Opinnäytetyö (AMK)

Tietojenkäsittelyn koulutusohjelma

Yrityksen tietoliikenne ja tietoturva

2016

Simo Oksanen

YLEINEN TIETOSUOJA-ASETUS JA KULUTTAJAREKISTERIEN KARTOITUS

– case: Raisio-konserni

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittelyn koulutusohjelma | Yrityksen tietoliikenne ja tietoturva

2016 | 40 sivua

Matti Kuikka

Simo Oksanen

YLEINEN TIETOSUOJA-ASETUS JA KULUTTAJAREKISTERIEN KARTOITUS

– case: Raisio-konserni

Tämän opinnäytetyön tavoitteena oli luoda tiivistelmä Euroopan unionin yleisen tietosuoja-asetuksen yksityiseen yritykseen liittyvistä artikloista ja selvittää Raisio-konsernin kuluttajarekisterien nykytila. Opinnäytetyön toimeksiantaja oli Raisionkaaren Teollisuuspuisto Oy, joka on osa Raisio-konsernia.

Työn teoriaosuudessa käsiteltiin asiakasrekisteriä ja siihen liittyvää Suomen lainsäädäntöä sekä Euroopan unionin tietosuojauudistusta. Teoria pohjustaa Suomen henkilötietolakia ja Euroopan unionin yleistä tietosuoja-asetusta. Lähdemateriaalina käytettiin Suomen lakia ja oikeusministeriön suomentamaa versiota Euroopan unionin yleisestä tietosuoja-asetuksesta vuodelta 2016 sekä aiheisiin liittyviä kirjallisuutta ja artikkeleita.

Empiirinen osuus koostui Raision kuluttajarekistereihin liittyvän kyselytutkimuksen suunnittelusta, toteutuksesta ja vastauksien analyysista. Tässä osassa tutkittiin kyselyn tuloksia ja tehtiin päätelmiä niiden perusteella. Osuus sisälsi myös kyselytutkimuksen tuloksien pohjalta tehdyn ehdotuksen kuluttajarekisterien selkeyttämiseksi.

Lopputuloksena yleinen tietosuoja-asetus tiivistettiin ja yksinkertaistettiin yksityiselle yritykselle sopivammaksi sekä kyselytutkimuksen tulosten avulla saatiin uutta tietoa Raisio-konsernin kuluttajarekistereiden nykytilasta. Opinnäytetyön tulosten avulla Raisio voi jatkaa valmistautumista Euroopan unionin tietosuojauudistusta varten.

ASIASANAT:

henkilötietolaki, henkilötietorekisteri, kuluttajarekisteri, kyselytutkimus, yleinen tietosuoja-asetus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communications and Information Security

2016 | 40 pages

Matti Kuikka

Simo Oksanen

GENERAL DATA PROTECTION REGULATION AND CONSUMER REGISTER SURVEY

– case: Raisio Group

The objective of this thesis was to create a summary of the European Union's General Data Protection Regulation's articles related to private companies and investigate the current state of Raisio Group's Consumer Registers. The thesis was assigned by Raisionkaaren Teollisuuspuisto Oy which is a part of Raisio Group.

The theoretical part of the thesis introduces the concept of customer register, and its legislation in Finland related to it and the European Union Data Protection Reform. The theory also covers the Finnish Personal Data Act and the European Union General Data Protection Regulation. Finnish Law and a version of the2016 General Data Protection Regulation translated into Finnish were used as source materials as well as relevant literature.

The empirical part of the thesis deals with the Raisio Group Consumer Register survey design, implementation and analysis of the results. This part reviews the results of the survey and then discusses conclusions drawn from the results. Finally, the empirical part includes a proposal for clarifying consumer registers on the basis of survey results.

As for the results, the General Data Protection Regulation was condensed and simplified to a more suitable version for a private company, and from the results of the survey Raisio Group gained new information regarding the current state of consumer registers. With the help of this thesis, Raisio Group can continue the preparation for the European Union's Data Protection Reform.

KEYWORDS:

consumer register, General Data Protection Regulation, Personal Data Act, personal data register, survey

SISÄLTÖ

KUVAT

SANASTO

CRM	CRM (Customer relationship management) eli asiakkuudenhallinta (Techtarget 2016b).
Profilointi	Luonnollisen henkilön arviointia käyttäen henkilön tiettyjä henkilökohtaisia ominaisuuksia (Yleinen tietosuoja-asetus 2016).
Pseudonymisointi	Henkilötietojen käsittely siten, että tietoja ei voida yhdistää yksittäiseen rekisteröityyn käyttämättä lisätietoja (Yleinen tietosuoja-asetus 2016).
VPN-yhteys	Virtual private network eli virtuaalinen erillisverkko, tapa jolla yksityisiä verkkoja voidaan yhdistää julkisen verkon yli (Techterms 2016).
Web UI	Web user interface eli internet-pohjainen käyttöliittymä (Techtarget 2016a).

1 JOHDANTO

Tämä opinnäytetyö tutkii Euroopan unionin yleistä tietosuoja-asetusta sekä kartoittaa Raision kuluttajarekisterien nykytilan. Opinnäytetyön toimeksiantajana toimi Raisionkaaren Teollisuuspuisto Oy. Työssä tutkitaan Euroopan unionin asetusta vuodelta 2016, joka toimii kehyksenä tulevalle tietosuojauudistukselle. Asetuksen pohjalta koottiin opinnäytetyöhön ne artiklat, jotka ovat oleellisia yksityisen yrityksen ja Raision kannalta. Liittyen Euroopan unionin laajuiseen tietosuojauudistukseen opinnäytetyöhön kartoitettiin myös Raisio-konsernin eri yksiköiden kuluttajarekisterien nykytila kyselytutkimuksella. Kyselytutkimuksen perusteella tehtiin ehdotus, jonka avulla voitaisiin parantaa kuluttajarekisterien tietosuojaa.

Raisionkaaren Teollisuuspuisto Oy on osa Raisio-konsernia. Raisio on suomalainen Raisiosta 1939 lähtöisin oleva kasvipohjaisen ravinnon erityisosaaja. Yritys on kansainvälinen, jonka päämarkkina-alueet ovat Suomi, Iso-Britannia, Venäjä, Puola ja Tšekki. Yritys on listattu Helsingin pörssiin ja sillä on noin 37 000 osakkeenomistajaa. Raisio työllistää noin 1 800 henkilö 12 maassa, ja vuoden 2015 liikevaihto oli 521 miljoona euroa ja liiketulos 52 miljoona euroa. (Raisio 2016.) Yritys halusi aloittaa valmistautumisen Euroopan unionin yleiseen tietosuojauudistukseen hyvissä ajoin ennen sen voimaan tuloa. Tärkeää oli selvittää, mitä uutta yleinen tietosuoja-asetus tulee mahdollisesti tuomaan Suomen lainsäädäntöön ja mikä on Raisio-konsernin eri yksiköiden kuluttajarekisterien nykytila. Näitä tietoja Raisio tarvitsee, jotta se voi sopeuttaa tulevaisuudessa toimintaansa oikealla tavalla ottaen huomioon tulevat muutokset tietosuojalainsäädännössä.

Opinnäytetyön lähestymistapa on tapaustutkimus (engl. Case study). Projekti alkoi helmikuussa 2016 suunnittelulla, josta siirryttiin Euroopan unionin yleisen tietosuoja-asetuksen tutkimiseen ja tiivistämiseen. Tämän jälkeen aloitettiin kyselytutkimuksen suunnittelu, toteutus ja viimeiseksi tuloksien analysointi. Projektin tuloksena olevat tiivistelmä yleisestä tietosuoja-asetuksesta ja kyselytutkimuksen vastaukset ovat sidoksissa toisiinsa, koska ne on toteutettu samaa tarkoitusperää varten. Tutkimusote on konstruktiivinen, minkä tavoitteena on antaa Raisiolle lisää valmiuksia EU:n tietosuojauudistusta varten.

2 ASIAKASREKISTERI

Asiakasrekisteri voidaan määritellä tietopankiksi, jossa säilytetään kaikkia olennaisia ja välttämättömiä tietoja asiakkaasta asiakkuuden ylläpitämiseksi. Rekisteriä voidaan kerätä joko automaattisesti tietokantoihin eri ohjelmia hyväksikäyttäen tai manuaalisesti. Tavoitteena on luoda näiden tietojen avulla kannattava asiakassuhde, joista molemmat asiakas ja yritys hyötyvät. (Rope & Pöllänen 1995, 113.)

Asiakasrekisterin sisältämä tieto voidaan jakaa viiteen perusluokkaan: yhteys-, segmentointi-, käyttö-, ja kokemus- sekä info- ja tulostiedot. Yhteystietojen avulla viesti toimitetaan asiakkaalle. Näiden tietojen on välttämätöntä olla tarkkoja ja jatkuvasti ajan tasalla. Segmenttitietojen avulla asiakkaat voidaan jakaa yrityksen haluamalla tavalla. Näitä tietoja hyväksikäyttäen voidaan esimerkiksi kohdistaa markkinointia tiettyyn asiakasryhmään. Käyttö- ja kokemustiedot ovat asiakkaiden ostohistorian ja palautteen kautta koottua tietoa. Infotietoja kirjataan asiakasrekistereihin asiakkaan ja yrityksen välisestä kommunikaatiosta. Näin saadaan esimerkiksi selville, mitä viestinnän kanavia asiakas suosii. Tulostiedot ovat liitännäistietoja, joita tallennetaan asiakasrekisteriin talouden seurannan kautta. Asiakaskannattavuus ja myyjätehokkuus ovat esimerkiksi olennaisia tulostietoja. (Rope & Pöllänen 1995, 113–116.)

Asiakasrekisterin kerääminen ja ylläpitäminen on oleellinen osa kannattavaa liiketoimintaa. Näin yritys voi tuottaa parempaa palvelua asiakkaille, kun tiedetään, mitä asiakas haluaa. Voidaan seurata asiakassuhteiden kehittymistä. Esimerkiksi ostavatko asiakkaat kerran palveluja vai ovatko he kanta-asiakkaita, ja minkälaista palautetta heiltä tulee. Ennen kaikkea asiakasrekisterit parantavat kommunikaatiota, kun on olemassa informaatio miten asiakkaaseen saa yhteyden ja mitä viestinnän kanavia asiakas suosii. (Schofield 2016.)

2.1 Lainsäädäntö

Kun yritys kerää asiakkaasta henkilötietoja eri rekistereihin, on yrityksen velvollisuus käsitellä henkilötietoja Suomen lain vaatimalla tavalla. Tästä vastaa ensisijaisesti henkilötietolaki 523/1999, jonka tehtävänä on suojata yksityiselämää ja ylläpitää hyvää tietojenkäsittelytapaa. Asiakasrekisterin kerääjän on oltava tietoinen, mitä oikeuksia ja velvollisuuksia hänellä on Suomen lain mukaan. Henkilötietolain lisäksi on monia muita lakeja, joissa käsitellään henkilötietoja. Henkilötietoja koskevia lakeja sovelletaan kun viranomainen, yritys, järjestö, muu yhteisö tai yksityinen henkilö toiminnassaan on tekemisissä kyseisten tietojen kanssa. Laki koskee automaattista tietojenkäsittelyä sekä manuaalisesti kerättyjä henkilötietoja henkilötietolain 3 pykälän määritelmän mukaisesti. (Tietosuojavaltuutetun toimisto 2016a.)

Seuraavaksi tutkitaan yksityiselle yritykselle tärkeitä henkilötietolain osia, jotka liittyvät asiakasrekistereiden keräämiseen, suojaamiseen, säilyttämiseen ja hävittämiseen. Lisäksi tarkastellaan, mitkä ovat yrityksen oikeudet ja velvollisuudet rekisterinpitäjänä. Kolmannessa luvussa tarkastellaan Euroopan unionin tietosuojauudistusta, jolla tulee olemaan myös vaikutusta Suomessa toimiviin yrityksiin. Uudistus astuu voimaan keväällä 2016 ja sitä aletaan soveltamaan keväällä 2018. (Eurooppa-neuvosto 2016.)

2.2 Henkilötietolaki

Henkilötietolaki on säädetty suojaamaan yksityiselämää ja muita yksityisyyden suojaa koskevia perusoikeuksia käsiteltäessä henkilötietoja. Lain tarkoituksena on kehittää hyvää tietojenkäsittelytapaa ja valvoa sen noudattamista (Henkilötietolaki 523/99, 1 §). Lakia sovelletaan henkilötietojen automaattiseen käsittelyyn ja muuhun henkilötietojen käsittelyyn, kun ne muodostavat tai niistä on tarkoitus muodostaa rekisteri tai osa sitä (Henkilötietolaki 523/99, 2 §). Laki koskee kaikkia, joiden toimipaikka on Suomessa tai Suomen oikeudenkäytön piirissä (Henkilötietolaki 523/99, 4 §). Henkilötietolaki on tullut voimaan 1. päivä kesäkuuta 1999 ja sillä kumottiin 30. päivänä huhtikuuta 1987 asetettu henkilörekisterilaki 471/1987 (Henkilötietolaki 523/99, 50 §).

2.2.1 Määritelmä

Henkilötietolaissa on 7 keskeistä määritelmää, joilla kuvataan, mitä laissa tarkoitetaan (Henkilötietolaki 523/99, 3 §):

a) *Henkilötieto* on merkintä, jolla voidaan kuvata luonnollista henkilöä, hänen ominaisuuksia, elinolosuhteita, ja tietoja joista hänet voidaan tunnistaa. Tämä koskee myös hänen perhettä tai hänen kanssa yhteisessä taloudessa eläviä;
b) *Henkilötietojen käsittely* on henkilötietojen kerääminen, tallentaminen, järjestäminen, käyttäminen, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen, tuhoaminen ja muut henkilötietoihin kohdistuvat toimenpiteet;
c) *Henkilötietorekisteri* on yhteenkuuluvista merkinnöistä muodostuva henkilötietoja sisältävä tietojoukko. Rekisteriä käsitellään joko osin tai kokonaan automaattisesti tiedonkäsittelyllä taikka järjestettynä kortistona, luettelona tai muuna näihin verrattavalla tavalla. Taustalla on, että tiettyä henkilöä koskevat tiedot löytyvät vaivattomasti ja kustannustehokkaasti;
d) *Rekisterinpitäjä* on yksi tai useampi henkilö, yhteisö, laitos taikka säätiö, jotka ovat perustaneet henkilörekisterin ja joilla on oikeus käyttää rekisteriä lain mukaan;
e) *Rekisteröity* on henkilö, jota kerätyt henkilötiedot koskevat;
f) *Sivullinen* on muu henkilö, yhteisö, laitos taikka säätiö kuin rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä;
g) *Suostumus* on vapaaehtoista, yksilöllistä ja tiedostettua tahdon ilmaisua, jolla rekisteriin lisätty henkilö voi hyväksyä hänen henkilötietojensa käsittelyn.

2.2.2 Rekisterinpitäjän velvollisuudet

Rekisterinpitäjä on velvoitettu käsittelemään henkilötietoja laillisesti, huolellisesti ja käyttäen hyvää tiedonkäsittelytapaa. Rekisteröidyn yksityisyyden turvaavia perusoikeuksia ei saa rikkoa ilman laissa säädettyä perustetta. Henkilötietojen käsittely on oltava perusteluta rekisterinpitäjän toiminnan kannalta. On määriteltävä mistä henkilötiedot hankitaan, mihin niitä luovutetaan ja mihin niitä rekisterinpitäjä tarvitsee. (Henkilötietolaki 523/99, 5–6 §.)

Rekisterinpitäjä on velvollinen, että käsiteltävät henkilötiedot ovat rekisterin tarkoituksen kannalta tarpeellisia (tarpeellisuusvaatimus). Rekisterinpitäjä on myös vastuussa, ettei rekisterissä ole virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja (virheettömyysvaatimus). Rekisterinpitäjällä pitää olla olemassa rekisteriseloste, josta käy ilmi: rekisterinpitäjä, mihin henkilötietoja käytetään, kuvaus rekisteröityjen tiedoista, mihin tietoja luovutetaan tai siirretään ja kuvaus rekisterin suojauksesta. Tämä seloste on oltava saatavilla tarvittaessa. (Henkilötietolaki 523/99, 9–10 §.)

Henkilötietolaissa on määritelty, mitkä lasketaan arkaluonteiseksi tiedoiksi, joiden käsittely on kielletty. Rekisterinpitäjä ei saa kerätä henkilötietoja etnisyyttä, vakaumusta, ammattiliiton kuulumista, rikoshistoriaa, terveydentilaa, seksuaalista suuntautumista tai sosiaalihuollon tarvetta koskien. Näitä tietoja saa yleensä vain kerätä joko yksilön suostumuksella ja oikeuden tai viranomaisten luvalla. Henkilötunnusta saa käsitellä vain rekisteröidyn antamalla suostumuksella. Henkilötunnuksen käsittelylle on oltava laillinen perusta ja rekisteröidyn yksilöiminen on oltava tärkeää. (Henkilötietolaki 523/99, 11–13 §.)

Suoramarkkinoinnissa ja mielipide- tai markkinatutkimuksissa rekisterinpitäjä saa käyttää henkilörekisterien tietoja, ellei rekisteröity ole kieltänyt henkilötietojensa käsittelyn. Henkilötietolaki rajaa, että henkilörekisteriä saa käyttää suoramarkkinointiin ja muihin osoitteellisiin lähetyksiin seuraavien ehtojen puitteissa (Henkilötietolaki 523/99, 9 §.):

a) Rekisteriä käytetään yksilöityyn ja lyhytaikaiseen markkinointiin, joka ei vaaranna rekisteröidyn yksityisyyden suojaa;
b) Rekisterissä on vain tietoa nimestä, arvosta tai ammatista, iästä, sukupuolesta ja äidinkielestä, yhdestä rekisteröityyn liitettävästä tunnistetiedosta ja yhteystiedoista;
c) Jos rekisterissä on tietoja rekisteröidyn asemasta elinkeinoelämässä tai julkisessa tehtävässä, ja rekisteriä käytetään hänen työtehtävään liittyvän informaation toimittamiseen.

Henkilötietolain mukaan rekisteröidyllä on oikeus kieltää rekisterinpitäjää käyttämästä hänen tietojaan suoramarkkinoinnissa sekä markkina- ja mielipidetutkimuksissa (Henkilötietolaki 523/99, 30 §). Henkilötietoja kerättäessä rekisteriin on rekisterinpitäjän huolehdittava, että rekisteröity voi halutessaan saada tiedot rekisterinpitäjästä, tämän edustajasta, mihin hänen henkilötietoja käytetään ja mihin tietoja luovutetaan. Suoramarkkinointia varten kerätyn henkilörekisterin nimi, rekisterinpitäjä ja hänen yhteistiedot pitää myös ilmoittaa pyydettäessä. (Henkilötietolaki 523/99, 24–25 §.)

Rekisterinpitäjä on vastuussa, että rekisteri on ajan tasalla. Tämä tarkoittaa, että rekisterinpitäjän on poistettava tai muokattava rekisterin sisältämiä henkilötietoja tarvittaessa tai rekisteröidyn pyynnöstä. Muutosten on tapahduttava ilman aiheetonta viivytystä ja ilman että rekisterin tiedot pääsevät leviämään. (Henkilötietolaki 523/99, 29 §.)

Tietoturvallisuuden kannalta asiakastietorekisteriä varten on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet. Asiattomilta on oltava pääsy kielletty tietoihin. Rekisterinpitäjä on vastuussa, että henkilötietoja ei vahingossa tai laittomasti hävitetä, muuteta, luovuteta, siirretä tai käytetä muuhun laittomaan toimintaan. Jokainen joka on tekemisissä henkilötietorekisterin kanssa, on vaitiolovelvollinen jos rekisteri sisältää tietoja henkilökohtaisista oloista, taloudellista asemasta tai henkilön ominaisuuksista. Mikäli henkilötietorekisteri ei ole enää rekisterinpitäjän toiminnan kannalta tarpeellinen, on yritys velvollinen poistamaan rekisterin tietoturvallisella tavalla. Poikkeuksena edellä mainittuun on, jos rekisteri sisältää tietoja jotka ovat erikseen säädetty tai määrätty henkilötietolain pykälän 35 mukaan arkistoitavaksi. (Henkilötietolaki 523/99, 32–34 §.)

Rekisterinpitäjä on velvollinen korvaamaan rekisteröidylle tai muulle henkilölle aiheuttamansa vahingot Suomen lain vastaisesta henkilötietojen käsittelystä (Henkilötietolaki 523/99, 47 §). Henkilötietolain 48 pykälässä on säädetty erikseen rangaistussäännöksistä ja mikä lasketaan tahalliseksi tai törkeäksi huolimattomuudeksi tätä lakia vastaan.

3 YLEINEN TIETOSUOJA-ASETUS

Euroopan unionin tämän hetkinen tietosuojalainsäädäntö eli henkilötietodirektiivi tulee vuodelta 1995 ja sitä on täydennetty vuonna 2008. Tällä direktiivillä oli kaksi tavoitetta: antaa tietosuojaa koskeva perusoikeus ja mahdollistaa henkilötietojen vapaa liikkuvuus jäsenvaltioiden välillä. Euroopan unionin päättävät toimielimet eivät enää pidä henkilötietodirektiivi tarpeeksi vahvana ja laajana, joten vuonna 2012 tehtiin ehdotus uudesta EU:n yleisestä tietoturva-asetuksesta. Ehdotetun asetuksen tarkoitus on vastata haasteisiin joita teknologian nopea kehitys ja tietojen jakaminen sekä kerääminen isossa mittakaavassa ovat tuoneet.

Teknologian kehitys on antanut yksityisille ja julkisille toimijoille mahdollisuuden käyttää henkilötietoja ennennäkemättömällä tavalla. Tähän kuuluvat myös yksityishenkilöt, jotka jakavat henkilötietojaan nykyään laajemmin ja julkisemmin. Henkilötietojen jakaminen ja hyväksikäyttäminen on EU:n mukaan aiheuttanut luottamuspulan kuluttajille kun puhutaan suhtautumisesta uusiin verkkopalveluihin. Tätä pidetään esteenä uusille teknologioille ja innovaatioille. Täten henkilötietosuoja on keskeinen osa Euroopan digitaalistrategiaa ja myös laajempaa Eurooppa 2020-strategiaa. (COM(2012) 11 final, 1.)

Joulukuun 18. päivänä 2015 Euroopan unionin päättävät toimielimet pääsivät sovintoon yleisestä tietoturva-asetuksesta. Asetuksen tuomat tietosuojauudistukset julkaistaan Euroopan Unionin virallisessa lehdessä keväällä 2016 ja ne tulevat voimaan 20 päivää julkaisun jälkeen. Asetusta aletaan soveltamaan kahden vuoden siirtymäajan jälkeen keväällä 2018. Siirtymäajan aikana oikeusministeriö muokkaa yleistä tietosuoja-asetusta Suomen lainsäädäntöön sopivaksi. (Oikeusministeriö 2016.)

Asetus luo EU:lle ajan tasalla olevan, yhtenäisen ja kattavan tietosuojakehyksen. Kehyksen tavoite on parantaa kuluttajien luottamusta online-palveluihin ja edistää EU:n digitaalisia sisämarkkinoita. Asetus tulee korvaamaan kokonaisuudessaan EU:n henkilötietodirektiivin, jota ei enää pidetä tarpeeksi vahvana ja laajana tietosuojakehyksenä nykyaikaisessa tietoyhteiskunnassa. Tietosuoja-asetus tulee koskemaan kaikkia EU:n jäsenmaita ja kaikkia henkilötietoja, joita niiden rajojen sisällä käsitellään. Kyseessä on jäsenvaltioissa suoraan sovellettava asetus, joka tulee yhdenmukaistamaan EU:n tietosuojasäätelyä. Suomessa tietosuoja-asetus tulee olemaan suoraan sovellettavaa lainsäädäntöä, jonka täytäntöönpanosta vastaa oikeusministeriö. (Tietosuojavaltuutetun toimisto 2016b.)

Seuraavaksi tutkitaan yleistä tietosuoja-asetusta yksityisen yrityksen kannalta. Asetusta tarkastellaan niiden artiklojen osalta, joilla on vaikutusta yrityksen henkilötietojen keräämiseen, käsittelyyn ja suojaamiseen. Artikloissa käsitellään rekisteröidyn ja rekisterinpitäjän oikeuksia kuin velvollisuuksia.

3.1 Periaatteet

Rekisterinpitäjän täytyy henkilötietoja käsitellessä noudattaa hyvää tietojenkäsittelytapaa. Tämä tarkoittaa, että käsittely pitää tapahtua lainmukaisesti, asianmukaisesti ja läpinäkyvästi rekisteröidylle. Henkilötietoja saa kerätä vain nimenomaista ja lainmukaista tarkoitusta varten, minimoiden niiden määrä vain tarkoitusperälle tärkeisiin tietoihin. Tietojen minimoimista vain tarpeellisiin tietoihin kutsutaan minimoinnin periaatteeksi. Henkilötietojen täytyy olla täsmällisiä ja päivitettyjä. Virheelliset tiedot täytyy oikaista mahdollisimman nopeasti niiden havaitsemisen jälkeen. Vastuu henkilötiedoista on rekisterinpitäjällä, jonka täytyy pitää huoli että tietosuoja-asetuksen säännöksiä noudatetaan. (Yleinen tietosuoja-asetus 2016, 5 artikla.)

Tietosuoja-asetuksen 6 artikla määrittelee, milloin henkilötietojen käsittely on lainmukaista. Lainmukaisuuden tärkein määritelmä on, että rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyä varten ja että se tapahtuu Suomen ja Euroopan unionin lainsäädännön mukaisesti. Rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksensa hänen henkilötietojensa käsittelyä varten. (Yleinen tietosuoja-asetus 2016, artikla 6.) Suostumuksen voi perua aina. Suostumus katsotaan pätemättömäksi, jos on olemassa epäsuhta, kuten se, ettei suostumusta voi käytännössä perua. Epäselvissä tilanteissa annetulla suostumuksella ei ole oikeusperustaa henkilötietojen käsittelyä varten. (Yleinen tietosuoja-asetus 2016, 7 artikla.)

Artikla 8 määrittelee alle 16-vuotiaan lapseksi, jolloin hänen henkilötietoja saa lainmukaisesti käsitellä vain silloin, kun siihen on saatu lapsen huoltajan suostumus. Jäsenvaltiot voivat säätää itse alemmasta iästä, joka ei saa olla alle 13 vuotta. Rekisterinpitäjä on vastuussa, että tarvittavat toimenpiteet on toteutettu huoltajan suostumuksen todentamiseksi. (Yleinen tietosuoja-asetus 2016, 8 artikla.)

Tietosuoja-asetuksen periaatteiden mukaan henkilötiedot, jotka käsittelevät rotua, etnisyyttä, poliittista mielipidettä, uskontoa, filosofista vakaumusta tai ammattiliittoon kuulumista sekä geneettisiä ja biometrisiä tietoja, terveyttä, seksuaalista orientaatiota tai ovat

rikoksiin liittyviä, ei saa käsitellä ilman rekisteröidyn suostumusta tai oikeudellista perustetta. (Yleinen tietosuoja-asetus 2016, 9 artikla.)

3.2 Rekisteröidyn oikeudet

Rekisterinpitäjällä on oltava henkilötietojen käsittelyä ja rekisteröidyn oikeuksia varten läpinäkyvät toimitavat. Rekisterinpitäjän on toimitettava pyydettäessä kaikki rekisteröidyn henkilötietoja koskevat tiedot rekisteröidylle helposti ymmärrettävässä ja saatavilla olevassa muodossa. (Yleinen tietosuoja-asetus 2016, 12 artikla.)

Tietosuoja-asetuksen 13 artiklassa on määritelty mitä tietoja rekisteröidylle pitää toimittaa pyydettäessä:

a) Rekisterinpitäjän ja tämän edustajan yhteistiedot;
b) Tietosuojavastaavan yhteistiedot;
c) Henkilötietojen käsittelyn tarkoitus;
d) Rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut;
e) Henkilötietojen vastaanottajat tai vastaanottajaryhmät;
f) Tieto, jos henkilötietoja siirretään kolmanteen maahan tai kansaväliselle järjestölle.

Lisäksi seuraavista pitää toimittaa rekisteröidylle lisätietoja asianmukaisen ja läpinäkyvän käsittelyn takaamiseksi:

a) Henkilötietojen säilytysaika;
b) Tieto oikeudesta päästä käsiksi häntä käsitteleviin henkilötietoihin;
c) Oikeus peruuttaa suostumus henkilötietojen keruuseen;
d) Oikeus tehdä valitus valvontaviranomaiselle;
e) Tieto, jos henkilötietojen antaminen on lakisääteistä tai sopimukseen perustuvaa;
f) Kuvaus käsittelylogiikasta profiloinnin yhteydessä.

Jos rekisteröidyn tietoja käsitellään edelleen muuhun tarkoitukseen kuin niiden alkuperäinen tarkoitus oli, on rekisteröidylle myös ilmoitettava jatkokäsittelyn tarkoitus. (Yleinen tietosuoja-asetus 2016, artikla 13.) Rekisteröidyllä on oikeus saada tietää käsitelläänkö hänen henkilötietoja vai eikö niitä käsitellä. Mikäli henkilötietoja käsitellään, on rekisteröity oikeutettu pääsemään käsiksi henkilötietoihinsa sekä käsittelyä koskeviin oleellisiin

tietoihin. Rekisterinpitäjän on toimitettava jäljennökset käsiteltävistä henkilötiedoista, jos rekisteröity niitä vaatii. (Yleinen tietosuoja-asetus 2016, 15 artikla)

Rekisteröidyllä on oikeus vaatia henkilötietojensa oikaisua, jos hänen henkilötiedot ovat epätarkkoja tai virheellisiä. Rekisterinpitäjän pitää oikaista tiedot ilman aiheetonta viivytystä, jos ne todetaan virheellisiksi. (Yleinen tietosuoja-asetus 2016, 16 artikla.) Rekisteröidyllä on myös oikeus tulla unohdetuksi. Tämä tarkoittaa, että rekisteröidyllä on oikeus vaatia henkilötietojensa poistoa ja käsittelyn lopettamista. Rekisterinpitäjän pitää poistaa tiedot ja lopettaa niiden käsittely ilman aiheetonta viivytystä, jos rekisteröity sitä vaatii, ellei käsittelylle löydy rekisteröidyn oikeudet kumoava oikeusperusta. (Yleinen tietosuoja-asetus 2016, 17 artikla.) Oikaisun ja unohtamisen lisäksi rekisteröidyllä on oikeus pyytää henkilötietojensa käsittelyn rajoittamista, jos hänellä on siihen tietosuoja-asetuksen mukainen perusta (Yleinen tietosuoja-asetus 2016, 18 artikla). Kaikissa kappaleessa mainituissa tapauksissa rekisterinpitäjän täytyy ilmoittaa muutoksista rekistereissä jokaiselle näitä henkilötietoja vastaanottaneelle (Yleinen tietosuoja-asetus 2016, 19 artikla).

Rekisteröity voi vastustaa henkilötietojensa käsittelyä milloin tahansa, ellei rekisterinpitäjä pysty esittämään käsittelyyn tärkeää ja perusteltua syytä, joka syrjäyttäisi rekisteröidyn oikeudet. Sama pätee myös jos rekisteröidyn henkilötietoja käytetään suoramarkkinointiin. Jos rekisteröity vastustaa henkilötietojen käsittelyä ja se hyväksytään, rekisterinpitäjä ei voi enää käsitellä kyseisen rekisteröidyn henkilötietoja. (Yleinen tietosuoja-asetus 2016, 21 artikla.)

Mikäli rekisterinpitäjä käyttää automatisoitua henkilötietojen käsittelyä, rekisteröity ei saa joutua sellaisen päätöksen kohteeksi, joka perustuu pelkästään tämän kaltaiseen käsittelyyn. Tämän kaltaisia päätöksiä ovat esimerkiksi profiloivat ja oikeusvaikutukselliset päätökset. (Yleinen tietosuoja-asetus 2016, 22 artikla.)

3.3 Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet

Euroopan unioni haluaa tehdä rekisterinpitäjistä enemmän vastuullisia keräämistään henkilötiedoista tekemällä heistä tilivelvollisia toiminnastaan ja henkilötietojen suojaamisesta. Tietoturvallisuus pitää ottaa huomioon kaikessa henkilötietoja koskevassa toiminnassa jo suunnittelu vaiheesta alkaen. Vaikutusten arviointi täytyy tehdä, jos henkilötietojen luonne sitä vaatii. Yleinen tietosuoja-asetus tekee rekisterinpitäjästä velvollisen ilmoittaa tietovuodoista ja – rikkomuksista. Näistä rikkomuksista voi asetuksen mukaan

seurata sakkoja. Myös henkilötietoja ydintehtävänään käsittelevien rekisterinpitäjien ja julkisten toimielimien täytyy nimetä tietosuojavastaava. Tämän henkilön toimenkuva on neuvoa ja valvoa että tietosuoja-asetusta noudatetaan. (Yleinen tietosuoja-asetus 2016.)

3.3.1 Yleiset velvollisuudet

Henkilötietojen käsittelyn luonteen, laajuuden ja tarkoituksen mukaan rekisterinpitäjän pitää toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joiden avulla voidaan tarkistaa että yleistä tietosuoja-asetusta noudatetaan. Tähän kuuluu myös, että asianmukaiset tietosuojaperiaatteet ovat kunnossa. Edellä mainitut toimenpiteet pitää tarkastaa ja päivittää, jos tarvetta huomataan. (Yleinen tietosuoja-asetus 2016, 24 artikla.) Toimenpiteiden toimivuudesta vastaa viime kädessä valvontaviranomainen, jonka kanssa rekisterinpitäjän on tehtävä yhteystyötä aina pyydettäessä (Yleinen tietosuoja-asetus 2016, 31 artikla).

Sisäänrakennetun ja oletusarvoisen tietosuojan määrittämisessä henkilötietojen käsittelyä varten rekisterinpitäjän on toteutettava tehokkaat tietosuojaperiaatteet. Tällä tarkoitetaan, että tietosuoja on otettava huomioon heti palvelun tai tuotteen suunnittelusta asti, ja yksityisyydensuojaa edistävät oletusarvot ovat automaattisesti käytössä organisaation toiminnassa (Tietosuojavaltuutetun toimisto 2016c). Sisäänrakennetun ja oletusarvoisen tietosuojan takaamiseksi pitää toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet. Näitä toimenpiteitä on esimerkiksi henkilötietojen minimointi, pseudonymisointi ja tarvittavat suojatoimet. Tämä velvollisuus koskee henkilötietojen määrää, käsittelyä, säilytysaikaa ja saatavuutta. Toimenpiteiden avulla varmistetaan ensisijaisesti se, että tiedot eivät pääse rajoittamattoman henkilömäärään saataville. (Yleinen tietosuoja-asetus 2016, 25 artikla.)

Rekisterinpitäjä saa käyttää vain sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet rekisteröidyn oikeuksien suojaamiseksi. Nämä henkilötietojen käsittelijät eivät saa käyttää muiden käsittelijöiden palveluksia ilman rekisterinpitäjän erityistä lupaa. Henkilötietojen käsittelijän suorittamaa käsittelyä on aina säädeltävä sopimuksella tai muulla laillisella asiakirjalla, jossa selviää käsittelyn luonne ja tarkoitus. (Yleinen tietosuoja-asetus 2016, 28 artikla.) Kaikkien henkilötietojen käsittelijän tai rekisterinpitäjän alaisuudessa toimivien henkilöiden, joilla on pääsy henkilötietoihin, pitää käsitellä henkilötietoja vain rekisterinpitäjän ohjeiden mukaan (Yleinen tietosuoja-asetus 2016, 29 ar-

tikla). Käsittelytoimista, joita tehdään rekisterinpitäjälle pitää ylläpitää selostetta. Selosteesta pitää käydä ilmi oleelliset tiedot käsittelijöistä, käsittelyn tarkoituksesta, rekisteröityjen ryhmistä, henkilötietojen vastaanottajista ja siirtämisestä kolmansiin maihin tai kansanvälisille järjestöille. (Yleinen tietosuoja-asetus 2016, 30 artikla.)

3.3.2 Tietoturvallisuus

Tietoturvan tärkeyttä ei voi vähätellä nyky-yhteiskunnassa. Päivittäin voi lukea uutisia kuinka eri yritykset ovat joutuneet laittomien hyökkäyksien ja tietovarkauksien kohteeksi. Tietoturvan pyrkimys on suojella yrityksien tärkeiden tietojen pääsyä ulkopuolisille. Hyvä tietoturva ottaa huomioon niin yksilöt, organisaation, prosessit, tekniset kuin digitaaliset ratkaisut. Tietojen luottamuksellisuus, eheys, saatavuus, kiistämättömyys, pääsynvalvonta ja tarkastettavuus ovat kaiken toiminnan ydin. Jokaisen yrityksen on implementoitava tarvittavat toimenpiteet näiden saavuttamiseksi. (Suomen internetopas 2016.)

Euroopan unionin yleisessä tietosuoja-asetuksessa on määritelty rekisterinpitäjän velvollisuudet koskien tietoturvallisuutta. Tämä käsittää asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla pyritään varmistamaan henkilötietojen käsittelyn turvallisuus. Rekisterinpitäjän pitää toteuttaa henkilötietojen luonnetta vastaava turvallisuustaso. Näillä toimenpiteillä pyritään ylläpitämään henkilötietojen käsittelyn salaus, saatavuus, luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus. (Yleinen tietosuoja-asetus 2016, 32 artikla.)

Rekisterinpitäjä on velvollinen ilmoittamaan tietoturvaloukkauksista valvontaviranomaiselle. Tämän pitää tapahtua ilman aiheetonta viivytystä 72 tunnin sisällä loukkauksen ilmenemisestä. Rekisterinpitäjän täytyy antaa perusteltu selitys valvontaviranomaisille, jos ilmoitusta tietoturvaloukkauksesta ei anneta 72 tunnin sisällä. Tietoturvaloukkausilmoituksessa täytyy vähintään antaa tietoa seuraavista:

a) Kuvaus henkilötietojen tietoturvaloukkauksesta;
b) Tietosuojavastaavan henkilöllisyys ja yhteistiedot tai muu yhteyspiste lisätietoja varten;
c) Kuvaus tietoturvaloukkauksen seurauksista;
d) Kuvaus ehdotetuista tai toteutuneista toimenpiteistä koskien tietoturvaloukkausta.

Kaikki henkilötietoihin kohdistuvat tietoturvaloukkaukset on dokumentoitava rekisterinpitäjän toimesta. Dokumenteissa on pystyttävä osoittamaan tietoturvaloukkauksiin liittyvät seikat, vaikutukset ja korjaustoimet. (Yleinen tietosuoja-asetus 2016, 33 artikla.)

Rekisterinpitäjä on myös velvollinen ilmoittamaan rekisteröidylle, jos hänen henkilötietoihin on kohdistunut tietoturvaloukkaus. Poikkeus tähän on, jos rekisterinpitäjä on osoittanut valvontaviranomaiselle, että se on toteuttanut asianmukaiset tekniset suojatoimenpiteet koskien henkilötietoja. Tämä tekniset suojatoimenpiteet pitää sisällään keinot, joiden avulla henkilötiedot ovat muutettu muotoon, jota ulkopuoliset tahot eivät ymmärrä. Mikäli näin ei ole, on rekisteröidylle ilmoitettava, ellei ilmoituksen teko vaadi kohtuutonta vaivaa. Myös valvontaviranomainen voi vaatia ilmoituksen tekoa rekisteröidylle, jos rekisterinpitäjä ei ole sitä oma-aloitteisesti tehnyt. (Yleinen tietosuoja-asetus 2016, 34 artikla.)

3.3.3 Vaikutusten arviointi ja ennakkokuuleminen

Rekisterinpitäjän käsitellessä luonteeltaan, laajuudeltaan tai tarkoitukseltaan sellaisia henkilötietoja, joiden vuoksi rekisteröidyn oikeuksiin tai vapauksiin voi liittyä riskejä, on laadittava arvio suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle. Kyseisiä riskejä ovat profiloivien henkilötietojen käsittely, joista voi aiheutua rekisteröidylle oikeusvaikutuksia tai merkittävää haittaa; yleisölle avoimien alueiden valvonta; sekä erityisiin henkilötietoryhmiin kohdistuva laajamittainen käsittely.

Vaikutusten arviointi sisältää:

a) Kuvauksen suunnitelluista käsittelytoimista;
b) Arvion käsittelytoimien tarpeellisuudesta;
c) Arvion rekisteröidyn oikeuksia ja vapauksia koskevista riskeistä;
d) Toimenpiteet riskeihin puuttumiseen.

Vaikutusarvioinnin tapauksen mukaan rekisterinpitäjän on pyydettävä rekisteröityjen tai heidän edustajien näkemys käsittelytoimien mahdollisista vaikutuksista rekisteröityihin. Jos vaikutusarvioinnissa on huomautettavaa tai sen tietosuojassa on tapahtunut muutoksia, pitää rekisterinpitäjän tehdä arvioinnin uudelleentarkastus. (Yleinen tietosuoja-asetus 2016, 35 artikla.)

Mikäli vaikutusarviointi osoittaa, että henkilötietojen käsittely aiheuttaa korkean riskin, on rekisterinpitäjä velvollinen ennen käsittelyn aloittamista kuulla valvontaviranomaista.

Kuulemista varten rekisterinpitäjän pitää toimittaa kaikki henkilötietojen käsittelyä koskevat oleelliset tiedot valvontaviranomaiselle. Jos valvontaviranomainen katsoo, että rekisterinpitäjä rikkoo yleistä tietosuoja-asetusta ja käsittely aiheuttaa korkean riskin, on valvontaviranomainen oikeutettu käyttämään tutkintavaltuuksia tilanteen parantamiseksi. (Yleinen tietosuoja-asetus 2016, 36 artikla.)

3.3.4 Tietosuojavastaava

Suomen tietosuojavaltuutetun toimisto määrittelee tietosuojavastaavan erityisasiantuntijaksi, jonka tehtävä on ylläpitää hyvää henkilötietojen käsittelytapaa ja mahdollisten erityislakien edellyttämää korkeaa tietosuojatasoa. Tavoite on näin rakentaa ja säilyttää luottamus rekisterinpitäjän ja rekisteröidyn välillä. Tietosuojavastaava on apu organisaation henkilöstölle ja ennen kaikkea johdolle. (Tietosuojavaltuutetun toimisto 2010.)

Euroopan unionin yleinen tietosuoja-asetus laajentaa tietosuojavastaavan vastuita. Asetuksen mukaan jokainen viranomainen ja julkishallinnon toimielin on velvollinen nimeämään tietosuojavastaavan. Tämän koskee myös kaikkia yksityisiä rekisterinpitäjiä, joiden henkilötietojen käsittely on luonteeltaan, laajuudeltaan tai tarkoitukseltaan sellaista, joka vaatii rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. Konserneissa nimetään vain yksi tietosuojavastaava, jonka pitää olla jokaisen konsernin toimipaikan saatavilla tarvittaessa. Nimettäessä tietosuojavastaava, on otettava huomioon hakijan ammattipätevyys ja erityisesti tietosuojalainsäädännön sekä alan käytäntöjen tunteminen. Tietosuoja vastaava voi olla rekisterinpitäjän oma työntekijä tai palvelusopimuksella palkattu ulkopuolinen. Nimitetystä tietosuojavastaavasta pitää aina julkaista yhteistiedot ja ilmoittaa valvontaviranomaiselle. (Yleinen tietosuoja-asetus 2016, 37 artikla.)

Tietosuojavastaavan asema on valvoa rekisteripitäjän henkilötietojen käsittelyä. Rekisterinpitäjän on otettava tietosuojavastaava mukaan kaikissa henkilötietojen suojaa koskevissa kysymyksissä organisaatiossa kuin rekisteröityjen keskuudessa. Tätä varten rekisterinpitäjän täytyy antaa tietosuojavastaavalle hänen tarvitsemansa resurssit, jotta hän pystyy hoitamaan velvollisuutensa. Rekisterinpitäjän on varmistettava, että tietosuojavastaava täyttää velvollisuutensa riippumattomasti, eikä ota vastaan ohjeita tehtäviensä hoitamisen yhteydessä. Tietosuojavastaava raportoi suoraan rekisterinpitäjän ylimmälle johdolle ja on tehtäviensä suhteen salassapitovelvollinen. Tietosuojavastaava voi myös hoitaa muita tehtäviä organisaatiossa, jos niillä ei ole eturistiriitaa tietosuojavastaavan tehtävien kanssa. (Yleinen tietosuoja-asetus 2016, 38 artikla.)

Yleisen tietosuoja-asetuksessa on määritelty ne tehtävät, jotka rekisterinpitäjän täytyy ainakin osoittaa tietosuojavastaavalle (Yleinen tietosuoja-asetus 2016, 39 artikla):

a) Antaa tietoa ja neuvoa Euroopan unionin yleisen tietosuoja-asetuksen, sekä unionin tai sen jäsenvaltioiden tietosuojasäännösten mukaisista velvollisuuksista;
b) Seurata yleisen tietosuoja-asetuksen noudattamista ja rekisterinpitäjän toiminta-menetelmiä, koskien henkilötietojen suojaa, sekä vastata siihen liittyvästä vastuunjaosta, koulutuksesta ja tarkastuksista;
c) Neuvoa vaikutusarvioinnin tekemisessä ja valvoa sen toteutusta;
d) Tehdä yhteistyötä valvontaviranomaisten kanssa;
e) Toimia yhteyspisteenä valvontaviranomaisille tietojenkäsittelyyn liittyvissä kysymyksissä, mukaan lukien ennakkokuuleminen.

3.3.5 Henkilötietojen siirto kolmansiin maihin tai kansanvälisille järjestöille

Euroopan unionin yleisen tietosuoja-asetuksen viidennessä luvussa on määritelty periaatteet koskien henkilötietojen siirtoa kolmansiin maihin tai kansainvälisiin järjestöihin. Kolmannet maat ovat maita, jotka eivät kuuluu Euroopan unioniin, ja niillä ei ole voimassa olevia kansainvälisiä sopimuksia EU:n kanssa (Procurement policy note 2012). Yleisen periaatteen mukaan henkilötietoja voi siirtää kolmansiin maihin tai kansainvälisille järjestöille, jos rekisterinpitäjä noudattaa yleisen tietosuoja-asetuksen viidennen luvun mukaisia säännöksiä. (Yleinen tietosuoja-asetus 2016, 44 artikla.) Säännöksissä todetaan, että henkilötietoja saa siirtää kolmansiin maihin, joilla on riittävä tietosuojan taso. Tietosuojan tasolla tarkoitetaan, että kyseisellä kolmannella maalla on voimassa oleva oikeusvaltioperiaate, asiankuuluva lainsäädäntö, riippumaton valvontaviranomainen ja kansainväliset sitoumukset. Näiden ehtojen täyttyessä henkilötietojen siirrolle ei tarvitse erillistä lupaa. Euroopan komissio arvioi onko kolmannella maalla tai kansainvälisellä järjestöllä riittävä tietosuojan taso. Euroopan unionin virallisessa lehdessä ja verkkosivuilla on luetteloitu ne maat ja kansanväliset järjestöt, joilla on ja ei ole riittävää tietosuojan tasoa. (Yleinen tietosuoja-asetus 2016, 45 artikla.)

Konsernilla pitää olla yhdenmukaiset ja sitovat säännöt henkilötietoja siirrättäessä kolmansiin maihin tai kansainvälisille järjestöille. Valvontaviranomainen vahvistaa konsernin tekemät säännöt ja ne ovat oikeudellisesti sitovia sekä niitä pitää soveltaa kaikkiin konsernin tai yritysryhmän jäseniin. Säännöt pitää laatia yhdenmukaisuusmekanismin

mukaan, jonka avulla edistetään yleisen tietosuoja-asetuksen yhdenmukaista soveltamista ja eri valvontaviranomaisten yhteistyötä kaikkialla Euroopan unionissa (Yleinen tietosuoja-asetus 2016, 47 ja 63 artikla.)

3.4 Oikeussuojakeinot, vastuu ja seuraamukset

Yleisen tietosuoja-asetuksen kahdeksannessa luvussa määritellään rekisteröidyn oikeussuojakeinoista, rekisterinpitäjän vastuista ja yleisen tietosuoja-asetuksen säännösten rikkomisen seuraamuksista.

Jokaisella rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, jos he katsovat että yleisen tietosuoja-asetuksen säännöksiä on rikottu. Rekisteröity on oikeutettu oikeussuojakeinoihin rekisterinpitäjää tai henkilötietojen käsittelijää kuin valvontaviranomista vastaan. Jokaisella rekisteröidyllä on oikeus nostaa kanne rekisterinpitäjää, henkilötietojen käsittelijää ja valvontaviranomaista vastaan, jos hän katsoo että henkilötietojenkäsittelyssä ei ole noudatettu yleistä tietosuoja-asetusta. Kaikki kanteet käsitellään ensisijaisesti siinä Euroopan unionin jäsenvaltion tuomioistuimessa jossa rekisterinpitäjän, henkilötietojen käsittelijän tai valvontaviranomaisen toimipaikka on. (Yleinen tietosuoja-asetus 2016, 77 – 79 artikla.) Jos tuomioistuin toteaa rekisterinpitäjän, henkilötietojen käsittelijän tai valvontaviranomaisen aiheuttaneen lainvastaisella toiminnalla vahinkoa käsittelyn yhteydessä tai yhteensopimattomuutta yleisen tietosuoja-asetuksen säännösten kanssa, on rekisteröity oikeutettu saamaan korvauksia (Yleinen tietosuoja-asetus 2016, 82 artikla).

Valvontaviranomainen on vastuussa hallinnollisten sakkojen määräämisestä. Sakkojen on oltava tehokkaita, oikeussuhteisia ja varoittavia. Sakon suuruuteen vaikuttaa muun muassa rikkomuksen luonne, laajuus, vakavuus, kesto, tahallisuus ja tuottamuksellisuus. Yleisessä tietosuoja-asetuksessa on kaksi hallinnollista sakkoluokkaa, jotka määräytyvät sen mukaan, mitä artikloita syytetty on rikkonut. Sakkoluokat ovat enintään 10 000 000 euroa tai 2 prosenttia edellisen tilikauden maailmanlaajuisesta kokonaisliikevaihdoista sekä enintään 20 000 000 euroa tai 4 prosenttia edellisen tilikauden maailmanlaajuisesta kokonaisliikevaihdoista. Sakon muoto täsmällisenä rahamääränä tai liikevaihdon mukaan määräytyy sen mukaan, kumpi näistä määristä on suurempi. Artiklassa 83 määritellään tarkemmin rikkomukset, jotka vaikuttavat sakon suuruuteen. (Yleinen tietosuoja-asetus 2016, 83 artikla.)

4 KULUTTAJAREKISTERIEN KARTOITUS

Tämän opinnäytetyön empiirisenä osiona on toteutettu kyselytutkimus Raisionkaaren Teollisuuspuisto Oy:lle. Opinnäytetyön toimeksianto on annettu 15.2.1016, tällöin sovittiin Raisio-konsernin tietohallintopäällikön Sami Halisen kanssa, että toteutetaan kyselytutkimus liittyen Raision kuluttajarekistereihin. Kuluttajarekisterit ovat asiakasrekistereitä, jotka sisältävät henkilötietoja kuluttaja-asiakkaista. Tarkoituksena oli selvittää, kuinka paljon, minkälaisia ja missä Raisiolla on kuluttajarekisterejä. Kyselytutkimuksen kohderyhmään sisältyi Suomen lisäksi Ison-Britannian ja Tšekin liiketoiminta. Koko tutkimuksen taustalla on Raision halu selvittää kuluttajarekistereiden nykytila, jotta se voi varautua ja tehdä mahdolliset tarvittavat muutokset EU:n yleistä tietosuoja-asetusta varten. Tutkimukseen kuuluu myös osana ehdotus, kuinka Raision kuluttajarekisterejä voitaisiin mahdollisesti selkeyttää ja tehdä niistä tietoturvallisempia.

4.1 Kyselytutkimus

Kyselytutkimuksen avulla on tarkoitus saada koottua ennalta valitulta joukolta vastauksia samoihin kysymyksiin. Tutkimuksen kohteena on yleensä otoksella valittu kohderyhmä tietystä perusryhmästä. Kohderyhmän koko voi vaihdella suuresti ottaen huomioon kyselyn laadun ja sen tarkoitusperän. Kyselyn tulisi olla hyvin mietitty etukäteen, jotta kysymyksiin vastaaminen sujuu mahdollisimman yksiselitteisesti ja empimättä. Tämän takia kyselylomake on hyvä suunnitella yhteistyössä kohderyhmän edustajan kanssa. Varsinkin kyselyn esikokeilu on tärkeää, jotta turhat ja epäselvät kysymykset voidaan korjata tai poistaa. Lopullisen kyselyn tulisi olla niin lyhyt, yksinkertainen ja suoraviivainen kuin mahdollista. (Virtuaaliammattikorkeakoulu 2016.)

Osana opinnäytetyötä toteutettiin kyselytutkimus. Kyselyn avulla kartoitettiin Raision kuluttajarekistereiden määrä ja niiden nykytila. Kysely toteutettiin käyttäen verkkoselainpohjaista Webropol-työkalua. Näin pystyttiin luomaan yksinkertainen, englanninkielinen ja suurimmaksi osin suljettuihin kysymyksiin pohjautuva kyselylomake, johon kohderyhmän jäsenet saivat kutsulinkin sähköpostitse. Kohderyhmä koostui yhteensä 20 ihmisestä, jotka oli valittu ennalta. Henkilöjen valinta perustui siihen, että heidän tiedettiin varmasti olevan tekemisissä Raision kuluttajarekistereiden kanssa. Ennakkovalinnan oli suorittanut Raisio, ja se ei ole osa tätä opinnäytetyötä.

Kyselytutkimus toteutettiin 8.3.–4.4.2016, ja siihen vastasi lopulta 16 henkilöä. Neljä henkilöä jätti vastaamatta. Näiden henkilöiden vastaukset on sisällytetty joko jonkun muun vastaajan vastauksiin tai he eivät voineet antaa vastauksia muista syistä. Kyselylomake sisälsi yhteensä 15 kysymystä, joista yksi oli avoin.

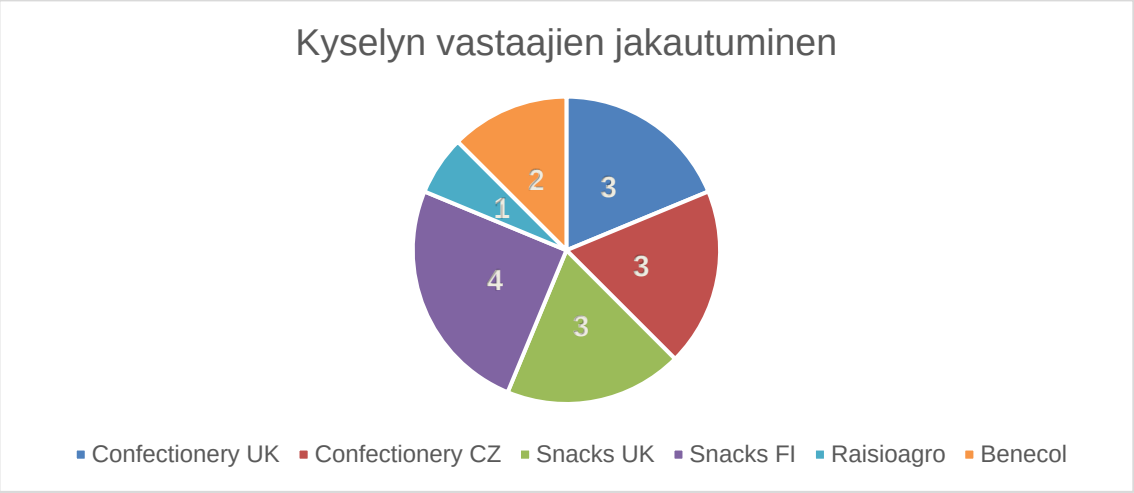
4.2 Kysely Raisio-konsernin työntekijöille

Kyselyn tuloksien analyysitavaksi on valittu yksikkölähtöisyys. Kyselyn vastaajat ovat kuudesta eri Raisio-konsernin yksiköstä. Nämä yksiköt ovat: Benecol, Confectionery CZ, Confectionery UK, Raisioagro, Snacks FI ja Snacks UK. Seuraavaksi käydään läpi kysymykset 2–15 yksilöllisesti ja analysoidaan, miten Raision yksiköt ovat vastanneet kysymyksiin. Yksiköiden vastaukset koottiin myös erilliselle Excel-taulukolle, joka on toimitettu Raisiolle. Excel-taulukosta selviää tarkemmin, mitä kukin vastaaja oli vastannut. Taulukkoa ei ole lisätty tähän työhön julkisesti, koska se sisältää tietoa jonka Raisio konserni haluaa pitää salassa.

Kysymys 2: *” Mikä on yksikkösi Raisio-konsernissa?”*

Vastausvaihtoehdot: “Confectionery UK”, “Confectionery CZ”, “Snacks UK”, “Snacks FI”, “Raisioagro” ja “Benecol”.

Vastaajia oli yhteensä 16. Jokaisesta yksiköstä oli vähintään yksi vastaaja, joten tuloksia pystyttiin analysoimaan kaikkien yksikköjen osalta. Vastaajien määrä vaihteli 1–4 yksikköä kohden. (Kuva 1)

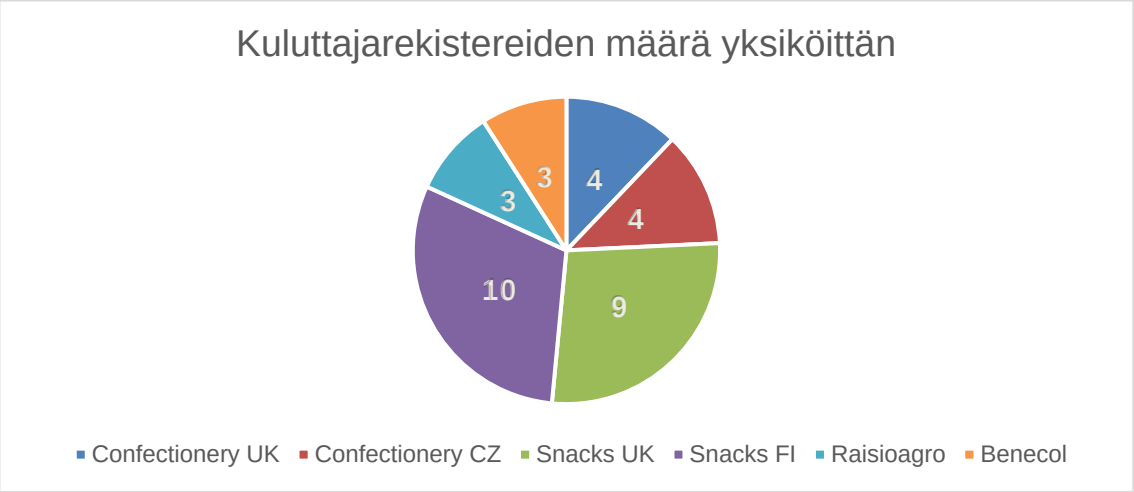


Kuva 1. Vastaajien jakautuminen.

Kysymys 3: *” Kuinka monta kuluttajarekisteriä teillä on? (Tarkka määrä)”*

Vastausvaihtoehto: Avoin numerokenttä

Kuluttajarekistereitä oli yhteensä 33, joissa suurimmassa osassa kahden yksikön alaiset toimijat ovat rekisterinpitäjinä. Loput rekisterit jakautuivat aika tasaisesti loppujen neljän yksikön kesken. Tuloksien perusteella voidaan päätellä, että tiettyjen yksiköiden toiminnassa henkilötietojen kerääminen on oleellisempaa ja laajempaa kuin muissa yksiköissä. (Kuva 2)

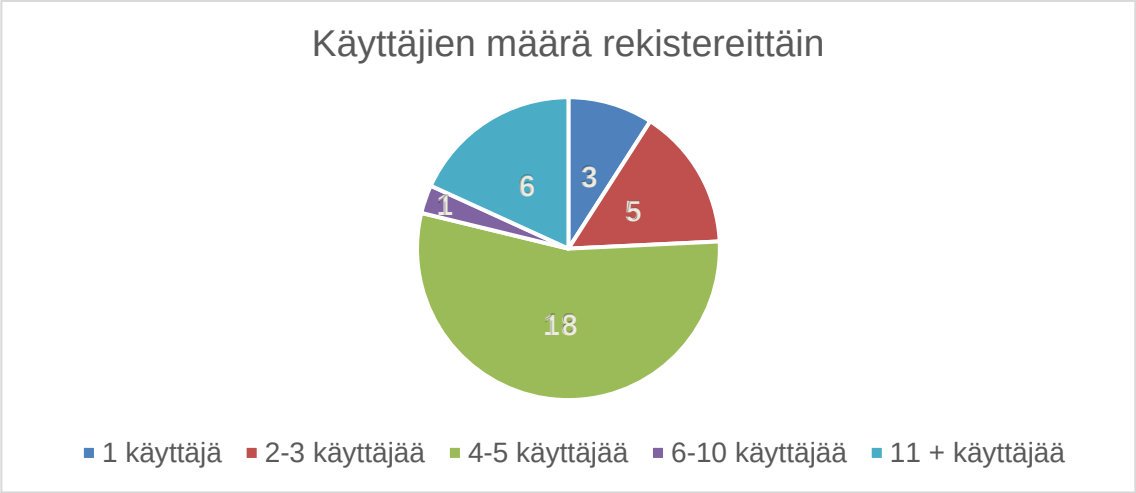


Kuva 2. Kuluttajarekistereiden määrä.

Kysymys 4: *”Kuinka monella työntekijällä on oikeus käyttää teidän kuluttajarekistereitä? (Arvio)”*

Vastausvaihtoehdot: ”1”, ”2–3”, ”4–5”, ”6–10” ja ”11 tai enemmän”

Enimmäkseen rekistereissä oli 4–5 käyttäjää tai alle. Nämä käyttäjämäärät ovat vielä hyviä ja suhteellisen tietoturvallisia, mutta mitä enemmän henkilöitä saa käyttää rekistereitä, sitä suuremmaksi tietoturvariskit nousevat. Kun henkilö määrä ylittää yli 11 ihmisen, pitäisi vakavasti harkita voitaisiinko tätä määrää rajoittaa pienemmäksi ja valvotummaksi. Tämä koskee eritoten rekistereitä, jotka sisältävät profiloivia tai arkaluonteisia henkilötietoja. Kolmessa yksikössä on kuluttajarekistereitä, joita saa käyttää 11 henkilö tai enemmän. Näiden rekistereiden kohdalla käyttäjämäärän uudelleenarviointi voisi olla paikallaan riippuen rekisterien luonteesta. (Kuva 3)



Kuva 3. Käyttäjien määrä rekistereittäin.

Kysymys 5: *”Kuinka monella työntekijällä on oikeus muokata teidän kuluttajarekistejä? (Arvio)”*

Vastausvaihtoehdot: ”1”, ”2–3”, ”4–5”, ”6–10” ja ”11 tai enemmän”

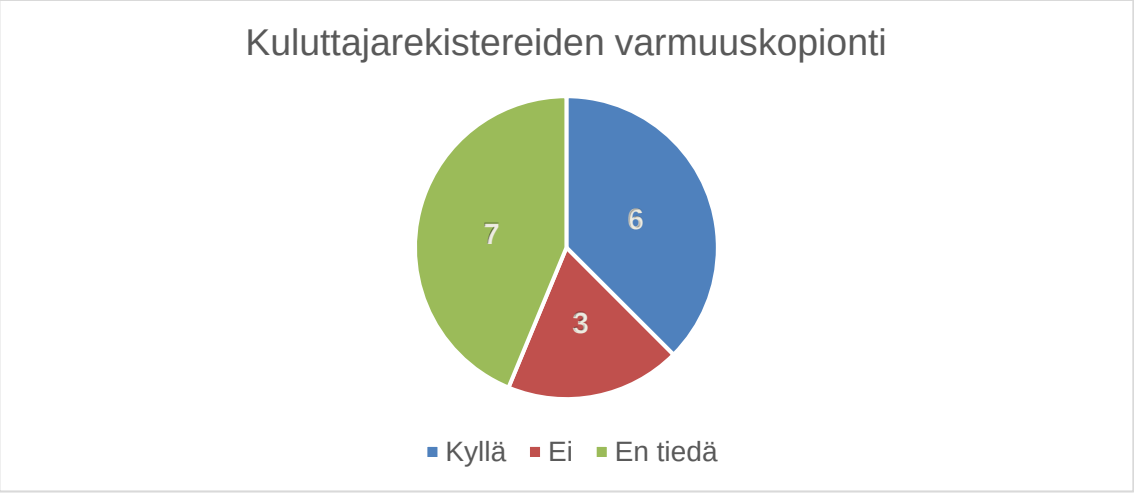
Muokkaajien määrä jäljittelee osittain edellä läpi käydyn käyttäjien määrää. Tämä ei ole mikään yllätys, koska työntekijä voi hyvin olla molemmat käyttäjä ja muokkaaja. Kun katsotaan kaikkia rekistereitä kokonaisuutena, niin huomataan että suurimassa osassa rekistereitä saa muokata 4–5 henkilöä tai alle. Tämä on hyvä asia, koska mitä pienempi muokkaaja määrää on, sitä pienempi virheiden ja rikkomusten mahdollinen määrä sekä vastuullinen henkilö on silloin helpompi selvittää. Kun muokkaajia alkaa olemaan 11 tai enemmän, niin muokkaajien määrän uudelleenarviointi voisi olla oleellista. (Kuva 4)

Kuva 4. Muokkaajien määrä rekistereittäin.

Kysymys 6: *”Otatteko varmuuskopioita kuluttajarekistereistänne?”*

Vastausvaihtoehdot: ”Kyllä”, ”Ei” ja ” En tiedä”.

16 vastaajasta kuuden vastaajan kuluttajarekisterit varmuuskopioidaan ja kolmen vastaajan rekistereitä ei varmuuskopioida. Varmuuskopiointi on järkevää kun tiedon uudelleen hankkiminen on vaikeaa tai se vaatii suuria kustannuksia. Kuluttajarekistereitä varmuuskopioidessa pitää ottaa huomioon, että tieto pysyy salaisessa muodossa myös varmuuskopiossa ja eikä siihen pääse käsiksi ulkopuolisia ihmisiä. Tähän kysymykseen ei ole konkreettista oikeaa vastausta, koska kuluttajarekistereiden varmuuskopioinnin tarpeellisuus riippuu paljon siihen mitä henkilötietoja rekisterit pitävät sisällään. Huolestuttavaa tämän kysymyksen kohdalla on se, että seitsemän vastaaja ei tiedä varmuuskopioidaanko heidän kuluttajarekistereitä. Tämä olisi hyvä selvittää jokaisen vastaajan kohdalla. Eritoten tietyn yksikön kohdalla, jonka kaikki vastaajat vastasivat ”En tiedä”. (Kuva 5)



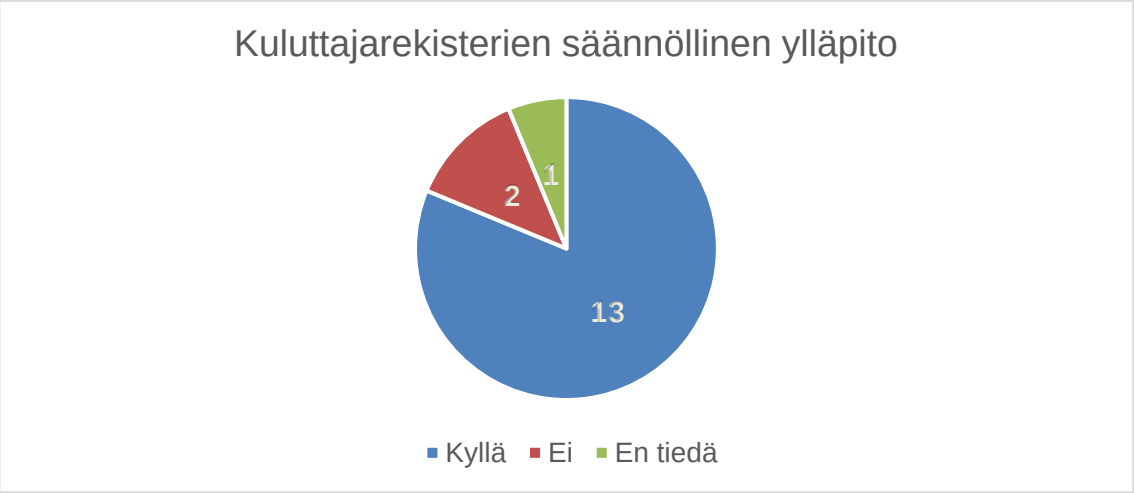
Kuva 5. Kuluttajarekistereiden varmuuskopiointi.

Kysymys 7: *”Ylläpidättekö kuluttajarekistereitänne säännöllisesti?”*

Vastausvaihtoehdot: ”Kyllä”, ”Ei” ja ” En tiedä”.

16 vastaajasta 13 vastasi, että heidän kuluttajarekistereitä ylläpidetään säännöllisesti. Tämä tieto on tärkeä, koska voidaan olettaa, että näiden vastaajien rekisterit ovat ajan tasalla ja niissä ei ole ylimääräisiä tai turhia henkilötietoja. Kaksi vastasi, että heidän rekistereitä ei säännöllisesti ylläpidetä ja yksi, että ei tiedä. Näiden vastaajien rekisterien

kohdalla pitäisi tarkastaa, ovatko nämä kuluttajarekisterit enää tarpeellisia. Jos rekisterit eivät enää ole tarpeellisia, ne tulisi poistaa heti kun on mahdollista. (Kuva 6)

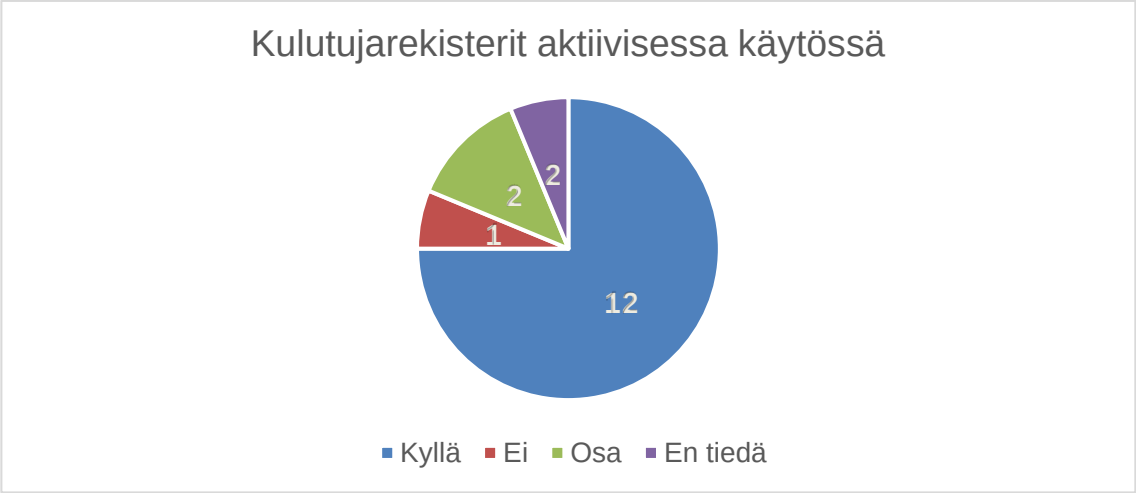


Kuva 6. Kuluttajarekisterien ylläpito.

Kysymys 8: *”Ovatko teidän kuluttajarekisterit aktiivisessa käytössä?”*

Vastausvaihtoehdot: ”Kyllä”, ”Ei”, ”Osa” ja ” En tiedä”.

Vastaajista 12 oli kaikki kuluttajarekisterit aktiivisessa käytössä. Näiden rekisterien osalta asiat ovat kunnossa, koska voidaan olettaa että myös ylläpito on ajan tasalla. Kaksi vastasi, että rekisterit ovat osittain käytössä. Näiden vastaajien rekisterien kohdalla pitäisi selvittää mitkä rekisterit on käytössä ja mitkä ei. Sama pätee myös ”En tiedä”-vastanneen henkilön kohdalla. Yleisesti ottaen kaikki rekisterit, jotka eivät ole aktiivisessa käytössä pitäisi poistaa, jos niille ei ole enää käyttötarkoitusta.(Kuva 7)

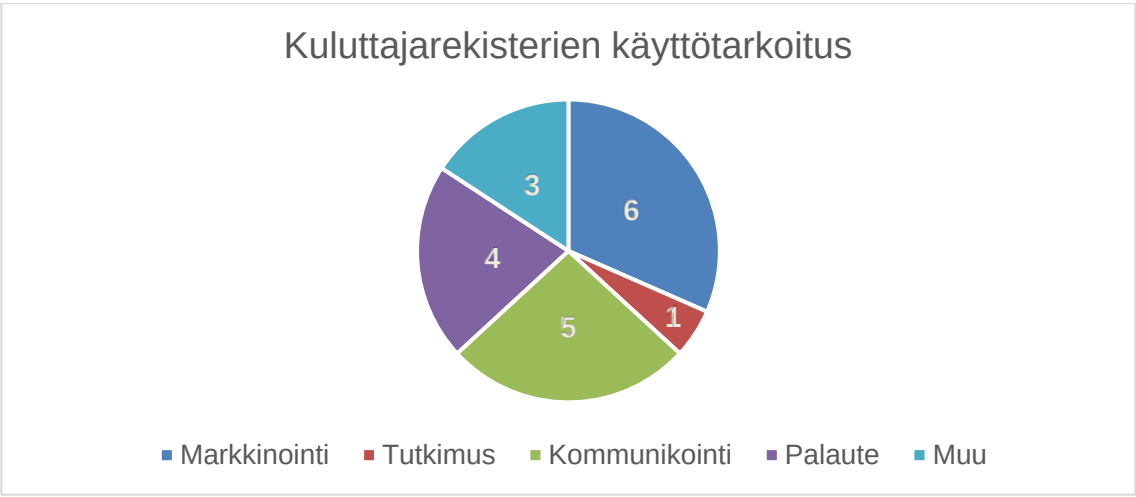


Kuva 7. Kuluttajarekisterit aktiivisessa käytössä.

Kysymys 9: *”Mitä käyttötarkoitusta varten keräätte henkilötietoja rekistereihinne?”*

Vastausvaihtoehdot: ”Markkinointi”, ”Tutkimus”, ”Kommunikointi”, ”Palaute” ja ”Muu”

Kaikki kuusi yksikköä keräsi henkilötietoja kuluttajarekistereihin markkinointia varten. Toiseksi tärkein käyttö kohde oli kommunikointi, jota varten viisi yksikköä keräsi henkilötietoja. Palautetta oli myös tärkeä käyttötarkoitus rekistereille ja sitä varten neljä yksikköä keräsi henkilötietoja. Muuta käyttötarkoitusta varten henkilötietoja keräsi kolme yksikköä ja tutkimusta varten vain yksi. Kysymyksen tulosten perusteella voidaan päätellä, että markkinointi ja kommunikointi ovat Raision tärkeimmät käyttötarkoitukset kuluttajarekistereille. (Kuva 8)

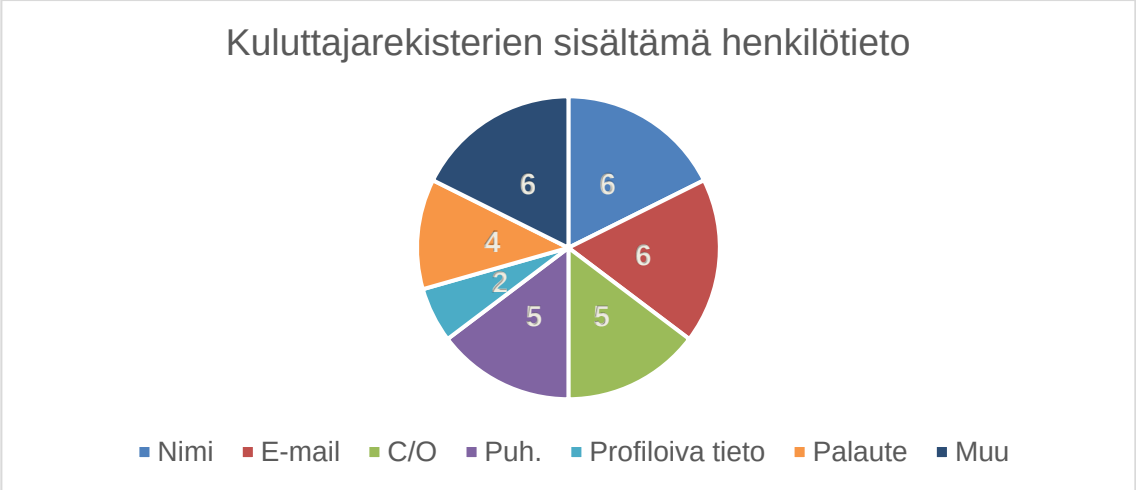


Kuva 8. Kuluttajarekisterien käyttötarkoitus.

Kysymys 10: *” Minkälaista tietoa keräätte teidän kuluttajarekistereihinne?”*

Vastausvaihtoehdot: ”Nimi”, ”Sähköposti”, ”Postiosoite”, Puhelinnumero”, ”Profiloivia tietoja”, ”Palaute”, ”Muu”

Kaikki kuusi yksikköä keräsi nimiä, sähköpostiosoitteita ja muita tietoja rekistereihinsä. Myös postiosoitteet ja puhelinnumerot olivat viidelle yksikölle tärkeitä. Kommunikointiin tarvittavat yhteistiedot ovat selvästi tärkeitä jokaisessa yksikössä. Palautteita ja muita tietoja kirjataan myös aktiivisesti rekistereihin. Profiloivien tietojen kohdalla kannattaa tarkastaa ovatko ne oleellisia EU:n yleistä tietosuoja-asetusta silmällä pitäen. (Kuva 9)



Kuva 9. Kuluttajarekisterien sisältämä henkilötieto.

Kysymys 11: *”Millä tavoin keräätte tietoja kuluttajarekistereihinne?”*

Vastausvaihtoehdot: ”Puhelimitse”, ”Sähköpostin avulla”, ”Kyselyjen avulla”, ”Markkinoinnin avulla”, ”Yhteystyökumppaneilta”, ”Ulkoisista tietokannoista” ja ”Muulla tavalla”

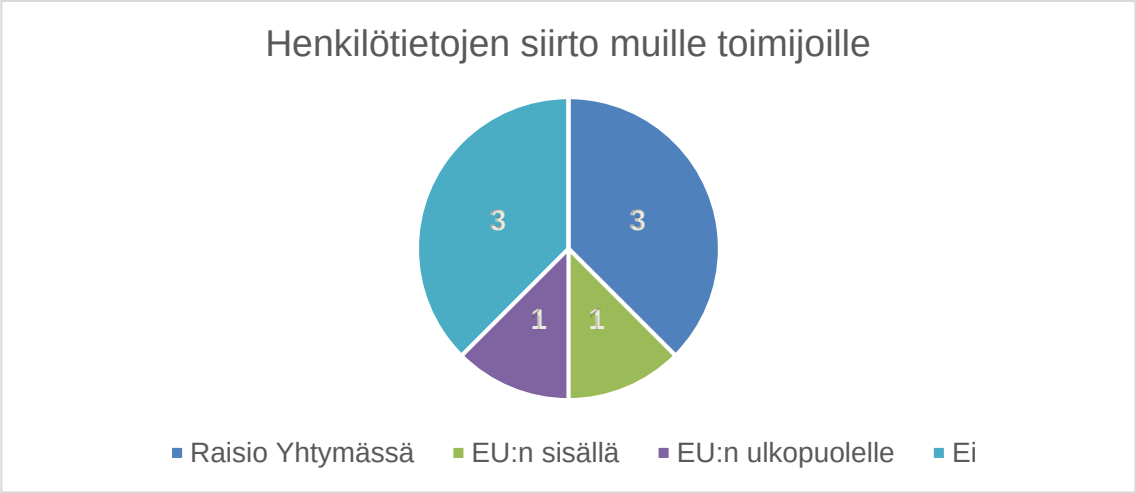
Kyselystä selviää, että yksiköt keräävät tietoa laajasti erilaisilla tavoilla. Tällä tavalla saadaan tavoitettua monia eri kohderyhmiä. Puhelin, sähköposti, markkinointi ja yhteistyökumppanien avulla tapahtuva tiedonkeruu oli selvästi suosituinta yksiköissä. Yllättävää tässä oli se, että puhelimitse tapahtuva tiedonkeruu on edelleen näin suosittua. Yksi asiakas kerrallaan tapahtuva tiedonkeruu ei yleensä ole kustannustehokasta, jos sama kohderyhmä voidaan tavoittaa joukkoviestinnän avulla. (Kuva 10)

Kuva 10. Henkilötietojen keräystavat

Kysymys 12: *”Siirrättekö henkilötietoja muille toimijoille?”*

Vastausvaihtoehdot: ”Raisio-konsernin sisällä”, ”Tutkimustarkoitukseen”, ”EU:n sisällä”, ”EU:n ulkopuolelle”, ”Ei”, ”Muu”.

Kolmessa yksikössä ei harjoitetta ollenkaan kerättyjen henkilötietojen siirtämistä muille toimijoille. Henkilötietojen siirto kannattaa aina minimoida, jos se ei ole liiketoiminnan kannalta olennaista. Näin pystytään pitämään henkilötiedot paremmin suojassa ja pois haitallisten osapuolten silmistä. Kolme yksikköä siirtää henkilötietoja Raisio-konsernin sisällä. Tämänlaisen tiedonsiirron yhteydessä on hyvä tarkastaa, että henkilötietojen siirto tapahtuu salatusti ja turvallisesti, jos tietojen luonne sitä vaatii. Tämä pätee myös yhden yksikön harjoittamassa EU:n sisällä ja ulkopuolella tapahtuvassa henkilötietojen siirtämisessä muille toimijoille. EU:n yleinen tietosuoja-asetus tuo uusia säännöksiä henkilötietojen siirtämiseen muille toimijoille, jotka pitää ottaa huomioon EU:n sisällä ja ulkopuolelle tapahtuvassa henkilötietojen siirrossa. Kuvassa 11 pitää ottaa huomioon, että sama yksikkö voi harjoittaa monenlaista tiedonsiirto muille toimijoille. (Kuva 11)

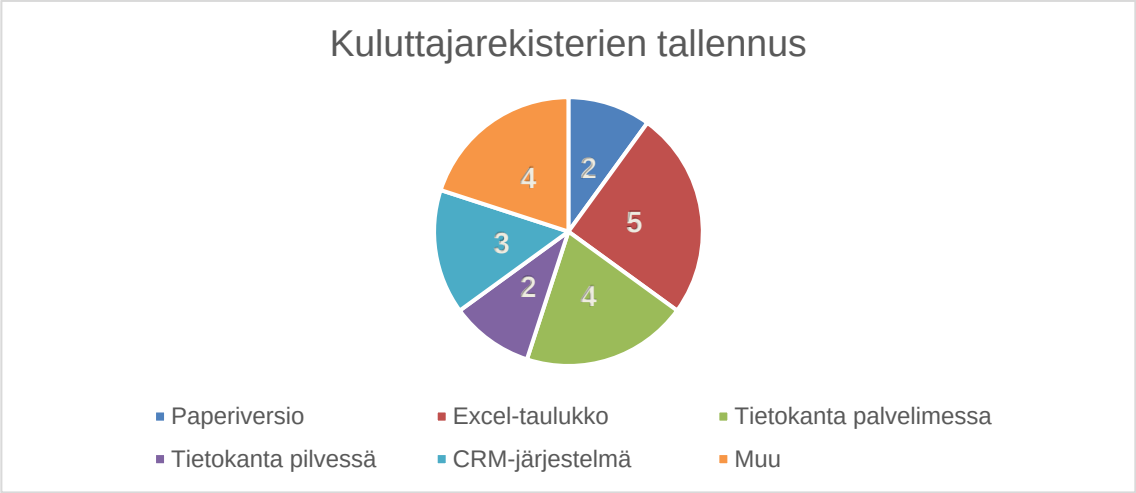


Kuva 11. Henkilötietojen siirto.

Kysymys 13: *”Minne tallennatte kuluttajarekisterinne?”*

Vastausvaihtoehdot: ”Paperiversioon”, ”Excel-taulukkoon”, ”Tietokantaan palvelimella”, ”Tietokantaan pilvessä”, ”CRM-järjestelmään” ja ”Muu”

Excel-taulukkoihin kuluttajarekisterien tallentaminen oli selvästi yleisin vastaus yksikköjen keskuudessa. Excel on hyvä ratkaisu, koska se on suhteessa paljon helpompi käyttää kuin erilaiset tietokannat tai CRM-järjestelmät. Toiseksi yleisin oli kuluttajarekisterien tallentaminen tietokantaan palvelimeen. Palvelimeen tallentaminen lisää tietoturvaa, varsinkin jos palvelimet sijaitsevat yksikön omissa tiloissa ja niihin saa yhteyden vain sisäverkon tai VPN-yhteyden kautta. Pilvipalvelua käytti kaksi yksikköä. Pilven hyvä puoli on tiedon helppo saatavuus paikasta riippumatta. Pienenä yllätyksenä tuli, että jotkut yksiköt luottavat vielä paperiversioina oleviin kuluttajarekistereihin. Suhteessa muihin menetelmiin tiedon paperiversioon kerääminen, jakaminen ja turvassa pitäminen on paljon työläämpää kuin muut olemassa olevat keinot. Nämä rekisterit olisi hyvä siirtää digitalliseen muotoon, jos ne ovat vielä oleellisia. CRM-järjestelmiä käytti vain puolet yksiköistä. CRM-järjestelmän hyvä puoli on tiedon käytön monipuolisuus, mutta myös vaatii käyttäjältä järjestelmän osaamista. (Kuva 12)



Kuva 12. Kuluttajarekisterien tallennus.

Kysymys 14: *”Minkälaisia tietoturvamenetelmiä käytätte turvaamaan kuluttajarekisterinne?”*

Vastausvaihtoehto: Avoin vastaus

Tämän kysymyksen avulla haettiin tarkemmin tietoa, minkälaisilla tietoturvatoimilla kuluttajarekisterit ovat suojattu. Vastauksien luonne vaihteli suuresti, koska kyselyn kohderyhmä sisälisi vastaajia monilta eri aloilta, eikä heiltä voi olettaa yksiköiden tietoturvatoimien tai IT-alan käytäntöjen laajaa osaamista. Täten vastaukset olivat erittäin suurpiirteisiä ja lyhyitä.

Yleisin vastaus kysymykseen oli yksinkertaisesti salasana. Vastauksissa ei määritellyt lähes ollenkaan mihin salasana edes liittyy. Muutamassa vastauksessa oli määritelty, että salasana liittyy Windows-käyttöjärjestelmään tai tiettyyn CRM-järjestelmään.

Osa yksiköistä vastasi, että saatavuutta ja muokattavuutta on rajoitettu. Näissäkään vastauksissa ei ollut lähes ollenkaan kuvailtu, miten tämä on toteutettu. Ainot tarkennukset olivat, että tietyissä yksiköissä pääsy palvelimeen, tiloihin ja Excel-tiedostoihin oli rajattu.

Edellä mainittujen lisäksi oli vastattu, että tietoturva on taattu käyttämällä yhteystyökumppania, mutta ei kerrottu miten tämä on toteutettu. Muut huomiotavat vastaukset olivat, että henkilötietoja ei jaeta kolmansien osapuolinen kanssa ja, että henkilötietojen käsittelyyn pyydetään aina kyseisten tietojen omistajan lupa.

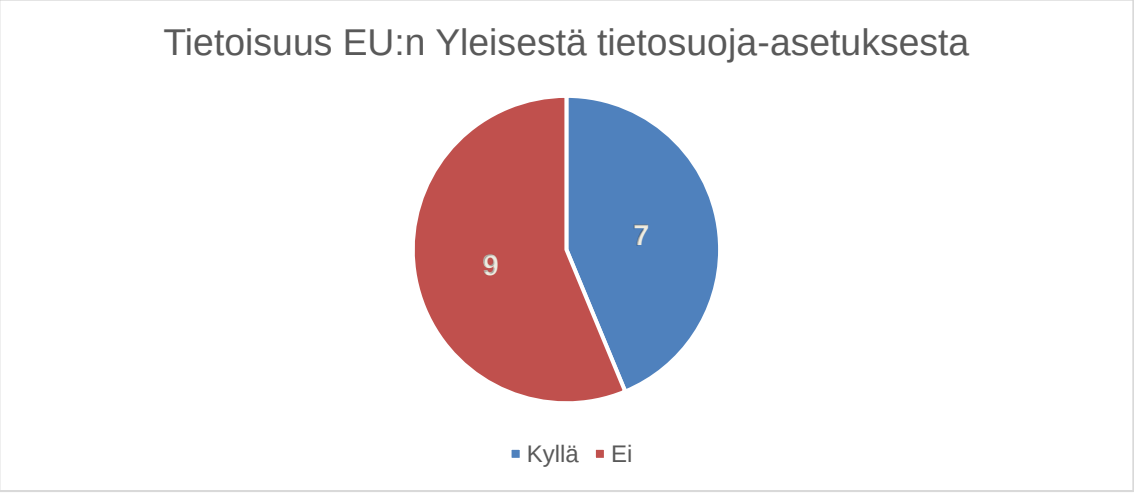
Tämän kysymyksen vastaukset osoittavat, että vastaajat eivät kovin hyvin tiedä miten heidän kuluttajarekistereitään suojataan, tai vastaajat olivat ymmärtäneet kysymyksen

väärin. Jos kysymys on tiedon puutteesta, asiaan olisi hyvä puuttua, jotta ne henkilöt jotka ovat vastuussa, tietäisivät edes perusasiat tietoturvasta liittyen heidän kuluttajarekistereihin ja niiden suojaamiseen.

Kysymys 15: *”Oletko tietoinen Euroopan unionin tulevasta yleisestä tietosuoja-asetuksesta?"*

Vastausvaihtoehdot: ”Kyllä” ja ”Ei”

Vastaajista seitsemän oli tietoinen Euroopan unioni tulevasta yleisestä tietosuoja-asetuksesta ja yhdeksän ei tiennyt asiasta. Tästä asiasta on hyvä järjestää koulutusta, kun 2016 kevään aikana tulee viimeinen virallinen versio yleisestä tietosuoja-asetuksesta. Asetusta ruvetaan panemaan käytäntöön kahden vuoden siirtymäajalla. Siirtymäajan aikana on hyvä saada jokainen Raisio-konsernissa työskentelevä rekisterinpitäjä ja henkilötietoinen käsittelijä tietoiseksi asetuksen tuomista uusista säännöksistä ja vastuista. (Kuva 13)



Kuva 13. Tietoisuus EU:n yleisestä tietosuoja-asetuksesta.

4.3 Kuluttajarekisterien selkeyttäminen

Kun vertaa eri yksiköiden vastauksia kyselyyn, huomataan että yksiöiden välillä on eroja kuluttajarekisterien hallinnan, säilyttämisen ja turvallisuuden ohella. Kuluttajarekisterien selkeyttämiseksi ja valmistamiseksi EU:n yleistä tietosuoja-asetusta varten olisi hyvä luoda yhtenäiset konsernitason ohjeistukset ja periaatteet, mitä jokaisen yksikön tulisi noudattaa. Näin pystyttäisiin paremmin valvomaan ja ohjaamaan kuluttajarekisterien keräämistä ja käyttöä.

Tämä prosessi olisi parasta aloittaa inventoimalla olemassa olevat kuluttajarekisterit. Ensisijaisesti käydä läpi kaikki olemassa olevat rekisterit ja määritellä ovatko ne enää liiketoiminnan kannalta tärkeitä. Olennaiset rekisterit säilytetään ja turhat rekisterit poistetaan tietoturvallisella tavalla. Kuluttajarekisterit, jotka säilytetään pitää myös inventoida epäoleellisen ja turhan tiedon varalta. Tämä prosessi on aikaa vievä, mutta mitä tehokkaammin tieto on minimoitu vain ajan tasalla oleviin olennaisiin henkilötietoihin, sitä pienemmät ovat tietoturvariskit. Tähän vaiheeseen sisältyy myös kuluttajarekisterien käyttäjien ja muokkaajien inventointi. Tällä hetkellä joissain rekistereissä nämä määrät vaikuttaa olevan aivan liian suuria. Olisi hyvä, että rekistereitä saisi käyttää ja muokata vain oleelliset ihmiset, varsinkin jos kuluttajarekisterit sisältävät arkaluonteisia henkilötietoja.

Kun kuluttajarekisterit on inventoitu ja minimoitu vain oleellisiin rekistereihin, niille on hyvä löytää yhtenäinen konsernin tasolla päätetty tallennustapa. Tällä hetkellä eri yksiköillä on monia eri tapoja säilyttää kuluttajarekistereitä. Tähän on tehtävä muutos. Paperiversion säilytettävät rekisterit tulisi digitalisoida ja sähköpostissa olevat rekisterit tulisi tallentaa muualle. Ongelmana on kuitenkin, mikä on hyvä tapa säilyttää kuluttajarekistereitä. Rekistereitä kuitenkin muokkaa ja käyttää ihmiset, jotka eivät ole IT-alan asiatuntijoita. Näin ollen tietokannat ja CRM-järjestelmät eivät välttämättä ole paras vaihtoehto sekä yhteistyökumppaneiden käyttö rekisterien tallennuskohteena on taas lisäkustannus.

Ehdotan, että kuluttajarekisterit, joissa Raisio-konsernin yksiköt ovat rekisterinpitäjiä, tallennettaisiin joko yhtenäisesti tai yksikkökohtaisesti luotettavalta toimijalta hankittuun pilvipalveluun. Tallennusmuoto olisi Excel-formaatti sen helppokäyttöisyyden takia. Näin Raisiolla olisi yhtenäinen kuluttajarekisteritietokanta, jota olisi helppo ja turvallinen muokata tarvittaessa. Kuluttajarekisterien valvonta olisi myös paljon helpompaa, kun kaikki

löytyvät yhdestä paikasta. Tämän uuden tietokannan valvonnasta, turvallisuudesta ja käyttöoikeuksista vastaisi Raisio-konsernin IT-osasto.

Toisena vaihtoehtona voitaisiin käyttää Raisio-konsernin olemassa olevia omia palvelimia tallennuskohteena. Tämä ei lisäisi kustannuksia, kun ei tarvitse hankkia lisäpalveluja. Ideana pysyisi edelleen yhtenäinen kuluttajarekisteritietokanta, josta eri yksiköiden asiankuuluvat henkilöt voisivat käyttää hyväkseen. Tämä voitaisiin esimerkiksi toteuttaa VPN-yhteyttä ja Microsoft Sharepointia tai Web UI:ta käyttäen.

Tallennustavan valitsemisen ja täytäntöönpanon jälkeen luotaisiin yhtenäiset ohjeistukset kuluttajarekisterien keräämiselle, käytölle ja ylläpidolle. Nämä ohjeet luotaisiin Euroopan unionin yleisen tietosuoja-asetusta noudattaen. Näin saataisiin ajan tasalla oleva toimintakehys millä valvottaisiin ja ohjattaisiin kuluttajarekistereihin liittyvää toimintaa tulevaisuudessa.

5 YHTEENVETO

Opinnäytetyön tavoitteena oli selvittää Raisio-konsernille Euroopan unionin tulevan yleisen tietosuoja-asetuksen olennaiset kohdat. 2016 keväällä voimaan tulevaa asetusta ruvetaan ottamaan käyttöön kahden vuoden siirtymäajalla. Raisio halusi varautua tähän hyvissä ajoin selvittämällä, mitä tietosuoja-asetus tuo mukanaan yksityisen yrityksen kannalta. Tietosuoja-asetukseen liittyen opinnäytetyöhön tehtiin myös kyselytutkimus Raisio konsernin kuluttajarekistereistä. Kyselytutkimuksen avulla selvitettiin Raisio-konsernin eri yksiköiden kuluttajarekisterien määrä ja nykytila kansainvälisesti.

Suomessa tällä hetkellä voimassa oleva henkilötietolaki määrittelee, miten ja mitä henkilötietoja saa kerätä erilaisiin rekistereihin. Suomen henkilötietolaki on jo nyt laaja ja kattava, mutta Euroopan unioni haluaa korvata kansallisen lainsäädännön yhteisellä kokonaisvaltaisella asetuksella. Yleinen tietosuoja-asetus tulee tuomaan lisää oikeuksia jokaiselle luonnolliselle henkilölle liittyen hänen tietojensa keruuseen, käyttämiseen ja säilyttämiseen. Tavoite tietosuoja-asetuksella on lisätä yksityisyyden vapautta unionin sisällä ja tehdä organisaatioista, jotka tätä asetusta rikkovat, tilivelvollisia Europan unionille, jäsenvaltiolle sekä rikkomuksen kohteelle.

Yleisen tietosuoja-asetuksen käyttöön ottaminen ei tule olemaan ongelmaton, koska jokaisen EU:n jäsenvaltion pitää ottaa se käytäntöön oman valtion ja lain määrittelemissä kehyksissä. Nähtäväksi jää, kuinka tarkasti jäsenvaltiot tulevat seuramaan ja tottelemaan asetusta. Suomessakaan tietosuoja-asetusta ei tulla ottamaan sellaisenaan käyttöön vaan sitä tullaan siirtymä-ajalla soveltamaan Suomen lakiin sopivaksi. Vain aika tulee näyttämään, luopuuko Suomi kokonaan omasta henkilötietolainsäädännöstä vai tehdäänkö siihen lisäyksiä EU:n asetuksen pohjalta.

Raisio haluaa joka tapauksessa valmistautua tulevaan muutokseen. Tässä opinnäytetyössä käydään yksityisen yrityksen kannalta ne yleisen tietosuoja-asetuksen luvut ja artiklat, jotka voivat mahdollisesti vaikuttaa Raision toimintaan. Nämä tiedot on kerätty vuonna 2016 tulleesta yleisestä tietosuoja-asetuksesta, joka oli opinnäytetyön tekohetkellä uusin mahdollinen lähdemateriaali. Tiedon keruussa oli jonkun verran ongelmia, mutta tietosuojavaltuutetun toimiston ja oikeusministeriön tiedotteiden avulla saatiin koottua tiivistelmä yleisen tietosuoja-asetuksen oleellisista artikloista.

Kyselytutkimuksen avulla saatiin selville, mikä on Raisio-konsernin kuluttajarekisterien nykytila ja missä on parantamisen varaa. Tutkimus toteutettiin käyttämällä Webropol-työkalua. Itse tutkimuksen tekeminen oli suoraviivainen prosessi kohderyhmän valinnasta kysymyspatterin tekemiseen englanniksi ja lopulta kyselyn täytäntöönpanoon. Kyselyn vastaukset olivat hyviä, ja niistä saatiin paljon uutta tietoa. Näiden tietojen pohjalta koottiin ehdotus, miten Raisio voisi mahdollisesti selkeyttää kuluttajarekistereitään. Prosessi olisi neljä vaihetta, joka sisältäisi inventoinnin, uudelleenjärjestämisen ja uudelleenohjeistuksen ja valvonnan. Ehdotuksen hyväksikäyttämien voisi antaa lisää valmiutta Raisiolle jatkaa valmistautumista Euroopan unionin yleistä tietosuoja-asetusta varten.

LÄHTEET

COM(2012) 11 final. Euroopan parlamentin ja neuvoston ehdotus yleisestä tietosuoja-asetuksesta. 10.3.2016 http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52012PC0011&from=EN

Eurooppa-neuvosto 2016. Tietosuojan uudistus. Viitattu 28.2.2016 http://www.consilium.europa.eu/fi/policies/data-protection-reform/data-protection-regulation/

Henkilötietolaki 523/99. Annettu Helsingissä 22.4.1999 [verkkoaineisto]. Valtion säädöstietopankki Finlex. Viitattu 23.2.2016 http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Oikeusministeriö 2016. Euroopan unionin tietosuojalainsäädännön uudistaminen. Viitattu 10.3.2016. http://www.oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/euroopanunionintietosuojalainsaadannonuudistaminen.html

Procurement policy note 2012. European legislative proposals on third country access to the EU public procurement market. Viitattu 21.5.2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62096/PPN-European-legislative-proposals-on-third-country-access-to-the-EU-public-procurement-market.pdf

Raisio 2016. Raisio-konserni. Viitattu 6.4.2016 http://www.raisio.com/fi/raisio-konserni

Rope, T. & Pöllänen, J.1995. Asiakastyytyväisyysjohtaminen. 3. painos. Juva: WSOY.

Schofield, T. 2016. What is a Customer Database? – Definition & Benefits. Viitattu 22.2.2016 http://study.com/academy/lesson/what-is-a-customer-database-definition-benefits.html

Suomen internetopas 2016. Tietoturva. Viitattu 21.3.2016 http://www.internetopas.com/yleistietoa/tietoturva/

Techtarget 2016a. User interface (UI). Viitattu 18.5.2016 http://searchsoa.techtarget.com/definition/user-interface

Techtarget 2016b. Customer relationship management. Viitattu 19.5.2016 http://searchcrm.techtarget.com/definition/CRM

Techterms 2016. VPN. Viitattu 18.5.2016 http://techterms.com/definition/vpn

Tietosuojavaltuutetun toimisto 2010. Tietosuojavastaavan toimenkuva, tehtävät ja asema. Viitattu 22.3.2016 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqN4sf1/Tietosuojavastaavan_toimenkuva_tehtavat_ja_asema.pdf

Tietosuojavaltuutetun toimisto 2016a. Ota oppaaksi henkilötietolaki! Viitattu 23.2.2016 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfq8WnQ7/Ota_oppaaksi_henkilotietolaki.pdf

Tietosuojavaltuutetun toimisto 2016b. EU:n tietosuojauudistus. Viitattu 10.3.2016 http://www.tietosuoja.fi/fi/index/lait/euntietosuojauudistus.html

Tietosuojavaltuutetun toimisto 2016c. Kysymyksiä ja vastauksia tietosuojauudistuksesta. Viitattu 21.5.2016 http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/kysymyksiajavastauksia.html

Virtuaaliammattikorkeakoulu 2016. Kyselyyn perustuvan tutkimuksen suorittaminen. Viitattu 6.4.2016 http://www2.amk.fi/digma.fi/www.amk.fi/opintojaksot/0709019/1193463890749/1193464131489/1194289345955/1194290010211.html

Yleinen tietosuoja-asetus 2016. Euroopan parlamentin ja neuvoston asetus. Viitattu 4.5.2016 http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN