Opinnäytetyö (AMK)

Liiketalous

2020

Olli-Matti Suominen

HENKILÖTIETOJEN KÄSITTELY YLEISEN TIETOSUOJA-ASETUKSEN MUKAISESTI

Case: Yritys X

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalous

2020| Sivumäärä 61

Olli-Matti Suominen

HENKILÖTIETOJEN KÄSITTELY YLEISEN TIETOSUOJA-ASETUKSEN MUKAISESTI

Euroopan unionin yleisen tietosuoja-asetuksen voimaantulo koski jokaista Unionin alueella olevaa yritystä tai yhteisöä, joissa käsitellään jollain tapaa yksilön henkilötietoja. Henkilötietoja tulee asetuksen mukaisesti käsitellä lainmukaisesti, asianmukaisesti sekä rekisteröidyn kannalta läpinäkyvästi. Henkilötietojen käsittely on osana yritysten päivittäisiä työrutiineja, ja siksi niiden käsittelyyn tulee kiinnittää erityistä huomiota.Tässä opinnäytetyössä selvitetään, miten henkilötietoja tulee käsitellä, ja miten tietosuoja-asetuksen noudattaminen näkyy toimeksiantajayrityksessä. Opinnäytetyö tulee keskittymään henkilöstöhallinnolle olennaisiin henkilötietoja käsitteleviin toimintaperiaatteisiin.

Opinnäytetyön teoriaosiossa esitetään ensimmäiseksi yleisiä tietosuoja-asetukseen liittyviä asioita ja olennaisia peruskäsitteitä, ja miten käsittely näkyy etenkin henkilöstöhallinnossa. Tämän jälkeen työssä tullaan avaamaan yksityiskohtaisemmin tärkeimmät tietojen käsittelyyn liittyvät periaatteet ja toimintatavat. Opinnäytetyö sisältää tärkeimmät henkilötietojen käsittelyn asiakokonaisuudet ja avaa perusteellisesti niihin liittyvät asiat. Teoriaosio lähtee liikkeelle henkilötietojen tunnistamisesta ja niiden käytön toimintaperiaatteista ja oikeusperusteista. Tämän jälkeen käydään läpi erityisiä henkilötietoryhmiä ja automaattista päätöksentekoa. Teoriasosion loppupuolella keskitytään henkilötietojen käsittelyn riskeihin ja niihin varautumiseen, jonka jälkeen avataan rekisteröidyn oikeuksia ja rekisterinpitäjän velvollisuuksia.

Empiirisen osion tarkoituksena on kartoittaa toimeksiantajayrityksen tietosuoja-asetuksen noudattamisen nykytilanne henkilötietojärjestelmiin tutustumisen ja haastattelusta saatujen vastausten perusteella. Empiirisessä osiossa tarkastellaan toimeksiantajayrityksen käyttämiä henkilötietojärjestelmiä, niiden toimintaa ja käyttöä henkilötietojen käsittelyn yhteydessä. Henkilötietojärjestelmien jälkeen tullaan haastattelua hyväksi käyttäen tarkastelemaan millaisissa tilanteissa ja miten tietosuoja-asetuksen noudattaminen yrityksen sisällä näkyy, ja kuinka mahdollisiin riskeihin on varauduttu.

ASIASANAT:

Henkilötieto, Käsittely, Rekisterinpitäjä, Rekisteröity, Tietosuoja-asetus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business administration

2020 | Total number of pages 61

Olli-Matti Suominen

PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH THE GENERAL DATA PROTECTION REGULATION

The entry of the General Data Protection Regulation of the European Union applied to any company or entity in the territory of the Union which in any way processes personal data of an individual. In accordance with the Regulation, personal data must be processed lawfully, properly and transparently for the data subject. The processing of personal data is part of the day-to-day work routines of companies and therefore special attention must be paid to their processing.This aim of this thesis is to explain how personal data should be processed and how compliance with the data protection regulation is reflected in the client company. The thesis focuses on the operating principles relevant to human resources management.

The theoretical part of the thesis first presents general issues related to the Data Protection Regulation and essential basic concepts, and how the processing is reflected especially in human resources management. After this, the main principles and operating methods related to data processing are opened in a more detailed way. The thesis contains the most important personal data processing issues and thoroughly opens the related issues. The theory section starts with the identification of personal data and the operating principles and legal bases for their use. This is followed by specific groups of personal data and automatic decision-making. Towards the end of the theoretical part, the focus is on the risks of processing personal data and preparing for them. Finally, the rights of the data subject and the obligations of the controller are examined.

The purpose of the empirical section is to map the current situation of the client company's compliance with the data protection regulation on the basis of access to personal information systems and responses to the interview conducted. The empirical section examines the personal information systems used by the client company, their operation and use in connection with the processing of personal data. Following the personal data systems, the interview is used to look at the situations in which compliance with the data protection regulation is reflected within the company, and how potential risks have been prepared for.

KEYWORDS:

Personal data, Processing, Data controller, Data subject, Data protection regulation

SISÄLTÖ

KUVAT

TAULUKOT

1 JOHDANTO

Tämä opinnäytetyö käsittelee Euroopan unionin tietosuoja-asetusta (2016/679), jota alettiin soveltaa täysimääräisesti 25.5.2018. Euroopan unionin tietosuoja-asetus koskee lähtökohtaisesti kaikkea henkilötietojen käsittelyä EU:n jäsenvaltioissa. GDPR (General Data Protection Regulation) koskee kaikkia rekisterinpitäjiä, jotka käsittelevät henkilötietoja, myös yrityksen omasta henkilöstöstä kerättyjä tietoja. Asetuksen soveltaminen vaatii, että kaikissa henkilötietoja käsittelevissä organisaatioissa henkilötietosuojan pitää olla asetuksen edellyttämässä kunnossa (Tietosuoja-asetus 2020). EU:n yleisen tietosuoja-asetuksen tehtävänä on suojata henkilöiden oikeutta henkilötietojen suojaan ja taata henkilötietojen vapaa liikkuvuus Euroopan unionin alueella. Asetus sisältää sääntelyn mm. siitä milloin henkilötietoja saa kerätä ja käsitellä ja mitä velvollisuuksia käsittelyyn liittyy. Asetusta sovelletaan sellaisenaan henkilötietojen käsittelyyn eli sitä ei panna täytäntöön kansalliseen lakiin. 1.1.2019 voimaan tullut tietosuojalaki (1050/2018) täsmentää ja täydentää asetusta kansallisella tasolla (EK 2020).

Opinnäytetyön toimeksiantajana toimii Satakunnassa sijaitseva teknologiateollisuuden yritys, joka on osa ruotsalaista konsernia. Euroopan Unionin yleisen tietosuoja-asetuksen edellyttämiä toimenpiteitä on noudatettu toimeksiantajayrityksessä vuoden 2018 soveltamispäivästä lähtien. Yrityksen tavoitteena on varmistua siitä, että tietosuoja-asetuksen velvoittamia toimenpiteitä noudatetaan jatkossakin lainmukaisella tavalla. Opinnäytetyö keskittyy erityisesti henkilöstö- ja palkkahallinnossa käytettäviin ja hyödynnettäviin henkilötietojen käsittelyyn liittyviin lainmukaisiin periaatteisiin ja toimintatapoihin. Koska tietojen käsittelyn toimintakäytännöt ja -periaatteet ovat molemmilla yrityksen hallinnoilla samanlaiset, ja kyseiset osa-alueet noudattavat samoja tietosuoja-asetuksen määräämiä toimintaohjeita, tulen opinnäytetyössä käyttämään vain nimeä henkilöstöhallinto.

Opinnäytetyön tavoitteena on tutkia, miten hyvin toimeksiantajayrityksen nykyiset järjestelmät ja toimintatavat vastaavat Euroopan unionin yleisen tietosuoja-asetuksen asettamia vaatimuksia. Tavoitteena on saada aikaan kattava kuva siitä, missä henkilötietoja säilytetään, miten tietojen käsittely käytännössä toimii, sekä kuinka hyvin yrityksessä tiedostetaan henkilötietojen suojaaminen ja käsittelyn eri toimenpiteet.

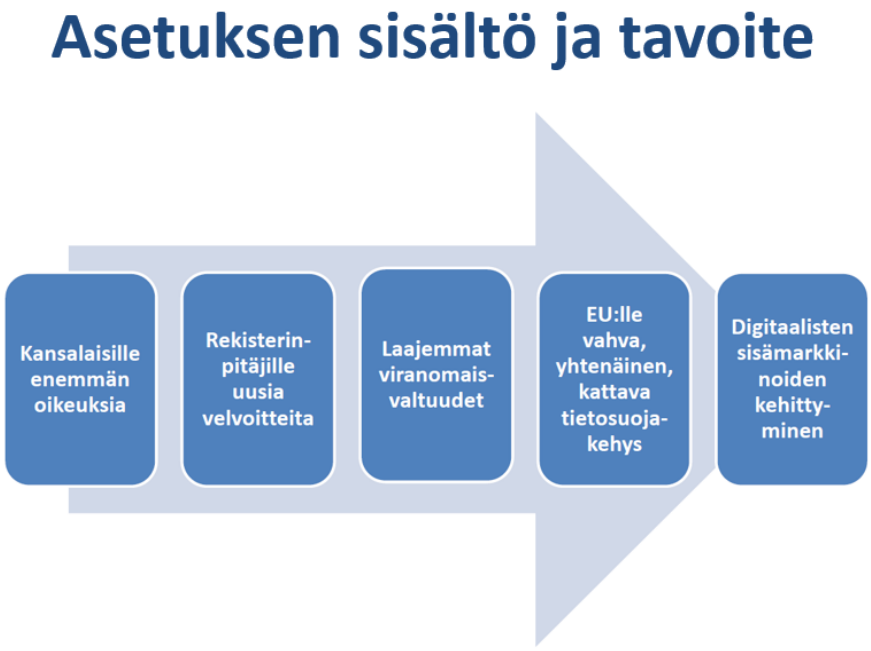
Opinnäytetyön tutkimus sijoittuu neljään pääkappaleeseen. Tutkimuksen aloittavassa kakkoskappaleessa käydään läpi yleisen tietosuoja-asetuksen pääsisältö. Kappaleessa avataan miten tietosuoja-asetus näkyy etenkin henkilöstöhallinnossa, ja mitkä ovat oleellisimmat henkilötietojen käsittelyyn liittyvät asiakokonaisuudet. Kolmannessa kappaleessa käydään läpi rekisteröidyn oikeuksia, sekä rekisterinpitäjän velvollisuuksia, joista jälkimmäinen keskittyy olennaisesti rekisterinpitäjän osoitusvelvollisuuteen. Neljännessä kappaleessa tutkitaan toimeksiantajayrityksen tietosuoja-asetuksen soveltamista käytännössä. Tutkimuksessa käytetään hyödyksi yrityksen henkilötietojärjestelmiä, sekä kahta kvalitatiivista haastattelua. Henkilötietojärjestelmiin tutustuminen tapahtui yksin, sekä yhdessä yrityksen henkilöstöpäällikön kanssa. Haastattelut suoritettiin etänä Microsoft Teams -sovelluksen ja sähköpostin välityksellä. Empiirisessä tutkimuksessa heijastetaan henkilötietojärjestelmistä ja haastatteluista saatuja tietoja opinnäytetyön teoriaosioon, ja tätä kautta saamaan kuva toimeksiantajan henkilötietojen käsittelyn nykytilanteesta. Viimeisessä kappaleessa on avattu tutkimuksesta saatuja johtopäätöksiä.

2 EU:N YLEINEN TIETOSUOJA-ASETUS (GDPR)

2.1 Mikä on GDPR?

GDPR on lyhenne sanoista General Data Protection Regulation (yleinen tietosuoja-asetus). Se on henkilötietojen käsittelyä sääntelevä laki, jota alettiin soveltaa kaikissa EU-maissa keväällä 2018. EU:n yleisen tietosuoja-asetuksen tavoitteina ovat yksilön oikeuksien ja vapauksien vahvistaminen, sisämarkkinoiden lujittaminen, tietosuojan globaalin ulottuvuuden huomioiminen sekä tietosuojasääntöjen täytäntöönpanon valvonnan tehostaminen. Asetuksen tavoitteena on luoda Euroopan unionille vahva, yhtenäinen ja kattava tietosuojakehys. Asetuksella pyritään myös parantamaan luottamusta online-palveluihin ja näin edistää EU:n digitaalista sisämarkkinoiden kehittämistä. (Opitietosuojaa 2020.)

Yleinen tietosuoja-asetus korvaa vuonna 1995 annetun henkilötietodirektiivin. Tietosuoja-asetus sisältää säännökset mm. henkilötietojen käsittelyä koskevista periaatteista, käsittelyn lainmukaisuudesta, henkilötietojen käsittelijän ja rekisterinpitäjän velvoitteista ja vastuista, rekisteröiden suostumuksen edellytyksistä ja arkaluonteisten tietojen käsittelystä. (Opitietosuojaa 2020.)



Kuva 1. EU:n tietosuoja-asetuksen sisältö ja tavoite (Opitietosuojaa 2020).

Yleisen tietosuoja-asetuksen taustalla on tarve vastata teknologian kehitykseen, sekä digitalisaatioon ja globalisaatioon liittyviin haasteisiin koskien henkilötietojen suojaa. Tavoitteena on yhtenäistää tietosuojaa koskevaa lainsäädäntöä Euroopan unionin alueella eli luoda yhdet yhteiset tietosuojapelisäännöt unionin yrityksille. Asetuksen tavoitteena on parantaa kuluttajien luottamusta digitaalisiin sisämarkkinoihin, sekä lisätä henkilötietojen käsittelyn läpinäkyvyyttä ja avoimuutta. Asetus parantaa yksilön perusoikeuksia ja -vapauksia sekä heidän oikeuttaan henkilötietojensa suojaan. Asetus koskee kaikkia organisaatioita, joilla on tallessa oman henkilökunnan tai yrityksen sidosryhmien henkilötietoja. Kaikkien organisaatioiden tulee noudattaa yleistä tietosuoja-asetusta riippumatta siitä onko yritys julkisella vai yksityisellä sektorilla. (Triuvare 2020.)

2.2 Tietosuoja-asetuksen peruskäsitteitä

Seuraavaksi esitetään henkilötietojen käsittelyyn liittyviä peruskäsitteitä.

- **Henkilötieto** tarkoittaa kaikkea tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvää tietoa. Luonnollinen henkilö voidaan tunnistaa joko suoraan tai epäsuorasti tunnistetietojen tai hänelle tunnusomaisten piirteiden perusteella. Tunnistetietoja ovat esimerkiksi nimi, henkilötunnus ja osoitetiedot. Tunnusomaisia piirteitä ovat esimerkiksi henkilön fyysiset, taloudelliset, kulttuurilliset tai sosiaaliset piirteet, kuten henkilön potilastiedot. (Minilex 2020a.) Henkilötiedot eivät rajaudu vain tutkittavia koskeviin tietoihin. Tutkimusaineistoihin voi sisältyä tunnistetietoja myös henkilön lähipiiristä tai muista kolmannen osapuolen henkilöistä. Kaikki yksittäiseen henkilöön liittyvät tiedot voivat olla henkilötietoja. Tiedot voivat liittyä yksityiselämään, perhe-elämään, henkilön terveydentilaan, fyysisiin ominaisuuksiin, ammatilliseen toimintaan tai taloudelliseen ja sosiaaliseen käyttäytymiseen. (Tietoarkisto 2020.)

- **Henkilörekisteri** tarkoittaa lainmukaisesti yhteen muodostetuista henkilötiedoista koostuvaa tietojoukkoa. Henkilörekisterille tyypillistä on, että sitä käsitellään esimerkiksi automaattisten tietojenkäsittelyn avulla. Henkilörekisteri on tavallisesti rakennettu niin, että sen käyttö on yksinkertaista ja tiedon etsiminen rekisteristä onnistuu nopeasti. (Axactor 2020.) Tietojoukkoa kutsutaan henkilörekisteriksi, mikäli sen tiedot ovat saatavilla tietyin perustein riippumatta siitä, onko tieto keskitetty, hajautettu tai esimerkiksi jaettu toiminnallisin tai

maantieellisin perustein. Henkilötiedot voidaan rekisteröidä esimerkiksi sähköisenä tiedostona, paperisina, mappeina, tai ääni- ja kuvatallenteina. (Minilex 2020b.)

- **Suostumus** on yksi oikeusperuste henkilötietojen käsittelylle, joka antaa rekisteröidylle mahdollisuuden valvoa henkilötietojensa käsittelemistä ja vaikuttaa henkilötietojensa käsittelyyn peruuttamalla suostumuksen. Suostumus luokitellaan päteväksi mikäli se on aidosti vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu. Rekisteröity voi antaa suostumuksen ennalta määriteltyyn, nimenomaiseen ja lailliseen tarkoitukseen. Jos tietojen käsittelyn tarkoitus muuttuu, rekisteröidyltä on pyydettävä uusi suostumus ennen käsittelyn aloittamista. Suostumusta pyydettäessä on yksilöitävä käyttötarkoitus, johon tietoja kerätään. Mikäli henkilötietoja käsitellään useaan eri tarkoitukseen, rekisteröidyn on voitava valita kaikki käyttötarkoitukset, joihin hän haluaa antaa suostumuksensa.

  Mikäli rekisteröity antaa suostumuksensa kirjallisessa ilmoituksessa, joka sisältää myös muita asioita, suostumusta koskeva pyyntö on esitettävä selvästi erillään muista asioista helposti ymmärrettävässä muodossa selkeällä ja yksinkertaisella kielellä. Rekisteröidyllä on oikeus peruuttaa suostumus milloin tahansa. Suostumuksen peruuttaminen ei vaikuta suostumuksen perusteella suoritetun käsittelyn lainmukaisuuteen. (Digiturvamalli 2017a.) Suostumus ei ole aidosti vapaaehtoinen, mikäli rekisteröity on heikommassa asemassa suhteessa rekisterinpitäjään. Heikompi asema voi tulla kyseeseen mikäli suostumuksen pyytäjä on rekisteröidyn työnantaja tai viranomainen. Suostumuksen antamisesta on oltava mahdollisuus kieltäytyä, ja se on voitava peruuttaa ilman rekisteröidylle koituvia haitallisia seurauksia. Peruuttamisen tulee olla yhtä helppoa kuin suostumuksen antamisenkin. (Tietosuojavaltuutetun toimisto 2020a.)

- **Rekisterinpitäjä** tarkoittaa ihmistä tai organisaatiota, joka määrittelee mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Rekisterinpitäjänä voi toimia esimerkiksi jäsenistään tietoja keräävä yhdistys, sosiaalisen median palvelu tai sairaala. (Tietosuojavaltuutetun toimisto 2020b.) Rekisterinpitäjä ei yleensä tarkoita yhtä henkilöä. Mikäli yritys päättää miten ja mihin tarkoitukseen henkilötietoja käsitellään, luokitellaan kyseinen yritys tässä tapauksessa

rekisterinpitäjäksi. Yrityksen henkilötietoja käsittelevät työntekijät käsittelevät tietoja suorittaakseen kyseisen yrityksen tehtäviä rekisterinpitäjänä. Mikäli yritys päättää yhdessä muiden organisaatioiden kanssa siitä miksi ja miten henkilötietoja käsitellään, on organisaatio tässä tapauksessa **yhteisrekisterinpitäjä**. Yhteisrekisterinpitäjien tulee sopia jokaisen osapuolen vastuista yleisen tietosuoja-asetuksen sääntöjen noudattamiseksi. Sopimuksen tärkeimmistä seikoista tulee ilmoittaa niille yksilöille, joiden henkilötietoja käsitellään. (Euroopan komissio 2020a.)

- **Rekisterinpitäjän oikeutettu etu** on kyseessä, kun henkilötietojen käsittelyä ei voida välttämättä perustella yksilön kanssa tehdyllä sopimuksella, tai lakisääteisillä velvoitteilla. Keskeisenä asiana tässä voidaan pitää yleistä tilannetta, jossa yrityksen on käsiteltävä henkilötietoja voidaakseen suorittaa liiketoimintaansa liittyviä tehtäviä. Henkilötietojen käsittely voi tässä tapauksessa olla perusteltua oikeutetun edun perusteella. Yrityksen tulee tarkastaa, että oikeutetun edun mukaisesta toiminnasta ei aiheudu vakavaa haittaa yksilöiden oikeuksille ja vapauksille. Mikäli toiminta aiheuttaa huomattavaa haittaa yksilölle, ei oikeutettu etu perusteena ole pätevä, ja yrityksen tulee löytää jokin toinen oikeusperusta. (Tietosuojavaltuutetun toimisto 2018.) Rekisterinpitäjän etu voi olla oikeutettu ja mahdollistaa henkilötietojen käsittelyn, jos kyseessä on esimerkiksi (Tietosuojatyöryhmä 2014):

    - asiakassuhde
    - suoramarkkinointi
    - tieteellinen ja historiallinen tutkimus tai tilastointi
    - henkilötietojen hallinnollinen siirtäminen yrityksen/organisaation sisällä
    - petoksen estäminen
    - IT-järjestelmien tietoturvan varmistaminen

  Yksityisen henkilön edut ja oikeudet ovat lähtökohtaisesti suojatumpia kuin rekisterinpitäjän. Henkilötietoja ei saa käsitellä, mikäli rekisteröidyn edut tai oikeudet syrjäyttävät rekisterinpitäjän tai muun kolmannen osapuolen edun. Vaikka rekisterinpitäjän edut olisivat vähäisiä, ne voivat syrjäyttää rekisteröidyn edut vain, mikäli niiden vaikutukset ovat vielä vähäisempiä. Merkittävät tai pakottavat intressit voivat kuitenkin oikeuttaa henkilötietojen käsittelyn, kunhan

tiettyjä takeita ja toimenpiteitä noudatetaan. (Tietosuojavaltuutetun toimisto 2020c.)

Oikeutettua etua ei tule käyttää perusteena, mikäli jonkin muun perusteen käyttäminen on mahdollista. Jos käsittely perustuu rekisterinpitäjän oikeutettuun etuun on rekisteröidyllä oikeus vastustaa henkilötietojensa käsittelyä. Mikäli oikeutettua etua käytetään perusteena, on kerrottava avoimesti mikä etu on kysymyksessä. Rekisteröidyn on kyettävä arvioimaan oikeutettu etu ja sen suhde hänen omiin oikeuksiinsa ja vapauksiinsa, joita käsittely mahdollisesti vaarantaa. Käsittelylle on kyettävä nimeämään todellinen tarve. Käsittelyn tarpeellisuus vain rekisterinpitäjälle ei itsessään anna perustetta oikeutetulle edulle, vaan pitää pystyä osoittamaan, että käsittelyn vaikutukset eivät aiheuta vahinkoa rekisteröidyn oikeuksille ja vapauksille. (Ala-Varvi 2020.)

- **Henkilötietojen käsittelijä** on taho, joka toimii rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi tarkoittaa yritystä, yksityistä elinkeinonharjoittajaa, viranomaista tai yhdistystä. Rekisterinpitäjän alaisuudessa toimivia henkilötietoja käsitteleviä työntekijöitä ei lasketa henkilötiedon käsittelijöiksi. Henkilötietojen käsittelijän tehtävät voivat olla laajoja ja yleisiä, ja niihin voi liittyä toisen organisaation palvelun hallinta esimerkiksi kyseisen yrityksen palkanlaskennan osalta. Yritys on kuitenkin rekisterinpitäjä sellaisten tietojen käsittelyssä, joita se käsittelee omasta puolestaan. Yritys on rekisterinpitäjä mikäli se käsittelee oman organisaation henkilökunnan henkilötietoja. (Tietosuojavaltuutetun toimisto 2020d.) Henkilötietojen käsittelijä ei saa itse päättää, mitä tarkoituksia varten tai kuinka henkilötietoja käsitellään. Käsittelijä ei päätä käsittelyn tietosuoja-asetuksen tarkoitetusta oikeudellisista perusteista tai tarkoituksista, vaan käsittelijän on noudatettava rekisterinpitäjän antamia ohjeita. (Suomen tilintarkastajat 2018.)

2.3 GDPR Henkilöstöhallinnossa

Yritysten on arvioitava EU:n yleisen tietosuoja-asetuksen vaatimusten kokonaisvaltainen henkilötietojen käsittelykäytäntö esimerkiksi asiakasprosesseissa, työntekijöiden henkilöstöhallinnossa ja sopimuksissa alihankkijoiden kanssa. Yrityksen kannattaa kartoittaa ja arvioida henkilötietojensa käsittelykäytänteiden ja tietosuojan nykytila.

Nykytilan kartoittaminen ja arviointi voidaan saada kuvaamalla esimerkiksi (Andreasson, Riikonen, Ylipartanen 2017, 39 - 40.):

1. mitä henkilötietovarantoja yrityksen hallussa on
2. mitä lakeja sen henkilötietojen käsittelyyn sovelletaan
3. miten tietosuojaperiaatteet on otettu huomioon
4. toimintaan liittyvät henkilötietovirrat
5. henkilötietojen käsittelyn oikeusperusteet
6. miten tietoturvasta on huolehdittu
7. miten henkilötietojen käsittelyyn liittyvä riskienhallinta on toteutettu.

Kartoituksen jälkeen on tärkeää selvittää, mitä muutoksia ja toimenpiteitä tietosuoja-asetuksen sääntely sen suorittamalle henkilötietojen käsittelylle tarkoittaa. Rekisterinpitäjään kohdistuvat velvoitteet määräytyvät pääsääntöisesti riskiperusteisen lähestymistavan mukaisesti. Toimenpiteiden laatu ja laajuus riippuvat esimerkiksi yrityksen käsittelemistä henkilötiedoista, käsittelyn riskistä ja nykyisistä käytännöistä. Johtohenkilöstön tuee tiedostaa lainsäädännössä tapahtuvat muutokset sekä niiden vaikutukset organisaation eri toimintoihin. (Andreasson ym. 2017, 39 - 40.)

Henkilöstöhallinnon tarkastelussa tietosuoja-asetuksen näkökulmasta, keskeisimpiä asioita ovat luottamus, selkeys, varmuus ja helppokäyttöisyys. Henkilötietojärjestelmän palvelu/palvelut tulee olla täysin luotettava. Palvelu pitää olla oikein suunniteltu ja sen pitää toimia täysin tietosuojalainsäädännön mukaisesti. Henkilötietoja käsittelevien henkilöiden tulee olla selkeästi tietoinen siitä, mitä henkilötietoja palvelussa käsitellään ja kuka yrityksessä pääsee kyseisiin tietoihin käsiksi. (Rauhala 2018a.)

Henkilötietojen käsittelytavan tulee olla toimintavarma. Varma toimintatapa edellyttää myös selkeän varautumisen mahdollisiin poikkeustilanteisiin esimerkiksi tietomurron sattuessa. Kaikki henkilötietojen käsittelyyn liittyvät asiat konkretisoituvat ja selkeytyvät sitä mukaa, mitä helppokäyttöisemmäksi henkilötietojen käsittelyn saa. Prosessit ja käyttöoikeudet on suositeltavaa pitää yksinkertaisina. Tämä takaa henkilötietopalvelun tarkoituksenmukaisen käyttämisen ja varmistaa tietosuoja-asetuksen toteutumisen käytännössä. (Rauhala 2018a.)

Työhaastattelun yhteydessä uudelta työnhakijalta voidaan lähtökohtaisesti kysyä vain työnhakuun ja työhön liittyviä kysymyksiä, ja tallentaa vain työnhakuun ja työhön liittyviä tarpeellisia asioita. Tiedot tulevat ensisijaisesti työnhakijalta itseltään. Muissa tapauksissa tiedon keräämiseen ja käsittelyyn tarvitaan työnhakijan suostumus.

Tietosuoja-asetuksen myötä työnantajan tulee antaa yksityiskohtaisempaa tietoa siitä, mitä tietoja käsitellään ja mihin tarkoituksiin. Tietoja saa kerätä vain tarpeellisiin tarkoituksiin, ja edes rekisteröidyn antama suostumus ei oikeuta rekisterinpitäjää käsittelemään työnhakijan henkilötietoja tarpeettomasti. Mikäli työnantaja päätyy suostumukseen, on tärkeää arvioida huolellisesti sen täyttämät asetetut vaatimukset ja muistaa, että rekisteröidyllä on aina oikeus purkaa suostumus tilanteesta riippumatta. (Kurvi, Sedig 2017.)

Yleinen tietosuoja-asetus vaikuttaa suuresti henkilöstöhallinnon työntekijöihin, sillä henkilötietojen käsittely on oleellinen osa työn kuvaa. Tietosuoja-asetus vaikuttaa järjestelmiin, prosesseihin ja erilaisiin arkipäiväisiin työrutiineihin. Tarkoituksena on lisätä tietoisuutta siitä, mitä henkilötietoja käsitellään ja miksi, missä tietoja säilytetään ja kenellä on oikeus päästä käsiksi tietoihin. Tietosuoja-asetuksen myötä henkilötietojen säilyttämiseen järjestelmän sisä - ja ulkopuolella on oltava järkevä peruste, ja on tärkeää, että työntekijät ymmärtävät miksi heidän tietoja kerätään ja millaisia rajoituksia tietoihin liittyy. (Aditro 2020.)

Tietosuoja-asetuksen myötä jokaisella henkilöllä on oikeus päästä käsiksi kaikkiin tietoihin, jotka yritys heistä on tallentanut, helposti luettavassa muodossa. Jokaisella henkilöllä on myös oikeus saada tiedot hävitettyä pysyvästi, oikeus siirtää tiedot toiseen järjestelmään ja oikeus saada tietää mahdollisista tietomurroista. Yrityksen tulisi tarkistaa, että henkilötiedot ovat tallennettuna järjestelmään, joka integroituu sujuvasti muihin järjestelmiin, että tietoja pidetään ajan tasalla helposti asianomaiselle luovutettavassa muodossa ja että henkilötiedot ovat vain tiettyjen sallittujen henkilöiden tarkasteltavissa. Koska tiedon kerääminen, tallentaminen ja sen muistaminen saattaa olla työlästä, voi avuksi käyttää yksinkertaista, mutta tehokasta muistilistaa joka auttaa henkilöstöhallintoa selvittämään järjestelmät, johon yritys/organisaatio tällä hetkellä tallentaa henkilötietoja. (Sympa 2017.)

Taulukko 1. Henkilötietojen käsittelyn muistilista (Sympa 2017)

	Missä tietoja käsitellään?	Miksi tietoja käsitellään?	Mitä tietoja käsitellään?	Kenellä on pääsy tietoihin?	Miten ja milloin tiedot poistetaan?	Kuka vastaa rekisteristä?
Työntekijöiden HRM						
Työntekijöiden HRD						
Työnhakijat						
Freelancerit						
Kumppanit						
Muut						

Taulukkoon listataan kaikki järjestelmät, joissa tietoja käsitellään. Luettelon on tarpeen olla kattava, joten on tärkeää jäljittää kaikki järjestelmät, tiedostot ja kansiot jotka sisältävät tiettyyn henkilöön yhdistettävissä olevia tietoja. Taulukko toimii hyvänä apuvälineenä henkilötietojen paikannukselle ja käsittelylle. (Sympa 2017.)

Kun yritys on valmis varmistamaan, tukeeko heidän toimintatavat yleisen tietosuoja-asetuksen vaatimuksia, on hyvä pohtia ja pyrkiä vastaamaan seuraaviin kysymyksiin:

1. Onko henkilön kaikki tarvittavat tiedot mahdollista toimittaa kohtuullisessa ajassa?
2. Onko henkilön tiedot helposti poistettavissa, jos tilanne sitä vaatii?
3. Onko henkilön kaikki tiedot helposti lähetettävässä sekä luettavassa muodossa?
4. Onko helposti osoitettavissa mitä tietoa, kenen toimesta ja mihin tarkoitukseen henkilön tietoja käsitellään?
5. Onko tiedossa, mitkä tiedot pitää lain mukaan säilyttää ja mitä voidaan poistaa?

Jotta henkilöstöhallinnon tietosuoja-asetuksen vaatimukset täyttyvät, järjestelmiltä ja prosesseilta vaaditaan liitettävyyttä toisiin järjestelmiin, sekä niiden joustavia käyttöoikeuksia ja muokattavia rajapintoja. Henkilöstöhallinnon on myös valmistauduttava tiedottamaan johtoa ja esimiehiä mahdollisista muutoksista ja tarpeen

vaatiessa henkilötietoa käsittelevien ohjelmien vaatimustenmukaisuuksien tarkastamiseen. (Rauhala 2018b.)

2.4 Henkilötietojen käsittely

Henkilötietojen käsittelyyn liittyy useita lakisääteisiä prosesseja, joita jokaisen henkilötietoja käsittelevän henkilön tai organisaation tulee noudattaa yleisen tietosuoja-asetuksen sääntöjen mukaisesti. Henkilötietojen käsittely voi tarkoittaa esimerkiksi henkilötietojen keräämistä, säilyttämistä, siirtämistä, käyttöä ja luovuttamista. Kaikki henkilötietoihin kohdistuvat toimenpiteet käsittelyn suunnittelusta poistamiseen ovat henkilötietojen käsittelyä. (Tietosuojavaltuutetun toimisto 2020b.)

2.4.1 Henkilötietojen tunnisteellisuus

Henkilötiedoiksi lasketaan kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot. Luonnollinen henkilö on tunnistettavissa erilaisten tunnistetietojen perusteella, joita ovat esimerkiksi nimi, sijaintitieto, tai henkilötunnus. Henkilö on myös tunnistettavissa, jos hänet voidaan tunnistaa kyseisen henkilön tunnusomaisen piirteen perusteella. Tunnusomaisiksi piirteiksi lasketaan fyysiset, geneettiset, psyykkiset, taloudelliset, sosiaaliset ja kulttuuriset tekijät. Edellä mainitut piirteet voivat olla esimerkiksi potilastietoja, henkilön lemmikin eläinlääkäritietoja tai vaikka henkilön vanhempien perinnölliseen sairauteen liittyviä tietoja. Tunnisteellisia henkilötietoja tulee säilyttää suojattuna riippumatta siitä, missä muodossa tietoja säilytetään. Tiedot voivat olla esimerkiksi tekstinä tietokoneen tiedostoissa, paperisena, kuvana, äänitallenteena, videotallenteena, biologisena näytteenä tai muuna sähköisenä muotona. (Minilex 2020c.)

Henkilö voidaan tunnistaa joko suoraan tai epäsuorasti erilaisten tunnistetietojen perusteella. On tärkeä muistaa, että henkilötiedot eivät rajaudu ainoastaan kyseisen henkilön omiin tietoihin, vaan henkilötietoihin voi sisältyä myös henkilön lähipiirin tai muiden kolmansien osapuolien tiedot. Henkilötiedot voivat olla objektiivisia tai subjektiivisia eikä niiltä odoteta totuutta tai todennettavuutta. Tieto on tunnisteellista, mikäli sen perusteella pystytään tunnistamaan yksittäinen henkilö tai havaintorypäs, kuten saman kotitalouden henkilöt. (Tietoarkisto 2020.)

Tietoa jotka yksin riittävät tunnistamaan luonnollisen henkilön ovat esimerkiksi henkilön koko nimi, henkilötunnus, henkilönimen mukainen sähköpostiosoite ja erilaiset biometriset tunnisteet kuten sormenjälki, silmän iiris ja henkilön käsin tehty allekirjoitus. (Tietoarkisto 2020).

Epäsuorat tunnisteet voidaan jakaa vahvoiksi epäsuoriksi tunnisteiksi tai epäsuoriksi tunnisteiksi. Vahvoiksi epäsuoriksi tunnisteiksi kutsutaan tietoa, joka ei suoraan kerro kuka henkilö on, mutta sen avulla henkilön pystyy kohtuullisen helposti tunnistamaan. Vahvoja epäsuoria tunnisteita ovat esimerkiksi henkilön postiosoite, auton rekisterinumero, puhelinnumero, henkilön julkaiseman teoksen viitetiedot, tunnistetietoja sisältävän verkkosivun osoite, muu kuin henkilönimen mukainen sähköpostiosoite ja harvinainen ammattinimike. Harvinaiset tapahtumat ja yksilöidyt koodit, joiden avulla rajatuiden henkilöiden joukolla on mahdollista tunnistaa henkilö yksiselitteisesti voidaan myös tilanteesta riippuen luokitella vahvoiksi epäsuoriksi tunnisteiksi. (Tietoarkisto 2020.)

Epäsuoria tunnisteita on tiedot, jotka yksin eivät riitä tunnistamaan yksittäistä henkilöä, mutta tietoja yhdistämällä henkilö on mahdollista saada tunnistetuksi. Epäsuorat tunnisteet voivat olla esimerkiksi henkilön sukupuoli, ikä, koulutus, pääasiallinen työmarkkina- tai markkina-asema, tulot, kansallisuus, siviilisääty, etninen tausta, työpaikka tai koulu. Epäsuora tunniste voi olla myös henkilön asuinaluetta koskevat epäsuorat muuttujat kuten postinumero, kaupunginosa, kunta, maakunta ja alue. Päivämäärät voidaan luokitella epäsuoriksi tunnisteiksi mikäli kyseessä on syntymäpäivä, kuolinpäivä tai uutiskynnyksen ylittänyt tapahtumapäivämäärä. (Tietoarkisto 2020.)

Henkilötiedot voidaan myös anonymisoida niin, ettei henkilön tiedot ole enää tunnistettavassa muodossa. Mikäli anonymisointi tapahtuu, sen on tapahduttava peruuttamattomasti jonka jälkeen tietoa ei luokitella enää henkilötiedoksi. Jos henkilötiedot ovat anonymisoitu, salattu tai pseudonymisoitu, mutta tietoja apuna käyttäen henkilö on jollain tapaa tunnistettavissa, tiedot luokitellaan edelleen henkilötiedoiksi ja ne kuuluvat yleisen tietosuoja-asetuksen soveltamisalaan. (Euroopan komissio 2020b.)

2.4.2 Tietosuojaperiaatteet

Henkilötietojen käsittelyssä on aina noudatettava yleisiä henkilötietoja koskevia periaatteita. Rekisterinpitäjän tulee pystyä osoittamaan, että kaikki tietosuojaperiaatteet toteutuvat tehokkaasti tietojen käsittelyn aikana. Tietosuoja-asetuksen tietosuojaperiaatteet ovat (Tietosuojavaltuutetun toimisto 2020d.):

a) lainmukaisuus, kohtuullisuus ja läpinäkyvyys
b) käyttötarkoitussidonnaisuus
c) tietojen minimointi
d) täsmällisyys
e) säilytyksen rajoittaminen
f) luottamuksellisuus ja turvallisuus

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Käsittelyn tulee olla edellä mainittujen asioiden lisäksi myös muilla tavoin lainmukaista. Käsittelyn yhteydessä on varmistettava kaikkien tietosuojaperiaatteiden ja muiden käsittelyä koskevien vaatimusten asianmukainen toteutuminen. Seuraavaksi perehdytään tarkemmin jokaiseen tietosuojaperiaatteeseen ja käydään läpi niihin kuuluvat yksityiskohdat. (Tietosuojavaltuutetun toimisto 2020d.)

Henkilötietojen käsittelyn tulee olla asianmukaista ja kohtuullista suhteessa käsittelyn tarkoitukseen. Käsittely pitää esittää ymmärrettävällä tavalla, eikä henkilötietojen käsittelystä kertova tieto saa olla harhaanjohtavaa. Henkilötietojen käsittelyä ei saa peitellä, käsittelystä ei saa antaa tietoa valikoivasti rekisteröityä manipuloivalla tavalla, eikä käsittely saa olla ennalta arvaamatonta ja odottamatonta rekisteröidyn kannalta. Rekisterinpitäjän tulee arvioida millaisia vaikutuksia henkilötietojen käsittely saattaa aiheuttaa rekisteröidylle. Käsittely ei saa aiheuttaa enempää haittaa kuin on käsittelyn kannalta välttämätöntä. (Tietosuojavaltuutetun toimisto 2020d.)

Läpinäkyvällä henkilötietojen käsittelyllä pyritään varmistamaan yhdenmukainen henkilötietojen suoja koko Euroopan unionin alueella. Henkilötietojen käsittelyssä on kerrottava tarkasti, mihin tarkoitukseen tietoja kerätään, mihin tietoja käytetään ja mihin tiedot tullaan mahdollisesti siirtämään. Tiedot tulee olla esitettynä tiiviisti, helposti ymmärrettävissä ja saatavilla olevassa muodossa. Läpinäkyvä henkilötietojen käsittely

tarkoittaa myös rekisterinpitäjän valmiutta toimittaa rerkisteröityä koskevat tiedot, tiiviisti selkeällä ja yksinkertaisella kielellä mikäli rekisteröity tätä pyytää. (Björk, R. 2018)

Käyttötarkoitussidonnaisuus

Käyttötarkoitussidonnaisuus tarkoittaa selkeästi suunniteltavaa ja määriteltävää henkilötietojen käsittelyä ennen käsittelyn aloittamista. Henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa myöhemmin käsitellä alkuperäiseen tarkoitukseen yhteensopimattomalla tavalla. Käyttötarkoituksen määritteleminen auttaa rekisteröityä ymmärtämään tietojen käsittelyn tarpeellisuuden, arvioimaan käyttötarkoituksen asianmukaisuutta ja päättämään, haluaako rekisteröity vaikuttaa omien tietojensa käsittelyyn. Tietojen käsittelyn rajaaminen auttaa lainmukaisuuden, asianmukaisuuden ja läpinäkyvyyden periaatteiden noudattamista. (Tietosuojavaltuutetun toimisto 2020e.)

Henkilötietojen käsittely on mahdollista tietyn käyttötarkoituksen ohella sellaiseen käyttötarkoitukseen, joka katsotaan yhteensopivaksi alkuperäisen käyttötarkoituksen kanssa. Vaikka käyttötarkoitus olisi sopiva alkuperäisen tarkoituksen kanssa, rekisterinpitäjän ei tule poiketa muista tietosuojasäännöksistä. Jos tietosuoja-asetuksen suojatoimia noudatetaan asianmukaisesti, henkilötietojen käsittely on yhteensopivaa jos käsittely on tilastollista tarkoitusta, tieteellistä tai historiallista tutkimusta tai yleisen edun mukaista arkistointia varten. (Tietosuojavaltuutetun toimisto 2020e.)

Rekisterinpitäjä voi myös arvioida sitä, olisiko henkilötietojen käsittely uuteen tarkoitukseen yhteensopivaa alkuperäisen tarkoituksen kanssa. Tässä tapauksessa rekisterinpitäjän tulee arvioida (Tietosuojavaltuutetun toimisto 2020e.):

- henkilötietojen keruun tarkoitusten ja myöhemmän käsittelyn tarkoitusten väliset yhteydet
- henkilötiedon keruun asiayhteys rekisterinpitäjän ja rekisteröidyn osalta
- henkilötietojen luonne
- myöhemmän käsittelyn mahdolliset seuraukset
- asianmukaisten suojatoimien olemassaolo.

Jotta henkilötietojen lainmukaisuus ja asianmukaisuus tulee varmistettua, on yleensä tarpeellista laatia uusi suostumus myös yhteensopivien käyttötarkoitusten osalta. Henkilötietojen käsittely alkuperäisestä poikkeavaan käyttötarkoitukseen on mahdollista

jos rekisteripitäjä noudattaa tietosuojasäännöksiä, uuteen tarkoitukseen saadaan rekisteröidyn suostumus ja käsittelylle on selkeä käsittelyperuste. (Tietosuojavaltuutetun toimisto 2020e.)

Tietojen minimointi

Henkilötietojen tulee olla riittäviä, mutta toisaalta rajoituttava siihen, mikä on välttämätöntä tietojen käsittelyn tarkoituksen osalta. Henkilötietojen tulee olla asianmukaisia ja olennaisia sekä niiden on oltava tarpeellisia määritellyn henkilötietojen käyttötarkoitusten kannalta. Rekisterinpitäjän on suositeltavaa tarkastaa, onko kaikki yrityksen keräämä tieto varmasti tarpeellista kyseiseen käyttötarkoitukseen. Esimerkiksi työnhakijalta voidaan kerätä vain työntekijän valinnan kannalta tarpeellista tietoa. Vaikka henkilötietoja voidaan kerätä henkilön suostumuksen perusteella, ei se oikeuta rekisteröityä käsittelemään henkilötietoja tarpeettomasti. Kaiken tiedon tulee olla tarpeellista tiettyyn käyttötarkoitukseen perustuvaa ja siksi rekisterinpitäjän on tärkeää muistaa, että tiedon kerääminen tulevaisuutta varten on tietosuojalainsäädännön vastaista ja kaiken kerättävän tiedon tarpeellisuus on määriteltävä jo ennen käsittelyä. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 49.)

Täsmällisyys

Henkilötietojen pitää olla täsmällisiä ja niitä on päivitettävä tarpeen vaatiessa. Yrityksen on toteutettava kaikki kohtuulliset toimenpiteet jotta mahdolliset virheelliset henkilötiedot oikaistaan tai poistetaan viipymättä. Rekisterinpitäjän tulee varmistaa keräämiensä henkilötietojen laatu ja tarkistaa aika ajoin henkilötietojen virheettömyys. (Hanninen ym. 2017, 50.)

Mitä tärkeämpää tieto on, sitä enemmän tulee tehdä toimenpiteitä tiedon oikeellisuuden varmistamiseksi. Rekisteröidyllä on oikeus arvioida rekisterinpitäjän käyttämiä henkilötietoja ja tarvittaessa esittää oikaisupyyntöjä mahdollisten virheellisten tietojen korjaamiseksi tai tarpeettomien tietojen poistamiseksi. Siksi on tärkeää, että rekisterinpitäjällä on osaamista ja käytössään menetelmiä tiedon täsmällisyyden ja oikeellisuuden säännölliseen arviointiin sekä mahdollisten tietojen päivitysten tekemiseen. Mikäli rekisterinpitäjä luovuttaa hallussaan olevia henkilötietoja eteenpäin, on tietojen vastaanottajista pidettävä kirjaa. Rekisterinpitäjällä on velvollisuus ilmoittaa henkilötietojen muutoksista kaikille vastaanottajille, joille henkilötietoja on luovutettu. Mikäli tietojen ilmoittamisen todetaan mahdottomaksi tai siitä koituu kohtuutonta vaivaa rekisterinpitäjälle, on tietojen oikaisusta mahdollista luopua. Rekisteröidyllä on oikeus

saada tieto jokaisesta vastaanottajasta, joka on saanut haltuunsa hänen henkilötietonsa. (Tietosuoja 2020.)

Säilytyksen rajoittaminen

Henkilötietoja saa säilyttää ainoastaan niin kauan kuin on tarpeellista käsittelyn tarkoituksen toteuttamista varten. Rekisterinpitäjällä on vastuuna tarkastaa määräajoin, onko henkilötietojen säilyttäminen edelleen tarpeellista vai olisiko jo aika poistaa tarpeettomat tiedot. Tietojen säilytysajan tulee olla mahdollisimman lyhyt. Yritykset kuitenkin käsittelevät paljon henkilötietoja, jotka on tarpeellista säilyttää pidemmän aikaa. Asiakassuhteen päättymisen jälkeen on tarpeellista miettiä kuinka kauan ja mitä tietoja on tarpeellista säilyttää esimerkiksi laskutuksen, perinnän, oikeudellisten toimenpiteiden, reklamaation tai takuun vuoksi. Tietoja on myös mahdollista säilyttää tarpeellista kauemmin, mikäli henkilötiedot säilytetään sellaisessa muodossa, josta rekisteröityä ei voi enää tunnistaa. Näin voi olla tarpeen esimerkiksi tilastollisten tutkimuksien vuoksi. Mikäli henkilötietoja päätetään säilyttää tarpeellista kauemmin, on syytä olla varma, ettei ketään luonnollista henkilöä pystytä yhdistämään kyseiseen tietoon. (Hanninen ym. 2017, 50.)

Luottamuksellisuus ja turvallisuus

Kaiken henkilötiedon käsittelyn tulee olla luottamuksellista ja turvallista. Mahdolliset riskit, tietosuoja- ja tietoturvaohjeistuksen taso sekä henkilötietojen suojaus on rekisterinpitäjän vastuulla. Suojausten riittävyyttä ja toimivuutta on punnittava suhteessa olosuhteisiin ja riskeihin. Henkilötietoja tulee suojata lainvastaiselta ja luvattomalta käsittelyltä, sekä vahingossa tapahtuvalta vahingoittumiselta, hävittämiseltä, tai tuhoutumiselta. Henkilötietoja on suojattava kaikissa käsittelytoimissa, ja on varmistettava, että tietojen suojaus pysyy varmana koko henkilötiedon elinkaaren ajan. (Tietosuojavaltuutetun toimisto 2020g.)

2.4.3 Henkilötietojen käsittelyn oikeusperusteet

Henkilötietojen käsittely on lainmukaista vain jos jokin seuraavista kuudesta eri käsittelyperusteesta täyttyy (Digiturvamalli 2017b):

1. ”rekisteröity on antanut **suostumuksensa** yhtä tai useampaa tarkoitusta varten;”

2. ”käsittely on tarpeen sellaisen **sopimuksen** täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;”
3. ”käsittely on tarpeen rekisteröidyn **lakisääteisen velvoitteen noudattamiseksi**;”
4. ”käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön **elintärkeiden etujen suojaamiseksi**;”
5. ”käsittely on tarpeen **yleistä etua** koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan **julkisen vallan käyttämiseksi**;”
6. ”käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen **oikeutettujen etujen toteuttamiseksi**, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet -ja vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.”

Suostumus

Suostumuksen on oltava vapaaehtoinen, tietoinen, yksilöity ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Rekisteröity voi myös antaa kirjallisen tai suullisen suostumusta koskevan lausunnon, tai ilmaista suostumuksena jollain muulla selkeällä tavalla. Suostumus edellyttää aktiivista toimintaa, joka voi olla esimerkiksi ruudun rastittaminen internetsivulla tai kirjallisen suostumuslomakkeen täyttäminen ja allekirjoittaminen. Jotta suostumus on pätevä, rekisteröidyn täytyy tietää, mikä taho hänen tietojaan käsittelee, mihin tarkoitukseen ja kuinka pitkälle menevästä käsittelystä on kyse. Hanninen ym. 2017, 35 - 38.)

Mikäli henkilötietoja käsitellään eri tarkoituksiin, mutta henkilöllä ei ole mahdollisuutta antaa erillistä suostumusta eri henkilötietojen käsittelytarkoituksille, suostumusta ei katsota vapaaehtoiseksi. Vapaaehtoisuus tarkoittaa myös rekisteröidyn tosiasiallista mahdollisuutta kieltäytyä suostumuksen antamisesta ilman, että siitä aiheutuu hänelle haittaa. Mikäli suostumusta pyydetään samassa yhteydessä muiden tietojen kanssa, tulee suostumuksen olla selkeästi ilmaistu ja selvästi erillään muista asioista. Rekisterinpitäjän tulee pystyä osoittamaan kuka on antanut suostumuksen, miten rekisteröityä on informoitu ja milloin suostumus on annettu. (Hanninen ym. 2017, 35 - 38.)

Sopimus

Rekisterinpitäjä ja henkilötietojen käsittelijä sopivat, miten käsittelijä suojaa rekisterinpitäjän sille luovuttamat henkilötiedot. Sopimusta voidaan nimittää sopimusta henkilötietojen käsittelystä, tietosuojasopimukseksi, tietojenkäsittelysopimukseksi, GDPR-sopimukseksi tai DPA:ksi (Data Processing Agreement). Sopimus tulee laatia jos yritys/organisaatio aikoo käsitellä joko yksilöltä tai toiselta yritykseltä saamia henkilötietoja. Sopimuksessa tulee määritellä henkilötietojen käyttötarkoitus, kohde, kesto, luonne, henkilötiedon tyyppi, rekisteröityjen ryhmät ja rekisterinpitäjän oikeudet ja velvollisuudet. (Sopimustieto 2020.)

Sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi *rekisteröidyn pyynnöstä* voi soveltua tilanteeseen, jossa esimerkiksi asiakasyritys pyytää toista yritystä lähettämään tarjouksen palvelustaan tai tuotteestaan. Kyseiseen tarkoitukseen liittyvä tietojen käsittely, kuten tarjouspyynnössä olevan tiedon säilyttäminen tietyn ajan, on oikeudellisen perusteen nojalla asianmukaista. Tietosuojaryhmä WP29 on todennut henkilötietojen käsittelyn sopimuksen täytäntöönpanemiseksi soveltuvan myös työsuhteeseen, jossa työnantaja käsittelee rekisteröidyn henkilötietoja työsopimuksen täytäntöön panemiseksi. Myös palkka- ja tilitietojen käsittely on tällä perusteella lainmukaista mikäli käsittelijänä toimii vain kyseisiin toimenpiteisiin luvan saanut henkilö, kuten palkanlaskija. (Hanninen ym. 2017, 30.)

Lakisääteinen velvoite

Rekisterinpitäjän lakisääteisten velvoitteiden noudattaminen voi antaa tälle valtuudet käsitellä henkilötietoja. Velvoite voi koskea niin yksityisen kuin julkisen sektorin rekisterinpitäjää. Lakisääteisen velvoitteen noudattaminen on kyseessä esimerkiksi silloin, kun työnantaja ilmoittaa työntekijöidensä palkkatiedot veroviranomaisille. (Tietosuojavaltuutetun toimisto 2020g.) Myös osakeyhtiön on osakeyhtiölain mukaisesti pidettävä yllä osakas- ja jäsenluetteloa, jolloin lakisääteinen velvoite henkilötietojen käsittelyyn toimii lainmukaisena perusteena. (Hanninen ym. 2017, 31.)

Elintärkeiden etujen suojaaminen

Jos henkilötietojen käsittely on tarpeellista rekisteröidyn tai jonkun toisen henkilön elintärkeiden etujen suojaamiseksi, on se lakisääteisesti sallittua. Elintärkeiden etujen suojaaminen voi sopia käsittelyperusteeksi tilanteissa, joissa kyse on elämästä ja kuolemasta, tai muista uhkista, jotka saattavat johtaa rekisteröidyn tai kolmannen osapuolen henkilön loukkaantumiseen tai terveyden vaarantamiseen. (Tietosuojavaltuutetun toimisto 2020g.)

Yleinen etu tai julkisen vallan käyttö

Henkilötietojen käsittely on sallittua, mikäli se on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi. Se mahdollistaa käsittelyn, joka on tarpeen viranomaisen tehtävien ja toimivallan kannalta. Mikäli tieteellinen tai historiallinen tutkimus taikka tilastointi vaatii henkilötietojen käsittelyä, voi yleistä etua käyttää käsittelyperusteena. (Korpisaari, Pitkänen, Warma-Lehtinen 2018, 251.) Yleistä etua tai julkista valtaa koskeva käsittelyperuste on täytynyt antaa lailla tai muilla oikeudellisilla säännöksillä. Tämä voi toimia perusteena sekä yksityisellä kuin julkisella sektorilla tilanteissa, jossa henkilötietojen käsittely koskee Euroopan unionin tai sen jäsenvaltion yleistä etua tai julkista valtaa. (Tietosuojavaltuutetun toimisto 2020g.)

Rekisterinpitäjän oikeutettu etu

Mikäli yrityksellä on tarve käsitellä henkilötietoja liiketoimintansa suorittamiseen, voidaan käsittelyperusteena käyttää rekisterinpitäjän oikeutettua etua. (Euroopan komissio 2020c.) Oikeutettu etu voi olla olemassa silloin, kun rekisteröidyn ja rekisterinpitäjän välillä on jokin merkityksellinen ja asianmukainen suhde, kuten esimerkiksi työntekijän ja työnantajan välinen työsuhde. Oikeutettu etu käsittelyperusteena kuitenkin edellyttää rekisteröidyn etujen ja oikeuksien erityisen tarkkaa huomioimista. Pitää kuitenkin muistaa, ettei oikeutettua etua käsittelyperusteena saa käyttää, mikäli se syrjäyttää rekisteröidyn oikeudet ja edut. Rekisterinpitäjän on tarkkaan huomioitava ja arvioitava, voiko oikeutettua etua käyttää perusteena. Arvioinnissa voi käyttää apuna niin kutsuttua tasapainotestiä, jossa oikeutetun edun käytön riskejä ja haittoja verrataan rekisteröidyn ja rekisterinpitäjän välillä. (Hanninen ym. 2017, 32 - 33.)

2.4.4 Erityiset henkilötietoryhmät

Tietyt henkilötiedot voivat olla erityisen riskialttiita ihmisen yksityisyyden kannalta. Tietosuoja-asetuksessa näitä kutsutaan nimellä erityiset henkilötietoryhmät, ja niihin liittyvien henkilötietojen käsittely on lähtökohtaisesti kiellettyä. Erityisten henkilötietojen käsittely on sallittua journalistisiin tarkoituksiin, taikka akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten. Riskiperusteisen lähestymistavan mukaisesti näiden tietoryhmien käsittelyssä tulee noudattaa tietosuoja-asetuksessa määritettyjä asianmukaisia suojatoimia. Esimerkiksi luonnollisen henkilön geneettinen tai biometrinen tieto, jota käsitellään henkilön yksiselitteistä tunnistamista varten, katsotaan erityiseksi henkilötiedoksi, ja siksi kyseiset tiedot ovat lähtökohtaisesti käsittelykiellon alaisia. Rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta kuvaava tieto ei katsota kuuluvan erityisiin henkilötietoryhmiin. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 148.)

Tieto lasketaan erityiseksi henkilötietoryhmäksi, mikäli se koskee jotakin näistä seuraavista (Tietosuojavaltuutetun toimisto 2020h):

- rotu tai etninen alkuperä
- poliittinen mielipide
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- terveyttä koskeva tieto
- seksuaalinen suuntautuminen tai käyttäytyminen
- geneettinen tai biometrinen tieto henkilön tunnistamista varten

Mikäli kieltoon on säädetty poikkeus tietosuoja-asetuksessa tai erikseen euroopan unionin oikeudessa tai kansallisessa lainsäädännössä, on erityisten henkilötietojen käsittely laillista. Erityisten henkilötietoryhmien käsittely pelkästään tietosuoja-asetuksen perusteella on mahdollista jos jokin seuraavista tapauksista käy toteen (Tietosuojavaltuutetun toimisto 2020h.):

- Rekisteröity on antanut nimenomaisen **suostumuksen** hänen henkilötietojensa käsittelylle.

- Jos rekisteröity on juridisesti tai fyysisesti **estynyt** antamaan suostumusta ja käsittely on tarpeen rekisteröidyn tai jonkun toisen henkilön **elintärkeiden etujen suojaamiseksi.**

- Käsittely koskee henkilötietoja, jotka rekisteröity on **nimenomaisesti saattanut julkisiksi.**

- Käsittely liittyy **poliittiseen, filosofiseen, uskonnolliseen tai ammattiliittotoiminnalliseen yhdistykseen**, tai muuhun voittoa tavoittelemattomaan yhteisöön ja sen lailliseen toimintaan. Käsittelyn tulee koskea vain yhteisön nykyisiä tai entisiä jäseniä, tai henkilöitä joilla on yhteisöön liittyvät säännölliset yhteydet. Tiedot ovat suojattava asianmukaisesti ja niitä ei saa jakaa yhteisön ulkopuolelle ilman rekisteröityjen suostumusta.

- Käsittely on tarpeen **oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi**. Käsittely on myös lainmukaista, jos se koskee tuomioistuimen lainkäyttötehtäviä.

Seuraavaksi esitetään tapauksia, joissa erityisten henkilötietojen käsittely suoraan tietosuojalainsäädännön perusteella ei ole mahdollista, vaan käsittely edellyttää tarkentavaa sääntelyä tai muuta menettelyä. (Tietosuojavaltuutetun toimisto 2020h.):

- Käsittely tehdään rekisteröidyn tai rekisterinpitäjän **velvoitteiden ja erityisten oikeuksien noudattamiseksi työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla** siltä osin, kuin se on sallittu unionin oikeudessa tai unionin jäsenvaltion lainsäädännössä tai työehtosopimuksessa.

- Käsittely koskee **tärkeää yleistä etua** unionin oikeuden tai jäsenvaltion lainsäädännön ohella. Käsittelyn sääntelyn tulee olla oikeassa suhteessa käsittelyn tavoitteisiin nähden, ja siinä tulee noudattaa keskeisiltä osin rekisteröidyn oikeutta henkilötietojensa suojaan. Samassa yhteydessä on säädettävä rekisteröidyn etujen ja oikeuksien suojaamista vaativat toimenpiteet.

- Käsittely koskee Euroopan Unionin oikeuden, jäsenvaltion tai terveydenhuollon ammattilaisen kanssa tehdyn sopimuksen mukaisesti **ennaltaehkäisevää terveydenhuoltoa, työterveydenhuoltoa, työkyvyn arviointia, lääketieteellistä diagnoosia, terveys- tai sosiaalihuollollista hoitoa tai terveys- tai sosiaalihuollon palvelujen ja järjestelmien hallintoa.**

- Käsittely koskee **kansanterveyteen liittyvää yleistä etua** sellaisen unionin oikeuden tai jäsenvaltion lainsäädännön perusteella, joissa säädetään rekisteröidyn oikeuksia ja vapauksia suojaavista toimenpiteistä, erityisesti salassapitovelvollisuudesta.

- Käsittely koskee tietosuoja-asetuksen mukaisesti unionin oikeuden tai jäsenvaltion lainsäädännön nojalla **yleisen edun mukaista arkistointia, tieteellistä ja historiallista tutkimusta tai tilastointia.** Käsittelyn tulee noudattaa keskeisiltä osin rekisteröidyn oikeutta henkilötietojensa suojaan, ja käsittelyn mahdollistavan sääntelyn tulee olla oikeassa suhteessa käsittelyn tavoitteisiin nähden. Käsittelyä varten on myös säädettävä rekisteröidyn oikeuksien ja etujen suojaamista vaativista toimenpiteistä.

Erityisiä henkilötietoja tulee suojella erityisen tarkkaan, koska niiden käsittely voi aiheuttaa huomattavia riskejä rekisteröidyn perusoikeuksille ja vapauksille. Rekisterinpitäjän on hyvin tärkeä tunnistaa ja arvioida, voiko kyseisiä tietoja tarkastella ainoastaan tietosuojalainsäädännön perusteella, vai vaatiiko käsittely asetuksen lisäksi vielä erityistä lainsäädäntöä tai sopimusmenettelyä. (Tietosuojavaltuutetun toimisto 2020h.)

Rekisteröity voi suostumuksen perusteella antaa nimenomaisen suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa tarkoitusta varten. On olemassa

kuitenkin poikkeustilanne, jossa lainsäädännössä säädetään, että kieltoa käsitellä arkaluonteista tietoa ei voida kumota rekisteröidyn suostumuksella. Laissa on säädetty, että suostumuksesta riippumatta työnantaja saa käsitellä vain ja ainoastaan välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen, työnantajan työntekijälle tarjoamiin etuuksiin taikka työntekijän työtehtävän erityisluonteeseen. Työnantaja ei siis edes työntekijän erityisellä suostumuksella saa käsitellä työntekijän arkaluonteisia tietoja kuten esimerkiksi työntekijän etnistä alkuperää, mikäli tämä ei ole työsuhteen kannalta välttämätöntä. Yritys rekisterinpitäjänä on kuitenkin oikeutettu käsittelemään tietoa työntekijän ammattiliittoon kuulumisesta jos esimerkiksi tarvitsee selvittää, ketkä kuuluvat työtaistelutoimien piiriin, määrittää soveltuva työehtosopimus tai tilittää ammattiliiton jäsenmaksu. (Hanninen ym. 2017, 40 - 43.)

Työnantajalla on oikeus käsitellä työntekijän terveydentilaan koskevia tietoja, mikäli työntekijä on kirjallisella suostumuksellaan antanut siihen luvan taikka henkilökohtaisesti kyseiset tiedot luovuttanut. Kuitenkin terveydentilaa koskevia tietoja saa yrityksessä käsitellä ainoastaan ne henkilöt, jotka terveydentilatietojen perusteella valmistelevat ja toimeenpanevat työsuhdetta koskevia päätöksiä. Yleisesti nämä henkilöt ovat työntekijän lähiesimiehiä tai henkilöstöhallinnon työntekijöitä. Työntekijän terveydentilaa koskevista tiedoista ei tule ilmaista sivullisille työsuhteen aikana eikä edes sen päättymisen jälkeen. Työnantaja saa kuitenkin rekisteröidyn suostumuksella luovuttaa työntekijän työkykyä koskevan lääkärintodistuksen työterveyshuollolle. Rekisterinpitäjän on myös tärkeä tietää, että työntekijöiden terveydentilaa koskevia henkilötietoja tulee säilyttää erillään muista työnantajan keräämistä henkilötiedoista. (Hanninen ym. 2017, 40 - 43.)

2.4.5 Automaattinen päätöksenteko ja profilointi

Henkilötietojen automattista käsittelyä, jossa ihmisen henkilökohtaisia ominaisuuksia arvoidaan, kutsutaan **profiloinniksi**. Profiloinnissa yleensä arvioidaan henkilötietoja hyödyntämällä esimerkiksi luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, käyttäytymiseen, ja sijaintiin liittyviä ominaisuuksia. (Hanninen ym. 2017, 21.)

Profilointi on joko automaattista tai osittain automaattista yksittäisen henkilön tai ihmisryhmän tiedon keräämistä, heidän piirteiden ja käyttäytymismalliensa arvioimista

tiettyyn kategoriaan tai ryhmään sijoittamisen tarkoituksessa. Yleensä profiloinnissa arvoidaan henkilöiden kykyä suoriutua jostain tietystä tehtävästä, heidän mielenkiinnon kohteita ja todennäköistä käyttäytymistä. (Tietosuojavaltuutetun toimisto 2020i.)

Profilointia saattaa olla vaikea hahmoittaa sekä havaita sillä esimerkiksi yrityksen asiakkaiden luokittelu iän ja sukupuolen perusteella tilastollisia tarkoituksia varten ei lasketa profiloinniksi. Tarkoituksena on saada kokonaiskuva asiakkaista tekemättä johtopäätöksiä yksittäisistä henkilöistä. Käsittelyn tarkoituksena ei siis ole yksittäisten asiakkaiden henkilökohtaisten ominaisuuksien arviointi. (Tietosuojavaltuutetun toimisto 2020i.)

Mikäli henkilötietojen käsittelyyn perustuva päätöksenteko on täysin automaattista, se aiheuttaa rekisteröityyn kohdistuvia oikeusvaikutuksia tai muita huomattavia vaikutuksia, on kyseessä **automaattinen päätöksenteko**. Automaattinen päätöksenteko voi sisältää minkälaista tietoa tahansa. Tieto voi olla henkilön itsensä antamaa tai esimerkiksi havainnoinnilla kerättyä. Henkilötietojen käsittely voi olla automaattista ilman profilointia, ja toisin päin. Pelkästään automaattisesta päätöksenteosta on kyse silloin, kun henkilö ei itse osallistu päätöksen tekemiseen. Tästä esimerkkinä tilanne, jossa automaattisen prosessin ohella syntyy tiettyä henkilöä koskeva suositus. (Tietosuojavaltuutetun toimisto 2020i.)

Tietojen käsittely voi kuitenkin sisältää sekä profilointia, että automaattista päätöksentekoa riippuen siitä miten henkilötietoja käsitellään. Mikäli henkilö arvioisi ja ottaisi huomioon lopputulokseen vaikuttavia tekijöitä, ei päätöksenteko olisi pelkästään automaattista. Jotta henkilön voidaan katsoa vaikuttaneena päätöksentekoon ja lopputulokseen, osallistumisen tulee olla merkityksellistä, eikä vain näennäistä osallistumista. (Tietosuojavaltuutetun toimisto 2020i.)

Yksilöllä on lähtökohtaisesti oikeus olla joutumatta sellaisen päätöksenteon kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, ja sillä on häntä koskevia oikeusvaikutuksia tai muita merkittäviä vaikutuksia. Oikeusvaikutus voi syntyä esimerkiksi automaattisesta sopimuksen päättymisestä. Muu merkittävä vaikutus voi syntyä esimerkiksi luottohakemuksen automaattisessa hylkäämisessä tai sähköisen rekrytoinnin käytännöistä, johon henkilö ei ole itse vaikuttanut millään tavalla. Kohdennetun markkinointiviestinnän ei kuitenkaan katsota aiheuttavan oikeusvaikutuksia, vaikka kohteena olisikin tietty yksittäinen henkilö. (Korpisaari ym. 2018, 258.)

Oikeus olla joutumatta automatisoidun päätöksenteon kohteeksi ei koske sellaisia automatisoituja päätöksentekoprosesseja, jotka ovat osittain manuaalisia eli prosessin päätöksentekoon osallistuu ihminen ainakin jossain vaiheessa prosessin kulkua ennen kuin viimeinen päätös on annettu. Tilanteet, joissa automaattisella käsittelyllä on oikeusvaikutuksia tai muita merkittäviä vaikutuksia ovat hyvin tukinnanvaraisia. Yleisenä sääntönä on, että mikäli yritys tekee automaattisen päätöksenteon perusteella päätöksen siitä, tarjoaako se palveluita tai tuotteita rekisteröidylle ja millä ehdoilla se niitä tarjoaa, aiheuttaa päätöksenteko oikeusvaikutuksia tai muita merkittäviä vaikutuksia rekisteröidylle. (Hanninen ym. 2017, 69 - 70.)

Suoramarkkinoinnin kohdistamisella ja esimerkiksi tietyntyyppisten tarjousten tai tuotteiden tarjoamisella ei katsota olevan oikeusvaikutuksia kohteena olevalla rekisteröidylle. Kohdennettu markkinointi ja sen mahdolliset oikeusvaikutukset ovat kuitenkin joissain tilanteissa myös tulkinnanvaraisia. Tästä WP29-tietosuojaryhmän antama esimerkki, jossa yritys määrittelee profiloinnin perusteella kohdehenkilöt joille lähetetään automaattisesti suoramarkkinointia. Mikäli markkinointi koskee esimerkiksi uhkapelimainontaa, voi se aiheuttaa merkittäviä vaikutuksia taloudellisesti ahdingossa oleville henkilöille. (Hanninen ym. 2017, 69 - 70.)

Rekisteröidyllä on oikeus olla joutumatta pelkästään automaattisen käsittelyn kohteeksi. On kuitenkin lakisääteisiä poikkeustilanteita, jolloin automaattinen käsittely on lainmukaista. Jotta automaattinen päätöksenteko on sallittua, päätöksen tulee

- olla välttämätöntä rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemiseksi tai täytäntöönpanemiseksi

- olla hyväksytty rekisterinpitäjää sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä

- perustua rekisteröidyn antamaan suostumukseen

Mikäli jokin edellä mainituista ehdoista täyttyy ja automaattinen käsittely olisi lainmukaista, rekisterinpitäjän tulee aina huolehtia toimenpiteistä, joissa rekisteröidylle kerrotaan tietojen käsittelystä, tarjotaan yksinkertaisia tapoja esittää oma kantansa ja mahdollisuus riitauttaa päätös. Käsiteltäviä tietoja ja algoritmejä tulee myös tarkistaa

säännöllisesti, jotta voidaan varmistua päätöksentekoprosessin tarkoituksenmukaisuudesta. Rekisteröidylle on myös tarjottava mahdollisuutta vaatia ihmisen osallistumista tietojen käsittelyyn. (Tietosuojavaltuutetun toimisto 2020i.)

Jos henkilötietojen käsittelyssä on kyse automaattisesta päätöksenteosta, käsittelytoimien läpinäkyvyyteen tulee kiinnittää erityistä huomiota. Päätöksenteon kohteena oleville henkilöille on kerrottava tieto suoritettavasta automaattisesta päätöksenteoste, myös profiloinnista. Käsittelyn logiikkaan liittyvistä merkityksellisistä tiedoista on informoitava käsittelyn kohteina oleville henkilöille. Kyseisen automaattisen päätöksenteon aiheuttamista mahdollisista riskeistä ja seurauksista tulee ilmoittaa kohteena oleville ihmisille. Rekisteröidyille tulisi kertoa yksinkertaisella ja selvällä kielellä päätöksenteon toimintaperiaatteista ja siihen liittyvistä painotetuista tekijöistä. . (Tietosuojavaltuutetun toimisto 2020i.)

2.4.6 Tietosuojaloukkaus

Tapahtumaa, jossa henkilötietoja tuhoutuu, häviää, muuttuu, luovutetaan luvattomasti tai pääsee käsittelemään asiaankuulumaton taho, kutsutaan tietosuojaloukkaukseksi. Tietosuojaloukkaus on vakava tietoturvaan liittyvä vaara jonka estämiseen ja siihen varautumiseen tulee kiinnittää erityisen tarkkaa huomiota. (Minilex 2020d.)

Rekisterinpitäjä on velvollinen korvaamaan vahingon, joka on aiheutunut tietosuoja-asetuksen rikkomisesta. Laki on poikkeuksellinen ja vaatii erityistä huomiota ja toimenpiteitä rekisterinpitäjältä. Vahingonkorvausvastuu voi nimittäin syntyä ilman tahallisuutta tai moitittavaa huolimattomuutta. Rekisterinpitäjällä on niin kutsuttu *ankara vastuu,* josta vapautuminen ei ole mahdollista vaikka rekisterinpitäjä kykenisi osoittamaan toimineensa tilanteessa kaikin puolin huolellisesti. Vaikka henkilötiedot vuotaisivat ulkopuolisille inhimillisen erehdyksen tai tietokoneessa olevan viruksen toimesta, on vahingonkorvausvastuu silti rekisterinpitäjällä. Henkilötietojen käsittelijän vastuu tietosuojaloukkauksessa on toissijaista, joka tarkoittaa että henkilötietojen käsittelijä vastaa vahingoista vain silloin, jos se ei ole noudattanut tietosuoja-asetuksessa henkilötietojen käsittelijälle asetettuja velvoitteita, tai mikäli henkilötietojen käsittelijä on toiminut vastoin rekisterinpitäjän laillista ohjeistusta. (Minilex 2020d.)

Dokumentointi ja ilmoitusvelvollisuus

Tietosuojaloukkauksen tapahtuessa rekisterinpitäjän tulee dokumentoida kaikki loukkauksen kohteena olevat henkilötiedot, ja pystyttävä osoittamaan niiden vaikutukset ja korvaavat toimet. Dokumentaation avulla valvontaviranomainen voi tarkistaa että kyseistä artiklaa on noudatettu lainmukaisesti. Dokumentointi ja sen esittämiseen varautuminen on rekisterinpitäjän kannalta hyvin tärkeää, jotta mahdollisilta rahallisesti merkittäviltä seurauksilta vältytään. (Tietosuojaloukkaus 2020.)

Mikäli henkilötietojen tietosuojaloukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille tai vapauksille, tulee rekisterinpitäjän laatia ilmoitus valvontaviranomaisille ja rekisteröidyille. Suomessa valvontaviranomaisena toimii Tietosuojavaltuutetun toimisto. Loukkauksesta on ilmoitettava ilman aiheetonta viivystystä 72 tunnin kuluessa siitä, kun rekisterinpitäjä on saanut tiedon tai imoituksen tietosuojaloukkauksesta. Jos ilmoittaminen myöhästyy, on rekisterinpitäjän tehtävä kirjallinen selvitys myöhästymisen syystä. Jos henkilötietojen käsittelijä saa tiedon loukkauksesta ensimmäisenä, tulee hänen ilmoittaa siitä ensin rekisterinpitäjälle mikäli ei ole erikseen sovittu, että käsittelijä voi tehdä ilmoituksen suoraan valvontaviranomaisille. Vastuu ilmoittamisesta on joka tapauksessa rekisterinpitäjällä. (Tietosuojavaltuutetun toimisto 2020k.)

Rekisteröidylle tehtävä ilmoitus tietosuojaloukkauksesta on tehtävä viipymättä, jotta asianomainen saa mahdollisuuden varautua mahdollisiin toimenpiteisiin. Ilmoitukseen on sisällytettävä seuraavat asiat (Tietosuojavaltuutetun toimisto 2020k.):

- selkeä kuvaus tietoturvaloukkauksesta
- tietosuojavastaavan (mikäli yritys on sellaisen nimittänyt) nimi ja yhteystiedot, tai muu vastaava yhteyspiste lisätiedon saamiselle
- tietoturvaloukkauksen todennäköiset seuraukset
- rekisterinpitäjän ehdottamat tai toteuttamat toimenpiteet mahdollisten haittavaikutusten lieventämiseksi

Tietosuojaloukkauksesta ei tarvitse tehdä ilmoitusta mikäli rekisterinpitäjä on tehnyt tarvittavat teknologiset ja organisatoriset suojatoimenpiteet, joita sovelletaan tietoturvaloukkauksen kohteena oleviin henkilötietoihin. Esimerkkinä tilanne, jossa

loukkauksen kohteena olevat henkilötiedot on ehditty salata tai muokata niin, ettei niitä pystytä yhdistämään tiettyihin henkilöihin. Ilmoitusta ei myöskään tarvitse tehdä, mikäli jatkotoimenpiteillä on varmistettu, ettei tietosuojaloukkaus aiheuta rekisteröidyn vapauksiin ja oikeuksiin kohdistuvaa korkeaa riskiä. Jos tapahtuu tilanne, että rekisteröityjä henkilöitä ei pystytä tavoittamaan tai syystä tai toisesta ei tiedetä, keitä rekisteröidyt ovat, voi ilmoituksen tekeminen vaatia kohtuutonta vaivaa, jolloin sen tekeminen ei ole välttämätöntä. Ilmoituksen tekeminen ei ole yksiselitteistä, vaan se tulee aina arvioida riskien mukaan. Mikäli rekisteröityihin ei pystytä ottamaan henkilökohtaisesti yhteyttä, ilmoitus on tehtävä julkista tiedonantoa tai vastaavaa toimenpidettä käyttäen. (Tietosuojavaltuutetun toimisto 2020k.)

Tietoturvaloukkauksen riskien arviointi on tärkeä ja välttämätön toimenpide loukkauksen tapahduttua. Riskien arviointien perusteella tiedetään mahdollisten jatkotoimenpiteiden laajuus. Mitä arkaluontoisempaan tietoon loukkaus kohdistuu, sitä suurempi riski siitä aiheutuu rekisteröidylle. Rekisterinpitäjän tulee arvioida loukkauksen kohteina olevien henkilötietojen luonne, määrä ja arkaluonteisuus, sekä loukkauksesta aiheutuvat mahdolliset seuraukset. Mahdollisten seurauksien vakavuus määrittelee tietosuojaloukkauksen riskitason. (Tietosuojaloukkaus 2020.)

Tietosuojaloukkauksen seuraukset voivat olla erilaiset riippuen siitä ovatko henkilötiedot esimerkiksi vuotaneet internetiin, vai onko kyseessä tietojärjestelmävika. Siksi riskien arviointi on tärkeä tietosuojaloukkauksen edellyttämä toimenpide. Tärkeä osa arviontia on tieto siitä, liittyykö loukkaus yksittäiseen henkilötietoon vai isompaan tietotyyppien yhdistelmään. Mitä suurempi määrä tietoja on loukkauksen kohteena, sitä suuremmat riskit siitä aiheutuu. Riskien vakavuutta lisää myös se, jos loukkauksen kohteena olevat tiedot kohdistuvat lapsiin tai muihin haavoittuvammassa taikka heikommassa asemassa oleviin henkilöihin. (Tietosuojavaltuutetun toimisto 2020k.)

Arvionnissa on otettava huomioon, kuinka helposti henkilöt ovat tunnistettavissa loukkauksen kohteina olevista henkilötiedoista. Tunnistettavuuteen voi vaikuttaa esimerkiksi se, onko tiedot salattu tai pseydonymisoitu. Erityisen vakaviksi seurauksiksi katsotaan ne tietosuojaloukkaukset, joista voi aiheutua esimerkiksi identiteettivarkaus, petos, psyykkinen ahdistus, nöyryytys tai maineen menetys. Riskien vakavuuteen vaikuttaa myös se, kenen haltuun henkilötiedot ovat joutuneet. Henkilötietojen väärinkäytön katsotaan todennäköisesti olevan suurempi, jos tiedot ovat päätyneet rikollisille. (Tietosuojavaltuutetun toimisto 2020k.)

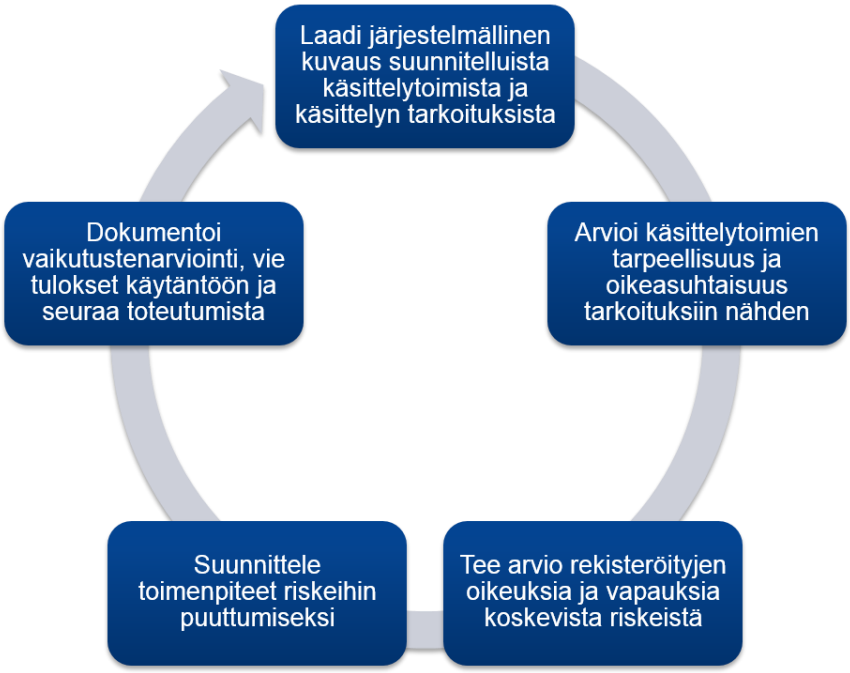
2.4.7 Vaikutustenarvionti

Vaikutustenarvionnilla tarkoitetaan prosessia, jossa tarkastellaan tietosuojan toteuttamiseksi suunniteltuja suojatoimia ja toimenpiteitä. Vaikutustenarvioinnin avulla lievennetään henkilötietojen käsittelystä rekisteröidylle aiheutuvia riskejä. Vaikutustenarvionti kuvaa henkilötietojen käsittelyä, ja arvioi käsittelyn tarpeellisuutta suhteessa riskeihin. Sen avulla pystytään varmistamaan, että henkilötietojen käsittelyssä on noudatettu tietosuoja-asetusta. (Hanninen ym. 2017, 115 – 116.)

Jos henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen aiheuttaa todennäköisen korkean riskin rekisteröidyn oikeuksille, on vaikutustenarvionnin tekeminen vaadittavaa. Rekisterinpitäjän tulee siis ensisijaisesti arvioida, onko vaikutustenarvioinnin tekeminen välttämätön toimenpide. Erityisesti vaikutustenarviointi tulee tehdä tilanteessa, jossa rekisteröityjen henkilökohtaisia ominaisuuksia arvioidaan automaattisen päätöksenteon yhteydessä, ja se voi aiheuttaa ihmisiä koskevia oikeusvaikutuksia tai muita merkittäviä vaikutuksia. (Hanninen ym. 2017, 115 – 116.) Vaikutustenarviointi vaaditaan myös tilanteissa, joissa kyseessä on laajamittainen henkilötietojen käsittely, joka kohdistuu erityisiin henkilötietoryhmiin, kuten henkilön terveydentilaa koskeviin tietoihin. Myös sellaisissa tapauksissa, joissa rekisterinpitäjä poikkeaa tietosuoja-asetuksen mukaisesta informoinnista ja kerää henkilötietoja muualta kuin rekisteröidyltä itseltään, on vaikutustenarvionnin tekeminen välttämätöntä. (Lexia 2018.)

Vaikutustenarvionnin tekeminen

Vaikutustenarvionti on suositeltavaa aloittaa mahdollisimman aikaisin käsittelyä suunniteltaessa ja se tulee laatia ennen kuin henkilötietoja käsitellään. Rekisterinpitäjän on aina tarpeen vaatiessa, eli käsittelytoimien riskien muuttuessa, tehtävä vaikutustenarvionti uudelleen. (Hanninen ym. 2017, 117 – 118.) Seuraavaksi tulen esittämään vaikutustenarvionnin tekemiseen hyödynnettävää prosessia ja sen vaiheita.



Kuva 2. Vaikutustenarvionnin prosessi (Tietosuojavaltuutetun toimisto 2020).

1. Ensimmäisessä vaiheessa on tärkeää laatia kuvaus tietojen käsittelyn luonteesta, laajuudesta, asiayhteydestä ja käsittelyn tarkoituksesta. On yksilöitävä rekisterinpitäjä ja mahdollinen henkilötietojen käsittelijä. Ensimmäisessä vaiheessa tulee käydä ilmi, miksi ja miten henkilötietoja tullaan käsittelemään. Kuvauksen tulee sisältää seuraavat tiedot:

    - mitä ja miten tietoa käsitellään
    - tarkoitukset, käyttötavat ja kuvaus käsittelyn toimenpiteistä
    - käsittelyyn käytettävät resurssit
    - henkilöt, joilla on pääsy tietoihin
    - tietojen säilytysaika
    - tietojen turvallinen hävitystapa

    On tärkeä ilmoittaa myös kuinka käsittelytoimenpiteet ja päätöksenteko dokumentoidaan. Jos käsittely perustuu rekisterinpitäjän oikeutettuun etuun, tulee tasapainotestin sisältyä kuvaukseen.

2. Seuraavaksi on tarpeen arvioida suunniteltua käsittelyä tietosuojaperiaatteen toteuttamisen kannalta. Rekisterinpitäjän tulee varmistaa, että käsittelylle on tietty, nimenomainen ja laillinen tarkoitus, ja että tietoja säilytetään vain niin kauan kuin se on tarpeen tietyn käyttötarkoituksen toteuttamiseksi. On suunniteltava toimenpiteet virheellisten henkilötietojen oikaisemiselle ja poistamiselle, ja varmistettava henkilötietojen suojaus teknisillä toimenpiteillä.

   Rekisterinpitäjän tulee huolehtia rekisteröidyn oikeuksia edistävistä toimenpiteistä. On huomioitava, että rekisteröityä on informoitu tarpeellisista asioista, ja että hänellä on pääsy omiin tietoihin, ja sitä kautta mahdollisuus tietojen poistamiseen, oikaisemiseen ja rajoittamiseen. Jos toteutetuista toimenpiteistä huolimatta käsittelystä koituu korkea riski, tulee laatia ennakkokuulemispyyntö tietosuojaviranomaisille.

3. Kolmantena vaiheena on tunnistaa käsittelyyn liittyvät riskit, joissa huomioidaan käsittelyn laajuus, luonne, asiayhteys, tarkoitukset ja riskin alkuperä. Riskien arvioinnin jälkeen voi siirtyä seuraavaan vaiheeseen, jossa arvioidaan ja suunnitellaan toimenpiteitä riskien vähentämiseksi.

   Riskien arvioinnissa on otettava huomioon rekisteröidyn oikeuksiin ja vapauksiin liittyvät riskit, uhkien tunnistaminen, riskin toteutumisesta aiheutuvat seuraukset sekä riskin todennäköisyys ja vakavuus. Henkilötietojen käsittelyyn liittyvät riskit liittyvät yleensä tietoturvaloukkaukseen, rekisterinpitäjän ratkaisuihin, työntekijöiden aiheuttamiin, ulkopuolisten luvattomaan henkilötietojen käsittelyyn, datankäsittelyyn- ja siirtoon, rikokseen tai yleisiin henkilötietojen käsittelyyn liittyviin riskeihin.

4. Neljännessä vaiheessa voidaan yksilöidä riskilähde jokaisen riskin osalta ja arvioida toimenpiteitä, joilla riskien toteutumisen todennäköisyyttä voidaan pienentää. Erilaisia keinoja voi olla muun muassa:

   - päätös olla käsittelemättä korkean riskin tietoja
   - käsittelyn täsmentäminen ja rajaaminen
   - lisäsuojatoimenpiteiden käyttöönotto tarvittaessa
   - tietojen anonymisointi tai pseydonymisointi

- tiedon säilytysaikojen lyhentäminen
- selkeiden sopimusten käyttöönotto
- tietosuojaoikeuksia tukevien järjestelmien ja menettelyiden käyttönotto

5. Viimeisessä vaiheessa dokumentoidaan käsittelyn edellä käsitellyt vaiheet ja perustellaan tehdyt valinnat ja toimenpiteet. Jokaisen riskin kohdalla on suositeltavaa kirjata ylös, mihin toimenpiteisiin ryhdytään riskin todennäköisyyden pienentämiseksi, ja arvioidaan onko riski kyseisillä toimenpiteillä vähennetty, hyväksytty vai poissuljettu. Rekisterinpitäjän tulee kuitenkin muistaa, että kaikkia käsittelyyn liittyviä yleisiä riskejä ei voida poissulkea.

   Jos toimenpiteiden käyttöönotosta huolimatta käsittelyyn liittyvä riski on korkea, eikä riskiä saada vähennettyä, rekisterinpitäjän tulee laatia ennakkokuulemispyyntö tietosuojaviranomaiselle. Kun käsittelyyn ryhdytään, on olennaista seurata valittujen toimenpiteiden riittävyyttä ja uudenlaisten riskien ja toimenpiteiden muuttumista. (Tietosuojavaltuutetun toimisto 2020l.)

2.4.8 Tasapainotesti

Jos henkilötietojen käsittelyssä rekisterinpitäjä vetoaa käsittelyperusteeksi oikeutetun edun, tulee arvioida, syrjäyttääkö rekisteröidyn edut rekisterinpitäjän tai muun kolmannen osapuolen edut. Tässä arvionnissa voi käyttää hyödyksi niin sanottua tasapainotestiä. Tasapainotestin kuvauksella voidaan myös toisaalta todentaa tietosuoja-asetuksen osoittamisvelvollisuutta. Seuraavaksi tulen esittämään tasapainotestin etenemisen käytännössä. (Iconics 2020):

a) Ensimmäisenä tulee arvioida onko oikeutettu etu käsittelyperusteena paras mahdollinen, vai onko mahdollisuus vedota johonkin toiseen perusteeseen.

b) Arvioidaan täyttyykö oikeutetun edun perusvaatimukset. Rekisterinpitäjän tulee pohtia onko etu lainmukainen, selkeästi ilmaistu ja todellinen ja välitön. Mikäli

kaikki edellä mainittujen kohtien vaatimukset täyttyvät, voi siirtyä seuraavaan vaiheeseen.

c) Arvioidaan, onko käsittely tarpeen edun saamiseksi. Mikäli etu voidaan saavuttaa ilman henkilötietojen käsittelyä, oikeutettua etua ei voi käyttää käsittelyperusteena.

d) Arvioidaan, syrjäyttääkö etu rekisteröidyn perusoikeudet ja -vapaudet. Rekisterinpitäjän tulee pohtia millaisesta rekisterinpitäjän edusta on kyse, millaista hyötyä edun käyttäminen käsittelyssä tuottaa ja minkälaiset haitat käsittelyn jättämisestä olisi.

   Tämän jälkeen tulee pohtia, millaisia vaikutuksia käsittely aiheuttaa rekisteröidylle. Tulee arvioida minkä luontoisista henkilötiedoista on kyse, miten tietoja käsiteltäisiin ja miten käsittelyn toimenpiteet vaikuttavat rekisteröityyn.

   Seuraavaksi tulee analysoida, osaisiko rekisteröity odottaa hänen henkilötietojansa käytettävän kyseisellä tavalla, onko todennäköistä että rekisteröity tulee vastustamaan tai kyseenalaistamaan tietojensa käsittelyä ja onko rekisteröidyn ja rekisterinpitäjän asemassa jotain erityistä esimerkiksi kuinka haavoittuvassa asemassa rekisteröity on.

e) Tässä kohtaa rekisterinpitäjän tulee varmistaa käsittelyyn liittyvät tietosuojan lisätakeet. Mahdollisina lisätakeina voi toimia tekniset tai organisatoriset toimenpiteet, joilla varmistetaan ettei henkilötietoja käytetä rekisteröityä koskeviin päätöksiin, anonymisointitekniikan käyttö, yksityisyyden suojaa parantavan tekniikan hyödyntäminen ja henkilötietojen salaus.

f) Viimeisessä vaiheessa tulee varmistaa toiminnan lainmukaisuus mahdollistamalla sen, että rekisteröity voi käyttää vastustamisoikeuttaan vapaasti. Tämän lisäksi tulee varmistua siitä, että käsittely on tarpeen huomattavan tärkeän ja perustellun syyn takia, joka syrjäyttää rekisteröidyn edun sekä varmistua siitä, että käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. (Tietosuojavaltuutetun toimisto 2020c).

3 HENKILÖTIETOJEN KÄSITTELYN OIKEUDET JA VELVOLLISUUDET

3.1 Rekisteröidyn oikeudet

Tietosuoja-asetuksessa säädetään yksityiskohtaisemmin rekisteröidyn oikeuksista. Seuraavaksi tullaan käsittelemään, mitä erilaisia oikeuksia rekisteröidyllä on.

Oikeus saada läpinäkyvää informointia käsittelystä

Tietosuoja-asetuksen mukaan rekisteröidyn tulee saada tieto siitä, miten häntä koskevia tietoja kerätään, mihin niitä käytetään ja missä määrin henkilötietoja tullaan käsittelemään. Tiedon on oltava tiiviisti esitettynä, läpinäkyvää, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä.

Kun rekisteröidyltä kerätään häntä koskevia tietoja, on rekisterinpitäjällä velvollisuus ilmoittaa mahdollisen tietosuojavastaavan yhteystiedot (jos yrityksessä ei ole tietosuojavastaavaa, on suositeltavaa antaa jonkun toisen henkilötietojen käsittelyyn luvan saaneen henkilön yhteystiedot), henkilötietojen vastaanottajien yhteystiedot (esimerkiksi yrityksen kanssa samaan konserniin kuuluva yhtiö), tapauksen mukaan tieto siitä, että henkilötietoja tullaan siirtämään kolmanteen maahan, rekisterinpitäjän oikeutetusta edusta (esimerkiksi työsuhde) ja henkilötietojen säilytysajasta. (Hanninen ym. 2017, 73.)

Oikeus saada pääsy tietoihin

Rekisteröidyn oikeus päästä tietoihin tarkoittaa, että rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus, mikäli häntä koskevia tietoja käsitellään, tai että niitä ei käsitellä. Jos henkilötietoja käsitellään ja rekisteröity pyytää siitä vahvistuksen, on vahvistukseen lisättävä jäljennös käsiteltävistä tiedoista. Tämän lisäksi on kerrottava seuraavat asiat (Digiturvamalli 2017c):

- käsittelyn tarkoitus;
- käsittelyssä kyseessä olevat henkilötietoryhmät;
- mahdolliset vastaanottajat, joille henkilötieto on luovutettu;
- tietojen säilytysaika tai ajan määrittämiskriteerit;

- rekisteröidyn oikeus pyytää tiedon poistamista, oikaisemista, vastustamista tai käsittelyn rajoittamista;
- oikeus tehdä valitus henkilötietoviranomaisille;
- tietojen keräyksen alkuperä (jos tietoja ei ole saatu rekisteröidyltä);
- mahdollinen automaattisen päätöksenteon olemassaolo.

Oikeus tietojen oikaisemiseen

Rekisteröidyllä on oikeus vaatia rekisterinpitäjää oikaisemaan häntä koskevat epätarkat ja virheelliset tiedot esimerkiksi toimittamalla lisäselvityksen tiedoista. Tässä kohtaa rekisterinpitäjän tulee kuitenkin huomioida, ettei rekisteröidyn historiaa koskevia tietoja ole pakollista muuttaa nykyhetken voimassa olevilla tiedoilla, vaikka rekisteröity sitä vaatii. (Hanninen ym. 2017, 81, 59 - 69.)

Oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää poistamaan häntä koskevat tiedot, eli tulla unohdetuksi seuraavissa tilanteissa:

- Henkilötietoja ei enää tarvita niihin tarkoituksiin, joihin ne kerättiin.
- Käsittely perustuu rekisteröidyn suostumukseen, ja rekisteröity päättää peruuttaa suostumuksen, eikä käsittelylle löydy enää muuta perustetta.
- Rekisteröity vastustaa käsittelyä tietosuoja-asetuksessa määritetyn vastustusoikeuden perusteella.
- Henkilötietoja on käsitelty vastoin tietosuoja-asetuksen periaatteita.
- Henkilötiedot on poistettava yrityksen lainsäädäntöön perustuvan velvoitteen noudattamiseksi

Edellä olevasta luettelosta käy ilmi, että rekisteröidyn oikeus tulla unohdetuksi on rajoitettu. Yrityksissä käsitellään monesti henkilötietoja rekisterinpitäjän oikeutetun edun perusteella, ja niin kauan kuin kyseinen peruste on voimassa, ei rekisteröidyllä ole oikeutta tulla unohdetuksi. (Hanninen ym. 2017, 81, 59 - 69.)

Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus tietojensä käsittelyn rajoittamiseen, mikäli jokin seuraavista ehdoista täyttyy (Hanninen ym. 2017, 81, 59 - 69):

- Rekisteröity kiistää tietojensa paikkansapitävyyden (käsittelyä rajoitetaan paikkansapitävyyden selvittämisen ajaksi).
- Käsittely on lainvastaista ja rekisteröity vaatii käytön rajoittamista tietojen poistamisen sijasta.
- Rekisterinpitäjä ei tarvitse enää henkilötietoja, mutta rekisteröity tarvitsee niitä oikeudellisiin toimenpiteisiin.
- Rekisteröidyn ja rekisterinpitäjän välillä on erimielisyys siitä, syrjäyttääkö rekisterinpitäjän oikeutetut perusteet rekisteröidyn perusteet.

Oikeus siirtää tiedot järjestelmästä toiseen

Oikeus tietojen siirtämiseen tarkoittaa sitä, että rekisteröidyllä on oikeus saada itseään koskevat rekisterinpitäjän käsittelemät henkilötiedot ja tallentaa ne itselleen henkilökohtaista käyttöä varten. Tämä tarkoittaa myös sitä, että rekisteröidyllä on oikeus saada häntä koskevat tiedot siirretyksi toiselle yritykselle tai muulle rekisterinpitäjälle jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa jos se on teknisesti mahdollista. Tietojen siirtämien järjestelmästä toiseen edellyttää, että tiedot perustuvat rekisteröidyn suostumukseen tai sopimukseen, ja tietojen käsittely suoritetaan automaattisesti. Tämä tarkoittaa sitä, ettei tietojen käsittely kata suurinta osaa paperiasiakirjoja, joten tiedot ovat helposti sähköisesti lähetettävissä. (Tietosuojatyöryhmä 2017.)

Vastustamisoikeus

Rekisteröidyllä on henkilökohtaisen erityisen tilanteen perusteella oikeus vastustaa häntä koskevien tietojen käsittelyä, joka perustuu rekisterinpitäjän oikeutettujen etujen toteuttamiseen. Tällöin tietojen käsittelyä ei saa jatkaa, ellei rekisterinpitäjä pysty osoittamaan käsittelylle olevan huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn oikeudet. Käsittelyä voidaan kuitenkin jatkaa jos se on tarpeen oikeusvateen laatimiseksi, esittämiseksi tai puolustamiseksi. Jos huomattavan tärkeää perustetta ja syytä ei löydy, tietojen käsittely tulee lopettaa rekisteröidyn näin pyytäessä. (Hanninen ym. 2017, 81, 59 - 69.)

Oikeus olla joutumatta automaattisen päätöksenteon kohteeksi

Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksenteon kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, ja jolla on häntä koskevia oikeusvaikutuksia tai muita merkittäviä vaikutuksia. (Hanninen ym. 2017, 81, 59 - 69.)

3.2 Rekisterinpitäjän velvollisuudet

Henkilötietojen käsittelyssä rekisterinpitäjän velvollisuuksiin liittyy paljon yksityiskohtaisia asioita, joita on tullut opinnäytetyön aikana esille. Tästä syystä tämä kappale tulee keskittymään vain rekisterinpitäjän osoitusvelvollisuuteen, eikä sisällä opinnäytetyössä aikaisemmin esitettyjä rekisterinpitäjän velvollisuuksia.

Rekisterinpitäjä on vastuussa siitä, että se toteuttaa kaikki tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja osoitetaan, että henkilötietojen käsittelyssä noudatetaan euroopan unionin yleisen tietosuoja-asetuksen vaatimuksia. Teknisiä ja organisatorisia toimenpiteitä voi olla esimerkiksi henkilöstön kouluttaminen, sisäiset ohjeistukset, tietojen salaus, salassapitosopimukset, käytön valvonta ja tekniset rajaukset. Sisäänrakennetun ja oletusarvoisen tietosuojan periaate edellyttää tietosuoja-asetuksen vaatimusten tunnistamista ja huomioimista jo ennen käsittelyn aloittamista. Tietosuoja-asetuksen riskiperusteisen lähestymistavan mukaan asetuksessa olevat konkreettiset toimenpiteet suhteutetaan rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Kaikki henkilötietojen käsittelyn lainmukaisuuteen liittyvät asiat ovat viime kädessä rekisterinpitäjän vastuulla. (Kuntaliitto 2017.)

Osoitusvelvollisuus

Henkilötietojen käsittelyn lainmukaisuuteen liittyy olennaisesti rekisterinpitäjän osoitusvelvollisuus. Osoitusvelvollisuus on keskeinen asia tietosuoja-asetuksessa, ja sen avulla rekisterinpitäjä pystyy osoittamaan, että yrityksen sisältämä henkilötietojen käsittely noudattaa tietosuojalainsäädäntöä. Tämä tulee kyseeseen esimerkiksi tietoturvaloukkauksen sattuessa, jolloin rekisterinpitäjä kykenee osoitusvelvollisuuden avulla näyttämään, että se on aktiivisesti pyrkinyt tunnistamaan tietosuojaan liittyviä riskejä, ja ottanut käyttöön tarvittavat toimenpiteet henkilötietojen suojaamiseksi. (Tietosuojavaltuutetun toimisto 2020m.)

Osoitusvelvollisuuden vaatimuksia on monenlaisia, ja niiden velvoittavuutta on arvioitava tapauskohtaisesti. Osoitusvelvollisuuden laajuus riippuu muun muassa siitä, kuinka paljon henkilöstöä yrityksessä on, kuinka paljon ja minkälaisia henkilötietoja yrityksessä

käsitellään. Seuraavaksi tulen esittämään etenkin yrityksen henkilöstöhallinnon kannalta oleellisimmat osoitusvelvollisuuden näyttöön liittyvät asiat (Tietosuojavaltuutetun toimisto 2020m.):

- Henkilötietojen käsittelyn yleinen kuvaus eli seloste käsittelytoimista.
- Yrityksen sisäänrakennettu tietosuojaperiaatteiden toteutuminen omassa toiminnassa.
- Mahdolliset laajemmat tietosuojaa koskevat toimintaperiaatteet.
- Informointikäytännöt. Esimerkiksi kuinka läpinäkyvää informointi on ja kuinka ymmärrettävää siihen liittyvä asiasisältö on.
- Käsittelyn oikeusperustetta koskevat arviot. Esimerkiksi dokumentti rekisteröidyn suostumuksesta, tai jos käsittelyperusteena käytetään rekisterinpitäjän oikeutettua etua, siihen liittyvä tasapainotesti.
- Yrityksen sisäinen ja ulkoinen ohjeistus kuten riskiarvioita koskeva dokumentaatio, henkilötietoja käsittelevien työntekijöiden ohjeistus ja sisäiset tarkastukset ja auditoinnit.
- Vaikutustenarviointia koskeva dokumentaatio.
- Tietoturvaloukkauksen dokumentaatio ja siihen liittyvä prosessi.
- Käsittelyyn liittyvät sopimukset.

Kuten edellä mainittiin, osoitusvelvollisuuden vaatimuksia on monenlaisia ja tilanteesta riippuen kaikki kohdat eivät välttämättä koske rekisterinpitäjän osoitusvelvollisuutta kyseisellä hetkellä. Siksi on suositeltavaa dokumentoida, miksi on päädytty kyseisten velvoitteiden noudattamiseen ja tiettyjen velvoitteiden noudattamatta jättämiseen. (Tietosuojavaltuutetun toimisto 2020m.)

4 GDPR TOIMEKSIANTAJA -YRITYKSESSÄ

4.1 Nykytilanteen kartoittaminen

Tässä osiossa kartoitetaan toimeksiantajayrityksen yleisen tietosuoja-asetuksen mukaisen toiminnan. Kartoitus tapahtuu yrityksen henkilötietojärjestelmiin tutustuen, ja kvalitatiivista haastattelua hyödyntäen. Ensimmäinen haastattelu käytiin Teamsin välityksellä yhdessä yrityksen henkilöstöpäällikön, talouspäällikön ja kirjanpitäjän välillä. Toinen haastattelu kohdennettiin yrityksen esimiehiin sähköpostia hyödyntäen. Tietosuoja-asetuksen laajuudesta johtuen, nykytilanteen kartoittaminen ei tule täydellisesti kattamaan kaikkia yrityksen noudattamia tietosuoja-asetukseen liittyviä yskityiskohtaisia toimenpiteitä tai lainmukaisuuksia. Tässä osiossa keskitytään siihen, mitä, miten ja missä henkilötietoja yrityksen sisällä käsitellään, ja tätä kautta luodaan kuva siitä, kuinka tietosuoja-asetuksen velvoittamia toimenpiteitä yrityksen sisällä noudatetaan. Toimeksiantaja korostaa yksilön oikeuksia ja vapauksia Tutkimusosion tarkoituksena on tutkia, että yrityksen tietojen käsittely toteutetaan tietosuoja-asetuksen periaatteita noudattaen.

4.1.1 Tietosuoja henkilötietojärjestelmissä

Toimeksiantajayrityksen henkilötietojärjestelmät sisältävät fyysisiä sekä sähköisiä kansioita ja dataa, joihin on valtuudet ainoastaan tietyillä yrityksen henkilöillä. Tästä syystä järjestelmiin tutustuminen tapahtui yhdessä yrityksen henkilöstöpäällikön kanssa. Järjestelmiä ollaan tarkasteltu vain päällisin puolin tietosuoja-asetusta noudattaen, ja tarkastelussa on käytetty hyväksi ainoastaan henkilöstöpäällikön sekä minun omia henkilötietojani.

Mfiles

Mfiles on tiedohallintajärjestelmä, joka tarjoaa älykkään tiedonhallinan ratkaisuja ja yhdistää eri järjestelmät ja niissä olevan liiketoimintatiedon. Toimeksiantajayrityksellä Mfiles on jokapäiväisessä käytössä, ja sitä hyödynnetään monenlaisiin työtehtäviin ja niihin liittyviin dokumentointeihin.

Henkilötietojen käsittelyssä Mfilesiä hyödynnetään esimerkiksi työntekijöiden erityisten henkilötietojen dokumentointiin ja säilytykseen. Mfilesissä yrityksellä on käytössään FIRASecure,- FIRAHR- ja FIRA Operations nimisiä kansioita, joissa säilytetään henkilötietoihin liittyvää dataa. FIRASecure voi sisältää myös erityisiin henkilötietoryhmiin luokiteltavaa työntekijöiden terveydentilaa koskevia tietoja, kuten sairauslomatodistuksia. Tietosuoja-asetuksen erityisten henkilötietoryhmien käsittelyn periaatteiden mukaisesti, tietoja säilytetään erillään muista tiedoista, ja näiden tietojen käsittely perustuu rekisterinpitäjän oikeutettuun etuun. Kyseiset tiedot dokumentoidaan ja säilötään FIRASecureen, johon on pääsy ainoastaan kyseisten tietojen käsittelyyn oikeutetuilla henkilöillä. FIRASecure sisältää myös tietoa kirjanpidosta, työntekijöiden palkkatiedoista ja vakuutuksista. Näihin tietoihin on valtuudet ainoastaan yrityksen toimitusjohtajalla, henkilöstöpäälliköllä sekä taloushallinnon työntekijöillä, jotka saavat käsitellä kyseisiä tietoja yrityksen liiketoiminnan suorittamiseen.

FiraHR- kansio sisältää tietoa, joihin on valtuudet ainoastaan toimeksiantajayrityksen toimitusjohtajalla ja henkilöstöpäälliköllä. Kyseinen kansio sisältää dokumentteja muun muassa työntekijöiden rekrytoinneista, työsopimuksista, kehityskeskusteluista, työsuojeluasioista ja palkkatilastoista.

FiraOperations sisältää esimerkiksi työntekijöiden työmatkoihin sisältyviä dokumentteja. Kansio sisältää erilaisia projektien käyttöönottajien henkilötietoja sisältäviä matka-asiakirjoja. Kyseiset tiedot ovat käyttöönottajien esimiesten, rekisteröidyn, matka-asioiden hoitajan ja henkilöstöpäällikön nähtävillä. Näiden tietojen käsittely perustuu käyttötarkoitussidonnaisuuden mukaisesti vain tiettyyn tarkoitukseen, joka tässä tilanteessa on työntekijöiden matka-asioiden hoitaminen työtehtävän toimeenpanemiseksi.

Henkilötietojen suojauksen varmistamiseksi FiraHR ja FIRASecure -kansiot ovat suojattu niin, että niitä pääsee tarkastelemaan ainoastaan henkilöt, joilla on valtuudet niissä sisältyviin henkilötietoihin. Tietojen suojaaminen on varmistettu niin, että vaikka Mfiles itsessään on jokaisen yrityksen työntekijän käytettävissä, kyseiset kansiot ovat löydettävissä ainoastaan, mikäli niitä etsivillä henkilöillä on valtuudet kyseisiin tietoihin. FIRAoperations sisältää paljon muutakin kuin henkilötietoja, joten kansio on itsessään kaikkien löydettävissä, mutta sen sisältämät henkilötietoja käsittelevät asiakirjat ovat ainoastaan valtuutettujen henkilöiden nähtävillä.

Workday

Workday on toimeksiantajayrityksen käyttämä globaali pilvipalveluna toimiva alusta henkilötiedon hallintaan ja prosessointiin. Jokaisella yrityksen työntekijällä on oma henkilökohtainen workdaytili ja kirjautumistunnus. Workdayssa käsitellään kaikkea työsuhteeseen liittyvää dataa. (Mfiles, Workday -opas 2020.)

Workdayssa säilytetään kaikkea työntekijöiden perustietoihin luokiteltavaa henkilötietoa, sekä työntekijöiden palkkatietoja. Järjestelmän sisältämät palkkatiedot ovat esimerkiksi työntekijän kuukausiansiot, vuosiansiot ja muut mahdolliset palkkaan sisältyvät tiedot kuten bonukset. Workday ei sisällä minkäänlaista erityisiin henkilötietoihin luokiteltavaa dataa. Nämä tiedot ovat käsittelyperusteiden mukaisesti erillään muista henkilötiedoista, ja toimeksiantajayrityksessä kyseiset tiedot ovat kokonaan eri järjestelmässä.

Workday on integroitu toimeksiantajayrityksen Learning portaliin, joka sisältää työntekijöille suunnattuja verkkokursseja esimerkiksi tietosuoja-asetukseen liittyen. Suoritus antaa automaattisesti ilmoituksen Workdayhin, ja on siellä henkilöstöpäällikön tarkasteltavissa. Workday ei kuitenkaan ole integroitu yrityksen palkanhallintajärjestelmään. Yrityksellä on erikseen käytettävissä Sonet premium palkanhallintajärjestelmä, joka sisältää kaiken tarvittavan henkilötietodatan palkanhallintaa varten. Kustannusten säästämiseksi Workdayn oma sisäinen palkanhallintajärjestelmän käyttö ei ole toimeksiantajalle oleellista, koska palkkatietojen käsittely on yrityksessä vähäisempää kuin isommissa saman organisaation yrityksissä. Mikäli henkilön palkkatiedot muuttuvat, ne ovat helposti päivitettävissä Sonet -järjestelmään ja sieltä tallennettavissa Workdayihin, mutta näiden järjestelmien välistä integraatio-ominaisuutta ei yrityksellä ole.

Tietosuoja-asetuksen rekisteröidyn oikeuksia noudattaen, rekisteröidyn perustiedot ovat helposti hänen löydettävissä ja muokattavissa. Jokaisella yrityksen työntekijällä on velvollisuus pitää omat tietonsa ajantasalla. Työntekijän henkilötietoihin on pääsy ainoastaan rekisteröidyllä itsellään, rekisteröidyn esimiehellä sekä yrityksen henkilöstöpäälliköllä. Tiedot ovat esimiessuojattu niin, ettei kukaan muu yrityksen henkilö pääse tietoja käsittelemään. Työntekijän esimies pääsee tarkastelemaan ainoastaan oman osaston alaisensa henkilötietoja, eikä siis muiden osastojen työntekijöiden tiedot ole jokaisen esimiehen tarkasteltavissa. Kaikki Workdayn henkilötietodataa sisältävät dokumentit ovat lähetettävissä ja ladattavissa helposti luettavassa ja ymmärrettävässä muodossa, mikäli rekisteröity tätä pyytää. Tiedot ovat suojattuna niin, että mikäli Rauman

yksikköön tapahtuu mahdollinen tietomurto, tai jokin muu rekisteröidyn oikeuksia vahingoittava riski, tiedot eivät katoa lopullisesti vaan ne pysyvät järjestelmässä pilvipalvelun takia.

Workday on käytössä maailmanlaajuisesti koko toimeksiantajayrityksen organisaatiossa. Toimeksiantajayrityksen henkilöstöpäälliköllä on valtuudet käsitellä kaikkea Workdayssa olevaa henkilötietodataa tietyn rajoituksin. Yrityksen henkilöstöpäälliköllä on valtuudet käsitellä ainoastaan henkilötietoja, jotka sijoittuvat organisaation Rauman yksikköön, eikä esimerkiksi Espoossa sijaitsevan saman organisaation yrityksen työntekijöiden tietoja ole mahdollista käsitellä toimeksiantajayrityksen henkilöstöpäällikön johdosta. Tiedot ovat suojattuna niin, että mikäli Workdayn hakukenttään laittaa toisessa kaupungissa tai valtiossa sijaitsevan yrityksen työntekijän nimen, haku löytää ainoastaan henkilön nimen, sähköpostin, työnimikkeen ja työtiimin. Henkilötietojen käyttörajoitukset ovat suojattuna niin, että mitä korkeampi työnimike henkilöstöhallinnon organisatorisella tasolla on, sitä laajemmat valtuudet henkilöllä on nähdä ja käsitellä organisaation työntekijöiden henkilötietoja. Esimerkiksi koko organisaation henkilöjohtajalla on valtuudet jokaiseen oman organisaation yritykseen maailmanlaajuisesti, kun taas toimeksiantajayrityksen henkilöstöpäällikön valtuudet rajoittuvat ainoastaan Rauman yksikköön.

Automaattinen päätöksenteko on toimeksiantajayrityksellä hyvin vähäistä, ja profilointia ei henkilöstöhallinnolla ole käytössä lainkaan. Ainoa automaattinen päätöksenteko, mitä yritys Workday -järjestelmllä hyödyntää on mahdollisen työnhaun yhteydessä tapaus, jossa ohjelma rajaa tiettyyn työtehtävään soveltuvat henkilöt esimerkiksi koulutuksen ja työkokemuksen perusteella. Tässäkään tapauksessa päätöksenteko ei ole täysin automaattista, koska ennen soveltuvien henkilöiden rajaamista, järjestelmän käyttäjän on täytynyt itse kirjoittaa tarvittavat hakuvaatimukset. Näin järjestelmä osaa automaattisesti rajata kyseiseen tehtävään soveltuvat henkilöt, ja näin auttaa henkilöstöhallintoa työntekijöiden hakuprosesseissa.

Kaikki Workdayssa ja Mfilesissä käsiteltävät työntekijän työsuhteeseen sisältyvät tiedot ovat tarkasti määriteltyjä, ja tiedot ovat tietosuojaperiaatteiden mukaisesti vain tiettyä tarkoitusta varten, ja niitä säilytetään vain työsuhteen tai rekrytoinnin kannalta oleellisen ajan verran. Työsopimuksen ja työsuhteen kannalta oleellisimmat henkilötietodokumentit kuten työtodistukset, ovat sijoitettuna järjestelmissä sekä palkanlaskentaprosessia varten palkkahallinnon lukituissa arkistoissa.

Onetrust

Onetrust on koko toimeksiantajayrityksen organisaation käyttämä järjestelmä, jolla pystytään todistamaan, että henkilötietojen käsittelyssä noudatetaan yleisen tietosuoja-asetuksen lainmukaisia periaatteita. Jokaisesta prosessista, jossa yritys jollain tasolla käsittelee henkilötietoja, laaditaan Onetrustiin niin kutsuttu ”assessment” -tiedosto, jolla pystytään todistamaan tietosuoja-asetuksen noudattaminen. Esimerkkinä työntekijän ja työnantajan välinen työsopimus, josta laaditaan ”assesments” -kansioon tiedosto työsopimuksen henkilötietojen käsittelystä. Onetrust kysyy jokaisen tiedoston kohdalla kysymyksiä kyseisen prosessin henkilötietojen käsittelystä. Onetrustiin täytyy kyseisen prosessin kohdalle kertoa esimerkiksi mikä henkilötietoja käsittelevä prosessi on kyseessä ja mihin tarkoitukseen käsittely on. Käsittelystä pitää kertoa esimerkiksi, missä henkilötiedot sijaitsevat, kuka on vastuussa tiedoista, onko kyseessä yrityksen sisäinen vai kolmannen osapuolen tietojen käsittely, keihin käsittely kohdistuu ja kuinka monen henkilön tietoja prosessissa käsitellään. Myös kyseisten tietojen suojausmekanismeista sekä tietojen muokkaamisesta ja hävittämisestä on laadittava selvennys Onetrustiin.

Onetrust sisältää paljon dataa erilaisista henkilötietojen käsittelyyn liittyvistä prosesseista, ja jokaiseen prosessiin tulee tehdä kuvaus siitä miten tietosuoja-asetusta tässä prosessissa noudatetaan. Näiden lisäksi Onetrustin ”assessments” -kansio sisältää ”GDPR Ready Assessment” -tiedoston, jossa määritellään yksityiskohtaisesti tietosuoja-asetuksen noudattaminen yleisesti kaikessa henkilötietojen käsittelyssä. Kyseinen tiedosto on muiden tiedostojen kanssa rekisterinpitäjän apuna mahdollisessa osoitusvelvollisuuden tilanteessa, ja näiden avulla pystytään osoittamaan asetuksen lainmukainen noudattaminen.

”GDPR Ready Assessment” -tiedostoon on ensimmäiseksi määritelty prosessien lainmukainen perusta kaikelle henkilötietojen käsittelylle. Ensimmäisessä osiossa määritellään esimerkiksi tieto siitä, onko jokainen prosessi dokumentoitu, niiden käsittelyn käyttötarkoitus määritelty, ja kohdentuuko tietojen käsittely jollain tapaan lapsiin. Seuraava osio tarkastelee rekisteröidyn oikeuksia, ja sitä onko niitä noudatettu asetuksen mukaisesti. Osiossa määritellään rekisteröidyn oikeuksien informoinnista ja oikeuksien käytön mahdollisuuksista esimerkiksi tietojen poistamisen tai oikaisemisen tilanteessa. Kolmannessa osiossa määritellään tarkkaan rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista, siitä tiedostetaanko velvollisuudet eri tilanteissa, ja keihin velvollisuudet kohdistuvat. Neljännessä osiossa kerrotaan tietosuojaimoituksen esittämisestä ja sen tarjoamisesta rekisteröidylle henkilötietojen

käsittelyn aikana. Tässä määritellään esimerkiksi, tarjotaanko rekisteröidylle tietoa tietosuojasta henkilötietojen keräämisen tai uuden käsittelytarkoituksen yhteydessä.

Viidennessä osiossa käydään läpi henkilötietojen suojausta ja toimenpiteitä suojauksen ylläpitämiseksi. Tähän on määritelty esimerkiksi jatkuva suojauksen testaus organisatorisilla toimenpiteillä, ja henkilötietojen pseydonymisointi, joista jälkimmäinen ei yrityksellä ole käytössä. Kohtaan on kuitenkin selvitetty, että tietojen varmuuskopiot ovat salattuna teknologisilla toimenpiteillä. Kuudes osio käsittelee mahdollista tietoturvaloukkausta ja siihen varautumista. Tähän on määritetty esimerkiksi tieto henkilöstön kouluttamisesta tietoturvaloukkauksen sattuessa, 72 tunnin tietoturvaloukkauksen ilmoitusajan varmistaminen ja tapahtumien torjuntasuunnitelman käyttö loukkauksen sattuessa. Kahdeksas kohta käsittelee sekin yksityisyydensuojaa ja henkilödatan suojausta. Sinne on määritelty yrityksen tiedostavan erityisten henkilötietojen käsittelyn, ja sen miten tietoja suojataan. Tämän lisäksi on kerrottu yrityksen käyttävän henkilödatan minimointia hyödyksi. Yhdeksänteen kohtaan on määritelty vaikutustenarvioinnin tiedostaminen. Osioon on ilmoitettu, että vaikutustenarvionnissa on otettu huomioon esimerkiksi erityiset henkilötiedot, automaattinen päätöksenteko ja profilointi sekä henkilötietojen käyttötarkoituksen muuttuminen. Kolmessa viimeisessä kohdassa määritellään tietosuojavastaavan hyödyntäminen, joka ei siis toimeksiantajayritykselle ole oleellista. Tämän lisäksi on määritelty henkilödatan siirtomahdollisuuksista esimerkiksi kolmansiin maihin.

4.1.2 Yrityksen tietosuoja-asetuksen mukainen toiminta

Tämän haastattelun ja esimiehille suunnatun kyselyn tarkoituksena on saada tietoa siitä, miten yleisen tietosuoja-asetuksen noudattaminen toimeksiantajayrityksen sisällä käytännössä tapahtuu.

Haastatteluun oli valittu 10 eri tietosuoja-asetukseen liittyvää kysymystä, joiden tarkoituksena on kartoittaa hieman laajemmin toimeksiantajayrityksen tietosuoja-asetuksen mukaista toimintaa. Haastattelu suoritettiin etänä Microsoft Teams -järjestelmän avulla, ja siihen osallistui yrityksen henkilöstöpäällikkö, talouspäällikkö sekä kirjanpitäjä. Kysymykset eivät olleet kohdistettu tietyille haastatteluun osallistujille, vaan tarkoituksena oli saada aikaan keskustelua, ja sitä kautta käydä läpi niihin liittyviä asioita.

Haastattelukysymykset:

1) **Onko yrityksellä tietosuojavastaavaa tai ajatusta sen hankkimisesta? Jos ei ole, miksi?**
   Talouspäällikkö kertoo, ettei toimeksiantajayrityksellä ole määritetty varsinaista tietosuojavastaavaa. Yrityksessä ei käsitellä niin laajamittaisesti henkilötietoja, eikä tiedot sisällä juurikaan erityisiin henkilötietoryhmiin luokiteltavaa tietoa. Tästä syystä virallisen tietosuojavastaavan nimittäminen ei yrityksessä ole niin välttämätöntä. Talouspäällikkö on kuitenkin yrityksessä henkilö, joka vastaa yleisistä tietosuoja-asetukseen liittyvistä asioista yhdessä henkilöstöhallinnon kanssa.

2) **Käsitteleekö henkilöstöhallinto missään muodossa asiakkaiden henkilötietoja, vai ainoastaan yrityksen omien työntekijöiden tietoja?**
   Henkilöstöpäällikön mukaan yrityksen henkilöstöhallinto ei käsittele ollenkaan asiakkaiden henkilötietoja. Yrityksen liiketoiminta liittyy olennaisesti B2B -kaupankäyntiin, joten yksittäisten asiakkaiden henkilötietoja ei henkilöstöhallinnossa käsitellä. Ainoa asiakkaiden henkilötietojen käsittely liittyy satunnaisesti asiakasyritysten toimihenkilöiden matkustusasiakirjojen dokumentointiin. Tämä on kuitenkin kyseisen projektin projekti-insinöörin tehtävä, eikä siis liity yrityksen henkilöstöhallintoon.

3) **Minkälaisissa tilanteissa henkilötietoja yleensä käsitellään?**
   Yleisimmät henkilötietojen käsittelyn tilanteet tapahtuvat henkilöstöpäällikön mukaan työntekijän rekrytointiprosessin aikana, jolloin tiedot kerätään ja tallennetaan henkilötietojärjestelmiin. Tietojen käsittely liittyy suurelta osin yrityksen omiin työntekijöihin kohdistuviin yleisiin velvoitteisiin, kuten kehityskeskusteluihin, palkanmaksuun ja työnajanseurantaan.

4) **Käsitteleekö yritys missään muodossa erityisiä henkilötietoja?**
   Henkilöstöpäällikön mukaan ainoat erityiset henkilötiedot joita henkilöstöhallinto käsittelee liittyy työntekijöiden terveydentilatietoihin, kuten terveystarkastuksiin. Kirjanpitäjä tarkentaa, että palkkahallinnossa terveydentilatietoja käsitellään ainoastaan tilanteissa, joissa esimerkiksi pidempiaikaisiin sairauslomiin haetaan Kela-korvausta. Lyhyemmät

sairaustodistukset säilytetään hetken aikaa palkkahallinnon lukituissa arkistoissa, jonka jälkeen ne hävitetään lopullisesti.

5) **Kuinka järjestelmällistä henkilötietojen käsittely on tietojen keräämisestä niiden dokumentointiin ja hävittämiseen?**
   Henkilöstöpäällikkö kertoo tietojen käsittelyn olevan toimeksiantajayrityksessä järjestelmällistä, ja kaikki tietojen käsittelyyn liittyvät prosessit tiedostetaan selkeästi. Henkilöstöhallinto tiedostaa tarvittavat toimenpiteet tietojen keräyksestä niiden hävittämiseen. Tietojen säilytyspaikat ovat tarkkaan määritelty ja suojattu.

6) **Minkälaisiin toimenpiteisiin henkilöstöhallinto on varautunut mahdollisen tietoturvaloukkauksen sattuessa?**
   Tietoturvaloukkauksen sattuessa henkilöstöpäällikkö kertoo loukkauksen kohteena olevien työntekijöiden informoinnin olevan prosessin ensimmäisenä vaiheena. Tämän jälkeen toimeksiantajayritys on velvoitettu ottamaan yhteyttä organisaation kriisiryhmään, joka yhdessä yhdessä yrityksen henkilöstöhallinnon, johtoryhmän ja IT-tukihenkilöiden avulla pyrkivät selvittämään tapahtumien kulkua. Toiminta tapahtuu organisaation kriisisuunnitelman mukaisesti. Yrityksellä on käytössään Information Security policy sekä Disaster Recovery plan, joiden noudattaminen on koko organisaation jokaisen yrityksen vastuulla mahdollisen kriisitilanteen sattuessa. Talouspäällikkö lisäsi vastaukseen vielä tietosuojavaltuutetulle ilmoittamisen, joka tapahtuu mahdollisimman nopeasti heti työntekijöille ilmoittamisen jälkeen.

7) **Miten ja mihin rekisterinpitäjän osoitusvelvollisuus ja siihen tarvittavat dokumentit on laadittu, ja miten velvollisuuden osoittaminen toteutetaan käytännössä?**
   Talouspäällikkö kertoo osoitusvelvollisuuden sisältyvän suurilta osin organisaation käyttämään Onetrust -järjestelmään, johon henkilötietojen käsittelyn prosessit on laadittu. Sitä kautta pystytään osoittamaan, miten henkilötietojen käsittelyn lainmukaisuutta on noudatettu missäkin tilanteissa.

8) **Millä tavoin yritys kouluttaa henkilöstöä toimimaan tietosuoja-asetuksen vaatimusten mukaisesti?**

Henkilöstöpäällikön mukaan ensimmäiset tietosuoja-asetuksen perehdyttämiset tapahtuvat yrityksen nettikursseja tehtäessä, jonka jokaisen uuden työntekijän tulee suorittaa. Kurssissa käydään läpi yleisimpiä tietosuoja-asetukseen liittyviä asioita. Tämän jälkeen yksityiskohtaisemmat koulutukset käydään läpi yhdessä esimiehen ja henkilöstöpäällikön kanssa. Koulutuksissa tarkastellaan yksityiskohtaisemmin työntekijän työtehtäviin liittyviä henkilötietoja sisältäviä kokonaisuuksia ja tietosuojan noudattamista.

9) **Minkälaisin toimenpitein yrityksessä on varauduttu henkilötietojen väärinkäytön riskien minimoimiseksi?**

Henkilöstöpäällikkö kertoo, että koko organisaatiota koskee tarkat ohjeistukset, miten eri tilanteissa tulee toimia. Tämän lisäksi riskien tapahtumisen todennäköisyyttä vähennetään säännöllisillä henkilöstön kouluttamisella. Myös yrityksen käyttämät henkilötietojärjestelmät ovat tarkkaan suojattu. Ohjelmat sisältävät paljon eri tasoisia suojausmekanismeja, joilla saadaan esimerkiksi rajoitettua ylimääräisten henkilöiden pääsyä tiettyihin tietoihin. Järjestelmissä näkyvät tiedot ovat tarkkaan määritetty tietyille profiilitasoille. Mitä korkeampi profiili organisaatiotasolla on, sitä enemmän tietoa henkilö pystyy käsittelemään. Järjestelmillä on tarvittavat lainmukaiset turvaluokitukset ja sertifikaatit, joilla voidaan todentaa järjestelmän luotettavuus ja turvallisuus.

10) **Kuka on vastuussa rekisteröidyn esittämään tarkastuspyyntöön, ja miten rekisteröidylle toimitettava jäljennös käsiteltävistä henkilötiedoista laaditaan?**

Mikäli rekisteröity pyytää henkilötietojensa käsittelyn tarkastusta, häneen liittyvät tiedot ovat talouspäällikön mukaan helposti Onetrustista tarkasteltavissa, josta pystytään katsomaan, mihin eri prosesseihin henkilötietoja on käytetty. Henkilöstöpäällikkö lisäsi vastaukseen Mfiles -järjestelmän käytön, josta henkilöstöhallinnon on mahdollista löytä tarvittavat rekisteröityä koskevat tiedot nimen perusteella, ja näin kerätä niistä tarvittavat asiat jäljennöksen laatimista varten. Jäljennös ei ole suoraan ladattavissa järjestelmistä, mutta sen laatiminen on yksinkertaista, koska käsiteltävät

henkilötiedot ovat järjestelmällisesti tallennettu ja helposti löydettävissä. Mahdollisen tarkastuspyynnön tapahtuessa, jäljennöksen laatiminen on yrityksen henkilöstöpäällikön vastuulla.

Ryhmähaastattelun lisäksi lähetin yrityksen esimiehille pienimuotoisen sähköpostihaastattelun, jonka tarkoituksena oli selvittää miten esimiehet käsittelevät alaistensa henkilötietoja. Haastattelukysymyksenä oli: ”Miten ja missä säilytät henkilöstöön liittyviä luottamuksellisia henkilötietoja sisältäviä dokumentteja?” Selvensin haastattelussa, että kysymyksen ”miten” -kohdassa voisi pohtia millaisessa muodossa dokumentteja säilytetään. ”Missä” -kohdassa tarkoituksena on miettiä mihin dokumentit arkistoidaan/tallennetaan, ja keillä on valtuudet kyseisiin dokumentteihin. Kysymys lähetettiin yhteensä 14 esimiehelle, joista yhdeksän pystyi siihen vastaamaan.

Yhdeksästä vastaajasta jokainen kertoi säilyttävänsä suurimman osan dokumenteista sähköisesti. Heistä kahdeksan säilyttää suurimman osan dokumentteja yrityksen Workday -järjestelmässä, ja kyseisiin tietoihin on pääsy ainoastaan esimiehellä itsellään, rekisteröidyllä sekä henkilöstöpäälliköllä.

Kuusi vastaajista kertoi käyttävänsä Workdayn lisäksi myös omaa henkilökohtaista levyasemaa hyödyksi henkilötietodokumenttien säilyttämiseen. Vain 1 yhdeksästä sanoi käyttävänsä pääosin henkilökohtaista levyasemaa dokumenttien säilytykseen. Jokainen vastaajista kertoi henkilökohtaisen levyaseman olevan salasanasuojattu, johon on pääsy vain esimiehellä itsellään.

Kolme yhdeksästä vastaajasta kertoi säilyttävänsä henkilötietodokumentteja workdayn ja levyaseman lisäksi myös Mfiles -järjestelmässä. Kyseisiin tietoihin on tiedon laadusta riippuen pääsy esimiehellä itsellään sekä yrityksen henkilöstöhallinnolla.

Haastattelun vastaajista suurin osa kertoi käsittelevänsä paperisia dokumentteja ainoastaan hetken aikaa vain jos siihen on tarve. Nämä tilanteet keskittyvät yleisesti tiedostojen skannaamiseen, jonka jälkeen kyseisten dokumenttien paperiset versiot hävitetään lopullisesti. Ainoastaan kolme vastaajista kertoi säilyttävänsä joitain henkilötietodokumentteja paperisina. Näitä tiedostoja on hyvin vähän ja jokainen vastaajista kertoi säilyttävänsä kyseisiä tiedostoja omassa henkilökohtaisessa lukitussa kaapissa.

Suurimmat henkilötietojen käsittelyn haasteet ja ongelmat kerrottiin liittyvän yrityksen sähköpostiin. Kuusi vastaajista kertoi tiedostavansa joidenkin henkilötietodokumenttien olevan sähköpostissa. Sähköpostissa olevia tiedostoja pyritään poistamaan aina, kun niiden käytölle ei ole enään tarvetta, mutta suurelle osalle ongelmaksi koituukin kyseisessä tilanteessa se, että kun satunnaisia henkilötietoja sisältäviä dokumenttejä lähetellään sähköpostissa, tiedostojen säilytysaikaa on vaikeaa määrittää ja kyseisiä tiedostoja ei pystytä poistamaan systemaattisesti. Sähköposti voi myös sisältää vanhoja tallennettuja dokumentteja, joiden käyttötarpeen määrittämistä ja säilytysaikaa voi olla hankalaa määrittää. Nykyään uusia dokumentteja on helpompi poistaa, mutta ongelmaksi vastaajat kertoivatkin koituvan juuri vanhat sähköpostissa olevat henkilötietodokumentit ja sen, että sähköpostissa liikkuu useita viestejä, joista jotkut saattavat satunnaisesti sisältää henkilötietoja.

Tässä osiossa olen käyttänyt hyödyksi yrityksen henkilötietojärjestelmiä ja haastatteluja, joiden avulla olen kartoittanut toimeksiantajayrityksen tietosuoja-asetuksen mukaisen toiminnan. Näiden avulla olen saanut tietoa siitä, miten yrityksen henkilöstöhallinto noudattaa tietosuoja-asetuksen mukaisia periaatteita henkilötietojen käsittelyn eri tilanteissa, ja miten henkilötietojen suojaaminen yrityksessä tapahtuu. Kaikkia yksityiskohtia ei kuitenkaan ole tässä tutkimuksessa käyty läpi. Esimerkiksi Onetrust -järjestelmään kuuluva GDPR Ready Assessment sisältää yhteensä 62 erilaista yksityiskohtaista kysymystä tietojen käsittelystä, eikä jokaisen kohdan erikseen avaaminen ole tarpeellista tietosuoja-asetuksen noudattamisen selvittämiseksi.

Järjestelmiin ja haastatteluun liittyvät oleellisimmat henkilötietojen käsittelyyn liittyvät asiat on kuitenkin käyty läpi. Esimiesten haastatteluvastauksista voi selkeästi todeta, että yrityksessä tiedostetaan kuinka henkilötietoja sisältäviä dokumentteja tulee käsitellä rekisteröidyn oikeuksia ja erityisten henkilötietoryhmien käsittelyperiaatteita noudattaen. Iso osa käsittelystä perustuu rekisterinpitäjän oikeutettuun etuun, ja tiedot ovat rekisterinpitäjän velvollisuuksia noudattaen suojattuna ja vain asianomaisten henkilöiden käsiteltävissä. Ainoaksi haasteeksi nousi sähköpostissa olevat satunnaiset henkilötiedot. Näiden tietojen käsittely on kuitenkin tietosuoja-asetuksen mukaisesti laillista, koska sähköposti on jokaisen työntekijän henkilökohtainen ja salasanalla suojattu. Tietojen käsittely sähköpostissa on näin tietosuojaperiaatteiden mukaisesti luottamuksellista ja turvallista. On kuitenkin tärkeä muistaa, että tiedostoja ei lähetetä vahingossa väärille henkilöille. Tärkeitä henkilökohtaisia tietoja on myös suositeltavaa lähettää salattuna, jotta tietojen suoja pystytään varmistamaan.

5 JOHTOPÄÄTÖKSET

Tässä opinnäytetyössä on tavoitteiden mukaisesti tutkittu miten hyvin toimeksiantajayrityksen nykyiset järjestelmät ja toimintatavat vastaavat Euroopan unionin yleisen tietosuoja-asetuksen asettamia vaatimuksia. Tutkimuksessa on käytetty hyväksi henkilötietojärjestelmiä ja haastatteluja, joiden avulla on saatu kartoitettua toimeksiantajayrityksen yleisen tietosuoja-asetuksen lainmukainen toiminta. Opinnäytetyön teoriaosiossa on käyty läpi Euroopan Unionin yleisen tietosuoja-asetuksen velvoittamia henkilötietojen käsittelyyn liittyviä periaatteita ja ohjeistuksia. Teoriaosio sisältää oleellisimmat ja tärkeimmät henkilötietojen käsittelyyn liittyvät toimenpiteet, joita noudattamalla pystytään minimoimaan henkilötietojen väärinkäyttöön liittyviä riskejä, ja näin toimimaan yleisen tietosuoja-asetuksen mukaisesti.

Empiirisessä tutkimusosiossa on henkilötietojärjestelmiä tarkastellen ja haastatteluja hyväksi käyttäen heijastettu toimeksiantajayrityksen henkilötietojen käsittelyn toimenpiteitä teoriaosiossa oleviin lainmukaisiin periaatteisiin, ja tätä kautta kartoitettu, miten ja missä henkilötietoja yrityksessä käsitellään, ja kuinka henkilöstöhallinto noudattaa tietosuoja-asetuksen lainmukaisuutta. Yrityksen hyödyntämät henkilötietojärjestelmät ovat hyvin luotettavia, ja niissä säilytettävät henkilötiedot ovat tarkasti suojattu. Tietojen säilytyspaikat ovat tarkkaan määritetty ja niihin pääsee käsiksi vain tietojen käsittelyyn valtuutetut henkilöt. Henkilötietoja käsittelevät työntekijät ovat koulutettu toimimaan tietosuoja-asetuksen mukaisesti, ja heillä on käytössään tarkat ohjeistukset tietosuojan ylläpitämiseksi. Toimeksiantajayritys on määrittänyt tarkkaan eri prosessit, joihin henkilötietoja käsitellään. Prosessit on tallennettu järjestelmään, joihin on pääsy vain valtuutetuilla henkilöillä. Järjestelmään tallennettujen prosessien avulla yritys kykenee osoittamaan henkilötietojen lainmukaisen käsittelyn. Jokaiseen henkilötietoja sisältävään prosessiin on yksityiskohtaisesti kuvailtu miten tietosuoja-asetusta siinä noudatetaan. Prosesseissa olevia henkilötietoja käytetään vain tiettyä tarkoitusta varten ja niiden säilytysajat ovat tarkasti määritetty. Jokaisen prosessin käyttötarkoitus on tarkasti esitetty tietosuojaperiaatteita ja rekisteröidyn oikeuksia noudattaen.

Haastattelun avulla on saatu selvitettyä miten henkilötietojen käsittely, tietojen suojaaminen, riskien minimointi ja niihin varautuminen yrityksessä käytännössä toimii. Yrityksessä on noudatettu yleistä tietosuoja-asetusta asetuksen soveltamispäivästä

lähtien. Henkilöstöhallinto tiedostaa tarkkaan yrityksen tietojenkäsittelyn vaiheet ja heillä on tieto siitä miten tietosuojaa pystytään vahvistamaan. Henkilötietojen käsittely keskittyy olennaisesti yrityksen omiin työntekijöihin, ja näihin liittyvät käsittelyn eri vaiheet tietojen keräyksestä niiden dokumentointiin ja hävittämiseen on tarkkaan tiedossa. Henkilöstöhallinta tiedostaa tietosuojaan liittyvät riskit, ja niihin varautumisen. Mahdollisiin kriisitilanteisiin on varauduttu organisatorisella tasolla noudattaen organisaation tarkkaan määritettyjä ohjeita ja toimenpiteitä. Haastatattelussa käy myös ilmi, että vaikka suurin osa tietojen käsittelystä liittyy henkilöstöhallinnon työtehtäviin, on myös toimeksiantajayrityksen muu henkilöstö koulutettu toimimaan tietosuoja-asetuksen vaatimuksen mukaisesti. Henkilötietojärjestelmiä ja haastattelua tarkastellessa on todettavaa, että yrityksessä tiedostetaan yleisen tietosuoja-asetuksen vaatimukset ja asetuksen lainmukainen noudattaminen yksilön oikeudet huomioon ottaen.

LÄHTEET

Aditro 2020. Yleinen tietosuoja-asetus henkilöstö- ja palkkahallinnossa – näin toimit oikein FI_Aditro_Whitepaper_GDPR_for_HR_and_payroll_highres. Viitattu 12.10.2020

Ala-Varvi, Jari 2020. Opsec. Oikeutettu etu henkilötietojen käsittelyn perusteena. https://www.opsec.fi/fi/2018/03/24/oikeutettu-etu-henkilotietojen-kasittelyn-perusteena/ Viitattu 10.10.2020

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2017. Osaava tietosuoja-vastaava. Helsinki: Tietosanoma Oy.

Axactor 2020. Henkilötietolaki. Mikä on henkilörekisteri? https://www.axactor.fi/henkilotietolaki

Björg, R. 2018. Centria bulletin. GDPR – mikä muuttuu? https://centriabulletin.fi/gdpr-mika-muuttuu/ Viitattu 13.10.2020

Digiturvamalli 2017a. Suostumuksen edellytykset. https://tietosuoja.fi/rekisteroidyn-suostumus Viitattu 10.10.2020

Digiturvamalli 2017b. Käsittelyn lainmukaisuus. https://fakta.digiturvamalli.fi/gdpr-asetus/6-kasittelyn-lainmukaisuus Viitattu 13.10.2020

Digiturvamalli 2017c. Rekisteröidyn oikeus saada pääsy tietoihin. https://fakta.digiturvamalli.fi/gdpr-asetus/15-rekisteroidyn-oikeus-saada-paasy-tietoihin Viitattu 21.10.2020

Elinkeinoelämän keskusliitto 2020. Tietopaketti yrityksille: EU:n yleinen tietosuoja-asetus ja tietosuojalaki. Mikä on yleinen tietosuoja-asetus? https://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen/

Euroopan komissio 2020a. Mikä on rekisterinpitäjä tai tietojen käsittelijä? https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fi Viitattu 10.10 2020

Euroopan komissio 2020b. Mitkä tiedot ovat henkilötietoja? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_fi Viitattu 13.10.2020

Euroopan komissio 2020c. Mitä tarkoittaa ’oikeutettu etu’? https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_fi Viitattu 14.10.2020

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely. EU-tietosuoja-asetuksen vaatimukset. Vantaa: Hansabook Oy.

Iconics 2020. Tasapainotesti. https://www.iconics.fi/tasapainostesti Viitattu 21.10.2020

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö, e-kirja. Saatavilla:https://verkkokirjahylly-almatalent-fi.ezproxy.turkuamk.fi/teos/BAXBBXATHBBED#/kohta:((20)Uusi((20)tietosuojalains((e4)((e4)d((e4)nt((f6)/piste:tcz Viitattu 14.10.2020

Kuntaliitto 2017. Yleinen tietosuoja-asetus. https://www.kuntaliitto.fi/yleiskirjeet/2017/yleinen-tietosuoja-asetus Viitattu 22.10.2020

Kurvi, Maiju. & Sedig, Riitta. 2017. Yrityselämän 360. Tietosuoja-asetus + HR = ?. https://yrityselaman360blog.ey.com/2017/08/24/tietosuoja-asetus-hr/ Viitattu 12.10.2020

Lexia 2018. Tietosuojaa koskeva vaikutustenarviointi: mitä, miksi ja milloin? https://www.lexia.fi/fi/tietosuojaa-koskeva-vaikutustenarviointi/ Viitattu 21.10.2020

Minilex 2020a. Mikä on henkilötieto? https://www.minilex.fi/a/mik%C3%A4-on-henkil%C3%B6tieto

Minilex 2020b. Mikä on henkilörekisteri? https://www.minilex.fi/a/mik%C3%A4-on-henkil%C3%B6rekisteri

Minilex 2020c. Henkilötiedot ovat tunnistetietoja. https://www.minilex.fi/a/henkil%C3%B6tiedot-ovat-tunnistetietoja Viitattu 13.10.2020

Minilex 2020d. Lainvastainen henkilötietojen käsittely johtaa ankaraan korvausvastuuseen. https://www.minilex.fi/a/lainvastainen-henkil%C3%B6tietojen-k%C3%A4sittely-johtaa-ankaraan-korvausvastuuseen Viitattu 16.10.2020

Opitietosuojaa 2020. EU:n tietosuoja-asetuksen velvoitteet johdolle. https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus

Rauhala 2018a. Henkilöstöhallinto ja tietosuoja-asetus - https://www.rauhala.fi/blog/henkilostohallinto-hr-ja-tietosuoja-asetus Viitattu 12.10.2020

Rauhala 2018b. Miksi GDPR on HR:n(kin) ystävä? https://www.rauhala.fi/blog/miksi-gdpr-on-hr-yst%C3%A4v%C3%A4 Viitattu 12.10.2020

Sopimustieto 2020. Sopimus henkilötietojen käsittelystä/tietosuojasopimus. https://sopimustieto.fi/sopimukset/5aPxRa-sopimus_henkilotietojen_kasittelysta_tietosuojasopimus?campaign_source=SDM_%7C_Haku_%7C_DSA_%7C_Yritys_%7C_Reach&campaign_ref=5aPxRa-sopimus_henkilotietojen_kasittelysta_tietosuojasopimus&gclid=CjwKCAjww5r8BRB6EiwArcckC3SD3mtiDKf45QODSa4AqT56-RsJq9wGDyZraMJgoCHLhPp2LQUiehoCXd0QAvD_BwE Viitattu 14.10.2020

Suomentilintarkastajat 2018. Milloin tilintarkastaja on rekisterinpitäjä ja milloin henkilötietojen käsittelijä? https://www.suomentilintarkastajat.fi/tilintarkastus/kysymyksia-ja-vastauksia/milloin-tilintarkastaja-on-rekisterinpitaja-ja-milloin-henkilotietojen-kasittelija Viitattu 12.10.2020

Sympa 2017. HR:n GDPR – muistilista. https://hub.sympa.com/hubfs/Downloadable_documents/HR_GDPR_lomake_FI.pdf Viitattu 12.10.2020

Tietoarkisto 2020. Tunnisteellisuus ja anonymisointi. Mitä on henkilötieto? https://www.fsd.tuni.fi/fi/palvelut/aineistonhallinta/tunnisteellisuus-ja-anonymisointi/ Viitattu 13.10.2020

Tietosuoja-asetus 2020. EU:n uusi tietosuoja-asetus koskettaa lähes jokaista yritystä ja yhdistystä. https://www.tietosuoja-asetus.org/

Tietosuojaloukkaus 2020. Usein tietosuojaloukkaus havaitaan liian myöhään, joskus ei lainkaan. https://www.tietosuojaloukkaus.fi/ Viitattu 16.10.2020

Tietosuojatyöryhmä 2014. Lausunto 6/2014 direktiivin 95/46/EY 7 artiklan mukaisesta rekisterinpitäjän oikeutetun intressin käsitteestä. Rekisteröidyn intressit ja oikeudet. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fi.pdf Viitattu 10.10.2020

Tietosuojatyöryhmä 2017. Oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat ohjeet. https://tietosuoja.fi/documents/6927448/8316711/Oikeus+siirt%C3%A4%C3%A4+tiedot+j%C3%A4rjestelm%C3%A4st%C3%A4+toiseen+fi.pdf/529297ab-7d1e-4f80-8fa3-a80b943d316f/Oikeus+siirt%C3%A4%C3%A4+tiedot+j%C3%A4rjestelm%C3%A4st%C3%A4+toiseen+fi.pdf Viitattu 3.11.2020

Tietosuojavaltuutetun toimisto 2018. Rekisterinpitäjän oikeutettu etu henkilötietojen käsittelyperusteena – varmista tasapainotestillä.https://tietosuoja.fi/-/rekisterinpitajan-oikeutettu-etu-henkilotietojen-kasittelyperusteena-varmista-tasapainotestilla Viitattu 10.10.2020

Tietosuojavaltuutetun toimisto 2020a. Organisaatiot. Rekisteröidyn suostumus.https://tietosuoja.fi/rekisteroidyn-suostumus

Tietosuojavaltuutetun toimisto 2020b. Henkilötietojen käsittely. https://tietosuoja.fi/henkilotietojen-kasittely Viitattu 10.10.2020

Tietosuojavaltuutetun toimisto 2020b. Henkilötietojen käsittely. https://tietosuoja.fi/henkilotietojen-kasittely Viitattu 13.10.2020

Tietosuojavaltuutetun toimisto 2020c. Rekisterinpitäjän oikeutettu etu. yksityishenkilön edut ja oikeudet etusijalla. https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu Viitattu 10.10.2020

Tietosuojavaltuutetun toimisto 2020d. Henkilötietojen käsittelijät. https://tietosuoja.fi/henkilotietojen-kasittelijat Viitattu 12.10.2020

Tietosuojavaltuutetun toimisto 2020d. Lainmukaisuus, asianmukaisuus ja läpinäkyvyys https://tietosuoja.fi/lainmukaisuus-asianmukaisuus-lapinakyvyys Viitattu 13.10.2020

Tietosuojavaltuutetun toimisto 2020e. Käyttötarkoitussidonnaisuus. https://tietosuoja.fi/kayttotarkoitussidonnaisuus Viitattu 13.10.2020

Tietosuojavaltuutetun toimisto 2020f. Luottamuksellisuus ja turvallisuus. https://tietosuoja.fi/luottamuksellisuus-ja-turvallisuus Viitattu 13.10.2020

Tietosuojavaltuutetun toimisto 2020f. Tietojen täsmällisyys. https://tietosuoja.fi/tietojen-tasmallisyys Viitattu 13.10.2020

Tietosuojavaltuutetun toimisto 2020g. Milloin henkilötietoja saa käsitellä. https://tietosuoja.fi/kasittelyperusteet#lakisaateinen-velvoite Viitattu 14.10.2020

Tietosuojavaltuutetun toimisto 2020h. Erityisten henkilötietoryhmien käsittely. https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely Viitattu 15.10.2020

Tietosuojavaltuutetun toimisto 2020j. Automaattinen päätöksenteko ja profilointi. https://tietosuoja.fi/automaattinen-paatoksenteko-profilointi Viitattu 15.10.2020

Tietosuojavaltuutetun toimisto 2020k. Tietoturvaloukkaukset. https://tietosuoja.fi/tietoturvaloukkaukset Viitattu 16.10.2020

Tietosuojavaltuutetun toimisto 2020l. Vaikutustenarvionnin tekeminen. https://tietosuoja.fi/vaikutustenarvioinnin-tekeminen Viitattu 21.10.2020

Tietosuojavaltuutetun toimisto 2020m. Osoita noudattavasi tietosuojasäännöksiä. https://tietosuoja.fi/osoitusvelvollisuus Viitattu 22.10.2020

Triuvare 2020. GDPR-opas 1: Mikä on GDPR? https://www.triuvare.fi/oppaat-ja-materiaalit/gdpr-opas-1-mika-on-gdpr/