiden on ollut pakko tarkistaa omien tietosuojakäytäntöjensä lainmukaisuutta. eli arvioida henkilötietojen käsittelyn nykytila sekä se, vastaavatko käsittely- ja tietosuojakytänteet lainsäädännön vaatimuksia. (Andreasson, Oravala & Toivonen 2023, 45).

Tietosuojan toteuttamisessa on oltava aina niin sanotusti ”askel edellä”. On pystyttävä ennustamaan tulevaisuutta sekä sen mukanaan tuomia muutostarpeita. Teknologian nopea kehittyminen ja globalisaatio tuovat henkilötietojen suojeluun uusia haasteita. Oikeusvarmuuden sekä luottamuksen kehittäminen käytännön toiminnan sujuvuuden osalta, niin luonnollisten henkilöiden, talouden toimijoiden kuin viranomaistenkin kesken, ovat EU:n yleisen tietosuoja-asetuksen määrittelemiä tavoitteita. (Asetus 2016/679/EU.)

Kun asiakkaan tietosuoja on oikein mitoitettu, ei tarpeettoman tiukka eikä liian heikko, siitä hyötyvät kaikki. Tämä tukee myös luottamuksellisen asiakassuhteen syntymistä. Tiedon korkealla laadulla ja toimivilla lainmukaisilla menettelytavoilla tietojen käsittelyssä vaikutetaan positiivisesti kaikkiin organisaation toiminnan osa-alueisiin. (Andreasson & Ylipartanen 2022, 15.)

Tärkeää on aina arvioida yhteistyökumppanin luotettavuus sekä sopimusehdot tietosuojaan liittyvissä asioissa tarkoin, jotta vältytään ongelmilta. On päästävä yhteiseen ymmärrykseen siitä, mitä riittävän tason toteuttaminen pitää sisällään. On myös pystyttävä arvioimaan se, kuinka paljon tietosuojan jatkuva hallinta ja päivittäminen vaatii yhteistyö kumppanilta aikaa, rahaa ja resursseja. Nämä kaikki on hyvä käydä tarkoin läpi ja arvioitava realistisesti sopimusneuvotteluissa.

Läpinäkyvyyden periaate on tärkeää tietosuojan kannalta. Rekisteröidyille pitää pystyä kertomaan, miksi heidän tietojaan käsitellään, eli mikä niiden käyttötarkoitus on. Myös tieto siitä, kuka on rekisterin pitäjä, täytyy pystyä kertomaan yksiselitteisesti viivyttelemättä. Rekisteröidyllä on oikeus saada tieto henkilötietojen käsittelyyn liittyvistä riskeistä, suojatoimista sekä rekisteröidyn oikeuksista. (Hanninen ym. 2017, 48.) Tämän vuoksi on tärkeää, että koko tietosuojaprosessi on organisaatiolla hallussaan, koska muuten heillä ei ole riittävästi osaamista eteen tulevien tilanteiden käsittelyä varten.



Kaavio 1: Yrityksen tietosuoja-asioiden ajan tasalla pitäminen eli henkilöinventaario (tietosisältö Aalto-Setälä & Viitala 2018, 41.)

Yllä kaaviossa 1 on sovellettu tietoa *kauppakamarin* julkaisemasta tietosuoja oppaasta yrityksille, jossa on käyty läpi henkilöinventaarion 4 kohtaa. Näiden askeleiden avulla organisaation tietosuoja-asiat pysyvät ajan tasalla. Kaavion 1 sisältämät vaiheet on käyty läpi alla olevana henkilöinventaariona:

- Kartoituksen tarkoituksena on käydä läpi koko organisaation toiminta henkilötietojen käsittelyn näkökulmasta. Tarkoituksena on saada näkyvyys siihen, mistä henkilötiedot yritykselle tulevat, missä ja millä tavoin niitä käsitellään. Kartoituksessa selvitetään henkilötietojen säilytystä, sekä sitä miten ne poistuvat tai poistetaan manuaalisesti.
- Hallintavaiheessa organisaatiossa luodaan henkilötietojen hallintasuunnitelma. Sen tarkoituksena on taata rekisteröidyille mahdollisuudet hallita tapoja, joilla heidän henkilötietojaan kerätään, käytetään ja käsitellään yrityksessä tai organisaatiossa. Hallintavaiheen tarkoituksena on myös määritellä tarkemmin henkilötietojen käyttöoikeudet, hallinta sekä käyttöön liittyvät käytännöt, käytänteet, roolit ja vastuut organisaatiossa.
- Suojausvaiheessa otetaan käyttöön tietoturvakontrollit, joiden avulla havaitaan haavoittuvuuksia, sekä estetään tietomurtoja. Suojausvaiheeseen kuuluu myös mahdollisiin tietomurtoihin reagointi.
- Raportointivaiheessa laaditaan organisaation johdolle raportit, sekä dokumentoidaan tietosuojaan liittyvä toiminta. Vaiheen aikana tehdään myös ilmoitukset rekisteröidyille sekä viranomaisille ja vastataan rekisteröityjen esittämiin pyyntöihin. Aina on myös huolehdittava siitä että, organisaatiolla on riittävät valmiudet käsitellä tietopyyntöjä. (Aalto-Setälä & Viitala 2018, 37–41.)

4 TIETOSUOJAPERIAATTEET

Tietosuoja-asetuksessa on säädetty henkilötietojen käsittelyä koskevista periaatteista, ja siitä mitä tulee ottaa huomioon niitä käsiteltäessä. Tietosuoja-periaatteet asettavat rajoituksia sille, miten tietoja on sallittua käsitellä. Usein arvioitaessa jonkin henkilötietojen käsittelyn käytännön toteutuksen lainmukaisuutta, joudutaan palaamaan alkuun periaatetasolle, ja tarkastelemaan siltä pohjalta mikä käsittelyssä on sallittua ja mikä ei. (Hanninen ym. 2017, 47.)

4.1 Rekisterinpitäjän osoitusvelvollisuus

Rekisterinpitäjällä on osoitusvelvollisuus ja hän vastaa, että käsittelyssä noudatetaan tietosuoja-asetuksen 2. luvun mukaisia periaatteita, joita *ovat:*

1. *”lainmukaisuus, asianmukaisuus ja läpinäkyvyys*
2. *käyttötarkoitussidonnaisuus*
3. *tietojen minimointi*
4. *täsmällisyys*
5. *säilytyksen rajoittaminen*
6. *luottamuksellisuus ja turvallisuus”* (Asetus 2016/679/EU, 5 artikla.)

4.2 Tiedon lainmukaisuus, asianmukaisuus ja läpinäkyvyys

Henkilötietojen käsittelyssä on otettava aina huomioon, että tietoja käsitellään lain- ja asianmukaisesti. Lisäksi on huomioitava, että käsittely on rekisteröidyn kannalta läpinäkyvää. Käsittelyn on aina oltava perusteltua esimerkiksi asiakas- työsuhteeseen perustuvaan oikeutettuun etuun. (Hanninen ym. 2017, 48). Käsittelyssä on otettava aina huomioon tietosuoja-asetus, sekä muut voimassa olevat lait, jotka käsittelyyn liittyvät.

Läpinäkyvyyden tarkoituksena on, että rekisteröidyillä on aina tieto rekisterinpitäjästä, sekä siitä miksi henkilötietoja käsitellään. Henkilötietojen käsittelyn tarkoitus täytyy määritellä tarkasti, sekä ilmoittaa tietojen keräämisen yhteydessä, mihin kerättyjä tietoja käytetään. Rekisterinpitäjällä on myös tiedonantovelvollisuus rekisteröidylle koituvista mahdollisista riskitekijöistä, tietojen suojaamisesta sekä rekisteröidyn omista oikeuksista henkilötietojen käsittelyyn liittyen. (Korpisaari ym. 2022, 95.)

4.3 Tiedon käyttötarkoituksen varmistaminen

Kun tunnistetaan, että kyseessä on henkilötieto, on tärkeää varmistaa mitä käyttötarkoitusta varten tietoa kerätään. Kirjassa, Henkilötietojen käsittely 2017, EU-tietosuoja-asetuksen vaatimukset käsitellään asiaa seuraavasti; *” Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten eli henkilötietoja tulee käsitellä aina jonkun tietyn tehtävän hoitamiseksi. Henkilötietojen käsittelyn tarkoituksia voivat olla erimerkiksi asiakassuhteen hoito, suoramarkkinointi, työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitaminen ja työntekijöiden valinta”*. (Hanninen ym. 2017, 49.)

4.4 Tietojen minimointi

Kun henkilötietoja kerätään, on tärkeää huolehtia, että tiedot ovat riittäviä, mutta rajoittuvat siihen, mikä on välttämätöntä tietojen käsittelyn tarkoituksen kannalta. Henkilötietojen on oltava aina olennaisia ja asianmukaisia niiden määritellyn käyttötarkoituksen kannalta. Rekisterinpitäjän täytyy tarkastaa kerättävien tietojen tarkoituksenmukaisuus kyseistä käyttötarkoitusta varten.

Työnhakijalta tietoja kerättäessä on kiinnitettävä huomiota siihen, että kerättävä tieto on tarpeellista ainoastaan valinnan kannalta. Vaikka henkilö on antanut suostumuksensa henkilötietojensa keräämistä varten, ei rekisterinpitäjällä silti ole oikeutta käsitellä keräämiään henkilötietoja tarpeettomasti. Kaikella kerättävällä tiedolla on oltava käyttötarkoitus, ja sen kerääminen on luvallista vain sitä tarkoitusta varten. Tämän vuoksi rekisterinpitäjällä on velvollisuus huomioida, että tiedon kerääminen tulevaisuutta varten on tietosuojalainsäädännön vastaista. Kerättävän tiedon tarpeellisuus on pystyttävä määrittelemään jo ennen kuin tietoa aletaan käsittelemään. (Hanninen ym. 2017, 49.)

Henkilötietojen minimoimisen kannalta on tärkeää tietojen täsmällisyys ja päivitys, joilla varmistetaan tietojen oikeellisuus. Kerättävän tiedon rajaaminen on pystyttävä arvioimaan suhteessa käyttötarkoitukseen.

Tietojen keräämisen tulee olla rekisterinpitäjän toiminnan kannalta tarpeellista ja asiallisesti perusteltua. Henkilötietoja ei saa myöhemmin käsitellä määriteltyjen käyttötarkoitusten kanssa yhteensopimattomalla tavalla. Yrityksen on siis varmistettava, ettei kerättyjä henkilötietoja käytetä muuhun kuin niiden ennalta määrittelemään tarkoitukseen. Mikäli jokin toimenpide voidaan tehdä ilman henkilötietojen käsittelyä, ei henkilötietoja tulisi käsitellä. (Hanninen ym. 2017, 49.)

4.5 Tietojen täsmällisyys

Rekisterinpitäjän velvollisuutena on aina huolehtia, että rekisteröityjen tiedot ovat täsmällisiä ja niitä on päivitettävä aina tarpeen niin vaatiessa. Virheellisiä henkilötietoja ei saa säilyttää, vaan ne ovat velvollisuus poistaa tai oikaista viivyttelemättä. (Asetus 2016/679/EU, 5 artikla.) Rekisterinpitäjän velvollisuutena on esimerkiksi huolehtia viallisen sähköposti ilmoituksen jälkeen, että henkilötieto päivitetään tai poistetaan, eikä sitä vain voi jättää ”roikkumaan listoille”.

4.6 Säilytyksen rajoittaminen

Henkilötietojen säilyttämisessä on otettava huomioon, että niitä saa säilyttää ainoastaan tarpeellisen ajan, mitä käyttötarkoituksen toteuttamista varten tarvitaan. Rekisterinpitäjällä on velvollisuus määräajoin tarkastella henkilötietojen säilyttämisen tarvetta ja huolehtia tarpeettomien tietojen poistamisesta. Hänellä on myös tarvittaessa velvollisuus pystyä perustelemaan perusteet henkilötietojen säilyttämiseen. (Asetus 2016/679/EU, 5 artikla.)

Asiakkuuden hoitaminen vaatii usein tietojen säilyttämistä koko asiakassuhteen ajan. Kun asiakassuhde päättyy, on rekisterinpitäjällä velvollisuus tarkastella kriittisesti, onko asiakassuhteen tietojen säilyttäminen enää tarpeen, vai täytyisikö ne poistaa. Tietojen säilyttämisen kannalta täytyy ottaa huomioon mahdolliset toimenpiteet laskutuksen, perinnän, oikeudellisten toimenpiteiden, reklamaatioiden ja takuun vuoksi. (Hanninen ym. 2017, 50.)

Lopullisen poistamisen sijaan rekisterinpitäjä voi myös anonymisoida tiedot luotettavasti, jolloin ne ovat käytössä esimerkiksi tilastointia varten (Tietosuojavaltuutetun toimisto 2024). Pseudonymisointia ja anonymisointia voidaan käyttää, jos halutaan muokata henkilötietoja ei tunnistettavaan muotoon (Andreasson, Oravala & Toivonen 2023, 263). Pseudonymisoinnin tehtävä on varmistaa, ettei henkilötietoja voida enää yhdistää henkilöön ilman lisätietoja. Pseunonymisoituja tietoja ei voi myöskään säilyttää samassa paikassa kuin henkilötietoja säilytetään. Vaikka tiedot ovat pseudonymisoitu, niin silti niiden avulla yksilön saattaa edelleen erottaa ja yhdistää eri tietoaineistossa. (Tietosuojavaltuutetun toimisto 2024.) Nämä tiedot ovat pseudonymisoinnista huolimatta edelleen henkilötietoja, ja niihin noudatetaan tietosuoja säännöksiä. Esimerkkinä tietokannat, jossa tietoa korvataan toisella tunnistettavuuden heikentämiseksi.

Anonymisoinnissa henkilötietoja käsitellään niin, että tiedoista ei voida enää lainkaan tunnistaa henkilöä. Tunnistaminen on tuolloin tehty peruuttamattomasti, eikä tietoja voida enää mitenkään palauttaa. Anonymisoidut tiedot eivät ole enää henkilötietoja, eikä myöskään tietosuojasäännökset enää koske niitä. (Hanninen ym. 2017, 21.)

Henkilötietojen säilytysaikaa määritettäessä täytyy ottaa huomioon myös mahdollinen kansallinen lainsäädäntö, jolla voi olla vaikutusta säilytysaikoihin.

4.7 Luottamuksellisuus ja turvallisuus

Rekisterinpitäjällä on velvollisuus käsitellä ja säilyttää henkilötietoja niin, että tietojen luvaton katseleminen ja lainvastainen käsittely estetään. Myös tietojen vahingossa häviäminen, tuhoutuminen ja vahingoittuminen on estettävä rekisterinpitäjän toimesta. (Asetus 2016/679/EU, 5 artikla.)

Rekisterinpitäjän täytyy etukäteen arvioida mahdolliset riskit, organisaation tietosuoja- ja tietoturvaohjeistuksen taso, sekä henkilötietojen tekninen suojaus. Suojatoimien riittävyyttä on punnittava suhteessa olosuhteisiin ja riskeihin. (Tietosuojavaltuutetun toimisto 2024.)

Henkilötietojen suojaaminen kaikessa käsittelyn vaiheissa sekä koko niiden elinkaaren ajan, on ensiarvoisen tärkeää, jotta niiden luottamuksellisuus säilyy.

4.8 Rekisteröidyn valitusoikeus

Jokaisen rekisteröidyn oikeuksiin kuuluu tehdä valitus valitusviranomaiselle, jos hän katsoo omien henkilötietojensa käsittelyssä tapahtuneen jotain, joka rikkoo tietosuoja-asetusta. Näin rekisteröidyn on mahdollista saattaa yrityksen henkilötietojen käsittelytoimet valvontaviranomaisen käsiteltäväksi vaikkapa silloin, jos yritys kieltäytyy toteuttamasta toimia, joita rekisteröity on pyytänyt. Valvontaviranomaisen oikeuksiin taas kuuluu valtuudet saada asiasta lisäselvitystä ja tarvittaessa määrätä yritys noudattamaan rekisteröidyn pyyntöjä. (Hanninen ym. 2017, 125.)

Henkilötietojen luovuttaminen

Rekisteröityjen henkilötietoja voidaan siirtää kolmannelle osapuolelle käsiteltäviksi. Rekisteröity voi tässä tapauksessa olla vaikkapa asiakas tai työntekijä ja tietojen siirtäjänä rekisterinpitäjä. Kyseessä on henkilötietojen luovuttaminen, kun vastaanottanut yritys on siirron jälkeen myös tietojen rekisterinpitäjä. Luovutus on kyseessä esimerkiksi silloin, kun työntekijästä luovutetaan palkkatietoja vaikkapa verottajalle tai muulle viranomaiselle. Tällainen tietojen luovuttaminen on lakisääteistä, eikä luovutuksesta ole tarpeen sopia erikseen verottajan kanssa. (Hanninen ym. 2017, 93.)

Tietojen siirtäminen käsiteltäväksi tapahtuu, kun niitä siirretään emoyhtiölle tai muulle samaan konserniin kuuluvalle yhtiölle. Tällöin käytetään myös termejä ulkoistaminen rekisterinpitäjän käsittelijälle, luovuttaminen rekisterinpitäjältä rekisterinpitäjälle tai yhteinen rekisteri. Kunkin konserniyhtiön rooli ratkaisee sen, mikä toimenpide on kyseessä. Jos henkilötietojärjestelmien ylläpitäjä siirron yhteydessä vaihtuu, tuolloin kyseessä on siirto, ei tietojen luovutus. Tällöin käsittelyn ulkoistamisesta tulee laatia erillinen käsittelysopimus. Jos myös tietojen päätösvalta kerättävistä henkilötiedoista muuttuu, on tuolloin tarpeellista laatia myös erillinen luovutussopimus. (Hanninen ym. 2017, 94.)

Yhteinen rekisteri tulee kyseeseen, kun saman konsernin alla olevilla yhtiöillä on yhteinen päätös henkilötiedoista, joita kerätään, sekä siitä mikä niinen käsittelyn käyttötarkoitus on. Tällöin on kyseessä yhteisrekisterinpitäjä. (Tietosuojavaltuutetun toimisto 2025.)

Erityisen tarkkana henkilötietojen luovuttamisessa eteenpäin on oltava erityisten henkilötietoryhmien kanssa.

4.9 Lapsen henkilötiedot sähköisenä etäpalveluna

EU:n tietosuoja asetus edellyttää jäsenvaltioita rajaamaan alaikäisten mahdollisuuksia omien henkilötietojensa käsittelyyn verkkoympäristössä.

Alle 13-vuotiaalla lapselle ei ole sallittua käsitellä henkilötietojaan Suomessa sähköisenä etäpalveluna, vaan siihen tarvitaan aina vanhemman suostumus. Yleisesti ikäraja on 16-vuotta mutta EU:n jäsenvaltiot voivat itse säätää sen alemmaksi, ei kuitenkaan alle 13-ikävuoden. Käytännössä tämä tarkoittaa, että tätä nuorempien täytyy saada vanhemmiltaan lupa käyttää verkkopalveluita, jotka tallentavat henkilötietoja. (Lastensuojelun keskusliitto 2019.)

Rekisterinpitäjällä on kohtuullisin toimin velvollisuus varmistua siitä, että suostumuksen on antanut lapsen huoltaja, ei lapsi itse. Suostumukseksi ei siten välttämättä riitä rasti ruutuun-menetelmä, vaan yrityksen tulisi arvioida etukäteen luottamus siihen, että lupa todella on saatu huoltajalta. (Hanninen ym. 39.) Tällöin varmistuksena voi olla esimerkiksi kysymys, johon lapsi ei osaa itse vastata (Andreasson ym. 2023, 48).

Jos yritykset ja yhdistykset ovat tekemisissä lasten kanssa, on heillä velvoite mukauttaa lapsille suunnattu tieto sen mukaisesti. Tiedon on oltava silloin helposti saatavilla yksinkertaisella ja selkeällä kielellä.

5 TIEDONHALLINTALAKI JA VIRANOMAISTOIMINTA

Tiedonhallintalaki eli Laki julkisen hallinnon tiedonhallinnasta (Laki julkisen hallinnon tiedonhallinnasta 906/2019) koskee lähtökohtaisesti kaikkia viranomaisia. Tietosuojalain tarkoituksena on täydentää ja täsmentää EU:n yleistä tietosuoja-asetusta, sekä sen soveltamista kansallisella tasolla (Tietosuojalaki 1050 /2018, 1 luku 1 §). Tiedonhallintalain tavoitteena on viranomaisten tietoaineistojen yhdenmukainen hallinta ja tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi. Laissa säädetään (Laki julkisen hallinnon tiedonhallinnasta 906/2019) seuraavista asioista:

- Tiedonhallinnan suunnittelusta ja kuvaamisesta
- Tietoturvallisuudesta
- Tietoaineistojen muodostamisesta
- Asian ja palvelujen tiedonhallinnasta (Eduskunta.fi 2025.)

Tiedonhallinnalla tarkoitetaan tietoprosessien järjestämistä siten, että tietojen saatavuus, löydettävyys ja hyödynnettävyys eri tarkoituksiin pyritään varmistamaan tiedon elinkaaren ajan. (Krakau & Haapalehto 2020, 21.)

5.1 Tiedonhallintalaki

Tiedonhallintalaki koskee kaikkea viranomaistoimintaa Suomessa. Laki julkisen hallinnon tiedonhallinnasta, sekä siihen liittyvät lait astuivat voimaan vuoden 2020 alusta. Sen tarkoituksena on edistää tiedonhallinnan yhdenmukaistamista, tietoturvallisuutta ja digitalisointia viranomaistoiminnassa. (Valtiovarainministeriö 2024a.)

Laki on säädetty, koska sen avulla on haluttu varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi. Tiedonhallintalaki myös mahdollistaa viranomaisten tietoaineistojen turvallisen ja tehokkaan hyödyntämisen, sekä edistää tietojärjestelmien ja tietovarantojen yhteen toimimista. Lakiin sisältyy määritelmät, soveltamisalat ja niiden rajoitukset. Lain tarkoitus on myös, että sen avulla järjestetään tiedonhallinta toimintayksikössä tiedonhallintamallin mukaisesti. (Laki julkisen hallinnon tiedonhallinnasta 2019.)

Lain säännöksiä on tarkennettu asetuksilla, jotka koskevat turvallisuusluokiteltavia asiakirjoja. Näistä esimerkkinä on asetus viranomaisen velvollisuudesta tietojen siirtoon salattuna. Tiedonsiirtoja voidaan tehdä myös jollakin muulla tavoin suojattuna tiedonsiirtoyhteyttä käyttämällä. Tietojen salaaminen on tehtävä aina, jos siirrettävät tiedot ovat määritetty salassa pidettäviksi. Viranomaisella on aina vastuu käyttöoikeuksien hallinnasta sekä lokitietojen keräämisestä, jotka koskevat käyttöä ja tietojen luovuttamista eteenpäin.

Tiedonhallintalain luvussa 5, 19 §:ssä tietoaineistojen muodostamisessa määrätään seuraavaa*; ”Jos asiakirja saapuu viranomaiselle muussa kuin sähköisessä muodossa, se on muutettava sähköiseen muotoon, jos asiakirja on säädetty pysyvästi säilytettäväksi tai lailla tai lain nojalla arkistoitavaksi”*. (Laki julkisen hallinnon tiedonhallinnasta 906/2019, 5.luku 19 §.) Sähköiseen muotoon asiakirjaa muutettaessa ja siirrettäessä säilytykseen ja/tai arkistoitavaksi, on otettava huomioon asiakirjojen turvallisuusluokitus sekä niiden käsittelyä koskevat vaatimukset.

5.2 Asian- ja palvelujen hallinta

Tiedonhallintayksiköllä on velvollisuus ylläpitää asiakasrekisteriä viranomaisen käsittelyssä olevista tai olleista asioista. Jokaisella käsiteltävällä asialla on oltava oma yksilöintitunnus, jonka avulla siihen liittyvien tietojen yksilöinti tapahtuu. Tietoaineistoon muodostuneet asiakirjat on rekisteröitävä palveluja tuotettaessa sekä oltava yksilöidysti haettavissa ja jälkikäteen todennettavissa. (Laki julkisen hallinnon tiedonhallinnasta 906/2019, 6.luku 27 §.) Asiakasrekisteriä pitämällä edistetään julkisuusperiaatteen muodostumista, hyvän hallinnon sekä oikeusturvan toteutumista. Asianhallinnan laatu syntyy koko organisaation toiminnan vaikutuksesta. (Kivivasara 2020.)

5.3 Salassapidon perusteet viranomaistoiminnassa

Laissa ei ole olemassa tarkkaa ohjetta viranomaistoiminnan salassa pidettävien asiakirjojen käsittelystä. Valmisteltavana eri viranomaistahoilla on julkisen hallinnon tiedonhallintalain pohjalta laadittuja suosituksia tätä koskien useampiakin. Verkkojulkaisuna löytyy esimerkiksi lautakunnille suunnattu suositus, jota myös muita kehotetaan käyttämään. Tämä opas on Valtiovarainministeriön ja tiedonhallintalautakunnan yhdessä kokoama vuodelta 2023 (Valtionvarainministeriö 2024b). Myös Digi- ja väestötietovirasto on julkaissut oman suositusluonnoksensa vuonna 2021 Tiedonhallintalautakunnan alaisessa tietoturvallisuussuositusten valmistelujaostossa. Tässä tiiviissä 15 sivuisessa oppaassa on kattavasti käsitelty salassapitovelvollisuutta, ja asiakirjojen käsittelyä. (Kinnunen, E. 2021).

6 TIETOSUOJA TYÖSUHTEESSA

6.1 Työntekijöiden henkilötietojen käsittely työsuhteen yhteydessä

Työntekijöiden henkilötietojen käsittelystä säädetään laissa yksityisyyden suoja työelämässä, joka on säädetty vuonna 2004 (Laki yksityisyyden suojasta työelämässä 759/2004, 1 luku 2 §). Laki on osittain kumottu ja muutettu vuonna 2019. Työntekijän oikeuden yksityisyyteen katsotaan olevan yleisesti tunnustettu perus- ja ihmisoikeus, joka sisältää oikeuden henkilötietojen suojaan. Henkilötietojen suojalla suojataan työntekijää henkilönä, hänen oikeuttaan ja etujaan. Työntekijän itsemääräämisoikeuteen kuuluu lähtökohtainen oikeus päättää itseään koskevista tiedoista ja vaikuttaa omien tietojen käsittelyyn. (Alapuranen ym. 2020, 7.)

Laki määrää, että työnantajalla on oikeus käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja. Tietojen on liityttävä suoraan työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen, työnantajan työntekijöille tarjoamiin etuuksiin tai niiden on johduttava työtehtävien erityisluonteesta. Tarpeellisuusvaatimuksesta ei voida poiketa edes työntekijän suostumuksella. Yrityksen on aina arvioitava työntekijöiden henkilötietojen käsittelyä oikeutetun edun lisäksi myös tietojen tarpeellisuuden perusteella. (Hanninen ym. 2017, 33.)

Työnantajalla on velvollisuus kerätä työntekijän henkilötietoja vain työntekijältä itseltään. Jos työnantaja kerää tietoja muilta, on se tehtävä vain hankkimalla ensin lupa työntekijältä siihen. Suostumusta ei kuitenkaan tarvita, jos viranomainen luovuttaa tietoja työnantajalle tämän laissa säädetyn tehtävän suorittamista varten tai jos tietotojen keräämisestä tai saamisesta laissa erikseen nimenomaisesti säädetään. Tällaisia tapauksia ovat esimerkiksi *turvallisuus selvitykset*. (Laki yksityisyyden suojasta työelämässä 759/2004, 1 luku 4 §).

6.2 Tietosuojavastaava

EU:n tietosuoja-asetuksen 37 artiklassa säädetään, että se edellyttää, että henkilötietojen käsittelijän ja rekisterinpitäjän on tietyissä tilanteissa nimitettävä tietosuojavastaava (Asetus 2016/679/EU, 37 artikla). Yrityksillä tietosuojavastaava on nimitettävä, jos toiminnan ydintehtävät muodostuvat henkilötietojen käsittelytoimista, tai jotka luonteensa, laajuutensa tai tarkoituksensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. Myös sillä on aina vaikutusta, jos käsiteltävänä on arkaluonteisia tietoja. Viranomaisilla ja julkishallinnon elimillä tietosuojavastaavan nimittäminen on aina pakollista. (Aalto-Setälä & Viitala 2018, 10.) Yleisen määritelmän mukaan tietosuojavastaava on organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa (Asetus 2016/679/EU, 37 artikla).

Tietosuojavastaavan nimittäessä olisi hyvä ottaa huomioon tehtävään nimitettävän tietosuojalainsäädännön ja alan käytänteiden tuntemus. Hänellä täytyy olla jo lähtökohtaisesti hyvä asiantuntemus, koska EU:n yleisessä tietosuoja-asetuksessa määritellään, että tietosuojavastaavaa nimitettäessä on huomioitava henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä sekä valmiudet toteuttaa artiklassa 39 määritellyt tehtävät. (Asetus 2016/679/EU, 39 artikla.)

Tämän lisäksi tietosuojavastaavan tulisi tuntea käytännössä tapauskohtaisesti eri toimintoja säätelevä erityislainsäädäntö ja sen soveltaminen. (Andreasson & Ylipartanen 2022, 249.) Tietosuojavas-

taava on aina riippumaton henkilö, eikä hän voi ottaa vastaan ohjeistuksia tehtävän hoitamisen yhteydessä. Tietosuojavastaavalla on raportointivelvollisuus suoraan henkilötietojen käsittelijän tai rekisterinpitäjän ylimmälle johdolle. Tietosuojavastaava voi olla organisaation jäsen, tai hän voi toimia tehtävässään myös palvelusopimuksen perusteella. (Sulin, I. 2017.)

Tietosuojavastaavaa ei ole lain mukaan lupa erottaa tai rangaista tietosuojatehtävien hoitamisen vuoksi. Tietosuojavastaavan keskeinen tehtävä on toimia neuvonantajana työnantajalleen sekä työntekijöilleen asioista, jotka liittyvät henkilötietojen käsittelyyn. Hänen tehtäviinsä kuuluu seurata organisaatiossa ilmeneviä puutteita ja tuoda esiin niitä. Tietosuojavaltuutetun tehtävänä on olla myös rekisteröityjen sekä tietosuojavaltuutetun yhteyshenkilö. Hänelle on myös hyvä nimittää varahenkilö poissaolojen varalta esimerkiksi tietoturvaloukkaus ilmoitusten tekemiseksi. (Tietosuojavaltuutetun toimisto 2024.) Tietoturva ilmoitus on tehtävä ilman aiheetonta viivytystä valvontaviranomaiselle, jos tietoturvaloukkaus on päässyt tapahtumaan, ja se aiheuttaa riskiä luonnollisten henkilöiden oikeuksille ja vapauksille. Ilmoituksen tulee sisältää vähintään tietoturvaloukkauksen kuvaus, sekä tiedot loukkauksen kohteena olevista rekisteröidyistä henkilöistä, tietosuojatyyppien mukaisista ryhmistä ja niiden arvioiduista lukumääristä. Ilmoituksessa tulee mainita myös tietosuojavastaavan yhteystiedot tai muu taho, josta lisätietoa tapahtuneesta on saatavilla. Myös mahdolliset seuraukset ja tulevat toimenpiteet asiaan liittyen tulee arvioida ilmoituksessa. (Hanninen ym. 2025, 109–111.)

Organisaatiossa tietosuojavastaavan toimenkuva saattaa jäädä epäselväksi, ja työyhteisössä ei tiedosteta mitä siihen kuuluu. Esimerkiksi organisaatioon voi olla nimettynä tietosuojavastaava johdon toimesta, mutta nimitetyllä ei välttämättä ole oikein tietoa mitä se sisältää. Johto voi olla siinä uskossa, että he ovat hoitaneet oman osansa velvollisuuksista, ja siirtäneet vastuun tietosuojavastaavalle. Nimitetyllä tietosuojavastaavalla ei varmaankaan ole riittävästi tietoa organisaatiossa olevien erilaisten työtehtävien sisällöstä, varsinkaan jos tietoturvasuunnitelmaa ei ole laadittu eri työtehtävien pohjalta. Eri osastot eivät välttämättä osaa asiasta kysyä, koska eivät tunne ja tunnista riittävästi tietosuojaan liittyviä ongelmia työssään. Tällöin työntekijät voivat olla siinä uskossa, että he hoitavat asian oikein, kun kukaan ei sen hoitamisesta ole koskaan valittanut. Näin jokainen tavallaan siirtää vastuuta aina seuraavalle, ilman että kukaan tunnistaa toimivansa väärin tai puutteellisesti asian toteuttamisen kannalta.

7 JULKISUUSPERIAATE

Julkisuusperiaate merkitsee oikeutta saada tietoja viranomaisten toiminnasta ja sen on tarkoitus parantaa kansalaisten osallistumismahdollisuuksia yhteiskunnalliseen toimintaan. Julkisuusperiaate antaa myös mahdollisuuden valvoa julkisen vallan käyttöä sekä viranomaisten toimintaa. Julkisuusperiaate Suomessa on kansainvälisellä mittapuulla hyvinkin laaja, eikä tiedon pyytämistä tarvitse perustella mitenkään. (Korpisaari ym. 2022, 19.)

7.1 Julkisuusperiaate

Julkisuusperiaatteen mukaan viranomaisten asiakirjat ovat aina julkisia, jollei tässä tai muussa laissa erikseen toisin säädetä. Tämän säätää laki viranomaisen toiminnan julkisuudesta (Laki viranomaisen toiminnan julkisuudesta 621/1999). Lain mukaan jokaisella on oikeus saada tietoja viranomaisen julkisista asiakirjoista. Suomessa vallitsee siis julkisuusperiaate. Lailla viranomaisten toiminnan julkisuudesta säädellään viranomaisten asiakirjojen ja muiden tietoaineistojen julkisuutta ja salassapitoa sekä tiedon antamista asiakirjasta ja siihen liittyvä menettelyä. Lisäksi laissa on säännökset viranomaisten velvollisuudesta edistää tiedonsaantia. (Valtionneuvoston kanslia 2024.)

Viranomaisen asiakirja määritellään laissa asiakirjaksi;

- *”jonka viranomainen tai sen palveluksessa oleva on laatinut*
- *joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa.*

Viranomaisen laatimana pidetään myös asiakirjaa;

- *joka on laadittu viranomaisen antaman toimeksiannon vuoksi*
- *viranomaiselle toimitettuna asiakirjana asiakirjaa, joka on annettu viranomaisen toimeksiannosta tai muuten sen lukuun toimivalle toimeksiantotehtävän suorittamista varten”.* (Laki viranomaisen toiminnan julkisuudesta (621/1999, 1.luku, 5 §.)

7.2 Julkisuuslaki

Julkisuuslaki on yleislaki, joka koskee viranomaisille tehtäviä tietopyyntöjä. Se on perustuslaissa säädetty, ja siitä voidaan poiketa vain lain erityissäännöksin. Tämän lain tarkoituksena on toteuttaa avoimuuden toteuttaminen viranomaistoiminnassa, sekä antaa yksilöille ja yhteisöille mahdollisuus valvoja julkisen vallan ja julkisten varojen käyttöä. (Krakau & Haapalehto 2020, 21.) Julkisuusperiaate antaa kansalaisille mahdollisuuden osallistua toimintaan yhteiskunnassa ja valvoa julkisen vallan käyttöä ja viranomaisten toimintaa. (Korpisaari ym. 2022, 18.)

Tietopyyntöä ei löydy suoraan käsitteenä lainsäädännöstä. Julkisuuslaki kuitenkin takaa jokaiselle oikeuden pyytää viranomaisten tietoja. Tiedonhallintalain tarkoituksena on säätää julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta viranomaisten tiedonhallinnassa. Tiedonhallintalaki koskee mm. viranomaistoimintaa, tuomioistuimia, valtion liikelaitoksia, kunnallisia viranomaisia sekä yliopistoja ja ammattikorkeakouluja. Tiedonsaannin kannalta ei ole merkityksellistä se, missä muodossa tieto on, vain tiedon sisältö. Asiakirjojen muoto on pääasiallisesti oltava sähköinen 1.1.2021 alkaen, eli vuosi tiedonhallintalain voimaan astumisen jälkeen. Tämä koskee kaikkia viran-

omaisille saapuvia ja viranomaisen laatimia uusia asiakirjoja. Ennen lain voimaantuloa muodostuneita tietoaineistoja säilytetään siten kuin ne ovat muodostuneet ennen siirtymäajan päättymistä. (Krakau & Haapalehto 2020, 34.)

7.3 Viranomaistiedot

Jokaisella on oikeus pyytää viranomaistietoja (Laki viranomaisen toiminnan julkisuudesta 621/1999, 3. luku, 9. §). Viranomaisilla on velvollisuus avustaa tiedon pyytäjiä tiedon etsinnässä, esimerkiksi halutun asiakirjan yksilöimisessä (Oikeusministeriö 2024). Tieto asiakirjasta on yleensä annettava pyytäjälle hänen haluamallaan tavalla, jollei siitä aiheudu kohtuutonta haittaa viranomaisen toiminnalle. Tieto on annettava viivytyksettä, kuitenkin pääasiassa viimeistään kahden viikon kuluessa asiakirjapyynnön saamisesta.

Jos päätös luovuttamisesta evätään, on se perusteltava sekä päätöksestä on käytävä syy siihen ilmi. Jos tieto evätään, on henkilöllä oikeus pyytää asia viranomaisen ratkaistavaksi. (Oikeusministeriö 2024.)

7.4 Asianosaisen tiedonsaantioikeus

Asianosaisella on oikeus saada tieto niistä viranomaisen asiakirjoista, jotka ovat voineet vaikuttaa hänen asiansa käsittelyyn. Tiedonsaantioikeus on tavallista laajempi, koska asianosaisella on oikeutenaan saada omaan tietoonsa myös salattuja asiakirjoja. (Valtionneuvoston kanslia 2024.) Asianosaisella tässä yhteydessä tarkoitetaan henkilöä, jonka etua oikeutta tai velvollisuutta asia koskee. (Oikeusministeriö 2024.)

Asianosaisella on mahdollisuus tarkistaa rekisterinpitäjiltä mitä häntä koskevia henkilötietoja he käsittelevät. Tällöin rekisteröidyn on myös mahdollista varmistaa tietojen oikeellisuus. Jokaisella rekisteröidyllä henkilöllä on oikeus saada jäljennös omista tiedoistaan rekisterinpitäjältä, siltä osin mitä ne henkilökohtaisesti koskevat. Oikeuksiin kuuluu myös saada tietoa lisäksi;

- Siitä mistä henkilötieto on hankittu?
- Miksi ja kuinka kauan sitä tarvitaan?
- Onko tiedon käsittelyssä käytetty automaattista päätöksentekoa?
- Onko henkilötietoja luovutettu tai aiottu luovuttaa eteenpäin sekä onko niitä siirretty EU:n ulkopuolelle?
- Rekisterinpitäjällä on vastausaikaa tietopyyntöön yksi kuukausi. Rekisterinpitäjä voi myös pyytää jatkoaikaa joissain tapauksissa, jolloin käsittelyaikaa on kolme kuukautta. Tiedonsaantia voidaan rajoittaa, jos erimerkiksi vaikkapa todistajien tietoja on salattava oikeudenkäynnissä. Tiedonsaannin rajoitus voi olla voimassa, jos tapauksen käsittely on keskeneräinen. Rekisterinpitäjällä ei ole oikeutta kieltäytyä vastaamasta tietopyyntöön kuin ainoastaan lakiperusteisesti. (Tietosuojavaltuutetun toimisto 2024.)

7.5 Viranomaisen laatimien asiakirjojen julkiseksi tulo

Asiakirjan katsotaan tulleen julkisesti pääsääntöisesti silloin, kun viranomainen on saanut asiakirjan tehtyä valmiiksi käyttötarkoitustaan varten. Asiakirjan julkisuuteen ei ole vaikutusta sillä, onko asia-

kirjan kuvaamasta asiasta parhaillaan tekemässä jotain päätöstä, tai mikä käsittelyvaihe sillä on parhaillaan menossa. Julkiseksi tuloon riittää se, että se on valmis käytettäväksi. (Krakau & Haapalehto 2020, 43.)

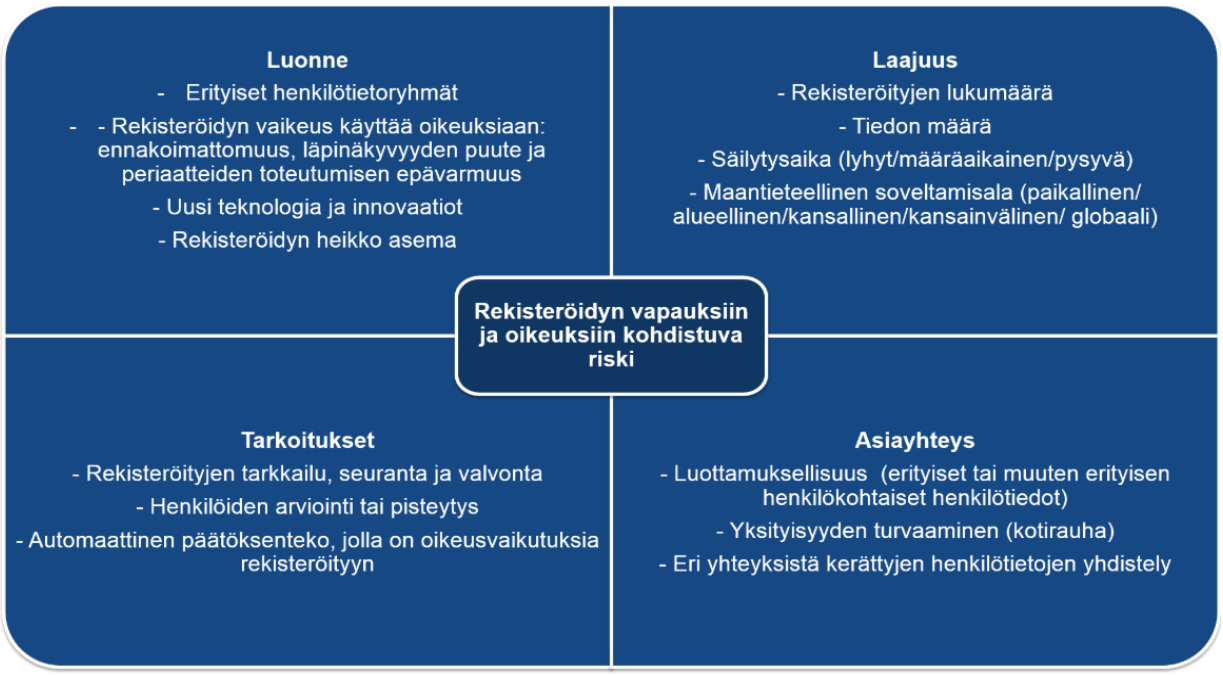
8 RISKIANALYYSI JA VAIKUTUSTENARVIOINTI

Rekisterinpitäjällä on oltava selkeä suunnitelma henkilötietojen käsittelyä koskevaa riskien tunnistamista varten. Riskianalyysin tekeminen on tähän hyvä työkalu. Rekisterinpitäjän velvollisuus on myös ratkaista, onko hänellä tarve tehdä vaikutustenarviointi, ja onko se lainmääräämää kyseisessä tilanteessa.

8.1 Riskien arviointi ja analyysin tekeminen

Riskianalyysin tekeminen on kannattavaa rekisterinpitäjälle, koska sen avulla riskien tunnistaminen jo suunnitteluvaiheessa on helpompaa niiden hallinnan kannalta. Riskianalyysin avulla rekisterinpitäjä voi hallita ja turvata henkilötietojen asianmukaista käsittelyä, sekä varmistaa tietosuojaperiaatteiden tehokas toteutus.

Rekisterinpitäjällä on oltava selkeä käsitys sen omasta henkilötietojen käsittelystä, jonka pohjalta riskiarviota tehdään. Arvioon on otettava huomioon käsittelyn luonne, sen laajuus, asiayhteydet sekä tarkoitukset. (Tietotosuojavaltuutetun toimisto 2024.)



Kuva 1. Kuvaleike Tietosuojavaltuutetun toimiston verkkosivulta vaikutustenarviointi (Tietosuojavaltuutetun toimisto 2024)

Kuvassa 1 on riskiarvio, jonka mukaan rekisterinpitäjä voi selkeyttää käsitystään omasta henkilötietojen käsittelytavastaan. Riskiä voidaan arvioida seuraavalla tavalla:

- Riskin **luonnetta** arvioitaessa otetaan huomioon, millaisesta riskistä on kyse? Tällöin vaikutusta on rekisteröidyn asemalla sekä oikeuksilla. Jos käsiteltävissä tiedossa on esimerkiksi erityisiksi luokiteltuja henkilötietoryhmiä, kasvaa riskin määrä. Uutta teknologiaa ja innovaatioita käyttöön otettaessa on oltava hyvin varovainen, koska niitä koskevista haavoittuvuuksista ei ole vielä tietoa tarpeeksi saatavilla.
- Riskin **laajuutta** arvioitaessa otetaan huomioon se, kuinka suuresta rekisteröityjen määrästä on kyse. Mitä enemmän tietoa ja rekisteröityjä lukumääräisesti, sitä suurempi riski tietojen vuodon

määrälle. Säilytysaikaa rajoittamalla mahdollisimman lyhyeksi lain puitteissa, pystytään kertyvän tiedon määrän tehokkaaseen minimointiin, Eli ei säilytetä tietoja turhaan.

- Rekisteröityjen tietojen **tarkoitus** määritellään riskiarviossa sen mukaan, mitä tiedolla tehdään? Tähän käyttötarkoitukseen kuuluvat esimerkiksi potilaskirjaukset terveydenhuollossa, työntekijöiden valinta tai suoramarkkinointi. (Hanninen ym. 2017, 49.)
- Tiedon **asiayhteyttä** arvioidaan riskin kannalta sen mukaan, millaista kerätty tieto on? Jos kerätty tieto sisältää esimerkiksi erityisen henkilökohtaisia henkilötietoja, seuraa niiden käsittelystä suurempi riski luottamuksellisuuden kannalta. Myös tietojen yhdisteleminen voi aiheuttaa riskin, jolloin esimerkiksi tunnistetietoja päätyy rekistereihin, joihin ne eivät kuulu, tai tieto ei enää kuulu siihen asiayhteyteen.

8.2 Riskien tunnistamisen merkitys

Rekisterinpitäjän määrittäessä teknisiä ja organisatorisia toimenpiteitä, riskien tunnistamisen merkitys korostuu. Näiden toimien tarkoituksena on varmistaa tietosuojan toteutuminen henkilötietojen käsittelyssä. Teknisiksi ja organisatorisiksi toimenpiteiksi kutsutaan esimerkiksi henkilöstölle annettuja ohjeita tietosuojan toteuttamiseksi. Näitä toimenpiteitä voi olla myös vaikkapa omavalvonnan kautta tapahtuva käytönvalvonta sekä tietojärjestelmien tietoturva ja tietojen salaaminen (Tietosuojavaltuutetun toimisto 2024.)

Riskiarviointi ei ole vain kerran tehtävä toimenpide, vaan sen on oltava jatkuvaa ja riittävää toimivuuden kannalta. Riskejä arvioidaan ja päivitetään aina tarvittaessa. Tätä kutsutaan riskiperusteiseksi lähestymistavaksi, ja rekisterinpitäjällä on osoitusvelvollisuus tämän noudattamisessa. (Tietosuojavaltuutetun toimisto 2024.)

Organisaation riittävällä ja jatkuvalla koulutuksella sekä ohjeistuksella on suuri merkitys riskien tunnistamisen kannalta (Aalto-Setälä & Viitala 2018, 35). Riskien havainnointi, tunnistaminen ja ennakointi paranee tämän myötä, ja myös päivittäminen helpottuu.

8.3 Vaikutustenarviointi

Vaikutustenarviointi on prosessi, jonka avulla tarkastellaan tietosuojan toteuttamiseksi suunniteltuja toimenpiteitä, suojatoimia ja mekanismeja, joiden avulla lievennetään henkilötietojen käsittelystä luonnollisten henkilöiden oikeuksille aiheutuvia riskejä. Vaikutustenarviointi eli DPIA on lyhenne sanoista Data Protection Impact Assesment. (Hanninen ym. 2017, 115–119.)

Vaikutustenarvioinnin tarkoituksena on aina kuvata, miten ja millaisia henkilötietoja käsitellään sekä kerätään. Rekisterinpitäjän on myös aina varmistettava tietojen tarpeellisuus ja oikeasuhtaisuus. Vaikutustenarviointi on jatkuvaa, ja sitä on tehtävä koko prosessin ajan aktiivisesti. Vaikutustenarviointi tehdään aina ennen kuin henkilötietojen käsittelyä aloitetaan. Vaikutusten arvioinnin tarkoituksena on aina kartoittaa vakavimmat riskit, joiden torjuntaan erityisesti on kannattavinta panostaa eniten. (Hanninen ym. 2017, 115–119.)

Vaikutustenarvioinnin tekeminen on aina pakollista, jos henkilötietojen käsittelystä mahdollisesti aiheutuu korkea riski henkilöiden oikeuksille ja vapauksille. Tavoitteena on arvioida jäljelle jääneen riskin oikeutus ja hyväksyttävyys vallitsevissa olosuhteissa. Vaikutustenarvioinnin tarkoituksena ei ole hankaloittaa rekisterinpitäjän työtä, vaan olla apuna tietosuojalainsäädännön noudattamisessa, sekä sen dokumentoinnissa ja osoittamisessa. (Tietosuojavaltuutetun toimisto 2024.)

Jos rekisterinpitäjä on nimittänyt tietosuojavastaava tehtävään, on hänellä neuvonantovelvollisuus vaikutustenarvioinnin tekemisessä. Muuten auttajana toimii henkilötietojen käsittelijä. (Tietosuojavaltuutetun toimisto 2024.)

Tietosuojavaltuutetun toimisto on antanut oman listauksensa toimista, joiden käsittelytoimien yhteydessä tulee aina tehdä vaikutustenarviointi. Lisäksi arviointi voidaan joutua tekemään myös tilanteissa, joissa siihen on määräys kansallisessa lainsäädännössä. Esimerkkinä yleisölle avoimen alueen valvonta järjestelmällisesti ja laajamittaisesti, sekä rikostuomioiden ja terveystietojen käsittely. Myös uuden teknologian käyttäminen henkilötietojen käsittelyssä tarvitsee vaikutustenarvioinnin tekemisen ennen henkilötietojen käsittelyn aloittamista. Erityisesti vaikutustenarviointi vaaditaan tilanteissa, joissa ihmisten henkilökohtaisia ominaisuuksia arvioidaan automaattisen käsittelyn keinoin, ja se johtaa päätöksiin, joilla on ihmisiä koskevia oikeusvaikutuksia tai muita merkittäviä vaikutuksia. Tällaisia voivat olla vaikkapa luottopäätökset verkon välityksellä tapahtuvan henkilön taloudellisen profiloinnin perusteella. (Hanninen ym. 2017, 115.)

Vaikutustenarviointi on tehtävä aina ennen kuin henkilötietoja aletaan käsitellä, eli arviota on tehtävä jo silloin, kun tietojen keräämistä aletaan suunnitella. Vaikutustenarviointia on myös mahdollisesti täydennettävä myös jatkossa ja huolehdittava sen ajantasaisesta päivittämisestä. Myös käsittelytoiminnan aiheuttamat riskit ovat vaikutustenarvioinnissa otettava huomioon. Riskien arviointi on tehtävä aina niiden ihmisten näkökulmista, joiden henkilötiedoista on kysymys. Vaikutustenarvioinnin tarkoituksena on aina auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. (Tietosuojavaltuutetun toimisto 2024). Tietoturvariskin toteutuessa ja vahingon sattuessa sen suuruuteen vaikuttaa paljon menetettävien tietojen arvo. Menetettävää arvoa vahingossa voi tulla myös organisaation maineelle, brändille ja luotettavuudelle. Myös ulkopuolisille voidaan joutua maksamaan korvauksia merkittäviä summia.

8.4 Riskiperusteinen lähestymistapa

Tietosuojasääntelyssä on omaksuttu riskiperusteinen lähestymistapa. Sen tarkoituksena on, että tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet suhteutetaan henkilötietojen käsittelyssä rekisteröidyn oikeuksille ja vapauksille mahdollisesti aiheutuvaan riskiin. Toisaalta tavoitteena on myös välttää vähäriskisten toimien ylisääntelyä. Erityisesti korkean riskin toiminnassa on huomioitava rekisteröidyn suoja riittävällä tasolla. Korkean riskin toiminnassa arvioidaan erityisen tarkasti muun muassa tietojen laatua, luonnetta, käsittelytarkoitusta ja niiden laajuutta. (Tietosuojavaltuutetun toimisto 2024.)

Kirjassa Osaava tietosuoja vastaava 2022, tietosuoja-asetuksen riskeillä tarkoitetaan henkilötietojen käsittelystä rekisteröidyille mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja esimerkiksi silloin, kun käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon, pseudonymisoinnin kumoutumiseen tai vaikka arkaluonteisten tietojen paljastumiseen sivulliselle. (Andreasson & Ylipartanen 2022, 32.)

9 TIETOSUOJALOUKKAUKSET JA LAIMINLYÖNNIT TETOTURVAN OSALTA

Tietoturvan ja tietosuojan parantamiseen Suomessa herättiin kunnolla Psykoterapiakeskus Vastaamon tapauksen myötä. Suuri tietomurto tapahtui vuosina 2018–2019, ja tuli julkiseksi lokakuussa 2020, jolloin varastettuja henkilö- ja potilastietoja julkaistiin Tor-verkossa tarkoituksena kiristää julkaisuilla rahaa. Tapaus koski lähes 40 000 potilasta. (Kärkkäinen 2021.)

Liikenne- ja viestintäministeriö asetti ajalle 9.11.2020 -31.1.2021 erillisen työryhmän selvittämään tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla. (Valtionneuvoston kanslia 2020). Työryhmä esitti loppuraportissaan lainsäädännön muutostarpeita ja muita toimenpiteitä tietoturvan ja tietosuojan parantamiseksi. Toimenpiteissä painotetaan erityisesti viranomaisten entistä tehokkaampaa ja järjestäytyneempää yhteistyötä, sekä tarvetta velvoittaviin tietoturvavaatimuksiin. (Valtionneuvoston kanslia 2020.) Myös vaatimusten säännölliseen arviointiin ja valvontaan otettiin kantaa loppuraportissa. (Lehtilä, Nyström, Ronikonmäki, Sirviö 2021.)

Loppuraportissa asiaa käsitellään seuraavasti:

” Psykoterapiakeskus Vastaamoon kohdistunut tietomurto osoitti, miten tietomurto tai kyberhyökkäys voi vaikuttaa merkittävästi tavallisten ihmisten arkeen ja paljastaa erittäin arkaluonteisia tietoja ihmisten elämästä. Tietomurrot ja tietosuojaloukkaukset voivat taloudellisten vaikutusten lisäksi aiheuttaa myös syvää inhimillistä kärsimystä, jonka merkitystä yhteiskunnallisena ja oikeudellisena epäkohtana ei pidä väheksyä. Julkisen vallan tehtävänä on perustuslain nojalla turvata kansalaisten yksityiselämän suoja ja muut perusoikeudet. Yksin viranomaistoimilla riittävää turvallisuustasoa ei kuitenkaan ole mahdollista saavuttaa, vaan tietoturvan ja tietosuojan merkitys on tunnistettava kaikkialla yhteiskunnassa ja myös yksityisen sektorin toimijoiden on sitouduttava siihen”. (Lehtilä ym. 2021.)

Tämän tapauksen myötä nousi esille tietomurtotapaukseen liittyvien näkökohtien selvityksessä se, että Suomessa on käytössä tietojärjestelmiä, joiden tietoturvan ja tietosuojan taso ei ole riittävällä tasolla siten kuin EU:n tietosuojalainsäädäntö edellyttää. (Valtionneuvoston kanslia 2020.)

9.1 Henkilötietojen tietoturvaloukkaus

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietosuoja-asetuksessa tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. Rekisterinpitäjällä sekä henkilötietojen käsittelijällä on aina vastuu kartoittaa tietoturvaan liittyvät riskit sekä pyrittävä ne käytettävissä olevin kohtuullisin keinoin ehkäisemään. (Hanninen ym. 2017, 17.)

Esimerkkejä tapauksista, joissa kyseessä on henkilötietojen tietoturvaloukkaus voi olla vaikkapa varastetuksi päätynyt kannettava tietokone, kadonnut muistikortti tai kovalevy, hakkerointi/haittaohjelmatartunta tai salaista tietoa sisältävän asiakirjan päätyminen väärälle henkilölle vaikkapa postittamisen seurauksena. Tällaisista tapauksista voi seurauksena olla esimerkiksi identiteettivarkaus tai petos. Rekisterinpitäjän velvollisuuksiin kuuluu arvioida riskin taso, mikä mahdollisesta tietoturvaloukkauksesta voi aiheutua sen kohteeksi joutuneille henkilöille. Tietojen suojaaminen on tehtävä arvioidun riskitason mukaan. Rekisterinpitäjällä on oltava myös laadittuna toimintaohjeet mahdollisia

tietoturvaloukkaustilanteita varten, ja niihin on pystyttävä reagoimaan mahdollisimman nopeasti. Riskin tason mukaan määritetään ne toimenpiteet, joihin rekisterinpitäjällä on velvollisuus ryhtyä. (Tietosuojavaltuutetun toimisto 2024).

Kaikki henkilötietojen tietoturvaloukkaukset sekä niistä aiheutuneet seuraukset kannattaa aina dokumentoida kaiken varalta. Tietosuoja-asetus vaatii dokumentointi- ja ilmoitusvelvollisuuden täyttämistä. EU:n tietosuoja-asetuksen mukaan rekisterinpitäjän on myös huolehdittava siitä, että tietojen saatavuus ja pääsy niihin turvataan mahdollisimman pikaisesti fyysisen tai teknisen vian sattuessa. (Asetus 2016/679/EU, 32 artikla.)

9.2 Tietovuodon seurauksien vakavuus

Tietosuojavaltuutetun toimiston mukaan tietoturvaloukkauksen seurausten voidaan katsoa olevan erityisen vakavia esimerkiksi silloin, kun siitä voi seurata identiteettivarkaus, petos, psyykkistä ahdistusta, nöyryytystä tai maineen menetys. (Tietosuojavaltuutetun toimisto 2024.).

Myös sillä, kenenkä haltuun tiedot ovat päätyneet, voi olla vaikutusta siihen, mitä seurauksia on odotettavissa. Väärinkäytön todennäköisyys on mahdollisesti aina suurempi, jos tietojen tiedetään päätyneen rikolliseen toimintaan. Arvioidessa tietoturvaloukkaukseen liittyvää riskiä, on otettava huomioon tietoturvaloukkauksesta mahdollisesti aiheutuvan seurauksen vakavuus ja todennäköisyys

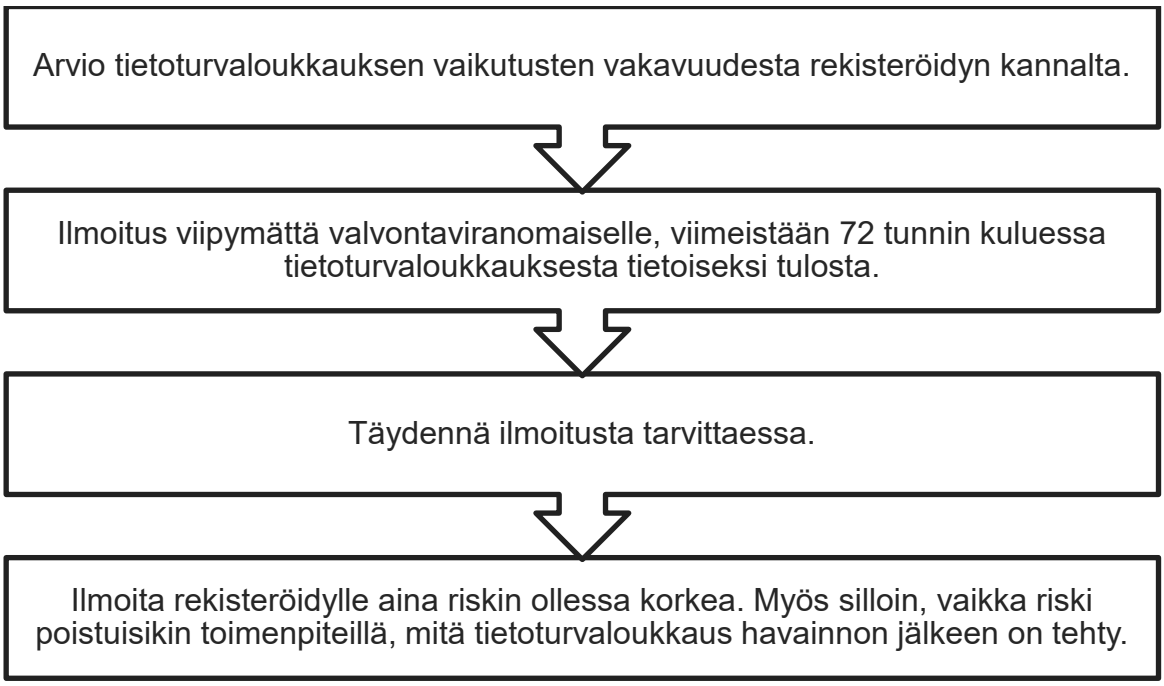
Rekisterinpitäjän ominaisuus vaikuttaa paljolti siihen, kuinka suuri riski tietoturvaloukkauksesta voi koitua. Esimerkkinä koulun oppilasrekisteri tai sairaalan potilastietokannan tietoturvaloukkaus aiheuttaa varmasti suuremman riskin kuin vaikkapa sanomalehden tilaajarekisteri. (Tietosuojavaltuutetun toimisto 2024).

9.3 Tietoturvaloukkauksesta ilmoittaminen viranomaiselle

Henkilötietojen tietoturvaloukkauksista on velvollisuus ilmoittaa aina valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille (Asetus 2016/679/EU, 33 artikla). Suomessa valvontaviranomaisena toimii tietosuojavaltuutetun toimisto. (Tietosuojavaltuutetun toimisto 2024).

Rekisterinpitäjän on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta viipymättä ja mahdollisuuksien mukaan 72 tunnin kuluessa tietosuojaloukkauksesta tietoiseksi tulostaan tietosuojavaltuutetun toimistolle. Jos ilmoituksen toimittaminen jostain syystä viivästyy, on rekisterinpitäjä velvollinen perustelemaan syyt valvontaviranomaiselle. Henkilötietojen käsittelijän täytyy ilmoittaa tietoturvaloukkauksesta ensin rekisterinpitäjälle, jollei erikseen ole tehty sopimusta, että käsittelijä voi ilmoituksen tehdä suoraan. Vastuu ilmoituksen tekemisestä on kuitenkin aina rekisterinpitäjällä. Ilmoituksen tekeminen onnistuu sähköistä lomaketta käyttäen. Ilmoituksen voi tehdä suoraan, tai alustavana ilmoituksena, jota täydennetään jälkikäteen ilmoituksen tekijän toimesta oma-aloitteisesti. (Tietosuojavaltuutetun toimisto 2024.)

Arvioidessa tietoturvaloukkauksesta aiheutuneita vaikutuksia ja vakavuutta, arvio tehdään aina rekisteröidyn kannalta, ei rekisterinpitäjän. Jos vaikutukset ovat *korkeat* tai *hyvin korkeat*, tulee rekisterinpitäjän ilmoittaa tapahtuneesta rekisteröidylle viivytyksettä. Tällä turvataan rekisteröidyn mahdollisuuksia suojautua esimerkiksi sulkemalla luottokorttinsa. Jos rekisterinpitäjä on arvioinut mahdolliset vaikutukset liian mataliksi, voi tietosuojavaltuutetun toimisto määrätä ilmoituksen tehtäväksi loukkauksen kohteeksi joutuneelle. (Tietosuojavaltuutetun toimisto 2024.)



Kaavio 2: Kaavio tietoturvaloukkauksen ilmoituksessa huomioitavista asioista (tietosisältö Tietosuojavaltuutetun toimisto 2024).

10 TUTKIMUKSEN TOTEUTTAMINEN

Lähtökohta tämän opinnäytetyön toteuttamiselle oli tutkia ja koostaa tietoa oikeuksista, velvollisuuksista sekä ohjeistuksista, joiden avulla tietosuojaa toteutetaan yrityksissä, yhteisöissä ja organisaatioissa. Opinnäytetyön koostaminen aihealueena oli minulle tärkeää, koska havaintojeni ja omien kokemuksieni kautta en ole aiemmin saanut riittäviä vastauksia siihen, mitä tietosuoja työelämässä tarkoittaa, ja mitä kaikkea minun tarvitsee tietää? Toimintatavat organisaatioissa eroavat toisistaan usein huomattavan paljon eri viranomaisten kesken, ja ohjeistusta asiasta on aina ollut saatavilla hyvin vaihtelevasti. Myös tiedottaminen siitä, mistä tietoa kannattaa asiasta hakea, on kokemusteni pohjalta ollut joskus puutteellista asian suhteen.

Tietosuojalaki ja siihen läheisesti liittyvät asetukset ovat hyvin laaja kokonaisuus, ja termit usein kovin samankaltaisia. Materiaalia, lainsäädäntöä, kirjallisuutta ja verkkojulkaisuja aihepiiriin liittyen on valtavasti. Suuri työ tässä opinnäytetyössä oli kerätä kaikesta saatavilla olevasta materiaalista tietämyksen kannalta vain olennaisin tieto, sekä koostaa siitä riittävän tietosuojatason täyttävä tiivis kokonaisuus. Tämän pohjalta kävin läpi hyvin paljon erilaista virallista lähdemateriaalia, sekä peilasin saatavissa olevaa tietoa omiin havaintoihini aihealueeseen liittyen. Tämän tutkimuksen tarkoituksena oli tehdä laajasta aineistopohjasta tiivistelmä, jonka avulla välittyisi kaikkein olennaisin tieto kirjallisessa muodossa. Lähestymistapa aihealueeseen tässä opinnäytetyössä tulee työntekijän tarpeista ja työelämän lähtökohdista.

Tiedon ajantasaisuuden tarkastaminen oli suuressa roolissa tätä opinnäytetyötä kirjoittaessa. Lakien, asetusten ja ohjeistusten tieto täytyi aina varmistaa voimassaolon näkökulmasta. Myös sillä oli oleellinen merkitys, oliko kyseessä lain päivittäminen, kumoaminen vai vasta sen valmisteleminen. Myös virallisten tietolähteiden tunnistaminen, varsinkin verkossa oli välillä haastavaa. Usein esimerkiksi ministeriöiden sivustoilla löytyi artikkeleita aiheeseen liittyen. Niiden pohjalta saattoi muodostua aivan erilainen käsitys, kun vertasi tietoa kirjallisuuteen tai ajantasaiseen lakitekstiin.

Koostin opinnäytetyötä laajasta lähdemateriaalista. Tutkimuksen aineistoon kuului yhteensä pari kymmentä teosta. Seurasin useita virallisia eri viranomaisten ylläpitämiä sivustoja verkossa, sekä luin lukuisia asiantuntija-artikkeleita ja uutisointeja aiheeseen liittyen. Myös painettuja koostettuja oppaita löysin useita verkkopainoksina eri viranomaissivustoilta. Opinnäytetyöt Theseuksesta aiheeseen liittyen kävin myös läpi, mutta niitä oli ihmetykseksenі melko vähän koskien tietosuojaa. Aineiston pohjalta rakensin kokonaiskuvan siitä, mitä oleellisimman tietopohjan saavuttaminen aihealueeseen liittyen vaatii. Päätietolähteenäni toimi viralliset Tietosuojavaltuutetun toimiston verkkosivut. Tieto kyseisellä sivustolla pysyy hyvin yleisellä tasolla ja on helposti ymmärrettävää. Tietosuojavaltuutetun sivustojen pohjalta omaa tietopohjaa oli helppo lähteä syventämään muun aineiston kautta, sekä luomaan runkoa tutkimukselle.

Usein työskennellessäni aineiston parissa, mietin asian merkitystä ja sen käyttöä todellisessa työelämässä. Tein tältä pohjalta karsintaa tarvittavan tiedon löytämiseksi. Vertailin useampaa tietolähdettä keskenään, ja valitsin niistä mielestäni aina sopivimman tiedon. Tätä tietoa käytin sitten opinnäytetyössäni. Ajantasainen tietokirjallisuus jakautui kokemukseni mukaan kahteen ääripäähän. Oli useita yleisoppaita, jotka oli kirjoitettu hyvin kepeään sävyyn jokaiselle lukijalle sopiviksi. Toisaalta oli myös todella syvälle meneviä lakiviittauksin eteneviä asiantuntijaoppaita, joiden pelkkä lukeminen ja tiedon tulkitseminen oli jo hyvin haastavaa.

Aikataulu opinnäytetyö prosessissani on ollut hyvin katkonainen, ja välille ajoittui pitkiäkin taukoja kirjoittamisessa. Toisaalta tämä syvensi ja kypsytti työskentelyäni paljon, koska tietosuojaan liittyen tuona aikana sattui useampiakin isompia tapauksia. Seurasin uutisia, ja tapausten etenemistä median välityksellä, ja kävin asioita läpi eri näkökulmista.

Toteutin tämän opinnäytetyön laadullisena- eli kvalitatiivisena tutkimuksena. Kyseessä oli aineistolähtöinen tutkimus, jossa tietoa rajattiin ja analysoitiin siirtäen ne työelämän tarpeita ajatellen kirjalliseen muotoon. Näiden rajausten pohjalta syntyi melko kattava perusasioihin pureutuva yleiskatsaus aihealueeseen liittyen. Lähtökohtana oli omat tutkijan tarpeeni, eli selvitin asioita, jotka ovat itseäni jo vuosien ajan askarruttaneet. Tutkimuksen suunnitelmavaiheessa nostin esiin asiantuntija haastattelujen mahdollisuuden opinnäytetyön tekemisessä, mutta en kokenut niiden tuovan lisäarvoa tutkimukselle. Näin jälkikäteen tarpeellisia olisivat voineet olla haastattelut, joita olisi tehty tavallisille ”rivi” työntekijöille, jotka tietosuojaa työssään tarvitsevat.

Tutkimuksessa jätettiin vähemmälle pureutuminen hyvin syvälle lakiteksteihin, sekä niiden sisältöihin. Syynä se, että koin kokonaisuudesta tulevan liian raskaan tulkittavaksi arkisen työelämän kannalta. Tähän perusteluna oma kokemuspohja tämän opinnäytetyön eri aineistoista, sekä siitä, miten eri tavoin sama asia voidaan ilmaista. Pyrkimykseni oli pitää teksti hyvin yleistajuisena, ja helposti tulkittavana. Havainnoin myös opinnäytetyötä tehdessäni, että mitä pidemmälle tutkimukseni eteni, sen vaivattomammaksi vaativampien lakitekstien ja kirjallisuuden tulkinta kohdallani muuttui. Työn loppuvaiheessa asetusten ja lakien selaaminen ja niistä toiseen siirtyminen sujui jo hyvin luontevasti, ja tarvittava tieto löytyi helposti.

Ratkaisuissa valittujen tietojen ja tietolähteiden osalta korostin tutkijana käytännönläheisyyttä, sekä tiedon ajantasaisuutta. Myös tietopohjan luotettavuus oli merkittävä lähtökohta tutkimuksen teossa.

11 YHTEENVETO JA JOHTOPÄÄTÖKSET

Tietosuojaa ja sen kokonaisuutta tarkasteltaessa tein johtopäätöksiä siitä, miten tietosuojaosaamista olisi hyvä organisaatioissa lähteä kehittämään. Työpaikoilla olisi tarpeellista aina varmistaa henkilökunnan *tietosuoja osaaminen taso. Tietosuoja osaamista* olisi organisaatioissa tärkeä lähteä kehittämään vaiheittain, ja aloittaa osaamisen päivittäminen perustermien läpi käymisestä. Kun organisaatiossa jokainen on ymmärtänyt ja sisäistänyt ne oikein, on mahdollista kaikkien puhua samaa kieltä asian suhteen. Viime vuosina on paljon puhuttu *Jargonista*, ja sen yleisestä käyttämisestä puhekielenä. Jargon on tietyn ryhmän käyttämä sisäinen kielenkäyttötapa, ns. ammattislangi. Sitä käytettäessä yleisesti puhekielenä työyhteisöissä, saattaa ongelmia ilmetä siinä, jos asiantuntijan käyttämä kieli ei kohtaakaan vastaanottajaa. Käytössä olevassa kielessä häiritsee tuolloin sen vaikeaselkoisuus ja tulkinnan vaikeus, jolloin asia jää helposti etäiseksi ja vieraannuttaa vastaanotettaessa. Tietosuoja-asioita läpi käytäessä, sekä ohjeistuksia laatiessa täytyisi asiantuntijan aina käydä läpi se, kenelle hän asiasta viestii.

Runsas tietomurtojen lisääntyminen organisaatioissa viime vuosina, on nostanut entisestään tarvetta reagoida tilanteisiin riittävän nopeasti, sekä lisätä ennakoinnin merkitystä riittävän tietosuojan toteuttamisen suhteen. *Tietosuoja osaamista* on päivitettävä koko ajan, ja organisaatioiden on myös pystyttävä reagoimaan sujuvasti mahdollisen tietosuojaloukkauksen kohdalle sattuessa. Organisaatioissa kannattaa huomioida myös tietosuojaan liittyvien laiminlyöntien seuraukset, sekä niistä mahdollisesti aiheutuvat sanktiot. Mainehaitta sekä asiakkaalle, että yritykselle/yhteisölle saattaa olla hyvinkin suuri, verrattuna siihen miten se olisi saatu etukäteen torjuttua riittävällä suunnittelulla ja toteutuksella.

Yrityksissä usein aliarvioidaan henkilöiden määrä, jotka joutuvat työtehtävissään käsittelemään rekistereitä, henkilötietoja, sekä myös salaisisiksi/arkaluonteisiksi luokiteltuja asiakirjoja. Organisaatiossa ei mahdollisesti edes tunnisteta tällaisen toiminnan olevan kyseessä joissain työtehtävissä. Riittävän ohjeistuksen puuttuessa salaisiksi määriteltyjä asiakirjoja saatetaan tulostella ja siirtää mappiin kaikkien helposti saataville. Listoille voidaan kerätä henkilöitä tunnistetietoineen ilman, että kukaan edes ymmärtää kyseessä olevan rekisteri. Myös asiakas saattaa luovuttaa omia tietojaan kenelle vain henkilökuntaan kuuluvalle tietämättömyyttään. Jokaisen organisaatiossa työskentelevän on ensiarvoisen tärkeää oppia tunnistamaan ja tiedostamaan mahdolliset tietosuojaan liittyvät tilanteet asianmukaisen toiminnan varmistamiseksi.

11.1 Tietosuojan toteuttamisen valvonta

Tietosuojan toteuttamisen valvonta organisaatioissa ei mahdollisesti ole aina riittävällä tasolla, ja usein saatavilla olevan tiedon tulkinta jääkin vain pintaraapaisuksi. Tästä hyvänä esimerkkinä kesän 2024 Helsingin tapaus, jossa jo Helsingin sanomat (Palkoaho, M. 2024) otsikot huusivat *“Asiakirja paljastaa: Pakollisesta koulutuksesta lintsaaminen johti alkeellisiin virheisiin”*. Raportit paljastavat muun muassa sen, että kolmena peräkkäisenä vuonna toimialan esihenkilöt eivät ole vaatineet tietosuojan peruskoulutuksen suorittamista uusilta työntekijöiltä. Vuoden 2022 tietotilinpäätöksestä käy ilmi, että koulutuksen Helsingin kaupungin palveluksessa olleista oli suorittanut vain 310 työntekijää (Palkoaho, M. 2024). Helsingin kaupungin palveluksessa työntekijöitä tuolloin on ollut Helsingin kaupungin henkilöstöraportin mukaan 37 531 ihmistä (Helsinki 2022).

Kehittämisehdotuksena edellä mainittuun tilanteeseen suosittelisin, että jokaisessa yrityksessä, yksikössä ja organisaatiossa olisi hyvä olla oma *tietosuoja osaamisen* suunnitelma, vaikkei sitä erikseen laissa vaadittaisikaan. Sen avulla *tietosuoja tason* riittävä ylläpitäminen ja päivittäminen on tehokkaampaa, ja myös toteutuksen valvonta on hallitumpaa. *Tietosuoja osaamisen* tasoa on pidettävä koko ajan yllä aktiivisesti organisaatioissa, ja suunnitelmaa on uudistettava aina tarpeen vaatiessa. Eri tehtävissä on tärkeä käydä läpi juuri ne termit ja asiat, mitä tietosuoja juuri sen työtehtävän kannalta merkitsee. Ei ole tarkoituksenmukaista, että kaikki työntekijät katsovat saman opetus tallenteen, koska sillä tiedolla, mitä eri työtehtävissä tarvitaan, on paljonkin eroavaisuuksia. Perusosaamisen tietosuojasta ollessa kaikilla hallussaan työyhteisössä, pohditaan yhdessä toimintatapoja mahdollisia vastaantulevia tietosuojaan liittyviä tilanteita varten, ja suunnitellaan kehittämis- ja tehostamistoimenpiteitä yhdessä.

Tietosuoja prosessin on oltava aina jatkuvaa, ja uuden työntekijän perehdytyksessä se on otettava huomioon jo alkuvaiheessa. Työntekijöille on kerrottava mistä tietoa saa luotettavasti ja ymmärrettävästi, sekä minkälaisissa tilanteissa he mahdollisesti tietoa asiaan liittyen joutuvat etsimään. Heille on myös kerrottava kenenkä puoleen organisaatiossa asian tiimoilta voi kääntyä. Työntekijöille on myös kerrottava se, miten tärkeässä asemassa he ovat tietosuojan käytännön toteuttamisen, sekä sen kehittämisen kannalta työpaikallaan. On myös hyvä yhdessä pohtia tietosuoja osaamisen vaikutuksia sidosryhmien kanssa toimittaessa. Tietosuojaan perehtymisen ja tiedon päivittämisen kannalta Tietosuojavaltuutetun verkkosivusto on hyvä ja virallinen tietolähde, jota voi suositella kaikille. Se on aina helposti saatavilla luotettavana ja ajantasaisena tiedonlähteenä verkkosivuston muodossa

11.2 Opinnäytetyön tavoitteet, eettisyys ja luotettavuus

Tutkimuksen tavoitteet täyttyivät. Laajasta tutkimusmateriaalista ja saatavissa olevasta tiedosta pystyin omasta mielestäni laatimaan aihealueen peruskysymyksiin vastaavan kirjallisen yleiskatsauksen tiivistetyssä muodossa. Tämän tutkimuksen tärkein merkitys minulle on ollut se, että sain luotua käyttööni kattavan tietopohjan tietosuojaa koskien, sekä soveltamaan sitä jatkossa myös käytännön työssäni. *Tiedonhaku valmiuteni* ovat myös kehittyneet työn edetessä paljon.

Yllättävän työlääksi opinnäytetyön viimeistely vaiheessa muodostui lähdeviittausten läpikäyminen. Kirjoittamaani tekstiin merkitsemäni lähde, osoittautuikin lähes aina lainaukseksi jostakin. Lähdeviittauksia tarkistaessani huomasin, että koska kyseessä kaiken pohjalla on lainsäädäntö, muiden kirjoittama teksti aiheesta onkin usein toisen käden lähteen käyttöä. Pohdittavaa aiheutti se, jos Oikeusministeriö, Tietosuojavaltuutetun toimisto tai tietokirjailija on kirjoittanut aiheesta jotain, niin kummanko lähteen tuolloin itse merkitsen. Jouduin tekemään jälkikäteen paljon ratkaisuja uudelleen kirjailijan ja lain/asetuksen välillä, minkä lähteeksi valitsin, ja millä perusteella.

12 POHDINTA

Opinnäytetyön aiheina pyörittelin muutamaa eri vaihtoehtoa, ja mieleeni palasi tapaus, jolloin muistan ensimmäisen kerran pohtineeni tietosuojaan liittyviä asioita syvällisemmin. Osallistuin päivän kestävään koulutukseen noin kahdeksan vuotta sitten, ja koulutuksen piti koskea arkistointia. Itseni, ja monen muun yllätykseksi kouluttaja käsittelikin koko päivän tulossa olevaa EU:n tietosuoja-asetusta, ja sen mukanaan tuomia muutoksia henkilötietojen käsittelyä ja niiden säilyttämistä koskien. Osa osallistujista pettyi, kun ei opetettukaan mapittamaan asiakirjoja. Osa totesi luennoitsijan puheen olleen kuin *Hepreaa*, ja iso osa osallistujista oli sitä mieltä, että tuleva uudistus ei koske heidän alaansa. Koulutukseen osallistujat olivat pääsääntöisesti kaikki kunnan, valtion tai terveydenhuolto-alan työntekijöitä. Minusta kaikki oli melko hämmentävää, koska tajusin kouluttajan puheista, että aikaa rakentaa toimiva tiedonohjausjärjestelmä on organisaatioissa enää vain muutama vuosi. Siihen aikaan vielä lähes kaikki tallennettiin ainakin varalta myös paperiversioina, ja aika harva oli kuullutkaan sanaa *tiedonohjaus-suunnitelma*. Tämän opinnäytetyön tavoitteena minulla oli, että pystyisin selvittämään mitä riittävä *tietosuoja toteuttamisen* taso nykypäivän työelämässä vaatii. Kun nyt pohdin tuota hetkeä mistä kaikki alkoi pieninä tiedonmurusina, ja vertaan tietämykseni tasoa tällä hetkellä tutkimukseni toteuttamisen jälkeen, voin todeta, että ammatillisen kasvun ja oman työskentelyni tavoitteet ovat ehdottomasti täyttyneet tämän prosessin aikana.

Opinnäytetyön tekeminen osalta ajoittui kohdallani melko pitkälle ajalle, ja sen tekeminen kesti kokonaisuudessaan kaikkiaan lähes vuoden ajan. Tämä oli työn tekemisen kannalta hyvä asia, koska tapani ja kykyni tulkita aineistoa kypsyi ja kehittyi tuona aikana hyvin paljon. Huomasin nopeasti, miten tärkeää on tuntea termit aihealueeseen liittyen, koska vain ne osaamalla tietoa pystyy keräämään, sisäistämään, ja tulkitsemaan oikein. Työskentelyni oli melko hidasta, koska jokaista kohtaa varten kävin läpi useampia lähteitä asiayhteyteen liittyen. Valitsemani aihe opinnäytetyölleni oli melko haastava erilaisten vaikeasti tulkittavien lakitekstien ja viranomaislausuntojen myötä. Myös aihealueeseen liittyvien lakien ja asetusten ajantasaisuuksien, sekä valmisteluvaiheiden kanssa piti olla hyvin tarkkana. Esimerkiksi laki saattoi olla vasta valmisteluvaiheessa tai se olikin jo kumottu toisella. Sen vuoksi varsinkin painettua kirjallisuutta läpi käydessä, kaiken ajantasaisuus piti varmistaa voimassa olevasta lainsäädännöstä.

Opinnäytetyössäni onnistuin löytämään mielestäni oleellisimmat asiat, joiden avulla itselleni asettamani tavoitteet täyttyivät. Sain luotua kattavan tietopohjan, sekä tutkijana hyvät tiedonhakuvalmiudet aihealueeseen liittyen.

LÄHTEET

Aalto-Setälä, M. & Viitala, M. 2018. Tietosuoja pähkinänkuoressa. Tietosuojaopas yrityksille. Helsinki: Kauppakamari. Verkkojulkaisu. https://kauppakamari.fi/wp-content/uploads/2020/05/tietosuoja-pahkinankuoressa.-tietosuojaopas-yrityksille.verkkoversio.pdf. Viitattu 10.12.2024.

Alapuranen, L., Lehtonen, L., Koskinen, S. & Wiberg, M. 2020. Henkilötietojen käsittely työelämässä. Helsinki. Edita.

Andreasson, A., Oravala, J. & Toivonen, M. 2023. Tietosuoja ja yksityisyys. Opas jokaiselle. Helsinki: Tietosanoma.

Andreasson, A. & Ylipartanen, A. 2022. Osaava tietosuoja vastaava ja EU:n yleinen tietosuoja-asetus (GDPR). Helsinki. Tietosanoma.

Asetus 2016/679/EU. Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Euroopan unionin virallinen verkkosivusto. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016R0679. viitattu 9.1.2025.

Eduskunta 2024. Eduskunnan virallinen verkkosivusto. https://www.eduskunta.fi/FI/Sivut/default.aspx. Viitattu 9.1.2025.

European Union 2025. EUR-Lex.europa.eu 2016. Yleinen tietosuoja-asetus (GDPR). Verkkojulkaisu. Päivitetty 07.01.2022. https://eur-lex.europa.eu/FI/legal-content/summary/general-data-protection-regulation-gdpr.html. Viitattu 07.01.2025.

Euroopan komissio 2025. Euroopan unionin virallinen verkkosivusto. Verkkopalvelu. https://commission.europa.eu/index_fi. Viitattu 9.1.2025.

Hanninen, M., Laine., E., Rantala, K., Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely, EU-tietosuoja asetuksen vaatimukset. E-kirja. Helsingin Kamari Oy ja tekijät.

Helsinki 2024. Henkilöstöraportti 2022/tilastot. Verkkojulkaisu. https://julkaisut.hel.fi/fi/julkaisut/henkilostoraportti-2022/tilastot. Viitattu 7.11.2024.

Kinnunen, E. 2021. Suositus salassa pidettävän tiedon käsittelystä. Digi- ja väestötietovirasto. Verkkojulkaisu. https://vm.fi/documents/10623/0/Suositus+salassa+pidett%C3%A4v%C3%A4n+tiedon+k%C3%A4sittelyst%C3%A4_+Erja+Kinnunen.pdf/afa21b09-1f02-fa94-6ad2-e9a8d6bb4329/Suositus+salassa+pidett%C3%A4v%C3%A4n+tiedon+k%C3%A4sittelyst%C3%A4_+Erja+Kinnunen.pdf?t=1632225020452. Viitattu 10.12.2024.

Kivivasara, S. 2020. Asianhallinta ja palvelujen tiedonhallinta. Valtiovarainministeriö. Verkkojulkaisu. https://vm.fi/documents/10623/9949343/Asianhallinta+ja+palvelujen+tiedonhallinta/fdcdf4ac-3f35-737a-c6b2-1659c8a48e52/Asianhallinta+ja+palvelujen+tiedonhallinta.pdf. Viitattu 9.1.2025.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2022. Tietosuoja. Helsinki. Alma Talent.

Krakau, T. & Haapalehto, S. 2017. Tietopyynnöt ja henkilötietojen luovuttaminen. Helsinki: Alma Talent.

Kärkkäinen, H. 2021. Vastaamon palvelimen portti 3306 oli auki nettiin 1,5 vuotta ja kiristys alkoi jo 2018 – julkisuuskatastrofia viivytettiin viimeiseen asti. Ilta-Sanomat. Verkkojulkaisu. https://www.is.fi/digitoday/tietoturva/art-2000007794906.html. Viitattu 18.1.2025.

Laki julkisen hallinnon tiedonhallinnasta. https://www.finlex.fi/fi/laki/alkup/2019/20190906#Pidm46263582929488. Viitattu 10.12.2024.

Laki viranomaisten toiminnan julkisuudesta. https://www.finlex.fi/fi/laki/ajantasa/1999/19990621. Viitattu 31.10.2024.

Laki yksityisyyden suojasta työelämässä. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759.Viitattu 19.1.2025.

Lastensuojelun keskusliitto 2019. Lapsi verkossa – Näkökulmia lasten oikeuksiin ja tietosuojaan digitaalisessa ympäristössä. Verkkojulkaisu. https://www.lskl.fi/wp-content/uploads/Lapsi-verkossa.pdf. Viitattu 19.1.2025.

Lehtilä, O., Nyström P., Ronikonmäki N-M. & Sirviö T-H. 2021. Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla. Työryhmän loppuraportti. Liikenne- ja viestintäministeriön julkaisuja 2021. Verkkojulkaisu. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162783/LVM_2021_1.pdf?sequence=1&isAllowed=y. Viitattu 18.1.2025.

Minilex 2025. Lakitietopalvelu. Minilex.fi verkkopalvelu. https://www.minilex.fi/a/rekisterinpit%C3%A4ji%C3%A4-koskevat-periaatteet. Viitattu 23.2.2025.

Oikeusministeriö 2024. Oikeusministeriön verkkopalvelu. https://oikeusministerio.fi/etusivu. Viitattu 9.1.2025.

Palkoaho, M. Helsingin tietomurto, Asiakirja paljastaa: Pakollisesta koulutuksesta lintsaaminen johti ”alkeellisiin virheisiin”. Helsingin Sanomat verkkojulkaisu. https://www.hs.fi/helsinki/art-2000010450742.html. Viitattu 7.11.2024.

Peda.net 2025. Koulutuksen tutkimuslaitos. Peda.net verkkopalvelu. https://peda.net/. Viitattu 23.2.2025.

Sulin, I. 2017. Yleinen tietosuoja-asetus. Kuntaliiton verkkojulkaisu. https://www.kuntaliitto.fi/yleiskirjeet/2017/yleinen-tietosuoja-asetus. Viitattu 1.12.2024.

Tietosuojalaki 1050/2018. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050. Viitattu 9.1.2025.

Tietosuojavaltuutetun toimisto 2024. Tietosuoja.fi verkkopalvelun tietosuojasta. https://tietosuoja.fi/tietosuojavaltuutetun-toimisto. Viitattu 1.11.2024.

Valtionneuvoston kanslia 2020. Valtioneuvoston ja ministeriöiden verkkopalvelu. https://valtioneuvosto.fi/etusivu. Viitattu 10.12.2024.

Valtioneuvoston kanslia 2017. Lainsäädäntösanasto. Verkkojulkaisu. https://valtioneuvosto.fi/documents/10616/3457861/Lains%C3%A4%C3%A4d%C3%A4nt%C3%B6sanasto+(fi-sv-en).pdf/4116fc9d-94b5-47de-ba23-39a5c6f8f94a/Lains%C3%A4%C3%A4d%C3%A4nt%C3%B6sanasto+(fi-sv-en).pdf?version=1.2&t=1493024149000. Päivitetty 21.4.2017. Viitattu 9.1.2025.

Valtiovarainministeriö 2024a. Valtiovarainministeriö.fi verkkopalvelu. https://vm.fi/tiedonhallintalaki. Viitattu 10.12.2024.

Valtiovarainministeriö 2024b. Valtiovarainministeriön julkaisut. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164557/VM_2023_4.pdf?sequence=1&isAllowed=y. Viitattu 1012.2024.

Your Europe 2025. Euroopan unionin virallinen verkkosivusto. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm. Viitattu 7.1.2025.