LUT
Lappeenranta
University of Technology

LUT School of Business and Management

Kauppatieteiden kandidaatintutkielma

Talousjohtaminen

Euroopan unionin tietosuoja-asetuksen vaikutukset pankkialaan Suomessa

The effects of General Data Protection Regulation on Finnish banking sector

15.4.2017

Tekijä: Jake Ahokas

Ohjaaja: Timo Leivo

TIIVISTELMÄ

Tekijä:	Jake Ahokas
Tutkielman nimi:	Euroopan unionin tietosuoja-asetuksen vaikutukset pankkialaan Suomessa
Akateeminen yksikkö:	School of Business and Management
Koulutusohjelma:	Kauppatiede / Talousjohtaminen
Ohjaaja:	Timo Leivo
Hakusanat:	EU, tietosuoja, tietoturva, pankkitoiminta, tietosuoja-asetus

Tämä kandidaatintutkielma on toteutettu laadullisena tutkimuksena ja sen tarkoituksena on tutkia Euroopan unionin toukokuussa 2018 voimaan astuvaa tietosuoja-asetusta ja sen vaikutuksia suomalaiseen pankkitoimintaan. Tutkielmassa keskitytään tietosuoja-asetukseen erityisesti henkilötietojen käsittelyn näkökulmasta. Tutkimuskysymyksiin pyritään vastaamaan tarkastelemalla muutoksia henkilöstön, asiakkaan ja järjestelmien näkökulmista. Tutkimuksen empiriaosuus toteutettiin teemahaastatteluna.

Tietosuoja-asetus tulee vaikuttamaan merkittävästi jokaiseen yritykseen, jonka liiketoiminta edellyttää henkilötietojen käsittelyä. Asetus tuo kuluttajalle lisää oikeuksia hänestä kerättyjä henkilötietoja kohtaan ja samalla se lisää rekisterinpitäjän vastuuta näitä tietoja kerätessä ja käsiteltäessä. Rekisterinpitäjän vastuulle jää yrityksen henkilöstön kouluttaminen ja järjestelmien päivittäminen sellaisiksi, että asetuksen vaatimukset tulevat täytetyiksi. Merkittävimmät muutokset koskevat henkilöstöä ja järjestelmiä. Henkilöstön osaamisesta varmistuakseen yrityksen tulee sekä käyttää paljon resursseja tietosuojakoulutuksiin että valvoa tietosuojaosaamisen tasoa yleisesti. IT-järjestelmien suunnittelussa tulee ottaa huomioon vaatimus oletusarvoisesta ja sisäänrakennetusta tietosuojasta, joka edellyttää jatkuvaa kouluttamista ja tietoisuuden lisäämistä. Toiminnan läpinäkyvyyden lisäämiseksi asiakas on osallistettu palveluiden suunnitteluun.

ABSTRACT

Author: Jake Ahokas

Title: The effects of General Data Protection Regulation on Finnish banking sector

School: School of Business and Management

Degree programme: Business administration / Financial Management

Supervisor: Timo Leivo

Keywords: EU, data protection, information security, banking sector, general data protection regulation

This bachelor's thesis has been carried out using a qualitative research and its purpose is to study the European union's general data protection regulation, that comes into effect on May 2018, and how it affects the banking sector in Finland. The study focuses on the regulation especially from the aspect of handling personal data. The answer to the study question "how will the European union's new general data protection regulation affect the banking sector in Finland" was approached by observing the changes from the personnel's, the client's and the systems' point of view. The empirical part of the study was carried out using a theme interview.

The new regulation will significantly affect every business that has to deal with handling personal data. The rights of the consumer will improve while the organizations that collect personal data will face a rise in the responsibilities concerning this information. Organizations must ensure that their personnel are trained and that their systems are updated in a way that complies with new requirements.

The most significant changes concern the personnel and the systems used. Organizations must allocate resources to data protection training and monitor the general level of data protection know-how in the organization in order to make sure that every single employee complies with the new regulation. The major change in systems is that planning IT systems requires that privacy is applied by default and by design which therefore requires continuous training and raising awareness. In order to enhance the transparency in actions the organization has involved the client in planning their services.

Sisällysluettelo

1 Johdanto 1
1.1 Tutkimuksen tavoitteet ja tutkimusongelmat 2
1.2 Tutkimuksen rajaukset ja teoreettinen viitekehys 2
1.3 Käsitteet 4
1.3.1 Tietosuoja 4
1.3.2 Tietoturva 5
1.3.3 Asiakaskokemus 5
1.3.4 Tietojärjestelmät 6
1.4 Tutkimusmenetelmät ja työn rakenne 6
2 Tietosuoja lainsäädännön kannalta 8
2.1 Tietosuoja suomalaisessa liiketoiminnassa 8
2.2 Euroopan unionin keskeiset tietosuojakäytännöt 9
3 Euroopan unionin uusi tietosuoja-asetus (GDPR) 11
3.1 Uuden tietosuoja-asetuksen keskeisimmät teemat 11
3.1.1 Avaintekijät henkilötietojen käsittelyssä 13
3.2 Henkilötietojen käsittelyn kannalta keskeiset kohdat 15
3.3 Tietosuoja-asetuksen hyödyt rekisterinpitäjälle 18
3.4 Aikaisemmat tutkimukset 20
4 Pankkialan tietosuoja 23
4.1 Tietojen merkitys pankkitoiminnassa 23
5 Tietosuoja-asetuksen vaikutukset pankkialaan 26
5.1 Valmistautuminen tietosuoja-asetukseen 26
5.2 Vaikutukset henkilöstön ja asiakkaan näkökulmasta 27
5.3 Haasteet valmistautumisprosessissa 29
6 Yhteenveto ja johtopäätökset 30
Lähdeluettelo 33

LIITTEET

Liite 1. Haastattelukysymykset

1 Johdanto

Tämä kandidaatintutkielma keskittyy tarkastelemaan Euroopan Unionin uutta tietosuoja-asetusta, jota lähes jokaisen yrityksen tulee noudattaa 25.5.2018 alkaen. Asetus hyväksyttiin Euroopan Parlamentissa jo 14.4.2016 (GDPR Portal 2018), joten niillä yrityksillä, joita se koskettaa, on ollut aikaa valmistautua asetuksen vaatimuksiin. Työssä tutkitaan erityisesti sitä, miten tämä tietosuoja-asetus tulee vaikuttamaan pankkialaan Suomessa. EU:n tietosuoja-asetusta tulee soveltaa lähes poikkeuksetta kaikessa henkilötietojen käsittelyssä, jonka kohteena ovat Euroopan unionin kansalaiset, joten sen vaikutukset tulevat koskettamaan monia (EU:n tietosuojauudistus 2017). Vaikka henkilötietojen suojaamiseksi on säädetty kansallisia lakeja (Henkilötietolaki 1998), on tämä uusi asetus kaikkia koskettava ja osaltaan yhdistävä tekijä Euroopan Unioniin kuuluvien maiden välillä.

Tutkielman aihe on erittäin mielenkiintoinen sen takia, että se tulee koskettamaan niin monia tahoja, ja koska asetusta on alettava soveltamaan jo reilun kuukauden kuluttua, on aihe myös ajankohtainen. Jokaisella yrityksellä on asiakkaita, henkilöstöä ja yhteistyökumppaneita, joten henkilötietoja käsitellään lähes poikkeuksetta jokaisessa yrityksessä. Pankkialan yritykset, eli pankit, ovat myös usein suuria, joten niillä on paljon niin henkilöstöä kuin asiakkaitakin; Suomesta voi olla melko vaikea löytää henkilöä, jolla ei olisi pankkitiliä tai esimerkiksi luottokorttia.

Tämä tutkielma toteutetaan laadullisena tutkimuksena, ja tutkimusstrategiana käytetään tapaustutkimusta. Tutkimusmetodina hyödynnetään teemahaastattelua. Syrjälän mukaan tapaustutkimukselle ominaista on se, että sen avulla pyritään ymmärtämään jotakin tutkittavaa ilmiötä syvällisemmin (Syrjälä 1994, 11-12). Tapaustutkimus sopii tähän työhön hyvin senkin takia, että sen avulla saadut tulokset voidaan esittää sellaisella kielellä, että se voidaan ymmärtää tuntematta asiaa sen tarkemmin (Cohen & Manion 1995, 123). Tutkimusmenetelmänä käytetään teemahaastattelua, jossa tutkija esittää aiheeseen vahvasti liittyviä kysymyksiä, ja se on tässä työssä suotuisa menetelmä, sillä sen avulla pystytään selvittämään tehokkaasti asioita, joista ei tiedetä ennalta paljon (Metsämuuronen 2005, 226).

Kysymykset tullaan laatimaan etukäteen, mutta valmiita vastausvaihtoehtoja ei ole, joten haastateltava saa vastata kysymyksiin laajemmin ja perusteellisemmin. Teemat

jaotellaan niin, että ne liittyvät olennaisesti tutkimuksen pää- ja alaongelmiin.

1.1 Tutkimuksen tavoitteet ja tutkimusongelmat

Tämän tutkielman tavoitteena on esittää EU:n uuden tietosuoja-asetuksen konkreettiset vaikutukset pankkialaa kohtaan Suomessa ja myös avata sitä, miten tähän on valmistauduttu/valmistaudutaan. Tutkielman pääongelmaksi muodostui:

Miten Euroopan Unionin uusi tietosuoja-asetus tulee vaikuttamaan pankkialaan Suomessa?

Tutkielman alaongelmat valittiin sellaisiksi, että ne vaikuttavat suoraan pääongelmaan:

Minkälaisia järjestelmiä hyödynnetään, jotta tietosuoja-asetuksen asettamiin vaatimuksiin pystytään vastaamaan?

Millä tavalla tietosuoja-asetuksen aiheuttamat muutokset tulevat näkymään asiakkaille?

Miten yritysten henkilökunta perehdytetään tietosuoja-asetuksen aiheuttamiin muutoksiin?

Kaikki alaongelmat liittyvät suoraan siihen, miten tuleva tietosuoja-asetus vaikuttaa niin yrityksen henkilö- kuin asiakaskuntaankin. Ensimmäinen alaongelma auttaa selventämään, miten yritysten järjestelmät mukautuvat vastaamaan tuleviin vaatimuksiin. Toisen alaongelman avulla pyritään selvittämään näkyvätkö uuden asetuksen vaikutukset suoraan asiakkaille, ja jos kyllä, niin millä tavoin. Kolmas, ja viimeinen, alaongelma taas liittyy siihen, miten henkilökunta pystyy omalla toiminnallaan edesauttamaan asetuksen läpiviemistä ja soveltamista työssään.

1.2 Tutkimuksen rajaukset ja teoreettinen viitekehys

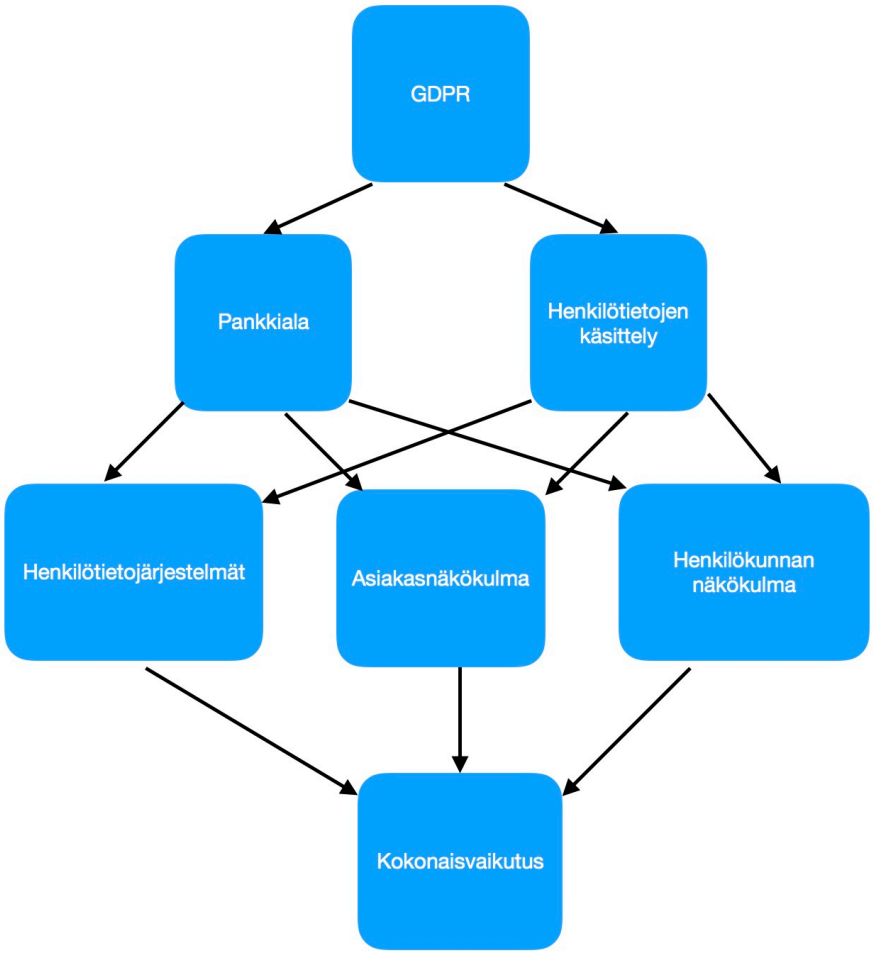
Tämä tutkimus on rajattu ensinnäkin pelkästään Suomen pankkialaa koskevaksi, koska tuleva asetus käsittää koko Euroopan Unionin, niin sen vaikutusten tarkastelu jokaisen EU-maan jokaista henkilötietoja käsittelevää tahoa kohtaan olisi tämänhetkisten tietojen puitteissa liki mahdotonta, ja toiseksi se tekisi tutkimuksesta

myös erittäin laajan. Rajauksesta huolimatta tutkimuksen tuloksia voi olla mahdollista soveltaa myös muihin EU-maihin, sillä tietosuoja-asetusta tulee soveltaa yhtä lailla jokaisessa maassa.

Pankkiala valikoitui siksi, koska pankkien toimintatavat ovat jokaisella toimijalla melko samanlaisia. Myös sen takia, että pankkien hallussa olevat tiedot henkilöistä ovat todella arkaluontoisia, ja joku epärehellinen taho voisi käyttää niitä häikäilemättä hyväkseen. Pankkien henkilötiedoista löytyvät ainakin sosiaaliturvatunnukset, osoitteet, henkilöiden tilitiedot ja usein myös lainatiedot (Pankkitoiminta 2017). On siis erittäin tärkeää niin asiakkaiden luottamuksen kuin liiketoiminnan tehokkaan toteuttamisenkin puolesta, että pankit pystyvät hallinnoimaan ja käsittelemään näitä tietoja sillä tavalla, että ne eivät joudu vääriin käsiin.

Seuraavalla sivulla esitetään tutkielman teoreettinen viitekehys (kuvio 1), joka kuvaa sitä, millä tavalla tietosuoja-asetuksen kokonaisvaikutus pankkialaan muodostuu eri tekijöiden kautta. Tähän olisi mahdollista lisätä muitakin näkökulmia ja tekijöitä, mutta tutkimuksen rajauksen kannalta viitekehys esittää niistä tutkittavaa ilmiötä kohtaan olennaisimmat.

Viitekehyksen ylimmällä tasolla on General Data Protection Regulation (GDPR) eli tietosuoja-asetus. Seuraavalla tasolla asetuksen vaikutukset tuodaan esille niin henkilötietojen käsittelyssä kuin pankkialan ominaisuuksienkin osalta. Toiseksi alimmalla tasolla tuodaan vaikutukset ilmi eri näkökulmista, jotka ovat järjestelmien, asiakkaan ja henkilöstön näkökulma. Lopussa nämä kaikki kiteytyvät yhteen tietosuoja-asetuksen kokonaisvaikutuksiin, joiden selvittäminen on tämän kandidaatintutkielman tarkoitus.



Kuva 1. Tutkielman teoreettinen viitekehys

1.3 Käsitteet

Tutkielma käsittelee pääsääntöisesti uutta tietosuoja-asetusta ja tietoturvaa yleisesti, ja vaikka se kohdistetaankin pankkialaan, tarkastellaan tietosuojan ja –turvan käsitettä hieman tarkemmin. Alatutkimusongelmat kohdistuvat asiakaskokemukseen ja henkilötietojärjestelmiin, mistä johtuen myös näiden ominaisuuksia tutkitaan. Tutkielmassa käytettäviä käsitteitä tarkastellaan tässä nimenomaan pankkialan näkökulmasta, jotta teoria kohdistuisi tutkimuksen kannalta olennaisimpiin seikkoihin.

1.3.1 Tietosuoja

Tietosuojan tärkeimmäksi tehtäväksi, henkilötietojen käsittelystä puhuttaessa, voidaan katsoa se, että henkilön perusoikeudet säilyvät aina tiedon saamisesta sen hävittämiseen asti. Se liittyy myös henkilön yksityisyyteen, sillä yksilöllä tulee olla mahdollisuus varmistua siitä, että käsiteltävät tiedot ovat paikkansa pitäviä ja

tarkoituksenmukaisia käyttävän tahon osalta. (Tietosuoja 2017)

Andreasson, Koivisto & Ylipartanen (2017) toteavat, että tietojen suojaaminen itsessään ei niinkään ole tietosuojan tehtävä, vaan pikemminkin rekisterinpitäjien ohjaaminen hyvien tietojenkäsittelykäytäntöjen noudattamiseen samalla turvaten muun muassa henkilön oikeuksia. Aikaisemmin tietosuojasääntely on perustunut käytännössä henkilötietolakiin ja Suomen perustuslakiin (Suomen perustuslaki 1999), mutta uuden tietosuoja-asetuksen myötä tietosuojakäytännöt päivittyvät paremmin maailman nykytilaa vastaavaksi.

1.3.2 Tietoturva

Tietoturvalla tai –turvallisuudella viitataan niihin keinoihin ja järjestelmiin, joiden tarkoitus on estää luottamuksellisten tai yksityisten sähköisten tietojen vuotaminen sellaisten tahojen käsiin, jotka eivät laillisesti ole oikeutettuja käsittelemään niitä (von Solms & von Solms 2008). Liiketoiminnassa nykypäivänä on tärkeää, että yritysten tulee turvata asiakkaidensa ja henkilöstönsä tietoja, mutta heidän on kyettävä tekemään näin ilman, että se haittaa heidän omaa liiketoimintaansa (Johnson 2018). Yritysten käyttämien sähköisten järjestelmien käyttö on yleistynyt viime vuosina; esimerkiksi asiakastiedon hallintaan tarkoitettujen ohjelmistojen, eli CRM-ohjelmistojen, käyttö on lisääntynyt viimeisen viiden vuoden aikana suomalaisissa yrityksissä (Tilastokeskus 2017; Tilastokeskus 2012). Organisaatiot eivät pysty hyödyntämään digitalisaation tuomia mahdollisuuksia kokonaisvaltaisesti, jos niiden tietoturva ei ole riittävällä tasolla. Organisaatiot ovat myös huomanneet tämän, mistä kertoo se, että monet suuret organisaatiot ovat ottaneet kyberturvallisuuden asiantuntijoita jopa yhtiöiden korkeimpaan johtoryhmään. (Andreasson et al. 2017)

1.3.3 Asiakaskokemus

Asiakaskokemus voidaan nähdä kaikkena toimintana yrityksen ja asiakkaan välillä; aina markkinoinnista ja palvelutoiminnasta ostopäätöksen tekoon asti. Asiakaskokemus nähdään kuitenkin vielä tänä päivänäkin ainoastaan kaupantekohetkenä sen sijaan, että huomioitaisiin myös sitä edeltävät ja sen jälkeen tapahtuvat vaiheet. (Meyer & Schwager 2007) Tänä päivänä asiakaskokemus voidaan

kuitenkin käsittää laajempana toimintona, sillä siinä tulisi onnistua myös esimerkiksi verkkopalveluissa ja sosiaalisessa mediassa, pelkän fyysisen asiakaskontaktin lisäksi. Shaw, Dibeehi & Walden (2010) esittävätkin, että asiakkaat odottavat saman kaltaista vuorovaikutusta sosiaalisessa mediassa kuin jos he oikeasti tapaisivat; asiakkaat vertaavat näitä kokemuksia keskenään. Asiakaskokemus pankin tietosuojan näkökulmasta voidaan tulkita niin, että asiakas otaksuu hänen tietojensa hankinnan, käsittelyn ja lopulta niiden hävittämisen sekä hyvänä palveluna että luottamuksen osoituksena, ja niin koko tietojenkäsittelyn elinkaari on osana muodostuvaa asiakaskokemusta.

1.3.4 Tietojärjestelmät

Tietojärjestelmien tehtävänä on kerätä, käsitellä, säilyttää ja jakaa tietoa sitä hallinnoivan tahon toiveiden ja tavoitteiden mukaisesti. Tänä päivänä suurin osa tietojärjestelmistä toimii tietokoneperusteisesti, vaikka näin ei välttämättä tarvitse ollakaan, ja niiden rakennuspalikoina toimivat muun muassa ohjelmistot, tietokannat ja tietoverkot. (Rainer & Prince 2015) Jaakohuhdan (2003) mukaan tietojärjestelmien ulottuvuudet käsittävät myös ympäristön, ihmiset, mediat ja dokumentaation, jotka jakaantuvat edelleen niiden alakategorioihin; esimerkiksi media-kohtaan hän esittää kuuluvaksi tallennuksen, varmistuksen, säilytystavan ja tietojen siirron. Tietojärjestelmien osa tiedon kaikessa käsittelyssä on siis olennainen, ja näin ollen tietojärjestelmät linkittyvät suoraan myös henkilötiedon kaikkeen käsittelyyn.

1.4 Tutkimusmenetelmät ja työn rakenne

Tämä kandidaatintutkielma toteutetaan kirjallisuuskatsauksena, jossa luodaan ikään kuin vuoropuhelu erilaisten teorioiden ja lähteiden välille, jonka tarkoituksena on tarjota kattava ja selkeä käsitys Suomen pankkialasta ja sen toimijoiden sekä tietosuojasta että –turvasta. Työssä käytetyt lähteet ovat pankkitoimintaa ja tietosuojaa koskevia artikkeleita, kirjoja ja muita julkaisuja, kuten uutisia, joten lähteitä tullaan tarkastelemaan erittäin kriittisesti. Myös julkaisujen ajankohtaan tullaan kiinnittämään erityistä huomiota, jotta saatu tieto on varmasti niin laadukasta kuin mahdollista.

Koska työssä tarkastellaan pakollista asetusta, on lähteenä käytetty luonnollisesti

myös Euroopan Unionin virallisia sivuja. Myös Suomen laki ja esimerkiksi GDPR-tietopaketit toimivat lähteinä sellaisissa kohdissa, joissa avataan jotakin asetuksen kohtaa tarkemmin. Tutkimuksessa haastatellaan erästä Suomessa toimivan pankkialan yrityksen henkilöä, koska on oletettavaa, että hänellä on riittävän kattava käsitys siitä, millä tavoin tämän uuden asetuksen vaikutukset näkyvät.

Kappaleessa 2 tarkastellaan tietosuojasta säädettyjä lakeja ja asetuksia niin Euroopan Unionin kuin suomalaisen liiketoiminnankin näkökulmasta, ja kappaleessa kolme uutta tietosuoja-asetusta ja sen merkittävimpiä artikloita, sekä muita keskeisiä kohtia. Johdantokappaleessa avataan myös muutamia tutkielman kannalta olennaisimpia käsitteitä. Luvussa kaksi perehdytään sekä suomalaisiin että Euroopan unionin sisäisiin tietosuojakäytäntöihin, ja luvussa kolme taas tarkastellaan uutta tietosuoja-asetusta sekä sitä koskevia aiempia tutkimuksia.

Neljännessä kappaleessa tarkastellaan suomalaista pankkialaa ja siihen liittyvää tietosuojaa sekä perusteita tietojen keräämiselle sekä niiden käsittelylle. Kappaleessa tarkastellaan suomalaisen pankkitoiminnan tietosuojan kehittymistä niin erilaisten sopimusten ja lakien kuin yleisesti käytettyjen tapojenkin kannalta, osittain kappaleessa kolme esitettyjen menetelmien pohjalta. Näiden lisäksi esitetään myös katsaus siihen, minkälaisia tietoja pankki asiakkaastaan tarvitsee toteuttaakseen liiketoimintaansa ja palvellakseen asiakkaitaan niin hyvin kuin mahdollista.

Viidennessä kappaleessa tuodaan haastattelussa selvinneitä asioita ilmi ja tehdään niiden perusteella analyysia viitaten samalla tutkimuksessa aiemmin esitettyyn teoriaan sekä muihin asioihin. Viimeisessä kappaleessa esitetään tutkimuksen tulokset ja johtopäätökset. Siinä vertaillaan myös ensimmäisessä kappaleessa esitettyä teoreettista viitekehystä saatuihin tuloksiin, sekä esitetään johtopäätös siitä, minkälaisia asioita pankkien tulisi ottaa huomioon tietosuoja-asetuksen astuessa voimaan.

2 Tietosuoja lainsäädännön kannalta

Tänä päivänä, kun teknologia kehittyy ja digitalisaatio jatkaa yhä kasvuaan, on erityisen tärkeää keksiä oikeanlaisia keinoja, jotta niiden mukana tuleviin haasteisiin pystytään vastaamaan. Suomalaisten yritysten ja rekisterinpitäjien tietosuoja-asioita koskien on tehty erilaisia päätöksiä niin kansallisella kuin Euroopan Union tasollakin. Uusi tietosuoja-asetus tulee kuitenkin tuomaan muutoksia molempiin edellä mainittuihin.

2.1 Tietosuoja suomalaisessa liiketoiminnassa

Suomen lainsäädäntö on jo pitkään ottanut kantaa tietosuojan eri osa-alueisiin, mutta nämä kannanotot eivät ole olleet kovinkaan yksiselitteisiä tai helposti selvitettävissä. Ensimmäinen henkilötietojen käsittelyä koskevan lain, eli henkilörekisterilain, voidaan katsoa tulleen voimaan vuonna 1988 (Henkilörekisterilaki 1987). Kun tarkastellaan tietosuojaa esimerkiksi henkilötietojen käsittelyn kannalta, voidaan nopeasti havaita, että kyseistä asiaa käsitteleviä erityislakeja löytyy monta kymmentä. (Henkilötietolaki 2013; Erityslainsäädäntö 2014)

Myös vuoden 2000 maaliskuussa voimaan tullut perustuslaki ottaa kantaa henkilön yksityiselämän suojaa koskevista oikeuksista, mutta tässäkin pykälässä ilmoitetaan henkilötietojen suojasta säädettävän erikseen toisella lailla (Suomen perustuslaki 1999). Käytännössä henkilötietolaki itsessään on ollut, ja tulee olemaan, tähän uudistukseen asti tärkein tietosuojalainsäädännön väline; joskin tähän on ollut suuria vaikutuksia Euroopan unionin henkilötietodirektiivillä (Henkilötietolain taustaa 2013). Euroopan unionin uusi tietosuoja-asetus tulee kuitenkin kumoamaan henkilötietolain, kun sen soveltaminen aloitetaan unionin maissa toukokuussa (Aalto-Setälä 2016).

Pankkitoiminnan kannalta tietosuojaan on osaltaan vaikuttanut myös niin kutsuttu pankkisalaisuus, joka perustuu lakiin. Pankkisalaisuus tarkoittaa sitä, että pankki tai sen toimihenkilöt ovat vastuussa siitä, että heidän asiakkaidensa tietoja ei leviä ulkopuolisten tietoon (Pankkisalaisuusohjeet 2009). Tästä voidaan kuitenkin joustaa joissakin erityistapauksissa; esimerkiksi kun asiakas itse hyväksyy tällaisen toimenpiteen, tai jokin toinen laki sen oikeuttaa (Hyvä pankkitapa 2015). Luottotietolain (2007/527) mukaan riittäviä syitä henkilön luottotietojen luovutukseen ovat muun

muassa sellaiset tilanteet, jotka liittyvät rikoksen selvittämiseen, tai ”jos tiedon antaminen perustuu viranomaiselle laissa säädettyyn tiedonsaantioikeuteen”. Samaisen lain mukaan luottotietojen rekisteriin saa tallettaa myös henkilön nimen, hänen yhteystietonsa ja henkilötunnuksen. Henkilötiedot kuuluvat siten myös tähän rekisteriin.

Myös laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista otetaan kantaa henkilötietojen käsittelystä, tavoitteena turvata yksityisyyden suojaa. Tämä perustuu kuitenkin henkilötietolaissa esitettyihin säädöksiin, mutta tunnistuspalvelun tai tunnistusvälityspalvelun tarjoajan näkökulmasta. (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 2009). Sähköinen tunnistaminen tarkoittaa esimerkiksi pankin verkkopankkitunnuksien avulla toteutettua henkilöllisyyden todentamista. Tietosuojavaltuutettu vastaa siitä, että henkilötietoja koskevia säännöksiä noudatetaan kyseisen lain asettamia velvollisuuksia, mutta muuten vastuu on pääasiassa viestintävirastolla. (Viestintävirasto 2017)

2.2 Euroopan unionin keskeiset tietosuojakäytännöt

Euroopan unionin henkilötietodirektiivi (Direktiivi (EU) 1995/46), joka annettiin lokakuussa 1995, painottaa juurikin yksilön suojaa käsitellessä henkilötietoja, ja direktiivi määritteleekin henkilötietojen käsittelyn kaikeksi sellaiseksi toiminnaksi, joka ”kohdistetaan henkilötietoihin joko automaattisen tietojenkäsittelyn avulla tai manuaalisesti”. (Euroopan parlamentin ja neuvoston direktiivi 95/46/EY) Toisin sanoen; myös erilaiset automaattisesti toimivat tietokannat ja –järjestelmät tulee pitää direktiivin antamien vaatimusten mukaisena.

Direktiivin kohdassa 8 todetaan, että ”henkilötietojen liikkuvuuden esteiden poistamiseksi yksilöiden oikeuksien ja vapauksien suojan tason kyseisten tietojen käsittelyssä on oltava sama kaikissa jäsenvaltioissa...” (Euroopan parlamentin ja neuvoston direktiivi 95/46/Ey). Henkilötietodirektiivi on kuitenkin antanut unionin maille melko vapaat kädet sen tulkinnassa ja soveltamisessa, mistä johtuen käytännöt eri maiden välillä ovat olleet vaihtelevia (Lehtola 2016). Tämän kaltaiset eroavaisuudet voivat haitata yksilönsuojaa, sillä EU:n kansalaisella on oikeus esimerkiksi avata pankkitili toisessa EU-maassa, vaikka et siellä asuisikaan (Pankkitili toisessa EU-maassa 2018); miten yksilö pystyy varmistumaan henkilötietojensa suojasta, jos

direktiiviä noudatetaan tai sovelletaan näissä kahdessa eri maassa täysin eri tavalla?

Edellä esitettyä henkilötietodirektiiviä (1995) on kuitenkin jälkeenpäin täydennetty Euroopan parlamentin ja neuvoston asetuksella 45/2001, jossa ohjeistetaan ”yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta”. Asetuksen osoittamista säännöksistä valvomisesta vastaa samaisessa asetuksessa perustettu valvontaviranomainen, Euroopan tietosuojavaltuutettu. (Asetus (EU) 2001/45) Yritys- ja yhteisötietolain (2001) mukaan tällaisiksi tahoiksi luokitellaan muun muassa osuuskunnat ja osakeyhtiöt, joita suuri osa suomalaisista pankeista, kuten Osuuspankki ja Nordea, ovat (OP osuustoiminta 2018; Nordea 2018).

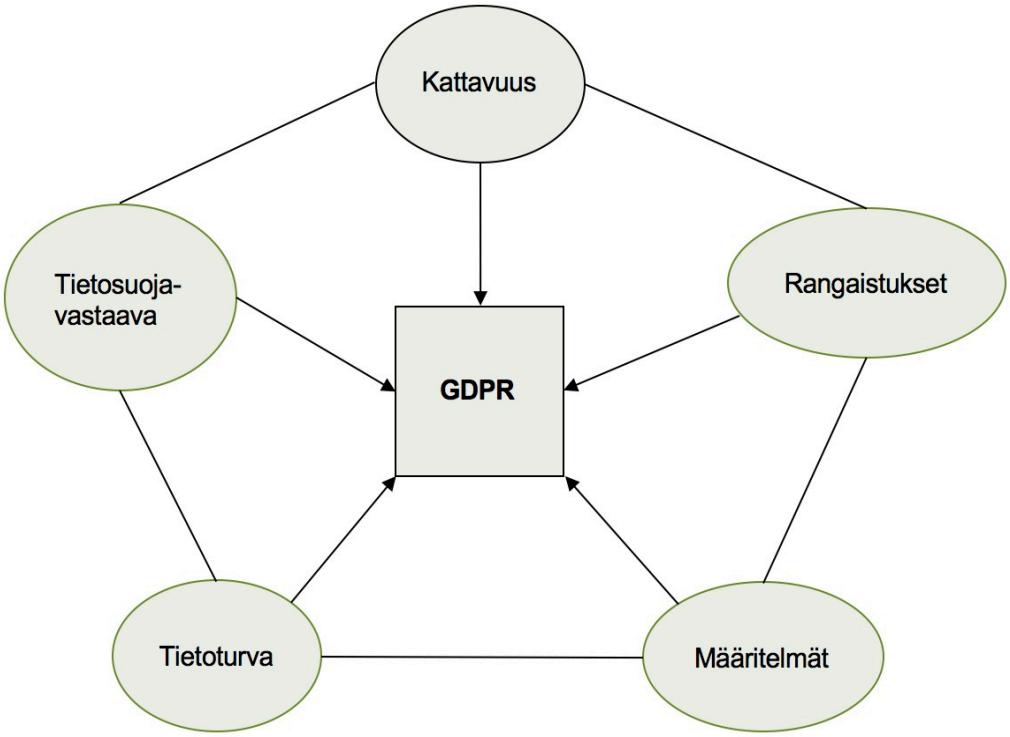
Globalisaatio ja digitalisaatio ovat saaneet aikaan sellaisen ilmiön, että maantieteelliset rajat ovat alkaneet hämärtyä tiedon ja palvelujen liikkuessa vaivattomasti paikasta ja maasta toiseen (Järvinen & Rousku 2017). Vapauden ja vapaan liikkuvuuden ollessa yksi Euroopan unionin tärkeimpiä arvoja ja tavoitteita (EU:n tavoitteet ja arvot 2018), on erityisen tärkeää, että myös henkilötiedot liikkuvat vaivattomasti ja turvallisesti maasta toiseen. Yksi uuden tietosuoja- asetuksen keskeisimmistä tehtävistä onkin eliminoida sellaiset eroavaisuudet maiden välillä, jotka voisivat jollakin tapaa haitata Euroopan Union sisämarkkinoilla tapahtuvaa tietojen liikkumista (Partanen 2014).

Sähköisen viestinnän alueella tapahtuvasta henkilötietojen käsittelystä ja yksityisyyden suojasta on säädetty myös Euroopan unionin tasolla, pääsääntöisesti henkilötietodirektiiviä tarkentaen. Sähköisen viestinnän tietosuojadirektiivin avulla pyritään takaamaan tietosuoja ja yksilöllisyyden suoja myös erilaisten sähköisten viestintäpalveluiden ja tietoverkkojen osalta. (Sähköisen viestinnän tietosuojadirektiivi 2002)

3 Euroopan unionin uusi tietosuoja-asetus (GDPR)

Huhtikuun 27. päivänä 2016 Euroopan parlamentti ja neuvosto antoi asetuksen ”luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta” (Asetus (EU) 20167/679). Samainen asetus kumoaa vuonna 1995 annetun direktiivin 95/46/EY, eli henkilötietodirektiivin. (Euroopan parlamentin ja neuvoston asetus 2016/679) Nyt kaksi vuotta asetuksen antamisen jälkeen on asetuksen soveltamisen aloittaminen lähellä, sillä 25.5.2018 on se päivämäärä, jolloin asetus kokonaisuudessaan astuu voimaan (Mitä jokaisen kuuluu tietää EU:n uudesta tietosuoja-asetuksesta GDPR 2018). Edellä mainittuun asetukseen viitataan myöhemmin tekstissä termeillä tietosuoja-asetus tai asetus.

3.1 Uuden tietosuoja-asetuksen keskeisimmät teemat



Kuva 2. GDPR keskeiset asiat (mukaillen Findwise 2018)

Edellisellä sivulla esitetty kuvio havainnollistaa tietosuoja-asetukseen kuuluvia keskeisimpiä osa-alueita, joilla on suuri vaikutus tietosuojaan ja henkilötietojen käsittelyyn. Kattavuudella tässä asetuksessa tarkoitetaan sitä, että asetus käsittää niin Euroopan unionin sisäiset kuin sen ulkopuolisetkin yritykset, jos ne käsittelevät unioniin kuuluvien yksilöiden henkilötietoja (Findwise 2018).

Asetus edellyttää, että henkilötietoja käsittelevän yrityksen tai muun organisaation tulee joissakin tapauksissa osoittaa tietosuojavastaava. Yrityksen näkökulmasta tällaisia tapauksia ovat ne tilanteet, joissa yrityksen pääasialliset tehtävät koostuvat juurikin henkilötietojen jatkuvasta ja organisoidusta käsittelystä, tai sitten tilanteet, joissa käsiteltäviä henkilötietoja voidaan pitää riittävän arkaluontoisina. Tärkein kriteeri tälle on kuitenkin toiminnan laaja-alaisuus, joten esimerkiksi pienen yksinyrittäjän tapauksessa henkilötietojen käsittely tuskin on riittävän mittavaa täyttääkseen asetuksessa annetut kriteerit. Tietosuojavastaavan tärkeimmät tehtävät liittyvät uuden asetuksen mukaisten vaatimusten noudattamiseen yrityksen sisällä. (Hanninen, Laine, Rantala, Rusi & Varhela 2017)

Valtiovarainministeriön VAHTI-raportin (2016) mukaan valvontaviranomaisella on mahdollisuus antaa sakkorangaistus sellaiselle taholle, joka epäonnistuu tietosuoja-asetuksen vaatimusten mukaisen toiminnan toteuttamisessa. Tämä sakko voi tulla yritykselle melko kalliiksi, sillä sakon enimmäismäärä on 20 miljoonaa euroa tai 4 % aikaisemman tilikauden liikevaihdosta. (VAHTI-raportti 2016). Sakkojen suuruutta mietittäessä otetaan kuitenkin huomioon muun muassa sellaiset asiat, kuin oliko epäonnistumisen syy tahallinen vai tahaton, sekä onko kyseinen taho aiemminkin jostakin syystä epäonnistunut tietojen asianmukaisessa suojaamisessa (Asetus (EU) 2016/679).

Tietoturvan osa-alue taas liittyy olennaisesti tietosuoja-asetukseen, sillä kuten edellä jo esitettiin, merkitsee tietoturva niitä toimintamalleja ja järjestelmiä, joiden avulla tietosuojasta pyritään varmistumaan. Hanninen et. al. (2017) mainitsevat, että tietosuoja-asetuksen myötä yritysten tulee myös osoittaa, että tietoturvan taso pystytään tehokkaasti varmistamaan ja ylläpitämään koko henkilötietojen käsittelyprosessin ajan. Jos tietojen turvaamisessa kaikista yrityksistä huolimatta epäonnistutaan, tulee yrityksen ilmoittaa siitä sekä tietosuojaviranomaiselle että henkilölle, kenen tietoja se koskee, viimeistään kolmen vuorokauden kuluttua

(Findwise 2018).

Määritelmillä tässä viitataan siihen, että esimerkiksi henkilötiedot käsittävät asetuksen mukaan kaikki sellaiset tiedot, joiden perusteella voidaan jotenkin selvittää, kenestä on kyse; joko suoraan tai epäsuorasti. Määritelmä kattaa nimen ja sosiaaliturvatunnuksen, mutta myös muun muassa taloudelliset ja sosiaaliset ominaisuudet, jos henkilö on niiden perusteella selvästi tunnistettavissa. Tämän lisäksi myös esimerkiksi käsittelyn ja profiloinnin määritelmät ovat todella laajoja. (Hanninen et. al. 2017)

3.1.1 Avaintekijät henkilötietojen käsittelyssä

Henkilötietojen käsittelyn turvallisuuteen liittyvät kyvykkyydet ja toimenpiteet ovat suuressa roolissa yrityksen tietosuojan onnistumisessa jatkossa. Tietosuoja-asetuksessa esitetään muun muassa sellaisia toimenpiteitä, kuin henkilötietojen pseudonymisointi ja tietojen palauttaminen jonkin häiriön tai vastaavan sattuessa (Asetus (EU) 2016/679). Edellä esitetyssä kuvassa havainnollistetaan asetusten vaatimusten mukaisen tietosuojan onnistumisen kannalta olennaisia tekijöitä tietoturvan osalta, sillä juuri tietoturvallisuuden korkea taso on avaimena näissä onnistumiseen.

Kuva 3. Edellytykset turvallisen tiedonkäsittelyn varmistamiseen (mukaillen Asetus (EU) 2016/679)

Luottamuksella tarkoitetaan tässä yhteydessä sitä, että tietoja pääsevät käsittelemään ainoastaan ne henkilöt, joilla on siihen oikeus. Yrityksen näkökulmasta tämä voidaan ajatella niin, että muilla samassa yrityksessä työskentelevillä henkilöillä ei automaattisesti ole oikeutta tietojen käsittelyyn, ellei heidän työnkuvansa sitä välttämättä edellytä. (Hanninen et. al. 2017) Tietojen järkevä salaaminen, esimerkiksi salasanoilla, tulee olemaan tärkeä osa näiden edellytysten täyttämiseen. Tämä tulee ottaa huomioon myös tietoa poistettaessa tai sen tullessa yrityksen kannalta tarpeettomaksi.

Tiedon eheys, tai toisin sanoen oikeellisuus, merkitsee sitä, että tiedon hankkimishetkestä alkaen rekisterinpitäjällä on vastuu siitä, ettei tieto muutu, kun sitä käsitellään tai siirretään paikasta toiseen. Tämän avulla pyritään varmistautumaan siitä, että tietoja ei muuteta niitä käsitellessä. (Hanninen et. al. 2017)

Henkilötietojen käytettävyys merkitsee tietosuoja-asetuksen kannalta sitä, että tietojen täytyy olla käytettävissä silloin, kun niitä on tarpeen käsitellä (Hanninen et. al. 2017). Käytettävyyden turvaamisen kannalta tulee yritysten huomioida myös sellaiset

tapaukset, joissa tieto jostain syystä menetettäisiin ja tähän tietoon pitäisi päästä nopeasti käsiksi (Miten valmistautua EU:n tietosuoja-asetukseen 2017).

Vikasietoisuus liittyy osaltaan myös järjestelmiin ja yrityksessä tehtäviin teknisiin ratkaisuihin, joiden avulla voidaan varmistua siitä, että myös esimerkiksi teknisen vian sattuessa henkilötietoja säilyttävä järjestelmä kykenee jatkamaan. Tämä tarkoittaa käytännössä sitä, että kun yksi osa-alue kohtaa vian, pystyvät muut osat ottamaan tehtävän hoidettavakseen. (Tietosuoja 2018)

Näiden tietoturvallisuuden osa-alueiden merkitys kokonaisvaikutukseen on luonnollisesti olennainen. Tietosuoja-asetuksen vaatimusten täysimittaisessa täyttämisessä tulee kuitenkin huomioida myös monia muita tietosuojaan liittyviä seikkoja, jotka tukevat näitä neljää periaatetta kokonaisvaltaisella tavalla.

3.2 Henkilötietojen käsittelyn kannalta keskeiset kohdat

Tietosuoja-asetuksen yleisissä säännöksissä säädetään monessakin kohtaa juuri henkilötietojen käsittelyä koskevia asioita, niin rekisterinpitäjän kuin rekisteröidynkin näkökulmasta. Tutkielman kannalta keskitymme kuitenkin pääasiassa ensimmäiseen näistä. Edellä olevassa taulukossa esitetään tärkeimmät artiklat ja avataan hieman niiden sisältöä. Taulukossa esitettyjen artiklojen lisäksi myös muun muassa artiklassa neljä käsitellään henkilötietoihin liittyviä muutoksia, mutta kyseinen artikla keskittyy määrittelemään erilaisia asetuksessa esitettyjä käsitteitä ja määritelmiä. Esimerkiksi henkilötietojen määritelmän laajentaminen ja muut tietosuoja-asetuksessa useasti käytetyt käsitteet. (Asetus (EU) 2016/679)

Taulukko 1. Henkilötietojen käsittelyn kannalta olennaisimmat artiklat (mukaillen EU:n tiedotetta asetuksesta 2016)

Artikla	Artiklan ydinasiat henkilötietojen käsittelyä koskien
5	Yleiset periaatteet henkilötietojen käsittelyssä. Esimerkiksi lainmukainen ja rekisteröidyn kannalta läpinäkyvä henkilötietojenkäsittely.
6	Määritelmät käsittelyn lainmukaisuuteen.
7	Henkilötietojen käsittelyyn suostuminen, sen vapaaehtoisuus, sekä suostumuksen peruuttaminen. Turvallisuustason tulee vastata tietojen käsittelyyn koskevaa riskiä.
17	Henkilöllä oikeus vaatia hänen henkilötietojensa poistamista rekisteristä tietyn edellytyksin.
18	Rekisteröidyllä oikeuksia rajoittaa käsittelyä tietyissä tilanteissa.
20 & 15	Henkilöllä oikeus saada tietoonsa, mitä tietoja rekisterinpitäjä on hänestä kerännyt. Henkilötietojen siirto rekisteristä toiseen.
22	Automaattisen henkilötietojenkäsittelyn rajoitukset.

Artikla viisi käsittelee tietojen käsittelyä koskevia periaatteita, jotka asettavat tiettyjä vaatimuksia käsittelyyn. Siinä otetaan huomioon koko tietojen elinkaari, sillä artikla ottaa kantaa niin tiedonhankinnan tarkoituksenmukaisuuteen kuin niiden olennaisuuteen niitä hallittaessakin. (Asetus (EU) 2016/679) Hanninen et. al. (2017) esittävät, että henkilötietojen käsittelyssä tulee aina olla taustalla jokin yrityksen kannalta tärkeä tarve. Tällaisia tärkeitä tilanteita ovat muun muassa asiakassuhteiden hoitaminen tai muut yritykset liiketoiminnan kannalta välttämättömät tilanteet. Artiklassa otetaan myös kantaa siihen, että henkilötietojen säilytys tulisi kestää ainoastaan niin kauan, kuin on tarkoituksenmukaista. Olennaista on siis se, että henkilötietojen käsittelyä tulisi toteuttaa ainoastaan silloin, kun sitä ehdottomasti vaaditaan.

Käsittelyn lainmukaisuutta käsitellään artiklassa 6, ja siinä esitetäänkin sellaiset tilanteet, joissa lainmukaisuuden ehto täyttyy; vähintään yhden artiklassa esitetyistä

vaatimuksista tulee täyttyä (Asetus (EU) 2016/679). Perusteita henkilötietojen käsittelyn lainmukaisuudelle ovat esimerkiksi suostumus, sopimus tai sellainen tilanne, jossa käsittely perustuu yleiseen etuun. Edellytyksen täyttyminen on kuitenkin ainut peruste henkilötietojen käsittelyn lainmukaisuudelle (Hanninen et. al. 2017).

Artikla 7 esittää rekisteröitävän suojan kannalta olennaisia oikeuksia. Muun muassa sen, että rekisteröitävän suostumus tietojen hankintaan ja niiden käsittelyyn pystytään tarvittaessa osoittamaan (Findwise 2018). Henkilön tulee myös tässä tilanteessa ymmärtää antavansa suostumuksen tietojensa käsittelyyn, ja hänellä on halutessaan myös oikeus perua tämä suostumus, joka tarkoittaa rekisterinpitäjän osalta velvollisuutta ”unohtaa” kyseinen henkilö järjestelmässään. Tietosuoja-asetus ottaa myös kantaa niin sanottuun sähköiseen allekirjoitukseen, eli suostumuksen voi tehdä esimerkiksi rekisteröintiä suorittavan tahon internetsivujen kautta; olettaen, että henkilö selvästi ymmärtää antavansa suostumuksensa tietojen käsittelylle. (Asetus (EU) 2016/679) Rekisteröidyn oikeuteen henkilötietojen poistamisesta paneudutaan syvemmin artiklassa 17.

Kuten edellisessä kappaleessa kerrottiin, artikla 17 koskee rekisteröidyn oikeutta tulla poistetuksi rekisterinpitäjän järjestelmästä, sekä rekisterinpitäjän näkökulmasta velvollisuutta poistaa kyseisen henkilön tiedot viivyttelemättä. Henkilötietojen poistamiseen vaaditaan kuitenkin, että ainakin yksi artikkelin osoittamista vaatimuksista täyttyy, joten rekisteröidyn oikeus vaatia tietojen poistamista ei ole täysin rajoittamaton. (Hanninen et. al. 2017) Tietosuoja-asetuksen (2016) 17:n artiklan mukaan tietojen poistamiseen oikeuttava tilanne voi olla esimerkiksi sellainen, jossa rekisterinpitäjä ei tarvitse keräämiään tietoja samaan tarkoitukseen, kuin mitä varten ne on alun perin hankittu, tai tilanne, jossa henkilötietoja on käytetty jollakin tapaa lainvastaisesti. Vaikka henkilöllä ei olisikaan oikeutta vaatia tietojensa poistamista, on hänellä tietyin edellytyksin mahdollisuus rajoittaa sitä, miten tietoja käsitellään; tätä selventää artikla 18.

Joissakin tilanteissa on mahdollista, että henkilöllä itsellään on oikeus vaikuttaa siihen, miten kattavasti hänen tietojaan saadaan rekisterinpitäjän toimesta käsitellä. Yksi tällainen tilanne on sellainen, jossa rekisteröity itse ilmoittaa, että hänestä kerätyt tiedot eivät pidä paikkaansa. Tämä johtaa käsittelyn rajoittamiseen ainakin siltä osin, kunnes tietojen oikeellisuus saadaan selvitettyä. (Hanninen et. al. 2017) Sellaisissa

tapauksissa, joissa käsittely on rajoitettua, on rekisterinpitäjällä oikeus tietojen käsittelyyn vain esimerkiksi rekisteröidyn suostumuksella (Oikeus käsittelyn rajoittamiseen 2017).

Tietosuoja-asetuksen 15. ja 20. artiklat antavat rekisteröidylle oikeuden saada selville käsitteleekö jokin taho hänen tietojaan, sekä oikeuden päästä niihin tietoihin, mitä henkilötietoja hänestä on kerätty. Henkilöllä on oikeus saada selville muun muassa mihin tarkoitukseen hänestä kerättyjä tietoja käytetään sekä mistä ja miten nämä tiedot on saatu; sellaisessa tapauksessa, jossa tietoja ei ole kerätty suoraan rekisteröidyltä. (Hanninen et. al. 2017) Tietosuoja-asetus (2017) velvoittaa rekisterinpitäjää myös toimittamaan rekisteröidylle, hänen niin halutessaan, kopion näistä tiedoista sellaisessa muodossa, kuin rekisteröity haluaa.

Taulukon alimmassa palkissa esitetty artikla 22 liittyy rekisteröidyn oikeuksiin automaattista tiedonkäsittelyä kohtaan. Hannisen et. al. (2017) mukaan tällaisia automaattisia käsittelyitä ovat esimerkiksi sellaiset sähköisessä rekrytoinnissa käytetyt keinot, joissa ihminen ei ole osallisena. Tulee kuitenkin huomata, että artiklassa säädetään ainoastaan kokonaan automatisoidusta käsittelystä; jos osa vaiheista toteutetaan jonkun luonnollisen henkilön toimesta, on kyseessä eri tilanne. Tällaista kokonaan automaattista käsittelyä on esimerkiksi profilointi, joka tarkoittaa kaiken henkilötietojen automaattisen käsittelyn lisäksi esimerkiksi henkilökohtaisten ominaisuuksien arviointia pelkästään henkilötietojen perusteella (Näkökohtia profiloinnista uudessa tietosuoja-asetuksessa 2017).

Tietosuoja-asetus luo yrityksille, tai rekisterinpitäjille yleensä, paljon velvollisuuksia. Nämä velvollisuudet voivat kuitenkin parhaassa tapauksessa tarjota rekisterinpitäjälle myös hyötyä, ja mahdollisuuden oman asemansa parantamiseen. Seuraavassa luvussa käsitellään niitä mahdollisuuksia ja etuja, joita tietosuoja-asetus rekisterinpitäjälle tarjoaa.

3.3 Tietosuoja-asetuksen hyödyt rekisterinpitäjälle

Vaikka tietosuoja-asetus tuokin mukanaan lukuisia haasteita rekisterinpitäjille, eli yrityksille, ja todennäköisesti aiheuttaa muutoksia useisiin toimintamalleihin ja järjestelmiin, on täysin mahdollista valjastaa tämä muutos yrityksen voimavaraksi.

Seuraavaksi esitettävässä kuvassa osoitetaan muutamia näistä eduista ja mahdollisuuksista, joita yritys pystyy saavuttamaan onnistumalla tietosuoja-asetuksen odotusten täyttämisessä parhaalla mahdollisella tavalla. Nämä saavutettavat hyödyt eivät ole kuitenkaan absoluuttisia tai välttämättä jokaiselle toimialalle yleistettävissä olevia, mutta ne tarjoavat pintapuolisen katsauksen niistä syistä, minkä takia tietosuoja-asetuksen vaatimusten mukaan toimimisella voidaan saada aikaan muutakin kuin pelkkiä kustannuksia.

Kuva 4. Tietosuoja-asetuksen soveltamisen hyödyt (mukaillen Findwise 2018; Boston Consulting Group 2013; Apsis 2017)

Trust advantage, eli luottamusetu, merkitsee Boston Consulting Groupin artikkelin mukaan käytännössä sitä, että asiakkaiden luovuttaessa tietojaan yrityksen käsiin, voivat he luottaa siihen, että tietoja käytetään vain ja ainoastaan sallittuihin tarkoituksiin. Koska ihmiset välittävät siitä, miten heidän tietojaan käsitellään ja mihin tarkoitukseen niitä käytetään, voi yritys luottamusedun saavuttamalla myös saada haltuunsa enemmän tärkeää tietoa. (Rose, Barton, Souza & Platt 2013) Williams (2013) uskookin, että luottamuksen luominen ja toiminnan läpinäkyvyys ovatkin yhdet tärkeimmistä työkaluista onnistuneeseen liiketoimintaan. Myös Wilde (2011) esittää,

että mitä paremmin yritys pystyy asiakassuhteitaan hoitamaan, sitä tuottavampi yritys on. Hän ehdottaa myös asiakkaiden osallistamista palveluiden suunnitteluvaiheeseen, silloin, kun keskinäisen luottamuksen taso on tarpeeksi korkea. Myös Shaw et. al. (2010) esittävät tutkimuksessaan tunnearvon hierarkiassa luottamuksen erittäin korkealla; se on siis yksi tärkeimmistä niin sanotuista pehmeistä arvoista asiakaskokemuksessa.

Kustannussäästöillä tarkoitetaan tässä Findwisen (2018) mukaan sitä, että niin turhien tietojen säilyttäminen kuin vanhentuneen tai epäolennaisen tiedon käyttäminenkin aiheuttavat yritykselle turhia kuluja. Tiedonhallinta on tärkeässä osassa yrityksen jokapäiväistä toimintaa, ja oikean tiedon puuttumisella on suuret vaikutukset liiketoimintaan, sillä se aiheuttaa suurien kustannusten lisäksi muitakin päivittäisiä liiketoiminnan ongelmia (Lecklin & Laine 2009, 146). Tietosuoja-asetuksen herättäessä yritykset muokkaamaan tiedonhallinnan mallejaan uusia vaatimuksia vastaavammiksi saa heidät samalla valveutuneemmiksi siitä, mikä on oikeaa ja tarpeellista tietoa; sellaista, mikä on liiketoiminnan kannalta tärkeää.

Henkilötietojen hallintaa varten käyttöönotetut tai kehitetyt järjestelmät ovat hyödynnettävissä muillakin liiketoiminnan osa-alueilla. Näiden toimintamallien ja –tapojen soveltaminen muihinkin tietojärjestelmiin voi auttaa yritystä parantamaan tiedonhallintaa paremmin yleisestikin. (Findwise 2018) Toisaalta tässä täytyy huomioida tietojärjestelmien lisäksi myös hallussa olevat teknologiat, joiden avulla tämä mahdollistetaan.

Viimeisenä edellisen sivun kuvan esittämistä hyödyistä on tietosuoja-asetuksen vastaisesti toimimisesta saatavan sakon välttäminen. Kuten aikaisemmin osoitettiin, sakko voi olla suuruudeltaan 20 miljoonaa euroa, tai 4 % konsernin edellisen tilikauden kokonaisliikevaihdosta, joten on jokaisen yrityksen etujen mukaista pyrkiä noudattamaan tämän uuden asetuksen velvoitteita.

3.4 Aikaisemmat tutkimukset

Tietosuoja-asetuksen vaikutuksia ei ole vielä tutkittu kovinkaan paljon, sillä asetus on astumassa voimaan vasta toukokuun 2018 loppupuolella. Vaikka tutkimusta ei aikaisemmin olekaan kohdistettu yksinomaan pankkialaan, on muita organisaatioita

tutkittu jo jonkin verran. Tässä alakappaleessa käydään läpi näitä tutkimuksia ja organisaatioita sekä sitä, miten tietosuoja-asetus tulee niihin vaikuttamaan.

Väisänen (2015) tutki tietosuoja-asetuksen vaikutuksia Oulun ammattikorkeakouluun opinnäytetyössään haastattelemalla organisaation henkilöstöä, ja tutkimuksessa selvisi, että suurimpia haasteita tulevat olemaan muun muassa asetuksen kokonaisvaltainen hahmottaminen sekä henkilöstön osaamisesta varmistuminen. Tutkimuksessa selvisi, että olennaisimmat vaikutukset liittyvät sellaisiin toimenpiteisiin, kuin tietosuojavastaavan nimittämiseen. Väisänen uskookin tämän johtavan esimerkiksi rekisterijärjestelmän päivittämiseen sekä tietojärjestelmien muuttamiseen.

Paajanen (2017) tutki tietosuoja-asetuksen vaikutuksia organisaatioihin diplomityössään, ja tutkimuksen tulokset vahvistavat, että asetus pakottaa organisaatioita ottamaan selvää niistä henkilötiedoista, joita heillä on hallussaan. Tämän jälkeen tulee suorittaa riskikartoitus, jonka avulla varmistutaan siitä, että käytössä olevat järjestelmät ja toimintatavat ovat sellaisella tasolla, joka minimoi mahdolliset riskit. Tutkimuksessa kuitenkin todetaan, että tulkinnanvaraisuudesta eri osa-alueiden kohdalla johtuen on organisaatioiden itse selvitettävä, mitkä ovat riittävät suojaustoimet.

Hakonen (2017) tutki opinnäytetyössään sitä, miten henkilötietojen turvallinen käsittely toteutuu tietosuoja-asetuksen vaatimusten edellyttämällä tavalla. Tutkimuksessa painotettiin erityisesti tietoturvan osallisuutta tässä. Hakonen spekuloikin, että datan, kuten henkilötietojen, määrän kasvaessa tulee niihin kohdistuvien riskien määrä kasvamaan entisestään, joten tietosuoja-asetus ei astu voimaan yhtään liian myöhään. Tutkimuksessa todettiin, että suurimmat vaikutukset organisaatioihin tulevat olemaan sekä tietosuojavastaavan nimittäminen että velvollisuus ilmoittaa tietoturvapoikkeamista, sillä se saattaa vaikuttaa ulkoisiin mielipiteisiin yrityksestä.

Myös Häkkinen (2017) tutki opinnäytetyössään tietosuoja-asetuksen vaikutuksia, tosin palkanlaskennan ja työsuhdetietojen näkökulmasta. Tutkimuksen kohdeyrityksen osalta suurimmat vaikutukset tulevat kohdistumaan kirjalliseen dokumentointiin ja erilaisten toimintatapojen päivittämiseen. Myös henkilöstön koulutus asetuksen vaatimuksiin nousi keskeiseksi muutokseksi. Erään tietoturvallisuutta yrityksien näkökulmasta tutkineen lähteen mukaan suurimmat haasteet riittävän tietosuojan

ylläpitämisessä ovat henkilöstön kouluttaminen tietoturvallisuuteen, yrityksen digitaalisen jalanjäljen kasvu verkkoympäristöissä sekä sosiaalisen manipuloinnin ehkäiseminen ja torjuminen. Sekä ensimmäiseen että jälkimmäiseen näistä pystytään valmistautumaan varmistautumalla siitä, että organisaation henkilöstö on ajan tasalla sen hetkisistä tietosuoja- ja tietoturvavaatimuksista. Henkilöstön osaamisen merkityksen korostuminen on siis ollut tähän mennessä toteutettujen tutkimusten yhtenäinen tutkimustulos.

Albrechtin (2016) mukaan tietosuoja-asetuksen läpinäkyvyyttä ja tietokäytäntöjen yksinkertaisuutta lisäävät kohdat mahdollistavat sen, että kuluttajat saavat käyttöönsä lisää valtaa yritykseen nähden. Tämän lisäksi myös kuluttajan suostumuksen merkitys arvo kasvaa liiketoiminnassa. Sisäänrakennettu ja oletusarvoinen tietosuoja tulee mahdollistamaan uudenlaisten innovaatioiden ja esimerkiksi kuluttajaystävällisempien palveluiden kehittämisen, joissa tietosuoja voi tarjota kilpailuedun lähteen. Nauwelaerts (2017) keskittyi tutkimuksessaan kuluttajien oikeuksien kasvuun ja näiden oikeuksien mahdollistamiin toimiin. Hän toteaakin, että asetuksen lisätessä kuluttajien oikeuksia, voivat asetukseen varautumattomat yritykset joutua oikeustoimien kohteeksi omien asiakkaidensa toimesta, mikä saattaa tulla yritykselle kalliiksi.

Purtova (2018) ottaa kantaa tietosuoja-asetuksen laajuuteen, ja kuvaakin sitä ”kaiken laiksi”. Tämä tulee hänen mukaansa johtamaan siihen, että asetuksen yrittäessä tarjota mahdollisimman korkeaa laillista suojaa kaikissa tilanteissa, tulee se kääntymään itseään vastaan, sillä sen noudattaminen käytännössä muodostuu mahdottomuudeksi rekisterinpitäjille.

4 Pankkialan tietosuoja

Pankkien ydintehtävän, eli rahoituksen välittämisen, takia pankkien asiakaskunta on usein laajaa. Yleisesti voidaan ajatella, että asiakaskunta koostuu niin rahoituksen tarjoajista, eli säästäjistä, kuin rahoituksen saajista, eli esimerkiksi luotonottajista. Joissakin tapauksissa toisena näistä osapuolista on kuitenkin yritys, jonka toiminnan takana on aina ihmisiä. Niinpä pankkien hallussa olevien henkilötietojen tulee olla erityisen laadullisia ja tarkkoja. Kontkasen (2011) mukaan pankkien tehtäväalueet kuitenkin laajentuvat yhä entisestään muun muassa teknologisen kehityksen ja globalisaation myötä, mikä osaltaan tulee lisäämään niin tarvittavia tietoja kuin todennäköisesti niiden henkilöiden määrää, joiden tietoja käsitellään. Rainer & Prince (2015) toteavat, että tietokoneohjelmat ovat muokanneet rahoitussektoria merkittävästi; erilaiset maksutapahtumat suorittaa jokin tietokoneohjelma ja esimerkiksi matkapuhelinsovelluksen avulla voidaan maksaa ostoksia omalta tililtä pelkästään matkapuhelinta näyttämällä. Tämän kaltaiset muutokset ovat toisaalta hyöyllisiä, mutta ne tuovat lisää vastuuta tietoturvaan ja –suojaan.

4.1 Tietojen merkitys pankkitoiminnassa

Pankkitoiminnan turvallisuudessa tulee palveluntarjonnassa huomioida erityisesti, että pankki tuntee asiakkaansa, toisin sanoen asiakkaan henkilöllisyyden varmistaminen. Kontkanen painottaakin tietoturvan suurta merkitystä pankkien toiminnassa, sillä ”pankkitoiminta rakentuu keskeisesti asiakassuhteista saadun tiedon varaan”. (Kontkanen 2011, 77) Tämä on ollut kuitenkin pankeille selvää jo pankkitoiminnan ensi hetkistä alkaen, sillä pankkisalaisuusperiaatetta on noudatettu niin kauan, kuin pankkeja on ollut, vaikka pankkisalaisuudesta säädettiin laissa vasta vuodesta 1970 alkaen. (Pankkisalaisuusohjeet 2009)

Henkilötietojen kerääminen ja hallinta ovat siis olennainen osa pankkien toimintaa niiden tehokkuuden varmistamiseksi. Asiakkaiden näkökulmasta asia ei kuitenkaan ole täysin itsestään selvää, sillä EY:n tuottaman pankkitutkimuksen mukaan yli puolet niin yksityisen kuin julkisenkin sektorin asiakkaista ovat huolissaan siitä, miten paljon tietoa nämä ovat heistä keränneet (EY 2016). Myös Yle uutisoi vuonna 2012, että asiakkaat ovat ihmeissään pankkien heille esittämistä kysymyksistä (Kirsi 2012).

Andreasson et. al. (2017) mainitsevat, että korkeatasoinen tietosuoja edesauttaa esimerkiksi luottamuksen syntymistä, ja jonka avulla kyetään muun muassa digitalisaation mahdollisuuksia entistä laajemmin. Seuraavaksi esitettävässä taulukossa esitetään sellaiset tiedot, joita suurimmat suomalaiset pankit keräävät asiakkaistaan.

Taulukko 2. Minkälaisia tietoja pankit asiakkaistaan keräävät? (Nordea 2018; OP 2018)

Yksilöintiin ja tunnistamiseen liittyvät tiedot sisältävät muun muassa sosiaaliturvatunnuksen ja asiakkaan nimen, ja yhteystiedot luonnollisesti eri kanavat yhteydenpitoon asiakkaan kanssa, eli muun muassa sähköpostiosoitteen ja puhelinnumeron. Kolmantena esitetty asiakassuhteeseen liittyvät tiedot käsittävät

esimerkiksi asiakasnumerot ja muut asiakassuhteen hoitamiseksi välttämättömät tiedot. Palveluja koskevat tiedot taas käsittävät esimerkiksi asiakkaan sijoituksia koskevat tiedot kattaen sijoitusten kohteet ja rahasummat. (Henkilötieto 2018) Terrorismin ja rahanpesun estämiseksi pankki tiedustelee asiakkaaltaan myös, onko tämä poliittisesti vaikutusvaltainen tai kuuluuko asiakas tällaisen henkilön lähipiiriin. Edellä esitetyt perustelut ovatkin yksi tärkeimmistä syistä, mahdollisimman hyvän palvelun tarjoamisen lisäksi, miksi pankkien tarvitsee tuntea asiakkaansa niin hyvin. (Miksi ja mitä tietoja pankki kyselee? 2016) Mahdollisimman hyvällä asiakastuntemuksella pankki kykenee Nordean lehdistötiedotteen (2016) mukaan toteuttamaan yhteiskunnallista vastuutaan ja ehkäisemään rahanpesun lisäksi myös esimerkiksi talousrikosten tapahtumista.

Yksi toinen keskeinen syy siihen, miksi pankkien tulee tuntea asiakkaansa niin hyvin, on sähköinen tunnistautuminen. Tunnistautumalla johonkin verkkopalveluun antaa mahdollisuuden hoitaa monia henkilökohtaisia asioita sähköisesti. Esimerkiksi sellaiset valtion ylläpitämät sivustot kuin Kela ja Vero antavat asiakkaan tehdä erilaisia toimenpiteitä tunnistauduttuaan verkkopalveluun, ja tämän voi tehdä juurikin pankkitunnuksilla. Tästä syystä pankki voikin esimerkiksi vaatia, että jos verkkopankin tunnuslukuja haluaa säilyttää suojattomassa paikassa, tulee niiden olla salakirjoitettu.

5 Tietosuoja-asetuksen vaikutukset pankkialaan

Tämä kappale käsittelee haastattelusta saatuja tuloksia. Haastattelu oli jaoteltu neljään eri teemaan, jotka käsittelivät alatutkimusongelmia. Metsämuurosen (2016) mukaan puolistrukturoitu eli teemahaastattelu sopii haastattelumenetelmäksi silloin, kun tutkittava aihe on heikosti tiedostettu. Ensimmäinen teema, eli valmistautuminen, ei kuitenkaan liittynyt suoraan yhteenkään alaongelmaan, mutta sillä on merkitystä kattavan kokonaiskuvan saamiseksi, sekä päätutkimusongelman selvittämisessä; alatutkimusongelmat ovat luotu juuri sen perusteella, että niiden avulla pystytään muodostamaan pohja päätutkimusongelmalle. Haastattelu suoritettiin puhelinhaastatteluna, joka nauhoitettiin matkapuhelimen äänityssovelluksen avulla haastateltavan luvalla. Tämän jälkeen haastattelun olennaisimmat kohdat litteroitiin, eli muutettiin kirjalliseen muotoon, jonka jälkeen näitä analysoitiin. Haastattelun teemarakenteen ansiosta vastaukset saatiin loogisessa järjestyksessä, jota käytetään myös tässä kappaleessa johdonmukaisen analyysin tuottamiseksi. Haastattelu lähti liikkeelle siitä, miten asetukseen on valmistauduttu. Toinen teema koski henkilökunnan näkökulmaa, ja kolmannessa tarkasteltiin vaikutuksia asiakkaaseen. Viimeiseen teemaan valitut kysymykset olivat sellaisia yleisluonteisia kysymyksiä, jotka eivät suoranaisesti sopineet mihinkään toiseen teemaan.

5.1 Valmistautuminen tietosuoja-asetukseen

Tietosuoja-asetukseen valmistautuminen on sisältänyt muun muassa uuden asianhallintaan liittyvän järjestelmän käyttöönoton.

”Organisaatiossa on otettu uusi järjestelmä käyttöön, joka liittyy asianhallintaan. Organisaatiossa seurataan esimerkiksi rekisteröityjen pyyntöjä ja sen käsittelyä tämmöisellä erillisellä asianhallintajärjestelmällä, jotta me pystytään olla varmoja siitä, että toteutetaan rekisteröityjen mahdolliset pyynnöt määräajassa”.

Asianhallintaan liittyvää järjestelmää käytetään siis rekisteröityjen asioiden hoitamiseen, eli järjestelmä toimii myös asiakaspalvelun apuna, jotta mahdollisiin tarpeisiin pystytään vastaamaan tehokkaasti. Myös vaikutustenarviointia varten on otettu käyttöön uusi työkalu. Tietosuoja edellyttääkin jatkuvaa ennakointia ja aktiivisuutta, sillä jälkeenpäin korjaamisen kustannukset voivat nousta suuriksikin,

esimerkiksi sakkorangaistuksen takia. Tietosuoja- asetukseen valmistautuminen aloitettiin alun perin jo vuonna 2012, jolloin Euroopan Komissio ensimmäisen kerran asiasta esitti, mutta varsinaisten muutosten toteuttaminen sitä varten aloitettiin 2016.

”Kyseessä yleinen lainsäädäntö, joka soveltuu käytännössä jokaisen yrityksen toimintaan, niin asioiden selvittämisen ja tekemisen laajuus on aika toiminnallinen haaste. Varmaan suurin haaste on tekemisen laajuus, että kaikki ymmärtävät, mitä tehdään. Tämä ei ole mikään pistemäinen juttu mikä vaikuttaa vain johonkin kulmaan organisaatiossa, vaan koko organisaation asia”.

Tietosuoja-asetus vaikuttaa siis kokonaisvaltaisesti jokaiseen organisaation osa-alueeseen, jolloin henkilöstön kouluttaminen tietosuoja-asetukseen edellyttää organisaatiolta paljon. Organisaation johdolla on tärkeä tehtävä siinä, että viesti saadaan menemään perille jokaiselle yksilölle. Andreasson et al. (2017) esittävät, että henkilöstön tietosuojakoulutukseen panostaminen maksaa itsensä takaisin esimerkiksi kustannussäästöjen kautta. Vaatimukset ovat kovat erityisesti organisaatioissa, joissa on paljon henkilöstöä ja paljon erilaisia työtehtäviä, sillä asetus vaikuttaa eri tehtävissä eri tavalla. Tällaisissa suurissa organisaatioissa ei ole mahdollista, että tietosuojavastaava juoksee yksin henkilöltä toiselle tarjoamassa yksityiskohtaista koulutusta, vaan tietosuojakoulutus tulee organisoida tehokkaasti niin, että niin henkilöstö kuin organisaatiokin saavat koulutuksesta parhaan mahdollisen hyödyn. Kuusela (2015) esittääkin, että henkilöstön osaamisen kautta organisaatio kykenee saavuttamaan päämääränsä. Tietosuojan ja -turvan kannalta osaamisen tulee olla kuitenkin jokaisen henkilöstön jäsenen asia, sillä organisaatio on vain niin vahva kuin sen heikoin lenkki.

5.2 Vaikutukset henkilöstön ja asiakkaan näkökulmasta

Henkilöstön kouluttaminen on tapahtunut kaikille pakollisen verkkokoulutuksen kautta, jonka lisäksi myös henkilön työtehtävien mukaista koulutusta erikseen työtehtävästä riippuen. Kouluttamisessa on huomioitu myös kehitysorganisaation kouluttaminen kehityksenohjausmalliin, jolla pyritään parantamaan tietoutta siitä, mitä kehittäjien tulee huomioida tietosuoja-asioissa. Koulutus sisältää siis niin sanotun yleiskoulutuksen sekä muut tehtäväkohtaiset koulutukset, ja koulutusta on tarjottu myös kumppaneille oman henkilöstön lisäksi. Andreasson et al. (2017) käyttävät

tämän kaltaisesta tietosuojaosaamisen kehittämisestä termiä työelämäinnovointi, jonka avulla yritys pystyy lisäämään työntekijöidensä osaamista ja oikeusturvaa, mikä voi parhaillaan johtaa tuottavuuden lisääntymiseen sekä säästöihin kustannuksissa.

Varmistuakseen siitä, että asetuksen mukaisia vaatimuksia noudatetaan, toteutetaan organisaatiossa muun muassa toimintaa tarkastelemalla ja erillisillä tarkastuksilla. Nämä eivät kuitenkaan tule organisaatioon uutena asiana, vaan sisäisen tarkastuksen prosessit ovat olleet käytössä jo ennestään, ja jatkossa niitä voidaan soveltaa myös tietosuojaan. Tietosuoja-asetus tulee näkymään myös asiakkaan näkökulmasta, mikä perustuu esimerkiksi läpinäkyvyyden periaatteeseen ja kattavaan informointiin. Asiakasta pyritään palvelemaan tietosuojan osalta kaikkien kanavien kautta.

”*Välttämättä se ei vaikuta niin paljon henkilöön, joka asioi pankkikonttorissa. Ei se varmaan siinä palveluprosessissa tule niin hirveästi näkymään se muutos. Ehkä se näkyy enemmän sähköisissä kanavissa ja siinä minkälaista tietoa me tuotetaan”.*

Verkkopalvelussa on julkaistu uusi työkalu asiakastietojen ja omien suostumusten hallinnointiin, joka tarjoaa asiakkaalle mahdollisuuden käydä tarkastelemassa omia asiakirjojaan, ja korjata joltakin osin omia tietojaan. Asiakkaita on osallistettu prosessiin esimerkiksi kyselemällä heiltä sellaisia asioita, joita asiakkaat itse haluaisivat nähdä näissä palveluissa. Palveluiden rakentamisessa on siis ollut käyttäjälähtöisyys suuressa osassa. Kuten kappaleessa 3 esitettiin (Wilde 2011), on asiakkaan osallistaminen palveluiden suunnitteluun yksi merkittävä osoitus korkeasta keskinäisen luottamuksen tasosta. Haastateltavan organisaatiossa tämä taso on selvästi saavutettu.

Asiakkaalta aiemmin kerätty tieto tulee analysoida ja varmistua siitä, että käsittelyperuste löytyy. Pääkäsittelyperusteena on kuitenkin sopimus asiakkaan kanssa, jolla tietojen käsittely oikeutetaan. Asetuksen (2016/679) mukaan sopimus ja/tai suostumus ovat perusteita henkilötietojen lainmukaiselle käsittelylle, kuten kappaleessa kolme esitettiinkin. Uusia suostumuksia aikaisemmin tehtyihin sopimuksiin ei siis tarvita, mutta jatkossa esimerkiksi uusien palveluiden tai tuotteiden osalta katsotaan vaatimuksia tarpeen tullen uudestaan.

5.3 Haasteet valmistautumisprosessissa

Suurin haaste riittävän tietosuojan ylläpitämisessä on haastateltavan mukaan seuraava:

”*Varmasti se vaatimus siitä sisäänrakennetusta ja oletusarvoisesta tietosuojasta, se on varmaan se haastavin, millä tavalla, sillä se edellyttää ihmisten jatkuvaa kouluttamista ja tietoisuuden lisäämistä, että jokainen it-järjestelmien suunnittelija osaa ottaa ne vaatimukset huomioon”.*

Tuote- ja palvelukehitys edellyttää siis jatkuvaa valppautta ja aktiivisuutta esimerkiksi järjestelmiä koodatessa. Tietosuoja-asetuksen edellyttämien vaatimusten tunteminen tulee siis olla jokaisella asiaa koskevalla henkilöllä. Limnéll (2015) esittää, että turvallisuuden tulee olla näissä asioissa sisäänrakennettuna aina palveluista järjestelmiin. Jos tietoja joudutaan siirtämään paikasta toiseen, esimerkiksi luovuttamaan niitä kolmannelle osapuolelle, seurataan tarkasti lainsäädännön vaatimuksia siitä, että tiedot pysyvät suojattuina koko ajan. Tällöin tietoturvan rooli nouseekin esille. Tässä on pohjana olennaisesti riskiperusteinen arvio, eli tietojen suojaamisen taso tulee vastata tilannetta koskevaa riskiä. Suurimmaksi muutokseksi selvisi toiminnan kokonaisvaltaisuuden lisäksi

”Riskiperusteinen arviointi, mikä tietosuoja-asetuksessa on, edellyttää muutosta toimintakulttuurissa, vaikka aiemminkin on toimittu huolellisesti niin nyt ne riskiarviot tulevat aina tietosuojankin osalta paperille”.

Toimintakulttuurin muutos liittyy siihen, että henkilöstö ymmärtää tietosuoja-asioiden periaatteet ja ymmärtävät, millä tavalla se heidän omaan työnkuvaansa vaikuttaa ja millä tavoin siitä kuuluu raportoida. Andreasson et al. (2017) mainitsevat puutteet tietosuojaosaamisessa sellaiseksi tekijäksi, joka voi pahimmillaan johtaa asiakastyytymättömyyteen tai jopa sakko- tai vankeusrangaistukseen.

6 Yhteenveto ja johtopäätökset

Tässä kandidaatintutkielmassa keskityttiin tutkimaan Euroopan Unionin toukokuussa voimaan astuvan tietosuoja-asetuksen vaikutuksia pankkialaan Suomessa. Tutkielman teoriaosuudessa tarkasteltiin niin tietosuojan tämän hetkistä tilannetta eri lakien ja muiden siihen vaikuttavien seikkojen osalta kuin tulevan tietosuoja-asetuksen erityspiirteitäkin. Näiden lisäksi esitettiin katsaus sellaisiin tietoihin, joita pankkien tietosuojalla ja –turvalla pyritään suojaamaan, sekä mihin tarkoitukseen pankit näitä tietoja tarvitsevat. Teoriaosuudessa esitettiin myös muita tietosuoja-asetusta käsitteleviä tutkimuksia sekä analysoitiin näiden tuloksia, jotta niitä voidaan verrata tämän tutkimuksen empiriaosuudessa toteutettuun teemahaastatteluun. Tutkimusongelmaa lähestyttiin kolmen alatutkimusongelman kautta, joista ensimmäinen oli

Minkälaisia järjestelmiä hyödynnetään, jotta tietosuoja-asetuksen asettamiin vaatimuksiin pystytään vastaamaan?

Tietosuoja-asetus tulee edellyttämään yritykseltä yhtenäisiä ja kokonaisvaltaisia käytäntöjä ja toimintamalleja, joten asetuksen vaatimuksiin vastaamisen avuksi on otettu käyttöön uudenlaisia järjestelmiä ja työkaluja. Näistä keskeisimmäksi nousivat asianhallintajärjestelmä ja vaikutustenarviointiin käytettävä työkalu. Asianhallintajärjestelmän avulla rekisteröidyn tarpeisiin pystytään reagoimaan tehokkaammin ja näin kehittämään asiakaspalvelua. Erilaisten IT-järjestelmien suunnittelussa tulee jatkossa myös huomioida vaatimus sisäänrakennetusta ja oletusarvoisesta tietosuojasta, jotta järjestelmä täyttää edellytetyt vaatimukset.

Toisen alatutkimusongelman avulla pyrittiin kartoittamaan vaikutuksia asiakkaan näkökulmasta, ja tutkimusongelma muotoiltiin seuraavalla tavalla

Millä tavalla tietosuoja-asetuksen aiheuttamat muutokset tulevat näkymään asiakkaille?

Asiakkaan näkökulmasta vaikutukset eivät tule ainakaan selvästi näkyvin osin esille, sillä esimerkiksi perinteisessä asiakastapaamisessa tietosuoja-asetus ei tuo muutoksia jo aiemmin käytettyihin toimintatapoihin. Kuitenkin esimerkiksi toiminnan läpinäkyvyys perustuu asiakkaan näkökulmaan, sillä se lisää keskinäistä luottamusta,

kun erilaiset toimenpiteet tehdään yrittämättä piilotella niitä asiakkaalta. Verkkopalvelussa vaikutukset ovat kuitenkin selvemmin näkyvissä. Asiakkaat pystyvät hallinnoimaan ja joiltain osin päivittämään ja korjaamaan omia tietojaan. Asiakkaita on myös osallistettu näiden palveluiden suunnitteluun, jolloin palveluista on saatu niin hyvin asiakkaiden tarpeita palveleva, kuin mahdollista. Kolmas, ja viimeinen, alatutkimusongelma valikoitui sen perusteella, että aiempien tutkimusten tulosten mukaan suurimmat vaikutukset tietosuoja- asetukseen valmistautumisessa liittyvät nimenomaan henkilöstöön ja henkilöstön osaamiseen. Viimeinen alatutkimusongelma onkin

Miten yritysten henkilökunta perehdytetään tietosuoja-asetuksen aiheuttamiin muutoksiin?

Organisaation henkilöstön kouluttaminen on tapahtunut ikään kuin kaksivaiheisesti. Jokaiselle työntekijälle on pidetty yhteinen verkkokoulutus, jonka lisäksi annetaan eri tehtävissä työskenteleville tehtäväkohtaista koulutusta. Tämän lisäksi myös kehitysorganisaatiota on koulutettu niin, että he osaavat huomioida, minkälaisia asioita tietosuoja-asioissa täytyy toteuttaa. Henkilöstön osaamisesta varmistuakseen organisaatiossa toteutetaan toiminnan tarkastelua yleisellä tasolla sekä erillisillä tarkastuksilla. Tämän kaltaiset sisäisen valvonnan mallit ovat kuitenkin olleet organisaatiossa jo ennestään, mutta niitä voidaan jatkossa soveltaa myös tietosuoja-asioissa.

Tutkimuksen päätutkimusongelmaan löytyi vastaus sekä alatutkimusongelmien että muiden haastattelussa ilmenneiden seikkojen kautta. Suurimmat vaikutukset pankkialalla tulevat liittymään henkilöstöön ja sen toimintaan, kuten aiemmissakin saman kaltaisissa tutkimuksissa todettiin. Henkilöstön kokonaisvaltainen kouluttaminen uuden asetuksen mukana tuleviin vaatimuksiin tulee vaatimaan organisaatiolta panostuksia ja henkilöstöltä valmiutta ottaa tietosuoja-asiat osaksi osaamistaan. Koulutuksen tuomat kustannukset maksavat kuitenkin itsensä takaisin siinä vaiheessa, kun uudet toimintamallit ovat kiinteä osa organisaatiota. Toinen merkittävä vaikutus näkyy riskiperusteisen arvioinnin käyttöönotossa, jossa jokaisen toiminnan riski tulee arvioida etukäteen, jotta siihen voidaan vastata tarpeeksi tehokkailla suojakeinoilla. Vaikka vaikutus onkin eniten näkyvillä organisaation sisällä, ei tule unohtaa, että kaikki toimenpiteet tehdään henkilön, eli asiakkaan,

suojaamiseksi. Tästä näkökulmasta katsottuna suurimmat vaikutukset kohdistuvat sittenkin asiakkaaseen. Jatkotutkimuksia ajatellen työtä voidaan käyttää pohjana tietosuoja-asetuksen muita osa- alueita tutkittaessa, tai tutkittaessa sen vaikutuksia johonkin toiseen toimialaan. Tutkimus voisi toimia perustana myös tietosuoja-asetuksen tutkimiselle sen jälkeen, kun asetus on ollut voimassa jo jonkin aikaa. Jatkotutkimukset voisivat kohdistua myös tietosuoja-asetukseen tietoturvan näkökulmasta.

Lähdeluettelo

Aalto-Setälä, M. (2016) EU:n tietosuoja-asetus tulee - valmistaudu ajoissa. [Verkkodokumentti]. [Viitattu 17.3.2018]. Saatavilla https://kauppakamari.fi/2016/03/31/eun- tietosuoja-asetus-tulee-valmistaudu-ajoissa/

Albrecht, J. P. (2016) How the GDPR will change the world. [Verkkodokumentti]. [Viitattu 27.4.2018]. Saatavilla https://edpl.lexxion.eu/data/article/10073/pdf/edpl_2016_03-005.pdf

Andreasson, A., Koivisto, J. & Ylipartanen, A. (2017) Tietosuojakäsikirja johdolle. 2. p. Helsinki, Tietosanoma Oy.

Cohen, L. & Manion, L. (1995) Research methods on education. 4. Edition. London, Routledge.

EU GDPR Portal (2018) General data protection regulation. [Verkkodokumentti]. [Viitattu 10.3.2018]. Saatavilla https://www.eugdpr.org/eugdpr.org.html

Euroopan komissio (2016) Standard eurobarometer 86. Media use in the European Union. [Verkkodokumentti]. [Viitattu 4.3.2018]. Saatavilla https://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/ResultDoc/.../64573

Euroopan parlamentin ja neuvoston asetus 2001/45 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. Annettu Brysselissä 18.12.2001

Euroopan parlamentin ja neuvoston direktiivi 2002/58 (sähköisen viestinnän tietosuojadirektiivi). Annettu Brysselissä 12.7.2002

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

Euroopan Unioni (2018) EU:n tavoitteet ja arvot. [Verkkodokumentti]. [Viitattu 18.3.2018]. Saatavilla https://europa.eu/european-union/about-eu/eu-in-brief_fi

EY (2016) The Relevance Challenge. What retail banks must do to remain in the game. [Verkkodokumentti]. [Viitattu 20.3.2018]. Saatavilla http://www.ey.com/Publication/vwLUAssets/ey-the-relevance-challenge/$FILE/ey-the- relevance-challenge-2016.pdf

Finanssialan keskusliitto (2009) Pankkisalaisuusohjeet. [Verkkodokumentti]. [Viitattu 30.3.2018]. Saatavilla http://www.finanssiala.fi/materiaalit/Pankkisalaisuusohjeet.pdf#search=pankkisalaisuus

Finanssialan keskusliitto (2015) Hyvä pankkitapa. [Verkkodokumentti]. [Viitattu 30.3.2018]. Saatavilla http://www.finanssiala.fi/materiaalit/Hyva_pankkitapa.pdf

Findwise (2018) Mitä jokaisen kuuluu tietää EU:n uudesta tietosuoja-asetuksesta GDPR? [Verkkodokumentti]. [Viitattu 28.3.2018]. Saatavilla https://findwise.com/en/gdpr-fi

Hakonen, P. (2017) Henkilötietojen turvallisen käsittelyn toteutuminen EU:n tietosuoja-asetuksen vaatimusten mukaisesti. Opinnäytetyö. Tampere, Tampereen ammattikorkeakoulu, liiketalouden koulutusohjelma, oikeudellinen asiantuntijuus.

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. (2017) Henkilötietojen käsittely – EU-tietosuoja-asetuksen vaatimukset. [Verkkodokumentti]. [Viitattu 19.3.2018]. Saatavilla https://kauppakamaritieto-fi.ezproxy.cc.lut.fi/fi/s/ak/kirjat/henkilotietojen-kasittely-eu- tietosuoja-asetuksen-vaatimukset-2017/?coll=4

Henkilörekisterilaki 1987/471. Annettu Helsingissä 30.4.1987 Henkilötietolaki 1999/523. Annettu Helsingissä 22.4.1999

Häkkinen, J. (2017) Tietosuoja työsuhdetietojen ja palkanlaskennan näkökulmasta. Opinnäytetyö. Lappeenranta, Saimaan ammattikorkeakoulu, liiketalouden koulutusohjelma, laskentatoimi.

Jaakohuhta, H. (2003) Tietojärjestelmien luotettavuus. Helsinki, Edita IT Press. Johnson, M. E. (2018) A broader context for information security. [Verkkodokumentti]. [Viitattu 22.3.2018]. Saatavilla http://www.ists.dartmouth.edu/library/159.pdf

Järvinen, P. & Rousku, K. (2017) Työpaikan tietoturvaopas – tunnista uhat, hallitse riskit. Helsinki, Alma Talent.

Kirsi, K. (2012) Pankissa kysytään: oletko poliittisesti vaikutusvaltainen? [Verkkodokumentti]. [Viitattu 9.4.2018]. Saatavilla https://yle.fi/uutiset/3-6396183

Kontkanen, E. (2011) Pankkitoiminnan käsikirja. 3. uud. p. Helsinki, Finanssi- ja vakuutuskustannus Oy.

Kuusela, S. (2015) Organisaatioelämää. Kulttuurin voima ja vaikutus. Helsinki, Alma Talent Oy.

Laine, R. O. & Lecklin, O. (2009) Laadunkehittäjän työkalupakki – Innovatiivisen johtamisjärjestelmän rakentaminen. Helsinki, Talentum.

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 2009/617. Annettu Helsingissä 7.8.2009

Lehtola, S. (2016) Uusi EU:n tietosuoja-asetus astuu voimaan 25.5.2018 – Ketä se koskee ja mitkä ovat sen keskeisimmät muutokset? [Verkkodokumentti]. [Viitattu 15.3.2018]. Saatavilla https://www.emce.fi/blog/uusi-eun-tietosuoja-asetus-astuu-voimaan-25-5-2018- keta-koskee-mitka-keskeisimmat-muutokset/

Limnéll, J. (2015) Digitaalinen turvallisuus kilpailuetuna. [Verkkodokumentti]. [Viitattu 9.4.]. Saatavilla https://digitalist.global/talks/digitaalinen-turvallisuus-kilpailuetuna/

Luottotietolaki 2007/527. Annettu Helsingissä 11.5.2007

Metsämuuronen, J. (2005) Tutkimuksen tekemisen perusteet ihmistieteissä. Jyväskylä, Gummerus.

Metsämuuronen, J. (2006) Tutkimuksen tekemisen perusteet ihmistieteissä. Jyväskylä, Gummerus.

Nauwelaerts, W. (2017) GDPR – The perfect privacy storm: You can run from the regulator, but you cannot hide from the consumer. [Verkkodokumentti]. [Viitattu 27.4.2018]. Saatavilla http://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl3&div=46&id=&page=

Nordea (2016) Miksi ja mitä tietoja pankki kyselee? [Verkkodokumentti]. [Viitattu 8.4.2018]. Saatavilla https://www.nordea.com/fi/media/uutiset-ja-lehdistotiedotteet/News- fi/2016/2016-11-24-miksi-pankki-kysyy-tietoja.html

Nordea (2018) Yhteenveto Nordeasta. [Verkkodokumentti]. [Viitattu 2.4.2018]. Saatavilla https://www.nordea.com/fi/tietoa-nordeasta/keita-olemme/Yhteenveto-Nordeasta/

Oikeusministeriö (2017) Miten valmistautua tietosuoja-asetukseen? [Verkkodokumentti]. [Viitattu 2.4.2018]. Saatavilla http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/o ppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

OP (2018) Henkilötieto. [Verkkodokumentti]. [Viitattu 8.4.2018]. Saatavilla https://uusi.op.fi/tietosuoja/henkilotieto

OP (2018) Osuustoiminta. [Verkkodokumentti]. [Viitattu 2.4.2018]. Saatavilla https://uusi.op.fi/op-ryhma/tietoa-ryhmasta/osuustoiminta

Opsec Oy (2017) Tietosuoja. [Verkkodokumentti]. [Viitattu 8.3.2018]. Saatavilla https://www.tietosuojakuntoon.fi/tietosuojatietoturva.html

Oikeusministeriö (2017) Miten valmistautua tietosuoja-asetukseen? [Verkkodokumentti]. [Viitattu 2.4.2018]. Saatavilla http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/o ppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Paajanen, E. (2017) Tietosuoja-asetuksen vaikutukset organisaatioihin ja Amazon web services –pilvipalvelualustan tuomat hyödyt. Diplomityö. Lappeenranta, Lappeenrannan teknillinen yliopisto, innovaatio- ja teknologiajohtaminen.

Partanen, H. (2014) Julkaisussa: Viestintäoikeus nyt: Viestintäoikeuden vuosikirja. [Verkkodokumentti]. [Viitattu 15.3.2018]. Saatavilla https://www.edilex.fi/artikkelit/17004.pdf

Purtova, N. (2018) The law of everything. Broad concept of personal data and future of EU data protection law. [Verkkodokumentti]. [Viitattu 27.4.2018]. Saatavilla https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176?scroll=top&needAccess=true

Rainer, R. K. & Prince, B. (2015) Introduction to information systems. 6. Edition. Hoboken, Wiley.

Rose, J., Barton, C., Souza, R. & Platt, J. (2013) The Boston Consulting Group. The trust advantage. [Verkkodokumentti]. [Viitattu 6.4.2018]. Saatavilla http://www2.stat-athens.aueb.gr/~jpan/Rose-2013.pdf

Shaw, C., Dibeehi, Q. & Walden, S. (2010) Customer Experience. Future Trends and Insights. New York, Palgrave Macmillan

Sinun Eurooppasi (2018) Rahoitustuotteet ja palvelut. [Verkkodokumentti]. [Viitattu 25.3.2018]. Saatavilla https://europa.eu/youreurope/citizens/consumers/financial-products- and-services/bank-accounts-eu/index_fi.htm

Suomen perustuslaki 1999/731. Annettu Helsingissä 11.6.1999

Suomen virallinen tilasto (SVT): Tietotekniikan käyttö yrityksissä [verkkojulkaisu]. ISSN=1797-2957. 2012, 5. Liiketoiminnan sähköistyminen. Helsinki: Tilastokeskus [viitattu: 10.4.2018]. Saatavilla http://www.stat.fi/til/icte/2012/icte_2012_2012-11-27_kat_005_fi.html

Suomen virallinen tilasto (SVT): Tietotekniikan käyttö yrityksissä [verkkojulkaisu]. ISSN=1797-2957. 2017, 5. Liiketoiminnan sähköistyminen. Helsinki: Tilastokeskus [viitattu: 10.4.2018]. Saatavilla http://www.stat.fi/til/icte/2017/icte_2017_2017-11-30_kat_005_fi.html

Syrjälä, L. (1994) Tapaustutkimus opettajan ja tutkijan työvälineenä. Laadullisen tutkimuksen työtapoja. Rauma, Kirjapaino Westpoint Oy, Kirjayhtymä Oy.

Tietosuojamalli (2017) Oikeus käsittelyn rajoittamiseen. [Verkkodokumentti]. [Viitattu 16.3.2018]. Saatavilla https://fakta.tietosuojamalli.fi/gdpr-asetus/18-oikeus-kasittelyn-rajoittamiseen

Tietosuojavaltuutetun toimisto (2013) Henkilötietolaki. [Verkkodokumentti]. [Viitattu 21.3.2018]. Saatavilla http://www.tietosuoja.fi/fi/index/lait/Henkilotietolaki.html

Tietosuojavaltuutetun toimisto (2013) Henkilötietolain taustaa. [Verkkodokumentti]. [Viitattu 21.3.2018]. Saatavilla http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/henkilotietolaintaustaa.html

Tietosuojavaltuutetun toimisto (2014) Erityislainsäädäntö. [Verkkodokumentti]. [Viitattu 21.3.2018]. Saatavilla http://www.tietosuoja.fi/fi/index/lait/erityislainsaadanto.html

Tietosuojavaltuutetun toimisto (2017) Pankkitoiminta. [Verkkodokumentti]. [Viitattu 16.3.2018]. Saatavilla http://www.tietosuoja.fi/fi/index/useinkysyttya/pankkitoiminta.html

Tietosuojavaltuutetun toimisto (2018) EU:n tietosuojauudistus. [Verkkodokumentti]. [Viitattu 10.3.2018]. Saatavilla http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Tilli, S. (2002) Kirjanpidon luotettavuus. Pro gradu -tutkielma. Lappeenranta, Lappeenrannan teknillinen korkeakoulu, kauppatieteiden osasto.

Valtiovarainministeriö (2016) EU-tietosuojan kokonaisuudistus. VAHTI-raportti. [Verkkodokumentti]. [Viitattu 4.4.2018]. Saatavilla https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Viestintävirasto (2017) Vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne. [Verkkodokumentti]. [Viitattu 1.4.2018]. Saatavilla https://www.viestintavirasto.fi/kyberturvallisuus/sahkoinentunnistaminenjaallekirjoitus.html

von Solms, S. H. & von Solms, R. (2009) Information security governance. [Verkkodokumentti]. [Viitattu 24.3.]. Saatavilla https://link-springer-com.ezproxy.cc.lut.fi/content/pdf/10.1007%2F978-0-387-79984-1.pdf

Väisänen, T. (2015) EU:n yleinen tietosuoja-asetus ja sen vaikutukset Oulun Ammattikorkeakoulu Oy:ssä. Opinnäytetyö. Oulu, Oulun ammattikorkeakoulu, Liiketalouden koulutusohjelma.

Wilde, S. (2011) Customer Knowledge Management. Improving Customer Relationship through Knowledge Application. [Verkkodokumentti]. [Viitattu 5.4.2018]. Saatavilla https://link-springer-com.ezproxy.cc.lut.fi/content/pdf/10.1007%2F978-3-642-16475-0.pdf

Williams, D.K. (2013) The most valuable business commodity: trust. [Verkkodokumentti]. [Viitattu 7.4.2018]. Saatavilla https://www.forbes.com/sites/davidkwilliams/2013/06/20/the- most-valuable-business-commodity-trust/#3b1487616500

Liite 1. Haastattelun kysymykset

Taustat

Titteli ja yritys

Työtehtävät ja vastuualueet

Aihealue 1. Valmistautuminen tietosuoja-asetukseen

Onko uuteen tietosuoja-asetukseen valmistautunut edellyttänyt uusien järjestelmien käyttöönottoa? Jos kyllä, niin minkälaisten? (Tarkistus: nimenomaan tietojärjestelmien)

Milloin valmistautuminen alkoi? Minkälaisia haasteita valmistautumisprosessissa on ilmennyt?

Aihealue 2. Henkilökunta

Minkälaista koulutusta henkilökunnalle on annettu/tullaan antamaan tietosuoja-asetukseen liittyen?

Minkälaisia keinoja käytetään, että henkilökunta saadaan noudattamaan asetettuja vaatimuksia?

Aihealue 3. Asiakkaan näkökulma

Miten uskotte, että asetus tulee näkymään asiakkaalle face-to-face –tapaamisissa? (Tarkennus: muuttuuko tapaamisissa jokin? Tarvitaanko enemmän lupia?) Entä mobiili- tai verkkopankissa?

Miten asetus vaikuttaa asiakkailta jo kerättyihin tietoihin? Tuleeko niihin muutoksia? Vaaditaanko lisää lupia/suostumuksia?

Aihealue 4. Järjestelmät

Mikä on ollut / tulee olemaan haastavinta riittävän tietosuojan ylläpitämisessä?

Jos tietoja joudutaan siirtämään paikasta tai järjestelmästä toiseen, miten saadaan

varmistuttua siitä, että tietosuoja pysyy koko ajan vaaditulla tasolla? (Tarkennus: esimerkiksi luovuttaessa tietoja kolmannelle osapuolelle?)

Mitkä ovat mielestänne merkittävimmät pankkialaan kohdistuvat muutokset / velvoitteet?