Opinnäytetyö (AMK)

Liiketalouden koulutusohjelma

Juridiikka

2017

Jutta Tammelin

ASIAKKAAN HENKILÖTIETOJEN SUOJA PANKKITOIMINNASSA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalous | Juridiikka

2017 | 42

Jutta Tammelin

ASIAKKAAN HENKILÖTIETOJEN SUOJA PANKKITOIMINNASSA

Tämän opinnäytetyön tavoitteena on kartoittaa ja havainnollistaa henkilötietojen suojan tämän hetkistä lainsäädäntöä ja tutkia henkilötietojen suojaan liittyvän sääntelyn vaikutusta toimeksiantajayrityksen työntekijöiden toimintaan asiakkaan henkilötietojen käsittelyn osalta. Henkilötietojen suojan sääntelyä tarkastellaan henkilötietolain ja sähköisen viestinnän tietosuojalain kautta.

Henkilötietojen suojan sääntely on lisääntynyt ja tiukentunut viime vuosien aikana. Yksi suurimmista syistä lisääntyneeseen sääntelyyn on nykyteknologia, joka mahdollistaa yhä suurempien henkilötieto määrien tallentamisen ja hallinnoinnin. Nykyinen sääntely vaatii yrityksiltä yhä enemmän tarkkuutta ja avoimuutta.

Opinnäytetyön teoriaosassa tiivistetään ja havainnollistetaan henkilötietolain sääntelyä. Teoriaosassa käsitellään henkilötietolain keskeiset käsitteet, henkilötietojen käsittelyä koskevat yleiset periaatteet, rekisteröidyn oikeudet sekä arkaluontoiset tiedot.

Työn toimeksiantaja toimii suomalainen finanssi- ja rahoitusalan yritys, joka kerää, käsittelee ja tallettaa toiminnassaan päivittäin suuria määriä henkilötietoja. Osa tiedoista on arkaluontoisia. Työn empiirisessä osassa pyritään toimeksiantajayrityksen työntekijöitä haastattelemalla saamaan kokonaiskuva, kuinka hyvin yrityksen työntekijät tuntevat tämän hetkisen henkilötietojen suojaan liittyvän sääntelyn ja miten se vaikuttaa heidän työhönsä.

Tämän työn ansiosta toimeksiantajayritys saa haastattelututkimuksen kautta tietää työntekijöiden toiveet mahdollisen lisäkoulutuksen suhteen sekä työntekijöiden kehitysehdotukset toimeksiantajayrityksen henkilötietojen suojaan liittyvän käytännön toiminnan osalta.

ASIASANAT:

henkilötietolaki, tietosuoja sähköisessä liiketoiminnassa, tietosuoja, henkilötieto, rekisteröity

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business | Jurisprudence

2017 | 42

Jutta Tammelin

PROTECTION OF CUSTOMER'S PERSONAL DATA IN BANKING BUSINESS

The aim of this thesis is to survey and illustrate the current legislation on the protection of personal data and research the effect of the legislation on the client's employees' actions in their daily work. The legislation on the protection of personal data is examined related to the Personal Data Act and the Act on the Protection of Privacy in Electronic Communications.

The legislation on the protection of personal data has increased and tightened during the past few years. One of the biggest reasons is modern technology which allows to store and administer greater amounts of personal data. The current legislation demands even more exactness and transparency from the companies.

The theoretical part of the thesis summarizes and illustrates the legislation on the protection of personal data. It consists of the central concepts, general principles, rights of the registered and sensitive information in the Personal Data Act.

The client of the thesis is a company that operates in the finance sector. The client company collects, stores, and handles great amounts of personal data daily. Some of the data is sensitive. In the empirical part of the thesis, the aim is to receive a general view of the client's employees´ knowledge of the current legislation on the protection of personal data and what kind of influence the legislation has on their work. This is done by interviewing the employees of the client company.

Due to this thesis, the client is able to find out if the employees would like to have some further training on the protection of personal data as well as the employees´ development suggestions for the practical actions related to the personal data in the workplace.

KEYWORDS:

personal data, data protection, Personal Data Act, the registered

SISÄLTÖ

LIITTEET

KUVIOT

1 JOHDANTO

Tämän opinnäytetyön tavoitteena on kartoittaa henkilötietolain sääntelyä Suomessa vuonna 2017 ja tuoda esille sen roolia nykyajan yritystoiminnassa. Lisäksi tavoitteena on tutkia, kuinka hyvin henkilötietolain sääntely tunnetaan toimeksiantajayrityksen työntekijöiden jokapäiväisessä toiminnassa.

Työn toimeksiantajana toimii suomalainen rahoitus- ja finanssialan yritys, josta käytetään tutkimuksessa nimeä Pankki. Toimeksiantajan työntekijät keräävät, tallettavat ja käsittelevät henkilötietoja jokapäiväisessä työssään. Nykyteknologia mahdollistaa yhä suurimpien henkilötieto määrien tallentamisen, joten pankin työntekijöiltä vaaditaan yhä enemmän tarkkuutta ja osaamista henkilötietojen käsittelyä koskevan sääntelyn suhteen. Työntekijöiden on osattava myös perustella asiakkaalle minkä vuoksi jotakin tiettyä tietoa hänestä pyydetään. Mitä laajemmat tiedot pankilla asiakkaasta on, sitä helpommin pankki pystyy estämään esimerkiksi oikeudettomat nostot asiakkaan tililtä tai asiakkaan pankkikortin väärinkäytökset.

Olen kiinnostunut henkilötietojensuojasta yhä enemmän viimeaikaisen henkilötietojensuojaa koskevan uutisoinnin myötä. Rekisteröidyn suostumus on noussut yhä vahvemmin esille ja ihmiset ovat tulleet tietoisemmaksi oikeuksistaan, jolloin myös asiakasrekisteriä ylläpitävän yrityksen täytyy olla yhä tarkempi ja avoimempi asiakasrekisteriä hallinnoidessaan. Nykypäivänä velvoitteena yrityksille ei ole enää vain henkilötietolaki, vaan myös valistuneemmat kansalaiset ja tätä kautta uhka median aiheuttamasta kohusta. Hyvä, huolellinen ja lainmukainen henkilötietojen käsittely yrityksessä on taas vastavuoroisesti asiakkaalle luotettavuutta ja turvallisuutta lisäävä tekijä.

Olen itse myös työelämässä ja erityisesti pankkityössä käsitellyt monenlaisia henkilötietoja ja saanut kokea käytännön kautta, kuinka paljon vastuuta siihen sisältyy. Erityisesti, kun otetaan huomioon nykypäivän kiihtyvä digitalisaatio. Se asettaa henkilötietojen käsittelylle vielä aivan omat haasteensa. Tämän vuoksi tässä työssä käsitellään myös tietosuojaa sähköisessä liiketoiminnassa, jota suurin osa yrityksistä tämän päivän Suomessa harjoittaa.

Työn empiirisessä osassa tehtävä tutkimus toteutetaan haastattelemalla toimeksiantajayrityksen valitsemia kahden eri pankkikonttorin työntekijöitä. Haastateltavat vastaavat haastatteluun anonyymisti ja saavat ennakkoon tutustua haastattelun kysymyksiin.

Lähteinä työssä käytetään pääasiassa tietosuojalautakunnan internetsivuja ja päätöksiä, henkilötietolakia käsittelevää kirjallisuutta sekä Finlexin tietokantaa. Henkilötietolaista ei ole, muun muassa sen nopeasti muuttuvan kansallisen lainsäädännön vuoksi, kirjoitettu montaa tietokirjaa Suomessa. Lähteenä käytetty kirjallisuus jää siis hieman suppeammaksi, mutta tieto, jota siitä saadaan, on sitäkin arvokkaampaa tälle työlle.

2 HENKILÖTIETOJEN SUOJA SUOMESSA VUONNA 2017

2.1 Henkilötietolaki ja sen soveltamisala

Suomen nykyinen henkilötietolaki (HeTiL) astui voimaan vuonna 1999. Sitä on noudatettava aina henkilötietoja käsiteltäessä. HeTiL on yleislaki, jonka ensimmäisen luvun 1§:n mukaan lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista ja toteuttaa hyvään tietojenkäsittelytapaan perustuva yhtenäinen käytäntö.

Henkilötietolakia koskevan hallituksen esityksen[1] mukaan henkilötietojen käsittelytoimien on ensisijaisesti perustuttava rekisteröidyn suostumukseen. Tämän vuoksi yksi keskeisimmistä tehtävistä HeTiL:n säädännössä onkin osoittaa, milloin tietojen käsittely on mahdollista ilman rekisteröidyn myötävaikutusta.[2]

HeTiL:n 2 §:n mukaan lakia sovelletaan automaattiseen henkilötietojen käsittelyyn sekä myös muuhun henkilötietojen käsittelyyn silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. 2 §:n momentissa 3 lain ulkopuolelle suljetaan kuitenkin henkilötietojen käsittely, jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin.

HeTiL yksi keskeisimmistä säätämisen syistä on pyrkimys löytää ratkaisumalli yksityisyyden suojan ja muiden henkilötietojen käsittelyyn liittyvien intressien välillä. Sen säätämisen tarkoituksena on ollut myös ennalta ehkäistä erityisesti tietotekniikan ja uuden teknologian käyttöön liittyviä tietosuojariskejä.[3]

[1] HE 96/1998.
[2] Vanto 2011, 18.
[3] Tietosuojavaltuutetun toimisto 2013.

2.2 Henkilötietolain keskeiset käsitteet

Tietosuojasta ja tietoturvasta puhuttaessa keskeisiä käsitteitä ovat henkilötieto, henkilötietojen käsittely, henkilörekisteri, rekisteröity sekä rekisterinpitäjä.

Edellä mainituista käsitteistä oleellisin on henkilötieto. HeTiL:n ensimmäisen luvun 3 §:n mukaan henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Olennaista henkilötiedon määritelmän kannalta siis on, onko tietty henkilö tunnistettavissa arvioitavana olevan tiedon perusteella. Täysin anonyymit tiedot eivät ole laissa tarkoitettuja henkilötietoja, mikäli niiden yhdistäminen tiettyyn henkilöön ei mitenkään ole mahdollista. Tämänkaltaisten anonyymien tietojen käsittely ei ole tietosuojalainsäädännön tarkoittamaa henkilötietojen käsittelyä. [4]

Heini Nurmi mainitsee tutkielmassaan[5], että henkilötiedon määritelmän täyttääkseen tiedon tulisi olla jollekin alustalle tallennettuna. Henkilötieto voi siis yhtä hyvin olla kynällä paperille kirjoitettu tieto, kuin koneellisesti tai sähköisesti tallennettu tieto. Henkilötiedoksi voidaan katsoa myös pankki asiointi puhelimitse, kuten myös videovalvonta.

Henkilötietojen käsittelyllä taas tarkoitetaan HeTiL:n ensimmäisen luvun 3 §:n mukaan: Henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä.

Omat erikoistilanteensa henkilötiedon määrittelyyn tuovat tilanteet, joissa henkilö, jonka henkilötietoja käsitellään ei ole enää valvomassa oikeuksiaan heikon terveydentilan, mielisairauden tai kuoleman johdosta.

Tietosuojalautakunta on antanut päätöksen[6] jutussa, jossa tietosuojalautakunta kielsi Memorium Oy:tä henkilötietolain vastaisesti käsittelemästä hautakivistä ilmeneviä hen-

[4] Virtuaalilakimies 2017.
[5] Nurmi 2008, 10.
[6] Tietosuojalautakunta 2008.

kilötietoja avoimessa tietoverkossa, jos henkilön kuolemasta on kulunut 25 vuotta tai vähemmän eikä rekisteröidyn tai hänen oikeudenomistajiensa suostumusta tietojen automaattiseen käsittelyyn ole hankittu.

> Henkilötietolaissa ei nimenomaan säädetä kuolleita henkilöitä koskevien tietojen käsittelystä. Lain soveltamiskäytännössä on kuitenkin katsottu, että henkilötiedon määritelmä sinänsä kattaa myös kuollutta henkilöä koskevat tiedot ja että henkilötietolain tarkoituksena on suojata henkilön itsensä lisäksi myös hänen muistoaan ja omaisiaan. Henkilötietolaki voikin tulla sovellettavaksi kuolleita henkilöitä koskevien tietojen käsittelyyn myös sillä perusteella, että kyseisten tietojen voidaan samalla katsoa koskevan tunnistettavissa olevia eläviä henkilöitä ja heidän yksityisyyttään. Henkilötietolain turvaaman yksityisyyden suojan tarpeen voidaan kuitenkin katsoa vähenevän, kun kysymys on tiedoista, jotka koskevat kauan sitten kuolleita. Arvioitaessa yksityisyyden suojan ajallista ulottuvuutta kuolleita koskevien tietojen osalta voidaan muussa lainsäädännössä olevia salassapitosäännöksiä pitää suuntaa-antavina. Yksityisyyden suojan tarvetta ja siten lain ajallista ulottuvuutta arvioitaessa on otettava huomioon myös käsiteltävien tietojen laatu.

Henkilörekisteri puolestaan on HeTiL:n 3 §:n mukaan:

> Käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta.

Rekisterinpitäjällä taas tarkoitetaan samassa artiklassa yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty. Rekisteröity puolestaan merkitsee yksinkertaisesti henkilöä, jota henkilötieto koskee.

2.3 Yksityisyyden suoja

Henkilötietojen suoja on nykyään ymmärretty melko vakiintuneesti osaksi yksityiselämän suojaa.[7] Tämän vuoksi yksityisyyden suojan käsite saa tässä työssä oman alalukunsa, jotta sen liitännäisyys henkilötietolakiin olisi helpompi käsittää. Yksityisyyden suojaan vaikuttavat lait ovat henkilötietolaki, laki viranomaisten toiminnan julkisuudesta, laki yksityisyyden suojasta työelämässä, tietoyhteiskuntakaari ja EU:n direktiivit.[8]

Oikeus yksityisyyden suojaan on Suomen perustuslain turvaama oikeusjärjestyksen suojelema etu.[9] Perustuslain 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Lisäksi perustuslain 10 § sisältää yksityiselämän suojaa koskevan yleislausekkeen (1. momentti), jonka mukaan yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä.

Valtiolta on yksityiselämän suojaamiseksi perinteisesti edellytetty, että se itse pidättäytyy loukkaamasta ihmisten yksityiselämää ja tämän lisäksi toteuttaa aktiivisia toimenpiteitä yksityiselämän suojaamiseksi toisilta tahoilta tulevilta uhkaavilta loukkauksilta.[10] Tämä pyritään toteuttamaan perusoikeuksien horisontaalisuhteisiin vaikuttavalla lainsäädännöllä.[11] Yksityisyydensuojan kannalta onkin pidetty merkityksellisenä esimerkiksi henkilöön kohdistettavia erilaisia valvonta- ja tarkkailuvaltuuksia.[12]

Perustuslain 10 §:n momentti 2 antaa suojan luottamukselliselle viestinnälle. Luottamuksellisen viestinnän suoja jakautuu kahteen elementtiin, jotka ovat viestin sisältö ja tieto viestinnän osapuolista ja tapahtumasta. Sisällön luottamuksellisuus suojaa molempia osapuolia, mutta molemmilla on oikeus luopua suojasta paljastamalla viestin sisältö ulkopuoliselle. Luottamuksellisen viestin sisällön paljastaminen voi kuitenkin johtaa seurauksiin, jos teko loukkaa yksityiselämän suojaa tai tekijänoikeutta.[13]

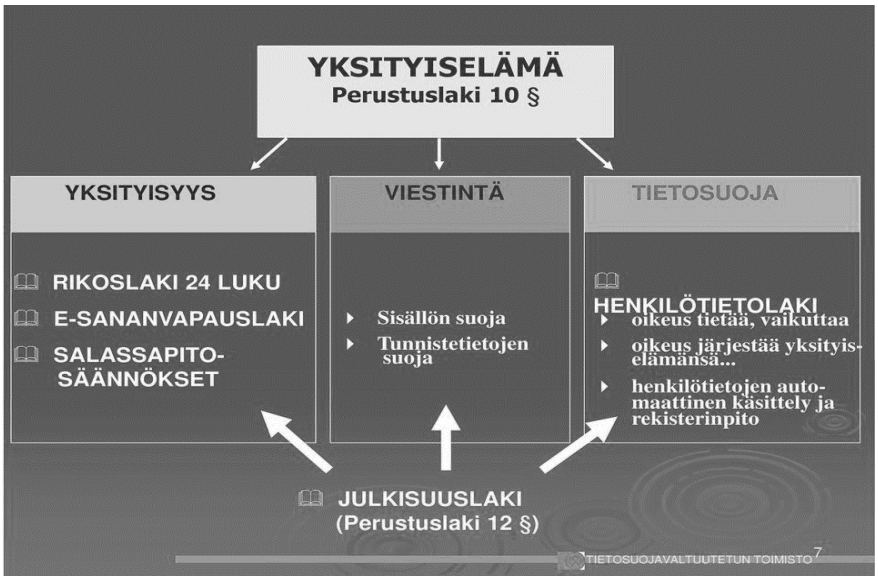
[7] Koillinen 2013, 171.
[8] Henkilötietodirektiivi (46/1995/EY) ja sähköisen viestinnän tietosuojadirektiivi (58/2002/EY).
[9] Viljanen 2017.
[10] HE 309/ 1993.
[11] Neuvonen 2014, 43.
[12] PeVL 5/1999.
[13] Neuvonen 2014, 41-42.

Esimerkiksi yritysten oikeutta tallentaa asiakkaidensa henkilötietoja on rajoitettu ja yksityiselämää loukkaavan tiedon julkaiseminen on kriminalisoitu rikoslaissa. Yksilön yksityiselämän suoja vaikuttaa siis rajoittavasti esimerkiksi toisten yksilöiden sananvapauteen.[14] Tällöin yksityiselämän suojan ja sananvapauden välille syntyy paradoksaalinen suhde.

Yksityisyyden suoja on turvattu myös YK:n ihmisoikeusjärjestelmässä kansalais- ja poliittisia oikeuksia koskevassa yleissopimuksessa (KP-sopimus), johon Suomi liittyi vuonna 1976 (SopS 7-8/1976). Sopimus täydentää vuonna 1948 annettua YK:n ihmisoikeuksien yleismaailmallista julistusta. [15]

Suomen kannalta kuitenkin velvoittavin sopimus yksityisyyden suojaan liittyen on Euroopan ihmisoikeussopimus, jonka 8 artiklassa yksityisyyden suoja on turvattu seuraavasti:

1. Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjevaihtoonsa kohdistuvaa kunnioitusta.
2. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kuin laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi



Kuvio 1. Mitä tietosuoja tarkoittaa? (Aarnio 2015)

[14] Neuvonen 2014, 43.
[15] Neuvonen 2014, 46.

3 HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVAT YLEISET PERIAATTEET

3.1 Käsittelyn yleiset edellytykset

Käsittelyn yleisten edellytysten tunnistaminen on tärkeää yritykselle, sillä ellei henkilötietojen käsittelyä pystytä perustelemaan lailla, ei kyseisiä henkilötietoja saa HeTiL:n mukaan käsitellä.[16]

HeTiL:n luku 2 koskee henkilötietojen käsittelyä koskevia yleisiä periaatteita.
Luvun 2 8 §:ssa mainitaan käsittelyn yleiset edellytykset, joiden mukaan henkilötietoja saa käsitellä ainoastaan:

> 1) rekisteröidyn yksiselitteisesti antamalla suostumuksella;
>
> 2) rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osallisena, taikka sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
>
> 3) jos käsittely yksittäistapauksessa on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi;
>
> 4) jos käsittelystä säädetään laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta;
>
> 5) jos rekisteröidyllä on asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan (yhteysvaatimus);
>
> 6) jos kysymys on konsernin tai muun taloudellisen yhteenliittymän asiakkaita tai työntekijöitä koskevista tiedoista ja näitä tietoja käsitellään kyseisen yhteenliittymän sisällä;
>
> 7) jos käsittely on tarpeen rekisterinpitäjän toimeksiannosta tapahtuvaa maksupalvelua, tietojenkäsittelyä tai muita niihin verrattavia tehtäviä varten;
>
> 8) jos kysymys on henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavista yleisesti saatavilla olevista tiedoista ja näitä tietoja käsitellään rekisterinpitäjän tai tiedot saavan sivullisen oikeuksien ja etujen turvaamiseksi; tai
>
> 9) jos tietosuojalautakunta on antanut käsittelyyn 43 § 1 momentissa tarkoitetun luvan.

[16] Salminen 2009, 55.

Yleisten edellytysten lisäksi henkilötietoja käsiteltäessä ja käsittelyä suunniteltaessa on noudatettava HeTiL:n mukaisia yleisiä periaatteita, jotka ovat:

- tarpeellisuusvaatimus ja virheettömyysvaatimus (9 §),
- käyttötarkoitussidonnaisuus (7 §),
- huolellisuusvelvoite (5 §),
- asiallisesti perusteltu käsittely ja käsittelyn tarkoituksen määrittely (6 §).

Käyttötarkoitussidonnaisuuten liittyen on tietosuojalautakunnan päätös (Tietosuojalautakunta 6/932/2006) liittyen luottotietotoimintaan[17]:

> Luottopäätössuositusten antaminen oli henkilötietolaissa tarkoitettua luottotietotoimintaa. Käyttötarkoitussidonnaisuuden periaatteen vuoksi perintätarkoituksiin kerättyjä henkilötietoja ei saanut käyttää luottotietotoiminnassa. Rekisteröidyn mahdollisesti antama toimeksianto ei oikeuttanut poikkeamaan käyttötarkoitussidonnaisuuden periaatteesta. Tietosuojalautakunnalla ei ollut toimivaltaa myöntää poikkeusta periaatteesta eikä myöskään toimivaltaa myöntää lupaa muiden kuin henkilötietolaissa tarkoitettujen henkilöluottotietojen käsittelyyn. Rekisteröityä koskevien tietojen antaminen luottopäätössuositusten muodossa ei ollut rekisteröidyn tarkastusoikeuden toteuttamista.
>
> Tietosuojavaltuutettu toteaa, että perintätoiminnasta säädetään perintälaissa (laki saatavien perinnästä 513/1999). Perintätoiminnassa kertyviä henkilötietoja voidaan käyttää vain perintätoiminnan edellyttämissä tilanteissa. Silloin kun perintätoiminnassa kertyneitä henkilötietoja käsitellään yksityisen luonnollisen henkilön taloudellisen aseman, sitoumusten hoito-kyvyn tai luotettavuuden arvioimisessa, on toimintaa arvioitava luottotietotoimintana. Tällaisessa tarkoituksessa henkilötietojen käsittelystä on tyhjentävästi säädetty henkilötietolain 4 luvun 20 §:ssä. Säännöstä on tulkittu siten, ettei henkilön suostumuksellakaan voida laajentaa sitä, mitä tietoja henkilöluottotietoina voidaan käsitellä.

3.2 Rekisteröidyn toimeksianto, asiallinen yhteys tai elintärkeä etu

HeTiL:n 8 §:n 1 momentin mukaan henkilötietoja saa käsitellä rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osallisena taikka sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.

Rekisteröidyn toimeksiannosta tapahtuvasta käsittelystä voidaan käyttää esimerkkinä tilannetta, jossa asianajotoimisto asiakkaan antaman toimeksiannon vuoksi käsittelee asiakkaansa henkilötietoja. [18] Tällöin täyttyy vaatimus rekisteröidyn toimeksiannosta ja asi-

[17] Tietosuojalautakunta 2007.
[18] Vanto 2011, 46.

anajotoimiston ja asiakkaan välille syntyy lisäksi molempia osapuolia velvoittava sopimus. Asiakassuhdetta edeltävien toimenpiteiden toteuttamiseksi tapahtuvaa henkilötietojen käsittelyä voi olla esimerkiksi puhelinliittymän avaamista varten tarvittavien henkilötietojen käsittely. [19]

Asiakassuhde syntyy siis jo, kun asiakas rekisteröityy yrityksen internetpalveluun tai esimerkiksi silloin, kun asiakas ilman rekisteröitymistäkin tilaa yrityksen tuotteen tai palvelun. Asiakassuhde voi syntyä myös vastikkeettoman palvelun käytöstä. [20]

Pelkkä vierailu yrityksen internetsivuilla ilman rekisteröitymistä palvelun käyttäjäksi tai tietojen antaminen itsestään esimerkiksi yksittäistä kilpailua varten ei kuitenkaan yleensä muodosta yrityksen ja kuluttajan välille asialliseksi yhteydeksi luokiteltavaa asiakassuhdetta. Vähäisten ja yksittäisten ostosten osalta asiallisen yhteyden muodostumista arvioidaan tapauskohtaisesti.[21]

Kolmantena rekisteröidyn taholta yleisiin edellytyksiin kuuluu rekisteröidyn elintärkeä etu. HeTiL:n 8 §:n 1 momentin mukaan henkilötietoja voi käsitellä, jos käsittely yksittäistapauksessa on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi. Keskeisintä tämän edellytyksen kannalta on, että edun on oltava elintärkeä, eli esimerkiksi ensiavun tarjoaminen onnettomuustilanteessa. [22]

3.3 Rekisteröidyn suostumus

Kuten HeTiL:n käsittelyn yleisissä edellytyksissä jo mainittiin: ”Henkilötietoja saa käsitellä ainoastaan rekisteröidyn yksiselitteisesti antamalla suostumuksella.”

HeTiL:n 3 §:n kohdan 7 mukaan suostumuksella tarkoitetaan kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Suostumuksen vapaaehtoisuus edellyttää siis todellista mahdollisuutta kieltäytyä suostumuksen antamisesta.

[19] Vanto 2011, 46.
[20] Salminen 2009, 57.
[21] Salminen 2009, 57.
[22] Vanto 2011, 46.

Hallitus on esittänyt, että suostumuksen ei välttämättä tarvitse olla kirjallinen ollakseen lain tarkoittama suostumus. Suostumuksen tietoisuus edellyttää, että rekisteröity suostumusta antaessaan tietää millaiseen henkilötietojen käsittelyyn, esimerkiksi rekisteriselosteessa olevat tiedot, hän suostumuksensa antaa.[23]

Euroopan unionin tietosuojatyöryhmä on suostumuksen merkitystä koskevassa mielipiteessään vuonna 2011[24] todennut, että keskeistä on annettujen tietojen laatu, kuten myös tietojen saatavuus ja näkyvyys. Työryhmän mukaan tiedot tulisi antaa niin, että esimerkiksi internetpalvelun keskivertokäyttäjä tiedot varmasti ymmärtää. Työryhmän mukaan hiljainen eli konkludenttinen suostumus ei täyttäisi tietosuojadirektiivin vaatimuksia, kun otetaan huomioon myös suostumuksen olemassaolon todistettavuuteen vaikuttavat tekijät.

Internetpalveluissa asiakkaan suostumus henkilötietojen käsittelyyn pyydetään yleensä rekisteröitymisen yhteydessä, samalla kun rekisteröity antaa tietojaan rekisteriä hallinnoivan tahon käyttöön.[25] Hyvän, avoimen ja luotettavan yritystoiminnan kannalta maininta suostumuksesta henkilötietojen käsittelyyn tulisi olla tarpeeksi isolla fontilla esitettynä ja helposti huomattavissa.

Tietosuojariskit asettavat nykyään omat haasteensa henkilötietojen käsittelyyn, vaikka nimenomainen suostumus olisikin rekisteröidyn taholta annettu. Esimerkkinä tapaus Tietosuojalautakunnan lausunnosta[26]:

> Näkövammaisten keskusliitto ry pyysi Helsingin sosiaalivirastoa lähettämään näkövammaisille heidän suostumuksellaan heitä koskevat viestit ja päätökset sähköpostitse, jolloin näkövammaiset pystyisivät lukemaan ne itse tietokoneeltaan.
>
> Sosiaalivirasto kieltäytyi tietojen lähettämisestä sähköpostitse, koska jo pelkkä tieto sosiaalihuollon asiakkuudesta on salassa pidettävä. Yleinen internet-sähköpostijärjestelmä on suojaamaton, eikä se mahdollista salassa pidettävien tietojen lähettämistä. Viranomaisella ei ole mahdollisuutta asioida sähköpostin välityksellä asiakkaan kanssa, vaikka siihen saataisiin asiakkaan nimenomainen suostumus. Sosiaaliviraston käytössä ei ole suojattua sähköpostiyhteyttä tai jotain muuta vahvaa tunnistamista hyväksikäyttävää tekniikkaa.
>
> Tietosuojavaltuutetun lausunto
>
> Rekisterinpitäjän on suojattava henkilötiedot mm. riittävin teknisin toimenpitein sivullisilta myös niitä sähköpostitse lähetettäessä. Rekisterinpitäjä ei voi poiketa tietojen suojaamisvelvollisuudestaan rekisteröidyn suostumuksella. Tieto sosiaalihuollon asiakkuudesta on salassa pidettävä. Tietojen suojaamisvelvollisuudesta ja

[23] Vanto 2011, 33.
[24] Data protection working party 2011.
[25] Salminen 2009, 56.
[26] Tietosuojavaltuutetun toimisto 2014a.

> salassapitovelvollisuudesta seuraa, että sosiaaliviranomainen voi lähettää asiakkaalle viestejä sähköpostitse vain, mikäli sillä on käytössään sähköposti, jossa on riittävän vahva salaus ja osapuolet voidaan tunnistaa. Tavallisessa suojaamattomassa internet-sähköpostissa tiedot eivät ole suojattu sivullisilta. Sitä ei voida käyttää salassa pidettävien tietojen lähettämiseen siitäkään huolimatta, että siihen olisi asiakkaan suostumus.

3.4 Laissa säädetty käsittely tai tietosuojalautakunnan lupa

HeTiL:n 8 §:n 1 momentin mukaan henkilötietoja saa käsitellä, jos käsittelystä säädetään laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta.

HeTiL soveltuu kuitenkin myös sellaiseen henkilötietojen käsittelyyn, josta on muussa laissa säädetty. Esimerkkinä laissa yksityisyyden suojasta työelämässä[27] säädetään työnantajan oikeudesta käsitellä työntekijän henkilötietoja ja luottotietolaissa[28] säädetään yrityksen oikeudesta, joka luottotietotoimintaa harjoittaa, käsitellä henkilöluottotietoja. [29]

HeTiL:n 43 §:n 1 momentin mukaan tietosuojalautakunta voi antaa luvan henkilötietojen käsittelyyn, jos käsittely on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi muussa kuin yksittäistapauksessa taikka yleistä etua koskevan tehtävän suorittamiseksi tai sellaisen julkisen vallan käyttämiseksi, joka kuuluu rekisterin pitäjälle tai sivulliselle, jolle tiedot luovutetaan. Lupa voidaan myöntää myös rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun edun toteuttamiseksi edellyttäen, ettei tietojen tällainen käsittely vaaranna henkilön yksityisyyden suojaa ja oikeuksia.

[27] Laki yksityisyyden suojasta työelämässä. 13.8.2004/759.
[28] Luottotietolaki. 11.5.2007/527.
[29] Vanto 2011, 47.

4 REKISTERÖIDYN OIKEUDET

4.1 Informointi tietojen käsittelystä

HeTiL:ssa rekisteröidylle säädettyjä nimenomaisia oikeuksia ovat:

- tiedonsaantioikeus
- tarkastusoikeus
- oikeus saada tietonsa korjatuiksi
- kielto-oikeus.[30]

Informoinnista voidaan poiketa erityistilanteissa, jotka ovat laissa säädetty. Informoinnista ei voida kuitenkaan poiketa silloin, kun tietoja käytetään rekisteröityä koskevassa päätöksenteossa.[31]

Jokaisella on salassapitosäännösten estämättä oikeus saada tietää mitä ja minkälaisia tietoja hänestä on henkilörekisteriin talletettu, tai ettei rekisterissä ole häntä koskevia tietoja. Rekisterinpitäjä on myös velvollinen ilmoittamaan rekisteröidylle rekisterin tietolähteet, sekä sen mihin tarkoitukseen rekisterin tietoja käytetään ja mihin niitä luovutetaan.[32]

HeTiL:n 28 §:ssa mainitaan tarkastusoikeuden toteuttamisesta seuraavaa:

> Rekisterinpitäjän on ilman aiheetonta viivytystä varattava rekisteröidylle tilaisuus tutustua tietoihin tai annettava tiedot pyydettäessä kirjallisesti. Tiedot on annettava ymmärrettävässä muodossa. Jos rekisterinpitäjä kieltäytyy antamasta tietoja, hänen on annettava tästä kirjallinen todistus. Todistuksessa on mainittava myös ne syyt, joiden vuoksi tarkastusoikeus on evätty. Tarkastusoikeuden epäämisen veroisena pidetään sitä, että rekisterinpitäjä ei ole kolmen kuukauden kuluessa pyynnön esittämisestä antanut kirjallista vastausta rekisteröidylle. Rekisteröity voi saattaa asian tietosuojavaltuutetun käsiteltäväksi.

HeTiL:n 29 §:n mukaan rekisterinpitäjän on rekisteröidyn vaatimuksesta tai omasta aloitteesta viivästyksettä oikaistava, poistettava tai täydennettävä rekisterissä oleva virheellinen, puutteellinen, vanhentunut tai tarpeeton tieto. Rekisterinpitäjä on myös velvollinen

[30] Tietosuojavaltuutetun toimisto 2014b.
[31] Tietosuojavaltuutetun toimisto 2014c.
[32] Mäenpää 2014.

huolehtimaan, että virheellinen tieto ei pääse leviämään, jos tieto voi vaarantaa rekisteröidyn yksityisyyden suojaa tai hänen muita oikeuksiaan.

Tarkastusoikeus voidaan evätä tietyissä HeTiL:ssa säädetyissä tilanteissa. Tarkastusoikeutta ei sovelleta pelkästään tieteellisiin tutkimustarkoituksiin ja tilastointitarkoituksiin kerättyihin tietoihin. Estettä tarkastusoikeuden toteuttamiseen ei tällöinkään kuitenkaan ole.

4.2 Kielto-oikeus

Rekisteröidyn oikeudesta kieltää käsittelemästä häntä itseään koskevia tietoja säädetään HeTiL:n 30 §:ssa. Sen mukaan rekisteröity voi kieltää tietojensa käytön suoramainontaa, etämyyntiä ja muuta suoramarkkinointia sekä markkina- ja mielipidetutkimusta samoin kuin henkilömatrikkelia ja sukututkimusta varten.

Kielto-oikeus (opt-out) on HeTiL:n mukainen pääsääntö. Se tarkoittaa, että henkilöltä edellytetään toimenpiteitä suoramarkkinoinnin estämiseksi tai rajoittamiseksi.[33] Eli tällainen suoramarkkinointi on mahdollista, kunnes rekisteröity kieltää rekisterinpitäjää käsittelemästä häntä koskevia tietoja.[34]

Kielto- oikeus (opt-in) taas merkitsee sitä, että sähköisen viestinnän tietosuojalaki edellyttää henkilön etukäteistä suostumusta tilanteessa, jossa suoramarkkinointi toteutetaan tekstiviestin, sähköpostin, ääniviestin, puheviestin tai kuvaviestin avulla. Tällöin suoramarkkinoinnin toteuttajalta vaaditaan eritystä aktiivisuutta.[35] Rekisteröity voi myös käyttää kielto-oikeuttaan jo tietojen keräämisvaiheessa esimerkiksi, kun hän liittyy jonkin yhdistyksen jäseneksi tai tilaa lehden suoramainonnan kautta.[36]

[33] Tietosuojavaltuutetun toimisto 2010a, 2
[34] Vanto 2011, 135
[35] Tietosuojavaltuutetun toimisto 2010a, 2
[36] Tietosuojavaltuutetun toimisto 2010a, 2.

4.3 Rekisteri- ja tietosuojaseloste

HeTiL:n 10 §:n mukaan rekisterinpitäjän on laadittava rekisteristä rekisteriseloste, josta ilmenee:

- rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot;
- henkilötietojen käsittelyn tarkoitus;
- kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä;
- mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle; sekä
- kuvaus rekisterin suojauksen periaatteista.

Lainkohdan mukaan rekisterinpitäjän on pidettävä seloste jokaisen saatavilla. Tästä velvollisuudesta voidaan poiketa vain, jos se on välttämätöntä valtion turvallisuuden, puolustuksen tai yleisen järjestyksen ja turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi taikka verotukseen tai julkiseen talouteen liittyvän valvonta tehtävän vuoksi. Hallitus on lisäksi esittänyt, että myös rekisteriselosteen tulee olla internetissä jokaisen nähtävillä, jos itse henkilörekisterikin on internetverkossa.[37] Tietosuojavaltuutetun toimiston verkkosivuilla on kattavat ohjeet rekisteriselosteen tekemiseen.

Toinen vaihtoehto rekisteriselosteelle on tietosuojaseloste. Tietosuojaselosteessa voi lain edellyttämän rekisteriselosteen tietosisällön lisäksi esittää rekisteröidylle, myös muut informaatiovelvoitteen täyttämiseksi vaadittavat tiedot, jolloin rekisteriselostetta ei tarvita. Selosteen avulla toteutetaan asiakkaan ulkoista informointivelvoitetta, jonka tarkoituksena on, että rekisteröity saa helposti ja yksinkertaisesti ymmärrettävää tietoa henkilötietojensa käsittelystä.[38]

Internetsivuilla tietosuojaseloste tulee pitää asiakkaiden saatavilla ja esittää heti tietojen keräämisen yhteydessä, kuten asiakkaan rekisteröityessä palveluun. Mikäli internetpalvelussa toimii useita eri rekisterinpitäjiä, vaaditaan jokaiselta erikseen oma rekisteri- tai tietosuojaseloste.[39]

[37] Vanto 2011, 54.
[38] Salminen 2009, 69 ja 71.
[39] Salminen 2009, 69.

Tietosuoja- ja rekisteriselosteessa asiakkaalle tulee informoida ainakin seuraavat asiat (kohdat 9-12 eivät ole välttämättömiä rekisteriselosteessa):

1. Rekisterinpitäjä
2. Rekisteriasioista vastaava henkilö
3. Rekisterin nimi
4. Henkilötietojen käsittelyn tarkoitukset
5. Rekisterin tietosisältö
6. Säännönmukaiset tietolähteet
7. Säännönmukaiset tietojen luovutukset ja tietojen siirto EU/ETA- alueen ulkopuolelle
8. Rekisterin suojauksen periaatteet
9. Evästeiden käyttö
10. Tarkastusoikeus ja tarkastusoikeuden toteuttaminen
11. Tiedon korjaaminen ja tiedon korjaamisen toteuttaminen
12. Muut mahdolliset oikeudet[40]

[40] Salminen 2009, 70.

5 ARKALUONTOISET TIEDOT JA HENKILÖTUNNUS

5.1 Arkaluontoinen henkilötieto ja sen määritelmä

HeTiL:n 11 §:n pääsäännön mukaan arkaluontoisten henkilötietojen kerääminen ja käsittely on kielletty. Lain mukaan arkaluontoisena pidetään henkilötietoa, joka kuvaa tai on tarkoitettu kuvaamaan:

- rotua tai etnistä alkuperää
- henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista
- rikollista tekoa, rangaistusta tai muuta rikollisen teon seuraamusta
- henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia
- henkilön seksuaalista suuntautumista tai käyttäytymistä
- henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Poikkeuksista säädetään HeTiL:n 12 §:ssa, jonka mukaan poikkeuksilla tarkoitetaan:

- tietojen käsittelyä, johon rekisteröity on antanut nimenomaisen suostumuksensa;
- sellaisen henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista koskevan tiedon käsittelyä, jonka rekisteröity on itse saattanut julkiseksi
- tietojen käsittelyä, joka on tarpeen rekisteröidyn tai jonkun toisen henkilön elintärkeän edun suojaamiseksi, jos rekisteröity on estynyt antamasta suostumustaan
- tietojen käsittelyä, joka on tarpeen oikeusvaateen laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi
- tietojen käsittelyä, josta säädetään laissa tai joka johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä
- tietojen käsittelyä historiallista tai tieteellistä tutkimusta taikka tilastointia varten;
- uskonnollista, poliittista tai yhteiskunnallista vakaumusta koskevien tietojen käsittelyä tällaista vakaumusta edustavien yhdistysten ja muiden yhteisöjen toiminnassa

- ammattiliittoon kuulumista koskevien tietojen käsittelyä ammattiyhdistysten ja niiden muodostaman liiton toiminnassa
- ammattiliittoon kuulumista koskevan tiedon käsittelyä, joka on tarpeen rekisterinpitäjän erityisten oikeuksien ja velvoitteiden noudattamiseksi työoikeuden alalla;
- terveydenhuollon toimintayksikköä tai terveydenhuollon ammattihenkilöä käsittelemästä tietoja rekisteröidyn terveydentilasta, sairaudesta tai vammaisuudesta
- vakuutuslaitosta käsittelemästä vakuutustoiminnassa saatuja tietoja vakuutetun ja korvauksenhakijan terveydentilasta, sairaudesta tai vammaisuudesta taikka häneen kohdistetuista hoitotoimenpiteistä
- sosiaalihuollon viranomaista tai muuta sosiaalihuollon etuuksia myöntävää viranomaista, laitosta tai yksityisten sosiaalipalvelujen tuottajaa käsittelemästä kyseisen viranomaisen, laitoksen tai palvelujen tuottajan toiminnassaan saamia tietoja rekisteröidyn sosiaalihuollon tarpeesta
- tietojen käsittelyä, johon tietosuojalautakunta on antanut 43 §:n 2 momentissa tarkoitetun luvan.

12 §:n mukaan arkaluontoiset tiedot on poistettava rekisteristä välittömästi sen jälkeen, kun käsittelylle ei ole lain 1 momentissa mainittua perustetta. Perustetta ja käsittelyn tarvetta on arvioitava vähintään viiden vuoden välein.

Henkilötietojen käsittelyä suunniteltaessa arkaluontoisiin tietoihin on hyvä kiinnittää erityistä huomiota. Käytännössä kyseisiä tietoja ei kannata kerätä lainkaan, ellei niiden käsittely ole toiminnan kannalta välttämätöntä.[41]

5.2 Henkilötunnus

Lähtökohtaisesti myös henkilötunnuksen keräämistä tulisi välttää, ellei käyttö ole välttämätöntä. Henkilötunnuksen liian laaja-alainen käyttö voi muodostaa rekisteröidylle tietoturvallisuus riskin ja aiheuttaa välillisiä riskejä myös yritykselle.[42]

Sähköisissä asiakasrekistereissä henkilötunnusta on usein tarpeellista käyttää asiakkaan yksilöintiin. Tällöin käyttötarkoitussidonnaisuus täyttyy, eli henkilötunnuksen käyttötarkoitus on tällöin erotella rekisteröidyt asiakasrekistereissä. Pelkkää henkilötunnuk-

[41] Salminen 2009, 74.
[42] Salminen 2009, 76.

sen kysymistä ei kuitenkaan tule käyttää tunnistamisen menetelmänä rekisteröinnin yhteydessä. Henkilötunnusta ei ole myöskään sallittua käyttää käyttäjätunnuksena. Henkilötunnuksen tarpeetonta käsittelyä voidaankin välttää luomalla rekisteröidyille järjestelmien sisäisiä asiakastunnisteita (asiakkaan id).

HeTiL:n 13 §:ssa säädetään henkilötunnuksesta seuraavaa:

> Henkilötunnusta saa käsitellä rekisteröidyn yksiselitteisesi antamalla suostumuksella tai, jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää:
> 1) laissa säädetyn tehtävän suorittamiseksi;
> 2) rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi; tai
> 3) historiallista tai tieteellistä tutkimusta taikka tilastointi varten.
>
> Henkilötunnusta saa käsitellä luotonannossa tai saatavan perinnässä, vakuutus-, luottolaitos-, vuokraus- ja lainaustoiminnassa, luottotietotoiminnassa, terveydenhuollossa, sosiaalihuollossa ja muun sosiaaliturvan toteuttamisessa tai virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa.
>
> Henkilötunnuksen saa lisäksi luovuttaa osoitetietojen päivittämiseksi tai moninkertaisten postilähetysten välttämiseksi suoritettavaa tietojen käsittelyä varten, jos henkilötunnus jo on luovutuksensaajan käytettävissä.
>
> Rekisterinpitäjän on huolehdittava, että henkilötunnusta ei merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

Tietosuojavaltuutetun verkkosivuille[43] on koottu vastauksia kysymyksiin henkilötunnuksen käsittelystä ja käytöstä.

1990-luvulla, kun henkilötietolaki tuli voimaan, henkilötietojen kerääminen internetistä ei ollut lainkaan yhtä laajaa, kuin nykyaikana. Nykyään, kun yksityishenkilöt julkaisevat henkilötietojaan laajalti sosiaalisissa medioissa, myös identiteettivarkaudet ovat yleistyneet. Usein henkilötunnus onkin ainoa identiteettivarkaalta puuttuva henkilötieto. Kun identiteettivaras saa haltuunsa henkilötunnuksen, pystyy hän yhdistämään sen sosiaalisista verkoista keräämiinsä muihin henkilötietoihin, jolloin esimerkiksi luottokorttitilien avaaminen ja muiden taloudellista vahinkoa aiheuttavien toimenpiteiden teko on helppoa ja nopeaa.[44]

Indentiteettivarkaudesta säädetään Suomen rikoslaissa. Tietoverkkorikoksia koskeva lainmuutos tuli voimaan 4.9.2015. Samalla myös indentiteettivarkaus säädettiin rangaistavaksi itsenäisenä rikoksena. Uusi säännös kattaa tilanteen, jossa on esimerkiksi luotu

[43] Tietosuojavaltuutetun toimisto 2014d.
[44] Vanto 2011, 69.

valeprofiili, mutta kunnianloukkauksen tai yksityiselämää loukkaavan tiedon kriteerit eivät täyty. Tekijä voidaan nykyisen lain mukaan tuomita esimerkiksi kunnianloukkauksesta, petoksesta tai väärän henkilötiedon antamisesta. [45]

Indentiteettivarkaus on asianomistaja rikos, eli syyttäjä ei voi nostaa syytettä, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi. Mikäli asianomistaja ei koe, että hänen identiteettiä on loukattu tai muusta syystä ei toivo syytteen nostamista, ei sitä tehdä vastoin hänen tahtoaan. Enimmäisrangaistus identiteettivarkaudesta on sakkorangaistus. [46] Identiteettivarkauteen kuitenkin usein liittyy välillisesti muita rikosnimikkeitä, jolloin rangaistus voi koventua sakosta vankeudeksi.

Lisäksi datavahingontekoa, tietoliikenteen häirintää ja tietojärjestelmän häirintää voidaan nykyisin pitää törkeänä, jos rikoksessa on käytetty niin sanottua bottiverkkoa (haittaohjelma, jonka avulla hyökkääjä hallitsee konetta), se on tehty rikollisjärjestön toiminnassa tai rikos on kohdistunut elintärkeään infrastruktuuriin, jolloin enimmäisrangaistus voi olla jopa viisi vuotta vankeutta.[47]

.

[45] Oikeusministeriö 2015.
[46] Oikeusministeriö 2015.
[47] Oikeusministeriö 2015.

6 HENKILÖTIETOJEN SUOJAAMINEN YRITYSTOIMINNASSA

6.1 Tietoturva

HeTiL:n 32 §:ssa mainitaan tietojen suojaamisesta seuraavaa:

> Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin tai vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimen piteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.
> Sen joka itsenäisenä elinkeinoharjoittajana toimii rekisterinpitäjän lukuun tai jolle rekisterinpitäjä luovuttaa tietoja teknisen käyttöyhteyden avulla on ennen tietojen käsittelyyn ryhtymistä annettava rekisterinpitäjälle asianmukaiset selvitykset ja sitoumukset sekä muutoin riittävät takeet henkilötietojen suojaamisesta 1 momentissa tarkoitetulla tavalla.

Suomessa ei ole säädetty erillistä tietoturvalakia. Tietoturvaa koskevat säädökset perustuvat henkilötietojen suojaamisen osalta henkilötietolakiin ja sähköisen viestinnän tietoturvan osalta sähköisen viestinnän tietoturvalakiin. Tietoturvaan kuuluu erityisesti tietojen luotettavuus, eheys ja käytettävyys.
Luotettavuuden vaatimus toteutuu, kun tietojärjestelmät ovat niiden käytössä, joille on annettu niihin käyttöoikeus. Eheys puolestaan, kun tiedot ovat varmasti oikeita ja ajantasaisia ja käytettävyys, kun tiedot ovat niiden käyttöön oikeutettujen henkilöiden käytettävissä aina tarvittaessa.
Tietojen täytyy olla lisäksi turvattuina esimerkiksi tahallisten väärinkäytösten, laitteisto-, tietoverkko- ja ohjelmistovikojen uhilta ja vahingoilta.[48]

Tietoturva voidaan lisäksi jakaa kolmeen eri ulottuvuuteen: tekniseen, fyysiseen ja hallinnolliseen. Tekniseen ulottuvuuteen sisältyy organisaatiossa käytettävien teknisten laitteiden tietoturva, jonka avulla mahdolliset hyökkäykset ja väärinkäytökset estetään. Fyysiseen puolestaan sisältyy käytettävät toimitilat, laitteistot, sekä kaikki muunlaiset fyysiseen turvallisuuteen liittyvät toimenpiteet, kuten esimerkiksi kulunvalvonta. Fyysisen

[48] Salminen 2009, 81.

ulottuvuuden tarkoituksena on ehkäistä erilaisia toimitiloihin kohdistuvia uhkia, esimerkiksi murtoyrityksiä. Hallinnolliseen ulottuvuuteen sisältyvät toimenpiteet, joilla pyritään kehittämään henkilöstön tietoturvaosaamista johtamisen ja hallinnon kautta.[49]

Finanssi-alan toimijat joutuvat usein nykyaikana erilaisten tietoturva hyökkäysten kohteeksi. Esimerkkinä tapaus Viestintäviraston internetsivulta vuodelta 2013[50], jossa S-pankin nimissä suomalaisille internetin käyttäjille oli lähetetty huijausviestejä:

> Huijausviestissä käyttäjiä on kehotettu turvallisuussyistä vahvistaman S-Pankki Oy:n tiedot avaamalla viestissä oleva haitallinen linkki. Mikäli viestin saaja avaa kyseisen linkin, ohjataan käyttäjän selain sivustolle, jossa pyydetään syöttämään kortin numero, voimassaoloaika sekä turvatunnus. Lisäksi sivusto pyytää syöttämään henkilökohtaisen S-Pankin käyttäjätunnuksen sekä salasanan.
> Huijaussähköpostin tunnistaa mm. seuraavasta virkkeestä: "Turvallisuussyistä, me tarvitsemme sinua vahvistamaan S-Pankki Oy: n tiedot. Ole hyvä ja kirjaudu profiilisivulla nyt."

Tapauksen kaltainen verkkourkinta eli tietojenkalasteluyritys on tietotekniikassa esiintyvää rikollista toimintaa. Sen tavoitteena on saada manipuloinnin keinoin haltuun luottamuksellisia tietoja, kuten henkilö- tai tilitietoja, esiintymällä tahona, joka on tiedon saantiin oikeutettu.[51]

6.2 Tietosuojavastaava

Tietosuojavastaavan nimeäminen on lakisääteistä terveyden- ja sosiaalihuollon palveluiden tarjoajille[52]. Nykyaikaisten sähköisten tietosuojajärjestelmien yleisyyden vuoksi tietosuojavastaavan nimeäminen on kuitenkin suotavaa kaikille henkilötietoja ja henkilörekistereitä hallinoiville yrityksille toimialasta riippumatta.

Tietosuojavastaava on organisaation erityisasiantuntija, jonka toimenkuvaan kuuluu auttaa rekisterinpitäjää saavuttamaan hyvä henkilötietojen käsittelytapa ja lain edellyttämä korkea tietosuojataso, joiden avulla säilytetään luottamus rekisterinpitäjän ja rekiste-

[49] Lepistö 2016, 11.
[50] Viestintävirasto 2013.
[51] Lehto 2013. Metropolia.
[52] Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) ja laki sähköisestä lääkemääräyksestä (61/2007).

röidyn välillä. Tietosuojavastaavan tehtävänä on antaa asiantuntija-apua henkilöstön lisäksi myös organisaation johdolle, joka viimeisenä vastaa organisaation henkilötietojen käsittelystä. Lainsäädäntö ei aseta tietosuojavastaavalle vaatimusta tietystä koulutustaustasta, tärkeintä on riittävä tietotaso ja koulutus tehtävään. Erityisen tärkeää on kuitenkin muistaa, että tietosuojavastaavan nimeäminen ei poista tai vähennä rekisterinpitäjän vastuuta.[53]

Tietosuojavastaavaan pääasiallisiin tehtäviin kuuluu:

- henkilötietojen käsittelyyn liittyvä suunnittelutoiminta;
- tietosuoja- ja tietoturvaohjeiden valmistelu ja ylläpito;
- henkilötietojen käsittelyn ja niiden suojausmenetelmien seuranta;
- osallistuminen henkilöstölle annattavaan tietosuojakoulutukseen;
- toimiminen yhdyssiteenä valvontaviranomaisiin;
- raportoiminen johdolle tietosuojan tilasta ja mahdollisista kehitystarpeista[54].

EU:n valmisteilla olevan tietosuoja-asetuksen myötä tietosuojavastaavan rooli korostuu entisestään. Uusi tietosuoja-asetus, joka hyväksyttiin keväällä 2016 ja tulee voimaan EU maissa kahden vuoden siirtymäajan jälkeen, asettaa tietosuojalainsäädäntöön tilintekovelvoitteen. Rekisterinpitäjät tulevat jatkossa olemaan velvollisia vastaamaan tietosuojan tasosta sakon uhalla ja raportoimaan sen toteuttamisesta entistä avoimemmin.[55]

6.3 Tietoturvatarkastukset ja -sertifioinnit

Rekisterinpitäjän henkilötietojen käsittelyn lainmukaisuuden arvioimiseksi voidaan järjestää tietoturvatarkastuksia (auditointeja). Auditoinnin avulla voidaan lainmukaisuuden ja sisäisen riittävän ohjeistuksen lisäksi varmistua niissä mahdollisesti olevista puutteista.

Auditoinnin avulla pystytään ehkäisemään henkilötietojen huolimattomasta käsittelystä aiheutuvia sanktioita ja vahingonkorvauskuluja. Näin tehostetaan organisaation taloudellista riskinsietokykyä. Yritys voi myös viestittää ulospäin hyvästä auditointituloksesta sidosryhmilleen ja hyödyntää hyvää tulosta esimerkiksi markkinoinnissaan.

[53] Tietosuojavaltuutetun toimisto 2010b, 2.
[54] Tietosuojavaltuutetuntoimisto 2010b, 3.
[55] Castrén 2015. Tietosuoja.

Auditoinnin objektiivisuuden ja tulosten hyödynnettävyyden kannalta on tärkeää, että auditoinnin suorittaa organisaation ulkopuolinen, riippumaton henkilö. Auditoijalta tulee edellyttää hyvää henkilötietojen suojaan liittyvien lakien tuntemusta. Tietoturvaa koskevat tekniset ratkaisut vaativat lisäksi riippumattoman teknisen asiantuntijan.[56]

Euroopan standardisointikeskus CEN:n tietosuoja-auditoinnin kehyksessä[57] auditointi määritellään systemaattiseksi ja riippumattomaksi tarkastukseksi, jonka tarkoituksena on henkilötietojen käsittelyn sisäisten toimintaohjeiden ja siihen sovellettavien lakien mukaisuus. Kehyksen mukaan auditointi jakautuu neljään päävaiheeseen:

- auditointitoimeksiannon laadinta;
- auditoinnin valmistelu → auditointisuunnitelma;
- auditoinnin toteutus;
- kirjallinen auditointituloksen laadinta, raportointi ja seuranta[58].

Auditoinnin lopussa laaditaan audiointiraportti. Se sisältää tarkastuksen toteuttaneen toimeksisaajan johtopäätökset ja mielipiteet toimeksiantajan henkilötietojen käsittelyn vaatimusten täyttymisestä. Jotta raportti olisi mahdollisimman hyödyllinen, siitä tulisi selkeästi käydä ilmi mahdolliset puutteet henkilötietojen käsittelyssä ja ne vaatimukset, jotka toimeksiantajaan kohdistuvat. Toimeksisaajan tulisi myös antaa toimeksiantajalle selkeitä ohjeita auditoinnissa havaittujen puutteiden korjaamiseksi.[59]

Yritys voi auditoinnin lisäksi tietosuojasertifikaatein osoittaa sidosryhmilleen toimintansa laatua. EU:n alueella yritykset voivat sertifioida tarjoamansa ohjelmiston tai IT-tuotteen, kuten pankin verkkosivuston

EU:n alueella toimivat yritykset voivat sertifioida IT-tuotteensa tai -palvelunsa, kuten esimerkiksi pankin verkkosivuston European Privacy Seal- laatuleimalla (EuroPrice).[60] EuroPricen sertifiointikriteerit perustuvat tietosuojadirektiiviin, sähköisen viestinnän tietosuoja direktiiviin sekä tietosuojatyöryhmän kannanottoihin. [61]

[56] Vanto 2011, 191.
[57] CEN Workshop Agreement 2006.
[58] Vanto 2011, 191 ja 192.
[59] Vanto 2011, 192 ja 193.
[60] EuroPriSe GmbH. European Privacy Seal 2008-2016.
[61] Vanto 2011, 195.

Keskeisintä EuroPrice- sertifioinnissa on, että IT-tuotteesta tai -palvelusta on olemassa kattava dokumentaatio, josta löytyvät henkilötietojen suojan kannalta relevantit ominaisuudet. Kattava dokumentointi nopeuttaa sertifiointia huomattavasti ja vähentää siitä aiheutuvia kustannuksia. EuroPrice on ollut käytössä vuodesta 2008 ja se on myönnetty muun muassa arkaluontoisia henkilötietoja käsitteleville ohjelmistoja valmistaville ohjelmistoyhtiölle, viestintäteknologia yrityksille ja pankeille.[62]

[62] Vanto 2011, 195.

7 TOIMEKSIANTAJA

7.1 Taustatiedot

Tämän opinnäytetyön toimeksiantajana toimii suomalainen finanssi- ja rahoitusalan yritys, jonka liiketoiminta-alueita ovat pankkitoiminta, vahinkovakuutus ja varallisuudenhoito, joista pankkitoiminta on liiketoimintasegmenttinä suurin. Haastattelututkimuksessa toimeksiantajayrityksestä käytetään nimeä Pankki.

Toimeksiantaja on vahvistanut vuonna 2016 uuden strategian, jossa tavoitteena on muuttua tämänhetkisestä finanssitoimijasta digitaalisen ajan monialaiseksi palveluyritykseksi, jolla on kuitenkin edelleen vakaa finanssiosaaminen. Strategian taustalla on asiakaskäyttäytymisen muutos, sekä finanssitoimialan nopeasti etenevä digitaalinen murros, jonka myötä myös kilpailu toimialalla on lisääntynyt.[63]

Toimeksiantajan asiakkaat koostuvat pääasiassa yksityis- ja yritysasiakkaista. Kotitalouksille toimeksiantajalla on tuotteita ja palveluita esimerkiksi talouden hoitoon ja asunnon hankintaan, yrityksille vastaavasti rahoituksen, kassanhallinnan ja maksuliikkeen hoitoon.[64]

Toimeksiantaja työllisti vuonna 2013 11 983 henkilöä. Suurin osa työntekijöistä on toimihenkilöitä ja toiseksi suurin osa asiantuntijoita. Sisäisessä toiminnassaan yritys panostaa voimakkaasti henkilöstön työhyvinvointiin, osaamiseen, johtamisen kehittämiseen ja palkitsemiseen. Henkilöstöä kannustetaan myös kehittämään osaamistaan koko työuran ajan.[65]

7.2 Henkilötietojen käsittely toimeksiantajayrityksessä

Toimeksiantajayritys käsittelee henkilötietoja palveluidensa ja suoramarkkinointinsa toteuttamiseksi, asiakassuhteen hoitamiseksi sekä verkkopalvelunsa laadun takaamiseksi. Tietoja toimeksiantaja hankkii rekisteröidyltä itseltään, hänen valtuuttamiltaan

[63] Toimeksiantajan verkkosivut.
[64] Toimeksiantajan verkkosivut.
[65] Toimeksiantajan verkkosivut

tahoilta, viranomaisten rekistereistä, luottotieto- ja asiakashäiriörekistereistä, sekä rekistereistä, joihin rekisteröity on antanut suostumuksensa tietojen luovuttamiseen. Tietoja voidaan luovuttaa toimeksiantajan sisällä asiakaspalvelua, asiakassuhteen hoitamista, markkinointia tai riskienhallintaa varten.[66]

Toimeksiantajan asiakkaalla on oikeus saada tarkistaa itseään koskevat tiedot, vaatia virheellisen tiedon oikaisua sekä vaatia virheellisen tai vanhentuneen tiedon poistoa yrityksen rekisteristä. Pyynnöt esitetään rekisterinpitäjälle, joka määräytyy asiakassuhteen mukaan. [67]

[66] Toimeksiantajan verkkosivut.
[67] Toimeksiantajan verkkosivut.

8 HAASTATTELUTUTKIMUKSEN TULOKSET

Työn tutkimus toteutettiin puolistrukturoituna haastattelututkimuksena, jossa haastateltiin toimeksiantayrityksen kahden eri konttorin työntekijöitä. Toimeksiantaja valitsi haastateltavat ja he olivat saaneet tutustua haastattelukysymyksiin ennakkoon. Haastateltavia oli yhteensä 16 ja he työskentelivät erilaisissa pankin työtehtävissä kuten asiakasneuvojina ja rahoitus- ja sijoitusasiantuntijoina. Haastateltavien koulutustaustat vaihtelivat, mutta yleisin koulutustausta oli kuitenkin liiketalouden eriasteiset tutkinnot. 75% haastateltavista oli työskennellyt toimeksiantajayrityksessä tai muissa pankeissa yli 10 vuotta ja loput 25% 1-5 vuotta.

Haastatteluille varattiin jokaisen haastateltavan kohdalla aikaa 15 minuuttia ja haastateltavat oli valittu toimeksiantajan puolesta ennakkoon. Omasta mielestäni yllättävä haastattelun tuloksista ilmenevä seikka oli, kuinka samankaltaisia vastuksia haastateltavat antoivat ja myöskään konttorikohtaisesti ei ollut havaittavissa selkeää eroa vastauksissa.

Kaikki haastateltavat kokivat tuntevansa henkilötietojen sääntelyn ja siihen liittyvän ohjeistuksen hyvin tai melko hyvin. Haastateltavat olivat lisäksi yleisesti sitä mieltä, että henkilötietoihin ja niiden suojaan kiinnitetään nykyään enemmän huomiota. Suurimpina muutoksina omassa työssään he mainitsivat, että nykyään asiakkaista kerätään selkeästi enemmän tietoja pankkiasiointia varten. Tästä johtuen myös tietojen dokumentointiin menee enemmän aikaa itse asiakaspalvelusta. Lisäksi henkilötietojen varmistamiseen ja tarkistamiseen menee aiempaa enemmän aikaa. Esimerkiksi nykyään asiakkaan henkilöllisyystodistus on skannattava järjestelmään, ennen riitti pelkkä henkilöllisyyden varmentaminen henkilöllisyystodistuksesta.

45% haastateltavista mainitsi epävarmuutta nousseen esiin henkilötietojen käsittelyn lain tai hyvän tavan mukaisuudesta tilanteissa, joissa henkilö, jolla ei ole suomen kansalaisuutta on halunnut avata asiakkuuden, tilin tai saada verkkopankkitunnukset. Tilanteessa haastateltavat ovat pohtineet onko asiakkaan esittämä henkilöllisyystodistus mahdollista todentaa ja täyttääkö se vahvan sähköisen tunnistautumisen kriteeristön, jota verkkopankkitunnusten avaamiseen vaaditaan. Lisäksi epävarmuutta on noussut esiin selvitettäessä, onko asiakas ulkomaille verovelvollinen ja jos hän on, mitkä lomakkeet on erityisesti täytettävä. Haastateltavat mainitsivat, että näitä tilanteita tulee työssä harvemmin vastaan, joten ohjeistusta ei aina täysin muista, kun tilanne tulee yllättäen

vastaan. Kollegoilta saa kuitenkin aina apua ja ohjeita. Tilanteet selvitetään useimmiten yhdessä.

Epävarmuutta toimintatavasta aiheuttavat myös iäkkäämmät asiakkaat. Voidaanko iäkkäälle asiakkaalle vielä antaa verkkopankkitunnukset, jos ei voida olla täysin varmoja, että hän ymmärtää niiden olevan henkilökohtaiset. Asiakkaan pankkisalaisuus ei saa vaarantua. Kolmantena epävarmuutta aiheuttavana tilanteena mainittiin tilanne, joissa asiakas ei suostu, että hänen tietojaan tai joitain lain hänestä vaatimaan tietoa talletetaan pankin järjestelmään.

Koulutus osiossa kaikki haastateltavat mainitsivat, että heitä on selkeästi ohjeistettu henkilötietojen käsittelyssä Pankin taholta ja 80 % haastateltavista oli sitä mieltä, että ohjeistus on ollut riittävää. Pankin yleisin ohjeistustapa ovat verkkokurssit, joita työntekijät seuraavat yhdessä tai omalla koneellaan. Lisäksi ohjeistuksia ja muutoksia käydään palavereissa yhdessä läpi. Ohjeistusta löytyy myös pankin sisäisestä intrasta.

20 % haastateltavista oli sitä mieltä, että ohjeistus on ollut hieman sekavaa ja sisäinen intra voisi olla selkeämpi, jotta tiedot ovat nopeasti löydettävissä. Ohjeista ja toimintatavoista voisi pitää myös kertauskursseja. Maahanmuuttajien muuttuvista tilanteista olisi hyvä myös saada tietoja nopeammin. Lisäksi toivottiin, että pankki panostaisi koulutukseen vieläkin enemmän, erityisesti uusien työntekijöiden perehdyttämisessä. Kaikille samat asiat eivät välttämättä ole yhtä selviä ja olisi hyvä varmistua siitä, että uudet työntekijät varmasti sisäistävät ohjeet ja toimintatavat.

Noin 40 % haastateltavista oli sitä mieltä, että myös itsellä on tietty vastuu omasta kouluttautumisesta. Tietoa tulee hakea ja ohjeistusta kerrata myös itsenäisesti. Kollegoiden kanssa keskustelemalla pystyy myös hyvin päivittämään omaa tietotasoaan. Itse asiakkaan henkilötietojen suojasta haastateltavat eivät kokeneet tarvitsevansa lisäkoulutusta. Tämän hetkinen tapa on toimiva. Asiakkaan henkilötietoihin liittyvän Pankin käytännön toiminnan osalta yleisin kehitysehdotus helpottamaan ja tehostamaan arjen työntekoa oli toive liittyen sovelluksiin, joihin asiakkaan henkilötietoja talletetaan. Haastateltavat toivoivat, että sovellukset keskustelisivat keskenään pankin järjestelmän sisällä. Tällä hetkellä sama tieto asiakkaasta täytyy merkitä moneen eri sovellukseen ja se vie turhaa aikaa. Järjestelmä voisi lisäksi automaattisesti muistuttaa puuttuvista asiakastiedoista.

Tämän lisäksi toivottiin digitaalisten palveluiden tehostamista. Vahvaa sähköistä tunnistautumista ja sähköistä allekirjoitusta voisi käyttää pankissa laajemminkin esimerkiksi

sopimuksissa. Tällöin sopimuksia ei tarvitsisi lähettää enää ollenkaan postitse asiakkaalle allekirjoitettavaksi, mikä lisäisi omalta osaltaan asiakkaan henkilötietojen suojaa.

Vastaajien määrä oli mielestäni sopiva haastattelukysymysten määrään ja tutkimuksen luonteeseen nähden. Henkilötietojen suoja on käsitteenä hyvin laaja ja haastattelusta olisi voinut tehdä vielä hieman pidemmän ja lisätä tarkentavia kysymyksiä. Kysymysten lisäämisessä olisi vain ollut se riski, että haastattelu eksyy liikaa itse aiheesta ja haastattelun tuloksista olisi vaikeampi saada selkeä kokonaiskuva, kun vastaukset olisivat olleet laaja-alaisempia.

9 JOHTOPÄÄTÖKSET

Tämän opinnäytetyön tavoitteena oli selvittää kuinka hyvin toimeksiantajayrityksen työntekijät tuntevat tämänhetkisen asiakkaidensa henkilötietojen suojaan ja käsittelyyn liittyvän sääntelyn ja kokevatko he tarvitsevansa aiheesta lisäkoulutusta työnantajansa taholta.

Tutkimus toteutettiin puolistrukturoidulla haastattelulla, jossa toimeksiantajayrityksen työntekijöille esitettiin valmiiksi muotoillut kysymykset. He saivat vastata kysymyksiin omin sanoin ja vastausten pituutta ei rajoitettu, tällöin myös haastattelutilanne oli vapaamuotoisempi ja keskustelunomaisempi. Mielestäni tätä menetelmää käyttäen päästiin mahdollisimman rehellisiin vastauksiin, joista saatiin hyvä kokonaiskuva tämänhetkisestä tilanteesta toimeksiantajayrityksen työntekijöiden toiminnasta henkilötietojen suojaan liittyvissä tilanteissa. Haastattelutilanne, jossa haastattelu tapahtuu kasvotusten, voi kuitenkin vaikuttaa haastateltavan vastauksiin. Haastateltava ei välttämättä halua kertoa omaa rehellistä mielipidettään suoraan vaan voi kaunistella omaa näkemystään. Lisäksi haastateltava voi kiireisestä aikataulustaan johtuen vastata lyhyemmin ja unohtaa asioita joita hänen piti vielä vastukseensa lisätä. Myös sillä on vaikutusta, onko haastateltava henkilö kiinnostunut aiheesta, josta häntä haastatellaan.

Vaihtoehtoinen tutkimusmenetelmä olisi ollut lomaketutkimus, jossa aiheesta olisi saatu vielä yksityiskohtaisempaa ja kattavampaa tietoa. Sähköisen kyselylomakkeen lähettäminen toimeksiantajayrityksen työntekijöille olisi kuitenkin kuormittanut heidän sähköpostiaan. Vastausprosentti olisi todennäköisesti jäänyt pieneksi, kun erillistä aikaa vastaamiselle ei olisi järjestetty ja kyselylomake olisi ollut vaan yksi sähköpostiviesti muiden joukossa. Haastattelututkimus oli toimivampi tälle työlle.

Työn teoriaosuudessa pyrittiin kertomaan kattavasti mitä henkilötietojen suojaan ja käsittelyyn sisältyy ja kartoittamaan sen tämän hetkistä sääntelyä. Sääntelyä selkeyttävät lainkohdat henkilötietolaista ja sähköisen viestinnän tietoturvalaista sekä tietosuojalautakunnan antamat päätökset henkilötietojen suojaan liittyen. Työn teoriaosuus tukee empiiristä osuutta mielestäni hyvin.

Mielestäni yrityksien, jotka päivittäin käsittelevät ja hallinnoivat henkilötietoja tulisi tulevaisuudessakin pitää huolta, että koko organisaation toimijat ovat varmasti tietoisia hen-

kilötietojen suojaan ja tietoturvaan liittyvistä sääntelymuutoksista. Kiristyvään ja tarkentuvaan sääntelyyn on pystyttävä vastaamaan. Ohjeistuksen tulisi olla nopeaa, jotta henkilötietojen suoja pystytään joka tilanteessa turvaamaan. Tietosuojariskit olisi myös otettava paremmin huomioon ja niiden ennaltaehkäisyyn olisi hyvä tehdä erillinen toimintamalli tai -suunnitelma. Tietosuojavastaava olisi hyvä olla nimettynä pienimmissäkin yrityksissä, sillä suurin osa tämän päivän yrityksistä hallinnoi sähköistä asiakasrekisteriä ja tietosuojariskit on hyvä tällöin olla tiedostettuina.

Henkilötietojen suojaan ja käsittelyyn liittyvän tutkimuksen voisi tehdä laajemminkin. Tutkimuksen voisi ulottaa koskemaan kokonaisen yrityksen tai organisaation toimintatapaa, ei ainoastaan sen työntekijöiden toimintaa. Näin saataisiin tutkimustuloksia koko organisaation toiminnasta henkilötietojen suojaan ja käsittelyyn liittyen. Olisi mielenkiintoista tutkia myös yrityksen asiakkaiden kokemuksia, kuinka he kokevat henkilötietojensa suojan toteutuvan yrityksen toiminnassa. Tutkimuksen voisi ulottaa myös eri toimialoille ja toimiala kohtaista sääntelyä ja sen puutteita voisi verrata. Tietosuoja ja -turva olisivat myös aivan omat tutkimusalueensa. Kiihtyvän digitalisaation vaikutus henkilötietojen suojaan olisi varmasti mielenkiintoinen tutkimuskohde.

LÄHTEET

Aarnio, R. Mitä tietosuoja tarkoittaa? Viitattu 6.2.2017
https://koulutus.fcg.fi/Portals/2/Dokumentit/Reijo%20Aarnio%20MIT%C3%84%20TIETO-SUOJA%20TARKOITTAA%5BCompatibility%20Mode%5D.pdf

Castrén, K. 2015. Tietosuoja. Viisas johtaja sijoittaa tietosuojaan ja tietoturvaan. Viitattu 18.1.2017
https://www.tietosuoja-lehti.fi/index.php?mid=2&pid=32&aid=3529

CEN Workshop Agreement 2006. Personal Data Protection Audit Framework. Viitattu 6.2.2017
ftp://ftp.cenorm.be/public/cwas/e-europe/dpp/cwa15499-01-2006-feb.pdf

Data protecion working party 2011. Opinion 15/2011 on the definition of consent. Viitattu 9.1.2017
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

EuroPriSe GmbH. European Privacy Seal. 2008-2016. Viitattu 23.1.2017
https://www.european-privacy-seal.eu/EPS-en/Product-and-Service-Privacy-Certification

HE 96/1998. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi. Viitattu 9.1.2017
http://www.finlex.fi/fi/esitykset/he/1998/19980096

HE 309/1993. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta. Viitattu 4.1.2017
http://www.finlex.fi/fi/esitykset/he/1993/19930309

Henkilötietolaki 523/1999. Annettu Helsingissä 22.4.1999. Saatavilla sähköisesti osoitteessa
http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Koillinen, M. 2013. Henkilötietojen suoja itsenäisenä perusoikeutena. Viitattu 4.1.2016
https://www.edilex.fi/oikeus/10414

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007. Annettu Helsingissä 9.2.2007. Saatavilla sähköisesti osoitteessa
http://www.finlex.fi/fi/laki/ajantasa/2007/20070159

Laki sähköisestä lääkemääräyksestä 61/2007. Annettu Helsingissä 2.2.2007. Saatavilla sähköisesti osoitteessa
http://www.finlex.fi/fi/laki/ajantasa/2007/20070061

Laki yksityisyyden suojasta työelämässä 759/2004. Annettu Helsingissä 13.8.2004. Saatavilla sähköisesti osoitteessa
http://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Lehto, K. 2013. Tietojenkalastelu eli Verkkourkinta (phishing). Viitattu 18.1.2017
https://wiki.metropolia.fi/pages/viewpage.action?pageId=62195969

Lepistö, T. 2016. Varmuuskopiointi ja tietoturva mikroyrityksessä. Kandidaattityö. Tietotekniikan koulutusohjelma. Lappeenranta: Lappeenrannan teknillinen yliopisto. Viitattu 18.1.2017
http://www.doria.fi/bitstream/handle/10024/124116/Kandidaatintyö_Lepistö_Toni_2016.pdf;jsessionid=427840F62444A8A83A0AF6B76633F967?sequence=2

Luottotietolaki 527/2007. Annettu Helsingissä 11.5.2007. Saatavilla sähköisesti osoitteessa
http://www.finlex.fi/fi/laki/ajantasa/2007/20070527

Mäenpää, P. 2014. Henkilötietolaki. BioMediTech. Viitattu 12.1.2017 http://biomeditech.fi/databank/naytelait/lait_henkilotieto.html

Neuvonen, R. 2014. Yksityisyyden suoja Suomessa. Helsinki: Lakimiesliiton kustannus.

Nurmi, H. 2008. Työnantajan oikeudesta käsitellä työntekijän henkilötietoja. Pro gradu. Yritysjuridiikka. Tampere: Tampereen yliopisto. Viitattu 4.1.2017 https://tampub.uta.fi/bitstream/handle/10024/78938/gradu02475.pdf?sequence=1

Oikeusministeriö 2015. Tietoverkkorikoksia koskevat säännökset täsmentyvät syyskuun alussa - identiteettivarkaus rangaistavaksi itsenäisenä rikoksena. Viitattu 25.1.2017 http://oikeusministerio.fi/fi/index/ajankohtaista/tiedotteet/2015/09/tietoverkkorikoksiakoskevatsaannoksettasmentyvatsyyskuunalussa-identiteettivarkausrangaistavaksiitsenaisenarikoksena.html

PeVL 5/1999 vp. Perustusvaliokunnan lausunto 5/1999 vp. Viitattu 21.3.2017 https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_5+1999.pdf

PeVL 5/2013 vp. Perustusvaliokunnan lausunto 5/2013 vp. Eduskunta. Viitattu 11.1.2017 https://www.eduskunta.fi/FI/vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiakirjat&docid=pevl+5/2013

Salminen, M. 2009. Tietosuoja sähköisessä liiketoiminnassa. Helsinki:Talentum.

Suomen perustuslaki 731/1999. Annettu Helsingissä 11.6.1999. Saatavilla sähköisesti osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Tietosuojalautakunta 2007. Toimivalta - Perintä - Luottotietotoiminta - Luottotiedot- - Käyttötarkoitussidonnaisuus - Toimeksianto – Tarkastusoikeus. Diaarinumero: 6/932/2006. Taltio:4/07 Viitattu 4.1.2017 http://www.finlex.fi/fi/viranomaiset/ftie/2007/20070004

Tietosuojalautakunta 2008. Soveltamisala - Henkilötieto - Arkaluonteinen tieto - Tietosuojalautakunnan määräys. Diaarinumero: 1/933/2008. Taltio: 2/2009. Viitattu 6.2.2017 http://www.finlex.fi/fi/viranomaiset/ftie/2009/20090002

Tietosuojavaltuutetun toimisto 2010a. Rekisteröidyn kielto-oikeus. Viitattu 12.1.2017 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqC7x0Z/Rekisteroidyn_kieltooikeus.pdf

Tietosuojavaltuutetun toimisto 2010b. Tietosuojavastaavan toimenkuva, tehtävät ja asema. Viitattu 18.1.2017 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqN4sf1/Tietosuojavastaavan_toimenkuva_tehtavat_ja_asema.pdf

Tietosuojavaltuutetun toimisto 2013. Henkilötietolaki. Viitattu 3.1.2017 http://www.tietosuoja.fi/fi/index/lait/Henkilotietolaki.html

Tietosuojavaltuutetun toimisto 2014d. Henkilötunnus. Viitattu 23.1.2017 http://www.tietosuoja.fi/fi/index/useinkysyttya/henkilotunnus.html

Tietosuojavaltuutetun toimisto 2014c. Miten huomioit rekisteröityjen oikeudet? Viitattu 12.1.2017 http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/mitenhuomioitrekisteroityjenoikeudet.html

Tietosuojavaltuutetun toimisto 2014b. Rekisteröidyn oikeudet. Viitattu 12.1.2017 http://www.tietosuoja.fi/fi/index/rekisteroidylle/rekisteroidynoikeudet.html

Tietosuojavaltuutetun toimisto 2014a. Viranomainen ei saa asiakkaan suostumuksellakaan lähettää salassa pidettäviä asiakastietoja suojaamattomassa sähköpostissa. Diaarinumero 423/49/2009. Viitattu 12.1.2017
http://www.tietosuoja.fi/fi/index/ratkaisut/viranomaineneisaaasiakkaansuostumuksella.html

Vanto, J. 2011. Henkilötietolaki käytännössä. Helsinki: WSOYpro Oy.

Virtuaalilakimies 2017. Keskeisiä käsitteitä. Viitattu 4.1.2017
https://virtuallawyer.fondiatools.com/Sivut/Keskeisi%C3%A4%20k%C3%A4sitteit%C3%A4.aspx

Viestintävirasto 2013. S-Pankin nimissä lähetetty huijausviestejä lukuisille suomalaisille internetin käyttäjille. Viitattu 18.1.2017
https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2013/11/ttn201311151000.html

Viljanen, V. 2017. Yksityisyydensuoja. Lainsäädäntö. Viitattu 6.2.2017
https://www.yksityisyydensuoja.fi/lains%C3%A4%C3%A4d%C3%A4nt%C3%B6

Haastattelulomake

Taustakysymykset

1. Kuinka kauan olet työskennellyt pankissa?
    - Alle vuoden
    - 1-5 vuotta
    - 5-10 vuotta
    - Yli 10 vuotta

2. Mikä on korkein suorittamasi koulutus/tutkinto?
    - Peruskoulu
    - Lukio tai ammattikoulu
    - Korkeakoulututkinto

Henkilötiedot

1. Kuinka hyvin koet tuntevasi henkilötietojen käsittelyyn liittyvän sääntelyn?

    - Hyvin
    - Melko hyvin
    - Melko huonosti
    - Huonosti

2. Minkälaisia henkilötietoja pääasiassa työssäsi käsittelet?

3. Oletko huomannut työssäsi, että henkilötietojen suojaan kiinnitetään nykyään aikaisempaa enemmän huomiota?

4. Onko lisääntyvä henkilötietojen suojan sääntely vaikuttanut työhösi?

5. Oletko kohdannut työpaikallasi tilanteita, joissa olet ollut epävarma henkilötietojen käsittelyn lain tai hyvän tavan mukaisuudesta?

Koulutus

6. Onko sinua ohjeistettu työpaikallasi henkilötietojen käsittelyssä ja minkä laista ohjeistusta olet saanut?

7. Onko ohjeistus ollut mielestäsi riittävää?

8. Onko sinulla jotain kehitysehdotuksia pankin henkilötietoihin liittyvän käytännön toiminnan osalta?

9. Onko sinulla kehitysehdotuksia koulutuksen osalta? Minkälaista koulutusta toivoisit?