Henri Uusoksa

Työntekijän tietosuojan toteutuminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

13.10.2021

Tiivistelmä

Tekijä:	Henri Uusoksa
Otsikko:	Työntekijän tietosuojan toteutuminen
Sivumäärä:	33 sivua
Aika:	13.10.2021
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikan tutkinto-ohjelma
Ammatillinen pääaine:	
Ohjaajat:	Osaamisaluepäällikkö Janne Salonen Toimitusjohtaja Jani Palmu

---

Insinöörityön tavoitteena oli tarkastaa työntekijöiden henkilötietojen käsittelyn ja tietoturvan dokumentaatio sekä verrata sitä henkilötiedonkäsittelystä annettuun viranomaisohjeistukseen sekä kerätä mahdolliset kehitystarpeet yrityksen kehitysjonoon.

Insinöörityö toteutettiin haastattelemalla yrityksessä työntekijöiden henkilötietoja käsitteleviä ihmisiä sekä toimitusjohtajaa. Haastatteluiden lisäksi käytiin läpi yrityksen dokumentaatiota henkilötietojen käsittelystä, tietoturvasta sekä niihin liittyvistä politiikoista, ohjeistuksista ja koulutusmateriaaleista.

Insinöörityön tuloksena huomattiin yrityksen työntekijöiden henkilötietojen tietosuojan olevan hyvällä tasolla lain ja viranomaisohjeistuksen mukaan. Yrityksessä käytössä on ollut epäformaali riskienhallintamalli, jonka mukaan tarvittavat tietosuojatoimenpiteet on valittu. Vanha malli päätettiin insinöörityön tutkimuksen perusteella korvata formalisoidulla riskienhallintamallilla. Henkilöstölle annettavassa tietosuojailmoituksessa huomattiin myös puutteita, joiden korjaamiseksi aloitettiin toimenpiteet.

Avainsanat: tietosuoja, tietoturva, yleinen tietosuoja-asetus, työntekijä

Abstract

Author:	Henri Uusoksa
Title:	Realization of the Employee Data Protection
Number of Pages:	33 pages
Date:	13 October 2021
Degree:	Bachelor of Engineering
Degree Programme:	Information Technology
Professional Major:	
Supervisors:	Janne Salonen, Head of School (ICT) Jani Palmu, CEO of Justin Group

---

The purpose of the thesis work was to inspect the documentation detailing processing of employees' personally identifiable information and information security related to the processing. Additionally, the purpose was to compare the processing and information security to the current law and regulatory guidance, and to collect any improvement need to the company's work backlog.

The thesis work was conducted by interviewing the personnel who process employee personally identifiable information and the Chief Executive Officer. In addition to the interviews, the thesis was conducted by reviewing documentation related to the processing and associated information security setup. Furthermore, the policies, works instructions, and training material related to privacy and information security was reviewed.

The conclusion of the thesis work was that the protection of the privacy of the employees in on a good level when compared to the law and available regulatory guidance. As part of the findings of the thesis work, the company decided to replace the informal risk management model, to which the protective measures were selected, with a formal risk management framework. Some shortcomings in the privacy notice provided to the employees were also found. Fixing of the shortcomings were started at the company.

Keywords: privacy, information security, GDPR, employee

Sisällys

Lyhenteet

CA: Certificate Authority: Yritys, joka myöntää toisille yrityksille tai yksilöille digitaalisia sertifikaatteja, joita käytetään tiedon salaukseen tai entiteetin kuten yrityksen tunnistautumiseen.

DPIA: Data Protection Impact Assessment: Vaikutuksen arviointi erityisesti tietosuojan osalta.

GDPR: *General Data Protection Regulation*. Englanninkielinen nimi yleiselle tietosuoja-asetukselle.

HTTP: Hyper Text Transfer Protocol: Hypertekstin siirtoprotokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon. Protokolla perustuu siihen, että asiakasohjelma (selain, hakurobotti tms.) avaa TCP-yhteyden palvelimelle ja lähettää pyynnön. Palvelin vastaa lähettämällä sopivan vastauksen, tavallisimmin HTML-sivun tai binääridataa kuten kuvia, ohjelmia tai ääntä.

HTTPS: Hyper Text Transfer Protocol Secure: HTTP-protokollan ja TLS/SSL-protokollan yhdistelmä, jota käytetään tiedon suojattuun siirtoon internetissä. Protokollan ansiosta siirto on salattu sekä palvelimelle että palvelimelta.

ISO 27001: International Organization for Standardization 27001: OSI:n standardinumero 27001 tarjoaa hyväksytyn prosessiperusteisen lähestymistavan organisaation tietoturvajohtamis- ja hallintajärjestelmän perustamiseen, toteuttamiseen, käyttämiseen, valvomiseen, päivittämiseen, huoltamiseen ja parantamiseen.

NIST: National Institute of Standards and Technology. Amerikan Yhdysvaltojen kansallinen organisaatio, jonka tarkoituksena on kehittää standardeja liittovaltion käyttötarkoituksiin.

SaaS: Software-as-a-Service: Ohjelmiston jakelumalli, jossa palvelun tarjoaja ylläpitää sovellusohjelmistoa palvelimillaan ja tarjoaa palvelua asiakkaille internetin välityksellä.

SOC 1: System and Organization Control 1: Auditointiraportti, jossa arvioidaan palveluntarjoajan taloudelliseen raportointiin ja sen kontrolleihin.

SOC 2: System and Organization Control 2: Auditointiraportti, jossa arvioidaan palveluntarjoajan muita kuin taloudellisia kontrolleja.

SSL: Secure Socket Layer: Tiedonsalausprotokolla.

TLS: Transport Layer Security: SSL:ää kehittyneempi tiedonsalausprotokolla.

WPA2: Wi-Fi Protected Access 2: Tiedonsalausprotokolla, jota käytetään yleisesti langattomissa lähiverkoissa.

WPA3: Wi-Fi Protected Access 3: Tiedonsalausprotokolla, jota voidaan käyttää langattomissa lähiverkoissa, ei yhtä yleinen vielä kuin WPA2.

1 Johdanto

Opinnäytetyö tehtiin Justin Group Oy:lle, joka on suomalainen henkilöstön omistama riippumaton liikkeenjohdon konsultointiin keskittynyt asiantuntijayritys [1]. Yrityksen filosofiaan kuuluu olennaisesti paikkariippumaton työskentely sekä työntekijöistä huolehtiminen ja työntekijöiden arvostaminen.

Edellä mainituista syistä yritys halusi varmistaa työntekijöiden henkilötietojen käsittelyn sekä käsittelyn dokumentaation olevan kaikilta osin vähintään viranomaisohjeistusten mukaisella tasolla.

Insinöörityön tavoitteena oli tarkastaa työntekijöiden henkilötietojen käsittelyn ja tietoturvan dokumentaatio sekä verrata sitä henkilötiedonkäsittelystä annettuun viranomaisohjeistukseen sekä kerätä mahdolliset kehitystarpeet yrityksen kehitysjonoon.

Teoriaosassa esitellään henkilötietojen käsittelyyn liittyvää viranomaisohjeistusta ja lakia sekä siihen liittyvän tarpeenmukaisen tietoturvan järjestämistä siltä osin kuin se on oleellista insinöörityön tavoitteiden kannalta.

Insinöörityö toteutettiin haastattelemalla yrityksessä työntekijöiden henkilötietoja käsitteleviä ihmisiä sekä toimitusjohtajaa. Haastatteluiden lisäksi käytiin läpi yrityksen dokumentaatiota henkilötietojen käsittelystä, tietoturvasta sekä niihin liittyvistä politiikoista, ohjeistuksista ja koulutusmateriaaleista.

2 Henkilötieto

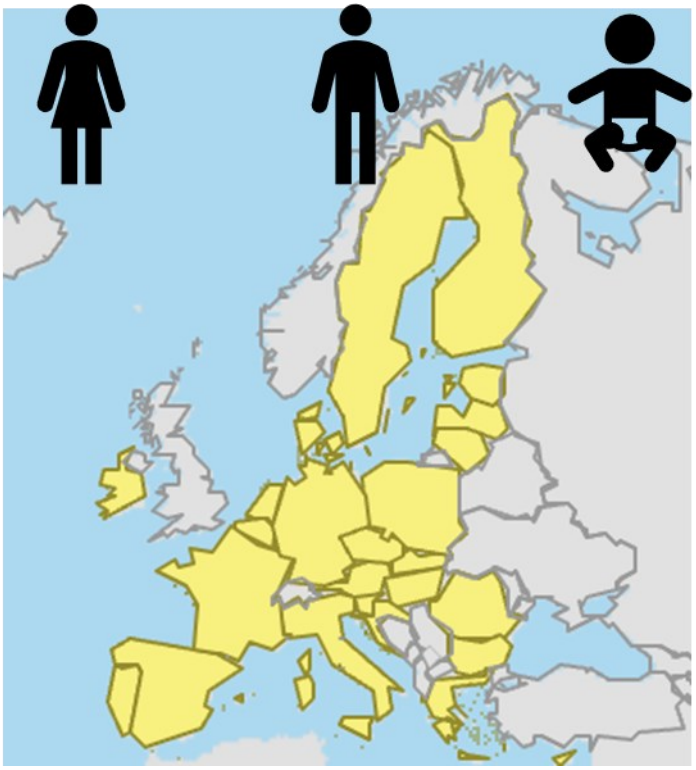
2.1 Yleinen tietosuoja-asetus

Euroopan unionin Your Europe-verkkosivusto kuvaa yleisen tietosuoja-asetuksen tarkoituksen seuraavalla tavalla.

> Yleisessä tietosuoja-asetuksessa asetetaan yrityksille ja organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat

> tarkat vaatimukset. Vaatimuksia sovelletaan sekä eurooppalaisiin organisaatioihin, jotka käsittelevät ihmisten henkilötietoja EU:ssa, että EU:n ulkopuolisiin organisaatioihin, joiden suorittama tietojen käsittely kohdistuu EU:n alueella asuviin ihmisiin. [2.]

Yleistä tietosuoja-asetusta, joka tunnetaan yleisemmin englanninkielisestä lyhenteestään GDPR, alettiin soveltamaan kaikissa EU maissa keväällä 2018 [3]. Näin ollen tällä hetkellä jokaisen suomalaisen yrityksen tulisi noudattaa kyseistä asetusta.



Kuva 1 Yleinen tietosuoja-asetus suojaa EU:n alueella asuvien ihmisten henkilötietoja riippumatta siitä, missä maassa tietoja käsitellään tai kerätään. EU-maat on kuvattu keltaisella värillä.

2.2 Henkilötieto

2.2.1 Määritelmä

Henkilötieto määritellään Tietosuojavaltuutetun toimiston internetsivujen mukaan seuraavasti.

> Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön [4].

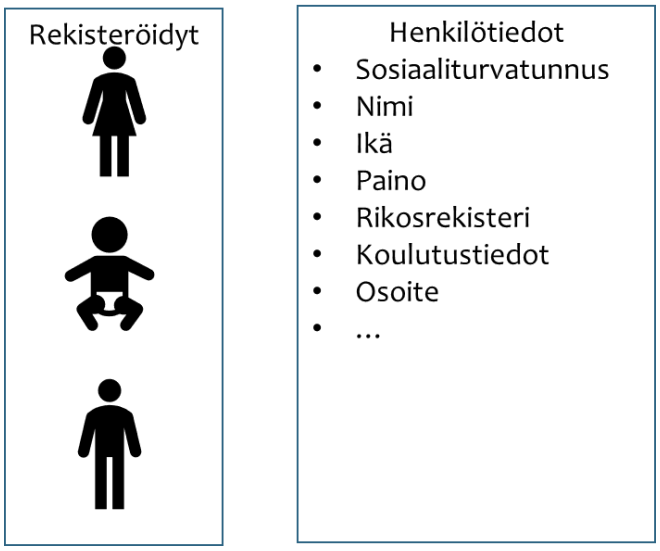
Euroopan unionin Your Europe sivulla annetaan henkilölle, kenen henkilötietoja käsitellään, lisänimike rekisteröity.

> Henkilötiedoilla tarkoitetaan kaikkia tietoja, jotka koskevat tunnistettua tai tunnistettavissa olevaa henkilöä, jota kutsutaan myös rekisteröidyksi [2].

Tietosuojavaltuutetun toimisto avaa laveita mutta lainmukaisia määrittelyjä, hieman esimerkin kautta.

> Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella. [4.]

Näin ollen esimerkiksi harvinaisen sukunimen ja kaupunginosan yhdistelmä voi jo mahdollistaa henkilön yksiselitteisen tunnistamisen. Lain mukaan se on henkilötietoa, jota kerätään rekisteröidystä.



Kuva 2 Esimerkki rekisteröidyistä ja henkilötiedoista, joita kerätään rekisteröitytyyn liittyen.

2.2.2 Rekisteröidyn oikeudet

Yleisessä tietosuoja-asetuksessa on lähdetty siitä ajatuksesta liikkeelle, että rekisteröity omistaa henkilötietonsa. Yleisen tietosuoja-asetuksen koko kolmas luku onkin omistettu rekisteröityjen oikeuksille. [5.]

Kuva 3 Rekisteröidyillä on EU:n lakien ja asetusten suojaamia oikeuksia ja vapauksia.

Rekisteröidyllä on oikeus

- tietää mitä henkilötietoja rekisterinpitäjä tallentaa ja miten niitä käsitellään
- nähdä tiedot ja pyytää rekisterinpitäjää korjaamaan väärä tieto
- oikeus tulla unohdetuksi, eli oikeus vaatia tietojen poistoa
- vastustaa henkilötietojen käsittelyä, erityisesti automaattista käsittelyä
- rajoittaa tietojen käsittelyä

- siirtää tiedot järjestelmästä toiseen ja rekisterinpitäjän tulee toimittaa tiedot siirrettävässä muodossa.

Yleisen tietosuoja-asetuksen [5] artikla 23 kuitenkin listaa erityistapauksia, kuten yleinen turvallisuus ja kansallinen turvallisuus, joissa rekisteröidyn oikeuksia voidaan rajoittaa.

Yleisen tietosuoja-asetuksen [5] artiklassa 34 kuvataan lisäksi rekisteröidyn oikeus saada tietää, jos rekisteröidyn henkilötietoihin on kohdistunut tietoturvaloukkaus.

2.2.3 Kategoriat

Henkilötiedot jaetaan karkeasti kahteen eri ryhmään: henkilötietoryhmiin, joina voinaan pitää esimerkiksi nimi ja osoitetietoja sekä erityisiin henkilötietoryhmiin. Yleinen tietosuoja-asetus kuvaa yhdeksännessä artiklassa erityiset henkilötietoryhmät alla olevalla tavalla.

> Sellaisten henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely on kiellettyä [5].

Erityisien henkilötietoryhmien tietojen käsittely on kuitenkin mahdollista samassa artiklassa määritellyissä erityistilanteissa esimerkiksi rekisteröidyn nimenomaisella suostumuksella tai jos rekisteröity on ne itse nimenomaisesti saattanut julkisiksi [5].

2.3 Henkilötietojen käsittely

2.3.1 Käsittelyn periaatteet

Yleinen tietosuoja-asetus ottaa vahvasti kantaa henkilötietojen keräämiseen, käsittelyyn, suojaamiseen sekä niihin liittyviin vastuisiin ja velvollisuuksiin.

Yleisen tietosuoja-asetuksen [5] viidennessä artiklassa kuvataan henkilötietojen käsittelyn periaatteet.

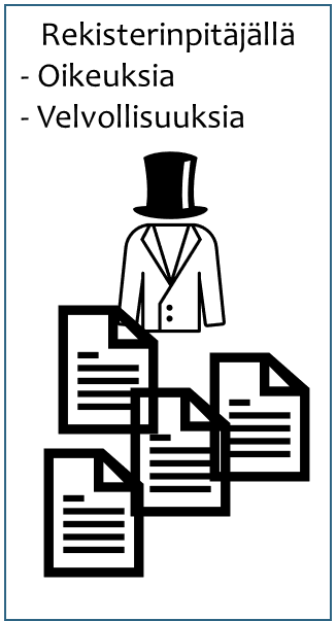
- lainmukaisuus, kohtuullisuus, ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus
- osoitusvelvollisuus.

Artikla siis määrää, että henkilötietoja tulee käsitellä lainmukaisesti, kohtuullisesti ja läpinäkyvästi. Henkilötietoja tulee kerätä vain tiettyä käyttötarkoitusta varten, ja rekisterinpitäjän pitää minimoida kerätyn tiedon määrä. Henkilötietojen tulee olla täsmällisiä ja tarvittaessa päivitettyjä, eikä rekisterinpitäjä saa säilyttää niitä pidempään kuin käyttötarkoitus vaatii. Lisäksi henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus. Rekisterinpitäjällä on myös osoitusvelvollisuus siitä, että periaatteita noudatetaan. [5.]

Rekisterinpitäjän pitää keräämisen yhteydessä siis kertoa rekisteröidylle, mihin tarkoitukseen tietoja kerätään, miten niitä käsitellään sekä kuinka kauan tietoja säilytetään. Rekisterinpitäjä on vastuussa siitä, että käsittely on lainmukaista ja tiedot ovat asianmukaisesti suojattuja sekä pystyä tarvittaessa osoittamaan valvovalle viranomaiselle toimivansa periaatteiden mukaisesti.

Yleisen tietosuoja-asetuksen [5] artikloissa 33 ja 34 kuvataan lisäksi rekisterinpitäjän velvollisuudet valvovia virnaomaisia ja rekisteröityjä kohtaan tietoturvaloukkauksien tapahtuessa.

Oman mausteensa käsittelyyn tuo myös Yleisen tietosuoja-asetuksen rajoitukset tiedon kansainväliseen siirtoon. Asetuksen mukaan henkilötietojen siirtämiseksi EU-maiden ulkopuolelle pitää siirronsaajan valtion tietosuojan olla EU:n mielestä riittävällä tasolla, eli valtiolla tulee olla niin kutsuttu adequacy decision eli tietosuojan riittävyyttä koskeva päätös. Vaihtoehtoisesti siirronsaajan tulee toteuttaa asianmukaiset suojaustoimenpiteet kuten erityisten lausekkeiden sisällyttäminen sopimukseen. Viimeisenä vaihtoehtona ovat vielä erityiset perusteet kuten rekisteröidyn suostumus. [2;5.]



Kuva 4 Rekisterinpitäjällä on oikeuksia, mutta erityisesti velvollisuuksia henkilötietojen käsittelyyn liittyen.

2.3.2 Käsittelyn lainmukaisuus

Yleisen tietosuoja-asetuksen [5] kuudennessa artiklassa kuvataan käsittelyn lainmukaisuuden määrittely.

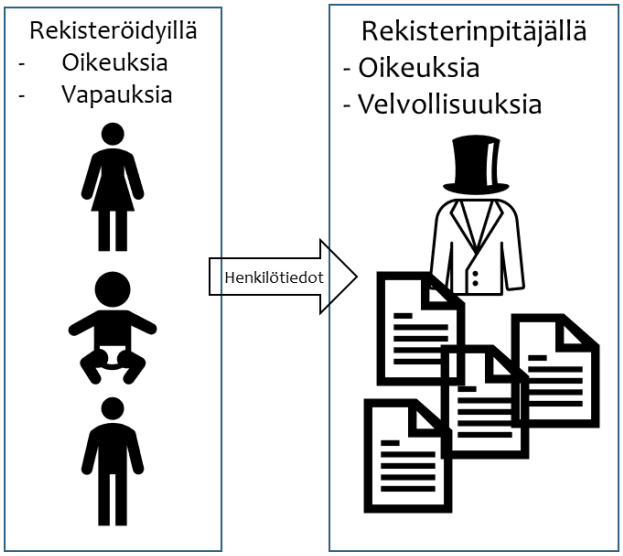
Artiklan mukaan henkilötietoja saa käsitellä vain, jos

- rekisteröity on antanut suostumuksensa
- käsittely on tarpeen sopimuksen täytäntöönpanemiseksi, tai sopimusta edeltävien toimenpiteiden toteuttamiseksi, ja rekisteröity on sopimuksessa osapuolena
- käsittely on tarpeellista rekisterinpitäjän lakisääteisen velvoitteen, kuten esimerkiksi kirjanpitolain noudattamisen, vuoksi tarpeen
- käsittely on rekisteröidyn tai toisen luonnollisen henkilö elintärkeiden etujen suojaamiseksi tarpeellista
- käsittely on yleistä etua koskevan tehtävän suorittamiseksi, tai rekisterinpitäjän julkisen vallan käyttämiseksi, tarpeellista
- käsittely on tarpeellista rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi tarpeellista.

Viimeisen kohdan osalta on erikseen mainittu rekisteröidyn etujen ja perusoikeuksien ja -vapauksien syrjäyttävän rekisterinpitäjän edut.

Suostumukseen liittyen Yleisen tietosuoja-asetuksen [5] seitsemännessä, kahdeksannessa sekä yhdeksännessä artiklassa on erikseen lueteltu suostumukseen liittyviä erityisehtoja kuten alle 16-vuotiaan lapsen osalta vanhempien suostumus ja erityisien henkilötietoryhmien osalta nimenomainen suostumus. Lisäksi suostumuksen tulee perustua vapaaehtoisuuteen ja rekisteröity voi

milloin vain peruuttaa suostumuksensa. Rekisterinpitäjällä on lisäksi osoitusvelvollisuus suostumuksen antamisesta.



Kuva 5 Käsittelyn lainmukaisuus toteutuu vain, jos rekisterinpitäjä huolehtii velvollisuuksistaan rekisteröityjen oikeuksia ja vapauksia kohtaan

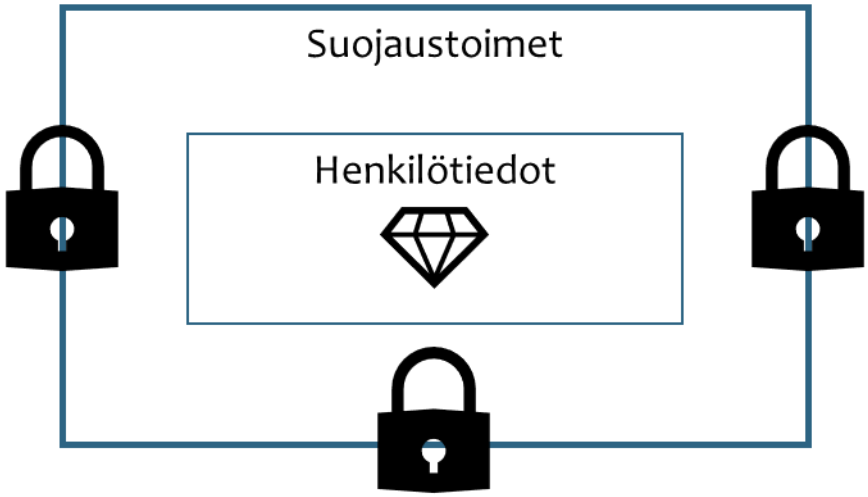
3 Tiedon suojaus

3.1 Henkilötietojen turvallisuus

Yleinen tietosuoja-asetus asettaa rekisterinpitäjälle velvollisuuden huolehtia käsittelemänsä tiedon turvallisuudesta.

> Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet [5].

Artikla ei siis suoraan kerro, mitä keinoja tulee käyttää, vaan siirtää vastuun rekisterinpitäjälle, jonka tulee itse arvioida käsittelemiensä henkilötietojen perusteella, miten niitä tulee suojata. Rekisterinpitäjän tulee suorittaa arviointi, joka perustuu rekisteröidyn oikeuksille ja vapauksille koituviin riskeihin. [5.]



Kuva 6 Rekisterinpitäjällä on velvollisuus huolehtia henkilötietojen käsittelyn turvallisuudesta sekä velvollisuus pystyä osoittamaan, että suojaustoimenpiteet ovat olemassa.

3.2 Riski ja riskienhallinta

3.2.1 Riski

National Institute of Standards and Technology määrittelee riskin vapaasti kääntäen muun muassa seuraavasti.

Riski on se vaikutus organisaation toiminnalle, joka syntyy tietojärjestelmän käytöstä johtuvan uhan vaikutuksen määrästä sekä todennäköisyydestä, jolla uhka käy toteen. Riski voi kohdistua yrityksen toimintoihin, imagoon, tai muuhun yrityksen arvoon tai arvon tuottamiseen tarvittavaan asiaan. [7.]

Yrityksen toimintaan kohdistuu siis riskejä, ja tämän insinöörityön kannalta erityisesti tietoturvaan ja tietosuojaan liittyviä riskejä.

Kyberturvallisuuskeskus muistuttaa, että viime kädessä yrityksen riskienhallinta ja tietoturva ovat yrityksen hallituksen vastuulla, ja tietoturva tulee nostaa osaksi yrityksien riskienhallintaa [8].

Yleinen tietosuoja-asetuskin velvoittaa rekisterinpitäjää arvioimaan riskejä. Asetuksessa riskejä velvoitetaan arvioimaan rekisteröidyn vapauksiin ja oikeuksiin kohdistuvien riskien kannalta yritykseen suoraan kohdistuvan riskin sijaan [5.]

3.2.2 Riskienhallinta

Yritysten tulee siis tehdä riskienhallintaa, mutta mitä se on?

Riskienhallinta määritellään muun muassa Valtioneuvoston Ohje riskienhallintaan -toimesta olevan järjestelmällistä ja tavoitteellista toimintaa, jolla tuetaan lisäksi organisaation johtamista ja kehittymistä ja jonka perusteella saadaan selville ne tasapainotetut toimet, joilla uhkia ja mahdollisuuksia hallitaan. Riskienhallintaan sisältyvät toimintakulttuuri, prosessit ja rakenteet, jotka edesauttavat mahdollisuuksien toteutumista ja joiden avulla hallitaan haitallisia tapahtumia. [9.]

Kyberturvallisuuskeskuksen [10] mukaan kaikessa riskienhallinnassa on yleisesti neljä mekanismia.

- riskin poisto
- riskin todennäköisyyden pienentäminen
- riskin vaikutuksen pienentäminen
- riskin hyväksyminen.

Yleensä joudutaan valitsemaan riskin todennäköisyyden ja riskin vaikutuksen pienentäminen ja hyväksymään jäljelle jäävä jäännösriski, koska riskiä ei voida kokonaisuudessaan poistaa [10].

Tärkeää on kuitenkin se, että riskit tunnistetaan ja se, mitä niille tehdään, kirjataan osaksi riskirekisteriä [9].

Yritysten ei kuitenkaan tarvitse keksiä riskienhallintamallejaan täysin itse, vaan he voivat ottaa käyttöön vaikkapa National Institute of Standards and Technologyn Risk Management Frameworkin, joka kuvaa, mitä yrityksen tulisi ottaa huomioon riskienhallintamallissaan ja sen käyttöönotossa.

NIST kuvaa Risk Management Frameworkin tarjoavan prosessin, joka integroi turvallisuuden, yksityisyydensuojan ja kybertoimitusketjun aktiviteetit osaksi järjestelmän kehityksen elinkaarta [11].

3.2.3 Uhka

Uhka, englanniksi threat, kuvataan NIST:in toimesta vapaasti kääntäen muun muassa seuraavalla tavalla.

> Uhka on mikä tahansa olosuhde tai tapahtuma, jolla on potentiaalinen negatiivinen vaikutus organisaatioon, organisaation omaisuuteen, yksilöön, toisiin organisaatioihin tai valtioon, joka tapahtuu järjestelmän läpi oikeudettoman pääsyn, tuhoamisen, tiedonannon, tiedon muokkauksen, ja/tai palveluneston avulla [12].

Uhka on siis mikä tahansa olosuhde tai tapahtuma, jolla on potentiaalinen negatiivinen vaikutus organisaatioon. Uhan vaikutus ja todennäköisyys sen sijaan muodostavat yritykselle riskin, jota riskienhallinnalla yritetään vähentää tai poistaa. Uhka taas muodostuu muun muassa uhka-aktoreista ja uhka-vektoreista. [9;10;12.]

3.2.4 Uhka-aktorit

Uhka-aktori viittaa tietosuojan ja tietoturvan kontekstissa henkilöön, organisaatioon tai valtiolliseen entiteettiin, jonka aikeena on toimeenpanna pahantahtoinen teko. Heihin viitataan myös englanninkielisellä termillä cyber threat actor eli CTA. [13.]

Uhka-aktorit käyttävät hyväksi tietojärjestelmien tai laitteiden haavoittuvuuksia varastaakseen, salatakseen, sabotoidakseen, saadakseen mainetta,

tehdäkseen rahaa tai muista syistä. Yleisesti uhka-aktorit kategorisoidaankin heidän motiiviensa ja kyvykkyyksiensä mukaan: mitä he saavat ja mitä resurs-seja heillä on käytettävissään. [13.]

Taulukko 1: Uhka-aktorien kategoriat, motivaatio, ja kyvykkyyksiensä taso [13].

Uhka-aktori	**Motivaatio**	**Kyvykkyyksien taso**
Kansallisvaltio	Geopoliittinen	Korkea
Kyberrikollinen	Raha	Keskiverrosta korkeaan
Aktivisti hakkerit	Ideologinen	Keskiverrosta korke-aan
Terroristi organisaatio	Ideologinen väkivalta	Matalasta korkeaan
Jännityksen hakijat	Mielihyvä	Matalasta korkeaan
Sisäpiiriuhka	Tyytymättömyys	Yleisesti matala

3.2.5 Uhkavektorit

Uhkavektori on reitti tai keino, mitä kautta tai minkä avulla uhka-aktori saa pääsyn tietojärjestelmään hyväksikäyttäen olemassa olevaa haavoittuvuutta reitillä [14].

Uhkavektorit muuttuvat hyökkäysvektoreiksi, kun joku aktori päättää käyttää tietämäänsä vektoria hyökätäkseen.

Yleisimpiä hyökkäysvektoreita ovat

- urkintasähköpostit
- päivittämättömät ohjelmistot
- kiristyshaittaohjelmat

- sisäpiiriuhat
- heikot tunnukset
- kolmansien osapuolien toimittajat
- huonot salausmenetelmät
- väärin konfiguroitu järjestelmä [15].

Tämä lista ei tietenkään kata kaikkia mahdollisia vektoreita, vaan organisaatio käsittelee vektoreita osana riskienhallintaa uhkien kautta.

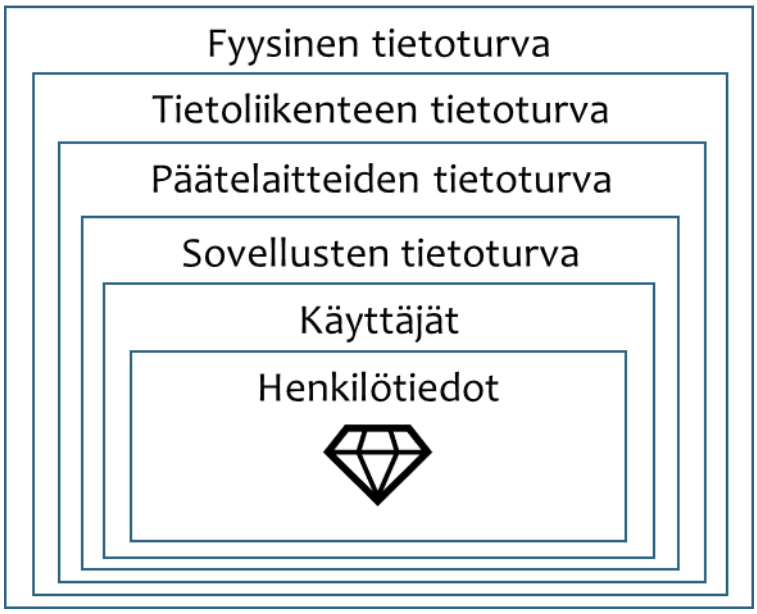
3.3 Tiedon suojaus

Tietosuojavaltuutetun toimisto muistuttaa organisaatioita siitä, että henkilötietojen käsittelyn on oltava luottamuksellista ja turvallista. Rekisterinpitäjän vastuulla on arvioida riskejä sekä sitä, onko organisaation tietosuoja- ja turvaohjeistus ja tekninen suojaus tarvittavalla tasolla. Rekisterinpitäjällä on myös osoitusvelvollisuus näistä suojaustoimista sekä niiden toimivuudesta. [16.]

Suojaustoimilla organisaatio tavoittelee Kyberturvakeskuksen riskienhallinnan mekanismeista joko riskin poistoa tai sen todennäköisyyden tai vaikutuksen pienentämistä ja hyväksyy mahdollisen jäännösriskin [10].

Suojaustoimet ovat luonteeltaan teknisiä tai organisatorisia. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstölle annettuja ohjeita tietosuojan toteuttamiseksi, käytönvalvontaa, tietojärjestelmien tietoturvaa, tietojen salausta ja muita suojatoimenpiteitä. [17.]

Tietoturva-alalla puhutaan yleisesti termistä defence-in-depth, jolla tarkoitetaan suojaustoimenpiteiden monikerroksista implementointia datan suojaamiseksi. Suojauskerroksia ovat käyttäjät, sovellusten tietoturva, päätelaitteiden tietoturva, tietoliikenteen tietoturva ja fyysinen tietoturva. [18.]



Kuva 7 Defence-in-depth eli suojaustoimenpiteet kerroksittain henkilötietojen ympärillä.

3.3.1 Käsittelijät

Käsittelijöistä, eli päätelaitteiden ja tietojärjestelmien käyttäjistä syntyvää riskiä vastaan käytetään yleisesti suojaustoimenpiteenä administratiivisia suojaustoimenpiteitä. Administratiivisia suojaustoimenpiteitä ovat muun muassa politiikat, menettelytapojen kuvaukset eli prosessikuvaukset, ja ohjeistukset, joilla käyttäjille kerrotaan, mitä he saavat tehdä missä ja miten. [18.]

Administratiivisena suojaustoimenpiteenä voidaan pitää myös turvallisuuskoulutuksia, joilla autetaan käyttäjiä tunnistamaan esimerkiksi sosiaalinen manipulointi. Sosiaalisen manipuloinnin tavoitteena on tietojärjestelmän haavoittuvuuksien sijaan käyttää haavoittuvuuksia ihmisten psykologiassa tai käyttäytymisessä, ja täten kiertää tekniset suojauskerrokset. [19.]

3.3.2 Päätelaitteet

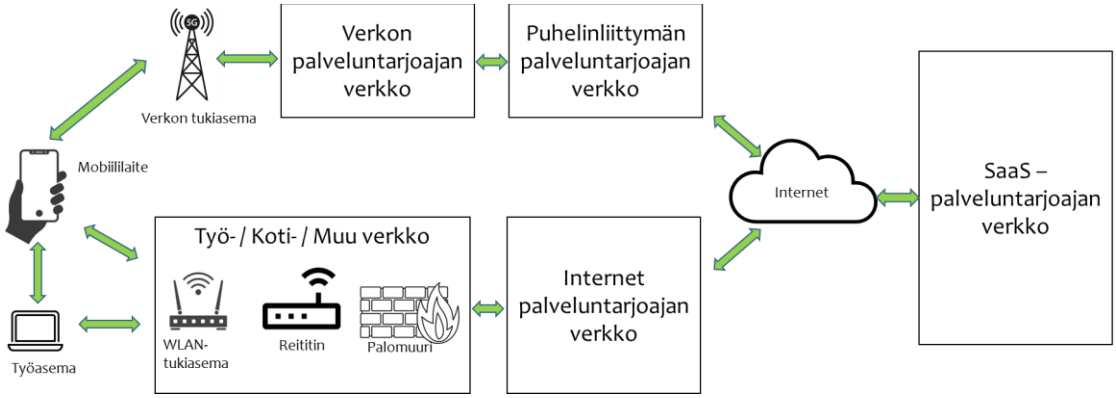
Päätelaitteista syntyvältä riskiltä suojaudutaan yleisesti huolehtimalla päätelaitteen sisältävän tarvittavia tietoturvaominaisuuksia kuten massamuistin

salauksen, virusturvan, haavoittuvuuksienskannauksen ja varmuuskopioimalla massamuisti [20; 21; 22].

Mahdollisuuksien mukaan päätelaitteet tulee myös liittää keskitetysti hallinnoitavaksi muun muassa pakotettuja päivityksiä varten ja tietoturvatapahtumien keräämisen sekä vaatimuksenmukaisuuden seuraamisen helpottamiseksi. Keskitetyllä hallinnalla pyritään saavuttamaan vakioitu laiteympäristö, jonka riskit tiedetään ja jossa tapahtuvat muutokset tunnistetaan. [20; 21; 22.]

3.3.3 Tietoliikenne

Tietoliikenteestä syntyvältä riskiltä suojaudutaan yleisesti salaamalla tietoliikenne. Nykyaikaisissa organisaatioissa tehdään paikkariippumatonta tai monipaikkaista työtä pilven reunalla pyörivien SaaS-palveluiden avulla. Paikkariippumaton ja monipaikkainen työntekotapa vaatii tietoliikenteen suojausta yrityksen tilojen lisäksi myös työntekijöiden kodeissa sekä vaikkapa vuokramökiltä tai lähikahvilasta.



Kuva 8 : Tietoliikenne SaaS-palveluntarjoajan ja päätelaitteiden välillä. Vihreät nuolet kuvaavat tietoliikenteen reittiä käyttäjän laitteilta SaaS-palveluntarjoajan verkkoon ja takaisin.

Päätelaitteen ja SaaS-palveluiden välillä on monia tietoliikennelaitteita, jotka eivät ole yrityksen hallinnassa, joten on tärkeää varmistaa päästä päähän -suojaus SaaS-palveluiden ja päätelaitteiden välillä.

Koska SaaS-palvelut ovat yleensä selaimella käytettäviä, huolehtimalla SaaS-palvelun tukevan HTTP-tietoliikenneprotokollan salattua versiota HTTPS-protokollaa, saadaan luotua suojatumpi tiedonsiirtoreitti SaaS-palvelun ja päätelaitteen välille. [23;24.]

HTTPS-protokolla käyttää Secure Socket Layer- tai Transport Layer Security -protokollaa salausta ja todennusta varten. SSL ja TSL perustuvat varmenteisiin, joita myöntäviä yrityksiä kutsutaan englanniksi Certificate Authority -nimellä. Salauksen lisäksi varmenteita käytetään myös todistamaan palvelua tarjoavan organisaation identiteetti, ja joskus myös palvelua kuluttavan organisaation tai muun entiteetin identiteetti. [25;26.]

Toinen tärkeä kohta, johon yrityksellä on mahdollisuus vaikuttaa, on päätelaitteen ja mobiililaitteen välinen tietoliikenne, sekä päätelaitteen ja mobiililaitteen sekä langattoman verkon tukiaseman välinen liikenne.

Organisaation tulisi ohjeistaa työntekijöitään olemaan liittymättä tuntemattomiin langattomiin verkkoihin ja käyttämään sen sijaan mobiilidataa. Lisäksi organisaation on hyvä ohjeistaa työntekijöitään huolehtimaan, että langaton liikenne esimerkiksi puhelimen ja kannettavan tietokoneen välillä on suojattu vähintään WPA2 Personal -tasoisella salauksella. Nykyaikaiset laitteet tukevat myös uudempaa WPA3-salausta. [27;28.]

3.3.4 Tietojärjestelmät

Tietojärjestelmien suojaukseen liittyy olennaisesti käyttäjät sekä päätelaitteiden- ja tietoliikenteen suojaus, mutta tässä luvussa keskitytään itse järjestelmässä tai järjestelmään tehtyä suojaustyötä, erityisesti SaaS-palveluihin liittyen.

Ostaessaan SaaS-palveluita organisaation on ensin arvioitava SaaS-palvelua tarjoavan yrityksen luotettavuutta tietoturvan ja tietosuojan osalta. Onko palveluntarjoajalla yleisiä vaatimuksenmukaisuus tietoturva sertifikaatteja kuten SOC, SOC 2, tai ISO 27001? Missä maassa / maissa palveluntarjoajan infrastruktuuri

ja henkilöstö sijaitsevat? Onko kyseisillä valtioilla Euroopan komissiona tietosuojan riittävyyttä koskeva päätös vai käyttääkö yritys Euroopan komission mallisopimuslausekkeita? Mikä palvelun luotettavuus on ja kuinka se skaalautuu? Minkälaiset palautumissuunnitelmat ja palvelulupaukset sillä on? Tuhotaanko asiakkaan tiedot luotettavasti, kun palvelun tilaus lopetetaan? Miten palvelun tiedot suojataan ja mikä on yrityksen taloudellinen tilanne? [5;29;30;31.]

Kun SaaS-palvelun tarkoituksenmukaisuus ja SaaS-palveluntarjoajan sopivuus on tarkistettu, yhtiön on lisäksi huolehdittava yleensä palvelua käyttävälle organisaatioille kuuluvista asioista kuten käyttäjiin liittyen käyttövaltuuksien hallinnan prosesseista, kertakirjautumistoiminnoista, keskitetystä identiteetinhallinnasta, ja monivaiheisesta autentikoinnista. Käyttövaltuuksien hallinnassa tulisi lisäksi huomioida pienimmän valtuuden periaate eli se, että käyttäjille annetaan vain tarvittavat oikeudet ja oikeudet poistetaan, kun tarve oikeuksille poistuu. [31.]

3.3.5 Fyysinen suojaus

Tietoteknisen ympäristön suojauksessa tulee ottaa huomioon myös fyysinen suojaus. Tiloja tulisi suojata muun muassa suojaamalla tiloihin kulkemisväylät kulkukortilla toimivilla sähkölukollisilla ovilla sekä asentamalla tiloihin hälyttimiä. Kulkukorttien käyttö tulisi tallentua myöhempää tarkastelua varten. Yleisiä tiloja ja kulkuväyliä tulisi valvoa tallentavilla valvontakameroilla. Lisäksi työntekijöitä tulisi kouluttaa sosiaalista manipulointia vastaan. [32;33.]

Monipaikkaisessa työssä organisaatiolla ei tietenkään ole mahdollista varmistaa kaikkien mahdollisten tilojen fyysistä suojausta, vaan organisaation on ohjeistettava työntekijöitä siitä, minkälaisissa tiloissa työvälineitä on sallittua varastoida sekä minkälaisissa tiloissa työtehtäviä saa suorittaa [34].

3.4 Osoitusvelvollisuus

Tietosuojavaltuutetun toimisto, joka toimii valvovana viranomaisena, kuvaa internetsivuillaan, miten rekisterinpitäjän tulisi osoittaa toteuttaneensa tarvittavat tekniset ja organisatoriset toimet henkilötietojen suojaamiseksi [35].

Osa osoitukseen tarvittavasta dokumentaatiosta, kuten seloste käsittelytoimista, koskee vain tietyn kokoisia organisaatioita, tai organisaatioita, jotka käsittelevät tietynlaista henkilötietoa. Käsittelytoimien selosteessa rajat ovat yli 250 henkilön organisaatio tai että joku seuraavista pitää paikkansa.

- Käsittelytoimet aiheuttavat todennäköisesti riskin rekisteröidyn oikeuksille ja vapauksille.

- Henkilötietojen käsittely ei ole satunnaista.

- Käsiteltävät henkilötiedot sisältävät erityisiä tietoryhmiä tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja. [36.]

Toinen osa osoitukseen vaadittavasta dokumentaatiosta vaaditaan kaikilta rekisterinpitäjiltä. Tästä esimerkkinä mainittakoon osoitusvelvollisuus siitä, että rekisteröityä on kerrottu käsittelystä ja että henkilötietojen käsittelystä kertova informaatio on helposti ymmärrettävää, kun otetaan huomioon rekisteröidyn kyky käsittää käsittelystä kertova dokumentaatio. [37.]

4 Työntekijöiden henkilötietojen käsittely Justin Group Oy:ssa

4.1 Yleiskuva

Työntekijätiedon käsittely elinkaari Justin Groupilla noudattaa mallia, joka lienee yleinen yrityksen toimialasta ja koosta riippumatta.

Kuva 9 : Kuvassa esitellään työntekijätiedon käsittelyn elinkaari Justin Group Oy:ssa.

Hakiessaan työtä tuleva työntekijä luovuttaa yritykselle henkilötiedoiksi luokiteltavia tietoja itsestään, jotka tallentuvat tai tallennetaan yrityksen tietojärjestelmiin osana rekrytointiprosessia. Rekrytointiprosessin aikana työnhakijalle saatetaan tehdä työtarjous, joka on luokiteltavissa henkilötiedoksi ja sisältää henkilötietoja. Työtarjous tallennetaan yrityksen tietojärjestelmiin. Rekrytointiprosessin aikana kerätyn tiedon laillinen peruste on työnhakijan antama suostumus lähettäessään tietoa vapaaehtoisesti. [38;39.]

Työsopimuksen allekirjoituksen jälkeen alkaa uuden työntekijän työntekijäksi tulemisen prosessi, jossa työntekijältä pyydetään lisätietoja kuten tilinumero palkanmaksua varten. Uusia ja aikaisemmin saatuja tietoja tallennetaan yrityksen erilaisiin tietojärjestelmiin yrityksen velvollisuuksien täyttämiseksi sekä työntekijän työtehtävien mahdollistamiseksi. [38;39.]

Työsuhteen aikana työntekijän rooli tai työtehtävien sisältö yrityksen sisällä voi muuttua, jolloin jo kerättyjä henkilötietoja käytetään myös uusiin tarvittaviin palveluihin. Yritys saattaa myös ottaa käyttöön uusia järjestelmiä tai poistaa järjestelmiä pois käytöstä. Uusien järjestelmien käyttöönottoon tai vanhojen järjestelmien poistamiseen, eli muutoksenhallintaprosessiin, kuuluu olennaisena osana vaikutuksenarviointi, eli Data Protection Impact Assessment, jolla arvioidaan

muutoksen vaikutusta työntekijöiden tietosuojan ja yrityksen tietoturvan tasoon. [38;39.]

Yrityksen toimialaan, johdon konsultointiin, kuuluu myös olennaisena osana työntekijöiden ansioluetteloiden lähettäminen asiakkaille ja potentiaalisille asiakkaille osana tarjousten lähettämistä. Työntekijöiden tietoja myös esitellään yrityksen julkisilla verkkosivuilla. [38;39.]

Työsuhteen aikana yrityksen järjestelmiin kerätään yrityksen, henkilöstön, asiakkaiden ja muiden sidosryhmien tietoturvan ja tietosuojan vuoksi osaksi henkilötiedoiksikin laskettavaa tietoa tietojärjestelmien käytöstä. Näitä tietoja ovat esimerkiksi IP-osoitteet, jotka liittyvät käyttäjätunnukseen, kirjautumistiedot, mitä dokumentteja käyttäjä on päivittänyt ja milloin sekä moni muu vastaava tieto.

Työsuhteen aikana tietojen keräämiseen käytetään useita eri laillisia perusteita riippuen kerätystä tiedosta [38;39].

Työsuhteen päättyessä käynnistyy työsuhteen päättämisen prosessi, jossa kuljetaan päinvastaiseen suuntaan kuin työntekijäksi tulemisen prosessissa. Työsuhteen päättyessä työntekijän tunnukset yrityksen järjestelmiin ensin suljetaan ja lopuksi poistetaan tietyn varoajan jälkeen. Yritys ilmoittaa asiakasyrityksille työntekijän poistuvan yrityksestä, jotta asiakasyritykset voivat aloittaa omat poistamisprosessinsa. [38;39.]

Työntekijäksi tulemisen ja työsuhteen aikana kerätyn tiedon laillisen syyn mukaan osaa henkilötiedoista pidetään tallessa vielä useita vuosia työsuhteen päättymisen jälkeen. Näiden henkilötietojen tallentamiseksi yleisin syy on yrityksen lakisääteiset velvoitteet. [38;39.]

4.2 Administratiiviset ja organisatoriset suojaustavat

4.2.1 Riskienhallintamalli

Yrityksessä on ollut käytössä epäformaali riskienhallintamalli, jonka perusteella yritys on valinnut käyttöönotettavat tiedonsuojausmenetelmät eri alueille. Riskienhallinta ei ole kuitenkaan asianmukaisesti dokumentoitu eikä riskienhallinnan prosessia tai muuta formaalia käsittelytapaa rooleineen ole määritelty. [38;39.]

4.2.2 Politiikat ja ohjeistukset

Justin Group suojelee työntekijöiden henkilötietoa teknisten suojausmenetelmien lisäksi myös administratiivisien ja organisatoristen suojauskeinojen kuten politiikkojen ja ohjeistusten avulla.

Yrityksessä on johdon hyväksymänä etätyöpolitiikka, tietoturvapolitiikka, henkilötietojen käsittelyn politiikka sekä dokumenttien hallinnan politiikka.

Etätyöpolitiikassa kuvataan henkilöstölle, minkälaisia työvälineitä etätyössä saa käyttää ja minkälaisessa ympäristössä työtehtäviä saa hoitaa. Lisäksi ohjeistetaan turvallisen tiedonsiirron järjestämisestä ja muistutetaan henkilöstölle, miksi politiikkojen noudattaminen on yrityksen ja rekisteröityjen kannalta tärkeää. [38;39.]

Tietoturvapolitiikassa kuvataan teknisten laitteiden toiminnallisia vaatimuksia ja niiden pakollisia tietoturvaa ja tietosuojaa parantavia ohjelmistoja. Tietojärjestelmien osalta kuvataan käyttäjähallinnan vaatimuksia ja teknisiä tietoturvavaatimuksia. Fyysisen tietoturvan osalta kuvataan vierailijakäytännöt sekä tietosuojamateriaalin tuhoamisen vaatimukset. [38;39.]

Henkilötietojen osalta kuvataan erityiset politiikat henkilötietojen käsittelyyn liittyen ja opastetaan henkilöstöä tunnistamaan tilanteet, joissa yritys on rekisterinpitäjä ja tilanteet, joissa yritys on käsittelijä. Henkilöstölle opastetaan myös,

kuinka kummassakin tilanteessa tulee toimia. Käytännön tasolla politiikat ohjaavat henkilöstön noudattamaan henkilötietojen käsittelyssä johdon hyväksymiä henkilötietojen käsittelyyn liittyviä prosesseja. [38;39.]

Dokumentinhallinnan politiikoissa henkilöstölle kerrotaan, missä mitäkin tietoa tulee yrityksessä tallentaa sekä mitä tietoa ei missään nimessä saa yrityksen järjestelmiin tallentaa [38;39].

Henkilöstöä koulutetaan politiikoissa tapahtuvista muutoksista kuukausittain ja ajantasainen tieto politiikoista ja koulutusmateriaalista on henkilöstölle yhtiön intranetissä aina tarjolla [38;39].

4.2.3 Prosessit

Prosessikuvauksia ja työohjeita voidaan pitää yhtenä administratiivisena tai organisatorisena suojausmenetelmänä.

Työntekijöiden henkilötietojen suojaamiseen liittyen yrityksessä on tunnistettu ja kuvattu tietyt prosessit.

Rekrytointiprosessi kuvaa, mitä henkilötietoja työnhakijasta kerätään ja mihin sitä saa tallentaa, kuka niitä tallentaa sekä miten tieto poistetaan. Prosessin kuvauksessa kerrotaan myös millä laillisella perusteella mitäkin tietoa kerätään. [38;39.]

Työntekijäksi tulemisen prosessi kuvaa, mitä lisätietoja työntekijästä kerätään ja mihin eri järjestelmiin mitäkin niistä tiedoista viedään ja kenen toimesta. Osana prosessikuvausta kuvataan millä laillisella perusteella mitäkin tietoja on kerätty. [38;39.]

Yrityksen toimialan takia työsuhteen aikana työntekijöiden henkilötietoja lähetetään asiakkailla tai potentiaalisille asiakkaille osana myyntiä tai tarjoukseen vastausta. Lisäksi työsuhteen aikana muuttuvien roolituksien vuoksi työntekijöiden tietoa voidaan lisätä uusiin järjestelmiin. [38;39.]

Työsuhteen aikana työntekijöiden henkilötiedoiksi laskettavaa käyttötietoa kerätään niissä tietojärjestelmissä, joihin työntekijälle on annettu käyttäjätunnukset, ja niistä laitteista, jotka työntekijälle on luovutettu. Tätä tietoa kerätään työntekijöiden, yrityksen ja yrityksen muiden sidosryhmien tietojen suojaamiseksi. [38;39.]

Työsuhteen päättymisen prosessissa kuvataan, mistä järjestelmistä poistetaan mitäkin tietoja ja missä vaiheessa prosessia. Prosessikuvauksessa kerrotaan myös, mitä tietoja ei voida poistaa työsuhteen päättyessä niihin kohdistuvien tarpeiden vuoksi. Yrityksellä on laillinen velvoite säilyttää tiettyjä tietoja jopa useita vuosia työsuhteen päättymisen jälkeen. Velvoitteet tulevat Suomen lainsäädännöstä tai viranomaisohjeistuksista. [38;39.]

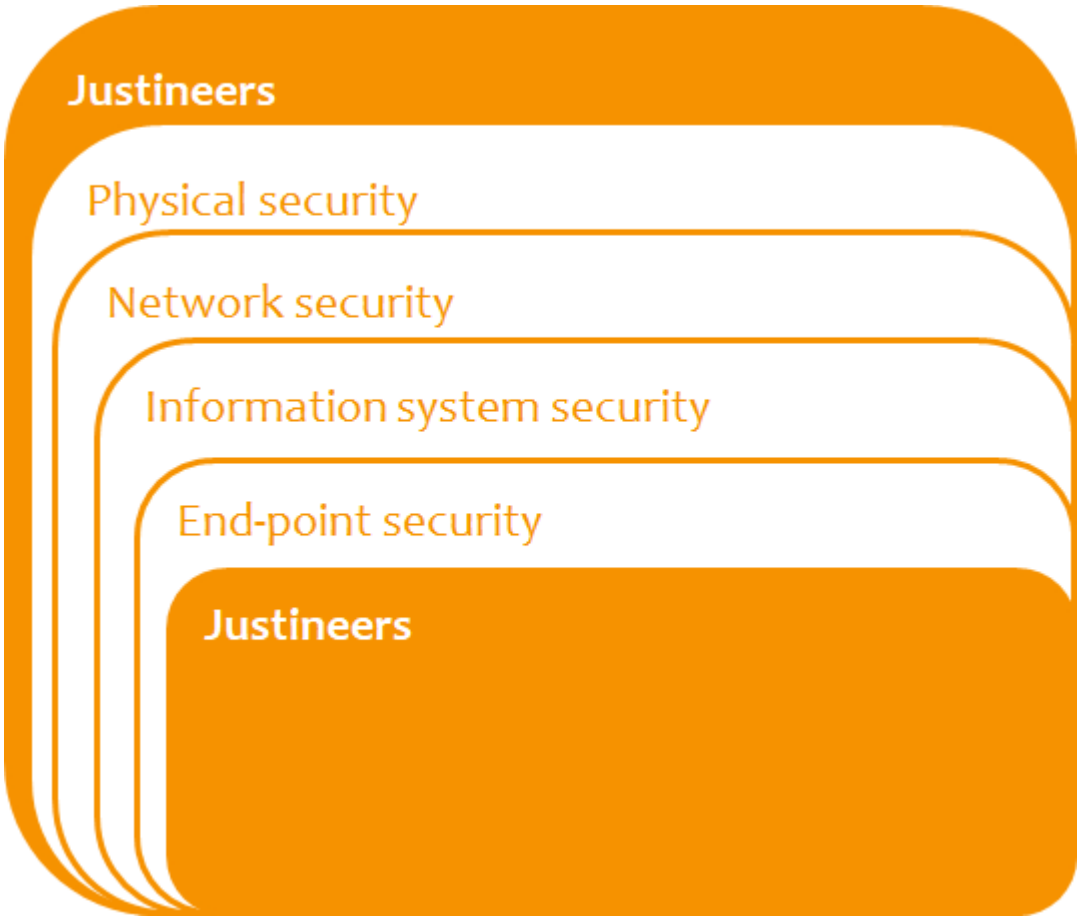
Muutoksenhallinnan prosessissa kuvataan yrityksen huolehtivan vaikutuksenarvioinnista, eli Data Protection Impact Assessmentista, osana muutoksenhallintaa [38;39].

Tietoturva- ja tietosuojapolitiikkojen päivitysprosessi kuvaa erilaiset tilanteet, joissa kyseisten politiikkojen päivitysprosessi käynnistyy sekä prosessin eri toimijat ja vaiheet uuden politiikan käyttöönottoon ja henkilöstölle kouluttamiseen asti [38;39].

Tietosuoja- ja tietoturvatapahtumien ja häiriöiden prosessi kuvaa, miten yritys huolehtii tietoturvaan ja tietosuojaan kohdistuvien tapahtumien ja häiriöiden hallinnasta [38;39].

4.3 Tietotekniset suojaustavat

Administratiivisten ja organisatoristen suojaustapojen lisäksi yrityksessä on käytössä useita erilaisia tietoteknisiä suojaustapoja.



Kuva 10 Justin Group Oy:n politiikka dokumentaatiosta lainattu kuva esittää tietoteknisen suojauksen kerrokset [39].

Henkilöstölle luovutetaan käyttöön vain yrityksen tietoturvapolitiikan mukaisia päätelaitteita, joissa on muun muassa levynsalaus, keskitetty hallinta, keskitetty päivitysten hallinta, virusskanneri sekä keskitetty virusten ja haavoittuvuuksien-hallinta. Yrityksellä on mahdollisuus keskitetysti estää laitetta pääsemästä käsiksi yrityksen tietoihin sekä poistaa tietoja kadotetuista laitteista. [38;39.]

Tietojärjestelmien osalta yrityksen IT-strategiassa keskitytään ostamaan tarvittavat ohjelmistot yleisesti tunnetuilta ja luotettavilta SaaS-palveluntarjoajilta, joilla on yritystä paremmat edellytykset huolehtia muun muassa tietojärjestelmien infrastruktuurin ylläpitoon ja sovelluskehitykseen liittyvistä tietoturvahaasteista. Yrityksen politiikoissa kuvataan järjestelmätoimittajiin kohdistuvia toiminnallisia vaatimuksia sekä tietoturva- ja tietosuojavaatimuksia, joita seurataan osana ostoprosessia sekä käytön aikana. [38;39.]

Tietojärjestelmien sisällä tallennetaan loki-tietoa siitä, kuka on tehnyt mitä, missä ja milloinkin, jotta mahdollisiin väärinkäytöksiin voidaan puuttua ja ne voidaan tarvittaessa todistaa [38;39].

Käytössä olevat tietojärjestelmät on kirjattu yrityksen rekisteriin. Tietojärjestelmien osalta on myös kuvattu, mikä yritys tietojärjestelmää tuottaa ja mikä yrityksen kotivaltio on. Rekisteriin on kirjattuna, onko kotivaltiolla ja muilla käsittelyvaltioilla EU:n tietosuojan riittävyyttä koskeva päätös vai onko käytössä Euroopan komission hyväksymät vakiolausekkeet ja missä kyseiset vakiolausekkeet on kuvattu. Rekisterissä on myös tallennettuna, missä toimittajan tietosuojailmoitus on kuvattu ja minkälainen tietoturva tietojärjestelmässä on toimittajan puolesta. [38;39.]

Yrityksen työntekijät tekevät monipaikkaista ja paikkariippumatonta työtä, jolloin kaikkia mahdollisia tietoliikenteeseen liittyviä laitteita ei voida hallinnoida yrityksen toimesta. Tietoliikenteen turvaamiseksi yrityksessä on keskitytty huolehtimaan käytettävien tietojärjestelmien tukevan tietoturvallista tiedonsiirtoa päästä päähän sekä ohjeistamaan henkilöstöä valitsemaan, millaisissa tilanteissa käytetään minkäkinlaisia tietoliikenneyhteyksiä. Esimerkiksi kahviloiden avoimien langattomien verkkojen käyttö on kielletty. [38;39.]

4.4 Fyysiset suojaustavat

Yrityksen toimitilojen suojana on henkilökohtaisilla kulkutunnisteilla toimivat sähkölukot sekä toimitiloihin kulkevien kulkuväylien varrella oleva nauhoittava kameravalvonta. Yrityksen politiikat kuvaavat lisäksi vierailijakäytännöt, joita tulee noudattaa. [38;39.]

Yrityksen työntekijät tekevät paikkariippumatonta ja monipaikkaista työtä, jolloin kaikkia mahdollisia tiloja, joissa työtä tehdään, ei voi suojata. Yrityksen toimitilojen ulkopuolella yrityksen työntekijät noudattavat etätyöpolitiikkaa, joka kuvaa, minkälaisissa tiloissa työtehtäviä saa suorittaa sekä miten työvälineitä tulee säilyttää. [38;39.]

5 Työntekijän tietosuojan toteutuminen

Yleinen tietosuoja-asetus tai Tietosuojavaltuutetun toimisto, joka toimii valvovana viranomaisena, ei anna yrityksille suoria ohjeistuksia siitä, minkälaisilla suojaustoimenpiteillä yritysten tulisi työntekijöiden henkilötietoja suojata, vaan ohjeistaa yrityksiä itse suorittamaan riskiarvioinnin ja toteuttamaan riskiarviota vastaavat suojaustoimenpiteet kaikkeen henkilötietoon liittyen.

> Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet [5].

Tietosuojavaltuutetun toimisto tarjoaa kuitenkin esimerkkiä siihen, miten yrityksen pitäisi huolehtia osoitusvelvollisuudestaan perustuen yrityksen kokoon ja käsiteltävään henkilötietoon [35].

Vaikka yrityksessä on suoritettu riskienhallintaa, yrityksessä ei ollut insinöörityön alkaessa käytössä formaalia riskienhallintamallia. Riskienhallintamallin formalisointi osaksi yrityksen toimintaa lisättiin yrityksen työjonoon ja se otettiin heti työn alle.

Riskiarvioinnin perusteella työntekijöiden henkilötiedon tietosuojaan on yrityksessä panostettu useilla eri tavoilla kaikilla defence-in-depth -mallin mukaisilla tasoilla. Tiedot ovat siis useiden eri administratiivisien ja tietoteknisten suojauskeinojen tavoin suojattuja. Kaikilla eri alueilla yrityksen valitsemat päätelaite-, tietoliikenne-, tietoliikennelaite-, sovellus- ja tietojärjestelmätoimittajat ovat maailmanlaajuisesti tai lokaalisti tunnettuja ja arvostettuja yrityksiä, jotka panostavat tietoturvan tasoon huimia rahasummia vuosittain jo oman etunsa vuoksi. [38;39.]

Insinöörityön aikana huomattiin myös tarvetta päivittää työntekijöille annettavaa tietosuojailmoitusta haastatteluissa löydettyjen tietojen pohjalta. Haastatteluiden

perusteella myös päivitettiin joitakin henkilötiedon käsittelyyn liittyviä prosessikuvauksia ja ohjeistuksia. Tietosuojailmoituksen päivittäminen lisättiin yrityksen työjonoon.

6 Yhteenveto

Insinöörityön tavoitteena oli tarkastaa työntekijätiedon käsittelyn dokumentaatio sekä verrata sitä henkilötiedonkäsittelystä annettuun viranomaisohjeistukseen sekä kerätä mahdolliset kehitystarpeet yrityksen kehitysjonoon.

Osana insinöörityötä haastateltiin työntekijätiedon käsittelyyn jollakin tavalla osallistuvia henkilöitä sekä tutustuttiin työntekijöiden henkilötietojen käsittelystä olemassa olevaan dokumentaatioon kuten prosessikaavioihin, työohjeisiin, politiikkoihin ja koulutusmateriaaleihin. Lisäksi tutustuttiin tietoturvaan liittyvään dokumentaatioon kuten tietoturvapolitiikoihin, työohjeisiin, koulutusmateriaaleihin sekä muuhun dokumentaatioon. Edellä mainittua yrityksen toimintaan liittyvää tietoa verrattiin viranomaisohjeistukseen ja lakiin.

Insinöörityön tuloksena huomattiin yrityksen työntekijöiden henkilötietojen tietosuojan olevan hyvällä tasolla lain ja viranomaisohjeistuksen vaatimusten mukaan. Puutteitakin silti löydettiin. Yrityksellä on ollut käytössä epäformaali riskienhallintamalli, johon perustuen tarvittavat tietosuojatoimenpiteet on valittu. Lisäksi työntekijöille annettavassa tietosuojailmoituksessa huomattiin puutteita. Puutteet raportoitiin yrityksen työjonoon, josta ne otettiin heti käsittelyyn asian korjaamiseksi. Prosessikuvauksissa tai muussa ohjeistuksessa olleita pieniä virheitä korjattiin osana insinöörityötä.

Insinöörityössä sivuutettiin tarkoituksenmukaisesti syvällisempi tutkiminen kansainvälisten siirtojen osalta. Kansainvälisten siirtojen osalta työ olisi siirtynyt liiaksi juridiikan puolelle, eikä täten osunut insinöörityötä tekevän osaamisalueelle. Kansainvälisten siirtojen osalta yritys jatkaa työtä lakimiesten kanssa.

Insinöörityön arvo yritykselle syntyi paremmasta käsityksestä työntekijöiden henkilötietojen käsittelystä sekä käsittelystä kommunikoimisesta yrityksen henkilöstölle. Insinöörityön tulokset ovat myös yrityksen johdolle ja yrityksen hallitukselle tärkeää tilannetietoa tietosuojan tilanteesta yrityksen toiminnassa.

Lähteet

1. Justin Group Oy. 2021. Verkkoaineisto. <https://www.justin.fi/fi/yritys/>. Luettu 28.09.2021.

2. Euroopan Unioni. 2021. Verkkoaineisto < https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm>. 26.3.2021. Luettu 28.9.2021.

3. Tietosuojavaltuutetun toimisto. 2021. Verkkoaineisto. <https://tietosuoja.fi/gdpr>. Luettu 28.9.2021.

4. Tietosuojavaltuutetun toimisto. 2021. Verkkoaineisto. <https://tietosuoja.fi/mika-on-henkilotieto>. Luettu 28.9.2021.

5. Euroopan Unioni. 2021. Verkkoaineisto. <https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI#d1e40-1-1>. Luettu 29.9.2021.

6. Tietosuojavaltuutetun toimisto. 2021. Verkkoaineisto. <https://tietosuoja.fi/documents/6927448/8214540/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+2020-+Tietosuojavaltuutetun+toimisto.pdf/3b506e9f-ae9a-c3fd-919a-df1c901ea6b8/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+2020-+Tietosuojavaltuutetun+toimisto.pdf?t=1600345504494>. Päivitetty 18.06.2021. Luettu 28.09.2021.

7. National Institute of Standards and Technology. 2021. Verkkoaineisto. <https://csrc.nist.gov/glossary/term/risk>. Luettu 30.6.2021.

8. Kyberturvallisuuskeskus. 2021. Verkkoaineisto. <https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas>. Päivitetty 4.2.2020. Luettu 30.9.2021.

9. Valtioneuvosto. 2021. Ohje riskienhallintaan. Verkkoaineisto. <https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf>.

10. Kyberturvallisuuskeskus. 2021. Verkkoaineisto. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/riskienhallinnan-hyvin-lyhyt-oppimaara>. Luettu 30.09.2021.

11. National Institute of Standards and Technology. 2021. Verkkoaineisto. < https://csrc.nist.gov/Projects/risk-management/about-rmf>. Luettu 30.9.2021.

12. National Institute of Standards and Technology. 2021. Verkkoaineisto. <https://csrc.nist.gov/glossary/term/cyber_threat>. Luettu 2.10.2021.

13. Iao, Kapua. 2021. Verkkoaineisto. <https://www.paubox.com/blog/what-is-threat-actor/>. Päivitetty 30.8.2021. Luettu 2.10.2021.

14. Iao, Kapua. 2021. Verkkoaineisto. <https://www.paubox.com/blog/what-is-a-threat-vector/>. Päivitetty 31.1.2021. Luettu 2.10.2021.

15. Tungal, Abi Tyas. 2021. Verkkoaineisto. <https://www.upguard.com/blog/attack-vector>. Päivitetty 24.9.2021. Luettu 2.10.2021.

16. Tietosuojavaltuutetun toimisto. 2021. Verkkoaineisto. <https://tietosuoja.fi/luottamuksellisuus-ja-turvallisuus>. Luettu 3.10.2021.

17. Tietosuojavaltuutetun toimisto. 2021. Verkkoaineisto. <https://tietosuoja.fi/arvioi-riskit>. Luettu 3.10.2021.

18. Swanagan, Michael. 2021. Verkkoaineisto. <https://purplesec.us/security-controls/>. Päivitetty 7.12.2021. Luettu 3.10.2021.

19. Fruhlinger, Josh. 2021. Verkkoaineisto. <https://www.csoonline.com/article/2124681/what-is-social-engineering.html>. Päivitetty 16.9.2021. Luettu 3.10.2021.

20. Tahto Group. 2021. Verkkoaineisto. <https://tahtogroup.fi/palvelut/it-ympäristöt/microsoft-365/paatelaitteiden-hallinta/>. Luettu 4.10.2021.

21. Järvinen, Petteri; Rousku, Kimmo. 2017. Työpaikan tietoturvaopas. Verkkoaineisto. <https://bisneskirjasto-almatalent-fi.ezproxy.metropolia.fi/teos/BAFBBXXTBBAED>. Luettu 5.10.2021.

22. Kadrich, Mark S. 2007. Endpoint Security. Verkkoaineisto. <https://learning.oreilly.com/library/view/endpoint-security/9780321436955/ch04.html>. Luettu 5.10.2021.

23. Microsoft. 2021. Verkkoaineosto. <https://azure.microsoft.com/en-us/overview/what-is-saas/>. Luettu 5.10.2021.

24. Cloudflare. 2021. Verkkoaineisto. <https://www.cloudflare.com/learning/ssl/what-is-https/>. Luettu 5.10.2021.

25. Wikipedia. 2021. Verkkoaineisto. <https://fi.wikipedia.org/wiki/HTTPS>. Päivitetty 7.7.2021. Luettu 5.10.2021.

26. Wikipedia. 2021. Verkkoaineisto. <https://fi.wikipedia.org/wiki/TLS>. Päivitetty 6.8.2021. Luettu 5.10.2021.

27. Solla, Katja; Dahlström, Rose-Maria. 2017. Verkkoaineisto. <https://yle.fi/aihe/artikkeli/2017/06/08/digitreenit-avoin-wifi-houkuttelee-ala-unohda-vaaroja>. Päivitetty 8.6.2017. Luettu 5.10.2021.

28. Panda. 2020. Verkkoaineisto. <https://www.pandasecurity.com/en/media-center/security/wpa-vs-wpa2/>. Päivitetty 8.4.2021. Luettu 5.10.2021.

29. Moody's Analytics. 2018. Verkkoaineisto. <https://www.moodysanalytics.com/articles/2018/best-practices-for-saas-security>. Päivitetty 4.2018. Luettu 5.10.2021.

30. Warren, Steven S. 2020. Verkkoaineisto. <https://searchcloudcomputing.techtarget.com/tip/Follow-this-SaaS-vendor-checklist-to-find-the-right-provider>. Päivitetty 11.5.2020. Luettu 5.10.2021.

31. Kucharczak, Justyna. 2020. Verkkoaineisto. <https://www.cyberark.com/resources/blog/how-to-secure-your-saas-applications>. Päivitetty 16.12.2020. Luettu 5.10.2021.

32. IEEE. Verkkoaineisto. <https://innovationatwork.ieee.org/physical-cyber-security-defenses/>. Luettu 5.10.2021.

33. Swinhoe, Dan. 2021. Verkkoaineisto. <https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html>. Päivitetty 4.8.2021. Luettu 5.10.2021.

34. Työturvallisuuskeskus. Verkkoaineisto. <https://ttk.fi/tyoturvallisuus_ja_tyosuojelu/tyoturvallisuuden_perusteet/tyoymparisto/mobiili_tyo_ja_etatyo>. Luettu 5.10.2021.

35. Tietosuojavaltuutetun toimisto. 2021. Verkkoaineisto. <https://tietosuoja.fi/osoitusvelvollisuus>. Luettu 5.10.2021.

36. Tietosuojavaltuutetun toimisto. 2021. Verkkoaineisto. <https://tietosuoja.fi/seloste-kasittelytoimista>. Luettu 6.10.2021.

37. Tietosuojavaltuutetun toimisto. 2021. Verkkoaineisto. <https://tietosuoja.fi/rekisteroidyn-informointi>. Luettu 6.10.2021.

38. Palmu, Jani. 2021. Toimitusjohtaja, Justin Group Oy. Keskustelut 28.09.2021 – 6.10.2021.

39. Yrityksen sisäinen dokumentaatio. 2021. Luettu 28.9.2021 – 6.10.2021.