KARELIA-AMMATTIKORKEAKOULU
Liiketalouden koulutusohjelma

Päivi Havukainen

HENKILÖTIETOJEN KÄSITTELY ASIAKASSUHTEESSA EU:N TIETOSUOJA-ASETUKSEN MUKAAN

Opinnäytetyö
Lokakuu 2018

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Syyskuu 2018** **Liiketalouden koulutusohjelma** Karjalankatu 3 80200 JOENSUU

Tekijä

Päivi Havukainen

Nimeke

Henkilötietojen käsittely asiakassuhteessa EU:n tietosuoja-asetuksen mukaan

Tiivistelmä

Tässä opinnäytetyössä käsiteltiin henkilötietojen käsittelyä asiakassuhteessa uuden EU:n tietosuoja-asetuksen, GDPR mukaan, jota sovelletaan kaikissa EU-maissa 25.5.2018 alkaen. Työn tarkoituksena oli selvittää henkilötietojen käsittelyyn yleisesti vaikuttavaa lainsäädäntöä ja erityisesti asiakassuhteisiin liittyviä säädöksiä.

Tutkimus Henkilötietojen käsittely perustuu Euroopan parlamentin ja neuvoston asetukseen (EU) 2016/679. Menetelmänä käytettiin lainopillista kirjoituspöytätutkimusta. Lähteinä opinnäytetyössä olivat voimassa olevat oikeuslähteet ja lisäksi oikeudellinen kirjallisuus sekä internet-sivut.

Euroopan unionin yleisessä tietosuoja-asetuksessa (EU) 2016/679 säädetään henkilötietojen käsittelystä. Asetus määrittelee tietosuojan käsitteet ja tietojen käsittelyn periaatteet. Suomeen ollaan säätämässä uutta tietosuojalakia, jonka tehtävänä tulee olemaan asetuksen täydentäminen ja täsmentäminen.

Kieli	Sivuja 34
suomi	

Asiasanat

Henkilötieto, tietosuojavastaava, tietosuoja-asetus, GDPR (General Data Protection Regulation)

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
September 2018
Business Economics

Karjalankatu 3
80200 JOENSUU
FINLAND
+ 358 13 260 600 (switchboard)

Author
Päivi Havukainen

Title
Processing Personal Data in Client Relationship under Regulation of the European Parliament and of the Council (EU) 2016/679

Abstract

In this thesis deals with the protection of private personal data in client relationships under the new EU General Data Protection Regulation (GDPR), which became effective on 25.5.2018 in all EU-countries. The objective of the thesis was to discuss the processing of personal data in general and especially the regulations pertaining client relationships.

The thesis was executed by using the methods of legal desk research. The research material included the valid sources of law and, additionally, the research literature and internet sources.

The Data Protection Regulation (EU) 2016/679 governs the protection of personal data. The GDPR defines the concept of data protection and the principles of handling personal data of natural persons. In alignment of the GDPR, Finland is going to enact a new Privacy Protection Act to complement and specify the GDPR.

Language
Finnish

Pages 34

Keywords
Personal data, data protection officer, GDPR (General Data Protection Regulation)

Sisältö

Lyhenteet

ETS	Emission Trading System
EU	Euroopan unioni
GDPR	General Data Protection Regulation
HE	Hallituksen esitys

1 Johdanto

Tietosuojan voidaan katsoa alkaneen kehittyä 2 500 vuotta sitten Hippokrateen valasta, joka velvoittaa turvaamaan potilaan yksityisyyden suojaa. Edelleen tänäkin päivänä lääkärit vannovat Hippokrateen valan. Yksilö ja yksilön oikeudet tulivat keskiöön 1700-luvulla suurten vallankumousten myötä. 1890-luvulla Yhdysvalloissa alettiin puhua yksityisyyden suojasta ja joukkotiedotusvälineet alkoivat kehittyä. Euroopassa 1940-luvulla, toisessa maailmansodassa, henkilötietoja hyödynnettiin juutalaisvainojen toteuttamiseen. (Andreasson, Koivisto, Ylipartanen 2016, 49–50.(

Suomessa ensimmäinen henkilötietoja koskenut laki oli vuoden 1987 henkilörekisterilaki. Tämän lain keskeinen säätämisen syy oli IT-teknologian kehitys. Suomen ensimmäinen henkilötietoja koskeva yleislaki tuli voimaan 1988 ja myöhemmin myös rikoslakiin, tieto- ja viestintärikokset, tehtiin huomattavia muutoksia 1995 ja perusoikeusuudistuksessa yksityiselämän suoja nousi suomalaiseksi perusoikeudeksi. Henkilötietojen suojasta säädetään nimenomaan Euroopan perusoikeuskirjan 8 artiklassa, 2009 voimaan tulleessa Lissabonin sopimuksessa. EU:n henkilötietodirektiivi 1995 tuli voimaan Suomessa 1999 henkilötietolailla. EU:n tietosuoja-asetus tuli voimaan 25.5.2018 ja se on sellaisenaan voimassa Suomessa. Tällöin aikaisempi EU:n henkilötietodirektiivi vuodelta 1995 kumoutui ja EU:n yleinen tietosuoja-asetus säätelee tietosuojaa ja henkilötietojen käsittelyä sitovana ja velvoittavana ohittaen kansallisen lainsäädännön. Suomen kansallinen lainsäädäntö oli tarkoitus sopeuttaa kevääseen 2018 mennessä. Kansallisen tietosuojalainsäädännön käsittely eduskunnassa on edelleen kesken. (Andreasson, Koivisto, Ylipartanen 2016, 49–50.(

Tärkein tietosuojasäännös Euroopan unionissa oli aikaisemmin vuoden 1995 henkilötietodirektiivi (95/46/EY9), jonka tavoitteena oli sisämarkkinoiden toiminnan turvaaminen sekä perusoikeuksien ja yksilön vapauksien suojaaminen. Henkilödirektiivin säännöt eivät enää riitä takaamaan oikeutta tehokkaaseen henkilötietojen suojaan nykyisessä digitaalisessa ympäristössä. Euroopan komission tammikuussa 2012 antamassa ehdotuksessa tietojenkäsittelyn uudistamisesta

parannetaan yksilön mahdollisuuksia valvoa henkilötietojaan esimerkiksi varmistamalla, että rekisteröidyltä pyydetään suostumus tietojen käsittelyyn ja oikeus tulla unohdetuksi. Tietosuoja-asetuksella turvataan myös sellaisten rekisteröityjen oikeus yksityisyyteen, jotka eivät ole kiinnostuneita eivätkä tietoisia oikeuksistaan. (Kalliojärvi 2016, 17–18.) EU:n tietosuojauudistuksen tavoitteena on luoda ajanmukainen, yhtenäinen ja kattava tietosuojakehys. Lisäksi sillä pyritään parantamaan luottamusta online-palveluihin edistämään EU:n digitaalista sisämarkkinoiden kehitystä. EU:n yleinen tietosuoja-asetus korvaa vuonna 1995 annetun henkilötietodirektiivin. (Andreasson ym. 2016.)

Suomeen ollaan säätämässä uutta tietosuojalakia, joka täydentää ja täsmentää Euroopan unionin yleistä tietosuoja-asetusta. Näissä laeissa säädeltäisiin henkilötietojen käsittelyn oikeusperusteesta ja erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyssä joissakin tilanteissa. Sellaisiin tilanteisiin, kuten henkilötietojen käsittelyyn oikeusperusteen säilyttämiseksi tietyissä tilanteissa tai tieteellisen tutkimuksen edellytysten säilyttämiseksi nykyisellään niin pitkään kuin mahdollista. Ehdotettu tietosuojalaki täydentää EU:n tietosuojalakia eli sitä tulee lukea rinnakkain tietosuojalain kanssa. Kansallisella lainsäädännöllä voidaan täsmentää asetusta vain yleisessä tietosuoja-asetuksessa kansallisen liikkumavaran puitteissa. Lainsäädännön mukaan henkilötietojen suoja perustuu perustuslain 10.1 §:n säännökseen, josta käy ilmi, että henkilötietojen suojasta säädetään lailla. Henkilötietojen käsittelyyn tulee siis olla lakisääteiset perusteet. (Voutilainen 2012, 51.)

Uuden tietosuojalain tarkoitus on täydentää ja täsmentää Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46EY eli yleisen tietosuoja-asetuksen kumoamisesta. Uudistusten tavoitteena on ollut luoda Euroopan unionille tietosuojakehys, joka olisi ajanmukainen, vahva, yhtenäinen ja kattava. Informaatiokehityksen nopean kehityksen vuoksi ja jäsenvaltioiden hajanaisten ja epäyhtenäisen soveltamisen vuoksi on ollut tarpeen uudistaa lainsäädäntöä. Palorannan (2008) mukaan rekisterinpitäjän tulee perustella henkilötietojen käsittely toimintansa kannalta. Hänen tulee määritellä

tarkoitus siten, että siitä käy ilmi, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään. (Tietosuojavaltuutetun toimisto 2018.)

Henkilötietojen käsittelyä koskevat periaatteet ovat lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus. Rekisterinpitäjän tehtävänä on vastata siitä, että vaatimuksia on noudatettu. Rekisteröidyn pitää antaa suostumuksensa henkilötietojen käsittelyyn. Käsittelyn tulee olla tarpeenmukaista sopimuksen täytäntöön panoa varten tai lakisääteisen velvoitteen noudattamiseksi. Käsittely on lainmukaista myös silloin, kun sillä suojataan rekisteröidyn tai toisen luonnollisen henkilön etuja tai se koskee yleistä etua tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Käsittely on tarpeellista myös rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteutumiseksi, ellei henkilötietoja suojaa rekisteröidyn edut tai perusoikeudet tai -vapaudet, varsinkin jos kysymyksessä on lapsi. Unionin oikeuden tai jäsenvaltion lainsäädännön tulee täyttää yleisen edun mukainen tavoite ja olla oikeassa suhteessa tavoiteltuihin päämääriin. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 artiklat 5 ja 6.)

Euroopan parlamentin ja neuvoston sopimus Euroopan komission ehdottamasta tietosuojauudistuksesta on tärkeä vahvistettaessa kansalaisten perusoikeuksia digitaaliajassa. Uusilla säännöillä helpotetaan yrityksiä koskevia sääntöjä sisämarkkinoilla. Tietosuoja-asetuksen tarkoitus on päivittää ja uudistaa periaatteita, joilla taataan oikeus henkilötietojen suojaan. Uudistus antaa ihmisille työkalut, joilla he voivat kontrolloida henkilötietojaan, joka on yksi EU:n perusoikeuksista. Henkilötietojen käsittelyn kasvuun ovat vaikuttaneet sosiaalisen median verkkosivustot, pilvipalvelut, sijaintiin perustuvat palvelut ja älykortit. Tietosuoja-asetukset ovat muuttuneet 25.5.2018 alkaen, jolloin sovelletaan EU:n yleistä tietosuoja-asetusta kaikissa EU:n jäsenmaissa. Osa tietosuojauudistusta on tietosuojadirektiivi, jonka tarkoituksena on taata luonnollisten henkilöiden suoja henkilötietojen käsittelyssä ja helpottaa henkilötietojen vaihtoa jäsenvaltioiden välillä. (Tietosuojavaltuutetun toimisto 2018.)

Eurooppalaisen tietosuojan uudistuessa asioihin voidaan entistä paremmin puuttua silloinkin, kun kaikki ei mene aivan pykälien mukaan. On tärkeää huomata, että kaikki vanhat, hyvät tietosuojaperiaatteet säilyvät. Tietosuoja-asetuksessa edellytetään, että rekisterinpitäjän tulee nimittää tietosuojavastaava tilanteissa joissa yrityksen ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät rekisteröityjen säännöllistä ja järjestelmällistä seurantaa tai yrityksen käsitellessä arkaluonteisia henkilötietoja. Tietosuojavastaavan tehtävänä on huolehtia siitä, että oma organisaatio noudattaa lakia omissa toimissaan. EU:n yleisessä tietosuoja-asetuksessa on ajateltu rekisterinpitäjän ja rekisteröidyn välisen suhteen lujittumista ja luottamuksen lisääntymistä. Tietoturvallisuuden vastuu kuuluu kuitenkin palvelun tarjoajalle, jonka tehtävänä on tarjota turvallinen asiointialusta. Asiakkaan luottamus ja koko henkilöstön riittävä tietosuojaosaaminen näkyy taloudellisesti viivan alla organisaation taseessa. (Andreasson ym. 2016,22—23, 120.)

Opinnäytetyöni käsittelee lähinnä pienissä yrityksissä tapahtuvaa henkilötietojen käsittelyä asiakassuhteessa EU:n tietosuoja-asetuksen mukaan. Opinnäytetyöni tutkimusmenetelmänä käytin lainopillista kirjoituspöytätutkimusta. Työssäni käyn läpi aluksi tietosuojaan liittyviä keskeisiä käsitteitä ja tietosuojaperiaatteita sekä lain vaatimuksia. Tämän jälkeen käsittelen henkilötietojen käsittelyä asiakassuhteessa eli millä perusteella tietoja voidaan käsitellä asiakassuhteessa tietosuoja-asetuksen perusteella.

Pääasiallisin oikeuslähde Suomen oikeusjärjestelmässä on laki. Kansallisen lainsäädännön muodostavat perustuslaki, muut lait, asetukset ja niiden nojalla annetut säädökset. Maan tapaa käytetään silloin, kun kirjallinen oikeuslähde puuttuu. Kyseessä pitää kuitenkin olla vakiintunut ja yleisesti velvoittava sekä kohtuullinen käytäntö. Useiden kansallisten säädösten taustalla on kansainvälinen oikeus. Suomen ollessa jäsenenä Euroopan unionissa ja Euroopan neuvostossa, olemme sidotut noudattamaan Euroopan lainsäädäntöä ja oikeuskäytäntöä. Lainsäädännön lisäksi muita oikeuslähteitä ovat lainvalmisteluaineistot eli esityöt ja kansallisten tuomioistuinten ratkaisukäytäntö, hallituksen esitykset ja valiokuntamietinnöt. Tärkeimpiä ylikansallisia tuomioistuimia ovat EU:n tuomioistuin ja Euroopan ihmisoikeustuomioistuin, joiden ratkaisukäytäntö on osittain kansallisia

viranomaisia sitovaa oikeutta. EU:n perussopimukset muodostavat yhdessä EU:n kirjoittamattomien oikeusperiaatteiden kanssa primäärioikeuden. EU:n toimielin- ja päätöksentekojärjestelmä toimii primäärioikeuden määrittämissä rajoissa, minkä toiminnan tuloksena syntyy sekundääristä oikeutta. (Tenhunen 2011, 13—27 ja 180.)

Oleellisimmat oikeustieteen tieteenhaarat ovat lainoppi, oikeushistoria, oikeussosiologia ja vertaileva oikeustiede. Näitä tarkoitustapoja voidaan myös yhdistellä työssä tai liikkua niiden välimaastossa. Suurin osa oikeustieteellisestä tutkimuksesta on lainoppia eli oikeusdogmatiikkaa, jonka keskeisimpänä tutkimusongelmana on selvittää voimassa olevan oikeuden sisältö kulloinkin käsiteltävässä oikeusongelmassa. Ensimmäinen lainopin keskeinen osa on oikeusjärjestykseen kuuluvien sääntöjen tutkiminen ja erityisesti niiden sisällön selvittäminen eli tulkitseminen. Toinen keskeinen tehtävä on systematisointi eli voimassa olevan oikeuden jäsentäminen. Systematisoinnin avulla pyritään luomaan ja kehittämään oikeudellista käsitejärjestelmää, jolla oikeutta tulkitaan. Systematisointi auttaa löytämään etsityt säännökset ja hahmottamaan kokonaiskuvaa oikeudellisista järjestelyistä ja niiden välisistä keskinäissuhteista. Oikeushistoriallinen tutkimusote on lainopin ohella yleinen. Oikeushistoria tutkii oikeusnormien tai oikeudellisen ajattelun kehitystä käyttäen hyväkseen historiantutkimuksen menetelmiä. (Husa, Mutanen & Pohjolainen 2001, 13—21.)

2 Tietosuoja-asetuksen keskeiset käsitteet ja tietosuojaperiaatteet

2.1 Tietosuoja-asetuksen keskeiset käsitteet

Tietosuoja-asetus sisältää suuren määrän käsitteitä, jotka pitäisi tietää ja ymmärtää voidakseen saada yrityksensä toiminnan ja dokumentaation asetuksen edellyttämälle tasolle (Hanninen, Laine, Rantala, Rusi, Varhela 2017,18). EU:n tietosuoja-asetus 2016/679 määrittelee 4 artiklassa käsitteet. Sen mukaan henkilötietoja ovat kaikki tunnistetut tai tunnistettavissa olevat tiedot, jotka voidaan liittää

luonnolliseen henkilöön eli rekisteröityyn henkilöön. Tällaisia tietoja ovat esimerkiksi nimi, henkilötunnus, sijaintitieto, sähköpostiosoite, yksi tai useampi tunnusomainen fyysinen, psyykkinen, sosiaalinen tms. tekijä.

Henkilötiedoilla tarkoitetaan henkilötietoja, joiden perusteella voidaan todeta, ketä ihmistä tarkoitetaan. Pelkästään suullinen tieto ei ole henkilötieto, ellei se perustu henkilörekisteriin tallennettuun tietoon. Henkilötiedon käsitteeseen sisältyy myös useampaa henkilöä koskeva tietojoukko, josta ei voida yksilöidä tiettyä luonnollista henkilöä. Henkilötiedon tunnusmerkistön täyttävät myös tiedot, joilla viitataan tiettyyn perheeseen tai yhteistaloudessa asuviin ilman, että tietoa voitaisiin yhdistää tämän rajatun joukon tiettyyn luonnolliseen henkilöön. Henkilötietojen suojan taso määritellään lailla, joka asettaa vaatimuksia muun muassa rekisterinpitäjälle tietoturvallisuuden varmistamisesta. Tietoturvallisuus on sekä periaate että käsite, jonka vuoksi kokonaisuus on vaikeasti hallittavissa. (Voutilainen 2012, 246—247 ja 37.)

Rekisteröidyllä tarkoitetaan luonnollista henkilöä, jonka henkilötietoja käsitellään. Henkilötietojenkäsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko manuaalisesti tai automattisesti. Tietojen käsittely on mm. keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista. Henkilötietojen automaattista käsittelyä kutsutaan profiloinniksi. Yritystoiminnassa profilointia käytetään markkinoinnin ja myynnin apuvälineenä. Henkilötietojen tunnistettavuuden poistamista kutsutaan anonymisoimiseksi. Tämän jälkeen henkilöä ei voida enää tunnistaa. (Hanninen ym. 2017, 20—21.) Anonymiteettisuojaan liittyy joitakin poikkeuksia sellaisissa tilanteissa, joissa asiakirjan antaminen riippuu viranomaisen harkintavallasta ja joissa oikeus saada tieto riippuu laissa määriteltyjen edellytysten täyttymisestä. Poikkeussäännöt koskevat lähinnä ei-julkisia ja salassa pidettäviä asiakirjoja samoin kuin asianosaisten julkisuus toteutuu. Asianosaisella on yleensä oikeus saada tieto salassa pidettävästä asiakirjasta, mutta viranomainen voi pyytää tiedon pyytäjältä lisäselvityksiä, kuten henkilöllisyystodistuksen. (Mäenpää 2000, 242.)

Rekisteri on mikä tahansa jäsenneltyä tietoa sisältävä tietojoukko, josta tiedot ovat saatavilla tietyillä perusteilla. Tietosuoja-asetuksen mukaan kysymyksessä on henkilötietojen käsittelystä. (Hanninen ym. 2017, 22.) Tiedonsaantioikeus asettaa tiedonhaltijalle velvollisuuden antaa tietoa silloin, kun tiedonsaantiin on olemassa lakiin säädetty peruste. Yleensä tietojenantovelvollisuus koskee tietoja, joita tiedonsaaja tarvitsee lakisääteisessä toiminnassaan välttämättömästi. (Voutilainen 2012, 41.) Rekisterinpitäjänä pidetään sellaista luonnollista tai oikeushenkilöä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Henkilötietojen käsittelijällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, jonka tehtävänä on käsitellä henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä ei päätä tietojen keräämisestä tai käyttämisestä, vaan se on rekisterinpitäjän tehtävä. Jokaisen henkilötietojen käsittelijän tulee käsitellä tietoja siten, ettei ne päädy sivullisille. Erityisesti arkaluonteisia tietoja käsiteltäessä tämä huolellisuusvelvoite korostuu, koska usein tällöin on kyse myös luottamussuhteesta henkilötietojen käsittelijän ja rekisteröidyn välillä. Tietojen vastaanottajalla tarkoitetaan luonnollista tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle henkilötiedot luovutetaan. (Hanninen ym. 2017, 22—23.)

Hyvällä tiedonhallintatavalla tarkoitetaan sitä, että viranomainen luodessaan ja toteuttaessaan tiedonhallintatapaa huolehtii asiakirjoista ja tietojärjestelmistä sekä niihin liittyvistä tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muista tekijöistä. Erityisen tärkeää on ensinnäkin pitää luetteloa tiedoista ja huolehtia, että tiedot ovat helposti löydettävissä. Toiseksi tulee laatia ja pitää saatavilla kuvaukset ylläpitämistään tietojärjestelmistä sekä niistä saatavissa olevista julkisista tiedoista. Kolmanneksi tulee selvittää tietojärjestelmien käyttöönottoa sekä hallinnollisia ja lainsäädännöllisiä uudistuksia kun valmistellaan suunniteltujen toimenpiteiden vaikutusta julkisuuteen, salassapitoon ja suojaan sekä tietojen laatuun sekä ryhtyä tarpeellisiin toimenpiteisiin. Neljänneksi tulee suunnitella ja toteuttaa asiakirja- ja tietohallintonsa, kuin myös ne tietojärjestelmät ja tietojenkäsittelyt joita ylläpitää niin, että asiakirjojen julkisuus on vaivattomasti toteutettavissa ja huolehdittava asiakirjojen asianmukaisesta arkistoinnista ja hävittämisestä. Lopuksi tulee huolehtia siitä, että työntekijöillä on tarvittava tieto käsiteltävien asiakirjojen julkisuudesta sekä tietojen

antamisesta ja käsittelystä sekä hyvän tiedonhallintatavan toteuttamiseksi annettujen säännösten, määräysten ja ohjeiden noudattamisesta. (Laki viranomaisten toiminnan julkisuudesta 621/1999 18 §.) Toimintamallia, jossa rekisteröidyn oikeudet otetaan huomioon oikeassa suhteessa, kutsutaan hyväksi henkilötietojen käsittelytavaksi. Tällä tavalla optimoidaan rekisteröidyn yksityisyyden suoja ulottamaan tietojenkäsittely vain käyttötarkoitukseensa nähden tarpeellisiin henkilötietoihin. (Voutilainen 2012, 41.)

Tietoturvaloukkauksella tarkoitetaan asetuksen mukaan siirrettyjen, tallennettujen ja muuten vahingossa tai lainvastaisesti tuhotuista sekä poistetuista tiedoista tai asiattomien pääsyä käsiksi tietoihin. (Hanninen ym. 2017, 23.) Kansallisen tietoturvaviranomaisen CERT-FI:n tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaiseminen sekä tietoturvauhista tiedottaminen. Tietojärjestelmiin kohdistuvat tietoturvaloukkaukset voivat olla moninaisia, pahimmillaan tietojärjestelmää voidaan käyttää hyväksi rikollisessa toiminnassa. Mikäli epäilee joutuneensa tietoturvaloukkauksen kohteeksi, niin kannattaa pysyä rauhallisena ja olla yhteydessä oman organisaation atk-tukeen ja palveluntarjoajaan ja CERT-FI -ryhmään sekä rikostapauksessa poliisiin. Nämä auttavat selvittämään ja korjaamaan tilanteen. Pitää myös ottaa yhteyttä organisaatioihin, joista hyökkäys on tullut sekä organisaatioihin, jonne hyökkäys on mahdollisesti edennyt. (Andreasson & Koivisto 2013, 21—22.)

Työntekijä voi ottaa yhteyttä tietosuojavastaavaan sellaisissa tapauksissa, joissa hänellä on syytä epäillä, että hänen tietojaan on urkittu. Syitä urkintaa on monia, kuten saman työpaikan tavoittelu, etulyöntiaseman tavoittelu, mustasukkaisuus tai uteliaisuus. Tällaisella toiminnalla on myös taloudellisia vaikutuksia varsinkin pienissä yrityksissä ja tapahtumat todennäköisesti vaikuttavat työpaikalla henkilöiden työtehoon ja työntekijöiden väliseen luottamukseen. Huolimatta siitä, että urkintaa tapahtuu, on työntekijöiden luottamus työpaikoilla melko suuri Euroopan komission Eurobarometri-tutkimuksen mukaan vuosilta 2003 ja 2008. (Andreasson ym. 2016, 66.)

Henkilötietojen käsittelijällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja

rekisterinpitäjän lukuun. Vastaanottaja on luonnollinen henkilö tai oikeushenkilö, virasto tai muu elin, jolle henkilötietoja luovutetaan riippumatta siitä, onko kyseessä kolmas osapuoli vai ei. Kolmannella osapuolella tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta toimielintä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää. Rekisteröidyn suostumus on mikä tahansa vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn tai toteuttaa selkeästi suostumusta ilmaisevan toimen. Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena tallennetut, siirretyt tai muulla tavalla käsitellyt henkilötiedot vahingossa tai lainvastaisesti tuhoutuvat, häviävät, muuttuvat, luovutetaan luvatta tai tietoihin voi päästä käsiksi ilman lupaa. Rekisterinpitäjän päätoimipaikka on keskushallinnon sijaintipaikka unionissa tai toimipaikka, jossa kyseiset päätökset on tehty. Henkilötietojen käsittelijän päätoimipaikka on keskushallinnon sijaintipaikka unionissa tai sellainen paikka, jossa pääasiallinen käsittely tapahtuu. Yrityksellä ymmärretään taloudellista toimintaa harjoittavaa luonnollista henkilöä tai oikeushenkilöä joka säännöllisesti harjoittaa taloudellista toimintaa. (Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.)

Käsittely tarkoittaa toimintoa tai toimintoja, jotka kohdistetaan henkilötietoihin tai henkilötietoa sisältäviin tietojoukkoihin automaattista tai manuaalista tietojenkäsittelyä käyttäen. Tällaisia toimintoja ovat esimerkiksi tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen tai tietojen luovuttaminen, levittäminen, yhteensovittaminen, poistaminen ja tuhoaminen. Tietojen käsittelyn rajoittamisella rajoitetaan niiden myöhempää käyttöä. Profilointi on mitä tahansa henkilötietojen automaattista käsittely, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä ominaisuuksia. Arvioidaan kyseisen luonnollisen henkilön työsuoritusta, taloudellista tilannetta, terveyttä, henkilökohtaisia mieltymyksiä, kiinnostuksen kohteita, luotettavuutta, käyttäytymistä, sijaintia ja liikkeitä. Pseudonymisoimisella tarkoitetaan henkilötietojen käsittelyä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn ilman, että käyttää lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä tai organisatorisia toimenpiteitä. Pseudonymisointia sovellettaessa henkilötietoihin asianomaisiin kohdistuvat riskit saattavat vähentyä sekä auttaa

rekisterinpitäjiä ja henkilötietojen käsittelijöitä noudattamaan tietosuojavelvoitteita. Pseudonymisoinnin tarkoituksena ei ole tarkoitus sulkea pois muita tietosuojatoimenpiteitä. Rekisteri on mikä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavissa tietyin perustein riippumatta siitä, onko tietojoukko keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. Rekisterinpitäjä on luonnollinen henkilö, viranomainen, virasto tai muu elin, joka yksin tai muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot (Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.)

2.2 Tietojen käsittelyn keskeiset periaatteet ja käsittelytarkoitukset

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 5 artiklasta löytyvät henkilötietojen käsittelyä koskevat periaatteet, joiden mukaan henkilötietoja käsitellään ja kerätään lainmukaisesti ja asianmukaisesti, eikä niitä käsitellä tavalla, joka ei ole tarkoituksenmukaista.Tietojen minimoinnilla tarkoitetaan sitä, että henkilötietojen tulee olla asianmukaisia, olennaisia ja tarpeellisia sitä tarkoitusta varten, kuin ne on kerätty. Täsmällisyys on sitä, että rekisterinpitäjän on huolehdittava tietojen täsmällisyydestä ja poistettava epätarkat ja virheelliset tiedot heti. Henkilötietojen läpinäkyvyydestä puhutaan silloin, kun rekisteröity saa tietoja itseään koskevasta henkilötietojen käsittelystä helposti ja ymmärrettävällä tavalla. Henkilötietoja säilytetään vain niin kauan, kuin se on tarpeellista käsittelytarkoituksen toteutumisen kannalta. Eheyttä ja luottamuksellisuutta koskeva periaate korostaa henkilötietojen käsittelyn turvallisuudesta huolehtimista. Rekisterinpitäjällä on velvollisuus osoittaa, että henkilötietojen käsittely on tietosuoja-asetuksen mukaista. Yleinen tietosuoja-asetus korostaa aiempaa lainsäädäntöä enemmän riskipohjaista lähestymistapaa, jonka keskeinen ajatus on, että rekisterinpitäjä ja henkilötietojen käsittelijä voi sovittaa henkilötietojen käsittelyn suojaamista koskevat toimenpiteet oikein suhteessa riskeihin. (HE 9/2018 vp s. 28—29.)

Tietosuojan periaatteet rajoitttavat sinänsä sallittua henkilötietojen käsittelyä vaikkapa rajoittamalla sitä, mitä tietoja saa käsitellä ja millä tavalla. Periaatteet vastaavat suurelta osin jo aiemmin voimassa olleet henkilötietojen käsittelyn periaatteita, vaikkakin niitä on jonkin verran täsmennetty uudesssa asetuksessa.

Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Läpinäkyvyyden periaate edellyttää erityisesti sitä, että rekisteröidyt saavat tiedon siitä, kuka on rekisterinpitäjä ja miksi henkilötietoja kerätään. Rekisteröidylle tulee selvittää henkilötietojen käsittelyn tarkoitus ja siihen liittyvät riskit. Kerättävät tiedot tulee olla olennaisia ja asianmukaisia ja tietojen tulee olla helposti rekisteröityjen saatavilla. Toisaalta henkilötietojen tulee olla riittäviä, mutta niiden tulee rajoittua käytttötarkotukseen. Henkilötiedot tulee aina kerätä asianmukaisen suostumuksella ja niitä tulee käyttää vain siihen tarkoitukseen, joihin rekisteröity on antanut suostumuksensa. (Hanninen ym. 2017, 47—49.)

Henkilötietoja tulee säilyttää mahdollisimman lyhyen ajan. Tietoja on mahdollista säilyttää kauemmin, jos rekisteröityä ei ole mahdollista tunnistaa esimerkisi silloin kun tarkastellaan ostoshistoriasta jonkun tietyn artikkelin kysyntää. Tiedot tulee myös suojata luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Rekisterinpitäjän on pystyttävä osoittamaan että tietosuojaperiaatteita on noudatettu kaikissa tietojenkäsittelyn vaiheissa. Tämä on olennainen muutos, sillä aiemman sääntelyn aikaan oli riittävää, että säännöksiä noudatetaan eikä erityistä dokumentointivelvoitetta ollut. Yrityksen tulee laatia omat sisäiset tietosuojaperiaatteensa ja kirjata ylös kaikki tietosuoja käytäntönsä ja koota kaikki tietosuojaa koskevat dokumentit ja selosteet siten, että ne ovat helposti löydettävissä ja että niiden avulla voidaan muodostaa kokonaiskuva yrityksen henkikötietojen käsittelystä ja tietosuojasta. (Hanninen ym. 2017, 49—51.)

Henkilötietojen käsittely on lainmukaista, jos rekisteröity on antanut suostumuksensa, käsittely on tarpeen sopimuksen täytäntöönpanemiseksi, lakisääteisen velvoitteen noudattamiseksi, toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi, yleistä etua koskevan tehtävän suorittamiseksi tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 artikla 6.) Rekisteröity voi antaa luvan henkilötietojensa käsittelyyn silloin, kun käyttötarkoitus on ennalta määritelty johonkin tiettyyn tarkoitukseen ja on lain mukaista. Kun henkilötietojen käsittelytarkoitus muuttuu, niin rekisterinpitäjän on pyydettävä uusi suostumus henkilötietojen käsittelyä

varten. Rekisteröidyllä on oikeus päättää, mihin käyttötarkoitukseen hänen henkilötietojaan saa käyttää, joten rekisterinpitäjän on yksilöitävä käyttötarkoitus, johon tiedot kerätään. (Tietosuojavaltuutetun toimisto 2018.)

Suostumuksen antamisen pitää olla vapaaehtoista eikä suostumisesta kieltäytymisestä saa aiheutua haitallisia seuraamuksia. Suostumisen antamisen ja perumisen tulee olla yhtä helppoja. Rekisterinpitäjän pitää pystyä osoittamaan, että hän on saanut suostumuksen rekisteröidyltä henkilötietojen käsittelyyn. Suostumus on yksiselitteinen ja selkeä tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Rekisteröidyn tulee toisin sanoen antaa tietoisesti lupa omien henkilötietojen käsittelyyn. Tähän tarkoitukseen eivät käy rasti ruutuun -periaate eikä se, että jotain jättää tekemättä tai vaikenee. Rekisterinpitäjän tulee esittää pyyntö selvästi erillään muista asioista, selkeästi niin, että rekisteröity ymmärtää sen helposti. Nimenomaista suostumusta tarvitaan esimerkiksi silloin, kun käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja (kuten terveystiedot tai etninen tausta). (Tietosuojavaltuutetun toimisto 2018.)

Huolimatta siitä, että yhteiskunta on kehittynyt ja digitalisoitunut, henkilötietodirektiivissä todetut henkilötietojen käsittelyä koskevat yleiset periaatteet ovat edelleen päteviä. Vastaavista henkilötietojen käsittelyä koskevista periaatteista säädetään myös yleisessä tietosuoja-asetuksessa. Henkilötietojen käsittelyä koskevia keskeisiä periaatteita ovat käyttötarkoitussidonnaisuus ja tietojen minimointi. Tarkoitussidonnaisuus tarkoittaa sitä, että henkilötietojen tulee olla asianmukaisia, eikä kerättyjä henkilötietoja saa myöhemminkään käyttää muihin tarkoituksiin, kuin ne on kerätty. (Tietosuojavaltuutetun toimisto 2018.)

2.3 Tietosuojavastaavan rooli

Tietosuoja-asetukseen valmistauduttaessa tulee selvittää, tarvitaanko organisaatioon nimittää tietosuojavastaava, miten organisaatiossa käsitellään henkilötietoja sekä millä perusteella henkilötietoja käsitellään. Henkilötietojen käsittelyn riskit tulee määritellä ja suoritetaan tarpeelliset toimenpiteet niiden ehkäisemiseksi. Organisaation tulee myös selvittää, miten tietosuoja-asetuksessa määriteltyjä

rekisteröityjen oikeuksia noudatetaan ja päivittää ne vaatimusten mukaisiksi. Tietoturvasta on huolehdittava ja ilmoitettava tapahtuneista tietoturvaloukkauksista. Organisaation tulee varmistaa, että toimeksiantosopimukset vastaavat asetuksessa säädettyjä ehtoja tilanteissa, joissa henkilötietojen käsittelyyn liittyviä tehtäviä on ulkoistettu. Organisaation toimiessa usean EU:n jäsenmaan alueella tulee määritellä johtava valvontaviranomainen. Lasten erityisasema tulee selvittää. Suomessa ikäraja ei ole vielä selvillä, mutta se tulee olemaan vähintään 13 ja enintään 16 vuotta. (Tietosuojavaltuutetun toimisto 2018.)

EU:n yleisen tietosuoja-asetuksen mukaan yritysten tulee nimittää tietosuojavastaava, jos yrityksen päätoiminnassa seurataan henkilötietoja laajasti tai yritys käsittelee arkaluonteisia tietoja. Johdon tehtävänä on varata tietosuojatyöhön tarpeelliset resurssit, kuten työaika-, kouluttautumis- ja työvälineresurssit. Tietosuojavastaavan tehtävät määritellään kirjallisesti ja näistä tehtävistä informoidaan yrityksen koko organisaatiota, jotta kaikille olisi selvillä yhteyshenkilö johon voi ottaa yhteyttä, mikäli operatiivisessa toiminnassa tai henkilötietojen käsittelyssä on epäselvyyksiä tai osaamisen puutteita. (Andreasson ym. 2016, 13—14.) Tietosuojavastaava käsittelee ja ratkaisee henkilötietojen käsittelyä koskevat asiat siten, kuin ne henkilötietolaissa säädetään sekä hoitaa laeista johtuvat tehtävät. Tietosuojavaltuutetun ensisijaiset tehtävät ovat rekisterinpidon lainmukaisuuden varmistaminen, hyvän tietojenkäsittelytavan kehittäminen ja tietosuojaloukkausten ehkäisy. Rekisterinpitäjät ja rekisteröidyt voivat pyytää ohjeita ja neuvoja tietosuojavaltuutetulta. Mikäli rekisterinpitäjä jättää noudattamatta ohjeita, tietosuojavaltuutettu voi saattaa lainvastaiseksi arvioimansa menettelyn tietosuojalautakunnan käsittelyyn. Tietosuojavaltuutettu valvoo ennakolta henkilötietojen käsittelyä ja on kuultavana sekä antaa lausuntoja viranomaisille, syyttäjille ja tuomioistuimille. Tietosuojavaltuutetun tehtäviin kuuluu myös herättää yleistä keskustelua ja jakaa informaatiota kansalaisille, viranomaisille ja muille rekisterinpitäjille. Tietosuojeluvaltuutetun toimisto toimii kansainvälisessä yhteistyössä sekä EU:ssa, että pohjoismaisella tasolla. (Tietosuojavaltuutetun toimisto. 2013).

3 Henkilötietojen käsittely asiakassuhteessa

3.1 Asiakassuhde ja siihen liittyvä tietojen käsittely

Asiakkaiden tarpeet, toiveet ja tyytyväisyys ovat markkinoinnin keskeinen lähtökohta. Markkinoinnin keskeinen tavoite on asiakassuhteen luominen ja ylläpitäminen. Asiakkaan ostaessa useita kertoja samalta myyjältä, puhutaan asiakassuhteesta. Asiakastietokantoihin kerätään tietoja asiakkaiden taustoista, ostoista, vaikuttimista jne. Markkinointiohjelmat suunnitellaan eri asiakasryhmille erikseen, jolloin on kyse asiakassuhdemarkkinoinnista. Pienyrityksille on tähdellistä löytää oma asiakaskunta ja tunnistaa sen tarpeet. Pienen yrityksen kilpailukeino on se, että asiakkaat kokevat yrityksen palvelut ylivoimaisiksi ja houkutteleviksi. Pienyritykselle saattaa olla parasta keskittyä yhteen tai kahteen asiakasryhmään. (Bergström & Leppänen 1997, 10—12, 18.)

Yrityksellä voi olla asiakkainaan eri ikäisiä sekä koulutukseltaan ja ammatiltaan erilaisia asiakkaita, jotka suhtautuvat yritykseen ja sen tuotteisiin toisistaan poikkeavin tavoin. Asiakkaat jaetaan kahteen eri ryhmään; potentiaalisiin ja ostaneisiin asiakkaisiin. Yritys voi segmentoida eli ryhmitellä asiakkaat, joita se tavoittelee keskenään erilaisiin asiakasryhmiin jonkinlaisen tietyn kriteerin mukaan. Aluksi selvitetään tavoitteet ja potentiaaliset asiakkaat, jonka jälkeen määritetään lohkomisperusteet ja jaetaan markkinat segmentteihin. Seuraavaksi valitaan markkinoinnin kohderyhmät, minkä jälkeen päätetään markkinointitapa. Lopuksi toteutetaan markkinointi ja seurataan tuloksia. (Lahtinen, Isoviita & Hytönen 1996, 20—22.) Tärkeintä on luoda pitkäaikaisia, luottamuksellisia ja kannattavia asiakassuhteita, joissa molemmat osapuolet ovat tyytyväisiä. Osapuolet voivat vaihtaa keskenään lupauksia ja molemmat osapuolet ovat tyytyväisiä, kun lupaukset pidetään. (Lahtinen & Isoviita 1994, 2.)

Henkilötietojen käsittely perustuu Euroopan parlamentin ja neuvoston asetukseen (EU) 2016/679, joka käsittelee luonnollisten henkilöiden suojelua henkilötietojen käsittelyssä sekä näiden tietojen vapaata liikkuvuutta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Euroopan parlamentin ja

neuvoston asetuksen (EU) 2016/679 mukaan luonnollisten henkilöiden suojelu henkilötietojen käsittelyssä on perusoikeus riippumatta heidän kansalaisuudestaan tai asuinpaikastaan. Luonnollisten henkilöiden henkilötietojen käsittelyä koskevien perusoikeuksien ja -vapauksien suojelua on tarkoitus suojella ja varmistaa henkilötietojen vapaa liikkuvuus jäsenvaltioiden välillä. Henkilötietojen käsittelyn suunnitteluvaiheessa tulee ottaa huomioon, että se palvelee ihmistä. Uusia haasteita henkilötietojen käsittelyyn on luonut teknologian nopea kehitys. Henkilötietojen käsittelyn tulisi olla laillista ja asianmukaista. Luonnollisten henkilöiden tulisi tietää, mihin heidän henkilötietojaan kerätään ja käytetään. Henkilötietoja tulisi käyttää vain siihen tarkoitukseen, johon ne on alun perin kerätty. Henkilötietojen rajoittavia menetelmiä voivat olla muun muassa valittujen tietojen siirtäminen toiseen käsittelyjärjestelmään, käyttäjien pääsyn estäminen valittuihin henkilötietoihin tai julkaistujen tietojen väliaikainen poistaminen verkkosivustolta. Järjestelmässä on ilmaistava selvästi henkilötietojen käsittelyn rajoittamisesta.

Pitkänen ym. (2013, 111—115) ovat todenneet, että arkaluonteisten tietojen käsittely on henkilötietolain perusteella kielletty. Tällaisia tietoja ovat muun muassa rotu tai etninen alkuperä, uskonnollinen vakaumus, rikollinen teko, henkilön terveydentila tai sairaus sekä seksuaalinen suuntautuminen. Arkaluonteisia tietoja voidaan kuitenkin käyttää, jos se on katsottu olevan rekisterinpitäjän tehtävien ja toiminnan kannalta välttämätöntä. Käytännössä on usein tilanteita, joissa on hankala päätellä, onko jokin henkilötieto arkaluonteinen vai ei. Esimerkiksi terveydenhuollon puolella tulee tällaisia tapauksia säännöllisesti vastaan. Arkaluonteisia tietoja siirrettäessä rekisteristä toiseen tulee huolehtia, että molemmat rekisterit täyttävät arkaluonteisten tietojen käsittelyn kriteerit.

Perusoikeuksia, kuten yksityiselämänsuojaa sekä muuta yksityisyyden suojaa turvataan henkilötietolain (523/1999) 1 §:ssä. Tietosuojalailla on tarkoitus täydentää ja täsmentää Euroopan unionin yleistä tietosuoja-asetusta ja sillä kumotaan henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Näissä laeissa säädellään henkilötietojen käsittelyn oikeusperusteesta ja erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyssä joissakin tilanteissa. Sellaisiin tilanteisiin, kuten henkilötietojen käsittelyyn oikeusperusteen säilyttämiseksi tietyissä tilanteissa tai tieteellisen tutkimuksen edellytysten säilyttämiseksi

nykyisellään niin pitkään kuin mahdollista. Ehdotettu tietosuojalaki täydentää EU:n tietosuojalakia eli niitä tulee lukea rinnakkain. (HE 9/2018 s. 4— 5).

3.2 Rekisteröityjen henkilöiden informointi

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 12 artiklan mukaan rekisterinpitäjän velvollisuus on toimittaa tiedot rekisteröidylle tiiviissä, läpinäkyvässä sekä helposti ymmärrettävässä ja saatavilla olevassa muodossa. Tiedot toimitetaan kirjallisesti tai muulla tavoin ja tapauksesta riippuen sähköisessä muodossa. Rekisterinpitäjän tehtävänä on helpottaa 15—22 artiklan mukaisten rekisteröidyn oikeuksien toteutumista. Rekisterinpitäjän tulee toimittaa tiedot toimenpiteistä, joihin on ryhdytty viivyttelemättä ja yleensä viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Kaikki tiedot ja toimenpiteet ovat pääsääntöisesti maksuttomia.

Yrityksellä on rekisterinpitäjän roolissa velvollisuus informoida avoimesti henkilötietojen käsittelystä ennen käsittelytoimien aloittamista. Tietosuoja-asetuksen määräämiä tietoja on rekisteröidyn pyynnöstä toimitettava tiiviisti esitettynä, läpinäkyvästi, helposti ymmärrettävässä ja helposti saatavilla olevassa muodossa sekä selkeällä ja yksinkertaisella tavalla. Tiedot tulee toimittaa kirjallisesti tai muulla tavoin ja tapauksesta riippuen sähköisessä muodossa. Asetuksen mukaan voidaan informoida myös informointivideon, virtuaalitodellisuuden toteutusten tai kuvien avulla. Tärkeintä on, että viesti on rekisteröidylle selkeä ja ymmärrettävä. (Pitkänen, Tiilikka & Warma 2013, 107—108.)

Rekisteriseloste antaa tietoa rekisteröidylle ja se edellyttää rekisterinpitäjältä suunnitelmallisuutta. Rekisteriselostetta laadittaessa tulee pohtia mm. sitä mihin tarkoitukseen henkilörekisteriä kerätään, rekisterin tietoturvaa ja ryhmää joka rekisteröidään. Ilman rekisteriselostetta rekisteröidyn on lähes mahdoton selvittää mihin tarkoituksiin hänen henkilötietojaan käytetään. Rekisteriselosteella turvataan henkilötietojen käsittelyn avoimuus. Jokaisesta henkilörekisteristä on laadittava oma rekisteriselosteensa ja sen pitää olla kaikkien saatavilla. Rekisteriselosteeseen tulee laittaa esimerkiksi rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot, henkilötietojen käsittelyn tarkoitus, kuvaus

rekisteröityjen ryhmästä, mihin tietoja säännönmukaisesti luovutetaan sekä kuvaus rekisterin suojauksen periaatteista. Tietosuojavaltuutetun laatimaa tietosuojaselostetta voidaan kuvata laajennetuksi rekisteriselosteeksi. Siinä kuvataan rekisteriselosteessa mainittujen tietojen lisäksi rekisteröidylle kuuluvat oikeudet eli tarkastusoikeus, oikeus vaatia virheellisen tiedon oikaisemista ja kielto-oikeus. (Pitkänen, Tiilikka & Warma 2013, 107—108, 110.)

Yrityksen on laadittava tietosuoja-asetuksen mukaiset selosteet käsittelytoimista viranomaisia varten. Rekisteröidylle on annettava tarpeelliset tiedot, kuten esim. yrityksen identiteetti ja yhteystiedot, henkilötietojen vastaanottaja ja henkilötietojen säilytysaika. Henkilötietojen käsittelijä käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti. Tämä merkitsee käytännössä sitä, että rekisterinpitäjän tulee antaa kirjalliset ohjeet. Ne henkilöt, joilla on oikeus käsitellä henkilötietoja, eivät saa antaa tietoja kolmannelle osapuolelle ilman rekisteröidyn suostumusta, koska heitä koskee lakisääteinen salassapitovelvollisuus. (Hanninen ym. 2017 82—85.) Informointi saattaa olla tehotonta, jos suostumukselle asetetut edellytykset eivät ole täyttyneet. (Voutilainen 2012, 246.)

3.3 Rekisteröityjen henkilöiden oikeudet

Euroopan parlamentin ja neuvoston 2016/679 asetus 16—20 artiklojen mukaan rekisteröidyllä on oikeus vaatia, että häntä koskevat virheelliset tiedot oikaistaan tai että tiedot poistetaan rekisteristä. Rekisteröidyllä on oikeus siihen, että hänen henkilötietojen käsittelyä rajoitetaan mm., jos ne eivät pidä paikkaansa tai käsittely on lainvastaista.

Rekisteröidyn oikeuksien lujittuminen on yksi tietosuoja-asetuksen tavoitteista. Yleisen tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus siirtää tietojaan järjestelmästä toiseen silloin kun henkilötietoja käsitellään suostumuksen tai sopimuksen perusteella. Rekisteröidyllä on oikeus saada tiedot lähtökohtaisesti sähköisesti. Tietosuoja-asetuksessa on kiinnitetty erityistä huomiota lapsen asemaan, joka ilmenee muuan muassa ikärajan kautta. Kun henkilötietojen käsittelyn

kohteena on lapsi, tulee informaation olla niin selkeää, että asianomainen itse sen käsittää. (HE 9/2018 s.30)

Rekisteröidyllä on oikeus saada korvausta, jos vahinko on johtunut asetuksen rikkomisesta. Rekisteröidyllä on oikeus valittaa valvontaviranomaisen päätöksestä. Suomessa tietosuojavaltuutetun päätöksestä valitetaan hallinto-oikeuteen. (HE 9/2018 s. 30) Rekisteröidyllä on oikeus vaatia, että yritys oikaisee häntä koskevat epätarkat ja virheelliset tiedot, mutta tietojen oikaisussa pitää ottaa huomioon tietojenkäsittelyn tarkoitukset. Rekisteröidyllä on oikeus pyytää yritystä poistamaan häntä koskevat tiedot yrityksen rekisteristä. Henkilötiedot voi pyytää poistamaan, kun niitä ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin. Asiakkaalla on oikeus tulla unohdetuksi esim. jostain kanta-asiakasjärjestelmästä tai kieltää suoramarkkinointi. Mikäli yritys käsittelee lainvastaisesti työntekijöidensä henkilötietoja, tiedot tulee poistaa rekisteröidyn pyynnön perusteella. Suoraan lapsilta kerätyt henkilötiedot voidaan myöhemmin poistaa. (Hanninen ym. 2017, 60–62.)

Tietosuoja-asetuksessa säädetään nykyään aiempaa yksityiskohtaisemmin rekisteröityjen oikeuksista ja lisäksi uusia rekisteröityjen oikeuksia on säädetty. Ohjeistuksen ja menettelyn tulee olla sellaisia, että rekisteröity voi käyttää oikeuksiaan suhteellisen helposti. Ohjeet voi laittaa internetsivustolle tai yrityksen sisäiselle intrasivustolle. Suunniteltaessa rekisteröintiä tulee varmistaa, että rekisteröity voi oikeuksiaan käyttää. Käytännössä oikeuksien käyttö hoidetaan yrityksen verkkosivuilla olevan omat tiedot -osion kautta, johon rekisteröity kirjautuu omilla tunnuksilla. Rekisteröidyn on mahdollista tulla myös henkilökohtaisesti yritykseen paikan päälle, jolloin hänen on todistettava henkilöllisyytensä. Mikäli pyyntö herättää epäilyksiä tai on puutteellinen eikä rekisteröity toimita tarpeellisia lisätietoja, yritys voi kieltäytyä toimimasta rekisteröidyn pyynnön mukaisesti. (Hanninen ym. 2017, 56–58.)

Rekisteröidyn oikeudet ovat pääsääntöisesti samat EU:n yleisessä tietosuoja-asetuksessa ja Suomessa jo aiemmin käytössä olevassa lainsäädännössä. Tämä tarkoittaa esim. sitä, että henkilöllä on edelleen oikeus tarkistaa itseään koskevat tiedot ja rekisterinpitäjän on oikaistava virheelliset tiedot sekä

poistettava tarpeeton tai virheellinen tieto. EU:n yleisen tietosuoja-asetuksen mukaan henkilöllä on oikeus saada omat tietonsa kokonaan poistettua eli tulla unohdetuksi. Tämän jälkeen tiedot hävitetään turvallisesti. Rekisteröity voi saada itseään koskevia tietoja sähköisesti ja siirtää jo antamansa tiedot järjestelmästä toiseen. Asiakkaiden luottamus tukee organisaation toimintaa ja tietosuojasta ei puhuta enää esteenä vaan mahdollistajana. Organisaation menestymisen kannalta on tärkeää riskien minimointi, hyvä maine sekä kuluttajien luottamuksen säilyminen. (Andreasson ym. 2016, 12—13.)

3.4 Tietojen käsittelyn perusteet

Euroopan neuvoston yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (ETS nro 108, tietosuojayleissopimus) oli ensimmäinen oikeudellisesti sitova instrumentti, joka koski kansainvälistä henkilötietojen suojaa. Euroopan neuvosto hyväksyi tietosuojayleissopimuksen vuonna 1981. Yleissopimusta sovelletaan automaattiseen henkilötietojen käsittelyyn koskien kaikkea henkilötietojen käsittelyä. Yleissopimus on ollut mallina myös henkilötietodirektiiville ja sen nojalla on annettu lukuisia henkilötietojen käsittelyä koskevia suosituksia. Yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR) tuli voimaan kaikissa EU:n jäsenvaltioissa 25.5.2018. Tietosuoja-asetuksella kumotaan vuonna 1995 annettu henkilötietodirektiivi ja yleistä tietosuoja-asetusta sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn. Lainsäädäntömuutoksella on pyritty yhdenmukaistamaan, vahvistamaan ja saattamaan ajan tasalle eurooppalaista henkilötietojen suojaa koskevaa lainsäädäntöä sekä vahvistamaan sisämarkkinoita. Asetus tulee sellaisenaan voimaan kaikissa jäsenvaltioissa, toisin kuin direktiivi joka edellyttää kansallista täytäntöönpanevaa lainsäädäntöä. (HE 9/2018 s.25—27.)

Tietosuojalain tarkoituksena on täsmentää ja täydentää yleistä tietosuoja-asetusta. Koska yleinen tietosuoja-asetus on kansallisesti suoraan sovellettavaa lainsäädäntöä, sillä voidaan vain täsmentää asetusta yleisessä tietosuoja-asetuksessa annetun kansallisen liikkumavaran puitteissa. Tietosuojalakia ei sovellettaisi sellaiseen henkilötietojen käsittelyyn, josta säädetään henkilötietojen

käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (xx/2018), jolla on tarkoitus panna täytäntöön Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaisen viranomaisen suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimusta, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta. (HE 9/2018 vp s.75–76.)

Euroopan unionin perusoikeuskirja takaa jokaiselle oikeuden vapaasti vastaanottaa ja välittää tietoja. EU on säätänyt direktiivejä, jotka täsmentävät viestinnän suojaa ja rekisteröidyn henkilötietojen suojaa, määrittelevät oikeuksien sisältöä ja jäsenmaiden velvoitteita ja menettelytapoja. EU valmisteli kansalaisten tietosuojaa parantavaa tietosuoja-asetusta neljä vuotta, koska se piti digitaalisia markkinoita Euroopalle tärkeinä. Asetuksella pakotetaan palveluntarjoajat huomioimaan teknisissä ratkaisuissaan henkilötietojen käsittely. (Pesonen 2017, 43—52.)

Euroopan parlamentin ja neuvoston asetus 2016/679 1 artiklan mukaan jäsenvaltioiden on suojeltava luonnollisten henkilöiden perusoikeuksia ja -vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan ja varmistettava, jos unionin oikeudessa tai jäsenvaltioiden lainsäädännössä edellytetään toimivaltaisten viranomaisten välistä henkilötietojen vaihtoa, ettei tällaista vaihtoa rajoiteta eikä kielletä syistä, jotka liittyvät luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä. Tietoihin pääsyä voidaan rajoittaa EU 2016/679 asetus 18 artiklan mukaan rekisteröidyllä on oikeus siihen, että rekisterinpitäjä rajoittaa käsittelyä, jos henkilötiedot eivät pidä paikkaansa, käsittely on lainvastaista tai henkilötietoja ei enää tarvita käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Lainvalmistelussa on huomioitava tietosuoja, kun sääntelykohteena on ovat henkilötiedot ja niiden käsittely. Erityisesti on kiinnitettävä huomiota henkilötietojen rekisteröinnin tavoitteeseen, rekisteröitävien henkilötietojen sisältöön, niiden sallittuihin käyttötarkoituksiin, tietojen luotettavuuteen sekä siihen, miten pitkään henkilötietoja säilytetään rekisterissä ja rekisteröidyn oikeusturvaan. (Voutilainen

2012, 41—42.) Henkilötietojen käsittelyssä yksityisyyden suoja muodostuu perusoikeuksista, joita henkilötietojen suojan lisäksi ovat muun muassa yksilön itsemääräämisoikeus, oikeus yksityiselämään, oikeus kunniaan, oikeus ihmisarvoiseen kohteluun sekä oikeus itseään koskeviin asioihin. Henkilön asioidessa viranomaisen kanssa, hän lähtökohtaisesti olettaa, että hänen henkilötietojensa käsittelyyn on lainmukaiset perusteet. Ellei lakisääteisiä perusteita ole, viranomaisen on pyydettävä rekisteröidyltä suostumus henkilötietojen käsittelyyn. (Voutilainen 2012, 51—52.)

Henkilötunnuksen käsittelylle on asetettu erityisiä vaatimuksia. Kaikki yritykset eivät voi kerätä asiakkaidensa henkilötunnuksia. Henkilötunnuksen tehtävä on yksiselitteisesti yksilöidä henkilö muista saman nimisistä, jotka mahdollisesti ovat samana päivänä syntyneetkin. Henkilötunnuksen keräämisen perusteeksi ei riitä se, että sen käyttö helpottaisi tai nopeuttaisi yrityksen henkilötietojen käsittelyä. Yritys saa käsitellä henkilötunnusta ainoastaan silloin, kun asiakas on antanut siihen yksiselitteisen suostumuksensa tai jos rekisteröidyn yksiselitteinen yksilöinti on tärkeää rekisteröidyn ja rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi. Henkilötunnusta saa lisäksi käsitellä muun muassa luotonannossa, vakuutustoiminnassa, terveydenhuollossa ja sosiaalihuollossa. Lakiluonnoksen mukaan henkilötunnuksen käsittelyn perusteet ovat jatkossakin samat kuin ennen. (Hanninen ym. 2017, 44—45.)

Markkinointi on eräs syy, miksi henkilötietoja kerätään. Yrityksen tulee kiinnittää huomiota siihen, millaisia henkilötietoja se tarvitsee markkinoimiseen, koska määrittely asettaa rajat sille, mitä tarkoituksia varten henkilötietoja voidaan myöhemmin käsitellä. Henkilötietojen käsittelyä varten tulee olla rekisteröidyn yksiselitteinen suostumus, joka käytännössä kannattaa olla kirjallinen, koska rekisterinpitäjällä on velvollisuus tarpeen tullen näyttää suostumus toteen. Yritys voi käyttää asiakasrekisterissään olevia asiakkaiden henkilötietoja markkinointiin. Voidakseen käsitellä henkilötietoja yrityksellä tulee olla asiakkaan suostumuksen lisäksi myös asiallinen yhteys asiakkaaseen. Yrityksen tulee laatia rekisteriseloste jokaisesta henkilörekisteristään. Yrityksen on markkinoinnissaan merkittävä osoitelähde näkyviin silloin, kun henkilötiedot on hankittu henkilörekisteristä. Jokaisella on oikeus tarvittaessa saada tietää, mitä tietoja hänestä on henkilörekisteriin

tallennettu, tai saada tietää, ettei häntä koskevia tietoja ole rekisterissä. Rekisteröidyllä on oikeus kieltää käyttämästä henkilötietojaan markkinoinnissa. Sähköistä suoramarkkinointia saa kohdentaa vain sellaisille luonnollisille henkilöille, jotka ovat etukäteen antaneet siihen luvan. Yhteystietoja hankittaessa ja jokaisen markkinointiviestin yhteydessä pitää ilmoittaa selvästi mahdollisuudesta kieltää kyseinen sähköinen markkinointi. (Paloranta 2008, 121–131.)

Suoramarkkinoinnissa henkilötietoja käytetään tietyille henkilöille tai kotitalouksille, jotka ovat tarkoitusta varten valittu esimerkiksi harrastuksensa vuoksi. Henkilötietoja voidaan käyttää markkinointiviestin perille toimittamiseen ja markkinointiviestin sisällön muotoilemiseen. Suoramarkkinoinnissa käytettävät henkilötiedot saadaan tavallisesti henkilöltä itseltään, ulkopuolisesta rekisteristä, muusta laillisesta lähteestä tai omista henkilörekistereistä. Tavallisesti yritys kerää henkilötietoja lisäksi esimerkiksi arvontaan tai kilpailuun osallistuneilta henkilöiltä. Suoramarkkinointikampanjaan osallistuu useimmiten monta eri tahoa, kuten markkinoija, mainostoimisto, osoitepalvelu- ja postitusyritykset. (Tietosuojavaltuutetun toimisto 2018.) Suoramarkkinointi on yksi markkinoinnin keino, jolla tarkoitetaan kokonaisvaltaista markkinointijärjestelmää, jossa käytetään yhtä tai useampaa mainosvälinettä ja saadaan aikaan runsaslukuinen palaute tai merkittävä muutos missä tahansa myyntipisteessä. Suoramarkkinointiin sisältyy viesti myyjältä asiakkaalle ja palaute asiakkaalta myyjälle. (Lahtinen & Isoviita 1994, 122—123.)

3.5 Henkilötietojen käsittelijän ja rekisterinpitäjän roolit ja vastuut

Rekisterinpitäjän ja henkilötietojen käsittelijän roolit ja vastuut määräytyvät tosiasiallisen aseman perusteella, eikä rooleista voi sopia toisin. Kunkin käsittelytilanteen rooli määräytyy sen mukaa, mikä taho määrittelee sitä, miten henkilötietoja käsitellään ja mitkä ovat käsittelyn tarkoitukset ja keinot. Lopullinen vastuu henkilötietojen käsittelyssä on aina rekisterinpitäjällä. Hänen onkin järkevää valita sopimuskumppani, joka huolehtii asianmukaisesti tietosuoja- ja tietoturvavaatimusten noudattamisesta. Tietosuoja-asetuksen myötä henkilötietojen käsittelijän vastuut kasvavat merkittävästi ja hänen on huomioitava tarkasti roolinsa rajat. (Hanninen ym. 2017, 24–28.)

Rekisterinpitäjä on vastuussa useista velvollisuuksista, koska hänen vastuualueensa on laaja lainsäädännön mukaan. Rekisterinpitäjä vastaa siitä, että rekisterissä olevien henkilöiden tietoja käsitellään lainsäädännön mukaisesti. Rekisteriselosteen laadinta kuuluu rekisterinpitäjän tehtäviin. Rekisteriseloste tulee laatia hyvin ja pitää se aktiivisesti esillä, jotta kohderyhmien luottamus kasvaa markkinoijaa kohtaan. Toiminnan tavoitteena on henkilötietojen käsittelyyn liittyvien kysymysten ja reklamaatioiden väheneminen. (Koivumäki & Häkkänen 2017, 170—173.)

Rekisterinpitäjän tulee käsitellä tietoja huolellisesti, joka tarkoittaa muun muassa hyvää tietojenkäsittelytapaa, sisäisten toimintaohjeiden laadintaa, vaitiolovelvollisuutta, suojaustoimia, tilojen asianmukaista lukitsemista ja henkilötietoja sisältävien tiedostojen ja asiakirjojen tietoturvallista tuhoamista. Markkinoijan tulee suunnitella etukäteen vähintään henkilötietojen käsittelyn tarkoitukset, henkilötietojen säännönmukainen hankintapaikka sekä säännönmukainen luovutuskohde. Tärkeintä on suunnitella tietojenkäsittelyn koko elinkaari rekisterin perustamisesta sen loppuun saakka. (Koivumäki & Häkkänen 2017, 173—175.)

Henkilötietoja saa käsitellä vain tavalla, joka on yhteensopiva kyseisen rekisterin määritellyn käyttötarkoitusten kanssa. Henkilötietojen käsittelyn tulee olla tarpeellisia määritellyn käsittelyn tarkoituksen kannalta. Henkilötiedot ovat silloin tarpeellisia käsittelyn kannalta, kun ne ovat asianmukaisia ja olennaisia, mutta eivät liian laajoja käsittelytarkoitukseen. Rekisterinpitäjän on huolehdittava, ettei virheellisiä, vanhentuneita tai epätäydellisiä tietoja ei käsitellä. Rekisterinpitäjällä on myös informointivelvollisuus, jonka tavoitteena on antaa rekisteröidyille tietoja heitä koskevasta tietojen käsittelystä sekä siitä, että käsittely on mahdollisimman avointa. Uuden asiakassuhteen perustamisen yhteydessä on suositeltavaa antaa hyvin valmisteltu ja selkeä informaatiopaketti asiakastietojen käsittelystä muiden yrityksen toimintatavoista kertovien esitteiden mukana. (Koivumäki & Häkkänen 2017, 176—178.)

3.6 Henkilötietojen luovuttaminen ja sanktiot

Rekisteröidyllä on oikeus tehdä valitus yhdelle valvontaviranomaiselle, jos hänen mielestään häneen liittyvässä henkilötietojen käsittelyssä on rikottu säännöksiä. Rekisteröity voi pyytää lisäapua valituksen tekemisen ja hänellä on oikeus saada viranomaiselta tietoa valituksen etenemisestä ja ratkaisusta. Rekisteröidyllä on oikeus saada korvauksia aiheutuneista vahingoista. Seuraamusten pitää olla tehokkaita, oikeasuhteisia ja varoittavia. (Euroopan parlamentin ja neuvoston direktiivi EU 2016/680 artiklat 52—57.) Vakuutusyhtiöt tarjoavat erilaisia tietoturvaan liittyviä tuotteita, joita yritys voi harkintansa mukaan käyttää. Vakuutus ei kuitenkaan tarkoita sitä, että rekisterinpitäjä voisi suhtautua välinpitämättömästi tietoturvaan. Usein inhimillinen erehdys on syynä tietoturvauhkaan tai tietoturva rikkeeseen. (Andreasson ym. 2017, 140—141.)

Rekisteröityjen tiedot voidaan rekisterinpitäjän toimesta siirtää kolmansille osapuolille joko käsiteltäviksi taikka niin, että tiedot vastaanottaneesta kolmannesta osapuolesta tulee tietojen rekisterinpitäjä. Tämäntyyppistä luovuttamista tapahtuu esimerkiksi silloin, kun työntekijän palkkatietoja luovutetaan verottajalle verotusta varten tai muulle viranomaiselle. Henkilötietoja voidaan luovuttaa vain siinä tapauksessa, jos sekä luovuttajalla että luovutuksensaajalla on laillinen peruste henkilötietojen käsittelyyn. Tietojen luovuttamisesta on asianmukaista tehdä luovutussopimus oikeutettujen etujensa saamiseksi. Tietosuoja-asetuksen keskeinen periaatteena on henkilötietojen siirtäminen ainoastaan asetuksessa mainittujen edellytyksien puitteissa. Valvontaviranomaisella on laajat tutkintavaltuudet, joihin kuuluu oikeus määrätä rekisterinpitäjät ja henkilötietojen käsittelijät antamaan tiedot, oikeus toteuttaa tarkastuksia ja oikeus saada tarvittavat tiedot, oikeus toteuttaa tarkastuksia ja oikeus saada pääsy henkilötietoihin sekä rekisterinpitäjän ja -käsittelijän tiloihin. Valvontaviranomainen voi antaa varoituksia, huomautuksia ja määräyksiä varmistaakseen sen, että yritykset noudattavat tietosuoja-asetuksia. Hallinnollisten sakkojen määrääminen on näistä merkittävämpiä sekä henkilötietojen väliaikainen tai pysyvä rajoittaminen. (Hanninen ym. 2017, 93—95, 124.)

4 Pohdinta

Henkilötietojen perusteet ulottuvat kauas historiaan ja niitä on päivitetty moneen kertaan erilaisten lakien avulla. Uusi tietosuoja-asetus asettaa yrityksissä velvoitteen omien tietosuojaperiaatteiden ja -käytäntöjen tarkistamiseen ja tarvittaessa korjaamiseen sekä päivittämiseen ajan tasalle. Henkilötietoja käsittelevien työntekijöiden on oltava koulutettu voimassa olevan tietosuojalain sisältöön ja soveltamiseen käytännössä sekä ymmärtää keskeiset käsitteet. Huolimatta siitä, että lakia noudatetaan ja ollaan huolellisia, yrityksien kannattaa varautua tietoturvaloukkauksiin ja niiden yrityksiin. Ennen kuin henkilötietoja käsittelyä suunnitellaan, tulisi arvioida ja minimoida riskit ja uhat.

Henkilötietojen käsittely asiakassuhteessa perustuu asiakkaan ja yrityksen väliseen luottamukseen. Tietosuojalaki antaa ohjeet, miten henkilötietoja käsitellään. Asiakkaalla on mahdollisuus tarkistaa itse, onko yrityksen toiminta lainmukaista. Asiakassuhteessa on mahdollista käsitellä monenlaisia tietoja, jotka voi liittää tiettyyn henkilöön. Tietojen tulee olla asiakassuhteen kannalta tarpeellisia. Useimmissa tapauksissa nimi- ja yhteystiedot ovat tärkeitä asiakkaan yksilöimiseksi. Tietojen pyytämiseksi tarvitaan kuitenkin lakisääteinen peruste.

Luonnollisten henkilöiden henkilötietojen suojelu on perusoikeus kaikille. Tätä tulisi kunnioittaa, koska se on laissa määrätty. Tietosuojavaltuutetulta voi pyytää neuvoja siihen, miten henkilötietoja asetuksen mukaan tulee käsitellä. Hänellä on suuri rooli henkilötietojen salassa pysymisen suhteen. Antaessaan tietoja erilaisiin rekistereihin tulee olla huolellinen ja harkita tarkkaan, millaisia tietoja pyydetään, ovatko ne tarkoituksenmukaisia juuri siihen käyttötarkoitukseen, kuin niiden kerrotaan olevan. Globaalissa maailmassa tietojen liikkuminen on hyvin helppoa, joten rekisteröidyn on käytännössä mahdotonta tietää, missä päin hänen tietojaan tosiasiassa säilytetään ja käsitellään.

Keväällä 2018, GDPR:n tullessa voimaan EU:n jäsenvaltioissa, se näkyi kuluttajille muun muassa sähköpostiin tulleista tiedotteista, joissa uutta tietoturvaa selostettiin. Tiedottaminen onkin rekisterinpitäjien yksi velvollisuus. Kuluttajille

tarjottiin ainakin joissakin kirjeissä mahdollisuus lisäkyselyihin ja määritellä se, minkälaisia tiedotteita ko. yritykseltä tulevaisuudessa haluaa. Isommissa yrityksissä on esimerkiksi järjestetty koko henkilöstöä koskevia koulutuksia, joissa on kerrottu ”mitä GDPR on ja mitä se tarkoittaa meidän yritykselle ja mitä se tarkoittaa yksittäisen työntekijän kannalta sekä kuka on yrityksemme tietosuojavastaava”. Erityisesti asiakkaiden kanssa työskenteleville henkilöille on annettu lisäksi ohjeistusta, kuinka yrityksen GDPR asioista kerrotaan.

Tietosuojalla pyritään takaamaan asiakkaan yksityisyys. Uusi tietosuoja laki antaa entistä tarkemmat ohjeet siitä, miten yrityksessä henkilötietoja käsitellään. Hyvässä asiakassuhteessa asiakas voi luottaa siihen, että yritys käsittelee hänen henkilötietojaan asianmukaisesti. Yrityksen tehtävä on huolehtia riittävästä tietoturvasta, jotta tietoturvaloukkauksia ei tapahtuisi. Mikäli tietoihin kuitenkin päästään käsiksi esim. hakkeroimalla tietokonetta tai väärälle henkilölle postitetaan toisen henkilön henkilötietoja, niin tulee rekisterinpitäjän korjata asia ja ilmoittaa asianosaisille.

Tietojen käsittelijöiden tulee olla huolellisia käsitellessään henkilötietoja, jotta minimoidaan inhimillisistä virheistä johtuvia tietoturvauhkia. Vääriin käsiin päätyessään henkilötietoja voidaan käyttää pahimmassa tapauksessa rikolliseen toimintaan. Tiedot voivat päätyä myös esim. johonkin suoramarkkinointitarkoitukseen tai kyselyihin. Henkilöille koituu tällaisissa tapauksissa ylimääräistä vaivaa joutuessaan poistamaan henkilötietojaan ei toivotuista rekistereistä. Henkilötunnusta voi käyttää vain, jos siihen on perusteltu syy. Asiakkaan kannattaa käyttää harkintaa, mitä tietoja itsestään antaa ja ovatko ne välttämättömiä. Tällä tavalla voi välttyä ei-toivotulta suoramarkkinoinnilta. Yrityksen toiminnasta riippuu se, millaisia henkilötietoja ne tarvitsevat ja millaisiin tietoihin niillä on peruste kerätä.

Itse olen saanut taannoin kahdesti erään täysin vieraan vanhuksen kaikki tärkeät tiedot kunnalta, koska minut oli ilmeisesti inhimillisen erehdyksen seurauksena laitettu hänen omaisekseen. Kyse oli jopa kunnasta, jossa en koskaan ole edes asunut. Jouduin oikaisemaan asian kahdesti, ennen kuin asia korjattiin. Asiakaspalvelussa kaikki laitettiin atk-järjestelmien syyksi.

Sain idean opinnäytetyön aiheeksi Oikeudellisen viestinnän -kurssilla, jossa teimme raportin. Lähdin syventämään ja täsmentämään tietoturvaa juuri asiakassuhteessa tapahtuvaan henkilötietojen käsittelyyn. Aihe on ajankohtainen ja haasteellinen, mutta mielenkiintoinen. Asiahan koskee ihan kaikkia ihmisiä, ei vain henkilötietojen käsittelijöitä. Itse työ eteni verkkaiseen tahtiin lomittuen muun elämän kanssa. Pääasiallisina lähteinä käytin Euroopan parlamentin ja neuvoston 2016/679 asetusta ja tietosuojavaltuutetun toimiston nettisivuja. Lisäksi käytin lähteinä lain esitöitä ja oikeudellista kirjallisuutta. Nettilähteet olivat helpohko löytää ja kirjallisuuttakin oli mielestäni saatavilla riittävästi.

Tulevaisuudessa voisi tutkia sitä, miten tietosuojauudistus on käytännössä toteutettu ja miten siinä on onnistuttu. Millaisia haasteita yritykset ovat kohdanneet sekä miten kuluttajat ovat uudistuksen ottaneet vastaan.

Lähteet

Andreasson, A., Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tallinna: Tietosanoma.

Andreasson, A., Riikonen J., Ylipartanen, A. 2016. Tietosuojakäsikirja johdolle. Tallinna: Tietosanoma.

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

Asetus tietosuojalautakunnasta ja tietosuojavaltuutetusta 432/1994

Bergström, S., Leppänen, A. 1997. Yrityksen asiakasmarkkinointi. Helsinki: Edita. Edita.

Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46EY kumoamisesta 27.4.2016 (EU) 2016/679.

Euroopan parlamentin ja neuvoston direktiivi luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/YOS kumoamisesta 27.4.2016. (EU) 2016/680.

HE 9/2018 Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi**.**

Husa, J., Mutanen A., Pohjolainen, T. 2001. Kirjoitetaan juridiikkaa – Ohjeita oikeustieteellisten kirjallisten töiden laatijoille. Saarijärvi: Gummerus Kirjapaino Oy.

Kalliojärvi, T. EU:n yleinen tietosuoja-asetus: Tietoturvallisuudesta henkilötietojen käsittelyssä. Lapin yliopisto. Oikeustieteiden tiedekunta. Pro gradu -tutkielma. https://www-edilex-fi.tietopalvelu.karelia.fi/opinnaytetyot/16536.pdf. 3.5.2018.

Koivumäki, E., Häkkänen, P. 2017. Markkinointijuridiikka. Helsinki: Kauppakamari.

Korhonen, R. 2003. Perusrekisterit ja tietosuoja. Helsinki: Edita Prima Oy.

Lahtinen, J., Isoviita, A. 1994. Palveluviestintä. Kokkola: Avaintulos Oy.

Lahtinen, J., Isoviita, A., Hytönen, K. 1996. Markkinoinnin kilpailukeinot. Kokkola: Avaintulos Oy.

Laki viranomaisten toiminnan julkisuudesta 621/1999.

Mäenpää, O. 2000.Julkisuusperiaate. Helsinki: Hakapaino Oy.

Paloranta, P. 2008. Markkinointioikeus käytännössä. Tampere: Talentum.

Partanen, H. 2016 Kansallinen tietosuojapolitiikka ja EU:n tietosuoja-asetus. https://www-edilex-fi.tietopalvelu.karelia.fi/viestintaoikeus/17004.pdf. 3.5.2018.

Pesonen, P. 2017. Viestinnän lait. Keuruu: Edita.

Pitkänen, O., Tiilikka P., Warma, E. 2013. Henkilötietojen suoja. Helsinki: Talentum.

Rikoslaki 39/1889.

Tenhunen, S. 2011. Käsikirja oikeudellisen tiedon hakijalle: kansallisen ja eurooppaoikeuden keskeiset informaatiolähteet. Helsinki: WSOYpro Oy.

Tietosuoja suoramarkkinoinnissa. 1994. Helsinki: Tietosuojavaltuutetun toimisto Painatuskeskus Oy.

Tietosuojavaltuutetun toimisto 2018. Tietosuoja. Tietosuojavaltuutetun toimisto.http://tietosuoja.fi/fi/index/euntietosuojauudistus.html#tietosuoja-asetus. 6.3.2018.

Tietosuojavaltuutetun toimisto. 2013. http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat.html 6.3.2018.

Voutilainen, T. 2012. Oikeus tietoon – informaatio-oikeuden perusteet. Helsinki:

Voutilainen, T. 2016. Henkilörekisteriin kohdistuva rikos ja sen käsittely käräjäoikeuksissa. Porvoo: Edita.