Jussi Linnala

YLEINEN TIETOSUOJA-ASETUS (GDPR) PK-YRITYKSISSÄ

Opinnäytetyö

Opinnäytetyö
Teknologiaosaamisen johtamisen koulutus (YAMK)

2020

Kaakkois-Suomen ammattikorkeakoulu

Tekijä	Tutkinto	Aika
Jussi Linnala	Insinööri (YAMK)	Toukokuu 2020

Opinnäytetyön nimi

Yleinen tietosuoja-asetus (GDPR) pk-yrityksissä

53 sivua
5 liitesivua

Toimeksiantaja

Makuuni Oy

Ohjaaja

Matti Koivisto

Tiivistelmä

EU:n yleinen tietosuoja-asetus (GDPR) tuli voimaan 25.5.2016. Asetus koskettaa jokaista EU:n kansalaisen henkilötietoja käsittelevää yritystä ja yhteisöä. Tässä työssä kuvataan Makuuni Oy:n valmistautumista EU:n yleisen tietosuoja-asetuksen täytäntöönpanoon. Yleinen tietosuoja-asetus tarjoaa rekisteröityneille paremman suojan henkilötietoihinsa ja velvoittaa yritykset, organisaatiot ja viranomaiset noudattamaan asetuksen vaatimuksia viimeistään 25.5.2018.

Opinnäytetyön tavoitteena oli tarkistaa Makuuni Oy:n järjestelmät ja toiminnot henkilötietojen käsittelyn toteuttamisessa sekä korjata selvityksissä esiin tulleet puutteet ja kouluttaa työntekijät toimimaan asetuksen vaatimusten mukaisesti. Tässä työssä EU:n yleistä tietosuoja-asetusta käsiteltiin EU:n sisällä toimivan yrityksen näkökulmasta. Tarkoituksena oli avata tietosuoja-asetuksen keskeisimmät kohdat mahdollisimman selkokielisesti, jolloin opinnäytetyötä voitaisiin käyttää muidenkin yritysten ja yhteisöjen apuna tietosuoja-asetuksen vaatimuksien toteutuksessa.

Menetelmänä työssä käytettiin konstruktiivista tutkimusta, joka koostui haastatteluista ja verkkolomakekyselyistä. Kyselyillä pyrittiin kartoittamaan hyvin hajautettu laite- ja ohjelmistokanta. Saatujen aineistojen pohjalta suunniteltiin Makuuni Oy:n tietosuojaprojekti, jossa käytiin läpi yrityksen digitaalinen ja fyysinen tietoturva sekä tarkastettiin yhdessä järjestelmätoimittajien kanssa yrityksen käytössä olevat ohjelmistot ja toimintatavat. Turhat ohjelmistot poistettiin ja toiminnalle välttämättömät päivitettiin vastaamaan uusia vaatimuksia. Ohjelmistojen päivityksen lisäksi laadittiin koulutussuunnitelma uusien toimintatapojen juurruttamiseksi jokapäiväiseen työskentelyyn. Projektin yhteydessä toteutettiin myös tietosuoja-asetuksen vaatimat dokumentaatiot, joissa listattiin yrityksen henkilörekisterit ja toimitettiin seloste yrityksen henkilötietojen käsittelytoimista. Samalla poistettiin kaikki vanhentuneet tai ilman oikeutusta säilytettävät henkilörekisterit.

EU:n tietosuoja-asetus saattaa vaikuttaa vaativalta toteuttaa pienissä yrityksissä ja yhteisöissä, mutta monessa tapauksessa pelkällä ohjeistuksella, toimintatapojen muutoksella ja toimien perustelulla saavutetaan riittävä taso. Laajasti tai arkaluontoisia henkilötietoja käsittelevillä yrityksillä kannattaa tietosuoja-asetukseen suhtautua sen ansaitsemalla vakavuudella ja tehdä kattavat selvitykset yrityksen henkilörekistereistä ja järjestelmistä.

Asiasanat

tietosuoja, asetukset, EU, henkilörekisterit

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Jussi Linnala	Master of Engineering	May 2020

Thesis title

GDPR on small and medium enterprises

53 pages
5 pages of appendices

Commissioned by

Makuuni Oy

Supervisor

Matti Koivisto

Abstract

The EU General Data Protection Regulation (GDPR) entered into force on 25 May 2016. GDPR affects every company and organization that processes personal data of an EU citizen. This paper describes Makuuni Oy's preparations for the implementation of GDPR. Makuuni was a nationwide movie rental chain in Finland. The GDPR provides data subjects (individuals) with better protection of their personal data and obliged companies, organizations and authorities to comply with the requirements of the Regulation by 25 May 2018.

The object of the thesis was to review Makuuni's systems and practices with regard to the processing of personal data, rectify the identified shortcomings and train employees to comply with the requirements of the regulation. In this thesis, the EU general data protection regulation was addressed from the perspective of a company operating within the EU. The aim was to clarify the main points of the data protection regulation so that the thesis could serve as a manual for other companies and communities in implementing the requirements of the data protection regulation.

The method used in the study was constructive research which consisted of interviews and an online questionnaire. The questionnaire surveys aimed to define the range of varied devices and software used in the business locations. On the basis of the findings, a data protection project was planned for Makuuni in which the company's digital and physical information security was reviewed and the software and operating methods used by the company were inspected together with systems suppliers. In addition to updating the essential, and deleting unnecessary software, a training plan was developed to introduce new modes of operation into daily work routines. As part of the project, the documentation required by the data protection regulation was also made, listing the company's registers that use personal data and providing a description of the company's record of processing activities. At the same time, all obsolete or unauthorized personal registers were deleted.

The EU data protection regulation may seem cumbersome and demanding to implement in small businesses and communities, but based on this study, in many cases it is possible to use just new instructions, policy changes and well explained decisions to comply with the regulation. Companies that process vast quantities of or extremely sensitive personal data should carefully study the data protection regulation with the seriousness it deserves and carry out comprehensive inquiries into the company's personal records and systems.

Keywords

GDPR, Privacy Policy, personal register

SISÄLLYS

LIITTEET

1 JOHDANTO

Tämä opinnäytetyö käsittelee EU:n yleistä tietosuoja-asetusta (2016/679) ja sen voimaantuloon valmistautumista pk-yrityksessä. EU:n yleinen tietosuoja-asetus astui voimaan 24.5.2016 ja sitä alettiin soveltaa kahden vuoden siirtymäajan jälkeen 25.5.2018 kaikissa EU:n jäsenvaltioissa. Suomen tapauksessa asetus korvasi vuoden 1995 tietosuojadirektiivin (95/46/EY) ja sen kansalliseen täytäntöön panemiseksi lyödyn henkilötietolain (523/1999). Pitkän siirtymäajan tarkoituksena oli antaa yrityksille riittävästi aikaa asetuksen soveltamiseen ennen voimaantuloa. Asetuksen tarkoitus on suojata EU:n kansalaisten henkilötietoja ja lisätä henkilötietojen käsittelyn avoimuutta sekä jäljitettävyyttä. Uusi sääntely velvoittaa henkilötietoja käsitteleviä yrityksiä ja yhteisöjä noudattamaan ja tarpeen tullen osoittamaan, että henkilötietoja säilytetään ja käytetään asetuksen mukaisesti. Siirtymäajan jälkeen voidaan yritykselle määrätä mittavat sanktiot asetuksen rikkomisesta tai laiminlyönnistä. Opinnäytetyössä on käytetty hyväksi alan kirjallisuutta ja internetin GDPR-lähteitä (General Data Protection Regulation). Näitä lähteitä ei kuitenkaan ollut yleisesti vielä käytettävissä kun varsinainen valmistautuminen tehtiin yrityksessä.

Tämän työn tavoitteena on tarkastella EU:n tietosuojalakia yleisesti ja pyrkiä keskittymään selkokielisesti asioihin, jotka jokaisen pienen ja keskisuuren yrityksen tulisi ottaa huomioon tietoturvassa ja henkilötietojen käsittelyssä. Tarkoitus on tuottaa tarkistuslista, jonka avulla yritykset voivat käydä läpi ja korjata omia toimintojaan sekä varmistaa käyttämiensä ohjelmistojensa tietoturva. Tässä opinnäytetyössä uutta tietosuojalakia tarkasteltiin Makuuni Oy ketjun (jäljempänä Makuunin tai ketjun) kannalta, mutta sitä voidaan käyttää ohjeena muillekin yrityksille. Käytännön työnä on toteuttaa Makuunin tietoturvakartoitus ja päivittää toiminnot sekä ohjelmistot asetuksen vaatimalle tasolle.

Opinnäytetyö toteutettiin lineaarisesti etenevänä tietosuojaprojektina. Työn keskeisenä menetelmänä oli konstruktiivinen tutkimus, jonka tuloksena oleva kehittämisehdotus oli tarkoitus ottaa käyttöön mahdollisimman pikaisesti. Työ eteni seuraavien vaiheiden mukaisesti: tietosuojaprojektin määrittely, perehtyminen aiheeseen kirjallisuuskatsauksen avulla, tiedon kerääminen kohdeyritykseltä haastattelujen sekä verkkolomakkeen avulla ja ehdotuksen toteutus.

Työn tuloksena syntyneet tuotokset olivat tarkoitettu pääasiassa toimeksiantajan tietoturvan kehittämiseen ja valmistautumiseen tietosuoja-asetuksen voimaantuloon, mutta ne ovat hyödynnettävissä tapaustutkimuksen periaatteiden mukaisesti myös muissa saman kokoluokan yrityksissä.

Työn rakenne on seuraava: Luvussa 2 kerrotaan yleisesti oikeudesta yksityisyyden suojaan ja sen tarpeesta tietoverkoissa. Luvussa 3 kuvataan EU:n tietosuoja-asetuksen keskeisimmät vaatimukset ja yrityksen velvollisuudet rekisterinpitäjänä. Luvussa 4 esitellään toimeksiantaja ja kerrotaan työssä käytettävät menetelmät. Luvussa 5 käydään läpi Makuunissa suoritettu kartoitus ja tietosuojaprojektin aikana tehdyt toimenpiteet. Luku 6 on pohdinta.

2 YKSITYISYYS TIETOVERKOISSA

Oikeutta yksityisyyteen pidetään ihmisen perusoikeutena. Se on osa ihmisoikeuksien julistusta, joka on hyväksytty YK:n yleiskokouksessa jo 10.12.1948 (United Nations 1948). Luvussa tarkastellaan yksityisyyden käsitettä ja sen suojaa sekä verrataan yksityisyyden ja tietoturvan vaatimuksia nykypäivänä suhteessa markkinoinnin ja yritystoiminnan tarpeisiin.

2.1 Yksityisyys ja yksityisyyden suoja

Suomessa yksityisyys on suojattu ja siitä säädetäänkin useassa laissa. Perustuslaissa yksityisyyden suoja on sielläkin määritelty perusoikeudeksi. Perustuslaki turvaa jokaiselle oikeuden yksityiselämään, kunniaan ja kotirauhaan. Normaalioloissa kirjeet, puhelut ja muiden luottamuksellisten viestien salaisuudet ovat loukkaamattomia. Lailla tähän voidaan kuitenkin säätää poikkeuksia esimerkiksi rikosten tutkinnan yhteydessä.

Yksityisyyden suoja on perusoikeus, mutta eri maiden lait ja asetukset sen takaamiseksi ovat olleet hyvinkin kirjavia tai jopa puutteellisia. Nykyisin yksityisyyttä suojataan koko EU:n tasolla yleisellä tietosuoja-asetuksella, jota myös Suomessa sovelletaan sellaisenaan tai osana kansallista lainsäädäntöä.

2.2 Yksityisyys tietoverkoissa ja tietosuoja

Tietosuoja on osa yksityisyyden suojaa. Yksityisyyden suojan mahdollistavia lakeja säädettäessä oli mahdotonta edes kuvitella nyky-yhteiskunnan verkoissa liikkuvan tiedon määrää. Tietosuoja tarkoittaa, että henkilöillä on aikaisempien yksityisyyden suojan lisäksi oikeus tietää ja lisäksi vaikuttaa sekä päättää itseään koskevien tietojen käsittelystä. Henkilöllä on oikeus tulla arvioiduksi virheettömien ja tarpeellisten tietojen perusteella. Henkilöllä on myös oikeus saada tietoonsa perusteet, joihin automaattiset päätökset perustuvat. Oikeus luottaa tietoturvallisuuteen sekä saada apua ja neuvontaa eri viranomaisilta. (Aarnio 2015.)

Vaikka yksityisyys tietoverkossa on suojattu lailla ja asetuksilla, ovat ihmiset vaihtaneet monet oikeuksistaan tässä asiassa mahdollisuuteen käyttää yhä kasvavaa määrää erilaisia digitaalisia palveluita. Samalla ihmiset ovat huolissaan, mitä heistä kerätyllä tiedolla tehdään. Tuntuu kuitenkin, etteivät tavalliset käyttäjät ole riittävän huolissaan, että tekisivät niin perustavanlaatuisia muutoksia, mitä oikea yksityisyys verkossa vaatisi. Me vaihdamme jatkuvasti tietoja itsestämme monikansallisille yrityksille, jotta saamme vastineeksi käyttää heidän ilmaiseksi mainostamiaan palveluja. Jos käyttäjä ei maksa palvelusta jota käyttää, ei hän yleensä olekaan asiakas vaan tuote. On myös vaikea selvittää, mitä kaikkea tietoa sinusta kerätään ja kenelle tiedot kaupataan.

Verkkopalveluissa yksityisyyden suoja on sidoksissa maahan, jossa palvelu on tuotettu ja toimii. Monet suosituimmista verkkopalveluista sijaitsevat USA:ssa ja ovat sen lakien alaisuudessa. USA:ssa laki antaa esimerkiksi FBI:lle mahdollisuuden vaatia verkko-operaattoreilta ja verkkopalveluiden toimittajilta tietoja asiakkaistaan kansallisen turvallisuuden nimissä. Tästä ei myöskään tarvitse ilmoittaa kyseisten henkilötietojen omistajalle. Monet maat ovat lisäksi säätäneet lakeja, jotka sallivat vakoilla kaikkea ulkomaille tai ulkomailta tulevaa viestintää. Esimerkiksi Ruotsissa puolustusministeriön alainen organisaatio Försvarets radioanstalt eli FRA saa seurata ja kuunnella kaikkea Ruotsin läpi kulkevaa viestiliikennettä. FRA saa siis lain mukaan vakoilla omia ja muiden maiden kansalaisia melkein rajoituksetta, jos dataliikenne vain kulkee Ruotsin läpi. Suomalaiset ovat tässä asiassa huonossa asemassa, sillä suurin osa ulkomaille suuntautuvasta dataliikenteestä kulkee

Ruotsin kautta ja melkein kaikki suosituimmat sovellukset ja verkkopalvelut, kuten Microsoft, Google, Facebook ja Amazon, sijaitsevat USA:ssa. Varsinkin USA:ssa kehitys näyttää menevän vielä huonompaan suuntaan, kun sitä tarkastellaan yksityisyyden suojan kannalta. Uusia lakeja, jotka mahdollistavat tarkkailun on säädetty ja säädetään terrorismin uhan varjolla. Paine yksityisyyden suojan kaventamiselle kasvaa koko ajan. Yhtenä uhkana yksityisyyden suojalle on myös yhä kasvava supervalta Kiina. Kiinassa kansalaisten valvonta tietoteknisin keinoin on huomattavasti pidemmällä, kuin missään muussa maassa ja lait yksityisyyden suojasta ovat heppoisia tai puuttuvat kokonaan. Lisäksi tulevaisuudessa Kiina tulee tuottamaan yhä isomman osan digitaalisista palveluista ja siten sen lait ja valvontakäytännöt vaikuttavat jatkossa myös Suomen kansalaisiin. Jatkuva valvonta ja Euroopan unionin säädöksiä huomattavasti höllemmät tai olemattomat yksityisyyden lait mahdollistavat Kiinan ja USA:n tapauksessa jättimäisen edun koneoppimisessa, kun tarvittavaa dataa on enemmän ja helpommin saatavissa. Tässäkin asetus pyrkii parantamaan unionin asemaa varmistamalla turvallisen datan liikkuvuuden ja käytettävyyden. (Viljanen s.a.; Niemelä 2018.)

2.3 Digitaalinen ja fyysinen tietoturva

Tietoturvasta puhuttaessa voidaan tarkoittaa perinteisen määritelmän mukaista tiedon luottamuksellista säilytystä, saatavuuden varmistamista ja ylläpitoa. Saatetaan myös tarkoittaa kyberturvaa, joka nykyään onkin erottamaton osa tietoturvaa. Kyberturvaa kuvatessa mennään yleensä syvällisemmin prosesseihin ja itse aktiivisiin toimiin turvallisuuden takaamiseksi tietoverkoissa. Tietoturva ja kyberturva ovatkin läheisiä käsitteitä ja molemmat liittyvät tiedon suojaamiseen, jotta tieto on eheää ja saavutettavissa lakien ja asetusten mukaisesti.

Tieto- tai kyberturvaa tarkasteltaessa ei saa koskaan unohtaa perinteistä fyysistä tietoturvaa. Mikään yritys ei ole tietoturvallinen, jos esimerkiksi kulunvalvonta puuttuu ja yrityksen tiloihin on mahdollista tunkeutua ja päästä käsiksi luottamuksellisiin tietoihin. Lisäksi pitää huomioida fyysiset uhat, kuten tulipalot, vesi- ja sähkövahingot, jotka saattavat tuhota palvelimia, tietokoneita ja varmistuksia. EU:n tietosuoja-asetukseen kannattaa tutustua huolimatta siitä,

puhutaanko tietosuojasta, tietoturvasta tai kyberturvasta, ja huolimatta siitä, onko kyseessä yrityksen toimitusjohtaja, asiakaspalvelija tai asiakas.

3 EU:N TIETOSUOJA-ASETUS

EU:n yleinen tietosuoja-asetus, General Data Protection Regulation (GDPR), jäljempänä asetus, on nimensä mukaisesti yleinen asetus, jota jokaista kansalaista ja yritystä EU:ssa velvoitetaan noudattamaan. Luvussa kuvataan tietosuoja-asetusta eurooppalaisten yritysten näkökulmasta. Asetuksessa viranomaisilla on mainittu monia erityisvelvoitteita ja vapautuksia, joita ei tässä työssä käsitellä.

3.1 Yleistä

EU:n jäsenmailla on jo vuosia ollut eritasoisia tietosuoja-asetuksia ja lakeja, joiden on tarkoitus suojella kansalaisia ja heidän yksityisyyttään. Onkin ollut yhä vaikeampaa tietää, ovatko tietosi turvassa ja mitä lainsäädäntöä kukin jäsenmaa käyttää tietoturvan ja tietosuojan osalta. Tarvittiin siis yksi yhteneväinen ohjeistus, jota velvoittamalla saavutetaan kaksi tärkeää päämäärää (ITGP Privacy Team 2017, 12):

1. suojella jokaisen EU:n kansalaisten oikeuksia, yksityisyyttä ja vapautta
2. vähentää liike-elämältä esteitä datan vapaassa liikkuvuudessa koko EU:n alueella.

Ratkaisuksi kehitettiin yleinen tietosuoja-asetus. EU:ssa asetus eroaa direktiivistä ratkaisevasti siinä, että asetuksessa jäsenmaiden ei tarvitse muuttaa omaa lainsäädäntöään, vaan asetukset toimivat heti lakeina ja syrjäyttävät tai vahvistavat vastaavia kansallisia lakeja. (ITGP Privacy Team 2017, 12.) Tämä mahdollistaa melko nopean ja varsinkin yhtäläisen käsittelyn. Verrattain lyhyellä kahden vuoden siirtymäajalla saatiin koko EU:n kattava ohjeistus tietosuojalle, jota jokaisen maan tulee sitä modifioimatta noudattaa.

Asetus koostuu EU:n direktiivien standardin mukaan kahdesta osasta. Ensimmäinen osa koostuu asetuksista ja toinen osa sisältää artiklat. Asetukset tuovat kontekstia ja ohjeistusta, jotta toisen osan artiklat ovat helpommin ymmärrettävissä. (ITGP Privacy Team 2017, 13.) Suuri osa asetuksista on melko

vaikeaselkoisia, vaatien jopa lakiteknistä osaamista, toisten ollessa hyvinkin selkeitä ja ytimekkäitä.

Artiklat sisältävät säännökset, joita asetuksen kohteiden, esim. yritysten, yhteisöjen ja julkisen vallan edustajien on noudatettava. Kaikki artiklat eivät kosketa yrityksiä, vaan osa on varattu esimerkiksi jäsenvaltioiden valvontakomissioille. (ITGP Privacy Team 2017, 13–14.) Jako on mielestäni melko selkeä. Tutkiessa asetusta kannattaakin aloittaa artikloista ja syventyä sitten kunkin yritystä tai yhteisöä koskettavan artiklan sisältämiin asetuksiin. Tässä työssä keskitytään yritykselle suunnattuihin artikloihin. Asetuksen esittämät vaatimukset pitää saada sisällytettyä organisaation normaaliin toimintaan (ITGP Privacy Team 2017, 17).

3.2 Kohde ja tavoitteet

Asetuksen ensimmäisessä artiklassa määritellään asetuksen kohde ja tavoitteet. Asetuksen tarkoituksena on vahvistaa säännöt luonnollisten henkilöiden suojelulle hänen tietojaan käsiteltäessä sekä säännöt näiden henkilötietojen liikkuvuutta ajatellen. Asetuksella suojellaan henkilöiden perusoikeuksia ja heidän oikeuttaan henkilötietojen suojaan. Artiklassa myös tähdennetään, ettei henkilötietojen vapaata liikkuvuutta EU:n alueella saa estää tai rajoittaa syistä, jotka liittyvät henkilön suojeluun henkilötietoja käsiteltäessä. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 1.)

Artiklassa 2 määritellään asetuksen soveltamisala. Yrityksen kannalta voidaan olettaa, että kaikki kirjatut henkilötiedot, jotka muodostavat rekisterin tai niistä on tarkoitus muodostaa rekisterin osa, kirjaustavasta ja tekniikasta riippumatta, kuuluvat asetuksen piiriin. Henkilötiedot määritellään seuraavassa luvussa. Henkilökohtaisessa tai kotitaloutta koskevassa toiminnassa asetusta ei sovelleta. Jos kuitenkin ulkoinen taho tarjoaa keinot tällaiseen henkilötietojen käsittelyyn, niin asetusta sovelletaan tähän rekisterinpitäjään/henkilötietojen käsittelijään. Asetusta ei myöskään sovelleta, mikäli rekisteröity on kuollut, rekisteröity on oikeushenkilö tai rekisterin tietoja käsittelee henkilö, joka toimii sellaisissa tarkoituksissa, jotka eivät kuulu hänen alaansa, liiketoimintaansa tai ammattiinsa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 2.)

Asetuksen tarkoitus on havainnollistettu kuvassa 1. Sen mukaan asetuksen tarkoitus on varmistaa kansalaisten oikeudet, velvoittaa rekisterinpitäjät huolehtimaan tietoturvasta ja varmistamaan keräämiensä henkilötietojen tarpeellisuus sekä antaa viranomaisille tarvittavat laajemmat valtuudet. Näin saavutetaan EU:lle yhtenäinen ja kattava tietosuojakehys sekä edistetään digitaalisten sisämarkkinoiden kehittyminen. (Suomen tietosuojapalvelut 2020)

Kuva 1. Asetuksen sisältö ja tavoite (Suomen tietosuojapalvelut 2020)

3.3 Tietosuoja-asetuksen keskeiset käsitteet ja sanasto

Asetuksen neljännessä artiklassa määritellään sanasto ja keskeisimmät käsitteet. Tässä esitellään, mitä tarkoitetaan henkilötiedolla, käsittelyllä ja rekisterillä, jotka ovat mielestäni yrityksen kannalta tärkeimmät asetuksen käsitteet.

Henkilötietoja ovat kaikki tiedot, mitkä liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön rekisterissä. Eli myös tiedot, jotka yhdistämällä toiseen tietoon luokitellaan henkilötiedoksi, mikäli yhdistäminen mahdollistaa suoraan tai välillisesti tunnistamisen. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 4.)

Taulukossa 1 on lueteltu esimerkkejä henkilötiedoista, kuten henkilötunnus, nimi, kotiosoite, sähköpostiosoite ja puhelinnumero. Lisäksi esitellään muuta-

mia esimerkkejä tiedoista, joita ei katsota henkilötiedoiksi, kuten yrityksen y-tunnus, yleiset sähköpostiosoitteet, kuten info@makuuni.fi, ja anonyymit tiedot. Nämä tiedot eivät ole yhdistettävissä luonnolliseen henkilöön ja eivät siis kuulu asetuksen piiriin. Tietoja, jotka katsotaan henkilötiedoiksi, on huomattava määrä, ja niihin kuuluu myös epäsuoran tai välillisen tunnistautumisen kautta paljon sellaista tietoa, jota ei ensi silmäyksellä epäilisi suojattavaksi tiedoksi. Tästä esimerkkinä on esimerkiksi pankkitilin numero, jonka pankkivirkailija pystyisi yhdistämään henkilöön, tai harvinainen ammattinimike.

Taulukko 1. Esimerkkejä henkilötiedoista ja tiedoista, jotka eivät kuulu asetuksen piiriin

henkilötietoja		**ei henkilötietoja**
henkilötunnus		yrityksen y-tunnus
nimi		yleiset
kotiosoite		sähköpostiosoitteet,
sähköpostiosoite		anonyymit tiedot
puhelinnumero		
auton rekisterinumero		
paikannustiedot		
IP-osoite		
potilastiedot		
kasvot sisältävä valokuva		
biometriset tunnisteet		

Käsittelyllä tarkoitetaan toimintoja, joita kohdistetaan henkilötietoihin. Käsittelyssä ei erotella automaattista tietojenkäsittelyä käsin tehtävästä tietojen keruusta tai muokkauksesta. Käsittely pitää sisällään kaiken tietojen muokkaamisen keräämisestä ja säilyttämisestä poistamiseen ja tuhoamiseen. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 4.) Tekipä yritys henkilötiedoillaan mitä tahansa, voidaan sitä sanoa henkilötietojen käsittelyksi ja yrityksen tulee ottaa silloin asetus huomioon.

Rekisteri on mikä tahansa joukko henkilötietoja, jotka yritys kerää tai pitää hallussaan ja josta tiedot ovat saatavilla tietyin perustein (EU-tietosuoja-asetus 2016/679 artikla 4). Luultavasti jokaisella yrityksellä on rekisterejä ainakin omista työntekijöistään ja asiakkaistaan. Lisäksi, kun tehdään tarkempia selvityksiä, saatetaan huomata, että yritykselle on toiminnan aikana kertynyt lukuisia muita rekistereitä, joista osaa ei enää käytetä. Kaikkiin näihin rekistereihin tulee suhtautua asetuksen säätämällä vakavuudella. Pitää myös huomioida,

että asetuksen mukaan turhia tai vanhentuneita tietoja ei pidä säilyttää vain varmuuden vuoksi. Rekisterin pidolla pitää olla pätevä syy.

3.4 Henkilötietojen käsittely ja säilytys

Henkilötietojen käsittelyä koskevat periaatteet on listattu artiklassa 5. Käsittelyssä tulee noudattaa lainmukaisuutta, kohtuullisuutta ja läpinäkyvyyttä. Mikäli henkilötietoja kerätään, on keräämisellä oltava tietty ja nimenomainen syy. Tulee myös huomioida, että tiettyä syytä varten kerättyjä henkilötietoja ei voi myöhemmin käyttää alkuperäisestä tarkoituksesta eriävällä tavalla ilman, että tietojen kohteelta kysytään uusi lupa. Kerättävien tietojen tulee olla asianmukaisia, mahdollisimman täsmällisiä ja yrityksen tai yhteisön tulee kerätä ja säilyttää vain ne tiedot, mitkä ovat kyseisen tarkoituksen mukaan tarpeellisia. Tietoja ei siis saa säilyttää pidempään kuin keräyksen yhteydessä mainittu syy vaatii. Yrityksen tulee myös huolehtia, että kerätyt henkilötiedot, eli rekisteri, säilytetään turvallisesti. Tiedot tulee suojata teknisesti turvallisesti ja asianmukaisella ohjeistuksella. Näin estetään tietojen luvaton ja lainvastainen käsittely, sekä varmistetaan tietojen oikeellisuus ja se, etteivät tiedot tuhoudu tai häviä. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 679 artikla 5.)

Tietojen säilytysajasta ja tietojen käyttötarkoituksesta poikkeuksena ovat tietyt tieteelliset tai historialliset tutkimukset sekä tilastolliset tarkoitukset (EU-tietosuoja-asetus 2016/679 artikla 89 kohta 1). Rekisterinpitäjän, eli yrityksen, on pystyttävä tarvittaessa osoittamaan, että henkilötietojen käsittely ja säilytys on toteutettu artiklan 5 osoittamalla tavalla (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 5).

Käsittelyn lainmukaisuutta ja sen periaatteita käsitellään artiklassa 6. Henkilötietojen käsittely ja säilytys on lainmukaista, mikäli yksi tai useampi alla olevista ehdoista täyttyy (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 6):

a) rekisteröity on antanut luvan henkilötietojensa käsittelyyn tiettyä tai tiettyjä tarkoituksia varten
b) henkilötietojen käsittely on tarpeen sellaisen sopimuksen käytäntöönpanossa, jossa rekisteröity on osapuolena tai mikäli rekisteröity on pyytänyt sopimuksen toteuttamiseksi tehtäviä edeltäviä toimenpiteitä

c) käsittely on rekisterinpitäjän lakisääteinen velvoite.
d) henkilötietojen käsittely tehdään rekisteröidyn elintärkeiden etujen suojaamiseksi
e) käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiselle tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi
f) käsittely on tarpeen rekisterinpitäjän oikeutettujen etujen turvaamiseksi, lukuun ottamatta tilannetta, jossa rekisteröidyn perusoikeudet tai edut/vapaudet syrjäyttävät rekisterinpitäjän edut.

Kohtaa f ei sovelleta viranomaisten suorittamaan käsittelyyn, mutta yrityksien pitää tarkasti verrata omia etujaan rekisteröidyn etuihin ja oikeuteen yksityisyydestä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 2016/679 artikla 6).

Yrityksen kannattaa ottaa käytännöksi suunnitella tarkoin, mihin tarkoitukseen henkilötietoja kerätään ja missä syntyvä rekisteri säilytetään sekä kenellä on pääsy rekisteriin ja kuinka kauan tietoja tarvitaan. Lisäksi kannattaa säilyttää rekisteröitävän mahdollisesti antama lupa henkilötietojensa käsittelystä. Jos lupaa ei ole, rekisterin yhteyteen on hyvä liittää selvitys, millä oikeudella tiedot on kerätty. Yrityksellä olisi hyvä olla julkisen tietosuojaselosteen lisäksi sisäiseen käyttöön listaus kaikista henkilötietorekistereistään, johon on myös liitetty tietoa rekisterin keräämisen syystä, käyttötarkoituksesta ja rekisterin säilytysajasta.

Yrityksen pitää olla tarkkana, mitä henkilötietoja se tallentaa rekistereihinsä. Yleisesti ottaen henkilötiedot, joista ilmenee rotu, etninen alkuperä, poliittiset tai uskonnolliset mielipiteet, seksuaalisuus ja yksilölliset biologiset tunnisteet ovat kiellettyä. Näiden henkilötietojen käsittely on sallittua vain artiklassa 9 mainituissa erityistapauksissa, kuten kun rekisteröity erikseen sallii edellä mainittujen tietojen käsittelyn. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 9.) Yrityksen kannalta rekistereihin tulee kuitenkin kirjata vain sen rekisterin kannalta oleelliset tiedot.

3.4.1 Suostumus

Monet rekisterit yritysmaailmassa perustuvat asiakkaan tai työntekijän suostumukseen. Mikäli rekisterin oikeutus on suostumus, pitää ottaa huomioon

artiklan 7 edellytykset suostumukselle. Rekisterinpitäjän pitää pystyä esittämään todiste rekisteröidyn luvasta henkilötietojensa käsittelyyn. Jos suostumus annetaan kirjallisena ja kyseisessä lomakkeessa tai ilmoituksessa on myös muita asioita tai kysymyksiä, pitää suostumusta koskeva pyyntö olla selkeästi eroteltuna muista asioista. Suostumuksen kieli ja ulkoasu tulee olla selkeä ja helposti ymmärrettävissä. Rekisteröidyllä tulee olla oikeus koska tahansa peruuttaa suostumuksensa ja suostumuksen peruuttaminen tulee olla yhtä helppoa kuin sen antaminen. Suostumuksen pitää myös olla vapaaehtoinen, eikä suostumuksesta kieltäytyminen saa estää yrityksen palveluiden käyttöä tai sopimuksen käytäntöönpanoa, ellei se ole välttämätöntä. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 7.)

Rekisteröidyn ollessa alle 16-vuotias lapsi henkilötietojen käsittely ei ole lainmukaista ilman lapsen huoltajan tai vanhempainvastuukantajan antamaa suostumusta. Yli 16-vuotiaat voivat antaa suostumuksen itse (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 7).

Jos yrityksellä oli asetuksen voimaantullessa kerättynä henkilötietoja eri rekistereihin, tuli sen kysyä lupa tai poistaa vanhat tiedot. Tämä olikin monella yrityksellä edessä esimerkiksi sähköpostilistojensa kanssa. Lupaa ei ollut kysytty oikein tai ei ollenkaan. Lisäksi osa tiedoista saattoi olla hyvinkin vanhaa. Myös tekniikan kehityksen myötä ja sähköpostimarkkinoinnin yleistyttyä lupia on vaikeampi saada asiakkailta. Yrityksen tuli sähköpostimarkkinoinnin tapauksessa myös varmistaa, että listalta on helppo poistua. Tässä on vieläkin tekemistä muutamilla yrityksillä. Poistuminen suoramarkkinointilistalta pitäisi olla asetuksen mukaan helppoa.

3.5 Rekisteröidyn oikeudet

Tässä luvussa käsitellään yleisesti rekisteröidyn oikeuksia EU:n tietosuoja-asetuksen 2016/679 artiklan 12 mukaisesti. Myöhemmin selvitetään yksityiskohtaisemmin seuraavissa artikloissa avatut rekisteröidyn oikeudet. Yritysten ja yhteisöjen tulee olla tietoisia rekisteröityneidensä oikeuksista liittyen kerättäviin henkilötietoihin.

3.5.1 Yleistä rekisteröidyn oikeuksista

Oikeutetun pyynnön saatuaan rekisterinpitäjäyrityksen tulee toimittaa, korjata tai poistaa rekisteröidyn henkilötiedot kaikista rekisterinpitäjäyrityksen järjestelmistä kuukauden kuluessa. Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella, mikäli pyyntö on erityisen monimutkainen tai vaativa. Poistettaessa tai korjattaessa tietoa pitää muistaa sisällyttää myös paperikopiot ja varmuuskopiot. Yrityksen tulee myös toimittaa rekisteröidylle tieto tehdyistä toimista. Tiedot tulee toimittaa tiiviisti esitetyssä ja helposti ymmärrettävässä muodossa. Selkeä ja yksinkertainen kieli on erityisen tärkeää, silloin kun tiedon vastaanottaja on lapsi. Tiedot tulee toimittaa yleisesti kirjallisena ja mahdollisuuksien mukaan sähköisesti tietosuoja huomioiden. Rekisteröidyn pyynnöstä tiedot voidaan toimittaa suullisesti, kunhan rekisteröidyn henkilöllisyys on ensin vahvistettu muulla tavoin. Henkilöllisyys on syytä aina tarkastaa ennen henkilötietojen toimittamista. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 12.)

Rekisterinpitäjän tulee helpottaa rekisteröidyn mahdollisuutta käyttää oikeuksiaan ja se ei saa kieltäytyä ilman painavaa syytä pyydetyistä toimista. Mikäli pyyntöä ei noudateta, on rekisterinpitäjän ilmoitettava rekisteröidylle syyt kieltäytymiseen ja informoitava mahdollisuudesta tehdä valitus valvontaviranomaiselle tai ryhtyä oikeudellisiin toimiin. Yleisesti kaikki rekisteröidylle toimitettavat tiedot ovat maksuttomia. Jos kuitenkin pyynnöt ovat toistuvia, erityisen työläitä tai perusteettomia, voi rekisterinpitäjä periä kohtuullisen maksun tietojen toimittamisen vaativasta työstä tai kieltäytyä suorittamasta pyyntöä. Rekisterinpitäjän vastuulla on osoittaa pyynnön kohtuuttomuus tai perusteettomuus. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 12.)

Edellä mainittu tietojen muuttaminen tai poistaminen ei ole yksinkertaista. Monissa yrityksissä nämä tiedot on varmistettu useaan kertaan ja niiden varmistusten avaaminen ei ole järkevää tai se on ainakin erittäin hankalaa ja kohtuuttoman kallista. Tällöinkin rekisteröidylle on syytä lähettää selvitys ja tieto, milloin henkilötiedot ovat pysyvästi poistetut tai korjatut. Monilla pitkään toimineilla yrityksillä tietoa on tallennettu vuosien ajan ja ensimmäiseksi onkin tehtävä laaja selvitystyö, missä arkaluontoista henkilötietoa on tallennettuna, onko se vielä ajankohtaista ja tarpeellista sekä keillä on pääsy kyseisiin tietoihin.

3.5.2 Ilmoitusvelvollisuus ja vastustamisoikeus

Henkilötietoja käsiteltäessä yrityksen on varmistettava, että rekisteröidyn oikeudet eivät ole uhattuna. Rekisterinpitäjän tulee ilmoittaa rekisteröidylle, kun hänen tietojaan kerätään rekisteriin. Alla on listattuna tärkeimmät kohdat, jotka ilmoituksessa pitää selvitä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 12–13):

a) kuka on rekisterinpitäjä ja rekisterinpitäjän yhteystiedot
b) minkä takia rekisteriä kerätään ja millä oikeutuksella. Mikäli oikeutus on artiklan 6 kohta f, niin myös rekisterinpitäjän tai kolmannen osapuolen edut, jotka sallivat henkilötietojen keräämisen
c) kuka on tietosuojavastaava ja hänen yhteystiedot.
d) kenelle tai mihin henkilötiedot menevät
e) tiedot, mikäli rekisterinpitäjän on tarkoitus siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle
f) kuinka kauan henkilötietoja on tarkoitus säilyttää
g) rekisteröidyn oikeudet omiin tietoihinsa. Rekisteröity voi pyynnöstä nähdä säilytettävät tietonsa, tehdä oikaisuvaatimus tai tietojen poisto tarvittaessa, rajoittaa tai vastustaa käsittelyä ja oikeus siirtää tiedot järjestelmästä toiseen
h) rekisteröidyn oikeus peruuttaa suostumuksensa milloin tahansa. Tämä ei kuitenkaan vaikuta ennen peruutusta tapahtuneeseen käsittelyn lainmukaisuuteen
i) rekisteröidyn oikeus tehdä valitus valvontaviranomaiselle.
j) tieto miksi henkilötiedot tulee luovuttaa. Onko lakisääteinen vai sopimuksellinen vaatimus? Mahdolliset seuraamukset mikäli rekisteröity ei tietoja luovuta
k) tieto mikäli yrityksen rekisteriin ja näin ollen rekisteröitävän henkilötietoihin käytetään automaattista profilointia. Tiedot käsittelyn logiikasta ja sen merkittävyys ja seuraukset rekisteröidylle
l) tieto, että mikäli rekisterinpitäjä jatkossa käsittelee henkilötietoja eri tavalla kuin siihen tarkoitukseen mihin henkilötiedot alun perin kerättiin, saa rekisteröity ilmoituksen jatkokäsittelystä ennen toimia

Kyseiset tiedot tulee toimittaa maksutta kaikille rekisteröityville. Mikäli kuitenkin rekisteröidyn pyynnöt tiedoista ovat kohtuuttomia ja toistuvia, on mahdollisuus periä kohtuullinen maksu toimista tai kieltäytyä toimittamasta tietoja. Rekisterinpitäjän tulee kuitenkin näissä tapauksissa osoittaa pyynnön kohtuuttomuus tai perusteettomuus. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 12–13.)

Vastaavat tiedot, niiltä osin kuin se on mahdollista, pitää toimittaa myös, kun tietoja ei ole saatu rekisteröidyltä. Koska tietoja ei ole saatu suoraan rekisteröidyltä itseltään, ei tietenkään ole voitu siinä tilanteessa myöskään toimittaa tietoja. Rekisterinpitäjän pitää toimittaa tiedot rekisteröidylle kohtuullisen ajan kuluessa, mutta viimeistään kuukauden kuluessa. Jos tietoja käytetään viestintään, kuten markkinointisähköpostiin, ovat nämä tiedot toimitettava ensimmäisen viestin yhteydessä. Mikäli henkilötietoja on tarkoitus luovuttaa edelleen, siitä on tiedotettava viimeistään silloin, kun tietoja luovutetaan ensimmäisen kerran. Tässäkin tapauksessa tietoja aiotaan käyttää muuhun tarkoitukseen kuin mihin ne on alun perin kerätty, tulee rekisteröidylle ilmoittaa ja mahdollisesti kysyä suostumus uudestaan. Tiedottamista ei tarvitse kuitenkaan tehdä, mikäli rekisteröity on jo saanut tiedon, tietojen toimittaminen osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa tai tiedot ovat luottamuksellisia ja salassa pidettäviä. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 14.) Tilastollisiin ja historiallisiin tarkoituksiin käytettävissä tapauksissa tiedotusta ei myöskään tarvitse tehdä, mikäli noudatetaan tietojen minimoinnin periaatteita ja tarvittavia teknisiä suojaustoimenpiteitä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 89).

Rekisteröidyllä on yleensä myös oikeus vastustaa henkilötietojensa käsittelyä artiklan 21 mukaan. Vastustamisoikeus on voimassa, jos henkilötietojen käsittely perustuu artiklan 6 kohtiin e tai f. Vastustamisen jälkeen rekisterinpitäjä ei saa enää käsitellä rekisteröidyn henkilötietoja, ellei hän pysty osoittamaan, että käsittelyyn on olemassa niin huomattava tai tärkeä syy, joka syrjäyttää rekisteröidyn edut ja oikeudet. Vastustamisoikeus pätee varsinkin, jos tietoja käsitellään suoramarkkinointia varten. Tämä vastustamisoikeus onkin hyvä olla mainittuna jokaisessa suoramarkkinointiviestissä. Viestiin on hyvä myös lisätä mahdollisuus vastustaa käsittelyä, eli esimerkiksi poistua automaattisesti suoramarkkinointilistalta, käyttäen teknisiä ominaisuuksia. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 21). Vastustamisoikeus pätee myös tilastollisiin, tieteellisiin ja historiallisiin tutkimuksiin, ellei käsittely ole tarpeen yleistä etua koskevissa tehtävissä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 89).

3.5.3 Oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus saada rekisterinpitäjältä tieto käsitelläänkö tai säilytetäänkö hänen henkilötietojaan. Rekisterinpitäjän pitää viipymättä, mutta viimeistään kuukauden kuluessa toimittaa kyselyn tekijälle tieto, onko hänen henkilötietojaan rekisterissä. Rekisterin tietojen jäljennöksessä tulee ilmoittaa, mitä henkilötietoja rekisteröitävästä rekisterissä on ja mikä on käsittelyn tarkoitus ja mahdollinen tietojen säilytysaika. Jos tietoja ei ole kerätty rekisteröidyltä suoraan, niin pitää ilmoittaa myös tietojen alkuperä. Myös aikaisemmin mainitut oikeudet oikaista, poistaa tai rajoittaa omien tietojensa käsittelyä, sekä oikeus tehdä valitus valvontaviranomaiselle tulee mainita tiedoissa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 13.)

Aina henkilötietoja toimitettaessa on vastaanottaja pystyttävä vahvistamaan. Henkilöllisyyden vahvistukseksi on mahdollista pyytää lisätietoa, mikäli rekisterinpitäjällä on perusteellinen syy epäillä pyynnön esittäjän henkilöllisyyttä. Jos henkilöllisyyttä ei rekisterinpitäjän toimesta pystytä varmistamaan, tulee siitä ilmoittaa rekisteröityneelle viipymättä. (Tietosuojavaltuutetun toimisto 2018.)

3.5.4 Tietojen oikaiseminen, käsittelyn rajoittaminen, ja poistaminen

Rekisteröidyllä on oikeus vaatia tietojensa oikaisemista ja niin ollen rekisterinpitäjällä on velvollisuus korjata epätarkat tai virheelliset henkilötiedot rekisteröidyn toimittamien lisäselvitysten mukaan. Korjaukset on tehtävä ilman aiheetonta viivytystä. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 16.)

Rekisteröity voi vaatia henkilötietojensa käsittelyn rajoittamista seuraavista syistä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 18):

a) rekisteröity kyseenalaistaa tietojensa paikkansapitävyyden. Rekisteröidyn tulee toimittaa oikaistut tiedot, jonka jälkeen rajoitukset poistetaan
b) henkilötietojen käsittely on todettu lainvastaiseksi, mutta poistamisen sijasta rekisteröity vaatii tietojensa käsittelyn rajoittamista.

c) rekisterinpitäjä ei enää tarvitse henkilötietoja alkuperäiseen tarkoitukseen, mutta rekisteröity tarvitsee tietoja oikeudellisiin tarkoituksiin
d) rekisteröity on vastustanut käsittelyä artiklan 21 kohdan 1 nojalla, käsittely rajoitetaan kunnes on todennettu syrjäyttävätkö rekisterin pitäjän oikeudet rekisteröidyn oikeudet.

Jos yllä olevien kohtien mukaan käsittely on rajoitettu, niin näitä henkilötietoja saa säilyttämisen lisäksi käsitellä vain oikeustoimissa sekä unionin tai jäsenvaltion yleistä etua koskevissa tapauksissa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 18.)

Rekisteröidyllä on myös oikeus tulla unohdetuksi, eli oikeus tietojensa poistamiseen. Rekisterinpitäjän pitää poistaa rekisteröidyn henkilötiedot ilman aiheetonta viivytystä, mikäli jokin alla olevista perusteista täyttyy (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 17):

a) henkilötietoja ei enää tarvita siihen tarkoitukseen johon ne alun perin kerättiin
b) rekisteröity peruuttaa suostumuksensa, eikä muuta laillista perustetta käsittelylle ole
c) rekisteröity vastustaa käsittelyä artiklan 21 mukaisesti, eikä muuta laillista perustetta käsittelylle ole
d) henkilötietoja on käsitelty laittomasti.
e) henkilötiedot on poistettava unionin tai jäsenvaltion lainsäädäntöön perustuen
f) henkilötiedot on kerätty lapselta huoltajan suostumuksella artiklan 8 mukaisesti.

Jos henkilötietoja on julkistettu tai jaettu eteenpäin on rekisterinpitäjän, käytettävissä olevalla teknologialla ja järkevillä kustannuksilla ilmoitettava muille rekisterinpitäjille, joilla tietoa on, rekisteröidyn vaatimuksesta poistaa kyseiset tiedot. Oikeutta unohtaa ei sovelleta, mikäli henkilötiedot koskevat sananvapautta, lakisääteisiä velvoitteita, kansanterveyttä tai oikeudellisia toimia. Poistamista ei myöskään tarvitse tehdä, mikäli henkilötiedot ovat tarpeen artiklassa 89 mainittuja yleisiä etuja edistävissä tieteellisissä, tilastollisissa tai historiallisissa tutkimuksissa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 17.)

Kaikissa oikaisu-, poisto- tai käsittelytapauksissa rekisterinpitäjän velvollisuus on ilmoittaa myös jokaiselle vastaanottajalle, joille henkilötietoja on jaettu, re-

kisteröidyn pyynnöstä oikaista, poistaa tai rajoittaa käsittelyä. Ilmoitus pitää tehdä aina, mikäli se on mahdollista eikä aiheuta rekisterinpitäjälle kohtuutonta vaivaa. Rekisteröidylle pitää myös pyydettäessä toimittaa tiedot näistä kolmansista osapuolista. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 19.)

Edellisten oikeuksien lisäksi rekisteröidyllä on oikeus siirtää häntä koskevat oman suostumuksensa mukaiset henkilötiedot toisiin järjestelmiin. Siirron tulee tapahtua suoraan rekisterinpitäjältä toiselle silloin kun se on mahdollista. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 20.)

3.6 Rekisterinpitäjän roolit ja vastuut

Jos yritys tai yhteisö kerää ja säilyttää henkilötietoja, on se automaattisesti rekisterinpitäjä ja kantaa vastuun henkilötietojen eli rekisterien säilytyksestä. Rekisterinpitäjän tulee kartoittaa todennäköiset riskit, jotka kohdistuvat rekisteröityjen henkilötietoihin ja tehdä tarvittavat tekniset ja organisatoriset toimenpiteet, jotta voidaan varmistaa ja tarvittaessa osoittaa, että on noudatettu asetuksen vaatimuksia. Yrityksen on tehtävä kattava selvitys ja tarvittavat toimenpiteet sekä tarvittaessa tarkistettava ja päivitettävä käytäntönsä jatkossakin. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 24.)

Yrityksen tai yhteisön, joka kerää, säilyttää tai käsittelee henkilötietoja, on hyvä tutustua artiklassa 40 kuvailtuihin käytännesääntöihin ja tehdä koko henkilöstölle tiedoksi käytänteet, joita noudatetaan. Käytännesäännöt tehdään kuitenkin yleensä toimialakohtaisesti. Artikla 40 mukaan käytännesääntöjen tekeminen ei ole velvoitus vaan mahdollisuus. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 40.)

Euroopan Unioni jäsenvaltioineen kannustavat yrityksiä ja yhteisöjä suorittamaan sertifiointeja ja osaamismerkkejä, joiden on tarkoitus osoittaa, että rekisterinpitäjä ja henkilötietojen käsittelijät soveltavat asetuksen määräämiä käsitteitä ja tietoturva-asiat ovat kunnossa. Sertifikaatit ja merkit eivät kuitenkaan vähennä käsittelijän tai rekisterinpitäjän vastuuta. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 42.)

3.6.1 Oletusarvoinen tietosuoja

Asetuksessa on määritelty, että rekisterinpitäjien täytyy varmistaa, että henkilötiedot ovat turvassa. Ensimmäisenä tulee määrittää tarvittavan suojauksen taso. Nimilista neljännen luokan hevoshulluista ei tarvitse kummoisia suojauksia sovittujen käytäntöjen lisäksi, mutta käsiteltäessä arkaluontoista tietoa, kuten henkilöturvatunnuksia, terveystietoja tai pankkisalaisuuksia, tulee asiaan kiinnittää erityisesti huomiota.

Määritettäessä tietosuojaa rekisterinpitäjän on otettava huomioon uusimman tekniikan mukaiset, järkevällä kustannuksella toteutettavissa olevat keinot suojella rekisteröityjen henkilötietoja. Rekisterinpitäjän tulee määritellä käsittelyn riskit rekisteröidyn oikeuksille ja toteutettava ohjeistuksella tietosuojakäytänteillä tarvittavat toimet tietojen varmistamiseksi. Näitä keinoja ovat muun muassa tietojen minimointi, tekniset suojaukset, tietojen pseudonymisointi ja muut tarvittavat suojatoimet. pseudonymisointi tarkoittaa tietojen käsittelemistä siten, että henkilötietoja ei enää voi yhdistää kyseiseen rekisteröityyn ilman lisätietoa. Nämä toimet on saatettava osaksi käsittelyä, jolloin jokaisella henkilötietojen käsittelijällä on tekninen varmuus ja ohjeistus, miten toimia oikein ja pitää rekisteröityjen tiedot ja oikeudet suojattuna. Lisäksi tulee varmistaa, että käsitellään vain kunkin tilanteen kannalta oleellisia henkilötietoja. Tilanteen kannalta oleellisia henkilötietoja määriteltäessä on otettava huomioon kerättyjen henkilötietojen määrä, käsittelyn laajuus, tietojen säilytysaika ja saavutettavuus. Mahdollisuus käsitellä henkilötietoja tulee antaa vain tarpeellisille henkilöille. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 25.)

3.6.2 Henkilötietojen käsittelijä

Henkilötietojen käsittelijä on rekisterinpitäjän määrittelemä henkilö, jolla on pääsy henkilötietoihin. Rekisterinpitäjä saa käyttää ainoastaan sellaisia käsittelijöitä, jotka käyttävät vaadittuja teknisiä ja ohjeistuksellisia tietoturvakäytänteitä käsitellessään henkilötietoja. Henkilötietojen käsittelijän ja rekisterinpitäjän välillä tulee olla sopimus, joka sitoo käsittelijän suhteessa rekisterinpitäjään. Sopimuksessa määritellään käsittelyn kohteet, kesto, käsittelyn luonne, tarkoitus, käsiteltävät henkilötiedot sekä rekisterinpitäjän oikeudet ja velvollisuudet. Erityisesti on määriteltävä alla olevat kohdat (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 28):

a) ne joilla on pääsy henkilötietoihin käsittelevät niitä vain rekisterinpitäjän ohjeistuksen mukaisesti
b) varmistaa, että henkilötietojen käsittelijät ymmärtävät ja sitoutuvat noudattamaan salassapitovelvollisuutta
c) henkilötietojen käsittelijä ja rekisterinpitäjä toteuttavat artiklassa 32 mainitut käsittelyn turvallisuuteen liittyvät toimenpiteet
d) henkilötietojen käsittelijä toimii rekisteröidyn oikeuksien mukaan ja toteuttaa tarvittaessa mahdollisuuksien mukaan velvoitteen vastata rekisteröityjen pyyntöihin koskien heidän omia tietojaan
e) henkilötietojen käsittelijä toimii ilmoitusvelvollisuuden mukaisesti
f) henkilötietojen käsittelijä poistaa tai palauttaa rekisterinpitäjälle kaikki henkilötiedot käsittelyn tarpeen päätyttyä. Ellei unionin tai jäsenvaltion lait edellytä tietojen säilyttämistä
g) henkilötietojen käsittelijä saattaa rekisterinpitäjälle kaikki asiaan liittyvä tieto, velvollisuuksien noudattamisen osoituksen varmistamiseksi ja sallii rekisterinpitäjän auditoinnin ja tarkastukset sekä osallistua niihin
h) henkilötietojen käsittelijä ilmoittaa rekisterinpitäjälle, mikäli katsoo ohjeistuksensa rikkovan asetusta, unionin tai jäsenvaltion tietosuojasäännöksiä.

Henkilötietojen käsittelijät voivat myös suorittaa sertifioinnin. Hyväksyttyjen käytännesäädöksien ja sertifioinnin suorittamista voidaan pitää osatekijänä, kun osoitetaan, että asetusta on noudatettu. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 28.)

3.6.3 Seloste käsittelytoimista (rekisteri ja tietosuojaseloste)

Yritykset ja järjestöt, joissa on yli 250 työntekijää, ovat velvoitettuja ylläpitämään kirjallista selvitystä henkilötietojen käsittelytoimista. Tämä koskee myös pienempiä yrityksiä ja yhteisöjä, mikäli henkilötietojen käsittely todennäköisesti aiheuttaa riskin rekisteröityjen oikeuksille ja vapauksille, käsittely ei ole satunnaista tai käsitellään artiklan 9 kohdassa 1 mainittuja erityisiä henkilötietoryhmiä. Rekisterinpitäjän lisäksi myös kukin henkilötietojen käsittelijä on velvollinen pitämään yllä selostetta käsittelytoimista. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 30.) Seloste on organisaation sisäinen asiakirja ja se on oltava kirjallinen sekä sähköisessä muodossa. Seloste on tarkoitettu selventämään henkilötietojen käsittelyä organisaatiossa ja osoittamaan, että henkilötietoja käsitellään tietosuoja-asetuksen mukaisesti. Selostetta ei ole tarkoitettu rekisteröityneille, mutta sitä voidaan käyttää tuotettaessa

informoivaa materiaalia tiedotukseen. Seloste on kuitenkin pyydettäessä saatettava viranomaisen saataville. (Tietosuojavaltuutetun toimisto 2018.)

Selosteessa on käsiteltävä ainakin rekisterinpitäjän ja tietosuojavastaavan nimet ja yhteystiedot, henkilötietojen käsittelyn tarkoitukset, kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä sekä mahdolliset tietojen säilyttämisen määräajat. Mikäli henkilötietoja luovutetaan kolmansille osapuolille, tulee selosteesta selvitä henkilötietojen vastaanottajat sekä mikäli kyseessä on henkilötietojen siirto kolmanteen maahan tai kansainväliselle järjestölle, tieto mihin maahan tai järjestölle henkilötietoja siirretään. Selosteeseen tulee myös mahdollisuuksien mukaan liittää tieto käsittelyn turvallisuudesta, mistä kerrotaan seuraavassa luvussa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 30.)

Asetuksessa ei edellytetä rekisteri- ja tietosuojaselosteen tekemistä ja ylläpitoa. Aikaisemmin henkilötietolaissa organisaatiot velvoitettiin ylläpitämään ja julkaisemaan kanavissaan nämä tiedot. Vaikka näitä selosteita ei enää virallisesti tarvitse olla julkaistuna, niin monet rekisteröidyt olettavat niiden löytyvän yrityksen nettisivuilta. Tietosuojaseloste on siis järkevä paikka informoida yrityksen asiakkaita ja rekisteröityjä selkeäkielisesti, mistä syystä ne monilla yrityksillä ovat nettisivuilla näkyvissä edelleen.

3.6.4 Käsittelyn turvallisuus

Rekisteröityjen tiedot on suojattava käsittelyn yhteydessä. Rekisterinpitäjän tulee varmistaa asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi. Rekisterinpitäjän tulee kartoittaa mahdolliset uhat ja peilata niitä mahdollisiin riskeihin ja henkilötietojen arkaluonteisuuteen. Tiedot tulee turvata käyttäen uusimpia, kustannuksiltaan järkeviä, tekniikoita ja ohjeistusta. Asetuksessa erityisesti mainittuja toimenpiteitä ovat henkilötietojen pseudonymisointi ja salaus,

3.6.5 Ilmoitusvelvollisuus viranomaisille ja rekisteröidylle henkilölle

Yksi erityisen tärkeä osa asetusta on uusi ilmoitusvelvollisuus tietoturvaloukkauksen tapahtuessa. Aikaisemmin yrityksillä oli mahdollisuus olla ilmoittamatta suuristakin tietomurroista. Vuosien saatossa satojen miljoonien ihmisten

henkilötietoja levisi vääriin käsiin ja tieto tapahtuneesta saatiin kuukausien tai vuosien päästä, jos silloinkaan. Useamman isonkin yrityksen järjestelmistä vuotaneet tiedot ovat sisältäneet käyttäjätunnuksia, salasanoja ja jopa luotto-korttitietoja. Pelkästään salasanojen vuoto on moninkertainen tietosuojariski, koska tutkimukset paljastavat, että vuonna 2018 jopa 59 % ihmisistä käytti samaa salasanaa jokaisessa, tai suurimmassa osassa, palvelussa mihin rekisteröityi (Lastpass by LogMeIn 2018, 7).

Artiklassa 31 rekisterinpitäjät ja henkilötietojen käsittelijät velvoitetaan tekemään yhteistyötä valvontaviranomaisten kanssa heidän tehtäviensä suorittamiseksi (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 31). Osa tästä yhteistyöstä on toimia nopeasti ja järjestelmällisesti tietoturvaloukkauksen tapahtuessa. Asetuksessa rekisterinpitäjät velvoitetaan ilmoittamaan tietoturvaloukkauksista valvontaviranomaiselle ja rekisteröityneille.

Ilmoitusvelvollisuuksia käsitellään asetuksen artikloissa 33 ja 34. Jos yritys havaitsee tietoturvaloukkauksen, sen on mahdollisuuksien mukaan ja viipymättä ilmoitettava tapahtuneesta valvontaviranomaiselle. Ilmoitus on tehtävä 72 tunnin kuluessa tietoturvaloukkauksesta. Mikäli ilmoitusta ei tässä ajassa ole tehty, rekisterinpitäjän on toimitettava valvontaviranomaiselle myös kattava ja perusteltu selitys. Suomessa ilmoitus tehdään tietosuojavaltuutetun toimistolle. Tietoturvaloukkauksesta ei tarvitse tehdä ilmoitusta mikäli on todennäköistä, ettei tapahtumasta koidu henkilötietojen omistajille oikeuksiin tai vapauksiin kohdistuvaa riskiä. Ilmoitusvelvollisuus koskee rekisterinpitäjää. Henkilötietojen käsittelijän tulee tietoturvaloukkauksen havaittuaan ilmoittaa siitä viipymättä rekisterinpitäjälle. Ilmoituksen valvontaviranomaiselle tulee pitää sisällään ainakin seuraavat asiat (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 33):

a) kuvauksen henkilötietojen tietoturvaloukkauksesta, mukaan lukien arvioidut lukumäärät, vaarantuneet rekisteröityjen ryhmät ja niiden arvioidut lukumäärät, henkilötietotyypit ja arvioidut lukumäärät
b) tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, mistä on saatavilla lisätietoa
c) kuvaus tietosuojaloukkauksen todennäköisistä seurauksista
d) kuvaus toimenpiteistä, joihin rekisterinpitäjä on ryhtynyt tai aikoo ryhtyä tietoturvaloukkauksen johdosta sekä tarvittaessa

myös toimenpiteet mahdollisten haittavaikutuksien lieventämiseksi.

Tietoja voi toimittaa osissa ja täydentää tilanteen kehittyessä ja kun uutta tietoa saadaan. Tärkeintä on tarttua heti toimeen. Rekisterinpitäjän tulee dokumentoida kaikki tietoturvaloukkaukseen liittyvät asiat vaikutuksista korjaaviin toimenpiteisiin. Tästä dokumentista valvontaviranomainen voi tarkistaa, että asetusta ja artiklaa 33 on noudatettu. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 33.)

Tietoturvaloukkauksen sattuessa rekisterinpitäjän tulee informoida suoraan myös rekisteröityneitä, joiden oikeuksille ja vapauksille tapahtuma aiheuttaa korkean riskin. Myös ilmoitus rekisteröityneille tulee tehdä ilman aiheetonta viivytystä ja ilmoituksessa tulee käyttää selkeää ja yksinkertaista kieltä. Ilmoitus rekisteröityneille tulee sisältää yllä olevasta luettelosta ainakin kohdat b, c ja d. Tätä ilmoitusta rekisteröityneille ei tarvitse tehdä, mikäli alla olevista edellytyksistä yksi tai useampi täyttyy (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 34):

a) tietoturvaloukkauksen kohteena olleet henkilötiedot on asianmukaisesti salattu. Eli on toimittu asetuksen mukaisesti ja vaarantuneet tiedot, eivät ole ulkopuolisten henkilöiden avattavissa tai ymmärrettävissä
b) rekisterinpitäjä on jo toteuttanut jatkotoimenpiteet, jonka ansiosta uhka rekisteröidyn oikeuksiin ja vapauksiin on poistettu.
c) ilmoitus suoraan rekisteröityneille aiheuttaisi kohtuutonta vaivaa. Tällöin kuitenkin tulee käyttää julkista tiedonantoa tai muuta tapaa tavoittaa rekisteröidyt tehokkaasti.

Valvontaviranomainen voi kuitenkin vaatia ilmoituksen tekemistä rekisteröityneille, mikäli katsoo rekisteröityneiden oikeuksien ja vapauksien olevan vaarassa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 34).

3.7 Tietosuojavastaava

Artiklassa 24 todetaan, että rekisterinpitäjän ja henkilötietojen käsittelijän tulee varmistaa ja tarvittaessa osoittaa, että käsittelyssä noudatetaan asetuksen säännöksiä. Tietosuojavastaavan nimittäminen ja resursoiminen on yksi tärkeä askel tähän. Tietosuojavastaava on yrityksissä asetuksen noudattamisen ja tilivelvollisuuden kulmakivi. Tietosuojavastaavan nimittämiseen kannuste-

taan myös silloin, kun se ei ole asetuksen kannalta välttämätöntä. Rekisterinpitäjän tulee varmistaa tietosuojavastaavalle riittävät resurssit. (Tietosuojatyöryhmä 2016, 5; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 37.)

Tietosuojavastaava on tietosuojan asiantuntija organisaatiossa. Hänen tehtävänä on varmistaa, että organisaatiossa seurataan asetusta henkilötietojen käsittelyssä ja auttaa säännösten tulkinnassa ja noudattamisessa. Tietosuojavastaava tai hänen tiiminsä, kannattaa jo ajoissa ottaa yrityksen toiminnassa mukaan kaikkeen tietosuojakysymyksiä sivuavaan suunnitteluun ja päätöksentekoon. Lisäksi tietosuojavastaavalla tulee olla suora yhteys organisaation johtoon ja hänet tulee säännöllisesti kutsua mukaan yrityksen ylemmän tai keskitason johdon kokouksiin. Mikäli yrityksessä tapahtuu tietoturvaloukkaus, on tietosuojavastaava otettava mukaan käsittelyyn mahdollisimman pikaisesti. Lopullinen vastuu on rekisterinpitäjällä ja henkilötietojen käsittelijällä. Tietosuojavastaava ei ole asemastaan huolimatta henkilökohtaisessa vastuussa asetuksen noudattamisesta, mutta hänen näkemyksilleen tulee antaa niiden ansaitsema painoarvo. Mikäli tietosuojavastaavan suosituksia ei noudateta, kannattaa molempien osapuolien dokumentoida syyt ja perusteet toiminnalle. (Tietosuojavaltuutetun toimisto 2018.)

Konserni voi nimittää vain yhden tietosuojavastaavan ja kyseinen tietosuojavastaava pitää olla tavoitettavissa kaikista konsernin toimipaikoista. Viranomaisilla ja julkishallinnon elimillä tietosuojavastaava voi toimia useamman instanssin edustajana. Tietosuojavastaavaa nimittäessä tulee ottaa huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä. Tietosuojavastaava tulee nimittää organisaatiolle, mikäli yksi tai useampi alla olevista ehdoista täyttyy. Tietosuojavastaavan voi nimittää vaikka mikään seuraavista ehdoista ei täyttyisikään (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 37):

a) henkilötietojen käsittelyä suorittaa viranomainen tai julkishallinnon elin, joka ei ole lainkäyttötehtäviä hoitava tuomioistuin, jotka on rajattu ulos asetuksen piiristä
b) rekisterinpitäjän ydintehtävät muodostuvat käsittelytoimista, jotka laajuutensa tai tarkoituksensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa

c) rekisterinpitäjän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu artiklan 9 mukaisiin erityisiin henkilötietoryhmiin tai artiklassa 10 mainittuihin rikostuomio/rikkomustietoihin

Nimetyn tietosuojavastaavan yhteystiedot on julkistettava ja lähetettävä valvontaviranomaiselle. Suomessa ilmoituksen voi tehdä tietosuojavaltuutetun toimiston internetsivuilla olevan ilmoituslomakkeen avulla. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 37.)

3.7.1 Tietosuojavastaavan asema ja tehtävät

Tietosuojavastaavalla tulee olla rekisterinpitäjän ja henkilötietojen käsittelijän tuki ja riittävät resurssit tehtävässään. Hänellä tulee olla pääsy käsiteltäviin henkilötietoihin ja käsittelytoimiin sekä mahdollisuus ylläpitää ja kehittää asiantuntemustaan. Vaikka tietosuojavastaavalla tulee olla rekisterinpitäjän tai henkilötietojen käsittelijän tuki, on myös tärkeää, että tietosuojavastaava pystyy työskentelemään tehtävässään ilman painostusta. Tietosuojavastaavan asema tulee olla sellainen, ettei häntä voida ohjeistaa toimimaan vastoin tehtävänsä velvoitteita ja ettei häntä voida erottaa tai rangaista niiden takia. Tietosuojavastaavan tuleekin raportoida suoraan organisaation ylimmälle johdolle. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 38.)

Rekisteröidyillä pitää olla mahdollisuus ottaa suoraan yhteyttä organisaation tietosuojavastaavaan asioissa, jotka koskettavat heidän henkilötietojen käsittelyä ja oikeuksia. Tietosuojavastaavaa sitoo tehtävässään salassapitovelvollisuus. Tietosuojavastaavalla voi organisaatiossa olla muitakin tehtäviä, kunhan on varmistettu, etteivät ne ole ristiriidassa tietosuojavastaavan tehtävien ja velvollisuuksien kanssa. (Tietosuojatyöryhmä 2016, 15–18; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 38).

Tietosuojavastaavan tehtäviä on organisaatiosta riippuen monenlaisia. Asetuksen artiklassa 39 on lueteltu muutamia oleellisimpia tehtäviä. Tietosuojavastaavalla tulee olla mahdollisuus (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 39):

a) antaa tietoa ja neuvoja, jotka koskevat asetuksen ja muiden unionin tai jäsenvaltion tietosuojasäännösten asettamia velvollisuuksia
b) varmistaa, että asetusta ja muita tietosuojasäännöksiä noudatetaan organisaatiossa. Analysoida organisaation henkilötietojen käsittelytoimet ja varmistaa, että ne ovat vaatimusten mukaisia. Huolehtia, että henkilöstö saa asianmukaiset ohjeistukset ja koulutukset
c) pyydettäessä antaa neuvoja koskien vaikutusarviointia ja valvoa sen toteutusta
d) toimia yhteistyössä viranomaisten kanssa
e) toimia yhteyspisteenä organisaation ja viranomaisten välillä.

Tietosuojavastaavan tulee työssään arvioida ja priorisoida käsittelytoimiin liittyvät suurimmat riskit ja niiden muodostamat tilanteet sekä keskittyvä ensisijaisesti niiden ehkäisemiseen, unohtamatta kuitenkaan pienempiä riskejä. Riskiarvioinnissa tulee ottaa huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. (Tietosuojatyöryhmä 2016, 20–27; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 39).

3.7.2 Käytännesäännöt ja seuranta

Asetuksen artiklat 40 ja 41 keskittyvät käytännesäännösten laatimiseen ja seurantaan. Vaikka yksittäinen rekisterinpitäjä tai henkilötietojen käsittelijä voikin laatia käytännesääntöjä, on ne suunniteltu ensisijaisesti laadittavan heitä edustavien yhteisöjen toimesta. Käytännesääntöjen on tarkoitus selventää ja edesauttaa tietosuojalainsäädännön toimialakohtaista soveltamista. Käytännesääntöjä koskeva ohjeistus on julkaistu tietosuojavaltuutetun toimiston verkkosivuilla. EU:n tietosuojaviranomaisten laatima ohjeistus antaa käytännön neuvoja ja tulkintaohjeita käytännesääntöjä koskevien artikloiden soveltamiseen. (Minilex s.a.; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 40–41).
Käytännesääntöjen laadinta ei normaalisti kosketa tämän työn kohdeyrityksiä, joten asiaa ei käsitellä tässä työssä enempää. Tietosuojavaltuutetun toimiston ohje on verkkopalvelussa www.tietosuoja.fi.

3.7.3 Vaikutusarviointi, ennakkokuuleminen ja sertifiointi

Asetuksessa on esitetty rekistereitä kerääville yrityksille useita vaatimuksia ja ohjeistuksia. Yrityksen tulee tarvittaessa pystyä osoittamaan, että asetuksen

vaatimat toimenpiteet ja ohjeistukset on todella tehty ja voimassa. Varsinkin tietoturvaloukkauksen tapahtuessa yrityksen tulee oman etunsa tähden pystyä osoittamaan, että riskeihin oli varauduttu tarpeeksi kattavasti. Asetuksessa tarjotaankin muutamia keinoja tähän avuksi.

Tietosuojavaltuutetun toimisto (2018) kehottaa vaikutusarvioinnissa ottamaan huomioon käsittelyn luonteen, laajuuden, asiayhteydet ja tarkoitukset sekä peilaamaan niitä luonnollisen henkilön oikeuksien ja vapauksien riskiin. Tässä tapauksella oikeuksilla tarkoitetaan yleensä oikeutta yksityisyyteen ja tietosuojaan, mutta se pitää sisällään myös muita perusoikeuksia, kuten sananvapauden. Vaikutusarvioinnissa tavoitteena on päättää ennen käsittelyn aloittamista, onko jäljelle jäänyt riski oikeutettu ja hyväksyttävissä. Arviota tehdessä tulee tietosuojavastaava ottaa mukaan käsittelyyn, mikäli sellainen on organisaatiossa nimitetty. Vaikutusarviointi auttaakin rekisterinpitäjiä dokumentoimaan ja osoittamaan, että asetuksen vaatimuksia on noudatettu. Vaikutusarviointi tehdään yksittäistä käsittelytoimea varten ja sitä on hyvä ajatella prosessina. Vaikutusarviointia on päivitettävä, mikäli riskit tai tarpeet muuttuvat. Vaikutusarviointi pitää tehdä myös käsittelytoimille, jotka on aloitettu ennen asetuksen voimaantuloa. Rekisterinpitäjän tulee tunnistaa ja kuvata tarpeelliset käsittelytoimet mahdollisen tietosuojavastaavan avustuksella, tehdä arvio käsittelytoimien tarpeellisuudesta ja asetuksen noudattamiseen osoittavista toimenpiteistä sekä kirjata ja toteuttaa suunnitellut toimenpiteet riskeihin puuttumiseksi. Rekisterinpitäjän tulee myös dokumentoida koko vaikutusarviointi ja järjestää käsittelylle seuranta ja tarkistus. Mikäli tilanne muuttuu, rekisterinpitäjän tulee korjata suunnitelma ja toimenpiteet. Vaikutusarvioinnin vaiheistus on esitetty kuvassa 2. (Tietosuojavaltuutetun toimisto 2018.)

Kuva 2. Tietosuojaa koskevan vaikutusarvioinnin eteneminen (Tietosuojatyöryhmä 2017, 19)

Vaikutusarviointi on tehtävä silloin, kun käsittelytoimi todennäköisesti aiheuttaa korkean riskin rekisteröityneelle. On siis arvioitava onko riski todennäköinen. Tapauksissa, jossa jää epäselväksi tarvitaanko vaikutusarviointi, on suositeltua tehdä se joka tapauksessa ja siten varmistaa asetuksen noudattaminen. (Tietosuojatyöryhmä 2017, 9–10.)

Artiklassa 35 luetellaan esimerkkitapauksia, joissa erityisesti vaaditaan tekemään vaikutusarviointi ennen käsittelyn aloittamista. Nämä kuitenkin ovat vain esimerkkejä ja tapauksia voi olla monia muitakin. Tärkeintä on tunnistaa käsittelyssä riskialttiin asiat, joita ovat esimerkiksi (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 35):

a) arkaluontoiset tiedot tai hyvin henkilökohtaiset tiedot
b) heikossa asemassa olevien rekisteröityneiden tiedot
c) tietojen laajamittainen ja tai automaattinen käsittely
d) järjestelmällinen valvonta yleisellä alueella.

Vaikutusarvioinnin osoittaessa korkeaa riskiä eikä rekisterinpitäjä kykene toimillaan pienentämään tätä riskiä, on rekisterinpitäjän ennen käsittelyä kuulta-

va valvontaviranomaista. Rekisterinpitäjän tulee tässä tapauksessa toimittaa valvontaviranomaiselle kaikki vaikutusarvioinnin tiedot, tarpeelliset yhteystiedot käsittelijöistä ja mahdollisesta tietosuojavastaavasta, toimenpiteet millä rekisteröityneiden oikeudet ja vapaudet on pyritty suojaamaan sekä kaikki muut valvontaviranomaisen pyytämät tiedot. Valvontaviranomaisen on enintään kahdeksan viikon kuluessa annettava rekisterinpitäjälle kirjalliset ohjeet. Määräaikaa voidaan tarvittaessa jatkaa kuusi viikkoa tai kunnes valvontaviranomainen on saanut rekisterinpitäjältä pyytämänsä lisätiedot. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 36.)

Toinen keino varmistaa asetuksen noudattamista ja sen osoittamista on sertifiointi. Jäsenvaltio, valvontaviranomaiset, tietosuojaneuvosto ja komissio kannustavat organisaatioita ja rekisterinpitäjiä ottamaan käyttöön sertifiointimekanismeja, tietosuojasinettejä ja -merkkejä, jotka unionin tasolla osoittavat rekisterinpitäjien noudattavan tätä asetusta. Sertifiointi ei millään tavalla vähennä rekisterinpitäjän vastuuta asetuksen noudattamisessa, mutta tarjoaa tavan tarkistaa organisaation toimintatapoja ja osoittaa mahdollisissa tarkastuksissa, että asetusta on pyritty noudattamaan. Sertifiointi voidaan myöntää kerrallaan kolmeksi vuodeksi ja sertifiointi tulee olla vapaaehtoista, helposti saatavilla sellaisen menettelyn perusteella, joka on läpinäkyvä. Tietosuojaneuvosto kokoaa ja julkaisee kaikki sertifiointimekanismit, tietosuojasinetit ja –merkit. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 42.)

3.8 Sanktiot

Vaikka asetus voi varsinkin monista pienistä yrityksistä kuulostaa työläältä, niin se kannattaa ottaa vakavasti. Ääritapauksissa yritykselle, joka on jättänyt tietoturvallisuutensa hoitamatta, voidaan tietomurron yhteydessä määrätä jopa 20 miljoonan euron sakko tai vastaavasti 4 % sakko yrityksen koko konsernin liikevaihdosta. Tämän suuruisesta sakosta monen yrityksen olisi mahdotonta selviytyä. Muita seuraamuksia voivat olla varoitukset, huomautukset sekä henkilötietojen käsittelyn rajoittaminen ja kieltäminen. (Pyyhtiä 2019, 38.)

Asetuksen ja sanktioiden tarkoituksena ei kuitenkaan ole pelotella yrittäjiä ja organisaatioita, vaan edistää digitaalisten sisämarkkinoiden kehittymistä, kilpailukykyä ja kasvua sekä tietenkin parantaa rekisteröityneiden oikeuksia.

Sanktiot määrätään kunkin yksittäistapauksen mukaan ja eivät ole varmasti ensimmäiset keinot tarttua selviäviin epäkohtiin.

4 OPINNÄYTETYÖN TOIMEKSIANTAJAN JA TYÖSSÄ KÄYTETYN MENETELMÄN ESITTELY

Tässä luvussa esitellään työn toimeksiantaja sekä työlle asetetut tavoitteet. Luvussa esitetään lyhyesti myös käytettävä tutkimusmenetelmä ja miten sitä sovelletaan tässä työssä.

4.1 Toimeksiantaja

Työn toimeksiantaja toimi Makuuni Oy ketju, jäljempänä Makuuni. Makuuni on vuodesta 1985 toiminut videovuokrausketju, jonka liikevaihto koostuu pääosin elokuvien vuokraamisesta ja myynnistä sekä irtomakeisten myynnistä. Ketjulla oli parhaimmillaan melkein 100 liikettä ympäri Suomea, ja se oli pitkään johtava elokuvavuokrausketju Suomessa. Makuuni toimi vuosia franchising-ketjuna, useiden yrittäjien ja lokaatioiden takia ohjelmistot ja laitekannat olivat hyvin erilaisia. Tämä tietenkin teki projektista haastavan. Tietosuojaprojektin osana olikin selvittää, ja mahdollisesti poistaa, ohjelmistot, joita liikkeillä oli käytössä.

Vuokraustoiminnan luonteen takia oli välttämätöntä säilyttää asiakasrekisteriä, jossa asiakkaasta oli tallennettuna kaikki vuokraustoiminnan kannalta oleellinen tieto. Väärinkäytöksien sattuessa asiakas piti olla varmasti jäljitettävissä, jotta yrityksen omaisuus voitiin periä takaisin. Kassajärjestelmän vuokrausohjelmassa oli siis tallennettuna Makuunin kaikkien asiakkaiden tiedot henkilötunnusta myöten. Makuunin oli siis toimittava rekisterinpitäjänä. Uuden EU:n tietosuoja-asetuksen julkistuksen jälkeen Makuunissa haluttiin kerralla varmistaa, että asetuksen vaatimukset täyttyvät ketjussa ja sen käyttämissä järjestelmissä. Tietosuojaprojekti suoritettiin asetuksen julkaisun ja sen voimaantulon välissä vuosina 2016–2018. Makuuni hakeutui yrityssaneeraukseen kesäkuussa 2018. Saneeraus ei tuottanut tulosta, vaan yritys hakeutui konkurssiin ja ketjun liikkeet sulkivat ovensa lopullisesti 5.9.2018.

4.2 Opinnäytetyön tavoite ja menetelmä

Työn tavoitteena on saattaa toimeksiantajayrityksen järjestelmät, käytännöt ja ohjeistus EU:n tietosuoja-asetuksen velvoittamalle tasolle. Projekti toteutettiin konstruktiivisena tutkimuksena, jonka tuloksena syntyi päivitetty ohjeistus yrityksen henkilöstölle sekä dokumentoidut tiedot yrityksen käyttämistä järjestelmistä ja niiden turvallisuudesta henkilötietojen käsittelyssä. Menetelmäksi valittiin konstruktiivinen tutkimus, sillä tiedon lisäksi tarvittiin myös konkreettinen ohjeistus ja monien ohjelmistojen kohdalla muutostyö tietosuojan korjaamiseksi. Tässä tapauksessa konstruktiivisessa tutkimuksessa tavoitteena oli saada ongelmaan käytännön ratkaisu, joka oli perusteltu asetuksen artikloissa. Konstruktiivisessa tutkimuksessa olisi suotavaa, että ongelman ratkaisu osoittautuisi toimivaksi myös muissa kuin tutkimuksen kohdeorganisaatiossa. (Ojasalo ym. 2015, 66.)

Konstruktiivisen tutkimuksen vaiheet on kuvattu kuvassa 3. Tutkimus alkaa ongelman tunnistamisella ja valinnalla. Ongelman etsimisen jälkeen tutustutaan syvällisesti teoriaan, eli hankitaan mahdollisimman tarkasti tietoa tutkimuksen kohteesta. Hankittujen tietojen pohjalta laaditaan ratkaisuehdotus, jonka toimivuus toteutukseen jälkeen testataan. Seuraavissa vaiheissa ratkaisussa käytetyt teoriakytkennät kuvataan ja osoitetaan ratkaisun uutuusarvo sekä tarkastellaan ratkaisun soveltamisalueen laajuutta. Konstruktiivisessa tutkimuksessa, kuten missä tahansa tieteellisessä tutkimuksessa, on tärkeää dokumentoida eri vaiheet. (Ojasalo ym. 2015, 67.)

Kuva 3. Konstruktiivisen tutkimuksen prosessi (Ojasalo ym. 2015, 67)

Tietosuojaprojektin alussa tarvittiin tieto yrityksen ja ohjelmistojen tietoturvasta ja nykyisestä tietosuojan tasosta. Tätä lähdettiin kartoittamaan kvantitatiivisia ja kvalitatiivisia menetelmiä käyttäen. Kvalitatiivisena eli laadullisena menetelmänä toteutettiin yrityksen valikoitujen avainhenkilöiden avoin haastattelu. Kvantitatiivinen eli määrällinen menetelmä oli tässä tapauksessa koko henkilöstölle avoin nimetön kysely lomakehaastatteluna. Tietoa hankittaessa on hyvä käyttää kahta tai useampaa menetelmää, jotka tukevat toisiaan. Näin saadaan kattavampi kuva ongelmasta, jota lähdetään ratkaisemaan. (Ojasalo ym. 2015, 40,68 ja 104–105.)

Kyselyllä ja haastatteluilla saatiin selvitettyä yrityksen tietotekninen nykytila ja tietojen pohjalta rakennettiin toimintasuunnitelma projektin läpivienniksi. Konkreettista tietoa suunnitelman pohjaksi saatiin tutustumalla alan kirjallisuuteen sekä asetuksen tekstiin, osallistumalla erilaisiin tietosuoja-asetusta käsittele-

viin seminaareihin ja yhteistyöyritysten konsultoinnin avulla. Haastatteluiden ja teorian avulla määritettiin tarvittavat toimenpiteet yrityksen saattamiseksi tietosuoja-asetuskelpoiseksi.

5 MAKUUNI OY TIETOSUOJAPROJEKTI

Luvussa käsitellään Makuuni Oy ketjussa tehtyjä haastatteluita ja tietosuojaselvityksiä sekä muita toimia valmistautuessa tietosuoja-asetuksen soveltamiseen. Tiedonhankinnan ja suunnittelun jälkeen esitellään havaitut ongelmakohdat ja toimenpiteet tilanteen korjaamiseksi. Lisäksi luvussa kuvataan myös yrityksen sisäiseen käyttöön tehty seloste käsittelytoimista sekä rekisteröityneiden informoimiseksi tehty tietosuojaseloste.

5.1 Nykytilan kartoittaminen

Projektin alusta asti oli selvää, että onnistuakseen projektissa tulisi hankkia tarkasti tieto käytetyistä ohjelmistoista, käytänteistä ja laitteista, joita ketjulle oli vuosien saatossa kertynyt. Makuunin ketjun haltuun oli viimeisten vuosien aikana otettu kaikki aikaisemmin franchising-pohjalla toimineet liikkeet. Yrittäjävetoisissa liikkeissä oli vaadittu laitekannan ja ohjelmistojen käytöstä ainoastaan kassalaitteena olevan Linux-päätteen, kassaohjelmiston ja sen oheislaitteiden yhtenäisyys. Muut tietokoneet, verkkolaitteet ja ohjelmistot hankittiin yrittäjän oman harkinnan mukaan, joskin monesti ketjun ohjeistusta mukaillen. Tietosuojaprojekti antoi hyvän mahdollisuuden kartoittaa ja korjata tilanne. Ketjun tilannetta lähdettiin kartoittamaan erityisesti valittujen avainhenkilöiden haastatteluilla ja niiden pohjalta toteutetulla laajemmalla lomakekyselyllä. Haastattelusta tai lomakekyselystä ei kirjattu mukaan vastaajan henkilötietoja ja näin vältettiin luomasta uusi rekisteri yritykselle.

Laitteiden ja ohjelmistojen lisäksi tarkastettiin ohjeistuksen tilanne ketjussa. Havaittiin, että vaikka ketjussa oli tarkat ja yksityiskohtaiset ohjeet järjestelmien käytöstä ja asiakastilanteiden hoidosta, ei niissä otettu huomioon voimaantulevaa asetusta oikeastaan ollenkaan. Henkilötietojen käsittely ei ollut asetuksen vaatimalla tasolla ja vaatisi uudelleenohjeistusta ja muutamissa tapauksissa myös ohjelmistojen muutoksia.

5.1.1 Haastattelut

Haastattelut suoritettiin pääosin kasvotusten yksi henkilö kerrallaan. Osa haastatteluista oli ketjun levinneisyyden takia tehtävä videoneuvotteluohjelman välityksellä ja osa sähköpostilla. Haastattelut kasvotusten, videoneuvottelut mukaan lukien, sopivat mielestäni huomattavasti paremmin tiedonkeruuseen. Sähköpostikyselyssä on liian helppo vastata lyhyesti, tai jopa jättää mainitsematta jotain aihetta kokonaan, ilman että haastattelija sitä huomaa.

Haastateltaviksi valittiin 10 ketjun eri osa-alueilla toimivaa avaintyöntekijää. Haastateltaviksi pyrittiin valitsemaan henkilöitä erilaisilla tietoteknisillä taustoilla. Haastateltaviksi valikoitui ihmisiä IT-puolelta, taloushallinnosta, johdosta, markkinoinnista, varastolta ja liikkeiden operatiivisesta johdosta. Pidimme tärkeänä, että heti alkuun saataisiin mahdollisimman kattava kuva koko ketjun toiminnasta tietosuojan ja ohjelmistojen kannalta tarkasteltuna.

Haastatteluun valmistautuessa haastateltavat saivat tehtäväksi tutustua uuden asetuksen keskeisimpiin käsitteisiin ja vaatimuksiin. Itse haastattelussa käytiin läpi haastateltavan työssään käyttämät ohjelmistot, hänen suorittama henkilötietojen käsittely sekä tarkasteltiin tietoturvaa digitaalisella ja fyysisellä tasolla. Haastatteluissa selvisi ensimmäisenä, että vaikka asetuksesta oli puhuttu mediassa ja ketjussa jo pidemmän aikaa, oli sen sisäistäminen jäänyt pinnalliselle tasolle. Asetuksen laajuutta, sen velvoitteita ja mahdollisia sanktioita ei tiedetty tai ne oli ohitettu ajatellen niiden kuuluvan vain järjestelmävastaavan toimenkuvaan. Haastattelut olivat hyvä tilaisuus kertoa asetuksen kokonaisvaltaisista velvoitteista organisaatioille.

Henkilökohtaisien haastatteluiden tuloksena syntyi lista ohjelmistoista ja työskentelytilanteista, joissa henkilötietoja käsitellään. Nämä rekisterit kerättiin tässä vaiheessa alustavaksi Makuunin listaukseksi henkilötietorekistereistä. Lisäksi havaittiin muutamia jo käytöstä poistuneita rekistereitä, jotka olivat jääneet tuhoamatta tai joita säilytettiin varmuuden vuoksi. Nämäkin listattiin ja merkittiin tuhottaviksi mahdollisuuksien mukaan. Listaus henkilötietoja sisältävistä ohjelmistoista ja fyysisistä materiaaleista täydentyi lomakekyselyn jälkeen.

5.1.2 Ohjelmisto ja tietosuojakysely työntekijöille

Haastatteluiden pohjalta muokattua kyselyä lähdettiin tekemään laajemmalle kohderyhmälle. Aluksi tarkoituksena oli tehdä lomakekysely vain liikkeiden vastuumyyjille ja toimiston työntekijöille, mutta otantaa päätettiin laajentaa, jotta saatiin varmistettua mahdollisimman kattava kuva nykytilanteesta. Kyselyyn vastaaminen tehtiin nimettömästi. Ideana oli, että näin saataisiin tietoon mahdollisimman paljon epävirallisia, ketjun ohjeistuksen ulkopuolelta asennettuja ohjelmia. Lisäksi toimintatapa varmisti, että vastauksia saatiin riittävä määrä ja ettei yksikään vanhentunut laite tai ohjelmisto jäänyt verkkoon tietoturvariskiksi.

Tiedonkeruun tämä osa päätettiin suorittaa käyttäen Googlen Forms-palvelua. Näin tulokset saatiin helposti koottua taulukoksi Excel-ohjelmaan. Linkki lomakkeeseen lähetettiin ketjun jokaiseen sähköpostiosoitteeseen ja sitä mainostettiin yrityksen sisäisissä kanavissa. Kaikkia työntekijöitä kannustettiin vastaamaan kyselyyn. Lomakekysely lähetettiin koko henkilöstölle noin 250 kpl ja vastauksia saatiin 43 kpl.

Lomakekyselyssä haettiin tietoa liikkeiden tietokoneista, muusta laitekannasta ja käytetyistä ohjelmistoista. Lisäksi kysyttiin henkilötietojen säilytyksestä liikkeissä. Lomakekyselyä ei käytetty tiedottamaan tietosuoja-asetuksesta, vaan sen tarkoitus oli kerätä tietoa ketjun tietosuojaprojektia varten. Kyselylomake on esitetty tämän työn liitteessä 1.

Vastauksia laitekannasta ja ohjelmistoista verrattiin tietoturvaohjelmisto F-Securen esittämiin tietoihin. Vertailussa huomattiin, että muutamia koneita ja useita ohjelmistoja ei ollut rekisteröitynyt F-Securen tietokantaan. Asiaa tarkemmin tutkittaessa, kyseessä oli vanhentuneita käyttöjärjestelmiä sisältäviä Windows-koneita, jotka olivat kuitenkin vielä liikkeessä ja osa myös verkossa. Kyselyn vastauksien perusteella pystyttiin myös täydentämään aikaisempaa listausta henkilötietorekistereistä yrityksessä. Taulukossa 2 on esitetty listaus Makuuni Oy:n henkilötietoja sisältävistä rekistereistä. Taulukossa näkyy myös, mitä henkilötietoja kyseisessä rekisterissä on tallennettuna sekä määrä tai arvio henkilöistä, joiden tietoja rekisterissä on. Myöhemmin tietosuojaprojektin edetessä taulukkoon lisättiin myös merkintä milloin rekisteri tai henkilötiedot

tulee poistaa. Aikaisemmin oikeastaan mitään tietoa ei poistettu rekistereistä, ellei sitä asiakas vaatinut. Huomioitavaa on, että oikeastaan kaikki digitaalinen aineisto oli varmennettuna yhteen tai useampaan kertaan ja niiden poistossa tuli huomioida myös nämä varmistukset. Taulukko on yrityksen sisäiseen käyttöön.

Taulukko 2. Makuuni Oy listaus henkilörekistereistä

Ohjelmisto	**Henkilötietoja**	**määrä tai arvio**	**Tietojen poisto**
Profix kassajärjestelmä	Sotu, nimi, osoitteet ym.	500 000	2 vuotta viimeisestä asiakastapahtumasta
Lemonsoft tilausjärjestelmä	Nimi, sähköpostiosoite.	200	1 vuosi viimeisestä asiakastapahtumasta
sonet palkkaohjelmisto	Sotu, nimi, osoitteet ym.	5000	10 vuotta viimeisestä tilikauden päätöksestä
työajanseuranta / työvuorolistat	Nimi, sähköpostiosoite, IP-osoite ym.	2000	10 vuotta viimeisestä tilikauden päätöksestä
sähköposti	Nimi, sähköpostiosoite ym.	5000	
markkinointi-sähköpostisuorat	Nimi, puhelinnumero, postinumero, sähköpostiosoite, sukupuoli.	150 000	Poisto mikäli sähköposti ei mene perille tai asiakkaan pyynnöstä
intranet	Nimi, sähköpostiosoite, IP-osoite ym.	300	työsuhteen päättyessä
Vanha Clubi	Nimi, sähköpostiosoite, käyttäjätunnus, salasana	50 000	poisto heti
Vanha sähköpostisuora	Nimi, sähköpostiosoite	100 000	poisto heti
vanhat käyttäjätunnukset	Nimi, sähköpostiosoite, käyttäjätunnus, salasana	300	poisto heti
Alaikäisen vuokrauslupalaput	Sotu, nimi, osoitteet ym.	?	kunnes asiakas on täysi-ikäinen
Sähköpostimarkkinointilupa	Nimi, puhelinnumero, postinumero,	?	
Dropbox	Liikekohtaisia tietoja	?	

Kyselyn toteutustapa mahdollisti paljon vastauksia. Vastauksia tuli myös ihmisiltä, jotka eivät tunteneet tietotekniikkaa tai laitteita. Tästä syystä lomakkeessa oli käytössä vapaat vastauskentät. Vapaiden vastauksien takia vaadittiin paljon käsityötä vastausten käsittelyssä. Tämä oli kuitenkin harkittua ja vastauksien monimuotoisuuden ja määrän takia järkevää.

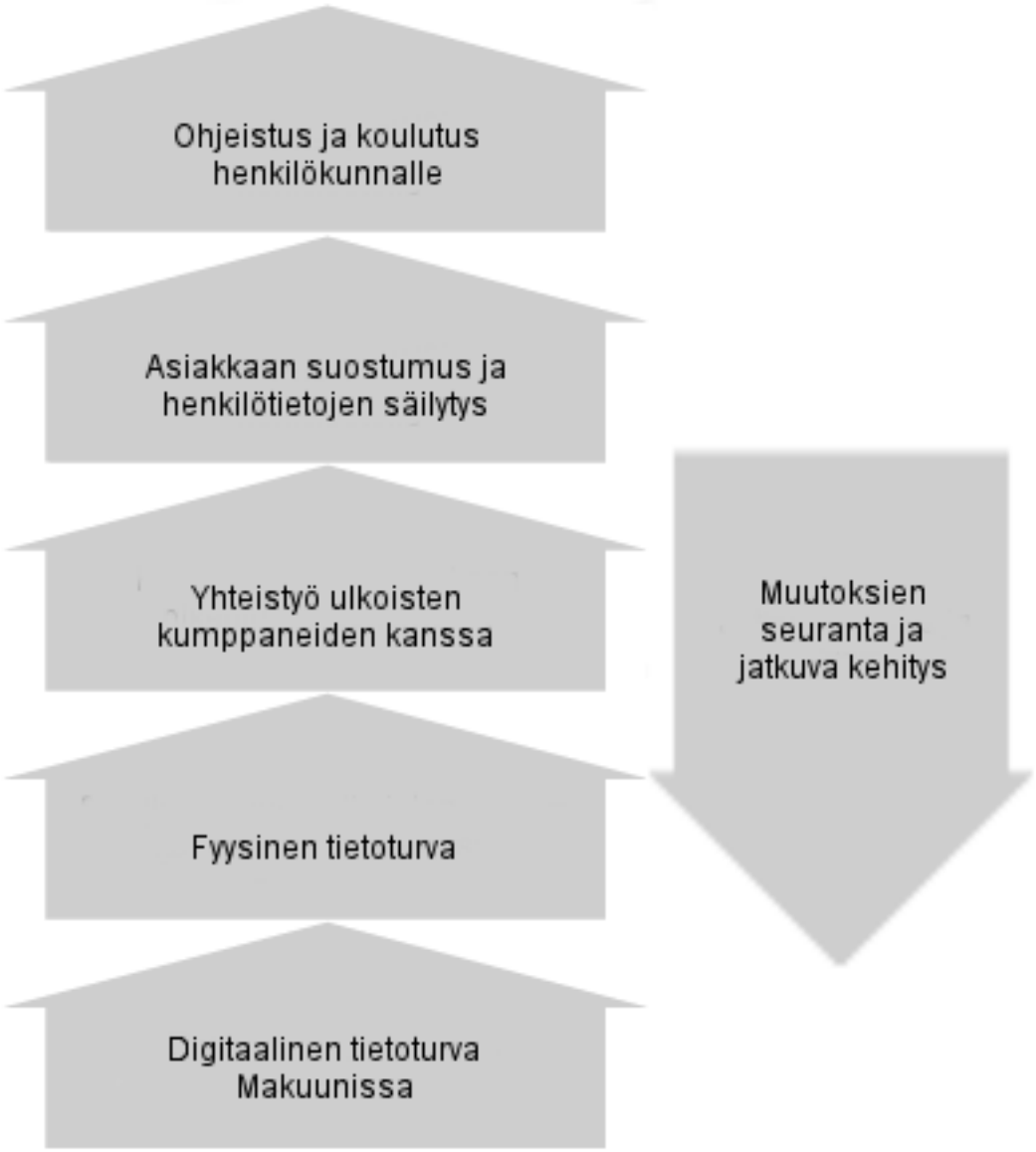
5.2 Tietosuojavastaavan nimitys ja vastuu

Makuunin ydintehtävien toimittaminen vaati henkilötietojen verrattain laajaa käsittelyä, joten ketjulle oli tarpeen nimittää tietosuojavastaava. Makuunin tapauksessa oli luonnollista, että tietosuojavastaava nimitettiin omasta henkilöstöstä. Vaatimukset huomioiden esitin itseäni tietosuojavastaavan tehtävään.

Nimittämisen yhteydessä Makuunin johto antoi tukensa ja resurssit tehtävän hoitamiseen. Oli kuitenkin aika selvää, etteivät tietosuoja-asiat olleet pääosassa yrityksen kamppaillessa selviytymisestään. Samasta syystä tietosuojaa saikin suunnitella ilman painostusta. Päätehtäväksi määriteltiin Makuuni Oy:n valmisteleminen tietosuoja-asetuksen käyttöönottoon.

5.3 Toimenpiteet

Haastatteluilla ja kyselyillä saadulla tiedolla pystyttiin aloittamaan suunnittelu tietosuojan saattamiseksi asetuksen vaatimalle tasolle. Tämä tarkoitti ohjelmistojen päivittämistä tai poistamista, tietoturvakäytäntöjen tarkistusta sekä ohjeistuksen päivittämistä ja henkilöstön koulutusta. Toimintasuunnitelma on esitetty kuvassa 4. Ensimmäisenä keskityttiin digitaalisen ja fyysinen tietoturvan varmistamiseen. Seuraavaksi varmistettiin yhteistyön ulkoisten kumppaneiden kanssa ja jatkettiin henkilötietojen säilytyksen oikeutuksen määrittelyyn ja tarvittavien tietosuojadokumenttien tekemiseen. Lopuksi keskityttiin henkilöstön ohjeistukseen ja koulutukseen. Tietosuojaprojektin on tarkoitus olla jatkuva ja kehittyvä prosessi yrityksessä. Projektin päätteeksi tarkastellaan tuloksia, kehitetään toimintaa ja varmistetaan, että tehdyt toimenpiteet toteutuvat.



Kuva 4. Toimintasuunnitelma Makuuni Oy tietosuojaprojekti

5.3.1 Digitaalinen tietoturva Makuunissa

Makuunin kassajärjestelmä ja toiminnot oli jo aikaisemmin suojattu toteuttamalla suljettu verkko, jossa kaikki arkaluonteinen data liikkui vpn-tunnelia pitkin. Verkko oli toteutettu rautapohjaisella ratkaisulla, johon oli lisäksi pääsy rajatulla käyttäjämäärällä ohjelmistopohjaisella ratkaisulla. Kassajärjestelmän saattaminen tietosuoja-asetuksen vaatimalle tasolle suoritettiin yhdessä järjestelmäntoimittaja Solteq Oy:n kanssa. Siitä kerrotaan lisää luvussa 5.3.3.

Kyselyssä esiin tulleet epämääräiset käyttöjärjestelmät ja laitteet piti saada pois verkosta aiheuttamasta riskiä. Ketjulla oli käytössä F-Securen Protection Service For Business, jonka hallintaportaalin kautta pystyttiin valvomaan kaik-

kia siihen liitettyjä koneita ja niiden ohjelmistojen päivityksiä. Kyselyissä ilmenneet vanhat laitteet joko poistettiin tai liitettiin tähän valvontaan. F-Securen kautta hajanainen konekanta saatiin hallintaan ja etäohjauksella pystyttiin nyt varmistamaan, että kaikissa koneissa oli ajan tasalla olevat käyttöjärjestelmät, ohjelmistot ja palomuuriasetukset.

Yrityksessä otettiin käyttöön salatut sähköpostiviestit. Palvelu ostettiin valmiina nykyiseltä sähköpostitoimittajalta OnlineSolutionsilta, jonka SecMail-suojattu sähköposti mahdollisti arkaluonteisten henkilötietojen lähettämisen turvallisesti. Lisäksi palkkatiedot lähetettiin uudistuksen jälkeen salatusti.

Haastatteluissa oli myös ilmennyt salasanakäytäntöjen heikkenemistä ja saman salasanan käyttöä ja jakamista. Tässä yhteydessä tehtiin myös täydellinen salasanojen uusiminen. Ohjeistuksella ja ohjelmistojen mahdollisuuksia käyttäen velvoitettiin henkilökunta vaihtamaan salasanat yrityksen järjestelmiin. Aluepäälliköt velvoitettiin varmistamaan, että asian vakavuus ymmärrettiin. Lisäksi aina kun mahdollista salasanojen kompleksisuus ja vaihto pakotettiin ohjelmallisesti. Tästä seurasi jatkossakin IT-osastolle lisätöitä, kun uusia vaikeita salasanoja ei aina muistettu, mutta se ei ollut ongelma.

Yksi kompastuskivi oli ketjun vanha extranet-järjestelmä. Aikaisemmin raportointiin, yhteydenpitoon ja tiedottamiseen tarkoitettu järjestelmä oli auttamattomasti aikaansa jäljessä. Extranet oli sidoksissa makuuni.fi sivuston ylläpitoon ja sille oli siitäkin syystä annettu jatkoaikaa ja sitä oli korjattu toimimaan uusimpien selainten versioilla. Tietoturvan nimissä ikiaikainen järjestelmä, jonka toiminnoista suurin osa oli jo siirretty muualle, tuli lopettaa kokonaan. Järjestelmän sisällä oli kuitenkin useiden vuosien raportointi ja lisäksi useampi henkilörekisteri. Osa henkilörekistereistä oli vanhaa tietoa, jota ei ollut tuhottu varmuuden vuoksi tai rahan säästämiseksi. Näitä tietoja olivat vanhat käyttäjätunnukset, asiakkaiden jo lopetetut netticlubitiedot ja sähköpostimarkkinoinnin listat. Nämä tiedot eivät täyttäneet tietosuoja-asetuksen vaatimuksia ja ne poistettiin tietokannoista ja varmistuksista. Tarkoituksena oli tehdä nykyaikainen sosiaalinen intranet korvaamaan vanha extranet. Extranetin alasajo ja uuden nykyaikaisemman rakentaminen ehdittiin aloittaa, mutta konkurssin tullessa kaikki kehitystyö ymmärrettävästi lopetettiin.

Makuunilla ja tytäryhtiö M-Logisticsilla oli käytössä yhteinen tilausjärjestelmä, jossa oli pitkään käytetty yhteisiä tunnuksia tilauksia tehdessä. Nämä tunnukset oli alun perin tehty vastuumyyjän nimellä ja sisälsivät lisäksi hänen sähköpostiosoitteensa. Käyttäjätunnukset siis muodostivat rekisterin. Jatkossa päätettiin tehdä tunnukset liikekohtaisesti käyttäen liikkeen kustannuspaikkaa ja sähköpostiosoitetta, jolloin asetuksen määritelmässä ei henkilötietorekisteriä syntynyt.

Lisäksi ohjeistuksella hoidettiin ohjelmistojen kuten Dropboxin käytössä ilmenneet ongelmat. Henkilötietoja sisältäviä dokumentteja ei jatkossa tallennettu järjestelmiin, joissa data mahdollisesti poistuu EU:n alueelta.

5.3.2 Fyysinen tietoturva

Tarkasteltaessa tietoturvaa tuli muistaa myös fyysisen tietoturvan varmistaminen. Kokonaisvaltaista kartoitusta tehdessä käytiin läpi myös tämä puoli. Tässä yhteydessä varmistettiin, että tiloissa, joissa dataa tai muuta arkaluonteista materiaalia säilytettiin, ei ollut mahdollista liikkua muut kuin työvuorossa olleet henkilökunnan jäsenet. Paperisia arkaluontoisia materiaaleja, kuten vuokraus-lupalappuja ja kirjallisia sähköpostisuoralupia säilytettiin lukkojen takana niiden muodostaessa henkilörekisterin. Henkilötietoa sisältävät paperit menivät pois heitettäessä tietosuojajätteeseen.

Fyysiseen tietoturvaan kuului myös varautuminen tulipaloilta sekä sähkö- ja vesivahingoilta. Lisäksi asetuksen vaatiman datan eheyden varmistamiseksi tehtiin tarkistukset järjestelmien varmistuksesta. Onnettomuuden sattuessa datat olisivat olleet palautettavissa.

Ketjulle oli kertynyt varastoon suuri määrä vanhoja tietokoneita, joko suljetuista liikkeistä tai laiterikkojen johdosta. Käytäntönä oli korvata rikkoutunut laite uudella ja ajaa varmistuksesta tiedot uudelle koneelle. Tietosuojaprojektin aikana poistettiin suuri määrä vanhoja tietokoneita käytöstä sekä varastosta kierrätykseen. Varsinkin kassajärjestelmän koneissa oli kovalevyllä varmistukset henkilörekistereistä, joten varmuuden vuoksi kaikista koneista poistettiin ennen kierrätystä kovalevyt, jotka tuhottiin asianmukaisesti. Ohjeistuksella toimintatavasta tehtiin pysyvä.

5.3.3 Yhteistyö ulkoisten kumppaneiden kanssa

Makuunilla tunnistettiin kolme kumppania, joilla oli mahdollisesti pääsy toimittamiensa järjestelmiin tallennettuihin henkilötietoihin. Näiden kumppaneiden kanssa tehtiin henkilötietojen käsittelysopimukset ja sovittiin yksityiskohtaisesti mitä toimia järjestelmätoimittajilla oli lupa tehdä. Lisäksi yhteisesti ryhdyttiin varmistamaan, että ohjelmistot ja niissä olevat henkilötiedot olivat turvassa ja täyttivät asetuksen vaatimukset.

Lemonsoft ja Sonet toimittivat hyvissä ajoin tarjouksen EU:n tietosuoja-asetuspäivityksestä. Näissä järjestelmissä oli ketjun henkilöstön tiedot työaikaa, palkkaa ja tilauksia varten. Lisäksi henkilötietoja oli verrattain vähän. Järjestelmiin oli pääsy vain muutamalla henkilötietojen käsittelijällä, joten näistä selvittiin kevyellä päivityksellä, sekä muuttamalla ohjeistusta.

Solteqin toimittama kassajärjestelmä otettiin käsittelyyn erityisesti. Kassajärjestelmässä käytettävä henkilörekisteri oli paitsi laaja, sisälsi se myös asiakkaan nimen ja osoitetietojen lisäksi myös henkilötunnuksen. Vuokraustoiminnan luoteen takia oli perustelua kerätä rekisteriä ja myös käyttää henkilöturvatunnusta vahvana tunnestautumisen keinona liikkeissä asioidessa. Solteqin kanssa tutkittiin mahdollisuutta luopua henkilötunnuksen käytöstä järjestelmässä, mutta kustannustehokasta ja järkevää korvaavaa tapaa ei löytynyt. Järjestelmätoimittajaa pyydettiin kertomaan oma näkemyksensä tarvittavista muutoksista kassajärjestelmäohjelmistoon tietosuoja-asetuksen vaatimuksesta. Vaikka vastuu olikin rekisterinpitäjällä, eli Makuunilla, haluttiin yhteistyökumppaneiden kanssa lähteä yhdessä ratkaisemaan asiaa mahdollisimman kustannustehokkaasti ja kattavasti.

Solteqin omassa selvityksessä ja tarjouksessa oli hyvin huomioitu ja kommentoitu asetusta. Tarjous oli perusteellinen ja odotettavasti melko hintava. Tarjouksen pääkohdat olivat kassajärjestelmään tallennettujen henkilötietojen tarkistus, tietojen korjaus, poisto, rajoittaminen tai käytön vastustaminen, oikeus siirtää tiedot järjestelmästä toiseen, tietojen automaattinen poistaminen järjestelmästä halutun aikajakson jälkeen sekä käyttöoikeuksien tarkistus ja tietojen

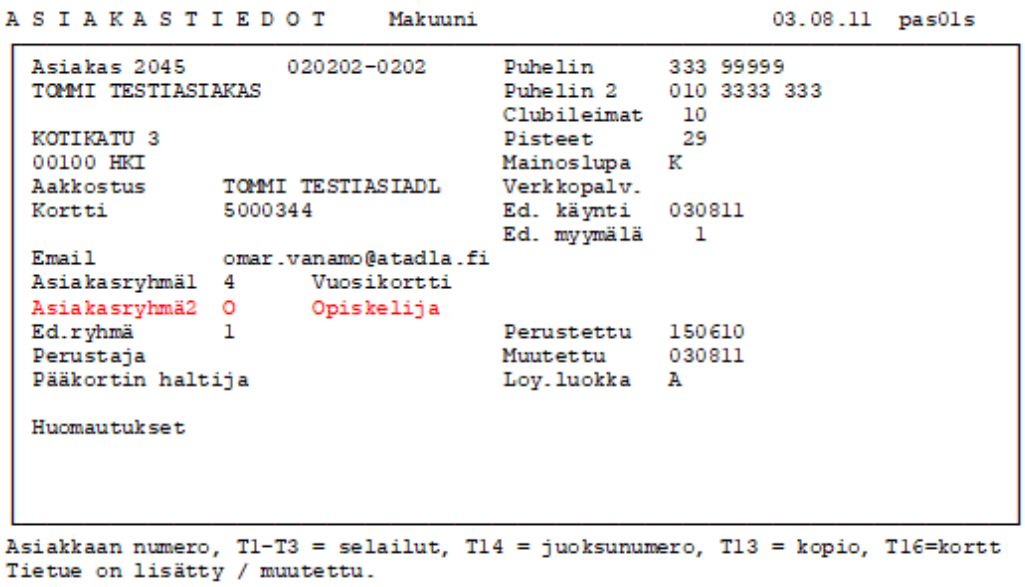
suojaus. Lisäksi tarjouksessa esitettiin uutta lokitusohjelmaa, johon tallentuisivat kaikki henkilökunnan tekemät toimet helposti luettavaan muotoon.

Asiaa tutkittiin ja todettiin, että lukuun ottamatta automaattista ajastettua poistoa ja tietojen suojauksen parantamista, kaikki tarjouksessa olevat kohdat olivat toteutettavissa ohjeistuksella ja toimintatapojen muutoksilla. Lisäksi nykytason suojaus määriteltiin riittäväksi ja suojauksen parantaminen siirrettiin jatkokehityskohteeksi. Rekisteröidyn ja yrityksen kannalta järkeväksi asiakastietojen säilyttämisajaksi määriteltiin kaksi vuotta. Kahden vuoden kuluttua viimeisestä asiakastapahtumasta automaattinen tarkistus varmisti, ettei asiakkaalla ollut yhtään avointa tapahtumaa (esim. palauttamatta jäänyttä vuokraelokuvaa) ja mikäli kaikki oli kunnossa, järjestelmä poisti asiakkaan tiedot Makuunin rekisteristä. Järjestelmässä oli jo olemassa loki ja vaikka sinne tallennettuja tietoja ei ollut helposti saatavilla tai etsittävissä, sen katsottiin täyttävän asetuksen vaatimukset ja sen muutokset jätettiin toteuttamatta.

5.3.4 Asiakkaan suostumus ja henkilötietojen säilytys

Rekisterinpitäjällä, eli tässä tapauksessa Makuunilla tuli olla pätevä oikeutus kerätä, käsitellä ja säilyttää henkilötietoja. Monissa tapauksissa syy olikin helppo perustella, kuten esimerkiksi palkanlaskennan hoitaminen tai käyttäjätunnusten säilyttäminen. Jos kuitenkin lupa käsitellä tietoja vaati asiakkaan suostumuksen, piti rekisterinpitäjän pystyä osoittamaan, että rekisteröity oli suostumuksensa antanut. Makuunin tapauksessa lupaa käsitellä henkilötietoja tuli pyytää, kun asiakas ensimmäisen kerran vuokrasi elokuvan. Samalla kysyttiin myös markkinointilupaa. Suostumus käsitellä henkilötietoja oli välttämätön vuokraussuhteen toteutumiseksi. Markkinointilupia ei tietenkään edellytetty. Mikäli kuitenkin asiakas antoi Makuunille oikeuden markkinoida sähköpostilla ja samalla siis tallentaa henkilötietoja sitä tarkoitusta varten, lupa säilytettiin.

Asiakkaalta kassajärjestelmään kerätyt henkilötiedot on esitetty kuvassa 5. Tärkeimpiä tietoja olivat nimi, henkilöturvatunnus, osoite, puhelinnumero ja sähköpostiosoite. Näiden tietojen lisäksi myös asiakkaan osto- ja vuokraushistoria tallentui kahden vuoden ajalta.



Kuva 5. Makuunin kassajärjestelmään kerätyt henkilötiedot

Erityistä huomiota kiinnitettiin alaikäisen suostumuksiin. Makuunilla tällainen suostumus oli alaikäisen vuokrauslupa. Alle 18-vuotiaat eivät saaneet itse tehdä sopimusta vuokrauksesta, siihen tarvittiin vanhemman tai huoltajan lupa. Tästä säilytettiin kirjallinen lupa ja lisäksi tallennettiin kassajärjestelmään tieto huoltajan toimittamasta luvasta ja missä lupaa säilytettiin.

Mikäli oikeutus annetaan sähköisesti, on hyvä, jos järjestelmäloki tallentaa ajan ja sen, mitä tehtiin järjestelmään mahdollista myöhempää selvitystä varten. Makuunin kassajärjestelmän tapauksessa kaikki tallentuu lokille, joka ei ole tavallisen käyttäjän oikeuksilla kuitenkaan nähtävissä.

Artiklassa 13 mainittavat rekisteröityneille toimitettavat tiedot Makuunissa olivat näkyvillä yrityksen internetsivuilla, sekä ensimmäisen vuokrauksen yhteydessä annettavalla käyttöehdot-lehtisellä. Lehtisessä esiteltiin rekisterinpitäjä ja yhteystiedot, henkilötietojen käsittelyn perusteet ja oikeutus, sekä henkilötietojen säilytysaika. Lisäksi ohjeessa informoitiin rekisteröityä hänen oikeuksistaan henkilötietoihinsa. Nämä tiedot tuli aina olla asiakkaalle nähtävillä myös internetsivuilla ja fyysisesti liikkeissä. Samalla materiaalilla informoitiin myös sähköposti-, ja markkinointiluvasta, sekä niiden peruuttamisesta. Sähköpostimarkkinointi oli tietenkin peruutettavissa jokaisen saadun viestin mukana toimitettavalla linkillä.

5.3.5 Ohjeistus ja koulutus henkilöstölle

Monet tietosuoja-asetuksen vaatimuksista olivat Makuunissa toteutettavissa muuttamalla ohjeistusta ja toimintatapoja. Tämä kuitenkin vaati aikaa, ohjeistusta ja koulutusta toteutuakseen pysyvästi.

Henkilökunnalle kirjoitettiin erillinen uusi ohjeistus koskien tietosuoja-asetuksen velvoitteita Makuuni Oy:ssä. Ohjeistuksessa täsmennettiin rekisteröityneen eli asiakkaan oikeudet ja rekisterinkäsittelijän velvollisuudet. Työntekijöille opastettiin toimintatavat, jotka otettiin jokapäiväiseen käyttöön asiakaskohtaamisissa ja myymälätyöskentelyssä. Ohjeen pääkohdat on esitetty lyhyesti liitteessä 2.

Menettelytapojen ohjeiden lisäksi tehtiin suunnitelma henkilöstön koulutukselle tietosuoja-asetuksen käytännön vaikutuksista Makuunissa. Koulutus toteutettiin verkkoluentona kaikille vastuumyyjille ja toimiston väelle. Vastuumyyjille toimitettiin materiaalit viedä tieto myös kaikille liikkeen myyjille ja vahvistamaan myyjäkohtaisesti, kun koulutus on käyty. Lisäksi jokaiseen ketjutapaamiseen suunniteltiin pidettäväksi tietoturvaosio, jossa käsiteltäisiin myös asetuksen toteutumista Makuunissa. Asiat hyvin perustelemalla voitiin välttää muutosvastarintaa ja toteutetut ohjeistukset tulivat hyvin käyttöön nopealla aikataululla.

Menettelytapojen lisäksi täytettiin seloste käsittelytoimista yrityksen sisäiseen käyttöön. Liitteenä 3 olevassa selosteessa on nähtävissä Makuuni Oy:n henkilörekisterit ja tiedot käsittelystä. Tyhjä versio ja opastusta selosteesta on löydettävissä tietosuojavaltuutetun toimiston nettisivuilta.

5.3.6 Muutoksien seuranta ja jatkuva kehitys

Tietosuojaprojektin valmistuessa Makuunissa pidettiin erityisen tärkeänä, että huomiota kiinnitettiin muutosten tarkkailuun ja varmistukseen, että uudet käytännöt tulivat varmasti voimaan. Muutosvastarinta oli todellinen ongelma pitkään toimineessa yrityksessä ja koska monet tietosuoja-asetuksen osa-alueet toteutettiin muuttamalla toimintatapoja ja ohjeistusta, oli kehitettävä järjestelmä tarkistaa ja varmistaa, ettei vanhoihin toimintatapoihin palattu.

Seurantaa varten perustettiin työryhmä. Työryhmän tuli kartoittaa ja varmistaa uusien käytänteiden toteutumista sekä miettiä jatkokehitystä. Työryhmään valittiin ihmisiä ketjujohdosta, markkinoinnista, IT-puolelta sekä liikkeiden työntekijöistä. Työryhmä velvoitti aluepäälliköt raportoimaan liikkeidensä tilanne työryhmälle kuukausittain. Vastuumyyjien tuli raportoida aluepäällikölle viikoittain. Työryhmän tarkoitus oli myös kehittää tietosuoja-asetukseen ja toimintaan liittyvää ohjeistusta ja koulutusta koko ketjulle.

5.4 Jatkokehitys

Tietosuojaprojekti oli määritelty valmistumaan ennen asetuksen voimaantuloa. Aikataulullisesti tässä onnistuttiin, mutta joitakin osa-alueita oli jätettävä pois tai päätettiin, että niihin voidaan palata myöhemmin. Näitä olivat mm. asiakkaan mahdollisuus itse päivittää, poistaa tai rajoittaa henkilötietojaan, verkkoliikenteen tarkempi tarkkailu ja tietosuoja-asetukseen liittyvät erilaiset sertifikaatit ja merkit.

Kassajärjestelmän laaja henkilörekisteri pysyi ajan tasalla vain silloin, kun asiakas kävi asioimassa liikkeessä. Muutot, sukunimen vaihtaminen tai vastaava ei tietenkään päivittynyt suljettuun järjestelmään. Järjestelmän toimittaja Solteq tarjosi mahdollisuutta ottaa käyttöön vahvaa tunnistautumista käyttävä portaali, jossa asiakas voisi tarkistaa omat tietonsa ja päivittää muutoksista. Samalla asiakas olisi voinut myös tarkistaa ostohistoriaa ja kertyneitä etuja. Vaikka idea oli hyvä, tätä ei nähty kiireellisenä toimena vaan projektin puitteissa hoidettiin henkilötietojen poisto, päivittäminen ja rajoittaminen ohjeistuksella.

Aikataulu ja projektin kustannukset eivät sallineet tehdä laajempaa selvitystä verkon valvonnasta ja datan suojauksen parantamisesta. Suljetussa vpn-verkossa liikkuva data katsottiin riittäväksi suojaukseksi. Makuunissa haluttiin kuitenkin jatkossa varmistaa arkaluontoisen tiedon suojaus ja siihen suunniteltiin verkonvalvonnan käyttöönottoa. Verkonvalvonnalla oli tarkoitus tarkkailla ja pysäyttää siirto, mikäli datassa liikkui esimerkiksi useampia suojaamattomia henkilöturvatunnuksia.

Yksi selvä jatkokehityskohde oli asetukseen liittyvät sertifikaatit, sinetit ja merkit. Näillä olisi pystytty helposti osittamaan, että asetusta noudatettiin ja saamaan lisäkoulutusta sekä opastusta alan ammattilaisilta.

6 POHDINTA

Opinnäytetyön tavoitteena oli tutkia ja toteuttaa Makuuni Oy:n tietosuojakartoitus ja varmistaa yrityksen järjestelmien tietoturvallisuus ja henkilöstön osaaminen EU:n tietosuoja-asetuksen tullessa voimaan. EU:n tietosuoja-asetus vaatii pieniltä ja keskisuurilta yrityksiltä monesti liikevaihtoon nähden suuria resursseja. Kalliin projektin lopputuloksena ei luultavasti pystytä kasvattamaan liikevaihtoa, mutta kattavalla tietoturvakartoituksella saadaan kuitenkin varmistettua, että yrityksen tietoturva-asiat ovat hoidossa tai ainakin, että riskit tiedostetaan asianmukaisella tavalla.

Tässä työssä on keskitytty tietosuoja-asetukseen EU:n alueella toimivan yrityksen näkökulmasta. Mikäli yritys toimii EU:n ulkopuolella tai ulkopuolelle, tulee se ottaa huomioon valmistelussa. Tämä työ on tehty Makuuni Oy:lle ja vaikka onkin sovellettavissa muihinkin yrityksiin, suosittelen harkitsemaan tarkasti oman tietosuojasuunnitelman läpikäymistä alan lakimiehen kanssa. Asetuksessa on tulkinnanvaraisia kohtia, mutta tarvittaessa apua ja ohjeistusta saa tietosuojavaltuutetun toimistolta. Asetuksen tulkinnanvaraisuus on luonut myös erilaisille konsulttiyrityksille mahdollisuuden myydä osaamistaan asetuksen tulkinnan ja tietosuojaprojektien muodossa.

EU:n tietosuoja-asetus vaikuttaa isolta, hankalalta, lakitermejä tihkuvalta järkäleeltä. Varsinkin pienten yritysten ja yhteisöjen kannalta katsottuna se vaikuttaa työläältä. Asetuksesta on median avustuksella tehty pelottavampi kuin se on. EU:n normaalikansalainen ei välttämättä tiedä asetuksesta muuta kuin, että nettisivuilla pitää nykyään aluksi hyväksyä jotain ja yritysten edustajat pelkäävät kasvavia kustannuksia ja isoja sakkoja. Tosiasiassa on kuitenkin huomattava, että yhdellä laajalla asetuksella saatiin katettua kaikki EU:n alueen yritykset ja kansalaiset saman lainsäädännön alle ja ohjataan näitä yrityksiä miettimään toimintaansa ja päivittämään käytäntöjään sekä ohjelmistojaan. Yksityisen kuluttajan oikeudet ja suoja paranivat asetuksen myötä huomattavasti. Monet asetuksen vaatimukset on toteutettavissa jo pelkällä ohjeistuksel-

la ja eivät vaadi isoja rahallisia satsauksia. On kuitenkin tärkeää tehdä tarvittavat muutokset ja dokumentoida tekeminen mahdollisimman tarkasti. Mielestäni yritysten ja yhteisöjen kannattaa aloittaa tutkimalla tarkasti mitä tietoja organisaatiossa kerätään ja millä oikeutuksella niitä säilytetään henkilörekistereissä. Listaamalla organisaation henkilörekisterit ja oikeudet tietojen keräämiselle ja säilyttämiselle, saadaan hyvä aloitus tietosuojan varmistukselle.

Mielestäni siirtymäaika asetuksen voimaantulossa olisi saanut olla pidempi ja asetuksessa olisi voitu siirtymäajan aikana jo enemmän puuttua uusien järjestelmien suunnittelun ohjaamiseen. Makuunin tietosuojaprojektille haasteita aiheutti yrityksen taistelu olemassaolostaan. Vaikka projektilla oli johdon tuki, oli rahoituksen varmistaminen ja työn priorisointi oli haasteellista, kun keskityttiin yrityksen pelastamiseen. Haastavasta tilanteesta huolimatta projekti saatiin toteutettua ja henkilörekisterit sekä niiden käyttö saatettiin asetuksen vaatimalle tasolle.

LÄHTEET

Aarnio, R. 2015. Mitä tietosuoja tarkoittaa? PDF-dokumentti. Saatavissa: https://koulutus.fcg.fi/ [viitattu 12.2.2020].

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. PDF-dokumentti. Päivitetty 4.5.2016. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI [viitattu 13.5.2020].

ITGP Privacy Team. 2017. EU Genaral Data Protection Regulation (GDPR). 2. painos. United Kingdom: IT Governance Ltd.

LastPass by LogMeIn. 2018. Psychology of Passwords: Neglect is Helping Hackers Win. PDF-dokumentti. Saatavissa: https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/logmein-lastpass-survey-ebook-v8.pdf [viitattu 13.5.2020].

Niemelä, A. 2018. Datan maailma. Kauppapolitiikka. Verkkolehti. Päivitetty 4.12.2018. Saatavissa: https://kauppapolitiikka.fi/datan-maailma [viitattu 13.5.2020].

Minilex Oy. s.a. Käytännesäännöt. WWW-dokumentti. Saatavissa: https://www.minilex.fi/a/käytännesäännöt [viitattu 13.5.2020].

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. 4. painos. Helsinki: Sanoma Pro Oy.

Pyyhtiä, T. 2019. Digiajan johtajan käsikirja. Helsinki: BoD – Books on Demand.

Suomen tietosuojapalvelut. 2020. OpiTietosuojaa. WWW-dokumentti. Saatavissa: www.opitietosuojaa.fi [viitattu 13.5.2020].

Tietosuojatyöryhmä. 2016. Tietosuojavastaavia koskevat ohjeet. Pdf. Päivitetty 5.4.2017. Saatavissa: https://tietosuoja.fi/documents/6927448 [viitattu 19.4.2020].

Tietosuojatyöryhmä. 2017. Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu "korkea riski" 4. PDF-dokumentti. Päivitetty 5.10.2017. Saatavissa: https://tietosuoja.fi/documents/6927448/8316711/Vaikutustenarviointi+fi.pdf/af51e999-5326-4223-9deb-e21bdd2e0a63/Vaikutustenarviointi+fi.pdf [viitattu 19.4.2020].

Tietosuojavaltuutetun toimisto. 2018. Tietosuoja-asetus ei edellytä entisen kaltaista rekisteri- tai tietosuojaselostetta. Blogi. Päivitetty 3.5.2018. Saatavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuoja-asetus-ei-edellyta-entisen-kaltaista-rekisteri-tai-tietosuojaselostetta [viitattu 13.5.2020].

United Nations. 1948. Universal Declaration of Human Rights General Assembly resolution 217 A. pdf. Saatavissa:

https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217(III) [viitattu 13.5.2020].

Viljanen, V. s.a. Lainsäädäntö. WWW-dokumentti. Saatavissa: https://yksityisyydensuoja.fi/lainsäädäntö [viitattu 13.5.2020].

Liite 1.

KUVALUETTELO

Liite 2.

TAULUKKOLUETTELO

Liite 3.

Kyselylomake

MAKUUNI

Ohjelmisto ja tietosuojakysely

* Required

Kustannuspaikkanumero KPN *

Your answer

Liikkeen nimi

Your answer

Tietokone1: *

Merkitse myös maksupäätteen pohjasta HW/ID koodi ja kuittarin malli.

Your answer

Muut tietokoneet oheislaitteineen. Merkitse merkki ja mallkinumerot mahdollismman tarkkaan. *

Your answer

Muut laitteet.Merkitse merkki ja mallkinumerot mahdollismman tarkkaan. *

Your answer

Käytössä olevat ohjelmistot. Windows koneilla käytössä olevat/asennetut ohjelmistot

Your answer

Säilytetyt henkilötiedot. Merkitse tähän kaikki digitaaliset tai paperiset henkilötietoja sisältävät asiakirjat tai ohjelmat.

Your answer

Liite 4.

Pääkohdat liikkeiden tietosuoja-asetuksen ohjeistuksesta

Sähköpostin käyttö

Makuuni.fi-päättyiset sähköpostit lähetetään ja vastaanotetaan suojatusti, mutta vain silloin kun molemmat osoitteet ovat makuuni.fi päättyviä. Jos on tarve lähettää henkilötietoja sisältävä sähköposti ulkopuoliseen osoitteeseen, se lähetetään ensin toimistolle, josta viesti välitetään turvatusti eteenpäin. Erityisesti tämä koskee sähköposteja joissa esiintyy Henkilöturvatunnuksia.

Muut henkilötietolistat

Jatkossa pyritään välttämään tallentamasta mitään sähköisiä listoja, jotka sisältävät henkilötietoja.

Huomatkaa, että jos teillä on työvuorolistoja ym. niin niitä voi säilyttää. Kunhan kerätyllä listalla on ajankohtainen käyttötarkoitus. Pitäkää vain huoli, että listat ovat turvallisesti säilytetty ja ette lähetä niitä avoimen netin ylitse.

Henkilötiedoiksi lasketaan tiedot, joilla joku tietty ihminen voidaan yksilöidä, ja tällaisia ovat esimerkiksi nimet, osoitteet, terveystiedot tai sähköpostiosoitteet.

Asiakkaan oikeus omiin tietoihinsa

Mikäli asiakas haluaa tietonsa poistettavan tai haluaa rajoittaa niiden käyttöä Makuuni Oy:n järjestelmissä niin ilmoittakaa siitä välittömästi osoitteeseen makuuni@makuuni.fi.

Toimistolla tarkastetaan, ettei asiakkaalla ole keskeneräisiä tapahtumia ja tiedot poistetaan sekä asiakkaalle ilmoitetaan toimista.

Asiakkaan tietoja voi päivittää entiseen tapaan esim. asiakkaan osoitteen muuttuessa itse kassajärjestelmässä.

Kassajärjestelmä ja säilytettävät tiedot

Uusi tietosuoja-asetus kieltää henkilötietojen käytön ja säilytyksen, mikäli tiedoille ei ole tarvetta. Tätä silmällä pitäen kassajärjestelmästä poistetaan vanhoja asiakastietoja. Vanhat vuokraustiedot ovat poistettu automaattisesti kuten ennenkin, mutta jatkossa koko asiakastieto poistetaan, mikäli asiakas ei ole asioinut liikkeessä 2 vuoteen ja hänellä ei ole keskeneräisiä tapahtumia tiedoissaan.

kassajärjestelmään on lisäksi tehty muutoksia taustajärjestelmiin, jotka tallentavat järjestelmän käyttöä ja seuraavat mitä tietoja liikkeissä käytetään.

Liite 5.

Makuuni Oy seloste käsittelytoimista

Nimi ja yhteystiedot		Tietosuojavastaava (jos nimitetty)		Edustaja (jos tarpeen)	
Organisaation nimi	Makuuni Oy	**Nimi**	Jussi Linnala	**Nimi**	
Osoite	Porrassalmenkatu 1 C, 50100 Mikkeli	**Osoite**	Porrassalmenkatu 1 C, 50100 Mikkeli	**Osoite**	
Sähköposti	makuuni@makuuni.fi	**Sähköposti**	jussi.linnala@makuuni.fi	**Sähköposti**	
Puhelinnumero	040552317	**Puhelinnumero**	0400373329	**Puhelinnumero**	

Seloste käsittelytoimista					
Tehtävä, johon tietoja käsitellään	**Käsittelyn tarkoitus**	**Rekisteröityjen ryhmät**	**Henkilötietojen ryhmät**	**henkilötietojen käsittelyä koskeva sopimus**	**Tietojen säilytysajat, tai sen määrittämisen kriteerit**
Profix kassajärjestelmä	Vuokraustoiminta ja makuuni-clubi	Makuuni Oy:n rekisteröityneet asiakkaat	Henkilötunnus, nimi, osoite, sähköposti, puhelinnumero	Solteq käsittelysopimus	Poisto automaattisesti 2 vuotta viimeisen tapahtuman jälkeen.
sonet palkkaohjelmisto	Palkkahallinnon hoito	Makuuni Oy:n henkilöstö	Henkilötunnus, nimi, osoite, sähköposti, puhelinnumero	Sonet käsittelysopimus	Palkkatietojen säilytys 10 vuotta
työajanseuranta / työvuorolistat	Henkilöstön työvuorojen esitys ja seuranta	Makuuni Oy:n henkilöstö	Nimi, Sähköposti		Palkkatietojen säilytys 10 vuotta
markkinointisähköpostisuorat	Asiakkaiden tieotus, mainostus asiakkaan suostumuksella	Makuuni Oy:n rekisteröityneet asiakkaat	Nimi, puhelinnumero, postinumero, sähköpostiosoite, sukupuoli		Poistuu automaattisesti, mikäli sähköpostiosoite ei ota viestejä vastaan tai asiakkaan pyynnöstä
intranet	Henkilökunnan tiedotus, raportointi	Makuuni Oy:n henkilöstö	Nimi, sähköposti, puhelinnumero, IP-osoite		Työsuhteen päättyessä
Alaikäisen vuokrauslupalaput	Varmistaa alaikäisen lupa vuokrata elokuvia Makuunista	Makuuni Oy:n rekisteröityneet alaikäiset asiakkaat	Henkilötunnus, nimi, osoite, sähköposti, puhelinnumero		Asiakkaan tullessa täysi-ikäiseksi