LAUREA AMMATTIKORKEAKOULU Uuden edellä

Luonnosehdotus tietosuojan organisoinnista S-ryhmässä

Karonen, Jarkko

2012 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Luonnosehdotus tietosuojan organisoinnista S-ryhmässä

Jarkko Karonen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Huhtikuu, 2012

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Turvallisuusalan koulutusohjelma

Jarkko Karonen

Luonnosehdotus tietosuojan organisoinnista S-ryhmässä

Vuosi 2012 Sivumäärä 42

Tietosuojalla suojataan henkilön oikeutta yksityisyyteen. Kyseessä on perustuslaillinen oikeus ja henkilötietojen käsittelystä säädetään tarkemmin henkilötietolaissa. Yrityksen näkökulmasta tietosuojalla tarkoitetaan niin yrityksen työntekijöiden, kuin asiakkaidenkin henkilötietojen ja yksityisyyden suojaamista.

Tietosuojalainsäädäntö on muutoksen edessä. Nykyinen Euroopan Unionin (EU) tietosuojadirektiivi on vuodelta 1995 ja jäsenvaltiot ovat implementoineet sen jokainen omalla tavallaan, mikä on johtanut vaihtelevaan lainsäädäntöön EU:n alueella. Myös tietotekniikka ja internetin käyttö ovat kehittyneet paljon 17 vuoden aikana. Vastatakseen nykyaikaisiin tietosuojahaasteisiin, Euroopan Komissio julkaisi tammikuussa 2012 luonnoksen uudesta tietosuoja-asetuksesta. Asetus tulee vielä muotoutumaan ennen lopullista julkistamista, mutta varmaa on se, että tietosuojalainsäädäntö tulee oleellisesti kiristymään koko EU:n alueella.

Tämä opinnäytetyö on Suomen Osuuskauppojen Keskuskunnan (SOK) Riskienhallinta-yksikölle tuotettu luonnosehdotus tietosuojan organisoinnista S-ryhmässä. Työn tavoitteena oli kehittää malli, joka mahdollistaisi tietosuojan keskitetyn kehittämisen ja koordinoinnin koko S-ryhmän tasoisesti. Työ tuotettiin tutkimuksellisen kehittämisen menetelmiä käyttäen ja työ oli osa suurempaa, koko S-ryhmän tietosuojan kehittämiseen tähtäävää projektia.

Työn teoriapohja muodostuu voimassaolevasta lainsäädännöstä, valvovan viranomaisen ohjeista sekä Euroopan Komission luonnoksesta uudeksi tietosuoja-asetukseksi. Keskeisen aineiston muodostavat asiantuntijahaastattelut, joissa S-ryhmän omilta asiantuntijoilta kysyttiin, miten tietosuoja tulisi organisoida S-ryhmässä.

Asiasanat: tietosuoja, yksityisyys, lainsäädäntö, henkilötietolaki

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Security Management

Jarkko Karonen

Draft proposal for organizing data protection in the S-Group

Year 2012 Pages 42

Data protection refers to a person's right to privacy, which in Finland is a constitutional right. The Personal Data Act sets out rules for personal data protection in more detail. For companies, data protection means not only protecting the privacy of the employees but the customers as well.

The data protection legislation is about to change. The current European Data Protection Directive was released in 1995. Technology and the use of the Internet have substantially evolved during this 17 year period. In addition, all the member states of the European Union (EU) have implemented the directive differently causing incoherent legislation within the EU. In January 2012 the European Commission published a draft of the new General Data Protection Regulation. The draft is not final during the time of writing this, but it is clear that the rules will be notably tightened throughout the EU area.

This thesis is a draft proposal produced for the SOK Corporation's Risk Management Unit. The proposal concerns organizing data protection in the S-Group. The objective was to develop a centralized model for managing data protection in a way that allows coordination and development of data protection in the whole S-Group. This thesis is a case study and it was part of a bigger project focusing on developing data protection within the S-Group.

The theory basis of this thesis consists of the current Finnish legislation, the Data Protection Ombudsman's directions and the European Commission's draft of the new General Data Protection Regulation. The main part of the information in this thesis was collected by interviewing the experts on data protection within the S-Group.

Keywords: Data Protection, Data Privacy, Legislation, Personal Data Act

Sisällys

1 Johdanto

Suoritin työharjoitteluni Suomen Osuuskauppojen Keskuskunnan (SOK) Riskienhallinta-yksikköön, josta tarjottiin tilaisuutta myös opinnäytetyön tekemiseen. Opinnäytetyöni aiheeksi rajautui luonnosehdotuksen tekeminen S-ryhmän tietosuojan kehittämiseen tähtäävän projektiin. Projektin tavoitteena on kehittää tietosuojaa S-ryhmässä ja tuottaa S-ryhmälle yhteinen ja koordinoitu tietosuojan toimintamalli (Tupala 2012).

Tietosuojalainsäädäntö on muutoksen edessä, sillä Euroopan Komissio julkaisi tammikuussa 2012 luonnoksen uudesta tietosuoja-asetuksesta. Suurin syy lainsäädännön uudistumiseen on se, että teknologian kehittyminen ja globalisaatio ovat muuttaneet tapaa, jolla henkilötietoja käsitellään. Lisäksi tällä hetkellä voimassaoleva, 17 vuotta sitten julkaistu tietosuojadirektiivi tehtiin silloisen internetin tarpeisiin. Merkittävin syy uudistukselle on kuitenkin se, että vuoden 1995 direktiiviä on sovellettu eri EU maissa eri tavoin, jonka vuoksi EU:ssa ei ole yhtenäistä tietosuojalainsäädäntöä. Uuden tietosuoja-asetuksen tarkoituksena on luoda koko EU:n alueelle yksi yhtenäinen tietosuojalainsäädäntö, jota kaikki noudattavat samalla tavalla. Uusi tietosuoja-asetus tulee kiristämään tietosuojalainsäädäntöä Suomessakin lisäämällä kuluttajan oikeuksia ja rekisterinpitäjän velvollisuuksia. (Euroopan Komissio 2012.)

Tietosuoja on ollut ajankohtainen aihe Suomessa vuoden 2011 loppupuolella tapahtuneiden tietovuotojen takia (Salminen 2011). Aihe oli esillä myös hiihtäjä Mika Myllylän kuolinsyyntutkintaan liittyen, kun julkisuuteen levisi epäilys siitä, että mahdollisesti jopa 200 poliisia kävi vain uteliaisuuttaan tekemässä hakuja poliisin tietojärjestelmästä (Helsingin Sanomat 2012).

Suomessa tietosuojaa valvova viranomainen, tietosuojavaltuutetun toimisto toimii aktiivisesti tietosuojan kehittämiseksi ja edistämiseksi. Tietosuojavaltuutetun toimisto suoritti vuoden 2011 lopulla tarkastuksen, joka kohdistui noin sadan yrityksen kanta-asiakasjärjestelmiin. Tarkastuksessa selvitettiin henkilötietojen käsittelyä ja siitä viestimistä. Tarkastuksen tuloksena tietosuojavaltuutettu toteaa, että laajimpien järjestelmien ylläpitäjillä vaikuttaa olevan hyvä tietämys tietosuoja-asioista (Tietosuojavaltuutetun toimisto 2012b).

Tietosuojavaltuutetun toimiston tarkastuksessa havaittiin, että suurimmat haasteet yleisellä tasolla liittyvät toiminnan läpinäkyvyyden puutteisiin. Haasteita aiheuttavat informaation löydettävyys, hajanaisuus sekä ajantasaisuus. Tietosuojavaltuutetun mukaan kuluttaja joutuu itse olemaan aktiivinen tiedonetsinnässä ja kokonaiskuvan muodostaminen kanta-asiakkuudesta voi olla hankalaa. (Tietosuojavaltuutetun toimisto 2012b.)

Asiakasomistaja on S-ryhmän strategian ytimessä. Korkealla tietosuojan tasolla varmistetaan se, että asiakkaita palvellaan lainsäädännön vaatimusten mukaisesti. Vaatimustenmukaisuus ilmenee myös S-ryhmän vastuullisuusperiaatteista, joiden keskiössä on lakien noudattaminen ja oman toiminnan jatkuva parantaminen. Tietosuoja liittyy myös S-ryhmän arvoihin, joissa todetaan, että asiakkaita palvellaan rehellisesti, ystävällisesti ja että S-ryhmässä toimitaan eettisesti. (Tupala 2012.)

2 Opinnäytetyön tavoite, rajaukset, määritelmät & kohdeorganisaatio

Tässä luvussa kuvataan opinnäytetyön tavoitteet, rajaukset ja määritelmät sekä kohdeorganisaatio. Tuomen ja Sarajärven (2009, 156-157) mukaan työn tavoite tulee ilmaista selkeästi. Aiheen rajaaminen on tärkeää, koska muuten työstä voi tulla mahdottoman laaja (Hirsjärvi, Remes & Sajavaara 2009, 81-88).

Määritelmillä pyritään siihen, että lukija ymmärtäisi jonkin tietyn termin mahdollisimman samalla tavalla kuin kirjoittaja (Hirsjärvi ym. 2009, 152). Kohdeorganisaation kuvaaminen on tärkeätä, sillä S-ryhmän osuustoiminnalle tyypillinen omistus- ja ohjausrakenne vaikuttaa merkittävästi tässä työssä esitettyihin tuloksiin.

2.1 Tavoite

Kenellä on vastuu rekisterinpidosta? Kuka kouluttaa rekisterin käyttäjät? Kuka valvoo rekisterin omistajaa? Lain mukaan vastaus on selvä, rekisterinpitäjänä toimiva yritys eli loppukädessä sen johto vastaa siitä, että tietosuojalainsäädäntöä noudatetaan henkilötietojen käsittelyssä (Henkilötietolaki 1999/523, 5 §). Käytännössä rekisterinpitäjänä toimiva yritys päättää itse miten rekisterinpitoon liittyvät tehtävät ja vastuut organisoidaan käytännössä.

Opinnäytetyön tavoitteena on luoda S-ryhmälle kehittämisehdotus tietosuojan organisoinnista. Mallin tulee mahdollistaa tietosuojan keskitetty kehittäminen ja koordinointi koko S-ryhmässä ja lisätä yhteistyötä rekisterin omistajien välillä. Työssä tulee ottaa huomioon myös tuleva EU-tasoinen lainsäädäntömuutos, siten kun se tässä vaiheessa on järkevästi toteutettavissa.

Lisäksi työn tavoitteena on tukea S-ryhmän tietosuojan kehittämiseen tähtäävää projektia ja siihen liittyvää päätöksentekoa. Työ tukee myös tietosuojaprojektin tuotosten jalkauttamista S-ryhmässä.

2.2 Rajaukset

Tämä opinnäytetyö keskittyy tietosuojan organisoinnin kehittämiseen S-ryhmässä. S-ryhmällä tarkoitetaan kaikkia osuuskauppoja ja SOK-yhtymää (Tietoa S-ryhmästä 2012).

Työn ulkopuolelle on rajattu viranomaistoiminta sekä yksityisten henkilöiden suorittama henkilötietojen käsittely. Lakia yksityisyyden suojasta työelämässä huomioidaan vain tarvittavilta osin. Työssä keskitytään lähinnä organisatorisiin toimenpiteisiin, tekniset järjestelyt ja ratkaisut on rajattu selvityksen ulkopuolelle.

Tässä työssä ei tehdä erotella yrityksen työntekijöitä asiakkaista, vaan työ keskittyy yhtälailla molempien yksityisyyden suojaamiseen.

2.3 Määritelmät

Hirsjärven ym. (2009, 152) mukaan määritelmiä tarvitaan monesta eri syystä, ne rajaavat käsitteet ja antava niille merkitykset. Määritelmät myös luovat normit ja sitovat yhteen käsitteen ja sen nimityksen (Hirsjärvi ym. 2009, 152). Määritelmillä siis pyritään varmistamaan, että lukija ymmärtää termin samalla tavalla kuin kirjoittaja. Tässä alaluvussa on määritelty tämän opinnäytetyön kannalta keskeiset termit

Tietosuojalla tarkoitetaan ihmisten yksityiselämän suojaa ja muita sitä turvaavia oikeuksia henkilötietoja käsiteltäessä (Tietosuojavaltuutetun toimisto 2012a). Tässä selvityksessä tietosuojalla tarkoitetaan niitä keinoja, joilla rekisterinpitäjä suojaa henkilötiedot asiattomalta pääsyltä ja vahingossa tai laittomasti tapahtuvalta hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä (Henkilötietolaki 1999/523, 32 §).

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 (Henkilötietolaki 1999/523, 3 §).

Henkilötietojen käsittelyllä tarkoitetaan henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä (Henkilötietolaki 1999/523, 3 §), eli käytännössä kaikkea mitä henkilötiedoille tehdään.

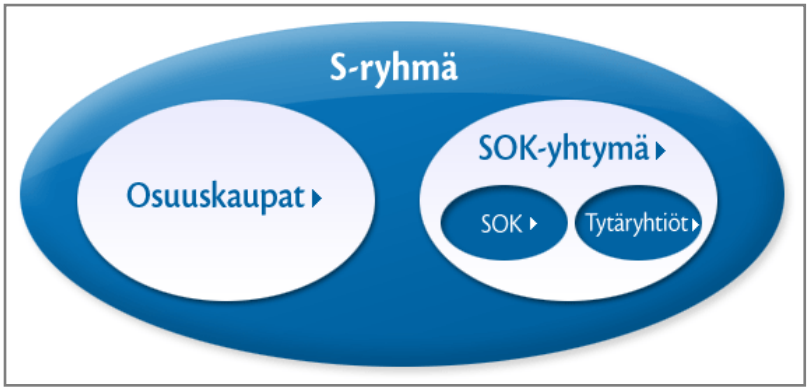
Henkilörekisterillä ja myöhemmin rekisterillä tarkoitetaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitel-

lään 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 (Henkilötietolaki 1999/523, 3 §).

Rekisterinpitäjällä tarkoitetaan juridista yritystä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty (Henkilötietolaki 1999/523, 3 §).

2.4 Kohdeorganisaatio

Opinnäytetyön tilaaja oli Suomen Osuuskauppojen Keskuskunnan (SOK) Riskienhallinta-yksikkö ja tietoturvallisuuspäällikkö Vesa Tupala toimi työn ohjaajana tilaajan puolelta.



Kuva 1: S-ryhmän rakenne (Tietoa S-ryhmästä 2012).

S-ryhmä muodostuu osuuskaupoista ja Suomen Osuuskauppojen Keskuskunnasta (SOK) sekä sen tytäryhtiöistä (Kuva 1). Alueosuuskaupat ovat osuustoiminnallisia juridisesti itsenäisiä yrityksiä, jotka yhdessä omistavat SOK:n. S-ryhmän tarkoituksena on palvelujen ja etujen tuottaminen asiakasomistajille. Asiakasomistajat ovat nimensä mukaisesti alueosuuskauppojen omistajia. (Tietoa S-ryhmästä 2012.)

Alueosuuskauppoja on 21 ja ne ovat jakautuneet koko maan kattavaksi verkostoksi. Suurin alueosuuskauppa on pääkaupunkiseudulla toimiva HOK-Elanto. Alueosuuskauppojen lisäksi S-ryhmään kuuluu 8 paikallisosuuskauppaa. (Tietoa S-ryhmästä 2012.)

S-ryhmä tarjoaa asiakkailleen päivittäistavara- ja käyttötavarakaupan, liikennemyymälä- ja polttonestekaupan, matkailu- ja ravitsemiskaupan, auto- ja autotarvikekaupan sekä maatalouskaupan palveluja. S-ryhmällä on myös verkkokauppoja. S-ryhmän ketjuja ovat mm. Prisma, Sokos, S-market, Sale, Sokos Hotels, ABC ja Automaa. (Tietoa S-ryhmästä 2012.)

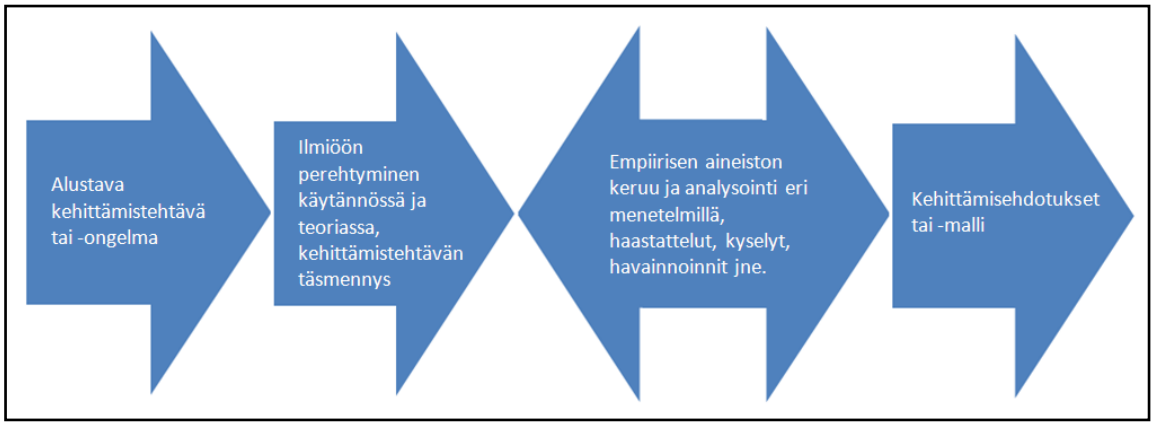
Asiakasomistajia S-ryhmällä on noin 2 miljoonaa ja henkilöstöä 42 000. Vuonna 2011 koko S-ryhmän vähittäismyynti oli noin 11 460 miljoonaa euroa. Tulos ennen satunnaisia eriä oli 269 miljoona euroa. Toimipaikkoja S-ryhmällä oli vuoden 2011 joulukuun lopussa 1668, joista 1643 Suomessa. Sekä päivittäistavarakaupan, että käyttötavarakaupan myynti kasvoivat edellisestä vuodesta. (Taloustiedote 2012.)

SOK on vuonna 1904 perustettu osuuskunta, jonka alueosuuskaupat omistavat. SOK:n tehtävänä on tuottaa keskitetysti yhteisiä palvelu- ja tukitoimintoja sekä kehittää ja ohjata S-ryhmän strategioita. SOK:lla on myös omaa liiketoimintaa Baltian alueella ja Pietarissa. SOK:n pääjohtajana toimii Kuisma Niemelä. (Tietoa S-ryhmästä 2012.)

SOK Riskienhallinta on seitsemän hengen asiantuntijayksikkö, jonka tehtävänä on ohjata ja kehittää S-ryhmän kokonaisvaltaista riskienhallintaa. Riskienhallintayksikkö tukee yhtiöitä ja muita yksiköitä riskienhallinnan toteuttamisessa. Riskienhallintayksikkö tarjoaa asiantuntijapalveluita mm. seuraavilta osa-alueilta: kokonaisvaltainen riskienhallinta, yritysturvallisuus, tietoturvallisuus, vakuuttaminen, hävikinhallinta sekä liiketoiminnan jatkuvuussuunnittelu. (Koskinen 2009.)

3 Työn toteutus ja menetelmät

Tämä opinnäytetyön on tapaustutkimus, jonka tuottamiseen on käytetty laadullisen tutkimuksen menetelmiä. Ojasalon, Moilasen ja Ritalahden (2009, 37-38) mukaan tapaustutkimus soveltuu hyvin menetelmäksi tilanteisiin, joissa tavoitteena on tuottaa kehittämisehdotuksia jollekin tietylle organisaatiolle. Tapaustutkimukselle on tyypillistä se, että varsinaista muutosta tai kehittämisideaa ei vielä toteuteta organisaatiossa (Ojasalo ym. 2009, 38), kuten meneteltiin myös tämän työn kohdalla.



Kuva 2: Tapaustutkimuksen vaiheet (Ojasalo ym. 2009, 54.)

Opinnäytetyö toteutettiin tapaustutkimuksen vaiheistusta (Kuva 2) noudattaen. Alustava kehittämistehtävä oli tuottaa selvitys tietosuojaan liittyvistä rooleista SOK-yhtymän tietosuojan kehittämisprojektia varten. Aiheeseen eli ilmiöön perehtyminen tapahtui lainsäädäntöä, valvovan viranomaisen ohjeita sekä S-ryhmän tietosuoja ja -tietoturvaohjeita analysoimalla. Myöhemmin varsinaiseksi kehittämistehtäväksi tarkentui luonnosehdotuksen tekeminen tietosuojan organisoinnista koko S-ryhmässä.

Empiirinen aineisto kerättiin pääosin asiantuntijahaastattelujen avulla. Ojasalon ym. (2009, 40) mukaan kehittämistyössä on suositeltavaa käyttää useampia menetelmiä, koska eri menetelmät täydentävät toisiaan. Työn tietoperusta kerättiin dokumenttianalyysin avulla lainsäädännöstä ja tietosuojavaltuutetun ohjeista.

Työn tulokset eli kehittämisehdotukset on esitelty työn loppupuolella. Kehittämistyössä on tarkoituksena tuottaa kehittämisen tueksi uutta tietoja, työn yleisö on yleensä jokin muu kuin tiedeyhteisö (Ojasalo ym. 2009, 46-47). Tässä opinnäytetyössä tarkoitus oli tuottaa tietoa S-ryhmän tietosuojan kehittämisprojektiin ja opinnäytetyö tuotettiin SOK Riskienhallinnalle.

3.1 Lähtökohdat

Opinnäytetyön lähtökohdat olivat selkeät ja aiheen asetti SOK Riskienhallinta -yksikkö, eli työn tilaaja. Työn aiheena oli luonnosehdotuksen tekeminen tietosuojan organisoinnista koko S-ryhmässä.

SOK-yhtymässä oli tehty vuoden 2011 aikana tietosuojaan kohdistuva arviointi, jossa yhdeksi kehittämiskohteeksi tunnistettiin yhtenäisemmän tietosuojan ohjausmallin kehittäminen. Rekistereihin liittyvää toimintaa on aiemmin ohjattu rekisteri- ja yksikkökohtaisesti. Tietosuojaa on kehitetty riskienhallinnan ja lainsäädännön näkökulmista, mutta ohjausvastuuta ei ole osoitettu yksiselitteisesti.

Edellä mainitun tarkastuksen tunnistettuihin kehittämiskohteisiin pohjautuen tämän työn tavoitteena oli määrittää ehdotus tietosuojan keskitetystä kehittämisestä ja koordinoinnista koko S-ryhmässä. Ehdotuksen tuli valmistaa tulevaan tietosuojalainsäädännön muutokseen siten, että tulevien vaatimusten toteuttaminen olisi mahdollista varmistaa mahdollisimman tehokkaasti.

3.2 Aineiston hankinta

Haastattelu, kysely, havainnointi ja erilaisiin dokumentteihin perustuva tieto ovat yleisimpiä laadullisessa tutkimuksessa käytettäviä aineistonhankintamenetelmiä (Tuomi & Sarajärvi 2009, 71). Tässä opinnäytetyössä aineiston hankinta perustui haastatteluista ja dokumenteista saatuun tietoon. Tuomen ja Sarajärven (2009, 71) mukaan eri aineistonkeruumenetelmiä voi käyttää vaihtoehtoisesti, rinnan tai eri tavoin yhdisteltyinä. Ojasalon ym. (2009, 46-47) mukaan eri menetelmiä tulisikin käyttää rinnan, jotta kehittämisen tueksi saadaan mahdollisimman monipuolista tietoa. Haastatteluja käytettiin syventämään ja tarkentamaan dokumenttien pohjalta saatua tietoa juuri S-ryhmälle sopivaksi.

Suomen henkilötietolaki, tietosuojavaltuutetun toimiston ohjeet ja Euroopan Komission luonnos uudesta tietosuoja-asetuksesta ovat merkittävimmät dokumentit, joita käytettiin lähdeaineistona. Voimassa olevan henkilötietolain tarkoituksena on suojata henkilöiden oikeutta yksityisyyteen ja edistää hyvän tietojenkäsittelyntavan kehittämistä ja noudattamista (Henkilötietolaki 1999/523, 1 §). Tietosuojavaltuutetun toimiston yhtenä tehtävänä on tuottaa henkilötietolaista kertovaa ohjaus ja tiedotemateriaalia (Tietosuojavaltuutetun toimisto 2012d). EU:n tietosuojalainsäädäntö on opinnäytetyön kirjoittamishetkellä uudistumassa ja luonnos uudesta tietosuoja-asetuksesta julkaistiin 25.1.2012. Kyseessä on luonnos, joka tulee vielä muotoutumana ennen virallista julkistamista, mutta kyseinen dokumentti valittiin lähteeksi, sillä siitä saadaan tietoa suunnasta, johon tietosuojalainsäädäntö on kehittymässä.

Opinnäytetyö oli osa suurempaa tietosuojaprojektia, joten oli luontevaa valita aineistonkeruun tavaksi haastattelu, kyseisen menetelmän joustavuuden takia. Haastattelussa on tärkeintä saada mahdollisimman paljon tietoa tutkittavasta asiasta (Tuomi & Sarajärvi 2009, 73). Haastattelu on erityinen tiedonkeruumenetelmä, koska siinä ollaan suorassa kielellisessä vuorovaikutuksessa tutkittavan kanssa (Hirsjärvi ym. 2009, 207-208).

Hirsjärven ym. (2009, 164) mukaan laadullisessa tutkimuksessa on tyypillistä, että kohdejoukko valitaan tarkoituksenmukaisesti. Eliittiotanta on otantamenetelmä, jossa pieneksi tai suureksi kohdejoukoksi valitaan henkilöitä, joilta oletetaan saavan parhaiten tietoa tutkittavasta asiasta (Tuomi & Sarajärvi 2009, 86). Tapaustutkimukselle haastattelu on tyypillinen menetelmä, koska tietoa halutaan saada kehitettävän ilmiön asiantuntijoilta (Ojasalo ym. 2009, 55). Tässä opinnäytetyössä haastateltaviksi henkilöiksi valittiin asiantuntijoita eli S-ryhmän tietosuojan kehittämiseen tähdänneen projektin työryhmän jäseniä ja rekisterien käytöstä päättäviä tahoja.

Haastattelut toteutettiin avoimina asiantuntijahaastatteluina, joissa aihe oli sovittu etukäteen. Avoimessa haastattelussa selvitetään haastateltavan ajatuksia, mielipiteitä ja käsityksiä sen mukaan kuin ne tulevat esiin keskustelussa (Hirsjärvi ym. 2009, 209-211). Osaa haastateltavista haastateltiin useampaan kertaan joidenkin vastausten tarkentamiseksi. Haastattelut toteutettiin sekä yksilö-, pari-, että ryhmähaastatteluina. Ryhmähaastattelu on tehokasta, sillä samalla saadaan tietoja eri henkilöiltä yhtä aikaa, toisaalta dominoivat henkilöt voivat johdattaa koko ryhmää omaan suuntaansa (Hirsjärvi ym. 2009, 209-211). Mahdollisimman monipuolisen aineiston saamiseksi tässä opinnäytetyössä käytettiin sekä ryhmä-, pari-, että yksilöhaastatteluja.

Haastatteluja pidettiin yhteensä 16 kpl.

3.3 Analyysi

Aineiston analyysitapojen määrittely ei ole Hirsjärven ym. (2009, 223) mukaan aina yksiselitteistä ja aineiston kerääminen sekä analysointi voivat tapahtua samanaikaisesti. Tässä opinnäytetyössä haastatteluja suoritettiin useita ja osaa haastateltavista haastateltiin useaan otteeseen, joten oli luontevaa tehdä analyysiä jo tiedon keräämisvaiheessa. Pääperiaatteen mukaan analyysi valitaan siten, että saadaan parhaiten vastaus ongelmaan tai tutkimustehtävään (Hirsjärvi ym. 2009, 224-225).

Haastatteluilla haettiin vastausta siihen, miten tietosuojaa tulisi kehittää ja mikä on haastateltavien mielestä keskeistä henkilötietojen käsittelyssä. Tarkoituksena oli hyvien toimintatapojen kartoittaminen ja niiden kuvaaminen koko S-ryhmälle sopiviksi. Lähestymistapa analyy-

sin oli teoriaohjaava, kyse oli abduktiivisesta päättelystä, jossa tutkija tekee analyysiä aineistoa ja valmiita malleja yhdistelemällä (Tuomi & Sarajärvi 2009, 96-97).

Alastalon ja Åkermanin (2010, 389-390) mukaan asiantuntija-analyysin päätavoitteena on yleensä tuoda esiin faktoja, jotka tuotetaan yhdessä haastateltavan kanssa haastattelun tai tutkimusprosessin kuluessa. Tässä opinnäytetyössä olemassa olevia toimintatapoja myös kyseenalaistettiin ja tarkasteltiin kriittisesti. Ennen kaikkea haastatteluiden tavoitteena oli saada esille haastateltavan näkemystä siitä, mitä haasteita he ovat kokeneet tietosuojan alalla ja kuinka asioita tulisi edelleen kehittää.

Faktaluenta on analyysimenetelmä, jossa aineiston keruu ja analyysi limittyvät yhteen (Alastalo & Åkerman 2010, 390). Selvityksessä analysointia tehtiin jo haastatteluiden aikana ja tulevat haastattelut muotoutuivat aikaisempien haastattelujen perusteella. Tässä selvityksessä esitetyt haastattelut on analysoitu ja tiivistetty siten, että vain keskeiset tietosuojaan ja henkilötietojen käsittelyyn sekä niiden organisointiin liittyvät asiat on liitetty raporttiin. Alkuperäiset pöytäkirjat jäivät opinnäytetyön tilaajalle.

4 Lainsäädäntö & valvovan viranomaisen linjaukset

Tietosuojalainsäädäntö on muutoksen edessä. Voimassaolevat EU:n tietosuojadirektiivit on implementoitu Suomen lainsäädäntöön eli käytännössä henkilötietolakiin (Tietosuojavaltuutetun toimisto 2011b). Euroopan Komissio kuitenkin valmistelee tämän työn kirjoittamishetkellä uutta tietosuoja-asetusta, ja koska kyseessä on asetus, EU:n jäsenmaat eivät enää suorita omaa implementointia, vaan lainsäädäntö tulee voimaan sellaisenaan.

Tässä luvussa tarkastellaan mitä henkilötietolaki määrää henkilötietojen käsittelystä, kuinka tietosuojavaltuutettu on ohjeistanut lain tulkinnasta ja mitä keskeisiä muutoksia EU:n valmisteilla oleva tietosuoja-asetus on tuomassa lainsäädäntöön. Aineistosta on pyritty korostamaan organisointiin liittyviä kohtia, jotka esitetään luvun lopussa rooleittain jaoteltuina.

4.1 Henkilötietolaki 1999/523 & tietosuojavaltuutetun ohjeet

Suomessa oikeudesta yksityisyyteen säädetään perustuslaissa (Suomen perustuslaki 1999/731, 10 §), jossa määrätään myös, että henkilötietojen suojasta säädetään henkilötietolaissa. Edellisten lisäksi muita niin sanottuja tietosuojalakeja ovat laki yksityisyyden suojasta työelämässä, sähköisen viestinnän tietosuojalaki sekä laki viranomaisen toiminnan julkisuudesta. Lisäksi henkilötietoja koskevia erityissäännöksiä löytyy lukuisista muista laeista, esimerkiksi väestötietolaista ja laista ajoneuvoliikennerekisteristä. (Tietosuojavaltuutetun toimisto 2012e.)

Henkilötietolain vaatimuksia tulee noudattaa kaikessa henkilötietojen käsittelyssä (Henkilötietolaki 1999/523, 3 §). Käytännössä rekisterinpitäjän velvoitteet jakautuvat organisaatiossa eri henkilöille. Tietosuojavaltuutetun ohjeistuksen mukaan organisaation on syytä määritellä henkilötietojen käsittelyyn liittyvät tehtävät ja vastuualueet. Myös tietosuojasta vastaava henkilöstö tulee olla määritettynä. Erityisen tärkeätä on selkeä vastuun- ja työnjaon määritteleminen tietoja käsittelevän ja tietosuojasta vastaavan henkilöstön välillä. (Tietosuojavaltuutetun toimisto 2010c, 5.)

Henkilötietolaissa korostuu itseohjautuvuus (Tietosuojavaltuutetun toimisto 2012f), rekisterinpitäjän tulee oma-aloitteisesti huolehtia henkilötietolain velvoitteiden toteuttamisesta. Henkilötietolaki ei edellytä, että atk:n avulla käsiteltävien henkilötietojen tulisi muodostaa henkilörekisteri, jotta toiminta olisi henkilötietolain alaista (Silvennoinen 2004, 12). Tietosuojalainsäädäntö ei myöskään ota kantaa rekisterin muotoon tai kokoon, pelkkää postituslistaa koskevat samat säännökset kuin laajempaakin rekisteriä. Toiminnan pienimuotoisuus tai käsiteltävien tietojen suppea määrä ei siis oikeuta rekisterinpitäjää laiminlyömään velvollisuuksiaan. (Tietosuojavaltuutetun toimisto 2012c.)

Juridisen määritelmän mukaan rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöön henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty (Henkilötietolaki 1999/523, 5 §). Juridisessa mielessä rekisterinpitäjä ei kuitenkaan ole yrityksen keräämien tietojen osalta yrityksen yksittäinen työntekijä (Tietosuojavaltuutetun toimisto 2002).

Käytännössä yritys on rekisterinpitäjä henkilöstönsä ja asiakkaidensa osalta, ja viime kädessä yrityksen johto vastaa siitä, että toiminta on lainsäädännön vaatimusten mukaista. Johdon tehtävänä on huolehtia yrityksen tietosuojaan ja henkilötietoihin liittyvät vastuiden asianmukaisesta määrittelystä, henkilöstön ohjaamisesta ja koulutuksesta sekä yrityksen käyttämien tietojärjestelmien lainmukaisuudesta. Edellä mainitut vastuut tulisi sisällyttää osaksi muiden tehtävien hoitoon liittyvää operatiivista vastuuta. (Tietosuojavaltuutetun toimisto 2002.)

Henkilötietojen käsittelyn ulkoistaminen ei poista rekisterinpitäjänä olevan organisaation vastuuta ja tätä ei voi muuttaa edes kahdenkeskisillä sopimuksilla. Kuitenkin lain mukaan se, joka käsittelee tietoja rekisterinpitäjän lukuun, on velvollinen antamaan riittävät selvitykset henkilötietolain noudattamisesta ennen henkilötietojen käsittelyn aloittamista (Henkilötietolaki 1999/523, § 32). Tietosuojavastaavan nimeäminen ei myöskään poista vastuuta yrityksen johdolta, vastuu säilyy aina rekisterinpitäjänä olevalla organisaatiolla. (Tietosuojavaltuutetun toimisto 2010b, s2.)

Henkilötietolaissa (1999/523, 32 §) tietojen suojaamisesta on säädetty siten, että rekisterinpitäjä on velvollinen toteuttamaan ne tarpeelliset tekniset ja organisatoriset toimenpiteet, joilla henkilötiedot suojataan. Toimenpiteitä toteutettaessa tulee huomioida tekniset mahdollisuudet, kustannukset, käsiteltävien tietojen laatu, määrä, ikä sekä tietojen merkitys rekisteröidyn yksityisyyden suojan kannalta (Henkilötietolaki 1999/523, § 32). Rekisterinpitäjän tulee siis suorittaa riskiarviointia ja mitoittaa henkilötietojen suojaaminen arvioinnin tulosten perusteella.

Rekisterinpitäjän tulee tietosuojavaltuutetun toimiston (2010b, s2) mukaan vähintään

- määritellä henkilötietojen keräämisen ja käsittelyn tarkoitus
- suunnitella henkilötietojen käsittelytoimet koko tiedon elinkaaren ajaksi
- analysoida, kirjata muistiin ja kuvata rekisterinpitäjän tehtävien hoitoon liittyvät henkilötietojen käsittelyt ja niihin liittyvät vastuut, toimivallat ja menettelyt
- varmistua henkilötietojen käsittelyn lainmukaisuudesta
- huolehtia tietojen laadusta, tarpeellisuudesta ja virheettömyydestä
- varmistua henkilötietojen suojaamisesta
- huolehtia rekisteröityjen oikeuksien toteutumisesta, erityisesti tarkastus-, tiedonkorjaus- ja kielto-oikeuden toteuttamisesta
- laatia tietosuojaseloste ja informoida rekisteröityjä
- huolehtia mahdollisesti tarvittavien viranomaisilmoitusten tekemisestä
- laatia henkilöstön käyttöön tietosuoja-ohjeet
- seurata ja valvoa henkilötietojen käsittelyä.

4.2 EU:n uusi tietosuoja-asetus

Tällä hetkellä voimassa oleva EU:n henkilötietodirektiivi 95/46 EY julkaistiin vuonna 1995. Silloisen direktiivin periaatteet ovat vieläkin päteviä, mutta jokainen EU:n jäsenmaa on implementoinut direktiivin omalla tavallaan maansa lainsäädäntöön. Tämän takia tietosuojalainsäädäntö ei ole yhteismitallinen EU:n alueella, vaan eri maiden tietosuojalait ovat hyvinkin erilaisia. Myös tekniikan nopea kehittyminen ja globalisaatio asettavat uusia haasteita yksityisyyden suojalle. Uuden tietosuoja-asetuksen tarkoituksena on luoda koko EU:n alueelle yhtenäinen tietosuojalainsäädäntö. (European Commission 2012c, 1.)

Suomen nykyinen henkilötietolaki on saatettu vastaamaan EU:n henkilötietodirektiiviä 95/46 EY (Tietosuojavaltuutetun toimisto 2011b). Opinnäytetyön kirjoittamishetkellä luonnosvaiheessa oleva EU:n uusi tietosuoja-asetus on asetusmuotoinen, mikä tarkoittaa sitä, että sitä ei enää erikseen implementoida kohdemaan lainsäädäntöön. Kyseessä on luonnos, joka tulee varmasti vielä muuttumaan ennen lopullista muotoaan, asetus on tarkoitus ottaa käyttöön vuosina 2014 - 2016. On kuitenkin varmaa, että tietosuojalainsäädäntö tulee oleellisesti

muuttumaan ja kiristymään, joten asetuksen vaatimuksia on syytä ottaa huomioon ennakoiden.

4.2.1 Määritelmät

EU:n tuleva asetus laajentaa henkilötiedon ja henkilötietojen käsittelyn määritelmiä. Tulevan lainsäädännön mukaan henkilötiedolla tarkoitetaan kaikkea tietoa, joka koskee rekisteröityä. Nykyiseen lainsäädäntöön verrattuna uusi asetus esittelee myös geneettisen ja biometrisen tietotyypin, joiden kummankin käsittely on lähtökohtaisesti kiellettyä. Henkilöturvatunnusta ei uudessa asetuksessa ole enää nostettu omaksi kategoriakseen. (European Commission 2012a, 41-42, 45.)

Voimassaolevassa henkilötietolaissa puhutaan vain rekisterinpitäjästä. Uudessa asetuksessa on kuitenkin määritelty eri osapuolet tarkemmin, esimerkkinä termit ”controller” ja ”processor”. Ensimmäisellä tarkoitetaan nykylainsäädännön mukaista rekisterinpitäjää, jolla on oikeus ja velvollisuus määrätä henkilötietojen käsittelystä. Jälkimmäisellä tarkoitetaan määritelmän mukaan tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. (European Commission 2012a, 41-42.)

4.2.2 Rekisterinpitäjän velvollisuudet

Rekisterinpitäjä on velvollinen tekemään tarvittavat toimenpiteet, joilla varmistetaan ja voidaan näyttää toteen se, että henkilötietojen käsittely täyttää lainsäädännön vaatimukset. Rekisterinpitäjän tulee ylläpitää asiamukaista tietosuojaan liittyvää dokumentaatiota ja implementoida asetuksessa määritellyt tietoturvavaatimukset. Tietosuojavastaavan nimittäminen ja yhteistoiminnasta valvovan viranomaisen kanssa asetettujen vaatimusten täyttäminen kuuluu rekisterinpitäjän velvollisuuksiin. (European Commission 2012a, 55-56.)

Kun henkilötietojen käsittely aiheuttaa erityisen riskin henkilön yksityisyydelle ja oikeuksille, pitää rekisterinpitäjän suorittaa erityinen tietojen suojaamisen tehokkuuden arviointi, ”data protection impact assesment”. Euroopan Komission määritelmien mukaisia erityisen riskin aiheuttavia käsittelymuotoja ovat esimerkiksi profilointi ja julkisten alueiden kameravalvonta. Euroopan Komissio tulee luultavasti vielä tarkemmin määrittämään muodon tälle arvioinnille. (European Commission 2012a, 62-63.)

Suomen voimassa oleva henkilötietolaki ei tällä hetkellä erottele profilointia muusta henkilötietojen käsittelystä, mutta tulevassa asetuksessa se on määritelty omaksi käsitteekseen. Profiloinnin käsite on melko laaja ja kattaa esimerkiksi henkilön tehokkuuteen työpaikalla, taloudelliseen tilanteeseen, sijaintiin, terveyteen, henkilökohtaisiin mieltymyksiin, luotettavuu-

teen tai käyttäytymiseen kohdistuvan arvioinnin tai ennustamisen. Profilointi on sallittua, mikäli siihen saadaan rekisteröidyn suostumus, se kuuluu sopimuksen täytäntöönpanoon tai on jonkin muun lain mukaan nimenomaisesti sallittu. Lähtökohtaisesti rekisteröidyllä on oikeus kieltäytyä profiloinnista. (European Commission 2012a, 54.)

Uuteen tietosuoja-asetukseen on kirjattu periaatteet ”privcy by design” ja ”privacy by default”. Ensimmäinen tarkoittaa sitä, että tietoturva ja tietosuoja tulee ottaa huomioon jo järjestelmiä ja henkilötietojen käsittelyä suunniteltaessa. Ei siis riitä, että tietoturvamekanismeja tai sääntöjä asetetaan jälkikäteen. Jälkimmäinen tarkoittaa sitä, että tietosuoja on oletusarvoista ja toimii lähtökohtana kaikelle henkilötietojen käsittelylle. Tietosuoja-asetusten tulisi olla helposti toteutettavissa etenkin rekisteröidyn näkökulmasta (European Commission 2012c, 1). Rekisterinpitäjän tulee toimia siten, että voi tarvittaessa esittää toteen näiden vaatimusten toteutumisen. Rekisterinpitäjän on myös valvottava periaatteiden toteutumista. Euroopan Komissio saattaa tarkentaa vaatimuksia esimerkiksi standardien muodossa. (European Commission 2012a, 27, 56, 66.)

4.2.3 Rekisteröidyn oikeudet

Tulevan tietosuoja-asetuksen painopiste on vahvasti rekisteröidyn puolella ja luonnokseen on kirjattu lukuisia uusia oikeuksia, joilla vahvistetaan yksityishenkilöiden asemaa. Rekisteröidyn oikeudet ovat käytännössä yleensä rekisterinpitäjän velvollisuuksia. Uuden asetuksen tavoitteena on lisätä rekisteröidylle ymmärrystä ja näkyvyyttä siitä, miten hänen henkilötietojaan käsitellään (European Commission 2012b, 1).

Uuden asetuksen mukaan rekisteröidyllä tulisi olla oikeus ja mahdollisuus päästä käsiksi omiin tietoihinsa helposti ja ilmaiseksi. Tämä tarkoittaa monessa tapauksessa järjestelmien, käyttöliittymien tai uusien rajapintojen kehittämistä, sillä nykyinen lainsäädäntö ei edellytä sähköistä tarkastusoikeutta ja tiedot pyydetäänkin useimmiten rekisteriasioita hoitavalta henkilöltä. S-ryhmän sähköinen asiointipalvelu S-kanava mahdollistaa jo nyt omien tietojensa tarkastamisen ja korjaamisen sähköisesti (S-kanava 2012). Tietojen helppo siirtäminen yritykseltä tai yhteisöltä toiselle on yksi uusista oikeuksista. Henkilötiedot tulisi olla saatavissa ja siirrettävissä yleisesti käytössä olevassa sähköisessä formaatissa. (European Commission 2012b, 2.)

Sähköinen asiointi aiheuttaa myös käytännön haasteita. Henkilön tunnistamisen tulee tapahtua asianmukaisesti, perinteisen virallisen henkilötodistuksen esittäminen ei onnistu internetissä, vaan on käytettävä sähköistä tunnistamista. Toisaalta myös koneellisesti järjestetyt, palvelun ruuhkauttamiseksi tarkoitetut hyökkäykset tulisi voida tunnistaa ja estää.

Lapset, eli EU:n määritelmän mukaan alle 18-vuotiaat, on huomioitu tietosuoja-asetuksessa, koska heiltä ei voi odottaa täyttä ymmärrystä tietojen käsittelyyn liittyvistä riskeistä ja seurauksista. Tietojen käsittelystä tulisi viestiä niin selkeästi ja yksinkertaisesti, että lapsikin ymmärtää mistä on kyse. Lasta ei saisi asetuksen mukaan profiloida ja tietojen käsittelyn lopettamisen sekä tietojen poistamisen tulisi onnistua helposti, sillä lapsella ei ole välttämättä tietojen käsittelyä aloitettaessa ollut täyttä ymmärrystä siitä, mihin hän suostui. (European Commission 2012a, 24-25 & 43-44.)

4.2.4 Ilmoittamisvelvollisuus ja sanktiomenettely

Suomen henkilötietolakiin ei tällä hetkellä ole kirjattu yleistä velvollisuutta ilmoittaa tietomurroista viranomaisille tai rekisteröidyille, ainoastaan teleoperaattorit ovat velvoitettuja ilmoituksen tekemiseen (Salminen 2011). Kuitenkin rikollisille kaikkein hyödyllisin hetki käyttää anastettuja tietoja, on heti tietojen saamisen jälkeen, koska rekisteröidyt eivät ole vielä tietoisia asiasta ja eivätkä siten ole ehtineet tehdä suojaavia toimenpiteitä (European Commission 2012b). Tietosuojavaltuutettu Reijo Aarnio toteaakin, että ilmoitusvelvollisuuden puute heikensi tiedottamisen onnistumista Suomessa marraskuussa 2011 tapahtuneissa tietovuototapauksissa (Salminen 2011).

Tiedottamisvastuun puutetta on tarkoitus korjata tulevaan asetukseen kirjatulla tietomurtojen ilmoittamisvelvollisuudella. Havaittuaan tietomurron, rekisterinpitäjän tulee ilmoittaa asiasta viranomaisille 24 tunnin kuluessa tapahtuneesta. Asiasta pitää myös ilmoittaa rekisteröidyille, joiden tiedot ovat olleet murron kohteena, ellei voida osoittaa toteen sitä, että vuotaneista tai murretuista tiedoista ei ole haittaa rekisteröidyille. Rekisteröidyille tulee myös kertoa, mitä vaikutuksia murrolla on ja kuinka he voivat minimoida seurauksia. Nopea tiedottaminen vaatii toimiakseen selkeitä viestintäkäytäntöjä ja -vastuita. (European Commission 2012a, 60-62.)

Tutkimusyhtiö Verizonin (2012, 3) tekemästä tietomurtoja käsittelevästä tutkimusraportista selviää, että 85 % tutkituista tietomurroista havaittiin aikaisintaan viikkojen kuluessa murrosta ja, että jopa 92 % tietomurroista havaittiin kolmannen osapuolen toimesta. Tämä tarkoittaa sitä, että enemmän kuin sisäisen tiedottamisen nopeuteen, organisaatioiden tulisi panostaa valvontaan, jotta mahdolliset tietomurrot voidaan havaita itse mahdollisimman nopeasti niiden tapahduttua.

Tulevaan asetukseen on kirjattu sanktioita tietosuojalainsäädännön noudattamatta jättämisestä. Huomattavaa on se, että valvova viranomainen on velvollinen määräämään sanktioita rekisterinpitäjälle, mikäli tämä ei noudata lainsäädäntöä. Tämä tarkoittaa sitä, että sanktioita voi tulla, mikäli rekisterinpitäjä vaatii korvausta rekisteriotteesta, toimittaa rekisteröidylle

vain vajaat tiedot, ei valvo tietojen säilytysaikoja tai käsittelee tietoja ilman lainmukaista perustetta. Sanktioiden määrä vaihtelee rikkeiden mukaan, mutta asetukseen on kirjattu prosentuaalinen sakko, joka voi olla suurimmillaan 0,5-2,0 % yrityksen globaalista liikevaihdosta. (European Commission 2012a, 92-94.)

Uusi asetus siirtää painopistettä rekisteröidyn puolelle, lisäten tämän oikeuksia. Asetus pyrkii siihen, että rekisteröidyn ymmärrys ja mahdollisuus vaikuttaa tietojensa käsittelyyn, parantuisi nykyisestä. Asetus sisältää lukuisia kohtia, joiden täytäntöönpano vaatii tarkkaa suunnittelua. Asetuksen toteuttaminen vaatii organisaatiolta selkeätä toimintamallia, jossa on kuvattu roolit ja tehtävät. Organisaatiolla tulee olla selkeä kuva henkilötietojen käsittelyn kokonaisuudesta ja tietosuojan sekä tietoturvallisuuden tulee olla osana kaikkea toimintaa, se ei voi olla vain päälle liimattu funktio. Seuraavassa alaluvussa on kuvattu tarkemmin tietosuojarooleja.

4.3 Tietosuojaroolit

Suomen henkilötietolaissa korostetaan itseohjautuvuutta (Tietosuojavaltuutetun toimisto 2012f), rekisterinpitäjä vastaa itse tietosuojan organisoimisesta ja vastuiden määrittelystä siten, että lakisääteiset vaatimukset täyttyvät. Tässä luvussa tietosuojaan liittyviä vastuita tarkastellaan neljän erilaisen roolin pohjalta.

Keskeisin rooli on organisaation tietosuojavastaava, joka toimii erityisasiantuntijana henkilöstölle ja yrityksen johdolle. Tietosuojavastaavan lisäksi merkittävä rooli on rekisterien omistajilla, jotka käytännössä vastaavat eri rekisterien käytöstä ja valvonnasta.

4.3.1 Tietosuojavastaava

Suomen nykyinen lainsäädäntö velvoittaa sosiaali- ja terveydenhuollon palvelujen antajaa, apteekkia, Kansaneläkelaitosta ja Terveydenhuollon oikeusturvakeskusta nimeämään tietosuojavastaavan (Tietosuojavaltuutetun toimisto 2010b, 2). Tietosuojavaltuutettu kuitenkin suosittelee, että yritykset joilla on kanta-asiakasjärjestelmiä, nimeäisivät tietosuojavastaavat (Tietosuojavaltuutetun toimisto 2012c), vaikka laki ei tähän pakota. Luonnosvaiheessa oleva EU:n tietosuoja-asetus määräisi tietosuojavastaavan, ”data protection officer” nimittämisen pakolliseksi kaikissa niissä henkilötietoja käsittelevissä yrityksissä, jotka työllistävät vähintään 250 henkeä (European Commission 2012a, 65).

Tietosuojavastaava toimii organisaation erityisasiantuntijana, joka auttaa rekisterinpitäjää lakisääteisten velvoitteiden toteuttamisessa. Tietosuojavastaava tarjoaa asiantuntija-apua organisaation henkilöstölle, sekä johdolle. Hän myös pitää huolta siitä, että koko henkilöstö

kaikilla organisaation tasoilla ymmärtävät vastuunsa tietosuojasta ja tietoturvasta. (Tietosuojavaltuutetun toimisto 2010b, 2 & Tietosuojavaltuutetun toimisto 2010c, 4.)

S-ryhmän alueosuuskaupat ovat juridisesti itsenäisiä osuustoiminnallisia yrityksiä, joten myös jokaiseen alueosuuskauppaan, tytär- ja osakkuusyhtiöön tulisi nimetä tietosuojavastaava, joka vastaisi tietosuojan tiedottamisesta ja kehittämisestä omalla vastuualueellaan. Tietoturvallisuuden osalta on noudatettu samanlaista mallia, S-ryhmän tietoturvallisuuden kehittämisestä ja koordinoinnista vastaa tietoturvallisuuspäällikkö, mutta jokaisessa alueosuuskaupassa on nimetty tietoturvallisuusvastaava, jonka tehtäviin kuuluu tietoturvallisuudesta tiedottaminen ja tietoturvallisuuden kehittäminen omalla vastuualueellaan (Tupala 2011).

Tietosuojavastaavalla tulee olla riittävä koulutus tehtäväänsä ja mahdollisuus pitää yllä ammattitaitoaan. Nykyinen lainsäädäntö tai tulevan EU:n tietosuoja-asetuksen luonnos eivät aseta mitään nimettyä koulutustaustaa. Tietosuojavastaavan tulisi olla sellaisessa asemassa, että hän voi suorittaa tehtävänsä mahdollisimman itsenäisesti. Mahdolliset eturistiriidat tulee ottaa huomioon ja rekisterinpitäjän on tarjottava riittävät resurssit tietosuojavastaavalle. Tietosuojavastaava nähdään ylimmän johdon tukena, hänen tulisi raportoida johdolle, tai ainakin olla oikeutettu siihen. Erityisen tärkeää on, että hänellä on yrityksen johdon tuki hoitaa tehtäväänsä. (European Commission 2012a, 65-66 & Tietosuojavaltuutetun toimisto 2010b, 2.)

Tietosuojavastaavalla tulee olla mahdollisuus osallistua organisaation henkilötietojen käsittelyä koskevaan suunnittelu- ja kehittämistoimintaan mahdollisimman varhain ja riittävän korkealla tasolla. Hänellä tulee olla mahdollisuus esittää kommentteja ja parannusehdotuksia näihin suunnitelmiin. Tietosuojavastaava on siis pidettävä ajan tasalla yrityksen asioista siten, että hänellä on myös mahdollisuus vaikuttaa niihin. (European Commission 2012a, 65-66 & Tietosuojavaltuutetun toimisto 2010b, 2.)

Tietosuojavastaava osallistuu organisaation tietosuojaohjeiden valmisteluun ja ylläpitoon. Hän myös huolehtii siitä, että ohjeet ovat ajantasaisia ja kaikkien saatavilla. Tietosuojavastaava pitää huolta myös siitä, että ohjeista tiedottaminen, ja niihin mahdollisesti liittyvä koulutus on riittävää. Kuten tietosuojavaltuutetun ”tee-se-itse” tarkastuslistasta (Tietosuojavaltuutetun toimisto 2010c) voidaan havaita, tietosuoja ja tietoturvallisuus ovat lähellä toisiaan. Luonnollista onkin, että tietosuojavastaava tekee yhteistyötä organisaation tietoturvallisuuspäällikön kanssa. (Tietosuojavaltuutetun toimisto 2010b, 2 & Tietosuojavaltuutetun toimisto 2010c.)

Yhteenvetona todettakoon, että tietosuojavastaava siis ylläpitää tilannekuvaa vastuualueellaan olevan organisaation henkilötietojen käsittelystä, henkilörekistereistä ja niiden omista-

jista. Hän myös tarkastaa ja hyväksyy rekisterinpitosuunnitelmat, jotka on kuvattu tarkemmin seuraavassa alaluvussa.

Henkilötietojen käsittelyn sekä niiden suojausmenetelmien valvonta kuuluu tietosuojavastaavan tehtäviin (Tietosuojavaltuutetun toimisto 2010b, 2). Toiminnan pitää olla tietosuojalainsäädännön vaatimusten mukaista ja tämä tarkoittaa sitä, että henkilöstön, etenkin rekisterin omistajien tulee toimia organisaation tietosuojaohjeiden mukaisesti. Rekisterinpidossa tulee noudattaa rekisterinpitosuunnitelmaa. Tietosuojavastaava valvoo erityisesti rekisterien omistajien toimintaa.

Tietosuojavastaava osallistuu henkilöstölle annettavan tietosuojakoulutuksen toteuttamiseen, koulutuksen tulee olla riittävää ja ottaa huomioon koulutettavien asema sekä työtehtävät (Tietosuojavaltuutetun toimisto 2010c). Lähtökohtaisesti rekisterin omistajalle pidettävä koulutus on laajempi, kuin rekisterin käyttäjälle pidettävä koulutus.

Tietosuojavastaava tukee henkilökuntaa ja rekisteröityjä tietosuoja-asioissa (Tietosuojavaltuutetun toimisto 2010b). Euroopan komissio esittää luonnoksessaan, että tietosuojavastaava pitää nimetä julkisesti ja että rekisteröidyillä tulee olla oikeus ottaa yhteyttä henkilötietojen käsittelyyn sekä rekisteröidyn oikeuksiin liittyvissä kysymyksissä (European Commission 2012a, 65). Tietosuojavastaava toimii tietosuojaan ja henkilötietojen käsittelyyn liittyvissä asioissa yhdyssiteenä viranomaisiin ja konsultoi näitä mahdollisuuksien mukaan oma-aloitteisesti.

Tietosuojan tilasta ja kehittämistarpeista raportointi organisaation johdolle kuuluu tietosuojavastaavan tehtäviin. Tietosuojavastaava suorittaa myös muita, yrityksen johdon osoittamia tietosuojaa tukevia tehtäviä. Luonnollisesti tietosuojavastaavan tulee noudattaa tehtävissään salassapitosopimusta (Tietosuojavaltuutetun toimisto 2010b, 2).

Tietosuojavastaava valvoo tietovuotoihin ja -murtoihin liittyvää dokumentointia, ilmoittamista ja viestintää. Euroopan Komission ehdotuksessa korostuu ennen kaikkea tietosuojavastaavan toimintaa valvova rooli. (European Commission 2012a, 65-67.)

Tietosuojavastaavalla tulee olla riittävät resurssit tehtävänsä suorittamiseen (European Commission 2012a, 65-66). Tämän resurssivaatimuksen täyttämiseksi, tietosuojavastaavalla voi olla apunaan tietosuojan kehitysryhmä, jota on kuvattu tarkemmin seuraavassa alaluvussa.

4.3.2 Tietosuojan kehitystyöryhmä

Lainsäädäntö ei edellytä kehitysryhmän perustamista, mutta suuressa organisaatiossa sen hyötyjä voi perustella useastakin eri näkökulmasta. Analogiaa voi hakea tietoturvallisuuden kehitysryhmien tehtävistä.

Tietosuojan kehitysryhmä tukee tietosuojavastaava tämän tehtävissä, tämä tukee myös tulevan EU-tietosuoja-asetuksen vaatimusta siitä, että tietosuojavastaavalle tulee varata riittävät resurssit tehtäviensä toteuttamiseen (European Commission 2012a, 65-66). Kehitysryhmän kokoonpano tulee valita siten, että sen jäsenet edustavat laajasti organisaation eri osia ja näkökantoja. Kehitysryhmä antaa tietosuojavastaavalle laajan näkemyksen organisaation tarpeista, haasteista ja prioriteeteista tietosuojaan liittyen. Kehitysryhmä toimii viestintäkanavana myös toiseen suuntaan, esimerkiksi tietosuojavastaavan näkemysten ja päätösten perusteluiden suhteen. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2004, 30.)

SOK:lle on perustettu tietoturvallisuuden kehitysryhmä, jonka toiminnasta voi hakea analogiaa myös tietosuojan kehitysryhmään. Tämä tarkoittaa sitä, että tietosuojan kehitysryhmän avulla tietosuojavastaava saa tietoa tietosuojaan liittyvistä kehityshankkeista ja organisaation muuttuvista prosesseista. Kehitysryhmän tulee seurata etenkin tietosuojaan ja henkilötietojen käsittelyyn liittyviä projekteja. Muuttuvan lainsäädännön, säädösten tai muiden ulkoisten vaatimusten seuraaminen tietosuojan alueella kuuluu kehitysryhmän tehtäviin. (Tupala 2010.)

Kehitysryhmä tunnistaa tietosuojan arviointitarpeita ja tuottaa tietosuojavastaavan johdolla tietosuojaohjeita sekä toimintatapoja, ja edistää hyvien käytäntöjen käyttöönottoa organisaatiossa. Kehitysryhmä tukee tietosuojavastaava ajankohtaisista asioista ja linjauksista päättämisessä. Tietosuojaan liittyvien päätöksien tiedottaminen tarvittaville toimielimille kuuluu myös tietosuojatyöryhmän vastuulle. (European Commission 2012a, 66 & Tietosuojavaltuutetun toimisto 2010b, 2 & Tupala 2010).

Kuten tietoturvallisuuspäällikkö tietoturvallisuuden kehitysryhmän osalta, tietosuojavastaava toimii tietosuojan kehitysryhmän puheenjohtajana ja koollekutsujana. Tietosuojan kehitysryhmän tulee kokoontua säännöllisesti ja tarvittaessa se voidaan kutsua koolle erikseen. (Tupala 2010.)

4.3.3 Rekisterin omistaja

Henkilötietolaissa on määritetty termi rekisterinpitäjä, tässä opinnäytetyössä rekisterin omistaja on yksikkö tai henkilö organisaatiossa, joka käytännössä vastaa rekisterinpitäjän velvoitteiden toteuttamisesta jonkin tietyn rekisterin osalta.

Kansallisen turvallisuusauditointikriteeristön (2011, 20), KATAKRIn mukaan, suojattaville kohteille pitää nimetä omistaja. Henkilötietojen osalta tämä tarkoittaa sitä, että henkilötiedoille tai henkilörekisterille on aina nimettävä omistaja ja siitä tulee ilmoittaa tietosuojavastaavalle ennen henkilötietojen käsittelyn aloittamista. On tyypillistä, että suuressa organisaatiossa on useita rekisterin omistajia.

Tietosuojavaltuutetun toimisto (2010e) on laatinut mallin henkilötietojen käsittelyn/henkilörekisterin rekisteritoimintojen analysoimiseksi ja mallia voi käyttää niin suunnitteilla olevan, kuin jo olemassa olevan rekisterin analysoimiseen. Malli soveltuu siis hyvin myös rekisterinpitosuunnitelmaksi. Ennen henkilötietojen käsittelyn aloittamista, rekisterin omistajan tulee tehdä rekisterinpitosuunnitelma, jossa on kuvattu kyseisen rekisterin käyttöön, suojaamiseen, rekisteröidyn oikeuksien toteutumiseen ja muihin lain vaatimuksiin liittyvät periaatteet.

Rekisterin omistaja hyväksyttää rekisterisuunnitelman organisaation tietosuojavastaavalla. Kun lupa rekisterin perustamiseen on annettu, rekisterin omistaja voi aloittaa henkilötietojen käsittelyn rekisterinpitosuunnitelmaa noudattaen. Kerättävien tietojen määrittely ja henkilötietojen käsittelyn suunnittelu ovat tietosuojavaltuutetun toimiston (2011a) mainitsemat kaksi henkilötietolain kannalta keskeistä vaatimusta. Hyvin ja huolellisesti täytetty rekisterisuunnitelma vastaa näihin velvoitteisiin ja näin myös dokumentointi tulee tehtyä.

Valtiohallinnon tietoturvallisuuden johtoryhmän (2004, 35) mukaan dokumentaatio on edellytys turvallisuuden hallinnalle ja se antaa tärkeätä tietoa kehittämiseen, sekä ongelmien ja poikkeamien selvittämiseen. Rekisterinpitosuunnitelman tekemisellä vastataan henkilötietolain (1999/523, 6§) suunnitteluvelvollisuuteen. Suunnitelmadokumentin avulla voidaan osoittaa, että lain vaatimukset on täytetty. Ellei kerättäviä tietoja määritellä, on mahdotonta arvioida mitkä tiedot ovat käsittelyn tarkoituksen kannalta tarpeellisia ja virheettömiä henkilötietoja (Tietosuojavaltuutetun toimisto 2011a).

Myös hyvän tiedonhallintatavan toteuttaminen on mahdotonta ilman loogisen kokonaisuuden pohjalta tehtyä suunnittelua (Tietosuojavaltuutetun toimisto 2011a). Rekisterinpitosuunnitelma toimii myös pohjana rekisteri- ja tietosuojaselosteen tekemisessä. Rekisterinpitosuun-

nitelman jakelu tulee pitää mahdollisimman pienenä, sillä se sisältää tietoja, jotka paljastuessaan saattaisivat aiheuttaa tietoturvariskin.

Rekisterisuunnitelman hyväksymisen jälkeen rekisterin omistaja vastaa siitä, että suunnitelmaa noudatetaan rekisterinpidossa. Mikäli käsittelyssä ilmenee ristiriitoja tai epäselvyyksiä suunnitelman kanssa, rekisterin omistajan tulee ilmoittaa asiasta välittömästi tietosuojavastaavalle.

Omistaja vastaa rekisterinsä käyttäjistä ja näiden käyttöoikeuksien hallinnoinnista. Omistajan tulee varmistua siitä, että käyttäjällä on riittävä koulutus tehtävään ja asianmukaiset vaitiolositoumukset tehtynä ennen käytön aloittamista. Ryhmätunnuksia ei saa käyttää ja järjestelmään ei saa olla pääsyä ilman asiamukaista valtuutusmenettelyä. Käyttöoikeuksien tulee myös vanheta automaattisesti. Lähtökohtaisesti käyttöoikeuksia tulee hallita siten, että henkilöllä on pääsy vain työtehtäviensä vaatimiin tietoihin ja jälkikäteen voidaan todentaa kuka on katsonut, muokannut, lisännyt tai poistanut tietoja, koska tämä on tapahtunut ja mikä tai mitkä tiedot olivat kohteena. (Tietosuojavaltuutetun toimisto 2010c, 4-8.)

Mikäli henkilötietojen käsittely, tai osia siitä ulkoistetaan, esimerkiksi rekisterin sisältävän tietojärjestelmän ylläpito, rekisterin omistaja vastaa siitä, että sopimukset tehdään asianmukaisesti ja että niissä otetaan huomioon kaikki tietosuojan ja tietoturvan velvoitteet niin lain kuin organisaation omien ohjeistusten mukaisesti. Sopimusten toteutumisen seuraaminen kuuluu myös rekisterin omistajan vastuulle. Rekisterin omistaja tukeutuu näissä asioissa tietosuojavastaavan. (Tietosuojavaltuutetun toimisto 2010c, 4-8.)

Rekisterin omistajan tulee valvoa, että käyttäjät toimivat lain ja tietosuojaohjeiden vaatimusten mukaisesti. Rekisterin omistajan vastuulla on valvoa myös mahdollisten ulkopuolisten käyttäjien toiminnan seuraaminen. Mikäli rekisterinpitoon liittyy jotain erityislainsäädäntöä, kuten esimerkiksi pankki- tai terveydenhuollon alalla, rekisterin omistajan tulee seurata tämän erityislainsäädännön vaatimusten toteutumista ja lainsäädännön kehittymistä.

Rekisterin omistajan vaihtuessa on huolehdittava siitä, että uusi omistaja perehdytetään tehtävään. Rekisterin käytöstä poistaminen ja arkistointi kuuluvat myös rekisterin omistajan vastuulle. Henkilötietoihin voi liittyä jotain erityislainsäädäntöä, joka velvoittaa tietojen säilyttämiseen. Tilanteessa, jossa rekisteriä ei enää tarvita, tulee selvittää tällaiset mahdolliset tietojen säilyttämisvelvollisuudet, esimerkiksi kirjanpitolaki tai rahanpesulaki. Tärkeintä on kuitenkin se, että rekisterin käyttö lopetetaan asianmukaisesti ja että rekisteri ei jää lojumaan mihinkään.

Yhteenvetona todettakoon, että rekisterinomistaja on erittäin keskeisessä roolissa tietosuojan toteutumisen kannalta. Rekisterinpitosuunnitelma on tehtävä huolella, rekisterinomistaja on se taho, joka vastaa sen ja lainsäädännön toteuttamisesta sekä rekisterin käytön valvomisesta. Rekisterinomistajille tulee antaa riittävän laaja ja tehokas koulutus, jotta voidaan varmistua siitä, että rekisterinomistajilla on mahdollisimman hyvät edellytykset tehtävän hoitamiseen.

4.3.4 Rekisterin käyttäjä

Lainsäädäntö ei suoraan aseta vaatimuksia rekisterin käyttäjille. Tässä opinnäytetyössä rekisterin käyttäjällä tarkoitetaan henkilöä, jolla on pääsy rekisteriin ja jonka työtehtäviin rekisterin käyttäminen kuuluu.

Rekisterin ylläpito tai henkilötietojen käsittely on voitu sopimuksin ulkoistaa palveluntarjoajalle, jolloin tämä käsittelee henkilötietoja rekisterinpitäjän lukuun. Kyse on tällöin henkilötietojen käytöstä eikä luovuttamisesta, palveluntarjoaja ei saa käyttää henkilötietoja omassa toiminnassaan, sopimuksen vastaisesti tai yhdistellä eri rekistereitä (Tietosuojavaltuutetun toimisto 2010a, 1).

Rekisterin käyttäjälle tulee antaa riittävä tietosuojakoulutus (Tietosuojavaltuutetun toimisto 2010c, 5), se tulisi järjestää ennen kuin käyttäjälle annetaan oikeudet rekisterin käyttöön. Keskeistä on määrittää mitä käyttäjä saa tehdä rekisterillä ja henkilötiedoilla. Tietosuojaohjeiden lisäksi rekisterin käyttäjän tulee olla tietoinen organisaation tietoturvallisuusohjeista (Tietosuojavaltuutetun toimisto 2010c, 5). Koulutuksia tulisi järjestää säännöllisesti, jotta voidaan varmistua osaamisesta. Rekisterin käyttäjä saa käyttää rekisteriä vain siten, kuten häntä on ohjeistettu.

Rekisterin käyttäjiä pitää vaatia allekirjoittamaan vaitiolo- ja salassapitositoumus (Tietosuojavaltuutetun toimisto 2010c, 4). Rekisterin omistajan tulee laatia mahdolliset rekisterin käyttöön liittyvät erityisohjeet, joissa otetaan kantaa erityistilanteisiin, esimerkiksi omien tietojen muokkaamiseen.

Käytännön valvonnan kannalta on keskeistä, että rekisterin omistaja on määrittänyt käyttöoikeudet tarkasti siten, että ne ovat vain niin laajoja, kuin työtehtävät edellyttävät (Tietosuojavaltuutetun toimisto 2010c, 4). Myös mahdolliset vaaralliset työyhdistelmät tulee ottaa huomioon. Järjestelmästä saatavien lokien tulee olla niin yksityiskohtaisia, että on mahdollista selvittää kuka on tehnyt toimenpiteitä rekisteriin (Tietosuojavaltuutetun toimisto 2010c, 4). Myös pelkästä rekisterin selaamisesta pitää jäädä jälki lokiin. Mikäli mahdollista,

tulee lokiseurannan olla järjestelmällistä (Tietosuojavaltuutetun toimisto 2010c, 7) ja mahdollisia automaattihälytyksiä asettaa.

Kun käyttäjän työsuhde päättyy tai hän siirtyy toisiin tehtäviin, tulee rekisterin käyttöoikeudet poistaa (Tietosuojavaltuutetun toimisto 2010c, 6-7). Mikäli mahdollista, poistamisen tulisi olla automaattista. Vain henkilöillä, joilla on todellinen työtehtävien edellyttämä syy käyttää rekisteriä, saa olla pääsy rekisteriin.

Rekisterin käyttäjä on velvollinen ilmoittamaan rekisterin omistajalle mahdollista havaitsemistaan rikkeistä tai poikkeamista rekisterin käytöstä. Tarvittaessa rekisterin käyttäjä voi ottaa yhteyttä suoraan organisaation tietosuojavastaavaan.

Yhteenvetona todettakoon, että rekisterin omistajat ja heidän käyttöoikeutena tulee määritellä erittäin huolellisesti ja tarkasti. Vaikka käyttöoikeudet on rajattu, tulee rekisterin käyttöä seurata aktiivisesti tarkoista käyttäjälokeista. Käyttäjillä tulee antaa riittävä koulutus tehtäväänsä ennen henkilötietojen käsittelyn aloittamista.

5 Asiantuntijahaastattelut

Asiantuntijahaastatteluja suoritettiin yhteensä 16 kpl. Haastattelut toteutettiin sekä ryhmä-, pari-, että yksilöhaastatteluina. Suurimmaksi osaksi haastattelut pidettiin osana projektipalavereja, mutta osa järjestettiin omina tilaisuuksinaan. Haastateltaville lähetettiin ennakkomateriaali, joka sisälsi kuvauksen koko tietosuojaprojektista, keskeisiä tietosuojaan liittyviä määritelmiä sekä pohjustavia kysymyksiä, joiden tehtävänä oli valmistella henkilö haastatteluun.

Haastateltaviksi henkilöiksi valittiin asiantuntijoita eli S-ryhmän tietosuojan kehittämiseen tähdänneen projektin työryhmän jäseniä ja keskeisten rekisterien käytöstä päättäviä tahoja. Haastatteluissa pyrittiin tuomaan esille jo olemassa olevia parhaita käytäntöjä, mutta myös kuvausta siitä, miten tietosuojaa voitaisiin edelleen kehittää ja kuinka voidaan valmistautua tuleviin lainsäädännön muutoksiin. Haastateltaville oli siis selvä kuva siitä, miten tietosuojaasiat oli järjestetty S-ryhmässä.

Seuraavaksi kuvataan analysoidut yhteenvedot jokaisen haastattelun pöytäkirjasta. Opinnäytetyön tilaajan pyynnöstä haastateltavien tahojen nimiä ei mainita.

5.1 Tiivistelmät yksittäisistä haastatteluista

1. Haastattelu

S-ryhmän osuustoiminnalle tyypillisen omistus- ja ohjausrakenteen ansiosta tietosuoja on oltava organisoitua paitsi S-ryhmätasolla, myös alueosuuskauppa- ja yhtiötasolla. Ajatus osuuskaupan ja SOK:n tytär- sekä osakkuusyhtiöiden tietosuojavastaavasta S-ryhmän tietosuojavastaavan rinnalla sai kannatusta. Alueosuuskaupan tietosuojavastaava tukisi oman vastuualueensa henkilöstöä tietosuoja-asioissa ja toimisi yhteyshenkilönä S-ryhmän tietosuojavastaavan. (1. Pöytäkirja 2012.)

Henkilötietojen ja henkilörekistereiden omistajuus nähdään selkänä asiana, jonka tulee olla aina kunnossa. Vastuiden tulee olla määriteltyinä selkeästi. Rekisterin käyttäjällä tulee olla pääsy rekisteriin vain työtehtävien sallimissa rajoissa. S-ryhmän tietosuojavastaava nähdään ennen kaikkea kokonaisuutta ohjaavana toimijana. Haastateltavat näkevät tärkeänä sen, että organisaation kaikilla tasoilla työskentelevät henkilöt tietävät keneen voi ja tulee ottaa yhteyttä tietosuoja-asioissa. (1. Pöytäkirja 2012.)

S-ryhmän tietosuojatyöryhmän haastateltavat näkevät ennen kaikkea toimintaa ohjaavana elimenä. Työryhmällä ei tule olla tuotannollista vastuuta, mutta ryhmä on S-ryhmän tietosuojavastaavan tukena ja osallistuu kommentointiin, linjausten tekemiseen, ajankohtaisten asioiden tunnistamiseen ja toimenpidesuunnitelmien laadintaan. Ryhmän kokoonpano tulee valita siten, että saadaan kattava otanta eri toimialoista. Kokoustavat tulee miettiä huolella, ryhmän ei tule kokoontua liian usein, ellei siihen ole todellista tarvetta. (1. Pöytäkirja 2012.)

2. Haastattelu

Haastateltava näkee käyttöoikeuksien hallinnan merkittävänä osana tietosuojaa. Oikeuksien tulee olla hajautettuja, jotta ns. vaarallisia työyhdistelmiä ei synny. Oikeuksin luomisen tulee aina edetä ennalta määritetyn prosessin mukaan. Käyttäjille pitää olla mahdollista asettaa järjestelmästä erilaisia rooleja. Käyttäjien toimien seuranta nähdään tärkeänä asiana. Lokeista pitää näkyä mitä käyttäjä on tehnyt tai katsonut. Lisäksi automaattinen lokien seuranta ja hälytykset koetaan hyväksi valvonnan keinoksi. Käsiteltävän tiedon laatu ja sen valvonta koetaan tärkeäksi. Tietoturvallisuuden testaamisesta huolehtiminen kuuluu haastattelun perusteella rekisterin omistajan vastuulle. (2. Pöytäkirja 2012.)

3. Haastattelu

Rekisterin omistaja vastaa henkilötietojen käsittelyn lainmukaisuudesta. Käyttöoikeuksia voivat myöntää vain tietyt henkilöt ja oikeuksien hallinta tehdään prosessin mukaan. On olemassa eritasoisia käyttäjiä erilaisia työtehtäviä varten. Rekisterin omistaja tekee yhteistyötä järjestelmätoimittajan kanssa. Rekisteröidyn suostumus ja etu koettiin tärkeäksi. Rekisteriä saa käyttää vain työtehtävien edellyttämissä rajoissa ja rekisterin omistaja vastaa käytön valvonnasta. Lokitiedoista nähdään kuka on tehnyt ja mitä toimenpiteitä. Rekisterin omistaja on tehnyt selvät ohjeet, jotka on koulutettu rekisterin käyttäjille. (3. Pöytäkirja 2012.)

4. Haastattelu

Rekisterin omistaja vastaa käyttöoikeuksien hallinnasta. Käyttäjän tulee suorittaa vaadittava koulutus hyväksytysti, ennen kuin oikeuksia voi hakea. Käyttöoikeuksia voivat myöntää vain tietyt henkilöt. Kun käyttöoikeuksille ei ole tarvetta, käyttöoikeudet poistetaan automaattisesti. Ulkoistamissopimukset ja niiden valvonta kuuluvat rekisterin omistajalle. Vain tarpeellisia tietoja käsitellään ja tietojen laatua valvotaan. Rekisterin omistaja toimii yhteyshenkilönä rekisteröityjen suuntaan, mutta vastaa myös tietosuojavaltuutetun selvityspyyntöihin. (4. Pöytäkirja 2012.)

Rekisteriseloste on ajan tasalla ja rekisterin omistaja vastaa siitä. Myös tietoturvatestaaminen ja palveluntarjoajan auditointi sekä sopimusten valvonta kuuluvat rekisterin omistajalle. Käyttäjälokien kerääminen nähdään tärkeänä. Kaikki toimenpiteiden pitää jäädä lokiin, myös pelkkä haku tai katsominen ilman toimenpiteitä. Järjestelmä mahdollistaa monipuolisten hälytysten ja raporttien ajamisen. (4. Pöytäkirja 2012.)

5. Haastattelu

Tämä haastattelu on analysoitu vain pöytäkirjasta, aikatauluhaasteista johtuen en itse ollut mukana haastattelutilanteessa.

Haastateltava näkee S-ryhmän tietosuojavastaavan erityisasiantuntijana koko S-ryhmälle. Käytännön toteuttamisessa SOK:lle keskityn ohjauksen ja koordinoinnin malli nähdään hyvänä ja toimivana asiana. Alueosuuskaupan puolella pitää huolehtia siitä, että saatavilla on riittävä tietoisuus tarjolla olevasta avusta. Tietosuojavastaavan tulee yhteistyössä tietosuojan kehitysryhmän kanssa tuottaa mahdollisimman selkeitä ja ytimekkäitä ohjeita sekä huolehtia niiden jalkauttamisesta. Käyttäjien valvonta ja riittävät lokitiedot nähdään tärkeänä asiana. Tärkeää on myös olla tietoinen erilaisista erityisvaatimuksista, joitain tietoja on luovutettava ja joitain tietoja ei saa luovuttaa. (5. Pöytäkirja 2012.)

6. Haastattelu

Tämä haastattelu on analysoitu vain pöytäkirjasta, aikatauluhaasteista johtuen en itse ollut mukana haastattelutilanteessa.

Rekisterin omistaja vastaa rekisteriselosteista. Tärkeänä asiana nähdään se, että rekisteriä käyttävät henkilöt kirjoittavat vaitiolositoumuksen. Selkeät mallit esimerkiksi tiedon tarkastus- tai korjaustilanteissa nähdään tärkeinä asioina. Toimintamalleja ja ohjeiden noudattamista tulee valvoa säännöllisesti. Rekisteröidyn oikeudet ymmärretään ja vastuu niiden toteuttamisesta kuuluu rekisterin omistajalle. (6. Pöytäkirja 2012.)

Erityisen huolellinen pitää olla tilanteissa, joissa järjestelmään tehdään muutoksia. Henkilötiedot eivät saa vaarantua esimerkiksi versionvaihtojen takia. Rekisterin omistajan tulee valvoa palveluntarjoajaa. Rekisteriselosteet ja muu viestintä tulee suunnitella asiakaslähtöisesti. Viestinnän näkökulmasta asiallinen ja tiivis viesti voi olla monimutkaista ja yksityiskohtaista selkeämpi ja rekisteröidyn helpommin ymmärrettävissä. (6. Pöytäkirja 2012.)

7. Haastattelu

Tietosuoja-asiantuntijuuden keskittäminen nähdään toimivana ratkaisuna. Haastateltava näkee, että johdon tehtävä on pitää huolta siitä, että aihe ja sen vakavuus ymmärretään, ja että siitä sekä ohjeista viestitään tarpeeksi. Yhteiset säännöt ja ohjeet nähdään hyvänä toimintaa selkeyttävänä asiana. S-ryhmän tietosuojavastaava nähdään ennen kaikkea erityisasiantuntijana, joka kykenee tarvittaessa auttamaan haasteiden selvittämisessä. On tärkeätä, että organisaatiossa on yksi kaikkien tiedossa oleva taho, jolta voi tarvittaessa hakea apua. (7. Pöytäkirja 2012.)

8. Haastattelu

Lähtökohtana tietojen keräämisen pitää aina olla laillinen peruste ja liiketoiminnan tarve. Tietoja kerättäessä on pidettävä mielessä rekisteröidyn näkökulma. Haastattelussa korostui tiedon tarpeellisuusvaatimus myös rekisterin omistajan näkökulmasta. Turhasta tiedosta ei ole kuin haittaa ja mikäli tieto on vanhentunutta heti kysymisen jälkeen, ei sitä ole mitään järkeä kysyä alkuunkaan. Ylimääräisen tiedon käsittely on paitsi laitonta, mutta sen ylläpito kuluttaisi vain turhia resursseja. (8. Pöytäkirja 2012.)

9. Haastattelu

Haastateltava näkee keskeisenä asiana sen, että tietosuojaan liittyvistä ohjeistuksista tulee tiedottaa selvästi ja niiden tulee olla helposti saatavilla. Tiedottamisen merkitystä korostetaan. Ohjeiden tulee olla ytimekkäitä ja toimivia, loppukäyttäjä tulee pitää mielessä. Haastateltavan mielestä on erityisen tärkeätä, että rekisteröity on ajattelun keskiössä. Toiminnan läpinäkyvyys korostui haastattelussa, rekisteröidylle pitää aina kertoa mihin tietoja käytetään ja miksi niitä kerätään. Läpinäkyvyys tarkoittaa selkeitä selosteita ja toimivia prosesseja tietojen tarkastamiseksi. (9. Pöytäkirja 2012.)

10. Haastattelu

Haastattelussa vahvistui käsitys siitä, että rekisterin omistaja on vastuussa henkilötietojen käsittelyn lainmukaisuudesta. Rekisterin omistajalla on paras käsitys siitä, miten tietosuoja toteutuu käytännön toiminnassa. Selkeät toimintaohjeet ja periaatteet nähdään tärkeänä asiana. Esitetty kuvaus rekisterin perustamisen prosessista saa kannatusta. (10. Pöytäkirja 2012.)

Keskitetty tietosuojan koordinointi ja ohjeistus nähdään toimivana mallina. Haastateltavien mielestä ei ole järkeä siinä, että samoja haasteita ratkaistaan usean tahon toimesta. Yhteistoiminnasta on etua kaikille ja se säästää resursseja, samalla varmistetaan toiminnan yhteismitallisuus. (10. Pöytäkirja 2012.)

Menettely, jossa rekisterin omistajan pitää hyväksyttää suunnitelma rekisterinpidosta tietosuojavastaavalla, koetaan hyvänä ratkaisuna. Menetelmän byrokraattisuutta pohditaan, mutta menetelmä takaa tietosuojavastaavalle yhden väylän vaikuttaa. Tietosuojavaltuutetun toimiston ohje rekisteritoimintojen analysoinnista vaikuttaa haastateltavien mielestä sopivalta myös rekisterisuunnitelmaksi. (10. Pöytäkirja 2012.)

11. Haastattelu

Haastateltavan mielestä rekisterin käyttöoikeuksien rajaaminen tarkasti vain tarpeellisia työtehtäviä varten on keskeistä. Käyttöoikeuksia ei pidä myöntää, mikäli niihin ei ole tarvetta. Käyttöoikeuksien hallinnointi kuuluu rekisterin omistajalle. Rekisterin omistaja myös vastaa palveluntarjoajan valinnasta ja valvonnasta. Myös palveluntarjoajan käyttöoikeuksien määrittely on tärkeätä, vaikka palveluntarjoaja ei käyttäisikään rekisteriä, voi sillä periaatteessa olla pääsy tietoihin varsinaisen tietokannan kautta. Palveluntarjoajan kanssa on tehtävä tarpeeksi tiukat sopimukset. (11. Pöytäkirja 2012.)

Haastateltavan mielestä on tärkeätä, että tietosuoja- ja tietoturvaperiaatteet ovat samat koko S-ryhmässä. Rekisteröidyn näkökulmasta on myös tärkeätä, että asioista viestitään selkeästi, ja että organisaatiolla on sama linja vaikka palvelut vaihtuvat. Tietosuojan ohjeistuksen ja koordinoinnin keskitetyn mallin haastateltava näkee toimivana. Rekisterikohtaisia erityispiirteitä lukuun ottamatta peruslähtökohdat ovat samat kaikilla, esimerkiksi tietoturvatestausten osalta. (11. Pöytäkirja 2012.)

Tärkeänä huomiona haastateltava näkee sen, että uudet tekniset järjestelyt tai prosessit eivät saa aiheuttaa ristiriitoja esimerkiksi rekisteriselosteen ja käytännön toiminnan välille. (11. Pöytäkirja 2012.)

12. Haastattelu

Haastateltavan mukaan tietosuoja on huomioitu myös vuosittaisissa riskianalyyseissä. Haastattelussa korostui erityisesti tietojen oikeellisuuden merkitys. Oikeellisuudella on suuri merkitys sekä rekisterinpitäjälle, että rekisteröidylle. Virheellinen tai vanhentunut data saattaa aiheuttaa suuriakin kustannuksia. Rekisteröidyn kannalta on tärkeätä, että yhteystiedot ovat oikein, jotta oikea henkilö tavoitetaan. (12. Pöytäkirja 2012.)

Toinen keskeinen haastattelussa korostunut teema oli palveluntarjoajat. Sopimusten tulee olla kunnossa ja rekisterin omistaja vastaa niistä sekä niiden valvonnasta. Sopimuksissa tulee huomioida erityisesti tietoturvallisuus sekä tietosuoja, erittäin tarkasti tulee kuvata toiminta tilanteissa, joissa on kyse tietojen luovuttamisesta. Sopimuksia tehdessä tulee kiinnittää huomiota myös valvonta- ja tarkastusmahdollisuuteen. (12. Pöytäkirja 2012.)

Rekisteröidyn näkökulma tulee ottaa huomioon viestinnässä, on mietittävä kuinka rekisteröity ymmärtää viestin. Rekisteröidyn suostumuksen tai kieltäytymisen kunnioittaminen nähdään tärkeänä asiana. Tietosuojan ohjeistuksen ja koordinoinnin keskitetty malli nähdään hyvänä ja toimivana ratkaisuna. Tietosuoja-asioita on järkevää käsitellä yhteisesti. (12. Pöytäkirja 2012.)

13. Haastattelu

Haastateltava on samaa mieltä siitä, että tietosuojaa on syytä kehittää yhteisvoimin. Peruslähtökohdiltaan tietosuojassa on kyse saman lainsäädännön noudattamisesta. Keskitetty ohjaus- ja koordinointimalli olisi haastateltavan mielestä toimiva ratkaisu. (13. Pöytäkirja 2012.)

Ohjeiden tuottamisen pitäisi tapahtua keskitetysti. Tietosuojaohjeiden tulee olla selkeitä, ytimekkäitä ja niissä tulee keskittyä oleelliseen. Haastateltava kokee riittävän tietosuoja-

asioista viestimisen tärkeäksi. On tärkeätä, että tietosuoja ymmärretään samalla tavalla eri puolella organisaatiota ja että myös toimintatavat ovat yhteismitallisia. (13. Pöytäkirja 2012.)

Haastattelussa tulee esille se, että ulkopuolisten sidosryhmien vaatimukset on huomioitu henkilötietojen käsittelyssä, ja että se kuuluu rekisterin omistajan vastuulle. Rekisterin käyttöoikeudet on jaettu työtehtävien perusteella. (13. Pöytäkirja 2012.)

14. Haastattelu

Haastateltavien mukaan tietosuoja tulee organisoida siten, että S-ryhmän osuustoiminnalle tyypillinen ohjausrakenne otetaan huomioon. Haastateltavat toivovat keskitetyltä mallilta yhteneväisyyttä ja selkeitä linjauksia, jotka ovat kaikille samat. Tuotettavien ohjeistuksien tulee olla tiiviitä ja selkeitä, ja niitä toivotaan oleellisista asioista. Ohjeen kohderyhmä tulee huomioida ohjetta tehdessä. Haastateltavien arvion mukaan tietosuojan merkitys tulee korostumaan tulevaisuudessa. (14. Pöytäkirja 2012.)

Tietojen oikeellisuus koetaan tärkeänä sekä rekisteröidyn, että rekisterin omistajan näkökulmasta. Vääristä tiedoista on vain haittaa molemmille. Haastateltavien mukaan on hyvä, että organisaatiosta löytyy yksi taho, josta voi hakea apua tarvittaessa. Yhteistyökumppaneiden ja palveluntarjoajien valvonta nähdään tärkeänä asiana, johon tulee olla tarjolla työkaluja. (14. Pöytäkirja 2012.)

15. Haastattelu

Haastateltava näkee keskitetyn ohjaus- ja koordinointimallin tarpeellisena ratkaisuna. Mallin tulee olla yksinkertainen ja turhaa byrokratiaa tulee välttää. Keskitetty malli sopii hyvin S-ryhmän osuustoiminnalle tyypilliseen ohjausrakenteeseen. Haastateltavan mukaan myös tuotettavien ohjeiden tulisi olla mahdollisimman yksinkertaisia ja niissä tulee ottaa kantaa vain oleellisiin asioihin. Tietosuojatietoisuuden lisäämisen haastateltava kokee tärkeänä. (15. Pöytäkirja 2012.)

Se, että organisaatiosta löytyy taho, jolta voi tarvittaessa kysyä apua, on tärkeää haastateltavan mielestä. Tietoiskut ja koulutukset kuulostavat haastateltavan mielestä toimivalta ratkaisulta. Haastateltava muistuttaa, että koulutuksen tulee olla jatkuvaa. Haastateltava näkee tietosuojan tarkemman organisoinnin positiivisena ja tarpeellisena asiana. (15. Pöytäkirja 2012.)

16. Haastattelu

Haastateltavat kokevat hyväksi sen, että on selkeästi yksi taho, joka ohjeistaa tietosuoja-asioissa, ja jolta voi tarvittaessa kysyä apua tietosuojaan liittyvissä asioissa. Tietosuojan keskittäminen asiantuntijoille on haastateltavien mielestä järkevä ratkaisu. Haastateltavat toivovat uudelta mallilta tukea muutoksiin ja projekteihin. (16. Pöytäkirja 2012.)

Haastateltavat ottavat omien sanojensa mukaan mielellään selkeitä ohjeita vastaan. Selkeät linjaukset ja prosessit helpottavat yhteistyötä palveluntarjoajien ja yhteistyökumppaneiden kanssa. Lainsäädännön ja muiden ulkoisten tietosuojaan liittyvien vaatimusten seuraamisen tulisi haastateltavien mielestä tapahtua keskitetysti. (16. Pöytäkirja 2012.)

5.2 Yhteenveto haastatteluista

Pidettyjen haastattelujen pohjalta vahvistui käsitys siitä, että S-ryhmässä on tarvetta tietosuojan keskitetylle ohjaukselle ja koordinoinnille. Koska kaikkien rekisterien pohjalla on sama lainsäädäntö, on järkevää, että perusteita ja ohjausta tuotetaan keskitetysti. Haastateltavat toivoivat myös nykyistä kattavampaa S-ryhmätasoista linjausta, joka asettaisi tiettyjä rajoja ja ohjaisi kaikkia tiettyyn samaan suuntaan.

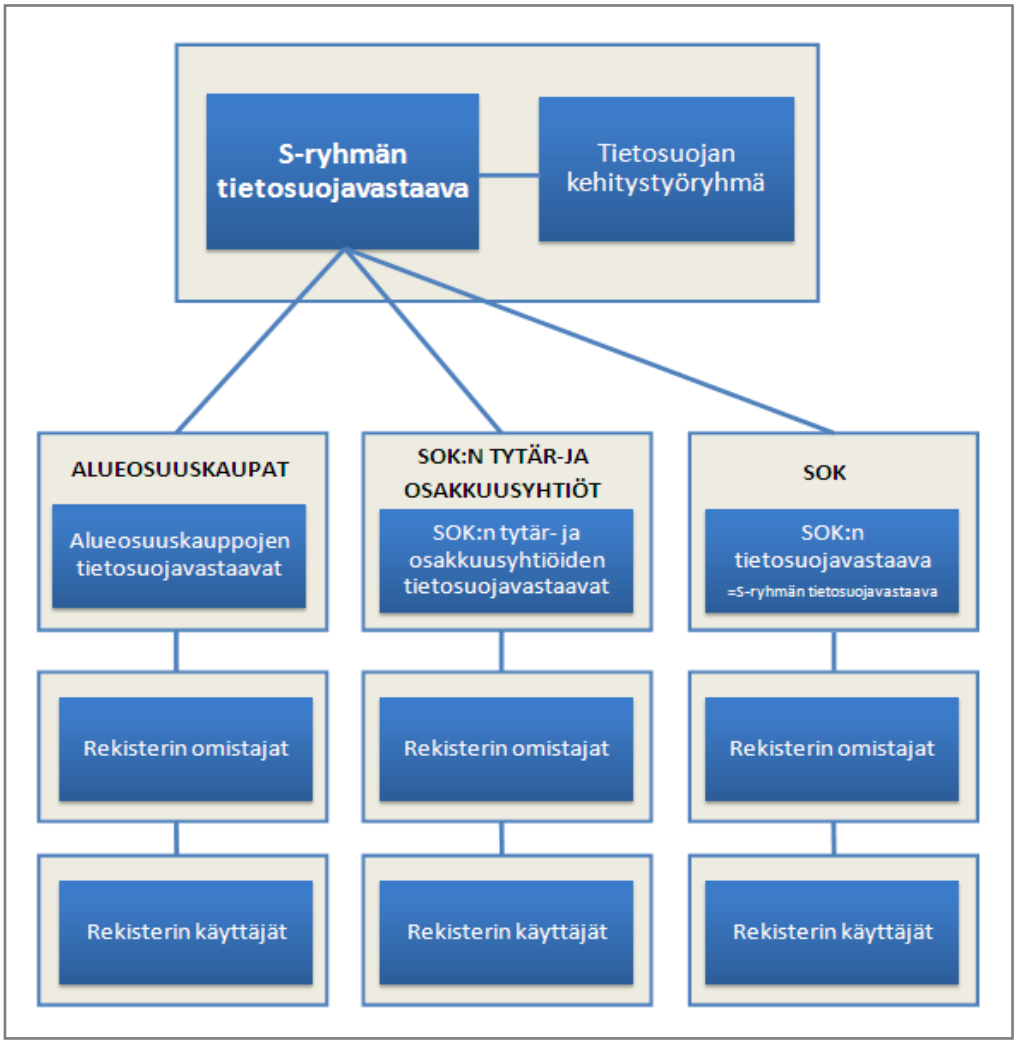
S-ryhmän tietosuojavastaavan nimeäminen ja siitä tiedottaminen koettiin hyväksi ratkaisuksi. Haastateltavat olivat yhtä mieltä siitä, että on järkevää, että tarvittaessa asiantuntevaa apua, on saatavilla organisaation sisältä yhdeltä kaikkien tiedossa olevalta taholta.

Haastattelujen pohjalta selvisi myös se, että tietosuojatietoisuutta tulisi entisestään nostaa. Vaikka merkittävien rekisterin osalta vastuuhenkilöillä oli selvä tietämys siitä mitä heiltä odotetaan, haastateltavat näkivät tarvetta yhtenäisten tietosuojakoulutuksien ja tietosuojaohjeiden kehittämiselle. Aiemmin kehittämistä oli tehty suurimmaksi osin rekisteri- ja yksikkökohtaisesti.

Yhteenvetona voidaan todeta, että haastatteluissa vahvistui käsitys tarpeesta tietosuojaan liittyvän yhteistyön lisäämiselle ja koordinoinnille. Tietosuojatyöryhmä olisi kanava hyvien käytäntöjen levittämiseen ja mahdollistaisi tiiviimmän yhteistyön keskeisten rekisterin omistajien välillä. Tarvetta on myös taholle, joka seuraa lainsäädännön ja ulkoisten vaatimusten muutoksia sekä tiedottaa niistä keskitetysti rekisterin omistajille. Seuraavassa luvussa esitetään ratkaisu haastatteluissa ilmenneisiin haasteisiin ja odotuksiin.

6 Tietosuojavastuiden organisointi S-ryhmässä

Tässä luvussa esitetään opinnäytetyön tulokset eli luonnosehdotus tietosuojan organisoinnista S-ryhmässä perustuen lakisääteisiin vaatimuksiin, tietosuojavaltuutetun ohjeisiin, tulevaan EU:n lainsäädäntöön ja pidettyihin asiantuntijahaastatteluihin pohjautuen. Esitys uudesta organisoinnista on kuvattu oheisessa luonnoksessa (kuva 3).



Kuva 3: Ehdotus tietosuojan organisoinnista S-ryhmässä

Nimettävä S-ryhmän tietosuojavastaava, joka toimii koko S-ryhmän erityisasiantuntijana ja koordinoi tietosuojan kehittämistä koko S-ryhmän tasolla. S-ryhmän tietosuojavastaava hoitaisi samalla SOK:n tietosuojavastaavan tehtävää ja valvoisi SOK:n rekisterin omistajia. S-ryhmän tietosuojavastaava toimisi tietosuojan osalta S-ryhmän yhteyshenkilöinä viranomaisiin. Tietosuojan kehitystyöryhmän koordinointi kuuluisi S-ryhmän tietosuojavastaavan tehtäviin.

Perustettava tietosuojan kehitystyöryhmä, joka tukee S-ryhmän tietosuojavastaavaa tämän tehtävän hoitamisessa. Kehitystyöryhmä koostuu ainakin keskeisten rekisterien omistajista, lainsäädännön ja järjestelmien tuntemusta omaavista tahoista. Kehitystyöryhmässä tulisi olla edustusta myös alueosuuskaupoista. Työryhmä antaa S-ryhmän tietosuojavastaavalle mahdollisimman hyvän tuen ja tietämyksen siitä, mitä organisaation eri osissa tapahtuu tietosuojan osalta. Kehitystyöryhmän avulla rekisterin omistajien näkemykset saadaan vahvasti mukaan kehittämiseen. Työryhmä mahdollistaa siirtymisen rekisteri- ja yksikkökohtaisesta tietosuojan kehittämisestä koko S-ryhmän tasoiseen tietosuojan kehittämiseen.

S-ryhmän osuustoiminnalle tyypillisestä omistus- ja ohjausrakenteesta johtuen alueosuuskaupat ovat juridisesti itsenäisiä toimijoita. Ne vastaavat viime kädessä itse omien henkilörekisteriensä käytöstä, joten myös jokaisen alueosuuskaupan tulisi nimetä oma tietosuojavastaava. Sama koskee myös SOK:n tytär- ja osakkuusyhtiötä. Alueosuuskauppojen, sekä tytär- ja osakkuusyhtiöiden tietosuojavastaavilla olisi kuitenkin S-ryhmän tietosuojavastaavan tuki ja ohjaus, joten rooli voisi olla aluksi lähinnä tiedottamiseen ja henkilötietojen käsittelyn tilannekuvan ylläpitoon liittyvä.

Tässä ehdotuksessa kukin tietosuojavastaava valvoo omalla vastuualueellaan mahdollisesti olevia rekisterin omistajia. Kun rekisterin omistajan pitää hyväksyttää rekisterinpitosuunnitelma tietosuojavastaavalla, tietosuojavastaava pysyy tietoisena vastuualueensa henkilötietojen käsittelystä ja pystyy myös vaikuttamaan siihen ennen käsittelyn aloittamista. Rekisterin omistajan vastuulla, kuten jo aiemminkin on ollut, on vastata, valvoa ja kouluttaa kyseisen rekisterin käyttäjiä ja vastata ennen kaikkea siitä, että toiminta on lainsäädännön vaatimusten mukaista.

Edellä kuvattua organisointia noudattamalla mahdollistetaan keskitetty ohjaus S-ryhmän tietosuojavastaavan ja tietosuojan kehitystyöryhmän kautta. Yhteisen linjan luominen tapahtuu S-ryhmän tietosuojavastaavan ja tietosuojan kehitystyöryhmän toimesta. Mallista selviää myös miten viesti kulkee rekisterin käyttäjältä S-ryhmän tietosuojavastaavalle asti, tai toiseen suuntaan. S-ryhmätasoiset tietosuojaohjeet vähentävät rekisterin omistajien tarvetta ohjeiden luomiseen, he voivat keskittyä ohjeiden jalkauttamiseen. Malli vähentää päällekkäisen työn määrää ja parantaa tiedonkulun tehokkuutta.

Mallin avulla varmistetaan myös se, että S-ryhmän tietosuojavastaavalla on mahdollisimman hyvä kuva tietosuojasta ja henkilötietojen käsittelystä koko S-ryhmässä ja sitä kautta parhaat mahdolliset edellytykset tehtävän hoitamiseksi. Tietosuojavastaava pystyy käytännössä myös vaikuttamaan henkilötietojen käsittelyyn organisaatiossa. Esitetyn mallin mukaan tulevien tiukentuvien tietosuojamääräysten jalkauttaminen on tehokkaasti toteutettavissa.

7 Työn arviointi

Ojasalon ym. (2009, 40-41) mukaan kehittämistyössä on tärkeätä menetelmien moninaisuus, jolla varmistetaan se, että kehittämisen tueksi saadaan mahdollisimman monipuolista tietoa. Tässä opinnäytetyössä haastateltiin S-ryhmän asiantuntijoita sekä yksilö-, pari-, että ryhmähaastattelujen muodossa. Dokumenttien analyysi oli toinen keskeinen työssä käytetty menetelmä.

Haastattelujen avulla saatiin esille monia mielenkiintoisia näkökulmia ja kehittämisehdotuksia myös tulevalle tietosuojavastaavalle ja tietosuojan kehitysryhmälle ratkaistavaksi. Mikäli työ tehtäisiin uudestaan, valitsisin haastateltavaksi enemmän henkilöitä alueosuuskaupoista ja SOK:n tytär- ja osakkuusyhtiöistä. Haastattelun otanta oli melko SOK:lle painottunut johtuen alun tiiviimmästä rajauksesta.

Asiantuntijahaastattelut olivat mielestäni oikea vaihtoehto työn toteuttamiselle, kuten Ojasalo ym. (2009, 40) toteavat, kehittämistyötä tehdään harvoin yksin. Menetelmiin liittyvänä arviona todettakoon, että mikäli työ toteutettaisiin uudelleen, saattaisin käyttää esimerkiksi alueosuuskaupoille suunnattua kyselyä apuna kokonaisvaltaisempien tulosten saamiseksi.

Benchmarking menetelmällä, jossa vertaillaan toimintaa toiseen kohteeseen (Ojasalo ym. 2009, 41) olisi myös voitu löytää hyviä käytäntöjä S-ryhmän ulkopuolelta. Työssä olisi voitu tarkastella sitä, miten muut ovat asian ratkaisseet. Tosiasia on kuitenkin se, että S-ryhmän osuustoiminnalle tyypillinen ohjaus- ja omistusrakenne aiheuttaa tiettyjä haasteita yleisten mallien hyödyntämiselle. Kriittisen tarkastelun kohta on myös se, että tähän työhön ei aikataulusyistä haastateltu tietosuojavaltuutettua, vaan työn lähteinä käytettiin ainoastaan saatavilla olevia materiaaleja, kuten tietosuojavaltuutetun lausuntoja ja tietosuojavaltuutetun toimiston ohjeita.

Aikataulusyistä kehittämisluonnosta ei viety käytäntöön opinnäytetyön puitteissa. Työ jätettiin tilaajalle, joka päättää sen jatkokäytöstä ja hyödyntämisestä. Olisi ollut mielenkiintoista tarkastella sitä, miten suunniteltu malli toimisi sen jalkauttamisen jälkeen ja mitä palautetta siitä tulisi. Valittu menetelmä, tapaustutkimus sopi hyvin työn toteuttamiselle ja työ eteni tapaustutkimuksen vaiheistusta noudattaen alusta loppuun.

Työn tilaajalta, SOK:n Riskienhallinta-yksiköltä saadun palautteen (Liite 1 - Lausunto opinnäytetyöstä) perusteella voin todeta olevani tyytyväinen tähän opinnäytetyöhön. Palautteesta käy ilmi, että työ täytti sille asetetut tavoitteet ja että työn tuloksia tullaan hyödyntämään S-ryhmän tietosuojan kehittämisessä.

8 Yhteenveto

Opinnäytetyön tavoitteena oli tuottaa S-ryhmälle kehitysluonnos tietosuojan organisoinnista. Voimassaolevasta lainsäädännöstä, EU:n tulevan tietosuoja-asetuksen luonnoksesta ja valvovan viranomaisen linjauksista koostuva teoriatieto yhdistettiin S-ryhmän asiantuntijoiden näkemyksiin, joiden pohjalta tuotettiin ehdotus siitä, miten tietosuoja tulisi järjestää S-ryhmässä. Työssä tavoitteena oli löytää nimenomaan S-ryhmälle sopiva toimiva ratkaisu. Mielestäni tästä työstä on kuitenkin hyötyä myös muille rekisterinpitäjille ja rekisterinpitoa suunnitteleville toimijoille.

Tutkimuksellisen kehittämisen menetelmiä käyttäen toteutetusta työstä oli hyötyä työn tilaajalle, sillä saadun palautteen (Liite - Lausunto opinnäytetyöstä) mukaan valmistunut työ huomioidaan S-ryhmän tietosuojan kehittämisessä ja ohjausmallin määrittämisessä. Prosessi eteni tavoitteen mukaisesti alusta loppuun ja mielestäni työn konkreettiset tulokset ovat helposti hyödynnettävässä muodossa. Todettakoon, että opinnäytetyö saavutti sille asetetut tavoitteet.

Lähteet

Alastalo, M. & Åkerman, M. 2010. Asiantuntijahaastattelun analyysi: faktojen jäljillä. Teoksessa J. Ruusuvuori, P. Nikander & M. Hyvärinen (toim.) Haastattelun analyysi. Tampere: Vastapaino.

Euroopan Komissio. 2012. Lehdistötiedote -Tietosuojasääntöjen kattava uudistus parantaisi käyttäjien mahdollisuuksia valvoa tietojaan ja vähentäisi yritysten kustannuksia. Viitattu 28.2.2012.
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=PDF&aged=0&language=FI&guiLanguage=en

European Commission. 2012a. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Viitattu: 14.2.2012.
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Commission. 2012b. How does the data protection reform strengthen citizens' rights?. Viitattu: 28.2.2012.
http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf

European Commission. 2012c. Why do we need an EU data protection reform?. Viitattu: 19.3.2012.
http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

Helsingin Sanomat. 2012. Kymmenet poliisit joutuvat esitutkintaan Myllylä-kaivelusta. Lehtiartikkeli. Viitattu: 21.3.2012.
http://www.hs.fi/kotimaa/Kymmenet+poliisit+joutuvat+esitutkintaan+Myllyl%C3%A4-kaivelusta/a1305556407250

Henkilötietolaki 22.4.1999/523.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15., uudistettu painos. Hämeenlinna: Kariston Kirjapaino.

Kansallinen turvallisuusauditointikriteeristö, 2. versio. 2011. Helsinki: Puolustusministeriö.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. 1.-2. painos. Helsinki: WSOYpro.

Salminen, J. 2011. Suomessa miljoona henkilörekisteriä. Viitattu: 28.2.2012.
http://suomenkuvalehti.fi/jutut/kotimaa/suomessa-miljoona-henkilorekisteria-isoilta-ruumiilta-valtytty

Silvennoinen, P. 2004. Yksityisyys ja henkilötiedot www-sivustoilla. Tampereen yliopisto. Tietojenkäsittelytieteiden laitos. Pro gradu - tutkielma. Viitattu: 17.2.2012.
http://www.cs.uta.fi/research/thesis/masters/Silvennoinen_Paula.pdf

Suomen perustuslaki 11.6.1999/731.

S-kanava. 2012. Suomen Osuuskauppojen Keskuskunta. Viitattu: 26.3.2012.
http://www.s-kanava.fi/web/vk/oma-s-kanava/kirjautumaton

Taloustiedote. 2012. Suomen Osuuskauppojen Keskuskunta. Viitattu: 27.2.2012.
http://www.s-kanava.fi/web/s-kanava-medialle/tiedote?announcement=209507_10816

Tietoa S-ryhmästä. 2012. Suomen Osuuskauppojen Keskuskunta. Viitattu: 14.2.2012. http://www.s-kanava.fi/web/s-kanava-tietoa-s-ryhmasta/tietoa-s-ryhmasta

Tietosuojavaltuutetun toimisto. 2002. Ota oppaaksi henkilötietolaki!. Viitattu: 14.2.2012. http://www.tietosuoja.fi/uploads/aue2z4d.pdf

Tietosuojavaltuutetun toimisto. 2010a. Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset. Viitattu: 14.2.2012. http://www.tietosuoja.fi/uploads/fqfq98_1.pdf

Tietosuojavaltuutetun toimisto. 2010b. Tietosuojavastaavan toimenkuva, tehtävät ja asema. Viitattu: 14.2.2012. http://www.tietosuoja.fi/uploads/939r21bdr3_1.pdf

Tietosuojavaltuutetun toimisto. 2010c. Tietosuojan ja tietoturvan ”tee se itse” - tarkastus. Viitattu: 14.2.2012. http://www.tietosuoja.fi/uploads/qmdum.pdf

Tietosuojavaltuutetun toimisto. 2010e. Malli henkilötietojen käsittelyn/henkilörekisterin rekisteritoimintojen analysoimiseksi. Viitattu: 14.2.2012. http://www.tietosuoja.fi/uploads/uoku8dvlt.pdf

Tietosuojavaltuutetun toimisto. 2011a. Tietoa rekisterinpitäjälle. Viitattu: 20.2.2012. http://www.tietosuoja.fi/1698.htm

Tietosuojavaltuutetun toimisto. 2011b. Kansainväliset normit ja ohjeet. Viitattu: 28.2.2012. http://www.tietosuoja.fi/2000.htm

Tietosuojavaltuutetun toimisto. 2012a. Sanasto. Viitattu: 16.2.2012. http://www.tietosuoja.fi/27247.htm

Tietosuojavaltuutetun toimisto. 2012.b Läpinäkyvyys on haaste yritysten kanta-asiakasjärjestelmille. Lehdistötiedote. Viitattu 14.2.2012. http://www.tietosuoja.fi/57435.htm

Tietosuojavaltuutetun toimisto. 2012d. Yleisohjaus ja sidosryhmäyhteistyö. Viitattu: 20.3.2012. http://www.tietosuoja.fi/11202.htm

Tietosuojavaltuutetun toimisto. 2012e. Lait. Viitattu: 26.3.2012. http://www.tietosuoja.fi/1556.htm

Tietosuojavaltuutetun toimisto. 2012f. Käytännesääntötyö. Viitattu: 26.3.2012. http://www.tietosuoja.fi/11203.htm

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. 9., uudistettu painos. Helsinki: Tammi.

Valtionhallinnon tietoturvallisuuden johtoryhmä. 2004. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. Helsinki: Edita.

Verizon. 2012. 2012 Data Breach Investigations Report. Viitattu: 2.4.2012. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Julkaisemattomat lähteet

1. Pöytäkirja. 2012. Asiantuntijahaastattelu 23.2.2012. Ryhmähaastattelu.

2. Pöytäkirja. 2012. Asiantuntijahaastattelu 6.3.2012. Yksilöhaastattelu.

3. Pöytäkirja. 2012. Asiantuntijahaastattelu 7.3.2012. Parihaastattelu.

4. Pöytäkirja. 2012. Asiantuntijahaastattelu 9.3.2012. Ryhmähaastattelu.

5. Pöytäkirja. 2012. Asiantuntijahaastattelu 9.3.2012. Ryhmähaastattelu.

6. Pöytäkirja. 2012. Asiantuntijahaastattelu 12.3.2012. Parihaastattelu.

7. Pöytäkirja. 2012. Asiantuntijahaastattelu 20.3.2012. Yksilöhaastattelu.

8. Pöytäkirja. 2012. Asiantuntijahaastattelu 20.3.2012. Yksilöhaastattelu.

9. Pöytäkirja. 2012. Asiantuntijahaastattelu 21.3.2012. Yksilöhaastattelu.

10. Pöytäkirja. 2012. Asiantuntijahaastattelu 26.3.2012. Ryhmähaastattelu.

11. Pöytäkirja. 2012. Asiantuntijahaastattelu 27.3.2012. Yksilöhaastattelu.

12. Pöytäkirja. 2012. Asiantuntijahaastattelu 28.3.2012. Yksilöhaastattelu.

13. Pöytäkirja. 2012. Asiantuntijahaastattelu 29.3.2012. Yksilöhaastattelu.

14. Pöytäkirja. 2012. Asiantuntijahaastattelu 2.4.2012. Parihaastattelu.

15. Pöytäkirja. 2012. Asiantuntijahaastattelu 2.4.2012. Yksilöhaastattelu.

16. Pöytäkirja. 2012. Asiantuntijahaastattelu 3.4.2012. Parihaastattelu.

Koskinen, M. 2009. SOK Riskienhallinnan esittely. SOK:n Riskienhallintayksikön päällikön esitys.

Tietosuojavaltuutetun toimisto. 2012c. Yritysten kanta-asiakasjärjestelmien tietosuoja. Muistio.

Tupala, V. 2010. Tietoturvallisuuden kehitysryhmän tehtävät ja kokoonpano. SOK:n tietoturvallisuuspäällikön ohje.

Tupala, V. 2011. Tietoturvallisuusvastaavan toimenkuvasuositus. SOK:n tietoturvallisuuspäällikön ohje.

Tupala, V. 2012. S-ryhmän tietosuojan toimintamallin kehittäminen - projektisuunnitelma. SOK:n tietoturvallisuuspäällikön esitys.

Liite 1 - Lausunto opinnäytetyöstä

LAUSUNTO JARKKO KAROSEN OPINNÄYTETYÖSTÄ

Jarkko Karosen opinnäytetyö (Luonnosehdotus tietosuojan organisoinnista S-ryhmässä) vastaa sisällöltään hyvin tälle opinnäytetyölle asetettuihin tavoitteisiin.

Opinnäytetyö kuvaa konkreettisesti keskeisiä tietosuojan järjestämiseen liittyviä lainsäädännön nykyisiä ja tulevia vaatimuksia sekä ehdottaa konkreettisia toimintamalleja vaatimusten toteuttamiseksi.

Opinnäytetyön tuloksia ja keskeisiä havaintoja hyödynnetään S-ryhmän tietosuojan kehittämisessä ja ohjausmallin määrittämisessä.

Helsingissä, 10. päivänä huhtikuuta 2012.

SUOMEN OSUUSKAUPPOJEN KESKUSKUNTA
Hallintopalvelut ja riskienhallinta

Vesa Tupala
Tietoturvallisuuspäällikkö

Osoite	Postiosoite	Puhelin	Faksi	Internet	Y-tunnus	Kotipaikka
Fleminginkatu 34 00510 HELSINKI	PL 1 00088 S-RYHMÄ	010 768 011	010 768 2390	www.s-kanava.fi	0116323-1	Helsinki