Opinnäytetyö AMK

Liiketalouden koulutusohjelma

2019

Ida Karbin

EUROOPAN UNIONIN TIETOSUOJA-ASETUKSEN TÄYTÄNTÖÖNPANO KÄYTÄNNÖSSÄ

– Case Cygnaeus Morgonklubb rf.

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ AMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalouden koulutusohjelma

2019 | 33 sivua, 10 liitesivua

Ida Karbin

EUROOPAN UNIONIN TIETOSUOJA-ASETUKSEN TÄYTÄNTÖÖNPANO KÄYTÄNNÖSSÄ

- Case Cygnaeus Morgonklubb rf.

Tämän opinnäytetyön tavoitteena on selventää Euroopan Unionin uuden Tietosuoja-asetuksen tuomia uudistuksia sekä ottaa selvää, miten se käytännössä vaikuttaa niin toimeksiantajaan kuin yksittäiseen yksilöön. Vuoden 2018 toukokuussa käyntäntöön astunut asetus muuttaa henkilötietojen käsittelyyn liittyviä periaatteita sekä täsmentää erilaisia vaatimuksia tietojen käsittelyn kannalta. Tarkoituksena on siis tarkastella niin käytännön kuin teorian tuomia muutoksia. Toteutan opinnäytetyön tutkimuksen toiminnallisena, jonka seurauksena luon tietosuoja-selosteesta dokumentaation. Toiminnallisen opinnäytetyön puitteissa olen käyttänyt erilaisia lähteitä tukemaan tutkimusta.

Teoriaosassa käydään läpi lain säätämiä periaatteita sekä muuta tietoperustaa, johon opinnäytetyö rakentuu. Toimeksiantajan osalta toteutetaan niin tietosuojaseloste kuin asiakasrekisteri. Käyn myös läpi erilaisia muutoksia, joita toimeksiantajan tulee implementoida käytäntöönsä, jotta tietosuoja-asetus toteutuu kokonaisuudessaan.

Mielestäni opinnäytetyö tuo onnistuneesti esiin uuden tietosuoja-asetuksen tuomia muutoksia sekä pureutuu niiden käytännön aiheuttamiin seikkoihin. Tutkimusta tehdessä olen ottanut huomioon muutokset yleisesti sekä yhdistyksen kannalta. Yhdistyksen kannalta toimintaan ei juurikaan tule muutoksia vaan ainoastaan hienosäätöä.

ASIASANAT:

Tietosuoja, Euroopan Unioni, GDPR General Data Protection regulation, henkilötieto, rekisteröity

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business

2019 | 33 pages, 10 pages in appendices

Ida Karbin

IMPLEMENTATION OF GENERAL DATA PROTECTION REGULATION IN PRACTISE

- Case Cygnaeus After-school association

The purpose of this thesis is to clarify the reforms brought together by the new European Union Privacy Regulation and to explore how it will affect both the client and the individual in practice. The regulation, which came into force in May 2018, will change the principles governing the processing of personal data and specify the different requirements for the processing of personal data. The aim is therefore to examine the changes brought by both practical and theoretical considerations. I carry out the research of this thesis as a practice-based thesis.I will create documentation from the privacy policy. I have used variety of sources to support my practice-based research.

The theory section covers the principles of law and the other knowledge base on which the thesis is based. Both the Privacy Policy and the Customer Register are created both in Finnish and Swedish. I will also go over the various changes that the client will need to implement in order to put into practise the privacy policy in its entirety.

In my opinion the thesis successfully highlights the changes brought by the new General Data Protection Regulation and addresses the practical implications of these changes. While making the research I have taken into account the changes in general and association terms. From the associations point of view, there is not that many changes but only fine-tuning.

KEYWORDS:

Data protection, European Union, GDPR General Data Protection regulation, personal data, registered

SISÄLTÖ

LIITTEET

KÄYTETYT LYHENTEET JA SANASTO

Lyhenne	Lyhenteen selitys
GDPR	General Data Protection Regulation
EU	Euroopan Unioni
L	laki
r.f.	Förening, yhdistys

Sana	Selitys
Henkilötieto	Henkilötietoja ovat kaikki ne tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön.
Rekisteröity	Rekisteröity on henkilö, jota henkilötieto koskee.
Rekisterinpitäjä	Henkilö, yritys, viranomainen tai yhteisö, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.
Henkilötietojen käsittelijä	Rekisterinpitäjän ulkopuolinen taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (Tietosuoja, 2017).

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on selvittää, miten Euroopan Unionin uudistunut tietosuoja-asetus astuu voimaan suoraan käytännössä kyseessäolevan yhdistyksen silmin. Toteutan opinnäytetyön toiminnallisen tutkimusmenetelmän puitteissa. Toiminnallisen opinnäytetyön tavoitteena on luoda tuotos ja tämän opinnäytetyön osalta se tarkoittaa rekisterien luomista. Tiedonhaussa olen käyttänyt ajantasaisia lähteitä kuten kirjallisuutta sekä internettiä. Olen myös osana tiedonhakua tutkinut muita opinnäytetöitä sekä seurannut aktiivisesti aiheesta tehtyjä raportteja ja blogeja. Hakusanoina olen käyttänyt muun muassa ”tietosuoja”, ”GDPR” sekä ”henkilötieto”.

Kun puhutaan GDPR:stä puhutaan General Data Protection Regulationista (GDPR 2016/679) eli tuttavimmin Euroopan Unionin uudesta tietosuoja-asetuksesta, joka on astunut voimaan suoraan sovellettavana lainsäädäntönä 25.5.2018 alkaen koko Euroopan Unionin alueella. Euroopan Unioniin kuuluu tällä hetkellä 28 jäsenmaata (Euroopan Unioni, 2019), joilla jokaisella on toistaiseksi ollut hyvinkin erilaisia tapoja toteuttaa henkilötietoihin kohdistuvaa sääntelyä. EU:n tietosuoja-asetuksen ensisijainen tehtävä onkin yhtenäistää näiden jäsenvaltioiden sääntelyä, sekä vaatia valtioita suojaamaan henkilötietoja entistäkin tehokkaammin samanaikaisesti, kun tuotetun datan määrä kasvaa kasvuaan. Teknologian nopea kasvu on aiheuttanut kasvavissa määrin lisää henkilötietojen syntyä ja niiden varastoiminen, sekä henkilön, että yrityksen kannalta on nähty tärkeässä valossa.

Henkilötietoja ovat kaikki ne tiedot, joilla on tekemistä tunnistettuun tai tunnistettavassa olevaan ihmiseen (Tietosuojavaltuutetun toimisto, 2018). Tälläisiä tietoja ovat esimerkiksi nimi, josta voidaan tunnistaa suoraan kyseinen henkilö tai ikä, josta voidaan tunnistaa välillisesti olemassa oleva henkilö. Esimerkkejä henkilötiedoista ovat muun muassa potilastiedot, puhelinnumero ja sähköpostiosoite. Henkilötietoja ei ole niin sanotut anonymisoidut tiedot eli henkilötiedot joita on käsitelty niin, ettei kyseistä henkilöä voida niistä enään tunnistaa. Kyseisessä yhdistyksessä käsitellään lasten henkilötietoja, joten niiden käsittely eroaa hieman normaalista proseduurista.

Suomessa voimassa ollut entinen Henkilötietolaki (523/1999) tulee poistumaan kokonaisuudessaan uuden tietosuojauudistuksen alta. Tämän seurauksena myös yhdistyksen tulee muuttaa henkilötietojen käsittelyä nykyiselle vaadittavalle tasolle.

2 EUROOPAN UNIONIN TIETOSUOJA-ASETUS

Euroopan Unionin tietosuoja-asetuksella 679/2016 tarkoitetaan uutta, Euroopan jäsenmaiden sääntelyä yhdistävää uudistusta, jota kutsutaan myös GPDR:ksi eli General Data Protection Regulation (Hanninen ym. 2017,11). Asetus astuu voimaan suoraan sovellettevana lainsäädäntönä vuoden 2018 toukokuusta alkaen koko Euroopan Unionin alueella. Euroopan Unioniin kuuluu tällä hetkellä 28 jäsenmaata (europa.eu, 2019). Ennen uudistusta on siis ollut ainakin yli muutama tusina erilaista henkilötietojen käsittelyyn liittyvää asetusta. Suomessa GPDR:n edeltäjä oli Henkilötietolaki 523/1999, joka kumottiin vuoden 2018 lopulla. Koska EU:n tietosuoja-asetus jättää todella vähän liikkumavaraa, on Suomessa säädetty Tietosuojalaki (1050/2018) tukemaan ja täydentämään EU:n säädöksiä. Asetuksen ja lain tulisi yhdessä toimia siten, että ne eivät poissulje toisiaan eivätkä heikennä toisen vaikutusta. Euroopan Unionin yleistä tietosuoja-asetusta sovelletaan sekä automaattisen, että manuaalisen henkilötietojen käsittelyssä (Andreasson ym. 2017, 30.)

Tietosuoja-asetuksen päivittämiselle on jo pidemmän aikaa ollut tarvetta. Ensinnäkin, henkilötietojen määrä lisääntyy yhtäaikaisesti datan määrän kasvaessa. Toiseksi, evästeiden käyttö ja tarve kohdentaa mainontaa ovat myös lisänneet tarvetta tarkastella henkilötietoja uudella tavalla. Kolmanneksi, kansainvälistyminen on lisännyt tarvetta yhtenäistää jäsenmaiden välisiä sääntelytapoja.

Turun Sanomat kirjoitti vuoden 2018 toukokuussa seuraavanlaisesti: ” Yhdistykselle pitää kirjata ylös sisäinen dokumentaatio, jossa kerrotaan, miten yhdistys käsittelee henkilötietoja, kuten nimiä ja sähköpostiosoitteita”. Suomen sosiaali- ja terveys ry:n lakimies Maarit Päivike ja kuntaliiton erikoisasiantuntija Tuula Seppo kertoivat Turun Sanomien julkaisussa uusimman tietosuoja-asetuksen vaikutuksista yhdistysten henkilötietopolitiikkaan. Päivikkeen mukaisesti yhdistysten dokumentaatiota tehdessä tulee selvittää, miksi henkilötietoja kerätään. Sama toimintatapa koskee yrityksiä. Dokumentaatiota tehdessä voidaan hyödyntää jo olemassa olevaa jäsenrekisteriä, jos yhdistykseltä sellainen löytyy. Toimeksiantajalla ei ole vielä olemassaolevaa rekisteriä, joten rekisteri tulee luoda kokonaisuudessaan. Jäsenrekisterin omaavien yhdistysten tulee selkeästi tiedottaa jäsenilleen miten ja miksi tietoja käsitellään. Yhdistyksessä tietosuojavastaavaa tarvittaisiin, jos yhdistys käsittelisi esimerkiksi arkaluontoisia tietoja. (Turun Sanomat. 2018.) Toimeksiantaja ei käsittele arkaluontoisia tietoja, joten tietosuojavastaavaa ei tarvita.

2.1 Yleiset lähtökohdat uudistukseen

Jo ennen uudistusta on ollut tarpeellista kiinnittää huomiota tietosuoja-asioihin. Moni ei ehkä tule miettineeksi sitä, mutta tietosuoja-asiathan koskevat lopulta jokaista kansalaista joka puolella maailmaa. Jo oma nimi voidaan lukea henkilötiedoksi ja ennen allekirjoitettua uudistusta tuota henkilötietoa on voitu käsitellä varsin eri tavoilla eri palveluntarjoajilla.

Euroopan Unioniin kuuluu 28 jäsenvaltiota. Jäsenvaltioiden välillä on ollut suuriakin eroja tietosuoja-asioiden saralla. Suomi on lähtökohtaisesti edustanut varsin edistyksellistä tietojenkäsittelyä, sillä meillä on ollut lainsäädäntö, jota ollaan noudatettu. Vasta myöhemmin itsenäisyyden saaneet maat eivät ole voineet saavuttaa samanlaista lainsäädäntöä samassa mittakaavassa kuin Suomessa, joten heillä on ollut selkeitä puutoksia henkilötietojen käsittelyä koskevissa säädöksissä. Euroopan Unionin päätavoitteena on yhdistää Euroopan Unionin jäsenvaltioiden säätelyä, sekä saavuttaa suurella mittakaavalla toimiva yhteisö. Yhteisö on toki niin taloudellinen kuin poliittinenkin liitto, jonka myötä jäsenvaltioiden poliitikot ovat olleet mukana luomassa uudistusta niin asiantuntijoiden kuin rivimiestenkin kanssa.

2.1.1 95/46/EY henkilötietodirektiivi

Tietosuoja-asetuksen uudistuksen taustalla on ollut kaksi tekijää. Säännösten tiukentuessa kansalaisten on helpompi hallita omia tietojaan, kun taas yritykset hyötyvät tasavertaisista toimintaedellytyksistä (Euroopan Komissio,2015). Tämän seurauksena Euroopan Unionin virallinen lehti julkaisi toukokuussa vuonna 2016 Euroopan parlamentin ja neuvoston asetuksen luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä, sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (Eur-Lex,2016). Direktiivi 95/46/EY on vuonna 1995 säädetty asetus, jossa on säädetty yksilöiden suojelusta henkilötietojen käsittelyssä. Tämä direktiivi on siis uuden tietosuoja-asetuksen esi-isä. Direktiivi sisältää 34 artiklaa, jotka käsittelevät yksityisyyden suojaa silloisessa ajassa. Vuonna 1995 ei kuitenkaan ollut samanlaisia perusteita esimerkiksi tietoteknisesti, sillä tietotekniikka itsessään ei ollut vielä tuolloin samalla tasolla kuin nyt. Direktiivin nimestäkin voi päätellä, että se on säädetty Euroopan Yhteisön olemassaolon aikana.

Vanhan direktiivin pohjalta muokattiin myös Suomessa Henkilötietolakia vastaamaan direktiivin vaatimuksia. Direktiivin taustalla on ollut tavoite taata perusoikeuksien- ja vapauksien toteutuminen. Direktiivissä on onnistuneesti otettu huomioon myös rajat ylittävä toiminta, sillä ” jotta yksilö ei jäisi vaille tämän direktiivin mukaisesti taattavaa tietosuojaa, kaiken yhteisössä tapahtuvan henkilötietojen käsittelyn on tapahduttava jonkin jäsenvaltion lainsäädännön mukaisesti; näin ollen tietyssä maassa toimivan rekisterinpitäjän vastuulla oleva tietojenkäsittely olisi suoritettava kyseisen valtion lainsäädännön mukaisesti” (95/46/EY kohta 18).

2.1.2 Henkilötietolaki 533/1999

Ennen uutta direktiiviä Suomessa sovellettiin Henkilötietolakia (1999/523), joka on sittemmin kumottu. Henkilötietolain tarkoituksena oli ” toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä, sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista” (Finlex,2019). On varsin selvää, että vuonna 1999 säädetty laki on aikoinaan ollut varsin kehittynyt ja pureutunut kansainvälisessä mittakaavassa hyvin yksityisyyden suojan turvaamisen perustaksi. Teknologian kehittyessä ja henkilötietojen määrän lisääntyessä on kuitenkin ollut tarvetta tarkemmalle, integroidummalle ja kehittyneemmälle lainsäändännölle.

Henkilötietolain ensimmäisen luvun kolmas pykälä pitää sisällään erilaisia määritelmiä. Laissa on avattu esimerkiksi mitä rekisterinpitäjällä ja reisteröidyllä tarkoitetaan. Uuden tietosuoja-asetuksen myötä määritelmiä on täsmennetty ja myöskin uusia määritelmiä on lisätty asetukseen.

Henkilötietolain vierellä toimi aiemmin myös Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta (1994/389). Tämä laki säädettiin aikoinaan tukemaan henkilötietolain asettamia vaatimuksia. Sittemmin laki on kumottu.

2.2 Euroopan Unionin tietosuoja-asetuksen vaatimukset

Uusi tietosuoja-asetus on tuonut tullessaan useita muutoksia henkilötietodirektiiviin verratuna. Uusi asetus antaa selkeitä täsmennyksiä voimassa olevaan sääntelyyn, sekä merkittäviä uudenlaisia sanktioita ja velvotteita, joita yritysten tulee noudattaa. Erilaisia tietosuoja-asetukseen liittyviä käsitteitä on täsmennetty ja niiden määrää lisätty. Uusia käsitteitä ovat esimerkiksi geneettiset tiedot ja biometriset tiedot.

Asetuksessa on tuotu esille myös laajemmin käsittelyperusteita verrattuna direktiiviin. Etenkin yleiset henkilötietojen käsittelyperusteet sekä arkaluonteisten tietojen käsittelyperusteet ovat tarkentuneet ja täsmentyneet.

Rekisterinpitäjien vastuut on eritelty selkeämmin, sekä tuotu esille myös rekisterinpidossa avustavien henkilöiden rooli. Rekisterinpitäjät ovat myös vastuussa organisaation osalta kertomaan erilaisista tietoturvaloukkauksista. Yksi suurimpia muutoksia on mielestäni kuitenkin organisaatioiden osoitusvelvollisuus (ns. prove it). Entisen henkilötietodirektiivin valossa on riittänyt että asetusta sovelletaan (ns. do it). Nykyinen tietosuoja-asetus kuitenkin säätelee, että organisaation on myös pystyttävä osoittamaan, että uusia tietosuojasäännöksiä noudatetaan täydessä muodossaan.

Yksi uusi vaatimus on myös se, että julkisella sektorilla toimivilla organisaatioilla tulee olla tietosuojavastaava. Kaikilla yrityksillä, jotka käsittelevät laajasti henkilötietoja tai arkaluontoisia tietoja, tulee olla tietosuojavastaava. Kuten jo aiemmin totesin, toimeksiantaja ei tarvitse tietosuojavastaavaa. Uudessa direktiivissä on myös säädetty tietosuojaviranomaisen toimivallasta, valtuuksista ja tehtävistä. Toimivaltaa on rajattu esimerkiksi oman jäsenvaltion alueen perusteella. Jotta jokaisen jäsenvaltion toiminnan yhdenmukaisuus voidaan todeta luodaan myös uusi yhdenmukaisuusmekanismi ja yhden luukun mekanismi. Tämä muutos on suuri askel kohti yhdenmukaista sääntelyä koko Euroopan Unionin alueella.

Euroopan Unionin valvontaviranomaisella on valtuudet langettaa erilaisia huomautuksia ja sanktioita organisaatioille, jotka eivät toimi uuden tietosuoja-asetuksen asettamien sääntöjen mukaisesti. Hallinnolliselle sakolle on asetettu 20 miljoonan euron maksimiraja tai 4 prosentin osuus organisaation liikevaihdosta, jos sen osuus on suurempi kuin 20 miljoonaa euroa. Sanktiot ovat siis suuria ja niiden avulla voidaan mahdollistaa rekisteröidyn kannalta yhdenmukaisempi toiminta (Andreasson ym. 2017, 44).

Kansallista liikkumavaraa on kuitenkin haluttu säilyttää, vaikka direktiivistä on siirretty asetukseen. Direktiivi itsessään ei ole yhtä velvoittavaa lainsäädäntöä kuin asetus. Henkilötietodirektiivin aikana jäsenvaltiot ovat voineet implementoida direktiivin hyvinkin erilaisissa muodoissa. Asetus taas velvoittaa sellaisenaan ja estää jäsenmaiden väliset eroavaisuudet sääntelyssä. Suomessa kansallisen lainsäädännön ja Euroopan Unionin lainsäädännön toteutumista tutkii oikeusministeriön asettama työryhmä. Työryhmän tehtäviin kuuluu muun muassa lainsäädäntötoimenpiteiden toteuttamisen tarkastaminen sekä jo olemassa olevan lainsäädännön oikeellisuuden tarkastaminen ja asetuksen jättämän kansallisen liikkumavaran antamien mahdollisuuksien tarkastelu. Oikeusministeriöllä on siis suuri vastuu, sillä se vastaa Suomessa asetuksen täytäntöönpanon edellyttämistä lainsäädäntötoimista.

2.3 Käsitteitä ja määritelmiä

Uudessa tietosuoja-asetuksessa on luotu uusia käsitteitä ja määritelmiä, jotka vastaavat nykyaikaa. Muutamia käsitteitä on ollut jo henkilötietodirektiivin aikana, mutta uutta asetusta varten niitä on päivitetty. Jotta tietosuoja-asetusta voi ymmärtää, tulee tietää siinä käytettävien käsitteiden määritelmät.

Ensimmäinen tärkeä käsite on henkilötieto. Kuten jo aikaisemmin mainittu, henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Luonnollisella henkilöllä tarkoitetaan ihmistä tai yksittäistä henkilöä, kun taas oikeushenkilö tarkoittaa kokonaista yritystä. Henkilötieto voidaan tunnistaa henkilöön joko suoraan tai epäsuorasti. Henkilötietoja on siis esimerkiksi henkilön nimi, ikä tai puhelinnumero. Henkilö voidaan tunnistaa hänen tunnusomaisen fysiologisen, geneettisen, fyysisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella (Hanninen ym. 2017,20.) Iltapäiväkerhon kannalta henkilötietoja kerätään niin lapsilta kuin vanhemmilta. Ei saa myöskään unohtaa miten tärkeä rooli rekisteröidyn suostumuksella on. Suostumuksen tulee olla vapaaehtoinen, tietoinen, yksilöity ja yksiselitteinen tahdonilmaisu, jolla rekisteröity suostuu henkilötietojensa käsittelyyn. Suostumusta voidaankin siis pitää yhtenä tärkeimmistä määritelmistä uuden tietosuoja-asetuksen kannalta, sillä ilman suostumusta ei ole mahdollisuutta käsitellä tietoja.

Profiloinnilla viitataan henkilötietojen automaattiseen käsittelyyn. Profiloinnin avulla henkilötiedoista voidaan luoda tietylle henkilölle profiloituja ominaisuuksia, esimerkiksi

hänen sijaintipalvelujen tai ostotottumusten mukaisesti. Profilointi on yksi suurimpia yrityksen käyttämiä keinoja tunnistaa asiakkaansa ja tarjota heille sisältöä henkilötietojen perusteella. Rekisteröidyllä tarkoitetaan sitä henkilöä, joiden henkilötietoja missäkin tilanteessa käytetään. Yrityksillä on siis rekistereissä useita rekisteröityjä joiden dataa (henkilötietoja) he käsittelevät profiloinnin avulla. Ajateltaessa toimeksiantajan yhdistyksen tarpeita, voidaan todeta, että profiloinnin tarve ei ole niin laaja. Lapsen iän mukaisesti hänet laitetaan tietyn iltapäiväkerhon mukaan, mutta muutoin tiedoilla ei luoda muuta markkinointiarvoa.

Tietojen anonymisointia on käytetty jo henkilötietodirektiivin aikana. Tällä tarkoitetaan käytännössä sitä, että henkilötieto ei ole enää tunnistettavissa tiettyyn henkilöön. Anonyymit tiedot eivät kuulu tietosuoja-asetuksen alaisuuteen, joten niiden merkitystä en avaa sen enempää. Puolestaan mielenkiintoisempi käsite on pseudonymisoiminen. Määritelmä on lähes samankaltainen kuin anonymisoinnissa, mutta pseudonymisoinnilla henkilötietoja ei voida yhdistää tiettyyn henkilöön ilman lisätietoja (tietosuoja.fi 2017.) Lisätiedot tulee kuitenkin säilyttää erikseen muista henkilötiedoista, jotta niiden mahdollinen käyttö on vaikeampaa. Hyvä esimerkki tietojen pseudonymisoimisesta on henkilötietojen mahdollinen koodaaminen. Koodi voidaan tarpeen vaatiessa purkaa niin, että kaikki sisältö on tunnistettavissa. Koodi voidaan myös rakentaa siten, ettei henkilö ole tunnistettavissa siltä osin.

Rekisteröidyltä kerätään siis henkilötietoja rekisteriin. Mikä rekisteri siis on? Käytännössä koko nykyaikainen tietosuoja-asetuksen mukainen lainsäädäntö perustuu rekisterien varaan. Rekisterillä tarkoitetaan ”mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein,oli tietojoukko sitten keskitetty,hajautettu tai toiminnallisin tai maantieteellisin perustein, oli jaettu” (Hanninen ym. 2017, 22.) Uuden tietosuoja-asetuksen seurauksena rekisterinpitäjä on saanut paljon velvoitteita toimintaansa.

Mitä tarkoitetaan henkilötietojen käsittelijällä ja vastaanottajalla? Molemmissa tapauksissa tietojen käsittelijä voi olla luonnollinen henkilö, oikeushenkilö, viranomaistaho tai jokin muu elin, joka syystä tai toisesta tietoja käsittelee. Henkilötietojen käsittelijä voi käsitellä tietoja ainoastaan rekisterinpitäjän antamien reunaehtojen mukaisesti. Vastaanottaja on tässä tapauksessa siis ulkopuolinen henkilö, jolle rekisterinpitäjä on luovuttanut henkilötietoja käsiteltäväksi. Toimeksiantajan osalta yhdistys toimii sekä henkilötietojen käsittelijänä että vastaanottajana.

Uutena määritelmänä esitellään myös tietoturvaloukkaus. Käsite tarkoittaa ”henkilötietojen tietoturvaloukkausta, jonka seurauksena on siirrettyjen,tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin” (Hanninen ym. 2017, 23). Hyvänä esimerkkinä tietoturvaloukkausesta mainittakoon verottajan viimeaikainen kömmähdys jonka yhteydessä verokirjeitä oltiin lähetetty 27 000 kappaletta väärien kotitalouksien hallintaan (Yle, 2019).

2.4 Rekisteröidyn oikeudet

On varsin selvää, että rekisteröidyillä henkilöillä on myös paljon oikeuksia. Heistä kerätään paljon tietoa ja heillä on myös oikeuksia koskien tietojenkeruuta- ja säilytystä varten. Yksi näistä oikeuksista on esimerkiksi rekisteröidyn oikeus tulla unohdetuksi. Tämä oikeus on noussut vahvasti esiin 2020-luvulla elettäessä, sillä yksilön oikeus tulla unohdetuksi pitää myös pystyä käytännössä toteuttamaan. Suuret maailmanlaajuiset yritykset kuten Google ovat jo käytännössä onnistuneet ”unohtamaan” henkilöiden tietoja ja jokaisella yksilöllä onkin oikeus pyytää tietojensa unohtamista. Yksilöllä tulee olla myös oikeus päästä näkemään käsiteltäviä tietoja.

”Tietosuoja-asetuksen mukaisesti rekisteröidyn oikeuksia ovat

i) oikeus saada läpinäkyvää informointia henkilötietojen käsittelystä,
ii) oikeus saada pääsy tietoihin,
iii) oikeus tietojen oikaisemiseen,
iv) oikeus tietojen poistamiseen eli oikeus tulla unohdetuksi,
v) oikeus käsittelyn rajoittamiseen,
vi) oikeus pyytää tieto sellaisista henkilötietojen vastaanottajista, joille rekisterinpitäjän on ilmoitettava henkilötietojen oikaisuista, poistoista ja käsittelyn rajoituksista,
vii) oikeus siirtää tiedot järjestelmästä toiseen,
viii) vastustamisoikeus sekä
ix) automatisoituihin päätöksiin ja profilointiin liittyvät oikeudet.”

(Hanninen ym. 2017,56).

Oikeuksia on siis paljon ja ne koskevat jokaista henkilötietojen käsittelyn vaihetta. On siis yrityksen velvollisuus täyttää nämä rekisteröidyn oikeudet myös käytännössä. Elina Lepomäki on käynyt blogissaan (Koivumäki, 2017) läpi edellä mainittuja rekisteröidyn

oikeuksia. Artiklassa 82 on kerrottu rekisteröidyn oikeudesta saada korvaus aiheutuneista vahingoista. Tämä korvausvelvollisuus koskee niin aineellista, kuin aineetonta vahinkoa. Artiklassa 77 kerrotaan rekisteröidyn oikeudesta tehdä valitus valvontaviranomaiselle. Tämä oikeus on tärkeä, sillä se takaa yksilön oikeuden tarkastaa käsiteltävät asiansa, sekä valittaa niiden virheellisestä käsittelystä.

2.4.1 Läpinäkyvyys ja sitä koskevat yksityiskohtaiset säännöt

Koko tietosuoja-asetuksen kenties keskeisin runko rakentuu läpinäkyvyyden ympärille. Uudella asetuksella on haluttu taata henkilöille oikeus siihen, että heidän tietojaan käsitellään niin, että toiminta on läpinäkyvää eikä pidä sisällään salassapitoa. Informoinnin tulee olla avointa ja sen avoimuutta on myös lisätty uuden asetuksen avulla. Jokaisen rekisteröidyn tulisi, tietää miten heidän henkilötietojaan käsitellään ja miten laajasti niitä käsitellään niin nyt kuin mahdollisesti tulevaisuudessakin.

> *”Tietosuoja-asetuksen määräämiä tietoja on toimitettava*
>
> *i)* *tiiviisti esitetysti*
> *ii)* *läpinäkyvästi*
> *iii)* *helposti ymmärrettävässä muodossa*
> *iv)* *helposti saatavilla olevassa muodossa ja*
> v) *selkeällä ja yksinkertaisella kielellä”* (Hanninen ym. 2017,73).

Suureen rooliin nousee myös oikeus helposti ymmärrettävässä muodossa olevaan tietojen toimittamiseen. Jokaisen tavallisen kansalaisen tulee siis ymmärtää helposti se, mitä heistä tiedetään ja miten heidän tietojaan oikeasti käsitellään. Tämä on selkeä muutos nykyaikana, kuten myös vaatimus toimittaa tietoja helposti saatavilla olevassa muodossa. Jos käsitellään vanhempien ihmisten henkilötietoja voidaan kysyä onko heille helposti luettavin muoto sähköposti vai kotiin tuleva kirje? Entäpä yritykset, joiden valta-osa asiakkaista puhuu kansainvälisiä kieliä eivätkä he ymmärrä suomea? Ei ole tarkoituksenmukaista, eikä myöskään läpinäkyvää toimittaa heille tietoja koskevaa informointia suomeksi. Useat yritykset paiskivat töitä tämän tyyppisten kysymysten takia, sillä jokaiselle rekisteröidylle pitää pystyä takaamaan samanlaiset oikeudet.

2.4.2 Informointi ja pääsy henkilötietoihin

Uuden tietosuoja-asetuksen myötä reskiteröityjä tulee myös informoida siitä, miten heidän henkilötietojaan käsitellään. Asetus ei kuitenkaan rajaa selkeästi niitä tapoja, joilla informointi tulee toteuttaa. Ajatuksena on, että informaation tulisi välittyä rekisteröidyille mahdollisimman ymmärrettävällä ja selkeäkielisellä tavalla. Informointi voitaisiin siis käytännössä toteuttaa niin kirjoitetun tekstin, kuin esimerkiksi videonkin muodossa. Informaatio tulee kuitenkin kokoajan olla rekisteröidyn saatavilla ja siten helposti löydettävissä. Jos informaatiota lähestyy toimeksiantajan puolesta uskoisin, että kirjoitettu tietosuojaseloste on kätevin, selkein ja kaikin puolin ymmärrettävin tapa luoda informaatio rekisteröidyille. Kyseessä on kuitenkin ruotsinkielinen yhdistys, joten on helpointa toteuttaa seloste niin suomeksi kuin ruotsiksi kirjoitettuna.

Yritykset voivat laajentaa jo olemassaoleviaan rekisteriselosteita ja täten luoda informointitavan, joka mukailee tietosuoja-asetuksen vaatimuksia. Toimeksiantajan pyynnöstä toteutan selosteen käyttämällä apuna Turun ammattikorkeakoulun taloushallinnon opiskelijoiden osuuskunnan luomaa selostepohjaa. Kun tietosuoja-seloste on tehty voidaan se lähettää esimerkiksi sähköpostilla kaikkien yhdistyksen jäsenten tileille, jotta he voivat tutustua siihen. Pääsyä henkilötietoihin rajataan siten, että yhdistyksen hallituksen jäsenillä on pääsy niihin henkilötietoihin, joihin on tarkoituksenmukaista saada pääsy. Lähtökohtaisesti rekisteröidyiltä (niin lapset kuin heidän vanhempansakin) ei kerätä tietoja, joita ei katsota tarpeellisiksi yhdityksen toiminnan kannalta.Tarpeellisuus toimii lähtökohtana niin tietojenkeruussa kuin käsittelyssä. Kaikki informaatio, jota ei tarvita tullaan hävittäämään niille erikseen tarkoitettuihin pisteihin, jolloin voidaan estää tietojen vuotaminen ja väärinkäyttö.

2.4.3 Tietojen oikaiseminen ja poistaminen

Uusi tietosuoja-asetus on tuonut mukanaan myös erilaisia mahdollisuuksia henkilötietojen oikaisuun ja poistamiseen. Rekisteröidyllä on oikeus vaatia häntä koskevien epätarkkojen tai virheellisten tietojen oikaisua. Hänellä on myös oikeus saada erilaiset puutteelliset tiedot täydennettyä, jos hän toimittaa puuttuvia lisäselvityksiä. Rekisteröity ei voi kuitenkaan pyytää tietojen oikaisua siltä osin, jos kyseistä henkilötietoa ei edes ole. Hyvänä esimerkkinä tilanne, jossa rekisteröity opiskelee ammattikorkeakoulussa, mutta ilmoittaa jonkin rekisterinpitäjän tietoihin olevansa jo valmistunut kyseisestä oppilaitoksesta. Yritysten on siis kyettävä pitämään

järjestelmiään ajantasalla siten, että niitä voidaan muokata koska tahansa ja miltä osin tahansa. Järjestelmän täytyy olla siis melko joustava, sillä henkilötiedot voivat muuttua useinkin. Tällöin tietoja pitää pystyä oikaisemaan. Lähtökohtaisesti yritysten tulisi kuitenkin pyrkiä toiminnassaan siihen, että henkilötiedot ovat hyvin täsmentäviä jo alusta alkaen, jotta oikaisupyyntöjä ei tulisi liian paljon (Hanninen ym. 2017, 61).

Mielestäni hyvä ja tarpeellinen uudistus on myös rekisteröidyn oikeus pyytää tietojen poistamista eli niin kutsuttu oikeus tulla unohdetuksi. Rekisteröidyllä on oikeus tulla unohdetuksi kuuden perusteen saralla. Ensinnäkin oikeus tulla unohdetuksi pätee silloin, kun henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne on alunperin kerätty. Toiseksi, rekisteröity voi peruuttaa suostumuksensa henkilötietojen käsittelyyn, jolloin hänellä on oikeus tietojen poistamiseen. Kolmanneksi, rekisteröity voi myös erikseen vastustaa henkilötietojensa käsitelyä seuraavassa kappaleessa mainitun vastustamisoikeuden nojalla. Neljäs kohta pitää sisällään oikeuden tietojen poistamiseen, jos tietoja on käsitelty lainvastaisesti. Viides kohta kertoo henkilötietojen poistamisesta, jos se perustuu yrityksen noudattaman lainsäädännön velvoitteeseen. Kuudes kohta on toimeksiantajan osalta tärkein kohta. Rekisteröidyllä on oikeus tietojen poistamiseen, jos tiedot on kerätty tarjottaessa tietoyhteiskunnan palveluja suoraan lapselle. Tietoyhteiskunnan palveluja ovat esimerkiksi sähköisessä muodossa olevat palvelut, joista maksetaan korvaus. Tämä oikeus takaa sen, että lapsen internettiin vahingossa luodut tiedot voidaan poistaa myöhemmin ja näin taata parempi tietosuoja.

Tietosuoja-asetus ei määrittele erikseen, miten tiedot tulee pyydettäessä poistaa. Tietosuoja-asetus toistaa samaa kaavaa, eli kertoo tarkat periaatteet henkilötietojen käsittelyn tueksi, mutta jättää yrityksille liikkumavaraa periaatteiden käytännön toteuttamiseen. Tämän seurauksena monikin yritys voi pyydettäessä poistaa tietoja erilaisin tavoin. Eräs seikka, jota pidän hieman omituisena nykypäivälle on se, että asetus ei ota kantaa varmuuskopioihin. Usein tietoja on monilla eri servereillä ja niitä varmuuskopioidaan. Jos rekisteröity siis pyytää tietojensa poistamista, on asetuksen mukaan tarpeellista poistaa tieto lähtökohtaisesti siltä alustalta, jossa sitä säilytetään. Jos rekisteröity ei erikseen vaadi varmuuskopion poistamista, ei yritys ole velvollinen sitä tekemään eli käytännössä tieto on silti olemassa ja yritys voi sitä edelleen säilyttää (Hanninen ym. 2017, 63).

2.4.4 Oikeus vastustaa henkilötietojen käsittelyä ja henkilötietojen käsittely yleisesti

Vastustamisoikeudella tarkoitaan oikeutta erityiseen tilanteeseen liittyvällä perusteella milloin tahansa vastustaa omien tietojen käsittelyä. Vastustamisoikeudella voidaan myös löytää peruste oikeutettujen etujen toteuttamiseen. Yritys voi kuitenkin estää vastustamisoikeudella vaaditun tiedon poistamisen, jos se on tarpeellista esimerkiksi oikeusvaateen puolustamiseksi. Yritys voi siis jatkaa tietojen käsittelyä, jos se löytää sen perusteeksi huomattavan tärkeän ja perustellun syyn, joka periaatteessa syrjäyttää yksilöden oikeudet ja vastustamisen. Erityisesti suoramarkkinoinnissa on kuitenkin pitäydytty siinä, että yksilön vastustamisoikeutta pidetään hyvinkin vahvana ja hänellä on aina oikeus vastustaa tietojen käsittelyä suoramarkkinoinnin parissa. Toimeksiantajan osalta tietoja käsitellään käytännössä toiminnan jatkuvuuden takaamiseksi. On tärkeää tietää, kuinka monta rekisteröityä on, heidän ikänsä ja esimerkiksi iltapäivätoiminnan kannalta riittävän henkilökuntamäärän takaaminen.

Tietosuoja-asetus pitää sisällään äärimmäisen paljon erilaisia periaatteita ja määritelmiä henkilötietojen käsittelyn tueksi. Lähökohtaisesti voidaan todeta, että asetus on suunniteltu turvaamaan yksilön oikeuksia ja siten rajaamaan yritysten pääsyä ja käsittelyoikeuksia yksilöiden tietoihin. Uskallan kuitenkin väittää, että useat rekisteröidyt eivät tiedä oikeuksiaan, eivätkä siten myöskään osaa vaatia niiden noudattamista rekisterinpitäjiltä, joten on eri asia miten hyvin nämä oikeudet käytännön elämässä toteutuvat.

Seuraavassa kappaleessa käsitellään tietosuoja-asetuksen käsittelyperusteita, jonka jälkeen pureudutaan tietosuojaperiaatteisiin.

3 TIETOSUOJA-ASETUKSEN KÄSITTELYPERUSTEET

Henkilötietojen käsittely on lainmukaista ainoastaan, jos vähintään yksi seuraavista ehdoista täyttyy. Artikla 6 pitää sisällään kaikki EU:n yleisen tietosuoja-asetuksen lainmukaisuuden perusteet.

3.1 Suostumus ja sopimus

”Käsittely on lainmukaista, kun rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten.” (Art 6 kohta 1a)

Tämä peruste pitää siis sisällään henkilötietoja käsittelevän tahon omaavan suostumuksen henkilöltä, jonka tietoja käsitellään. Antaessaan suostumuksen tietojensa käsittelyyn antaa henkilö samalla suostumuksensa niiden tietojen säilyttämiseen niin yhtä, kuin useampaa tarkoitusta varten. Tälläisiä tilanteita voisi olla esimerkiksi lääkärin vastaanotolle mentäessä, kun täyttää lomakkeen omien tietojen käsittelyyn suostumisesta. Tietoja voidaan käsitellä joko kyseisellä lääkäriasemalla tai jos suostumuksellaan on antanut luvan, myös muilla asemilla. Suostumuksen on oltava yksilöity, tietoinen, vapaaehtoinen ja selkeä tahdonilmaisu.

Tietosuojavaltuutettu Reijo Aarnio kertoo blogissaan, että suostumuksen tulisi olla viimeinen peruste, ellei tietosuoja-asetuksesta löydy muuta perustetta (Koivumäki, 2017). Tästä voidaan vetää johtopäätös siihen, että suostumus on aina peruutettavissa. Periaatteessa suostumus on siis lainmukainen peruste henkilötietojen käsittelyyn, mutta käytännössä heikko peruste, sillä henkilö voi koska vain vetää tämän suostumuksensa pois.

”Käsittely on lainmukaista, kun käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.” (Art 6 kohta 1b)

Tätä perustetta voidaan pitää kohtalaisen suosittuna ja yleisenä perusteena henkilötietojen keruuseen. Tälläinen peruste on nähtävissä usein etenkin pankkien tai lääkäriasemien kanssa. Sopimus velvoittaa molempia osapuolia ja siten myös palvelee molempien osapuolien tarpeita. On tärkeää myös huomauttaa Elina Koivumäen tavoin ”

ettei sopimuksen syntyminen edellytä rahan liikkumista rekisterinpitäjän ja rekisteröidyn välillä” (Koivumäki, 2017).

Populäärikulttuurissa hyvä esimerkki on Facebook. Kun luot itsellesi Facebook tilin, hyväksyt tai kieltäydyt hyväksymästä yrityksen tietosuojaehtoja. Jos hyväksyt ehdot, ikäänkuin samalla luot sopimuksen yrityksen kanssa siten, että saat käyttää Facebookkia omalla tililläsi ja samanaikaisesti yritys saa sinulta käyttöönsä henkilötietoja.

3.2 Lakisääteiset velvoitteet ja elintärkeä etu

”Käsittely on lainmukaista, kun käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi.” (Art 6 kohta 1c)

Lakisääteinen velvoite on suhteellisen aukoton periaate henkilötietojen keruuseen ja käsittelyyn. Laki vaatii (esimerkiksi osakeyhtiölaki) sen nojalla pitämään rekisteriä (osakasluettelo). Tässä yhteydessä mainittakoon, että yhdistyksen osalta jäsenyys voi mahdollistaa myös oikeutetun edun käytön jäsenluettelon ulkopuolella (Hanninen ym. 2017, 31).

”Käsittely on lainmukaista, kun käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi.” (Art 6 kohta 1d)

Kuten edellä mainitaan, henkilötietojen käsittelyyn voidaan nojata elintärkeään etuun nojaten. Tälläinen tilanne voisi olla jokin suuri humanitäärinen hätätilanne tai luonnonkatastrofi, jossa henkilötietoja käsitellään nopealla aikataululla ja suuren datan siivittämänä.

3.3 Yleinen etu tai julkisen vallan käyttö sekä oikeutettu etu

”Käsittely on lainmukaista, kun käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.” (Art 6 kohta 1e)

Tämän perusteen alle kuulunee paljon erilaisia tapauksia niin sosiaalialan kuin luottotietotoiminnan alta. Tämän perusteen alaisuuteen kuuluu myös yksilön oikeus tulla unohdetuksi. Tällöin yksilön oikeuksiin kuuluu, että rekisterinpitäjän tulee poistaa kaikki häneen liittyvät tiedot välittömästi ja viipymättä (Art 17 kohta 1). Olen käsitellyt yksilön oikeutta tulla unohdetuksi tarkemmin luvussa 2. Artiklassa 18 käsitellään myös oikeutta käsittelyn rajoittamiseen eli oikeutta vastustaa henkilötietojen käsittelyä.

”Käsittely on lainmukaista, kun käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.” (Art 6 kohta 1f)

Yrityksillä ja yhdistyksillä voidaan nähdä olevan erilaisiakin oikeuttavia etuja, mutta yleisesti tämä periaate on nähty melkoisen tulkinnanvaraisena. Suoramarkkinointi ja asiakaspalvelu ovat esimerkkejä tilanteista, joissa yrityksellä on oikeutettu etu kerätä henkilötietoja. Oikeutetun edun perusteena voidaan tällöin pitää henkilön ja rekisterinpitäjän välistä merkityksellistä ja asianmukaista suhdetta.

4 TIETOSUOJAPERIAATTEET

EU:n yleisen tietosuoja-asetuksen toinen luku sisältää asetusta rajoittavat periaatteet. Toisen luvun viides artikla pitää sisällään periaatteet. Toisen luvun kahdeksas artikla pitää sisällään lapsiin kohdistuvien henkilötietojen periaatteita. Kaiken kaikkiaan periaatteet on säädetty suojelemaan niin luonnollisen henkilön tietosuojaan kohdistuvaa sääntelyä kuin selkeyttämään uuden tietosuoja-asetuksen ulkoisia raameja. Keskeisesti periaatteet antavat tarkat ehdot, joilloin henkilötietoja voidaan käsitellä ja miten tietoja tulee minimoida. Henkilötietoja tulee kerätä ainoastaan tiettyä tarkoitusta varten, eikä niitä saisi myöhemmin käyttää sopimattomalla tavalla. Tietojen tulee olla myös eheitä ja luottamuksellisia. Tietoja ei myöskään tulisi säilyttää ikuisesti, vaan niiden säilyttämiselle tulee olla rajoitetut ehdot. Rekisterinpitäjä on myös velvollinen osoittamaan käsittelemänsä tiedot ja niiden säilytyksen. Kenties kuitenkin tärkein periaate käsittelee henkilötietojen käsittelyn lainmukaisuutta, kohtuullisuutta ja läpinäkyvyyttä.

4.1 Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Henkilötietoja tulee ja pitää käsitellä lainmukaisesti, kohtuullisesti ja läpinäkyvästi. Tästä voidaan ensimmäisenä mainita, että henkilötietojen käsittelyllä tulee olla jokin laillinen peruste (Hanninen ym. 2017, 48). Lainmukaisia perusteita ovat esimerkiksi suostumus ja sopimus, joista olen jo aiemmassa luvussa kirjoittanut. Toiseksi henkilötietoja tulee käsitellä niiden suhteessa ainoastaan kohtuullisen määrän vaatimalla tavalla. Hyvä esimerkki voisi olla yritys, joka käsitellee henkilötietoja mainostaakseen omaa tuotettaan. Henkilötietojen kannalta on kohtuullista tietää henkilön sukupuoli, jotta mainonta voidaan kohdentaa. On kuitenkin kohtuutonta tietää henkilön uskonnollinen taso, sillä se ei vaikuta tuotteen mainonnan kohdentamiseen. Kolmanneksi henkilötietojen käsittelyn tulee olla läpinäkyvää ja rekisteröidyn tulee tietää, kuka rekisterinpitäjä on ja miksi hänen henkilötietojaan käsitellään. Yksi suurimmista muutoksista tämän asetuksen nojalla perustuu juurinkin läpinäkyvyyn periaatteeseen. Rekisterinpitäjän tulee käyttää selkeää ja helposti ymmärrettävää kieltä selosteessaan, jotta rekisteröidyllä on mahdollisuus ymmärtää tietojensa käsittelyn tarkoitus.

4.2 Käyttötarkoitussidonnaisuus

Henkilötietoja tulee kerätä tiettyä, nimenomaista ja laillista tarkoitusta varten. (Art 5 kohta 1b) Henkilötietoja tulee käsitellä jonkun tarkoituksen suorittamiseksi siten, että tiedot on sidottu kyseiseen käyttötarkoitukseen. Hyvä esimerkki on työnhakijan henkilötietojen käsittely työnhaun yhteydessä. On työnantajan käyttötarkoituksen kannalta perusteltua saada tutustua rekisteröidyn henkilötietoihin ennen hänen palkkaamistaan. Jos työnantaja päättää palkata kyseisen henkilön, ei ole enään tarpeellista säilyttää henkilötietoja, eikä myöskään sidottu käyttötarkoitukseen käyttää niitä muussa asiayhteydessä. Tästä voidaan johtaa myös se, että jos henkilötietojen käsittely ei ole pakollista, niitä ei tulisi käsitellä. Rekisterinpitäjän tulee myös kiinnittää huomiota, että käyttötarkoitussidonnaisuus toteutuu käytännössä ja tietoja käytetään vain niihin tarkoituksiin, joihin ne on ennalta määrätty. Toimeksiantajan kannalta tulisi kerätä ainoastaan niitä tietoja, joita tarvitaan, jotta voidaan taata yhdistyksen toiminnan jatkuminen.

4.3 Tietojen minimointi ja täsmällisyys

Tietosuoja-asetuksen artiklan 5 mukaisesti ” henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. (Art 5 kohta 1c) Edellä on jo mainittu, että tietojen keräämiseen tulee olla lainmukaisia perusteita ja ne tulee olla sidoksissa käsiteltävään asiaan olennaisesti. Tietojen minimointi asettaa omanlaisen haasteensa henkilötietojen käsittelyyn. Yleisesti ottaen henkilöistä kerätään tietoa hyvinkin paljon nyky-yhteiskunnassa. Tämän seurauksena dataa on käytettävissä entistä enemmän kuin ennen. Tietojen minimointi kuitenkin rajoittaa henkikötietojen käsittelyn siihen, mikä on välttämätöntä tietojen käsittelyn tarkoituksen kannalta. Vaikka henkilö olisi suostumuksellaan antanut luvan henkilötietojen käsittelyyn voidaan kuitenkin todetta että, ei ole tarkoituksenmukaista käsitellä tietoja ikuisesti ja tarpeettomasti. Yritysten ja myös yhdistysten tulee päättää jo tietojen keruuvaiheessa ne tiedot, joita tarvitaan ja kyseiset tiedot tulee spesifioida. Tämän periaatteen nojalla ei ole siis sallittua kerätä tietoa sillä periaatteella, että niitä voisi joskus tulevaisuudessa tarvita. Tietojen minimointi takaa sen, että kerätyillä henkilötiedoilla on jokin tarpeellinen päämäärä juuri siinä hetkessä.

Henkilötietojen tulee myös olla täsmällisiä. (Art 5 kohta 1d) Koko tietosuoja-asetus on asetettu ensisijaisesti suojaamaan luonnollisten henkilöiden tietosuojaturvaa. Toisekseen asetus takaa paremmat välineet ja periaatteet yritykselle niiden käsitellessä henkilötietoja. Tietojen täsmällisyyden periaate asettaa yritykselle vastuun huolehtia siitä, että rekisterinpitäjän käsittelemät tiedot ovat täsmällisiä. Jos rekisterinpitäjällä on hallussaan vääriä tietoja, tulee ne poistaa välittömästi tai oikaista. Rekisterinpitäjä kantaa loppukädessä vastuun siitä, että rekisterin tiedot ovat ajankohtaisia. Tämä vaatii rekisterinpitäjältä toimia tarkastaa tietojaan aika ajoin. Tarvittaessa rekisterinpitäjä oikaisee tietojaan ja varmistaa, että henkilötiedot ovat oikein ja ajantasaisia.

4.4 Tietojen säilytyksen rajoittaminen

Tällä periaatteella halutaan rajoittaa rekisterinpitäjän oikeutta säilyttää rekisteröidyn henkilötietoja. Kuten jo aiemmin todettu, tiedot tulee säilyttää siinä muodossa että rekisteröity on tunnistettavissa rajoitetun ajan. Yleinen etu on tarkoituksena ainoa, jonka nojalla tietoja voidaan säilyttää pidempään kuin on tarpeellista. Myös tieteellisen tai historiallisen tutkimuksen nojalla tietoja voidaan säilyttää pidempiä aikoja. (Art 5 kohta 1e) Tietoja voidaan säilyttää pidempään myös silloin, kun rekisteröity ei ole tunnistettavissa säilytettävistä tiedoista. Tietoja voidaan siis säilyttää esimerkiksi tilanteissa, joissa seurataan tietyn tuotteen menekkiä ja ostajakuntaa, kunhan tietoja ei voida enää suoraa yhdistää kyseiseen henkilöön. Rekisterinpitäjän vastuulla on tarkastella sopivin väliajoin, onko tietojen säilyttäminen enää tarkoituksenmukaista ja jos näin ei ole, hänen tulee poistaa tiedot viipymättä.

4.5 Tietojen eheys ja luottamuksellisuus

Tähän mennessä on jo todettu useita erilaisia periaatteita, jotka säätelevät henkilötietojen käsittelyä. Henkilötietoja on käsiteltävä niin, että turvallisuus ja luottamuksellisuus korostuvat ja ovat ensisijaisen tärkeitä. Rekisterinpitäjällä on täten suuri vastuu tiedoista, joita he käsittelevät. Tiedot eivät saa joutua kolmansien käsiin eikä niitä saa hävitä muutoinkaan. Rekisterinpitäjä on vastuussa myös tietojen tuhoutumiselta ja vahigoittumiselta, siltä osin kun tietoja käsitellään. Rekisterinpitäjä pitää myös huolen, että kolmannet osapuolet eivät pääse käsiksi tietoihin. Tietojen tulee siten pysyä eheinä ja luottamuksellisina sillä rekisterinpitäjällä, jolla on lainmukainen oikeus käsitellä rekisteröidyn henkilötietoja.

4.6 Rekisterinpitäjän osoitusvelvollisuus

Viimeisenä, muttei vähäisempänä tulee seitsemäs henkilötietojen käsittelyä rajaava periaate, joka on rekisterinpitäjän osoitusvelvollisuus. Rekisterinpitäjän tulee noudattaa kaikkia yllämainittuja tietosuojaperiaatteita, mutta tämän lisäksi hän on myös velvollinen osoittamaan, että näin on toimittu. Suurin ero aikaisempaan henkilötietolakiin on kenties juuri tässä periaatteessa, sillä aiemmin osoitusvelvollisutta ei ollut. Olen avannut tätä enemmän ensimmäisessä luvussa. Tietosuojaperiaatteet on kirjoitettu aukottomiksi tietosuoja-asetukseen, mutta rekisterinpitäjän käsiin jää niiden käytännöntoteuttaminen. Rekisterinpitäjä eli tässä tapauksessa yhdistys, on velvollinen huolehtimaan, että periaatteita noudatetaan ja niiden toteuttaminen voidaan todeta. Tietosuojaseloste astuu kuvioihin tässä kohden. Rekisterinpitäjä tekee dokumentaation, jota myös tietosuojaselosteeksi kutsutaan, ja osoittaa dokumentaatiolla, mitä henkilötietoja käytetään ja miten niitä käytetään.

Käytännössä osoitusvelvollisuuden voi osoittaa monellakin eri tavalla, mutta helpoiten sen saa luettavaan muotoon luomalla tietosuojaselosteen. Yrityksen tulee myös laatia omat sisäiset tietosuojaperiaatteensa sekä kirjata ylös kaikki sitä koskevat dokumentaatiot ja selosteet niin että niistä on helposti muodostettavissa kokonaiskuva yrityksen tietosuojasta ja henkilötietoihin liittyvästä toiminnasta (Hanninen ym. 2017, 51).

5 CASE CYGNAEUS MORGONKLUBB RF

Suoritan opinnäytetyön toimeksiantona yhdistykselle Cygnaeus Morgonklubb rf. Yhdistys on ruotsinkielinen, jonka seurauksena tietosuojaseloste tulee tehdä myös ruotsinkielisenä. Yhdistys on perustettu 24.marraskuuta vuonna 2010. Yhdistys järjestää niin aamu- kuin iltapäivätoimintaa Cygnaeuksen koulun oppilaille luokka-asteilla 1-4 sekä aamutoimintaa Brahen koulun oppilaille luokka-asteilla 1-2. Aamu- ja iltapäivätoiminnan tarkoituksena on tukea lasten kasvatusta ja samalla vaikuttaa lasten viihtyvyyteen ja kehitykseen. Tällä hetkellä yhdistyksellä on yli sata jäsenperhettä. Cygnaeus koulun aamutoiminnassa on lapsia 106 ja iltapäiväkerhon listoilla on 42 lasta. Brahen koulun osalta aamukerhoon osallistuu 50 lasta. Tietosuoja-asetuksen näkökulmalta tulee siis luoda tietosuojaseloste, jossa käsitellään niin perheen lasten kuin vanhempienkin henkilötietoja. Yhdistyksen osalta tälläisiä henkilötietoja ovat esimerkiksi lasten nimet, vanhempien puhelinnumerot sekä perheiden osoitteet.

Yhdistyksen palkkalistoilla on tällä hetkellä pääsääntöisesti kuusi henkilöä. Näiden henkilöiden lisäksi yhdistyksessä toimii myös sijaisia. Cygnaeus Morgonklubb rf:n hallituksessa on tällä hetkellä viisi jäsentä. Hallitus toimii syksystä 2018 alkaen syksyyn 2019 saakka. Hallituksen puheenjohtaja on Pia Lindman ja varapuheenjohtajana toimii Reima Söderman. Rahastonhoitajana toimii Mikael Östergård ja sihteerinä Jessica Lindström. Hallituksen jäsenenä toimii Gurli-Maria Gardberg. Cygnaeus Morgonklubb rf saa rahoituksensa toimintaansa Sundells säätiöltä, Petrelius säätiöltä, Brita Maria Rehnlundin stipendisäätiöltä sekä Fruntimmersföreningen i Åbo ja Hem och Skola i Åbo yhdistyksiltä.

Yhdistys käsittelee siis myös lapsiin liittyviä henkilötietoja. Unicef on kirjoittanut oppaan, jossa keskitytään erityisesti lasten henkilötietojen käsittelyyn (Unicef,2017.) Irene Leino kirjoittaa että tietosuoja-asetuksessa on selkeästi asetettu ikäraja suostumuksen antamiselle henkilötietojen käsittelyyn. Tuo ikäraja on 13 vuotta. Voidaan päätellä, että suurimmaksi osaksi kaikki yhdistyksen toiminnassa mukana olevat lapset ovat alle 13 vuotiaita joten he eivät voi itse antaa suostumustaan henkilötietojen käsittelyyn. Leino myös kertoo miten huoltajien vastuulla on lähtökohtaisesti varmistaa että lapsen oikeudet toteutuvat perheympäristössä. Tämän vuoksi onkin tarpeellista että toimeksiantaja teettää vanhemmilla lomakkeen, jonka huoltaja allekirjoittaa ja antaa luvan yhdistykselle käsitellä lapsensa henkilötietoja (Liite 5).

Toimeksiantajan osalta yhdistys toimii rekisterinpitäjänä. Yhdistys kerää tiedot suoraan rekisteröidyiltä ja käsittelee tietoja. Yhdistys saa tiedot rekisteröityjen suostumuksella. Tietoja säilytetään ainoastaan siihen saakka, kun niitä on tarkoituksenmukaista käsitellä. Uusi tietosuoja-asetus ei varsinaisesti aseta suuria muutoksia toimeksiantajalla. Ehtoja ja periaatteita tulee noudattaa siinä missä aiemminkin. Uusi asetus kuitenkin vaatii dokumentaation henkilötietojen käsittelystä ja tämä onkin suurin muutos, joka yhdistyksen tulee toteuttaa.

5.1 Seloste ja rekisteri

Selosteella tarkoitetaan tässä tapauksessa kirjallista kuvausta organisaation tekemästä henkilötietojen käsittelystä. Rekisterinpitäjä tai/ja henkilötietojen käsittelijä on velvoitettu tekemään seloste toiminnastaan jos organisaatiossa on yli 250 työntekijää tai jos henkilötietojen käsittely aiheuttaa todennäköisesti riskin rekisteröidyn oikeuksille ja vapuksille. Seloste on velvoitettu tekemään myös, jos henkilötietojen käsittely ei ole satunnaista tai jos henkilötiedot sisältävät erityisiä tietoryhmiä (Tietosuoja, 2017.) Tietosuojaseloste voidaan ymmärtää yrityksen osoitusvelvollisuutena, jolloin sen velvollisuus osoittaa toimintansa täyttyy.

Jotta seloste olisi onnistunut, voidaan noudattaa muutamaa tasoa. Ensimmäiseksi tulisi kartoittaa henkilötietojen käsittelyn kokonaiskuva ja ymmärtää läpinäkyvyyden periaate. Toiseksi olisi hyvä tunnistaa se, mistä henkilötiedot saadaan. Jos henkilötiedot kerätään rekisteröidyltä, sovelletaan silloin artikloita 12 ja 13 tietosuoja-asetuksesta. Jos tiedot saadaan jostain muualta, sovelletaan artikloita 12 ja 14 samaisesta asetuksesta. Toimeksiantaja kerää henkilötiedot suoraan rekisteröidyiltä, joten sen toiminnassa sovelletaan artikloita 12 ja 13. Kolmanneksi olisi tärkeää tunnistaa kohderyhmä, sekä arvioida, mikä olisi heidän osaltaan paras mahdollinen informointimalli. Neljänneksi tulee varmistaa, että kieli on selkää ja ymmärrettävää. Viidenneksi ja mielestäni tärkeimmäksi nousee osoitusvelvollisuuden toteuttaminen. Tämä on osa läpinäkyvyyden periaatetta, jossa rekisterinpitäjän on pystyttävä osoittamaan miten rekisteröidyn tietoja käsitellään. Selosteen tulisi pitää sisällään siis tämä osoitusvelvollisuus. Viimeisenä tulee muistaa päivittää tietoja aina tarvittaessa.

5.2 Tietosuojaselosteen rakentaminen

Tietosuojavaltuutetun toimisto on luonut mallipohjan tietosuojaselosteen tekemiselle.

”*Seloste koostuu 12 eri osasta jotka ovat:*

1. *Rekisterinpitäjä*
2. *Yhteyshenkilö rekisteriä koskevissa asioissa vastaava henkilö*
3. *Rekisterin nimi*
4. *Henkilötietojen käsittelyn tarkoitus*
5. *Rekisterin tietosisältö*
6. *Säännönmukaiset tietolähteet*
7. *Tietojen säännönmukaiset luovutukset*
8. *Tietojen siirto EU:n tai Euroopan talousalueen ulkopuolelle*
9. *Rekisterin suojauksen periaatteet*
10. *Tarkastusoikeus*
11. *Oikes vaatia tiedon korjaamista*
12. *Muut henkilötietojen käsittelyyn liittyvät oikeudet”*

(Andreasson ym. 2015, 158.)

Mallipohjaa voi siis soveltaa tietosuojaselostetta tehdessä. Toimeksiantajani on kuitenkin päättänyt ostaa selosteen mallin Turun ammattikorkeakoulun taloushallinnon opiskelijoiden osuuskunnalta. Tämä mallipohja myötäilee pitkälti tietosuojavaltuutetun pohjaa, mutta siinä on muutamia kohtia, jotka on muutettu. Käyttämässäni mallissa käydään ensin läpi yleisesti se, ketä seloste koskee ja kenen puolesta se on tehty. Selosteessa käydään myös läpi tietosuojaperiaatteet sekä tekniset,fyysiset ja organisatoriset turvatoimet tietojen suojaamiseksi. Seloste pitää myös sisällään rekisteröidyn oikeudet sekä tiedot siitä, miten tietosuojaloukkauksista ilmoitetaan. Yhdistyksen yhteyshenkilönä toimii myös yhdistyksen hallituksen puheenjohtaja Pia Lindman. Lindmanin yhteystiedot esitetään jäsenrekisterissä, josta rekisteröity löytää yhteystiedot. Näiden tietojen pohjalta kirjoitin tietosuojaselosteen sekä asiakasrekisterin jotka ovat liitteenä (Liite 1, Liite 2). Liitteinä löytyvät myös ruotsinkieliset tuotokset (Liite 3, Liite 4).

Rekisterien teossa olen käyttänyt apunani ostettuun selosteen pohjaan tehtyjä seikkoja. Seloste tuo esiin yhdistyksen tämän hetkiset tietosuojaperiaatteet ja kertoo myös miten ja miksi henkilötietoja käsitellään. Tärkeää on myös selosteessa erikseen mainitut

rekisteröidyn oikeudet. Kuten jo aiemmin todettu, uusi tietosuoja-asetus on vahventanut rekisteröidyn oikeuksia ja siten halutaan myös taata niiden toteutuminen. Jäsenrekisterissä käy ilmi helposti yhdistyksen yhteyshenkilön yhteystiedot, sekä tarkemmin se, mitä tietoja jäseniltä on kerätty ja miten niitä käsitellään. Kaiken kaikkiaan pyrin tekemään selosteet hyvin selkokielisiksi ja helposti ymmärrettäviksi. Yksilön kannalta on kuitenkin tarkoituksenmukaista, että häntä koskevia tietoja käsitellään niin lain mukaisesti, kuin selosteessakin esitetyllä tavalla. Informoinnin tulee olla selkeää ja mielestäni olen onnistunut luomaan selkeän tietosuojaselosteen sekä jäsenrekisterin. Olen luonut rekisterit toiminallisen tutkimusmenetelmän toimin. Olen kerännyt tietoja erilaisista lähteistä ja näiden pohjalta luonut tuotoksen.

6 JOHTOPÄÄTÖKSET JA YHTEENVETO

Tämän opinnäytetyön tavoitteena oli selventää Euroopan Unionin tietosuoja-asetuksen tuomia uudistuksia, sekä ottaa selvää miten se käytännössä vaikuttaa niin toimeksiantajaan kuin yksilöön. Tavoitteena oli myös päivittää toimeksiantajan rekisterit vastaamaan uuden tietosuoja-asetuksen vaatimaa tasoa. Lakisanasto on pitkälti vaikeaselkoista ja sen ymmärtäminen kokonaisuudessaan voi olla vaikeaa. Olen kuitenkin mielestäni onnistuneesti avannut tietosuoja-asetuksen keskeisimpiä piirteitä tässä opinnäytetyössä ymmärrettävällä tavalla. Tietosuoja-asetus kokonaisuudessaan koskee kuitenkin kaikkia yrityksiä ja sillä on suoria vaikutuksia myös yksittäisiin henkilöihin. Uudistus on myös hyvin ajankohtainen, joka omalta osaltaan on helpottanut ajankohtaisten lähteiden löytämistä.

Voisin myös todeta, että GDPR ei ole varsinaisesti itsessään muutos. Kyseinen asetus aiheuttaa muutoksia ja tiukentaa henkilötietojen käsittelyn käyttötarkoituksia, mutta ei itsessään ole varsinainen muutos yritykselle. Euroopan Unionin tietosuoja-asetus aiheuttaa ennemminkin niin sanotun dominoefektin, jossa tapahtumat ovat seurausta muista sarjan tapahtumista. Avaan hieman tätä efektiä paremmin. Toimeksiantaja on toiminut aiemmin tietyissä puitteissa. Nyt puitteet ovat muuttuneet, joten toiminnan tulee muuttua sen mukana. Sanoisinkin, että tietosuoja-asetuksen suurin muutos ei ole varsinaisesti se, että asetus on alun alkaenkaan asetettu vaan se, että se aiheuttaa suoria muutoksia yritysten ja muiden oikeushenkilöiden toiminnoissa.

Opinnäytetyön alkuvaiheessa oli jo selvää, että opinnäytetyö toteutetaan toiminnallisen tutkimusmenetelmän avulla. Tutkimusmenetelmässä tietoa kerätään erilaisten lähteiden kautta. Toimeksiantajalle tuli luoda rekisterit, jotka noudattavat laindsäädäntöä ja takaavat toiminnan jatkumisen niin sanotussa uudessa maailmassa. Tutkin lähtökohtaisesti varsin ajantasaisia lähteitä ja loin sitä kautta pohjan opinnäytetyön teoriaosuudelle. Teoriaosuuden jälkeen tutkin, miten muutokset vaikuttavat toimeksiantajaan. Johtopäätöksenä voidaan todeta, että yhdistyksen osalta muutoksia ei juurikaan ole. Uutta tietosuoja-asetusta tulee noudattaa toki sellaisenaan, mutta Suomessa pohjalla toiminut Henkilötietolaki on mahdollistanut jo varsin tehokkaan sääntelyn. Yhdistyksen tulee noudattaa erilaisia periaatteita ja myös osoittaa se. Suurin muutos oli kuitenkin rekisterien luominen. Toimeksiantajalla ei ollut pohjalla toimivia rekistereitä, joten ne luotiin alusta alkaen vastaamaan uuden asetuksen vaatimuksia.

Nykyaikaisessa maailmassa ihmisistä kerätään entistä enemmän tietoa ja Big Dataa voidaan käyttää moniin eri tarkoituksiin. On siis selvää, että tarve uudelle asetuksella on ollut ja on hienoa nähdä, miten 28 jäsenmaata ovat yhdessä ottaneet käyttöön uuden tietosuoja-asetuksen. Rajat ylittävää toimintaa löytyy jokaiselta alalta, joten on erittäin tärkeää että jokaisella rekisteröidyllä on samat oikeudet ja velvollisuudet maasta riippuen. Toimeksiantajan yhdistys on kooltaan tosin pieni, eikä henkilötietoja ole suhteessa paljon. On kuitenkin tärkeää huomata, että myös pieni yhdistys noudattaa samoja sääntöjä kuin suuret yritykset. Olen huomannut teoriaa tutkiessani, että useatkaan yritykset eivät ole olleet aikaisemminkaan täysin tietoisia kaikista periaatteista, joita toiminnassa tulee noudattaa.

Tämän opinnäytetyön yhtenä johtopäätöksenä voidaan myös todeta, että yritysten tulee olla kokoajan ajantasalla omista toiminnoistaan, sekä valmiita muuttumaan muutoksen mukana. Nykyaikana muutokset tapahtuvat nopeasti, eikä niiden toteuttamiselle anneta joustovaraa, joten yritysten tulee toden teolla olla aina askeleen edempänä. Uusi tietosuoja-asetus ei välttämättä näy suoranaisesti yksilön jokapäiväisessä elämässä, mutta yrityksen kannalta on tärkeää tietää, mikä on muutoksen jälkeen sallittua ja mikä ei.

Tämä opinnäytetyö on tiivis kokoelma niistä muutoksista, joita uudistus tuo tullessaan eikä pureudu liian syvälle niihin yksityiskohtiin, joilla ei ole suoraa vaikutusta toimeksiantajaan. Aiheesta on kirjoitettu paljon, mutta olen mielestäni onnistunut tuomaan myös uusia näkemyksiä tämän opinnäytetyön myötä. Vaikka tietosuoja-asetus on laaja kokonaisuus, ei se varsinaisesti muuta toimeksiantajan toimintoja. Tietosuoja-asetuksen periaatteet aiheuttavat suurempia muutoksia niihin yrityksiin, joissa ei ole aikaisemmin noudatettu yhteisiä sääntöjä tai jotka eivät ole päivittäneet toimintaansa. Toimeksiantajalta tosin on puuttunut voimassaolevat rekisterit, vaikka ne olisi pitänyt löytyä jo viime vuoden toukokuussa. Tämän opinnäytetyön yhtenä tavoitteena oli luoda rekisterit ja tämä tavoite on täyttynyt niin omalta osaltani, kuin lainsäädännön puolelta.

Yhteenvetona voin todeta, että opinnäytetyön tekeminen ja koko prosessi on ollut mielenkiintoista ja opettavaista. Toiminnallinen tutkiminen sopii itselleni hyvin ja uskon, että olen pystynyt luomaan asiaperäistä sisältöä sen avulla. Toimeksiantaja saa tämän opinnäytetyön tuloksena oman toimintansa vastaamaan asetuksen tasoa, joten sekin tavoite on täytetty. Aiheesta on kirjoitettu todella paljon, mutta olen itse siinä mielessä hyvinkin onnekas, että olen saanut opinnäytetyön taustalle toimeksiantajan.

Toimeksiantaja tuo kirjoittamiseen selkät raamit ja rajaa aihetta paremmin, kuin mitä itse olisin pystynyt.

LÄHTEET

Andreasson, A,; Koivisto, J. & Ylipartanen, A. 2015. Tietosuojakäsikirja johdolle. Tallinna: Tietosanoma.

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

Hanninen, M,; Laine, E, Rantala, K & Varhela, M. 2017. Henkilötietojen käsittely – EU-tietosuoja-asetuksen vaatimukset. Vantaa: Kauppakamari.

Europa.eu, Perustietoa Euroopan Unionista. Viitattu 17.5.2019. https://europa.eu/european-union/about-eu_fi

Eur-Lex, Access to European Union Law. Document 31995L0046. Viitattu 15.6.2019. https://eur-lex.europa.eu/legal-content/EN-FI/TXT/?uri=CELEX:31995L0046&fromTab=ALL&from=FI

Eur-Lex, Access to European Union Law. Document 32016R0679. Viitattu 20.5.2019. https://eur-lex.europa.eu/legal-content/EN-FI-SV/TXT/?uri=CELEX:32016R0679&from=EN

Finlex, Henkilötietolaki 22.4.1999/523 (kumottu). Viitattu 17.5.2019. https://www.finlex.fi/fi/laki/ajantasa/kumotut/1999/19990523

Lepomäki, E. 2017. EU:n tietosuoja-asetus ja rekisteröidyn oikeudet. Kirjoitus Elina Lepomäen blogissa 4.9.2017. Viitattu 13.8.2019. https://www.elinakoivumaki.com/gdpr-rekisteroidyn-oikeudet/

Lepomäki, E. 2017. EU:n tietosuoja-asetus ja henkilötietojen käsittelyperusteet. Kirjoistus Elina Lepomäen blogissa 23.10.2017. Viitattu 20.5.2019. https://www.elinakoivumaki.com/tietosuoja-asetus-ja-henkilotietojen-kasittelyperusteet/

Turun Sanomat, Uusi tietosuoja-asetus tulee – ainakin nämä asiat yhdistysten pitää ottaa huomioon. Viitattu 20.5.2019. https://www.ts.fi/uutiset/kotimaa/3959958/Uusi+tietosuojaasetus+tulee++ainakin+nama+asiat+yhdistysten+pitaa+ottaa+huomioon

Tietosuojavaltuuten toimisto, Mitä tietosuoja on? Viitattu 3.8.2019. https://tietosuoja.fi/tietosuoja

Unicef, 2017. Tietosuoja-asetuksen vaikutukset lapsiin – yritykset lapsen tietosuojan ja mediataitojen tukena. Viitattu 13.8.2019. https://unicef.studio.crasman.fi/pub/public/pdf/tietosuoja-asetuksen-vaikutukset-lapsiin.pdf

Yle, Verottajalta lähtenyt 27 000 virheellistä verokirjettä – Apulaistietosuojavaltuutettu: Vakava tilanne Suomessa ja mahdollisuus väärinkäytöksiin on olemassa. Viitattu 12.8.2019. https://yle.fi/uutiset/3-10915662

Tietosuojaseloste

Yleistä	Tässä tietosuojaselosteessa kerrotaan yhdistys Cygnaeus Morgonklubb:n henkilötietojen käsittelyä sekä tietosuojaa koskevista käytännöistä, prosesseista ja teknologiasta, jolla yhdistys suojelee asiakkaidensa, jäsentensä sekä työntekijöidensä tietoja.
Laadittu	1.8.2019
Tietosuojan periaatteet	Cygnaeus morgonklubb:n tietosuojaperiaatteita ovat henkilötietojen • käsittely lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi • käsittely luottamuksellisesti ja turvallisesti • kerääminen ja käsittely tiettyä, nimenomaista ja laillista tarkoitusta varten • kerääminen vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden • päivittäminen aina tarvittaessa • suojaaminen teknisesti, fyysisesti ja hallinnollisesti • lainmukainen tarkastus-, korjaus- ja poistamispyyntömahdollisuus rekisteröidyn kannalta
Tekniset, fyysiset ja organisatoriset turvatoimet tietojen suojaamiseksi	Henkilötiedot on suojattu estämällä asiattomilta pääsy yhdistyksen tiloihin sekä tiedostoihin ja varmuuskopioimalla tiedostot säännönmukaisesti. Paperisena ylläpidettävät aineistot sijaitsevat tiloissa, joihin asiattomilta pääsy on estetty. Ainoastaan yksilöidyillä henkilöillä on oikeus käsitellä ja ylläpitää rekisterien tietoja. Rekistereitä hoitavat yhdistyksen hallituksen jäsenet ja työntekijät. Rekisterien käyttöoikeus on yhdistyksen jäsenillä ja työntekijöillä. Käyttäjien käyttöoikeuksia valvotaan. Yhdistyksen jäsenillä, hallituksen jäsenillä sekä työntekijöillä on vaitiolovelvollisuus koskien yhdistyksen parissa käsitellyissä henkilötiedoissa.
Rekisteröidyn oikeudet	Rekisteröidyllä on Euroopan Unionin tietosuoja-asetuksen 15-22 § mukaisesti oikeus: 1. tarkastaa henkilötiedot 2. tietojen oikaisemiseen 3. tietojen poistamiseen 4. käsittelyn rajoittamiseen 5. siirtää tiedot järjestelmästä toiseen häntä koskeviin tietoihin, joita hänestä on tallennettu yhdistyksen tietojärjestelmiin. Joidenkin rekisteröidyn oikeuksien toteuttamista rajoittaa jokin toinen pakottava lainsäädäntö, jonka perusteella Cygnaeus Morgonklubb rf:llä on oikeus ja velvollisuus kieltäytyä perustellusti tietojen oikaisemisesta, poistamisesta, käsittelyn rajoittamisesta tai siirtämisestä järjestelmästä toiseen.

	Niissä tilanteissa, joissa rekisteröity haluaa tarkastaa, korjata tai poistaa tietojaan yhdistyksen rekisteriin kuuluvista tiedoista, tulee rekisteröidyn tehdä tietojen tarkastus-, korjaus- tai poistamispyyntö rekisterinpitäjälle. Rekisteröidyn tulee tällöin osoittaa kirjallinen pyyntö alla mainittuun sähköpostiosoitteeseen. Pyynnössä tulee yksilöidä henkilötieto, jota halutaan tarkastaa, korjata tai poistaa, sekä antaa sen rekisterin nimi, jota pyyntö koskee. Pyyntö tulee lähettää sähköpostitse osoitteeseen: pia@lindman.fi
Tietosuoja-loukkauksista ilmoittaminen	Rekisteröidylle: Ilmoitus tehdään rekisteröidylle, jos tietosuojaloukkauksesta aiheutuu todennäköisesti korkea riski tämän oikeuksille ja vapauksille. Ilmoituksessa kerrotaan tietosuojaloukkauksen luonne sekä toimenpiteet, joihin on ryhdytty, lain edellyttämällä tavalla. Valvontaviranomaiselle: Ilmoitus tehdään tietoturvaviranomaiselle 72 h kuluessa ilmitulosta, mikäli tietosuojaloukkauksesta todennäköisesti aiheutuu luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvaa riskiä. Ilmoituksessa kerrotaan tietosuojaloukkauksen luonne sekä toimenpiteet, joihin on ryhdytty, lain edellyttämällä tavalla.
Tietosuoja- ja rekisteriselosteen päivittäminen	Cygnaeus Morgonklubb kehittää toimintaansa jatkuvasti ja pidättää oikeuden päivittää tätä tietosuojaselostetta sekä rekisteriselosteita. Päivitykset voivat perustua lainsäädännössä tapahtuviin muutoksiin ja niistä seuraavien vaatimusten toteuttamiseen.
Päivitetty viimeksi	1.8.2019

Jäsenrekisteri

Rekisterin nimi	Jäsenrekisteri
Sovellettu lainsäädäntö	Euroopan Unionin Tietosuoja-asetus (EU 679/2016) ja kansallinen tietosuojalainsäädäntö
Rekisterinpitäjä	Nimi: Cygnaeus Morgonklubb rf. Y-tunnus: 2395674-2 Osoite: Brahenkatu 14 E 135 20100 Turku Sähköposti: pia@lindman.fi Puhelin: 050 4839368
Yhteyshenkilö	Nimi: Pia Lindman Tehtävä: hallituksen puheenjohtaja Sähköposti: pia@lindman.fi Puhelin: 050 4839368
Rekisterin käyttötarkoitus sekä henkilö-tietojen käsittely ja oikeusperuste	Lain tarkoittama yhdistyksen jäsenluettelo ja sen tarkoitusperien toteuttaminen, kuten jäsentietojen ylläpito ja hallinta, jäsenmaksujen hoito, jäsentiedotteiden, -kutsujen ja -kirjeiden postitus, yhteydenpito yhdistyksen jäseniin sekä luottamus- ja vastuuhenkilöihin, sekä muut yhdistyksen säännöissä mainitut ja sääntöjen mukaan tehtyjen päätösten mukaiset tarpeelliset tehtävät.
Henkilötietoryhmät sekä tietosisältö	Henkilöryhmä, jonka tietoja voidaan käsitellä: • yhdistyksen jäsenet Rekisteröidystä kerättäviä tietoja voivat olla: • nimi • yhteystiedot (osoite, puhelinnumero, sähköpostiosoite) • tiedot jäsenmaksuista • jäsenyys yhdistyksen luottamustehtävissä
Rekisterin säännönmukaiset tietolähteet	Tiedot saadaan rekisteröidyltä itseltään.
Tietojen säännönmukainen luovuttaminen	Tietoja ei luovuteta kolmansille osapuolille. Henkilötietoja ei myydä eikä vuokrata muille osapuolille. Yhdistys voi olla velvollinen luovuttamaan henkilötietoja, mikäli sovellettava laki tai asetus tai oikeus- tai hallintoviranomaisen pyyntö tätä edellyttää.
Tietojen siirto EU:n tai ETA:n ulkopuolelle	Jäsenten tietoja käsitellään tietojärjestelmissä, jotka sijaitsevat Suomessa. Henkilötietoja ei siirretä Euroopan unionin tai Euroopan talousalueen ulkopuolelle, ellei jäsen sitä itse pyydä kirjallisesti. Jäsenen pyytämät tiedonsiirrot EU tai ETA-alueen ulkopuolelle tehdään Euroopan Unionin tietosuoja-asetuksen tiedonsiirtoja koskevat vaatimukset täyttäen.
Tietojen säilyttäminen ja poistaminen	Yhdistys säilyttää henkilötietoja tietojärjestelmissään osuuskunnan toiminnan edellyttämän, sekä lakien ja viranomaisten edellyttämän ajan, jonka jälkeen ne poistetaan.

	Henkilötiedot poistetaan viimeistään silloin, kun rekisteröity niin edellyttää, ellei esimerkiksi kirjanpitoon, maksunvälittämiseen tai lain velvoittamana jotakin henkilötietoa ole välttämätöntä säilyttää pidempään.
Rekisteriselosteen muuttaminen	Yhdistys kehittää toimintaansa jatkuvasti ja pidättää oikeuden muuttaa tätä rekisteriselostetta. Muutokset voivat perustua lainsäädännössä tapahtuviin muutoksiin ja niistä seuraavien vaatimusten toteuttamiseen.
Päivitetty viimeksi	1.8.2019

Datasäkerhertsbeskrivning

Generellt	Denna datasäkerhetsbeskrivning förklarar föreningen Cygnaeus Morgonklubbs principer för behandling av personuppgifter inklusive metoder, processer och tekniker för dataskydd enligt vilka föreningen skyddar sina kunders, medlemmars och anställdas information.
Utfärdad	1.8.2019
Principer för datasäkerhet	Cygnaeus Morgonklubbs datasäkerhets principer om personuppgifter är att • behandla den registrerade på ett lagligt, ändamålsenligt och transparent sätt • hantering av data konfidentiellt och säkert • insamling och behandling av data bara för specifikt, uttryckligt och lagligt syfte • endast samla in den mängd av data som krävs, för att behandla personuppgifter i syfte • uppdatera data vid behov • skydda data tekniskt, fysiskt och administrativt • laglig inspektion, rättelse och avlägsnande av begäran från den registrerade
Tekniska, fysiska och organisatoriska säkerhetsåtgärder för att skydda data	Personuppgifter skyddas genom att förhindra obehörig åtkomst till föreningens lokaler och filer och genom att regelbundet säkerhetskopiera filerna. Pappersunderhållna material är placerade i lokaler där obehörig åtkomst nekas. Endast identifierade personer har rätt att behandla och underhålla register. Registren hanteras av föreningens styrelseledamöter och arbetstagare. Föreningens medlemmar och arbetstagarer har rätt att få tillgång till registren. Användarbehörigheter övervakas. Föreningens medlemmar och styrelseledamöter har tystnadsplikt avseende de personuppgifter som behandlas i samband med föreningen.
Registrerades rättigheter	I enlighet med artikel 15-22 § i Europeiska unionens dataskyddsförordning har den registrerade rättigheter att: 1. kontrollera personuppgifter 2. justera uppgifter 3. radera data 4. begränsa behandling 5. överföra data från ett system till ett annat Av den data som han eller hon har lagrat i föreningens informationssystem.

	Genomförandet av en del av den registrerades rättigheter begränsas av en annan tvingande lagstiftning varigenom Cygnaeus Morgonklubb r.f. har rätt och skyldighet att vägra att korrigera rättelse, radering, behandling, begränsning eller överföring från ett system till ett annat. I situationer där den registrerade vill kontrollera, justera eller radera uppgifterna i föreningens register ska den registrerade göra en begäran om kontroll, justering eller radering till den registeransvarige. Den registrerade måste sedan skicka en skriftlig begäran till den e-postadress som anges nedan. I begäran ska det anges vilka personuppgifter som skall kontrolleras, justeras eller raderas och anges namnet på det register som begäran gäller. Begäran måste skickas med e-post till: pia@lindman.fi
Rapportering av datasäkerhetsöverträdelser	Registrerade: Anmälan kommer att göras till den registrerade om dataskydds-överträdelse vilket med sannolikhet utgör en hög risk för de rättigheter och friheter som föreligger. I tillkännagivandet förklaras typen av datasäkerhetsöverträdelse och vidtagna åtgärder som krävs enligt lagen. Tillsynsmyndigheten: Anmälan skall göras till säkerhetsmyndigheten inom 72 h, om datasäkerhetsöverträdelse med sannolikhet leder till en risk för den fysiska personens rättigheter och friheter. I tillkännagivandet förklaras typen av datasäkerhetsöverträdelse och vidtagna åtgärder som krävs enligt lagen.
Uppdatering av datasäkerhetsbeskrivningen och registerbeskrivningen.	Cygnaeus Morgonklubb utvecklar kontinuerligt sin verksamhet och förbehåller sig rätten att uppdatera denna datasäkerhetsbeskrivning och registerbeskrivningarna. Uppdateringar kan baseras på ändringar i lagstiftningen och genomförandet på därpå följande krav.
Senast uppdaterad	1.8.2019

Kundregister

Registrets namn	Kund register
Lagstiftning som tillämpas	Europeiska unionens dataskyddsförordning (EU 679/2016) och nationell dataskyddslagstiftning
Controller	Namn: Cygnaeus Morgonklubb RF. FO-nummer: 2395674-2 Adress: Brahegatan 14 E 135 20100 Åbo E-post: pia@lindman.fi Telefonnummer: 050 4839368
Kontaktperson	Namn: Pia Lindman Roll: styrelseordförande E-post: pia@lindman.fi Telefonnummer: 050 4839368
Syftet med registret och behandlingen av personuppgifter och rättslig grund	Förteckningen över medlemmar i sammanslutningen och genomförandet av dess syfte, såsom upprätthållande och förvaltning av medlemsuppgifter, tillhandahållande av bidrag, tillhandahållande av medlemsbrev, medlemsinbjudningar och medlemsbrev, kommunikation med kooperativa medlemmar och ansvariga personer, samt andra nödvändiga uppgifter som anges i samarbetsreglerna och i enlighet med lag och regleringar.
Kategorier av personuppgifter och datainnehåll	Den grupp personer vars uppgifter får behandlas: • medlemmarna i föreningen Uppgifter som samlats in från den registrerade kan innefatta: • namn • kontaktuppgifter (adress, telefonnummer, e-postadress) • information om bidrag • medlemskap i kooperativa förtroendeuppdrag
Registrets regelbundna datakällor	Information erhålls från den registrerade själv.
Regelbunden utlämnande av information	Informationen lämnas inte ut till tredje part. Personuppgifter säljs inte eller hyrs inte ut till andra parter. Föreningen kan vara skyldig att lämna ut personuppgifter om så krävs enligt gällande lag eller förordning eller på begäran av en rättslig eller administrativ myndighet.
Överföring av uppgifter utanför EU eller EES	Medlemsuppgifter behandlas i informationssystem som finns i Finland. Personuppgifter kommer inte att överföras utanför Europeiska unionen eller Europeiska ekonomiska samarbetsområdet om inte medlemmen själv begär detta skriftligt. Dataöverföringar som begärs av en medlem från EU eller utanför EES görs i enlighet med kraven för dataöverföring i Europeiska unionens dataskyddsförordning.
Datalagring och radering	Föreningen kommer att behålla personuppgifter i sina informationssystem under kooperativets giltighetstid, enligt det som krävs av lagarna och myndigheterna, och därefter utgå.

	Personuppgifterna kommer att raderas senast när det krävs av den registrerade, såvida inte till exempel bokföringen, överföringen av betalningen eller juridiskt bindande av någon personlig information är nödvändigt att behållas längre.
Uppdatering av registerbeskrivningen	Föreningen kommer kontinuerligt att utveckla sin verksamhet och förbehåller sig rätten att ändra denna registerbeskrivning. Dessa ändringar kan grundas på ändringar i lagstiftningen och på genomförandet av därpå följande krav.
Senast uppdaterad	01.08.2019

Anmälningsblankett, Hakemuslomake

Anmälningsblanketten för skolelever i åk 1-4, läsåret 2019-2020, Cygnaeusmorris och -eftis

Cygnaeus morgonklubb rf.

Vänligen fyll i blanketten tydligt och betala medlemsavgift (60 euro per familj). Kontonumret är FI64 6601 0010 5130 26 (Ålandsbanken), referensnummer 1012.

Personuppgifter sparas och hanteras i Cygnaeus Morgonklubb rf. enligt dataskyddslag-stiftning.

1.

Anmälningen gäller

morris (för elever åk 1-4)

eftis (för elever åk 3-4)

2.

Skolelevens efternamn och förnamn

3.

Skolelevens personbeteckning

4.

Näradress

5.

Postnummer- och anstalt

6.

Vårdnadshavarens efternamn och förnamn

7.

Vårdnadshavarens telefonnummer

8.

E-postadress

9.

Arbetsplats

10.

Arbetstid

11.

Vårdnadshavarens efternamn och förnamn (För andra familjmember)

12.

Vårdnadshavarens telefonnummer

13.

E-postadress

14.

Arbetsplats

15.

Arbetstid

16.

Barnets skola

17.

Barnets klassnivå på hösten

18.

Barnet får avhämtas av följande personer

19.

Annat som bör beaktas (allergier, dieter, medicinering eller annat specialbehov)

20.

Behovet av morgon/eftermiddagsklubb börjar (datum)

21.

Ifall vårdnadshavaren inte kan nås så kan följande person kontaktas (namn och telefonnummer)

22.

Får foto på vilket ert barn är avbildat publiceras på föreningens hemsida och/eller i massmedia? Får barnet intervjuas eller spelas in i massmedia?