KOSKA YKSITYISYYTESI ON MEILLE TÄRKEÄ

Tietosuoja ja tietoturva yrityksissä

Heimonen Kirsi

Opinnäytetyö
Joulukuu 2013

Liiketalouden koulutusohjelma
Yhteiskuntatieteiden, hallinnon ja kaupan ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) HEIMONEN, Kirsi	Julkaisun laji Opinnäytetyö	Päivämäärä 2.12.2013
	Sivumäärä 99	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty (X)

Työn nimi
KOSKA YKSITYISYYTESI ON MEILLE TÄRKEÄ
Tietosuoja ja tietoturva jyväskyläläisissä yrityksissä

Koulutusohjelma

Liiketalouden koulutusohjelma

Työn ohjaaja(t)

VANHANEN, Pekka ja HAUTAMÄKI, Jari

Toimeksiantaja(t)

Jyväskylä Security Technology (JYVSECTEC)

Tiivistelmä
Tietojen käsittelyn siirtyminen sähköiseen ympäristöön tuo yksilön tietosuojalle uudenlaisia ja entistä vaarallisempia uhkia. Suojautuminen niitä vastaan vaatii jatkuvaa kehitystyötä, jossa tutkimuksen toimeksiantaja JYVSECTEC on mukana. Tutkimuksen tavoitteena oli saada viitteitä siitä, voidaanko tietoturvakoulutuksissa motivoida tietoturvallisuuteen korostamalla lainsäädännön tietojen suojaamisvelvoitteita. Tutkimus rajattiin koskemaan asiakkaiden tietosuojaa ja heidän tietojensa suojaamista. Tutkimuksen avulla luotiin myös yleiskuva jyväskyläläisten toimijoiden tietosuojatietämyksen tasosta sekä tietoturvatoimien kattavuudesta.

Tutkimus toteutettiin kvantitatiivisella tutkimusotteella. Tutkimusmenetelmänä käytettiin kyselytutkimusta, ja kysely toteutettiin verkossa vastattavalla kyselylomakkeella. Tutkimukseen valittiin satunnaisotannalla tuhat jyväskyläläistä toimijaa, joille lähetettiin kutsu tutkimukseen. Kutsu ei tavoittanut kaikkia, ja netto-otos oli 732 tutkittavaa. Tutkimuksen kannalta oleellisia vastauksia kertyi 59 (8 %) netto- otoksesta.

Tutkimuksen aihe oli hyvin mielenkiintoinen ja erittäin ajankohtain. Tutkimuksesta kävi ilmi, että jyväskyläläiset toimijat eivät tunne lainsäädännön tietojen suojaamisvelvoitteita kovin hyvin, mutta pyrkivät silti huolehtimaan tietoturvasta. Lainsäädännön velvoitteet ovat toimijoille pitkälti itsestään selviä asioita. Riippumatta lain vaatimuksista asiakkaiden yksityisyyden suojaaminen on heille joka tapauksessa tärkeää. Tutkimustulosten avulla voidaan löytää toimijoiden heikoimmat osa-alueet tietoturva- ja tietosuojaosaamisessa, jolloin koulutuksessa osataan painottaa enemmän näitä alueita. Tutkimustulosten pohjalta tuli esille joitakin mielenkiintoisia kysymyksiä, joita voisi selvittää jatkotutkimuksin. Millaiset mahdollisuudet pienillä yrityksillä on kehittää tietoturva- ja tietosuojaosaamistaan?

Avainsanat (asiasanat)

tietosuoja, tietoturva, tietosuojalainsäädäntö

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
HEIMONEN, Kirsi	Bachelor´s Thesis	2.12.2013
	Pages 99	Language Finnish
		Permission for web publication (X)

Title
BECAUSE YOUR PRIVACY IS IMPORTANT FOR US
Privacy protection and information security at enterprises in the City of Jyväskylä

Degree Programme

Business Administration

Tutor(s)

VANHANEN, Pekka and HAUTAMÄKI, Jari

Assigned by

Jyväskylä Security Technology (JYVSECTEC)

Abstract
The transition of data processing to the electronic environment brings new and more dangerous threats to an individual's data privacy. Protection against them requires a continuous development, which JYVSECTEC, the client of this thesis, participates in. The aim of research was to explore if it is possible to motivate employees to observe information security through training by accentuating the obligation for protecting data in the existing legislation. The study was limited to the customers' confidentiality and the protection of their data. The study was also used to create a picture of the extent of the local professionals' awareness of information security and of the coverage of the measures taken for information security.

Quantitative methods were used in the survey, which was conducted by means of an online questionnaire. An invitation to participate in the survey was sent to 1000 randomly selected professionals. The invitation reached 732 addressees, out of whom 59 persons (8 percent) returned the questionnaire.

The topic of the research was very interesting and highly relevant. The investigation revealed that the professionals in Jyväskylä do not have a good awareness of the protection obligation of the current legislation but they strive to ensure information security. The clearly understand the legal obligations. Regardless of the legal requirements, protecting an individual's confidentiality is important for them. The results can be used to find the professionals' weakest sectors in information security and in the awareness of information security, which can be upgraded through training. Other questions needing further study were: What kinds of facilities do small enterprises have in order to develop their abilities in the fields of information security and confidentiality? Are the measures of enterprises for the protection of data privacy too modest or exaggerated in relation to the level of protection required by the data in question?

Keywords

privacy, security

Miscellaneous

Sisältö

1 Johdanto 5

2 Tietosuoja ja tietoturvallisuus 7

2.1 Tietosuoja ja yksityisyys 8

2.2 Henkilötieto, arkaluontoiset henkilötiedot ja henkilötietojen käsittely 9

2.3 Henkilörekisteri, rekisterinpitäjä ja sivullinen 10

2.4 Tietoturvallisuus 11

3 Tietosuojalainsäädännön vaatimukset tietoturvalle 16

3.1 Henkilötietolaki 17

3.2 Laki viranomaisten toiminnan julkisuudesta 23

3.3 Laki yksityisyyden suojasta työelämässä 27

3.4 Sähköisen viestinnän tietosuojalaki 29

3.5 Tietosuojalainsäädännön tulevaisuus 30

4 Tietosuoja ja tietoturva yrityksissä 34

4.1 Tietosuojan merkitys yrityksille 34

4.2 Yritysten yleisimmät tietosuoja- ja tietoturvauhat 36

5 Tutkimuksen lähtökohdat ja toteutus 40

5.1 Tutkimusmenetelmät 42

5.2 Tutkimusaineiston keruu ja analysointi 42

5.3 Tutkimuksen luotettavuuden arviointi 48

6 Tulokset 51

6.1 Vastaajien taustatiedot 52

6.2 Lainsäädännön tunteminen organisaatioissa 53

6.3 Toimijoiden tietoturvatoimet 68

6.4 Lainsäädännön vaikutus toimipaikan tietoturvatoteutukseen 74

7 Pohdinta 77

Lähteet 84

Liitteet 89

Liite 1. Kyselyn kysymykset 89

Liite 2. Saatekirje 97

Liite 3. Muistutuskirje 99

Kuviot

Kuvio 1. Tietosuojan ja tietoturvan painopisteet 8

Kuvio 2. Tietoturvan toiminnalliset osa-alueet 13

Kuvio 3. Perusjoukon ja aineiston jakautuminen 46

Kuvio 4. Tietotasot tietoturvatoimien laajuuden ja tehokkuuden arvioinnista 56

Kuvio 5. Tietotasot arkaluontoisten tietojen suojaamisessa 58

Kuvio 6. Tietotasot henkilötietojen ulkoistamisen vastuista 60

Kuvio 7. Tietotasot rekisterinpitäjän vastuista 62

Kuvio 8. Tietotasot henkilötietojen tuhoutumisesta, muuttumisesta ja katoamisesta 64

Kuvio 9. Tietotasot keskiarvolukuina kokoluokittain 66

Kuvio 10. Tietoturvatoimien valintaan vaikuttavat asiat 76

Taulukot

Taulukko 1. Vastaajat toimijan koon mukaan 53

Taulukko 2. Tietoturvatoimien laajuuden ja tehokkuuden arvioimiseen vaikuttavat seikat 55

Taulukko 3. Arkaluontoisten tietojen suojaaminen 57

Taulukko 4. Vastuut tietojen käsittelyn lainmukaisuudesta ja tietojen suojaamisesta henkilötietojen käsittelyn ulkoistamistilanteessa 59

Taulukko 5. Rekisterinpitäjän vastuu henkilötiedoista eri tilanteissa 61

Taulukko 6. Tietosuojatiedon tasot 66

Taulukko 7. Tietosuoja- ja tietoturvakoulutus sekä menettelytavat 67

Taulukko 8. Salasanojen ja käyttöoikeuksien käyttäminen tietotasoittain 68

Taulukko 9. Henkilötietoja sisältävien koneiden ja järjestelmien suojaaminen 69

Taulukko 10. Arkaluontoisia tietoja sisältävien rekisterien esiintyvyys eri tietotasojen joukossa 70

Taulukko 11. Kulun- ja kameravalvonta 71

Taulukko 12. Henkilörekisterin tallennuspaikka 72

Taulukko 13. Verkon ja koneiden käytöstä annetut ohjeet 72

Taulukko 14. Tietoaineiston luokittelu eri tietotasoilla 73

Taulukko 15. Henkilötietoja sisältävän rekisterin varmuuskopiointi 74

1 Johdanto

Tietotekniikan ja -verkkojen käyttö yleistyy ja monipuolistuu liiketoiminnassa jatkuvasti, ja verkossa käsiteltävän tiedon määrä kasvaa koko ajan. Toimijat verkottuvat kansainvälisesti ja tietoa vaihdetaan yli maantieteellisten rajojen. Tietojärjestelmiä ja -verkkoja hyväksikäyttäen tallennetaan ja siirretään muun muassa yrityssalaisuuksia, suunnitelmia ja viestejä. Lähes kaikki toimijat tallentavat ja käsittelevät myös asiakkaista kerättyä, joskus jopa arkaluontoisia tietoja.

Tiedon sähköistyessä yleistyvät yrityksiin kohdistuvat tietoturvahyökkäykset. Niiden takana ovat entistä ammattimaisemmat toimijat ja jopa valtiot. Hyökkäykset ovat yrityksille ja yksityisille henkilöille aiempaa vaarallisempia. Tietosuojan ja tietoturvallisuuden laiminlyönti uhkaa sekä yrityksen toimintaa että asiakkaiden ja henkilöstön yksityisyyden suojaa. Se saattaa johtaa myös merkittäviin kustannuksiin. Pahimmillaan hyökkäyksen kohteeksi joutunut yritys ei enää pysty jatkamaan liiketoimintaansa. (Suomen kyberturvallisuusstrategia ja taustamuistio 2013, 1.)

Suojautuminen näitä uhkia vastaan edellyttää paitsi lainsäädännön suojaamisvelvoitteiden tuntemista, myös jatkuvaa tietoturvallisuuden kehittämistä. Jyväskylä Security Technology (JYVSECTEC) on mukana tässä tietoturvallisuuden kehittämistyössä ja on tämän tutkimuksen toimeksiantaja. JYVSECTEC on ammattikorkeakoulun ICT-tulosalueen syyskuussa 2011 käynnistynyt Jyväskylä Security Technology -hanke eli JYVSECTEC. Hanke ylläpitää ja kehittää kyberturvallisuuden kehitys-, testaus- ja koulutusympäristöä, jonka avulla tuetaan yritysten kasvua, edistetään yritysten verkostoitumista sekä pk-yritysten pääsyä kansainvälisille markkinoille. Hanke jatkuu vuoden 2013 loppuun. Hankkeen myötä edellytykset turvallisuus- ja ICT-alan yrityksissä tapahtuvalle tutkimus- ja tuotekehitystoiminnalle ja sen laajenemiselle vahvistuvat merkittävästi. Myös yritysten turvallisuuden tietämys ja riskienhallinta lisääntyvät sekä turvallisuuden ylläpito paranee. Hankkeen tavoitteeksi on asetettu JYVSECTECin sijoittuminen Suomen johtavien kyberturvallisuuden kehittämis- ja koulutuskeskuksi-

en joukkoon. Tavoitteena on myös saada luotua Keski-Suomeen turvallisuusalan yritysten ja toimijoiden yhteistyöverkosto. (JYVCESTEC-projektin verkkosivut.)

Tutkimusongelma ja rajaus

Tietojen suojaamisen ja tietoturvallisuuden perusta on lainsäädännössä, ja ainakin tietoturvasta vastaavien tulisi olla tietoisia lainsäädännön vaatimuksista. Lain velvoitteista ja tietoturvallisuuden tärkeydestä huolimatta tietoturvasta huolehtiminen nähdään usein vain kustannuksina, joista voidaan säästää. Monet tutkijat ovat huomanneet tämän välinpitämättömän asenteen tietoturvaa kohtaan. He ovat pyrkineet tutkimuksissaan löytämään keinoja tietoturvatietoisuuden parantamiseksi. Muun muassa oululaisessa Kari Nykäsen (2011, 13–14) tekemässä tutkimuksessa on tutkittu tietoturvakoulutuksen vaikutusta yksilön tapoihin, käyttäytymiseen ja vastuunottamiseen omasta toiminnasta.

Tutkimusten mukaan laiminlyönnit tietoturvallisuudesta huolehtimisessa voivat ainakin osittain johtua yritysten välinpitämättömyydestä ja asenteista. Taustalla voi olla myös tietämättömyyttä lain tuomista velvoitteista, kuten Suomen tietoturvavaltuutetun kesällä 2012 tekemästä tarkastuksesta voidaan päätellä. Tietosuojavaltuutettu tarkasti 74 laajan tietomurtoaallon kohteiksi joutunutta yritystä, joista suurin osa ei edes tiennyt, miten laki velvoittaa heitä suojaamaan asiakkaiden henkilötietoja. (Tietosuojavaltuutettu vaatii yrityksiä panostamaan tietoturvaan 2012.)

Yritysten tietosuojaa on tutkittu niin asiakkaiden kuin työntekijöidenkin näkökulmasta. Tutkimattomampi alue on tietosuojalainsäädännön velvoitteiden tuntemisen vaikutus tietoturvasta huolehtimiseen. Tässä opinnäytetyössä tarkastellaan tietosuojalainsäädännön tietoturvallisuudelle asettamia vaatimuksia. Työssä pyritään löytämään tietosuojalainsäädännön kirjavasta joukosta ne merkittävimmät säädökset, joilla on vaikutusta yrityksen tai organisaation tietoturvaan. Aiheen kiinnostavuutta lisää mahdollisuus syventää tietämystä tietoturvallisuudesta sekä tietosuojalainsäädännön vaatimuksista tietojen suojaamiseksi. Lisäksi aihe on hyvin ajankohtainen, sillä tietosuoja puhuttaa kansaa tihentyvään tahtiin ilmitulevien tietovuoto- ja urkin-

taskandaalien vuoksi. Aihe on myös alueellisesti ajankohtainen. Valittiinhan Jyväskylä kesällä 2013 valtakunnalliseksi kyberturvallisuuden kehittämiskaupungiksi.

Tutkimuksen tarkoituksena on selvittää jyväskyläläisten toimijoiden tietämystä tietosuojalainsäädännön tietojen suojaamisvelvoitteiden osalta. Lisäksi on tarkoitus saada selville, onko näiden suojaamisvelvoitteiden tuntemisella ja tietoturvasta huolehtimisella yhteys. Tutkimuksen tavoitteena on saada käsitys siitä, miten tärkeää tietoturvakoulutuksessa on painottaa lainsäädännöstä lähteviä vaatimuksia tietoturvalle. Samalla voidaan myös arvioida, pystytäänkö organisaatioita motivoimaan tietoturvahalukkuuteen laintuntemusta lisäämällä. Tutkimuksessa haetaan vastauksia seuraaviin kysymyksiin:

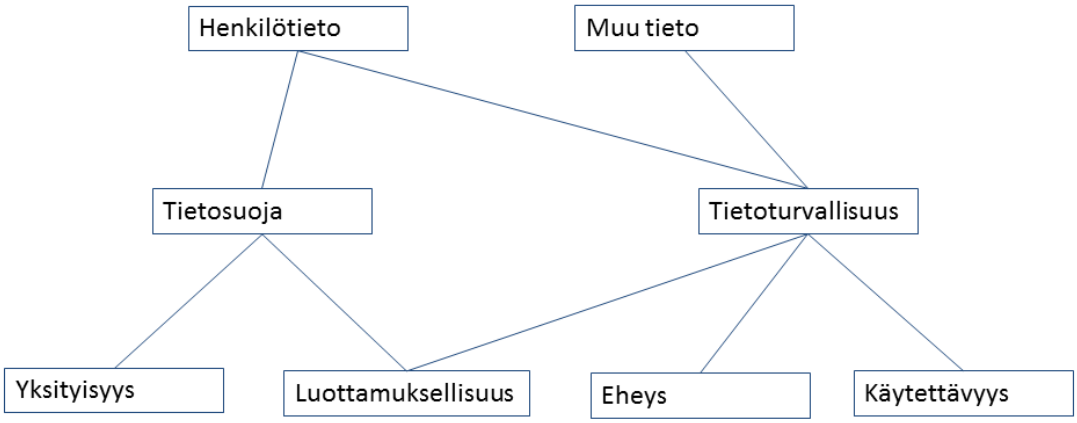
- Miten hyvin organisaatioissa tunnetaan henkilöasiakkaiden kannalta merkittävien tietosuojasäännösten tietojen suojaamisvelvoitteet syksyllä 2013?
- Vaikuttaako tietojen suojaamisvelvoitteiden tunteminen halukkuuteen huolehtia tietoturvasta?

Tutkimuksen ulkopuolelle rajataan toimialakohtaiset tietosuojalain säädökset ja niiden tunteminen ja mahdolliset vaikutukset tietoturvalle. Tietosuojaan vaikuttavia erityislakeja on laadittu jopa satoja, ja esimerkiksi terveys- ja sosiaalialan tietosuojalainsäädäntö useine erityislakeineen on varsin laaja alue ja voisi olla tutkimuksen kohde jo yksinään. Aiheesta onkin tehty useita tutkimuksia jo aiemmin. Tutkimuksen ulkopuolelle jäävät myös organisaatioiden henkilöstöä koskeva tietojen suoja. Myös henkilöstön tottumuksesta johtuvat toimintatavat ja käyttäytymismallit jäävät tutkimuksen ulkopuolelle. Myös näitä alueita on tutkittu aiemmin.

2 Tietosuoja ja tietoturvallisuus

Tietosuoja ja tietoturva ovat kansan keskuudessa usein ymmärretty samaksi asiaksi. Liittyväthän ne hyvin läheisesti toisiinsa, mutta ovat kuitenkin kaksi eri asiaa. Tietosuojan painopiste on yksityisyyden suojaamisessa ja henkilötietojen käsittelyn toi-

mintatavoissa, kun taas tietoturvalla pyritään varmistamaan tietojen luottamuksellisuus, eheys ja käytettävyys (ks. kuvio 1). Tietosuojan toteutuminen tarvitsee tietoturvaa. Henkilötietoihin tai niiden käsittelyssä käytettäviin tietojärjestelmiin kohdistuvat tietoturvauhat ovat myös uhka tietosuojalle. (Salminen 2009, 81.) Tässä luvussa selvitetään tietosuojaa sekä siihen läheisesti liittyviä käsitteitä sekä tietoturvaa ja siihen liittyviä tärkeimpiä käsitteitä tietosuojan näkökulmasta.



Kuvio 1. Tietosuojan ja tietoturvan painopisteet (Valtionhallinnon tietoturvakäsitteistö 2004, 13)

2.1 Tietosuoja ja yksityisyys

Tietosuoja on yksityisyyttä suojaava perusoikeus. Suomen perustuslain (11.6.1999/731) 10.1 § takaa jokaiselle oikeuden omaan yksityisyyteensä. Tästä perusoikeudesta ei pääsääntöisesti voida poiketa. Yksityisyyden suojaa voidaan kuitenkin rajoittaa lain säännöksin tietyissä tilanteissa, mutta ei asetuksilla eikä määräyksillä. Tietosuoja ei sinällään suojaa tietoja, vaan suoja kohdistuu yksilöön. (Saarenpää 2011, 325.) Yksityiselämän suojaamisen lisäksi lain 10.1 §:ssä annetaan kehotus säätää henkilötietojen suojasta tarkemmin erillisellä lailla. Perinteisen käsityksen mukaan tietosuoja on juuri henkilötietojen käsittelyä koskevan lainsäädännön huomioon

ottamista. (Andreasson, Koivisto & Ylipartanen 2013, 14.) Käytännössä tämä tarkoittaa sitä, että estetään asiattomien pääsy tietoihin, tietojen luovuttaminen ja siirtäminen asiattomalle taholle, tietojen tarkoitukseton hävittäminen ja muuttaminen sekä kaikenlainen tietojen laiton käsittely muun muassa asianmukaisilla tietoturvatoimenpiteillä (Jabe 2011, 44).

Tietosuoja turvaa yksilön yksityisyyden, jota ei ole laissa täsmällisesti määritelty eikä se Saarenpään mukaan ole edes tarpeellista. Liian täsmällinen määritelmä jäisi teknologian kehityksen jalkoihin, ja määritelmää sekä sitä koskevaa sääntelyä jouduttaisiin aika ajoin uusimaan. Säädännön uusiminen on melko hidasta, jolloin voitaisiin joutua epäoikeudenmukaisiin tilanteisiin. (Saarenpää 2011, 318.) Yksityisyyden kokemus on myös jokaisella yksilöllä erilainen, siihen vaikuttavat muun muassa aiemmat kokemukset, elämäntilanne ja tiedot. Yksityisyys voidaan käsittää jokaisen oikeutena ja mahdollisuutena suojautua ulkopuoliselta puuttumiselta. Sen lisäksi siihen kuuluu oikeus määrätä itseään koskevista henkilötietojen käsittelystä eli niin sanottu tiedollinen itsemääräämisoikeus. (Salminen 2009, 16.)

Tietotekniikan kehittyminen on tuonut tietosuojalle uusia haasteita helpon, nopean ja huomaamattoman henkilötietojen keruun ja analysoinnin vuoksi. Tietoja varastoidaan suuriin sähköisiin tietovarastoihin eikä tiedon omistajakaan aina tiedä, missä tieto fyysisesti sijaitsee. Tämän kehityksen myötä tietojen vääriin käsiin joutumisen ja väärinkäytösten riski on kasvanut. Toisaalta sosiaalisen median käytön lisääntyminen on tehnyt yksityisyydestä yhä julkisempaa. Silti yksityisyyden merkitys yhteiskunnassa on kasvanut yksilön itsemääräämisoikeuden vahvistuessa. (Saarenpää 2011, 318.)

2.2 Henkilötieto, arkaluontoiset henkilötiedot ja henkilötietojen käsittely

Henkilötiedon määritelmällä on merkitystä erityisesti silloin, kun mietitään, täytyykö tietojen käsittelyssä soveltaa tietosuojasäännöksiä (Täsmennystä henkilötiedon määritelmään 2007). Henkilötietolain (22.4.1999/523) määritelmän mukaan henkilötieto on mikä tahansa luonnollista henkilöä tai hänen elinolojaan koskeva tieto, josta

henkilö tai hänen perheenjäsenensä tai yhteisessä taloudessa asuva henkilö voidaan tunnistaa (L 22.4.1999/523, 3.1 §). Henkilötiedoksi voidaan nimen ja henkilötunnuksen lisäksi katsoa muun muassa verkkoviestintälaitteen IP-osoite, auton rekisteritunnus, tietokoneen evästetiedosto, valokuva, paikkatieto tai sähköpostiosoite, jos henkilö on kohtuullisella vaivalla tunnistettavissa tiedon perusteella (Vanto 2011, 22–23).

Henkilötieto on arkaluontoinen, jos se kuvaa (L 22.4.1999/523, 11 §):

- rotua tai etnistä alkuperää
- henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista
- rikollista tekoa, rangaistusta tai muuta rikoksen 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 etuuksia käsitteleviä tietoja.

Arkaluontoisten henkilötietojen käsittely on pääsääntöisesti kiellettyä, ja niiden suojaamiseen täytyy kiinnittää erityistä huomiota.

Henkilötietojen käsittelyksi katsotaan henkilötietojen kerääminen, tallentaminen, järjestäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen, tuhoaminen ja henkilötietoihin kohdistuvat toimenpiteet. Käytännössä kaikki yritystoiminnassa tapahtuva henkilötietoihin kohdistuva toiminta on henkilötietojen käsittelyä. (L 22.4.1999/523, 3 § 2 kohta.)

2.3 Henkilörekisteri, rekisterinpitäjä ja sivullinen

Henkilörekisterillä tarkoitetaan sellaista henkilötietojen joukkoa, jotka käyttötarkoituksensa vuoksi kuuluvat yhteen ja joista yhden henkilön tiedot löytyvät vaivatta. Tiedot voivat olla osittain tai kokonaan automaattisen tietojenkäsittelyn avulla käsi-

teltäviä. (L 22.4.1999/523, 3.3 §.) Tietojen keräämistavalla tai tallennuspaikalla ei ole merkitystä, vaan oleellista on tietojen sama käyttöyhteys. Jos henkilötietoja sisältävä rekisteri täyttää lain tarkoittaman henkilötietorekisterin määritelmän, tulevat sen osalta kaikki henkilötietolain rekisterin pitäjälle säädetyt velvoitteet noudatettaviksi. (Vanto 2011, 29.)

Henkilötietolain (22.4.1999/523) 3 § 4 kohdan mukaan rekisterinpitäjänä pidetään yhtä tai useampaa henkilöä sekä yhteisöä, säätiötä tai laitosta, jonka käyttöön henkilörekisteri on perustettu. Sen lisäksi sillä on määräysvalta rekisterin käyttöön. Toimija voi olla rekisterinpitäjä myös lain edellyttämänä. Rekisterinpitäjänä voi olla joko luonnollinen tai oikeushenkilö. Määritelmässä on merkityksellistä se, että rekisterinpitäjällä on oikeus määrätä rekisterissä olevien henkilötietojen käyttötarkoituksesta ja käsittelystä henkilötietolain mukaisissa rajoissa. Ilman tällaista määräysvaltaa oleva henkilötietojen käsittelijä katsotaan sivulliseksi. Rekisterinpitäjän ja sivullisen välinen ero on tärkeää ymmärtää erityisesti vastuiden ja velvollisuuksien määrittelemiseksi. (Vanto 2011, 30–31.)

Henkilötietolain (22.4.1999/523) 3 § 6 kohta määrittelee sivulliseksi sellaisen henkilön, yhteisön, laitoksen tai säätiön, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tällainen laissa määritelty sivullinen voi olla työnantajan palveluksessa oleva työntekijä, joka käsittelee henkilötietoja tai esimerkiksi ulkoistetun toiminnon palveluntarjoaja (Vanto 2011, 32).

2.4 Tietoturvallisuus

Tietoturvallisuudelle löytyy useita toisistaan hieman poikkeavia määritelmiä, mutta kaikissa on sama perusajatus: tietojen turvaaminen. Sähköisen viestinnän tietosuojalain (16.6.2004/516) määritelmän mukaan tietoturvalla tarkoitetaan sellaisia hallinnollisia ja teknisiä toimia, joilla varmistetaan, että tietoihin pääsevät vain ne, joilla on niihin oikeus ja silloin kun he tietoja tarvitsevat. Määritelmän mukaan tietoturvallisuuteen kuuluu myös se, etteivät tietoja voi muuttaa muut kuin siihen oikeutetut henkilöt. Toisin sanoen tietosuojan näkökulmasta tietoturvallisuudella tarkoitetaan

kaikkia niitä hallinnollisia ja teknisiä keinoja, joilla pyritään varmistamaan henkilötietojen käytettävyys, eheys ja luottamuksellisuus sekä turvaamaan ja suojaamaan rekisteröidyn yksityisyys. (Andreasson ym. 2013, 14.) Nämä mainitut tietoturvallisuuden peruspilarit eivät varsinaisesti huomioi tiedon tuottajaa tai omistajaa. Siitä syystä tietoturvallisuuden käsitettä on usein laajennettu käsittämään vielä tiedon kiistämättömyys ja pääsynvalvonta (Hakala, Vainio & Vuorinen 2006, 4–5).

Luottamuksellisuudella tarkoitetaan sitä, että tietoihin, järjestelmiin ja palveluihin pääsevät vain ne henkilöt, joilla on niihin oikeus. Luottamuksellisuuteen kuuluu myös se, ettei tietoja paljasteta sivulliselle eikä niitä muutoinkaan saateta sivullisen tietoon. (Korhonen 2010, 512.) Luottamuksellisuuteen voidaan pyrkiä muun muassa käyttämällä järjestelmiin sisään kirjautumisessa salasanoja sekä etenkin arkaluontoisten tietojen suojaamisella salasanoin. (Hakala ym. 2006, 4.)

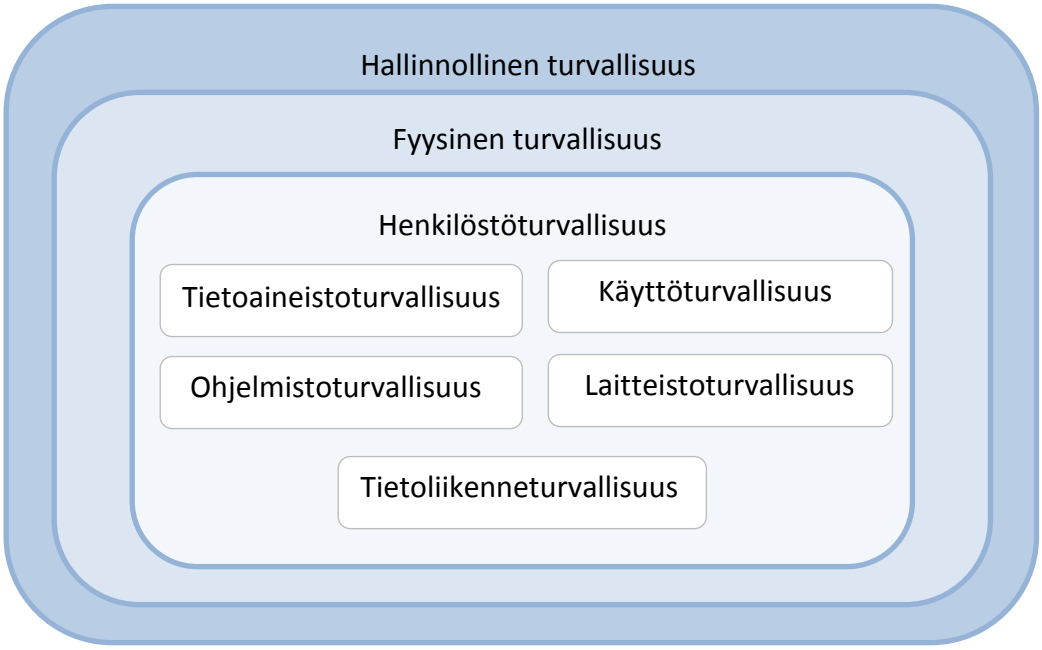
Eheydellä tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat muuttumattomia ja tallella, eikä inhimillinen virhe, laitteisto- tai ohjelmistovika tai luonnontapahtuma vaikuta tietojen muuttumattomuuteen. Käytettävyys tarkoittaa sitä, että ne henkilöt, joilla on oikeus päästä käsiksi tietoihin, järjestelmiin ja palveluihin, voivat hyödyntää niitä esteettä ja häiriöttä juuri silloin, kun heillä on siihen tarve. (Korhonen 2010, 512.)

Kiistämättömyydellä tarkoitetaan sitä, että järjestelmää tai tietoa käyttävän henkilöllisyys pystytään vielä jälkikäteenkin luotettavasti toteamaan. Tämä on tärkeää, jotta tiedon tuottaja voidaan varmistaa sekä mahdollinen tiedon tai järjestelmän luvaton käyttö selvittää. (Hakala ym. 2006, 5.)

Pääsynvalvonta käsittää kaikki ne menetelmät, joilla tietojenkäsittelyjärjestelmän käyttöä voidaan rajoittaa niin organisaation oman henkilökunnan kuin sivullisenkin luvattomalta käytöltä. Luvaton käyttö heikentää järjestelmää rasittamalla käytettävyyttä sekä vaarantaa luottamuksellisuuden ja eheyden. (Hakala ym. 2006, 5–6.)

Tietoturvan toiminnalliset osa-alueet

Tietoturvallisuuden käsitettä voidaan selkeyttää jakamalla se toiminnallisiin osiin. Sähköisen viestinnän tietosuojalaki jakaa hallinnollisen ja teknisen tietoturvan koskemaan toiminnan turvallisuutta, tietoliikenneturvallisuutta, laitteisto- ja ohjelmistoturvallisuutta sekä tietoaineistoturvallisuutta (L 16.6.2004/516, 19.1 §). Suomessa tietoturvan toiminnallisia osia on kuitenkin perinteisen näkemyksen mukaan kahdeksan. Ne ovat toimintasisällöiltään samansuuntaiset sähköisen viestinnän tietosuojalain kanssa, mutta ottavat paremmin huomioon muun muassa fyysiset ja henkilöstöstä johtuvat tietoturvauhat. Perinteisen jaottelun hallinnollinen ja fyysinen turvallisuus sekä henkilöstöturvallisuus ovat organisatorisina keinoina muun tietoturvatoiminnan perustana. Vasta kun nämä osa-alueet ovat hoidettu asianmukaisesti, voidaan muilla teknisin keinoin toteutettavilla osa-alueilla toimia järkevästi. (Kuvio 2.) (Rosendahl 2003.)



Kuvio 2. Tietoturvan toiminnalliset osa-alueet (Rosendahl 2003)

Hallinnollisen turvallisuuden piiriin kuuluvat tietoturvajohtaminen ja tietoturvan kehittämistoimet. Lainsäädännön vaikutusten arviointi on erityisen tärkeässä asemassa, sillä sen pohjalta luodaan organisaation tietoturvapolitiikka menettelytapoineen ja tietoturvaohjeineen. Henkilöstön sitouttaminen tietoturvatoimiin on yksi hallinnollisen turvallisuuden tehtävistä. (Hakala ym. 2006, 10–11.)

Fyysisen turvallisuuden aluetta on tietojärjestelmien ja laitteitten sekä sen myötä tietojen suojaaminen erilaisilta fyysisiltä uhilta. Muun muassa ovilla, lukoilla ja muilla rakennuksen turvallisuusratkaisuilla voidaan ehkäistä esimerkiksi tulipalojen, veden tai ilkivallan aiheuttamia vahinkoja. Samoilla keinoilla voidaan myös estää asiattomien henkilöiden pääsy tietojen luo. (Hakala ym. 2006, 11.)

Henkilöstöturvallisuus on henkilöstöön liittyvien tietoturvauhkien hallintaa. Se sisältää lähinnä henkilöstön luotettavuuteen, motivointiin, valvontaan ja liikkuvuuteen liittyvät asiat. Henkilöstöturvallisuus alkaa jo rekrytointivaiheessa työnhakijan taustojen tarkistamisella ja jatkuu työsuhteen päättymiseen asti. Henkilöstön kouluttaminen tietosuojaan ja tietoturvaan sekä uhkatilainteiden varalta on osa henkilöstöturvallisuutta. Henkilöstöturvallisuus on tärkeä osa myös henkilöstön eroamis- tai erottamistilanteissa, jolloin on huolehdittava, ettei salassa pidettäviä tietoja lähde työntekijän mukana. Henkilöstöturvallisuus on tärkeä tietoturvallisuuden osa-alue muun muassa siksi, että henkilöstö on usein tietoturvan suurin riski. (Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 57.)

Tietoaineistoturvallisuudella pyritään varmistamaan eri tallennusmuodoissa olevan aineiston tietosisältö. Se käsittää niin paperisen kuin kaiken sähköisessä tai optisessa tallennusmuodossakin olevan tiedon. Tietoaineistoturvallisuuden toimintasäännöillä varmistetaan tiedon eheys koko tiedon elinkaaren ajan, aina sen synnystä tuhoamiseen asti. Käytännössä tämä tarkoittaa muun muassa sitä, että tietoaineisto luokitellaan esimerkiksi julkiseksi ja salaiseksi ja että tietoja käsitellään sen mukaisesti hyvää tietojenkäsittelytapaa noudattaen. Tietoaineiston varmuuskopiointi ja turvallinen säilytys ja suojaus kuuluvat myös tietoaineistoturvallisuustoimiin. (Laaksonen ym. 2006, 67.)

Käyttöturvallisuus on joissakin tietoturvallisuuden luokitteluissa sisällytetty muihin osa-alueisiin, kun taas joissakin jaotteluissa sitä käsitellään omana osanaan. Useampaan osa-alueeseen jaoteltuna varsin laaja tietoturvallisuuden käsite muodostuu helpommin käsiteltäviksi osa-alueiksi. (Hakala ym. 2006, 10.) Käyttöturvallisuudella pyritään tietojen ja järjestelmien tehokkaaseen ja tarkoituksenmukaiseen käyttöön. Käyttöturvallisuus käsittää käyttöoikeuksien hallinnan, käyttäjän tunnistuksen ja erilaiset todennusmenetelmät. Niiden lisäksi käyttöturvallisuus on ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyviä turvallisuustoimenpiteitä. Käytännön toimia ovat muun muassa hyvät salasanakäytänteet ja järjestelmien suojaaminen erilaisilta viruksilta ja muilta haittaohjelmilta. Henkilöstön taito käyttää käytössä olevia ohjelmistoja on myös osa käyttöturvallisuutta. Myös hallinnon antamien sääntöjen ja määräysten noudattaminen esimerkiksi sähköpostin tai internetin sivustojen käytöstä toteuttaa käyttöturvallisuutta. (Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 65.)

Ohjelmistoturvallisuuteen kuuluvat käyttöjärjestelmien, ohjelmistojen ja sovellusten suojaukset sekä tunnistamiseen ja valvontaan liittyvät menetelmät. Myös ohjelmistojen varmuuskopioinnit ja tukipalvelut sekä muut ohjelmistojen ylläpitoon liittyvät asiat ovat osa ohjelmistoturvallisuutta. Ohjelmistoturvallisuuteen voidaan pyrkiä yrityksessä muun muassa sallittujen ja ehdottomasti kiellettyjen ohjelmien ja sovellusten määrittelemisellä sekä kouluttamalla ja ohjeistamalla henkilöstöä turvalliseen ohjelmistojen käyttöön. Esimerkiksi miten ohjelmistojen käytönaikaisilla sekä käyttöjärjestelmän ja mahdollisten väli- ja apuohjelmistojen asetuksilla voidaan vaikuttaa ohjelmistoturvallisuuteen. Ohjelmistojen ympäristön turvallisuutta voidaan parantaa muun muassa asentamalla turvapäivityksiä ja -ohjelmia. Ohjelmistoturvallisuus paranee myös, kun käyttäjien ja muiden ohjelmien pääsy ohjelmistojen sisältämään tietoon estetään. (Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 69.)

Laitteistoturvallisuus käsittää kaikkien laitteiden suojaamisen aina laitteen asennuksesta ylläpitoon ja poistoon. Laitteistoturvallisuus pyrkii turvaamaan laitteen koko elinkaaren. Käytännössä tämä sisältää takuun ja ylläpidon lisäksi tukipalvelut ja -

sopimukset. Näiden lisäksi myös poikkeamista palautuminen kuuluu laitteistoturvallisuuden piiriin. Se tarkoittaa lähinnä sitä, että käyttöjärjestelmistä, ohjelmistoista ja niiden asetuksista on olemassa varmuuskopiot. (Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 63.)

Tietoliikenneturvallisuus on hyvin laaja ja tärkeä osa-alue, joka yrityksissä ymmärretään varsin usein ainoaksi osaksi tietoturvaa. Tämä osa-alue sisältää monenlaisia teknisiä keinoja ja ratkaisuja, jotka kehittyvät jatkuvasti. Tekniikan kehittyminen onkin haaste tietoliikenneturvallisuudelle, sillä käytetyt menetelmät voivat kehityksen myötä käydä vanhoiksi ja tehottomiksi. Tietoliikenneturvallisuuden tarkoitus on tiedon luottamuksellisuuden, eheyden ja käytettävyyden turvaaminen tietojen siirron aikana. Tähän voidaan pyrkiä muun muassa riittävillä todentamis-, pääsynvalvonta- ja kiistämättömyysmenetelmillä. Verkon suojaaminen ja viestiliikenteen salaaminen ovat vain yksi keino muiden joukossa. (Laaksonen ym. 2006, 67.)

3 Tietosuojalainsäädännön vaatimukset tietoturvalle

Suomessa ei ole yhtä tiettyä tietosuojalakia, vaan tietosuojaa koskeva lainsäädäntö koostuu useista, jopa sadoista eri laeista. Tietosuojalainsäädännön tarkoitus on muun muassa toteuttaa yksilön oikeutta yksityisyyden suojaan erityisesti automaattisesti tapahtuvassa tietojen käsittelyssä. Alati kehittyvä tekniikka mahdollistaa kustannustehokkaan, monipuolisen ja yksityiskohtaisen tiedon keräämisen ja käsittelyn jopa yksilön tietämättä. Tietosuojalainsäädäntö kuitenkin rajoittaa vapaata tietojen keräämistä ja käsittelyä. Samalla se asettaa yrityksille haasteita tietoturvasta huolehtimiseen ja valvontaan. Tietosuojalainsäädäntö onkin tietoturvan kannalta keskeisessä asemassa. (Laaksonen ym. 2006, 21–22.) Tässä luvussa käsitellään tietoturvan kannalta merkittävimpiä tietosuojasäännöksiä ja niiden asettamia velvoitteita tietoturvallisuudelle.

3.1 Henkilötietolaki

Keskeisin yksilön tietosuojaa turvaava laki on henkilötietolaki (22.4.1999/523), joka on myös henkilötietojen käsittelyn peruslaki. Yleislakina henkilötietolain säännökset tulevat sovellettaviksi mahdollisen henkilötietojen käsittelyä ohjaavien erityislakien jälkeen. Kuitenkin sellaiset yleisvelvoitteet, joista ei ole erityislaissa erikseen säädetty, tulevat pääasiassa aina sovellettaviksi. Tällaisia velvoitteita ovat muun muassa suunnittelu-, huolellisuus- ja suojaamisvelvoitteet. Myös henkilötietolain rekisteröityjen oikeuksia ja ilmoitusvelvollisuutta koskevat säännökset tulevat aina sovellettaviksi. (Erityislainsäädäntö n.d.) Lakia sovelletaan automaattiseen henkilötietojen käsittelyyn sekä henkilörekisterin manuaaliseen käsittelyyn. Käytännössä tämä tarkoittaa sitä, että lakia sovelletaan kaikissa yrityksissä, joissa käsitellään henkilötietoja. Henkilötietolain tarkoitus on turvata jokaisen yksityiselämän suoja henkilötietoja käsiteltäessä. Samalla se pyrkii myös edistämään hyvää tietojenkäsittelytapaa ja sen noudattamista. (Henkilötietolaki n.d.)

Henkilötietojen käsittelyn yleiset periaatteet

Yksityisyyden suojan toteutuminen edellyttää tietojen suojaamista eli toisin sanoen tietoturvasta huolehtimista. Henkilötietolaki antaa tähän suoran kehotuksen rekisterinpitäjälle, mutta velvoitteita tietoturvaan voidaan nähdä myös henkilötietojen käsittelyn yleisistä periaatteista. Nämä käsittelyn yleiset periaatteet ilmenevät henkilötietolain (22.4.1999/523) toisesta luvusta.

Henkilötietolain 2:5 § käsittelee huolellisuusvelvoitetta. Sen mukaan rekisterinpitäjän täytyy laillisen henkilötietojen käsittelyn lisäksi noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa. Toiminta ei saa muutenkaan rajoittaa yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia. Huolellisuusvelvoitetta voidaan pitää henkilötietolain yleisvelvoitteena, koska sen toteutuminen edellyttää muiden henkilötietolain vaatimusten toteuttamista. (Vanto 2011, 39.)

Henkilötietojen käsittelyn suunnitteluvelvoite edellyttää, että henkilötietojen käsittelylle on asialliset perusteet. Rekisterinpitäjällä on siten velvollisuus perustella, miksi

henkilötietojen käyttö on sen toiminnassa tarpeellista sekä millaisia toiminnan kannalta tarpeelliset henkilötiedot ovat. Tarpeettomia ja perusteettomia tietoja ei voida kerätä. (Vanto 2011, 41.) Rekisterinpitäjän täytyy etukäteen suunnitella, mistä henkilörekisteriin hankitaan henkilötiedot ja mihin niitä mahdollisesti luovutetaan. Rekisterinpitäjän täytyy myös määritellä, millaisiin tehtäviin rekisterin tietoja tullaan käyttämään. (L 22.4.1999/523, 6 §.) Tietoturvallisuuteen suunnitteluvelvoite liittyy siten, että suunnitelmasta pitäisi selvitä, millaisin toimenpitein tietoturvasta huolehditaan. Siinä täytyisi vähintäänkin mainita tietojärjestelmän ja tietoliikenneyhteyksien yleiset vaatimukset tietoturvallisuudesta. (Laaksonen ym. 2006, 39.)

Henkilötietolain tietojen laatua koskevien periaatteiden mukaan käsiteltävien tietojen virheettömyys on rekisterinpitäjän vastuulla. Epätäydellisiä tai vanhentuneita tietoja ei saa käsitellä. (L 22.4.1999/523, 9.2 §.) Tämä tietojen virheettömyysvaatimus asettaa haasteita tietoturvalle nimenomaan tietojen eheyden turvaamisessa. Käytettävien järjestelmien täytyy olla sellaiset, etteivät tiedot pääse muuttumaan tahattomasti. Tietoturvatoimin täytyisi myös varmistaa, että tietoja pääsevät muuttamaan vain ne, joilla on siihen oikeus silloin, kun se on tarpeellista. (Laaksonen ym. 2006, 40.)

Arkaluontoisten tietojen käsittely on henkilötietolaissa kiellettyä joitakin lain sallimia poikkeuksia lukuun ottamatta (L 22.4.1999/523, 11 §). Arkaluontoisilla henkilötiedoilla on yksilön yksityisyyden kannalta suurempi merkitys kuin tavallisilla henkilötiedoilla. Sen vuoksi arkaluontoisten henkilötietojen suojaamiseen on käytettävä korkeampaa tietoturvan tasoa kuin mitä tavallisten henkilötietojen suojaaminen edellyttää. Arkaluontoisten tietojen käsittelyssä täytyy muutoinkin noudattaa erityistä huolellisuutta ja tarkkaavaisuutta, ja esimerkiksi arkaluontoisia henkilötietoja ei pitäisi lähettää sähköpostissa (Saako henkilötietoja lähettää sähköpostilla salaamattomana? 2008).

Suojaamisvelvoite ja suhteellisuusperiaate

Henkilötietolain (22.4.1999/523) 32.1 § antaa kehotuksen henkilötietojen suojaamisesta. Tämä suojaamisvelvoite edellyttää, että yksilöstä kerättävät henkilötiedot on

suojattava kaikenlaiselta asiattomalta käsittelyltä sekä vahingossa tapahtuvalta ja tahalliselta tietojen hävittämiseltä, muuttumiselta, luovuttamiselta ja siirtämiseltä. Näin suojaamisvelvoitteella on suora yhteys tietoturvaan. (L 22.4.1999/523, 38 §.)

Samasta lainkohdasta on luettavissa myös suhteellisuusperiaate tietojen suojaamisessa. Tietoturvaa toteutettaessa ei ole aina tarpeen käyttää kaikkia olemassa olevia keinoja tietojen suojaamiseen. Rekisterinpitäjän on itse arvioitava riittävä tietoturvan taso suhteellisuusperiaatteen mukaisesti. Sen mukaan käytettävien tietoturvatoimien laajuutta ja tehokkuutta arvioitaessa otetaan huomioon käytettävissä olevat tekniset mahdollisuudet ja toimenpiteiden aiheuttamat kustannukset. Myös käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta vaikuttavat siihen, miten tehokkaasti tietoturvaan on panostettava. (L 22.4.1999/523, 38 §.)

Tietoturvaan käytettävien resurssien järkevä kohdentaminen ja tietojen tarkoituksenmukainen suojaaminen edellyttää suojattavien tietojen luokittelua. Tietojen luokittelu on melko yksinkertainen ja tehokas tapa jakaa suojattavat tiedot erilaista suojausta vaativiin luokkiin muun muassa tietojen arkaluonteisuuden ja arvon mukaan. Tavallisen asiakasrekisterin suojaamiseen riittävät vaatimattomammat toimenpiteet ja resurssit kuin esimerkiksi terveyspalveluita tarjoavan yrityksen arkaluontoisia henkilötietoja sisältävän potilastietokannan suojaamiseen. (Laaksonen ym. 2006, 29.) Arkaluontoisten tietojen suojaamiseen käytettävien tietoturvamenetelmien täytyy olla ajantasaiset eivätkä taloudelliset syyt saa rajoittaa keinojen valintaa. (Voutilainen 2012, 318).

Tekniset ja organisatoriset keinot

Henkilötietolain (22.4.1999/523) 32.1 §:n suojaamisvelvoitteessa puhutaan tarpeellisista teknisistä ja organisatorisista keinoista tietojen suojaamiseksi. Lain määritelmä näistä keinoista on tarkoituksella jätetty avoimeksi. Tietoturvaloukkaukset samoin kuin tietojen suojaamiseen käytettävät menetelmätkin ovat kehittyneet teknologian kehityksen myötä. Sen vuoksi ei ole tarpeellista painottaa käytettäviä keinoja ja menetelmiä, vaan merkityksellisempää on se, mitä tietoja täytyy suojata ja miten tehok-

kaasti tietojen suojaamiseen on panostettava. (Vanto 2011, 138.) Jotta yrityksissä voitaisiin toteuttaa tietoturva henkilötietolain edellyttämällä tavalla, täytyy yrityksen tietoturvan kehittyä tekniikan kehityksen mukana. Se ei kuitenkaan tarkoita sitä, että tietoturva toteutetaan viimeisimmän teknologian mukaisin keinoin. Riittää, että käytettävät suojausmenetelmät ovat toimivia ja riittävän tehokkaita. (Laaksonen ym. 2006, 43–45.)

Hallituksen esityksessä henkilötietolaiksi (HE 96/1998) on mainittu joitakin suuntaa antavia ajatuksia, joita tietoturvatoimilla täytyisi tavoitella. Sen mukaan tietoaineistot ja -järjestelmät tulisi suojata teknisiä keinoja käyttäen niin, että jälkikäteenkin pystytään yksilöimään ja tunnistamaan henkilötietoja käsitelleet henkilöt. Rekisterinpitäjältä tämä usein edellyttää pääsynvalvontaa ja käyttäjien tunnistamista. Käytännössä se tarkoittaa vähintäänkin käyttäjätunnuksia ja salasanoja järjestelmiin kirjautumiseen. Työntekijöiden roolien määrittelyllä voidaan parantaa tietoturvan tasoa. Kaikkien ei tarvitse päästä käsiksi kaikkiin tietoihin, vaan käyttöoikeudet määräytyvät kunkin työtehtävien mukaan. Näin muun muassa työntekijöistä johtuvat tietoturvariskit vähenevät. Mitä laajempaa henkilötietojen käsittely on, sitä enemmän on kiinnitettävä huomiota käyttäjien oikeuksien määrittelyyn ja niiden hallintaan. Tarpeen vaatiessa pääsynvalvonta voidaan ulottaa koskemaan tietojärjestelmien lisäksi myös toimipaikan tiloja. (Laaksonen ym. 2006, 43.)

Tekninen tietojärjestelmien suojaus olisi toteutettava niin, että jo laittomasta järjestelmään tunkeutumisesta tai tietojen käsittelystä tulisi hälytys rekisterinpitäjälle. Mikäli mahdollista, suojausjärjestelmän täytyisi antaa tietoa myös laittoman yrityksen alkuperästä. (HE 96/1998.) Tällainen tunkeutumisen havaitseminen edellyttää yleensä verkon valvontaa sekä ulkoa että sisältä päin tulevan uhan varalta. Tietoverkkoa valvomalla voidaan tehokkaasti havaita mahdolliset tietomurrot tai väärinkäytökset sekä selvittää ongelmatilanteet myös jälkikäteen. (Laaksonen ym. 2006, 188–189.) Verkon valvonnassa täytyy ottaa huomioon Sähköisen viestinnän tietosuojalain tunnistamistietojen käsittelyä koskevat säännökset. Sen mukaan oikeus valvoa verkkoliikennettä on teleyritysten lisäksi myös yhteisötilaajilla. Yhteisötilaajana pidetään viestintäverkossa käyttäjien luottamuksellisia viestejä, tunnistamis- tai

paikkatietoja käsittelevää viestintäpalvelun tai lisäarvopalvelun tilaajana olevaa yritystä tai yhteisöä. (L 16.6.2004/516, 2 § kohta 11.) Sähköisen viestinnän tietosuojalaki määrittelee myös ne perusteet, joilla verkkoa on oikeus valvoa. Lain mukaan verkkoa voidaan valvoa esimerkiksi tietoturvasta huolehtimiseksi (L 16.6.2004/516, 20 §).

Tietojen eheyttä koskevat vaatimukset on varmistettava myös tietojen siirrossa (HE 96/1998). Tietojen eheyteen eli muuttumattomuuteen voidaan pyrkiä huolehtimalla muun muassa tietoliikenneturvallisuudesta. Tiedon siirrossa on käytettävä esimerkiksi salattua yhteyttä, jolla voidaan varmistaa tiedon muuttumattomuus. Lisäksi tiedon lähettäjä täytyy todentaa riittävän vahvasti. Se, milloin todennus on riittävän vahva, voidaan määritellä esimerkiksi riskianalyysin avulla. Jos viestintäympäristö on vahvasti suojattu, ei viestin lähettäjän todentamiseksi tarvita niin voimakkaita keinoja. Julkisissa eli avoimissa verkoissa todennuksen täytyy taas olla vahvempi. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 59.) Eheyden varmistamisen haasteena ovat eri standardeja noudattavat laitteet verkossa. Teknologian kehittyessä standardit poikkeavat usein ominaisuuksiltaan toisistaan, jolloin uusimpia standardeja noudattavien laitteiden ominaisuudet eivät välttämättä ole käytettävissä vanhempien laitteiden kanssa. (Pekkala 2012, 10.)

Hallituksen esityksessä mainitaan organisatorisina keinoina henkilötietojen käsittelyyn luotavat menettelytavat ja henkilöstön ohjeistus (HE 96/1998). Jotta siinä onnistuttaisiin, olisi hyvä tiedostaa tietojen käsittelyyn vaikuttava keskeinen lainsäädäntö. Sen pohjalta voidaan laatia käytännesäännöt ja toimintaperiaatteet liiketoiminnan erilaisiin tilanteisiin, kuten esimerkiksi siihen, miten toimitaan ja mitä täytyy sopia tietojen käsittelyn ulkoistamistilanteissa tai tietojärjestelmien ylläpitoon ja hankintaan liittyvissä asioissa. (Laadi tietotilinpäätös 2012, 6.)

Henkilöstön ohjeistuksella pyritään estämään mahdolliset ongelmat, mutta myös selviytymään tehokkaasti ongelmatilanteissa. Yrityksen toiminnasta riippuen ohjeistusta voidaan tarvita muun muassa tiedon käsittelyssä, internetin ja sähköpostin käytössä, vierailujen järjestämisessä, laitteiden ja järjestelmien käytössä sekä myös ongelmien ja poikkeusolosuhteiden varalta. Parhaimmassa tapauksessa yrityksen luomilla menettelytavoilla ja ohjeistuksilla voidaan vaikuttaa koko henkilöstön tietotur-

vaan kohdistuneisiin asenteisiin. Tietoturvamyönteinen tahtotila ja pysyvä asenne saavutetaan säännöllisellä ja aktiivisella koulutuksella. (Laaksonen ym. 2006, 146–147.)

Henkilötietojen käsittelyn ulkoistaminen

Yrityksen tai organisaation pyrkiessä kustannussäästöihin ja tehokkuuteen voi esimerkiksi IT-ylläpidon, talouspalveluiden tai asiakasrekisterin ulkoistaminen olla liiketoiminnan kannalta edullinen ja houkutteleva ratkaisu. Henkilötietojen käsittelyn ulkoistaminen etenkin Suomen ulkopuolelle vaatii ulkoistavalta organisaatiolta tarkkuutta ja huolellisuutta rekisteröidyn yksityisyyden suojan turvaamiseksi. Tietoturvan hallinta ulkoistamistilanteissa onkin yksi yrityksen merkittävä tietoturvan hallinnan osa-alue. (Laaksonen ym. 2006, 239.)

Henkilötietolain (22.4.1999/523) 2:5 §:n mukaan rekisterinpitäjä on vastuussa siitä, että henkilötietojen käsittely tapahtuu lainmukaisesti ja tiedot ovat turvassa. Sama vastuu on myös rekisterinpitäjän lukuun toimivalla palveluntarjoajalla. Itsenäisenä elinkeinonharjoittajana rekisterinpitäjän lukuun toimivan on ennen toimeen ryhtymistä annettava takeet henkilötietojen lainmukaisesta suojaamisesta (L 22.4.1999/523, 32.2 §). Käytännössä tämä tarkoittaa kirjallisesti tehtyä sitovaa sopimusta riittävästä tietoturvasta ja rekisterinpitäjän antamien ohjeiden ja määräysten noudattamisesta henkilötietojen käsittelyssä. Vaikka Suomessa tai Euroopan Unionin sisällä tapahtuvassa ulkoistamisessa laki edellyttää jo muutoinkin palveluntarjoajaa huolehtimaan riittävästä tietoturvasta, on kirjallinen sopimus silti hyvä tehdä. Ulkoistettaessa henkilötietojen käsittely Euroopan Unionin ulkopuolelle, on yksilön tietosuojan varmistamiseksi sopimuksella suuri merkitys. (Voutilainen 2012, 318–319.) Jo sopimusvaiheessa on hyvä huolehtia käyttöoikeuksien hallinnasta. Riskien minimoimiseksi täytyisi varmistaa, etteivät samat henkilöt huolehdi useista eri toiminnoista. Kun yritys ulkoistaa useita tukitoimintojaan samalle palveluntarjoajalle, kertyvät tälle valtavat tietovarannot yrityksen henkilöstön tai asiakkaiden henkilötiedoista. Tällöin riski henkilötietojen joutumisesta vääriin käsiin ja tietojen väärinkäytöstä kasvaa. (Castrén 2013.)

Henkilötietojen käsittelyn ulkoistamisessa on kyse tietojen siirrosta. Tieto sijaitsee tai sen käsittely tapahtuu yrityksen ulkopuolella, mutta tietojen tallennuspaikan haltijalla tai tietojen käsittelijällä ei ole itsenäistä oikeutta tietojen käsittelyyn. Käsittely tapahtuu ainoastaan rekisterinpitäjän toimeksiannosta rekisterinpitäjän lukuun ja sen antamien ohjeiden mukaan. (Penttilä 2012.) Rekisterinpitäjän on huolehdittava tietojen suojaamisvelvoitteen puitteissa riittävästä tietoturvasta myös tietojen siirrossa.

Henkilötietolain 5:22.1 §:n mukaan henkilötietoja voidaan siirtää Euroopan Unionin ja Euroopan talousalueen ulkopuolelle ainoastaan, jos kyseisessä maassa taataan tietosuojan riittävä taso. Euroopan Unionin tietosuojaviranomaiset katsovat kansainväliseksi tiedonsiirroksi esimerkiksi jo sen, että ulkomailta otetaan yhteyttä suomalaiseen tietokantaan. He myös suosittelevat, että palveluita ulkoistetaan vain sellaisille palveluntarjoajille, jotka pystyvät takaamaan tietojen kansainvälisen siirron lainmukaisen toteuttamisen. (Castrén 2013.)

Palveluntarjoajalle ei voida myöntää sen enempää oikeuksia kuin suomalainen lainsäädäntö antaa rekisterinpitäjälle. Yrityksen asiakkaiden ja henkilöstön tietosuojan turvaamiseksi on kiinnitettävä erityistä huomiota ulkoistettavasta palvelusta tehtävään toimeksiantosopimukseen. Jotta sopimuksella saavutettaisiin toivottu lopputulos, täytyy rekisterinpitäjän tuntea ulkoistettavien toimintoprosessien sekä siihen liittyvien tietosuojan turvaavien lakien vaatimukset. Euroopan unionin komissio on laatinut valmiita mallisopimuslausekkeita turvatakseen riittävän tietosuojan tason yrityksissä. (Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset 2010, 3—4.)

3.2 Laki viranomaisten toiminnan julkisuudesta

Lain viranomaisten toiminnan julkisuudesta (21.5.1999/621) eli julkisuuslain lähtökohtana on perustuslain (11.6.1999/731) 12.2 §:n takaama julkisuusperiaate. Sen mukaan asiakirja on julkinen ja salassapito on poikkeus, jolle täytyy olla laissa säädetty peruste. Julkisuusperiaatteen myötä jokaisella on oikeuden saada tieto viranomaisen julkisesta asiakirjasta. Julkisuuslain tarkoituksena on noudattaa hyvää tiedonhal-

lintatapaa ja avoimuutta viranomaisten toiminnassa. Julkisuuslakia sovelletaan viranomaisen laatimiin ja sen hallussa oleviin asiakirjoihin. (L 21.5.1999/621, 1–3 §.) Yksilön tietosuojan ja yksityisyyden suojaamisen kannalta julkisuuslaissa merkityksellisimpiä säännöksiä ovat lain salassapito- ja vaitiolovelvoitteet sekä hyvän tiedonhallintatavan vaatimus. Tietoturvallisuuteen liittyviä tarkentavia määräyksiä julkishallinnolle annetaan muun muassa Asetuksessa viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (12.11.1999/1030) eli julkisuusasetuksessa ja 1.10.2010 voimaantulleessa Tietoturvallisuusasetuksessa (681/2010). Julkishallinnolle ja erityisesti valtionhallinnolle suunnattuja tietoturvallisuuteen liittyviä ohjeita antaa myös Valtiovarainministeriö VAHTI-ohjeillaan. Lisäksi on lukuisia toimialakohtaisia lakeja ja asetuksia, jotka sisältävät määräyksiä tietoturvasta.

Hyvä tiedonhallintatapa

Julkisuuslain hyvää tiedonhallintatapaa koskeva 18 § sisältää asianhallinnan järjestämisvelvollisuuden, tietojärjestelmien avoimuuden, selvitys- ja suunnitteluvelvoitteen julkisuuden ja salassapidon kannalta sekä tietoturvallisuustavan määrittelyvelvollisuuden ja koulutus- ja ohjausvelvoitteen henkilöstölle. Näillä kaikilla toimilla voidaan varmistaa yksilön tietosuoja ja yksityisyys. Samalla jokainen velvollisuus ja tehtävä sisältävät tietoturvavelvoitteen. Hyvää tiedonhallintatapaa tarkentavia säännöksiä annetaan julkisuusasetuksessa (1030/1999) (Voutilainen 2012, 97.)

Julkisuuslain 18.2 § kohdan 1 ja 2 mukaisella *asianhallinnalla* tarkoitetaan suunnitelmallista ja yhdenmukaista asiakirjojen ja asioiden hallintaa. Asianhallinnalla tavoitellaan asiakirjojen julkisuuden vaivatonta toteuttamista ja salassa pidettävien asiakirjojen suojaamista asianmukaisesti. Sen tarkoitus on taata asian käsittelyn julkisuus sekä tietojen eheys, alkuperäisyys ja asiakirjojen löydettävyys. Asianhallinnan eteen tehdyt toimet varmistavat osaltaan myös tietojen saatavuuden. Asianhallinta tähtää myös tietojen oikeellisuuteen ja käytettävyyteen, ja siten viranomaisen on pidettävä rekisterinsä ajan tasalla. Asianhallinnan järjestämisestä on annettu tarkempia määräyksiä julkisuus- ja tietoturvallisuusasetuksessa. (Voutilainen 2012, 98–99, 101.)

Asianhallinnan toteuttamiseksi tietoturvallisuusasetuksessa suositellaan tietojen hallintaan asiakirjojen luokittelun eri suojaustasoille. Neliportaisella luokittelulla (erittäin salainen, salainen, luottamuksellinen ja käyttö rajoitettu) saadaan käsitys asiakirjan käsittelyn eri vaiheiden tietoturvallisuusvaatimuksista. (Tietoturvallisuusasetus 2012.) Luokiteltavaksi otetaan lähinnä salassa pidettävät asiakirjat, eikä kaikkia asiakirjoja voida tai ole edes tarpeen luokitella. Jokainen tietoaineisto on arvioitava erikseen. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 54–55.)

Salassa pidettävien asiakirjojen asianmukaisen suojaamisen toteuttamiseksi tietoturvallisuusasetus vaatii, että tietojenkäsittely-ympäristö suojataan vähintään tietoturvallisuuden perustason vaatimusten mukaisesti (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 35). Nämä vaatimukset tulevat ilmi tietoturvallisuusasetuksen 5 §:ssä. Lisäksi on huolehdittava siitä, että viranomaisen käytössä on riittävä osaaminen tietoturvatehtävien tarpeen arvioimiseksi, toimenpiteiden toteuttamiseksi, kehittämiseksi ja valvomiseksi sekä ohjauksen antamiseksi henkilöstölle. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 35.)

Selvittely- ja suunnitteluvelvoite asettaa omat vaatimuksensa viranomaisen toiminnalle silloin, kun otetaan käyttöön tietojärjestelmiä tai valmistellaan hallinnollisia uudistuksia. Velvoite edellyttää suunniteltujen toimenpiteiden vaikutusten selvittämistä asiakirjojen julkisuuteen, salassapitoon ja suojaan sekä tietojen laatuun. (L 21.5.1999/621, 18.2 § kohta 3.) Lisäksi viranomaisten on asianmukaisin menettelytavoin ja tietoturvajärjestelyin turvattava asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu. Turvaamisessa on huomioitava tietojen merkitys ja käyttötarkoitus suhteessa asiakirjoihin ja tietojärjestelmiin kohdistuviin uhkiin ja tietoturvatoimenpiteistä aiheutuviin kustannuksiin. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 28.)

Henkilöstön koulutus- ja ohjausvelvoitteella halutaan varmistaa virastossa asioivien mahdollisimman tehokas ja nopea palvelu, mutta myös tietoturvan toteutuminen. Viranomaisen palveluksessa olevalla tulisi sen vuoksi olla riittävät tiedot muun muas-

sa hyvän tiedonhallinnan ja työssä tarvittavan tietoturvan toteuttamiseksi. Viranomaisen vastuulla on kouluttaa ja ohjeistaa henkilöstöä niin, että se hallitsee tietojärjestelmien ja ohjelmistojen turvallisen käytön. Henkilöstön tulisi myös ymmärtää, että henkilöstö on organisaation suurin tietoturvauhka. (Voutilainen 2012, 127–128.)

Salassapitovelvoite

Julkisuuslain salassapitovelvoite sisältää asiakirjasalaisuuden, vaitiolovelvollisuuden ja hyväksikäyttökiellon. Yksilön tietosuojan näkökulmasta katsottuna salassapidon tarkoituksena on estää julkisuuden aiheuttama haitta tai vahinko yksityiselämälle tai yksityisyydelle. (Voutilainen 2012, 149.) Julkisuuslain (21.5.1999/621) 22 § sanoo, että laissa tai lain nojalla salaiseksi määrätty tai lain mukaan vaitiolovelvollisuuden alaisia tietoja sisältävä viranomaisen asiakirja on pidettävä salassa. Salassa pidettävää viranomaisen asiakirjaa ei saa saattaa millään tavoin ulkopuolisen nähtäville. Vaitiolovelvollisuuden puitteissa siitä ei saa edes puhua ulkopuolisille. Vaitiolovelvollisuus syntyy jo salassa pidettävän asiakirjan tai tapahtuman näkemisestä. Esimerkiksi sosiaaliviranomaisen asiakkaan kodissa tekemät näköhavainnot ovat vaitiolovelvollisuuden alaisia. Tähän asiakirjasalaisuuteen liittyy myös hyväksikäyttökielto, jonka mukaan tiedon saanut ei saa käyttää tietoa millään tavoin hyväkseen. Salassapito- ja vaitiolovelvollisuudet sekä tietojen hyväksikäyttökielto velvoittavat myös sen jälkeen, kun viranomaisen palveluksessa tai sen lukuun toimiminen on päättynyt. (Voutilainen 2012, 150–151.)

Vaikka salassapitovelvoite on lakisääteinen, on yhtenä tietoturvatoimena syytä muistuttaa henkilöstöä tästä salassapitovelvoitteesta. Erityisesti harjoittelijoille sekä muulle väliaikaishenkilöstölle voi olla tarpeellista tiedottaa salassapitovelvoitteesta. He voivat uusina työntekijöinä nähdä ja kokea työssään erikoisia tilanteita ja asioita, joista he haluaisivat kertoa kavereilleen ja tuttavilleen. Myös yhteistyökumppaneiden, alihankkijoiden ja muiden vastaavien yhteistyötahojen kanssa on tarpeellista laatia erilliset salassapitosopimukset. (Andreasson ym. 2013, 22–23.)

3.3 Laki yksityisyyden suojasta työelämässä

Yksityisyyden suojasta työelämässä annetun lain eli lain (13.8.2004/759) tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden turvaavia perusoikeuksia työelämässä. Laki koskee vain työnantajan ja työntekijän välistä suhdetta. Lain noudattamista valvovat työsuojeluviranomaiset ja tietosuojavaltuutettu. Lain noudattamista tehostetaan myös lain 24 §:n rangaistussäännöksillä. (Työelämän tietosuojalaki n.d.) Laki ei varsinaisesti liity asiakkaiden tietosuojaan, mutta sitä on kuitenkin syytä tarkastella tietoturvan toteuttamisen kannalta. Nykytekniikan avulla voitaisiin varsin tehokkaasti valvoa ja seurata työntekijöitä, tietoverkkojen käyttöä ja käyttäjiä ja siten toteuttaa tietoturvaa. Jokaisella on kuitenkin oikeus yksityisyyteensä myös työpaikalla eivätkä työnantajan päätökset saa loukata työntekijöiden yksityisyyttä. (Laaksonen ym. 2006, 50–51.)

Työelämän tietosuojalaissa (13.8.2004/759) mainittua teknistä valvontaa voidaan toteuttaa monin eri keinoin. Valvonta voi olla esimerkiksi kameravalvontaa, kulunvalvontaa tai tietoverkon valvontaa. Tässä luvussa tarkastellaan lähemmin kamera- ja kulunvalvontaa. Verkonvalvontaa ohjaa tarkemmin sähköisen viestinnän tietosuojalaki, jota käsitellään seuraavassa luvussa.

Kulunvalvonta ja kameravalvonta

Kulunvalvonnan tarkoituksena on yleensä estää asiattomien pääsy heille kuulumattomiin tiloihin sekä sallia työntekijöiden pääsy työtehtävien kannalta tarpeellisiin tiloihin. Se on kameravalvontaan verrattuna hieman kevyempi tietoturvakeino. Oikein toimiessaan kulunvalvonnalla pystytään tehokkaasti nostamaan fyysisen tietoturvan tasoa. Tietoturvallisuuden lisäksi kulunvalvontaa voidaan ajatella asiakaspalvelua parantavana tekijänä. Asiakas voidaan helposti ja nopeasti ohjata etsimänsä henkilön luo. (Laaksonen ym. 2006, 51.)

Kameravalvonta on yksi teknisin keinoin toteutettava valvontakeino, jolla voidaan toteuttaa fyysistä tietoturvaa. Työelämän tietosuojalain (13.8.2004/759) 16 § mukaan kameravalvonnasta on kyse, kun valvontaan käytetään joko jatkuvaa kuvaa vä-

littävää tai kuvaa tallentavaa teknistä laitetta. Kameravalvonnalla voidaan nostaa turvallisuuden tasoa kulunvalvonnan osana. Sen avulla voidaan esimerkiksi seurata, kuka tiloissa liikkuu ja estää asiattomien pääsy tiloihin. (Laaksonen 2006, 52.)

Kameravalvonta on ehdottomasti kiellettyä käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa tai muissa henkilöstötiloissa taikka työntekijöiden henkilökohtaiseen käyttöön osoitetussa työhuoneessa (L 13.8.2004/759, 16 §). Kameravalvonta ei ole tarkoitettu työntekijöiden valvontaan. Laki sallii kameravalvonnan työntekijöiden ja muiden tiloissa oleskelevien turvallisuuden varmistamiseksi ja turvallisuutta uhkaavien tilanteiden ehkäisemiseksi. Sallittua on myös järjestää kameravalvonta omaisuuden suojaamiseksi tai tuotantoprosessien asianmukaisuuden valvomiseksi sekä omaisuutta ja tuotantoprosessia uhkaavien tilanteiden ennaltaehkäisemiseksi. Kameravalvonnalla saatua materiaalia voidaan käyttää myös vaaratilanteiden selvittelyssä. (L 13.8.2004/759, 16 §.) Omaisuudeksi voidaan tässä yhteydessä lukea myös yrityksen tieto-omaisuus ja muut rekistereihin tallennettu tieto, kuten asiakasrekisteri.

Ennen kuin kameravalvontaa voidaan käytännössä toteuttaa, täytyvät työelämän tietosuojalain (13.8.2004/759) asettamien edellytysten täyttyä. Kameravalvonnan käytön on oltava aina asiallisesti perusteltua ja avointa. Ennen kuin kameravalvonta voidaan aloittaa, on selvitettävä työntekijöiden yksityisyyteen vähemmän puuttuvien keinojen käyttömahdollisuutta, esimerkiksi kulunvalvonta (L 13.8.2004/759, 17 §). Kameravalvonnan avulla työntekijöistä kertyneitä tietoja täytyy käsitellä henkilötietolain 5-7, 10 ja 32–34 § periaatteiden mukaisesti, vaikka kertyneet tiedot eivät muodostaisikaan henkilörekisteriä. Kameravalvonnasta kertyneen aineiston käsittelyssä täytyy siten noudattaa henkilötietolain suojaamisvelvoitetta, vaitiolovelvollisuutta sekä tietojen hävittämistä koskevia säännöksiä. (Koskinen, Alapuranen, Heino & Lehtonen 2012, 77.)

Teknisiä valvontakeinoja ei voida viedä äärimmäisyyksiin, vaan huomioon täytyy aina ottaa työelämän tietosuojalain rajoitukset työntekijöiden yksityisyyteen puututtaessa. Käytettävät tekniset valvontakeinot on suhteutettava suojattavien tietojen tärkeyteen ja merkitykseen yrityksen liiketoiminnalle tai suojattavien henkilötietojen

kohteen yksityisyydelle. Toimien täytyy siis olla mahdollisimman vähän työtekijöiden yksityisyyttä ja viestinnän luottamuksellisuutta uhkaavaa. (Laaksonen ym. 2006, 51.)

3.4 Sähköisen viestinnän tietosuojalaki

1.9.2004 tuli voimaan sähköisen viestinnän tietosuojalaki (16.6.2004/516) korvaten lain yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta. Sen tarkoitus on muun muassa turvata viestinnän luottamuksellisuus ja yksityisyyden suojaa sähköisessä viestinnässä. (L 16.6.2004/516, 1§.) Laki tulee sovellettavaksi yleisissä viestintäverkoissa tarjottaviin verkko-, viestintä- ja lisäarvopalveluihin kuten myös palvelun käyttöä kuvaavia tietoja käsitteleviin palveluihin. Edellisten lisäksi lakia sovelletaan yleisissä viestintäverkoissa tapahtuvaan suoramarkkinointiin sekä tilaajaluettelopalveluihin ja numerotiedotuspalveluihin. (L 16.6.2004/516, 3 §.) Lähes jokaisessa yrityksessä käsitellään työntekijöiden tai asiakkaiden tunnistamistietoja tai luottamuksellisia viestejä. Näin ollen sähköisen viestinnän tietosuojalaki tulee pääsääntöisesti sovellettavaksi useimmissa yrityksissä. Lain soveltamisalan ulkopuolelle jäävät täysin yleisestä tietoverkosta suljetut, sisäiset tietoverkot, esimerkiksi intranet-verkot. (Laaksonen ym. 2006, 54–55, 61.)

Sähköisen viestinnän tietosuojalain (16.6.2004/516) 19 § velvoittaa huolehtimaan verkkopalvelun sekä mahdollisista käyttäjiensä tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta. Tunnistamistietoja ovat tiedot, joita käsitellään viestintäverkossa tietojen siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi ja jotka ovat yhdistettävissä käyttäjään tai tilaajaan. Tunnistamistietoja ovat esimerkiksi tietoturvatoimena tapahtuvasta verkon valvonnasta tai verkkoselailusta kertyvät tiedot. Näistä tiedoista voivat selvitä muun muassa viestinnän osapuolet ja ajankohta, verkkovierailun kesto sekä käytetyt palvelut. (Innanen & Saarimäki 2012, 27.) Tietoturvatoimin täytyy varmistaa toiminnan turvallisuus, tietoliikenneturvallisuus, laitteisto- ja ohjelmistoturvallisuus sekä tietoaineistoturvallisuus. Lainkohta ei kuitenkaan velvoita tietoturvaan hinnalla millä tahansa, vaan siitä on luettavissa suhteellisuusperiaate. Sen

mukaan käytettävät tietoturvatoimet voidaan suhteuttaa uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin. (L 16.6.2004/516, 19 §.)

Tunnistamistiedoista voi kertyä runsaasi tietoa. Yhdistämällä nämä tiedot muualta verkosta vapaasti saatuun tietoon voi antaa yksittäisen henkilön viestinnässä hyvinkin kattavan kuvan. (Innanen & Saarimäki 2012, 28). Jos tunnistamistiedoista voidaan kohtuullisella vaivannäöllä tunnistaa käyttäjä, täytyy niitä käsitellä henkilötietolain määräysten mukaisesti (Laaksonen ym. 2006, 194). Myös kaikki muu sähköisen viestinnän avulla kertynyt tieto on luottamuksellista, ellei sitä ole tarkoitettu julkiseksi. Vaitiolovelvollisuuden vuoksi ei palveluntarjoaja saa ilmaista ulkopuolisille tahoille saamaansa luottamuksellista viestiä ja tunnistamistietoja, ellei asianosainen ole antanut siihen suostumustaan. Palvelun tarjoaja ei saa edes itse käyttää näitä tietoja hyväksi, vaan sillä on sähköisen viestinnän tietosuojalain mukaan hyväksikäyttökielto. Vaitiolovelvollisuus ja hyväksikäyttökielto koskevat niin itse yritystä kuin sen työntekijöitäkin, jotka työsuhteessa tai toimeksiantosopimuksen perusteella käsittelevät luottamukselliseksi luokiteltua tietoa. (L 16.6.2004/516, 5 §.)

Perustuslaissa taattuun yksityisyyden suojaan voidaan puuttua, mikäli siitä on erikseen laissa säädetty. Sähköisen viestinnän tietosuojalaki antaa tähän mahdollisuuden, jos sähköisesti tapahtuvan palvelun tietoturva on uhattuna. Uhan torjumiseen ja selvittämiseen käytettävät toimenpiteet on suhteutettava häiriön vakavuuteen, eikä viestin loukkaamattomuutta ja yksityisen suojaa saa vaarantaa enempää kuin on tarpeen. (L 16.6.2004/516, 20 §.)

3.5 Tietosuojalainsäädännön tulevaisuus

Teknologian kehitys ja tietojen käsittelyn siirtyminen sähköiseen ympäristöön on mahdollistanut liiketoiminnan globalisoitumisen. Vanhentunut ja hajanainen tietosuojalainsäädäntö ei enää pysty huomioimaan riittävästi yksilön tietosuojaa tässä muuttuneessa ympäristössä. Sen vuoksi Euroopan Komissio on nähnyt tarpeelliseksi yhtenäistää, yhdenmukaistaa ja uudistaa tietosuojalainsäädäntöä Euroopan Unionin jäsenmaiden alueella. (EU:n tietosuojauudistuksen tavoitteena vahvistaa yksilön oi-

keutta valvoa henkilötietojaan 2012.) Euroopan komissio antoi ehdotuksensa 25.1.2012 tietosuoja-asetukseksi ja -direktiiviksi. Sen tavoitteena on luoda Euroopan unionille ajan haasteisiin vastaava ja vahva tietosuojakehys. Uudistuksen nähdään myös parantavan luottamusta online-palveluihin. Luottamus on puolestaan omiaan edistämään Euroopan Unionin digitaalisten sisämarkkinoiden kehittämistä. (Euroopan unionin tietosuojalainsäädännön uudistaminen 2013.) Uusi asetus tulee olemaan kaikilta osiltaan velvoittava, ja se tulee sellaisenaan sovellettavaksi kaikissa Euroopan Unionin jäsenvaltioissa (Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta 2012, 101).

Uudistus on tuomassa rekisterinpitäjille lisää vastuita ja velvollisuuksia sekä rekisteröidyille enemmän oikeuksia. Tietoturvasta huolehtimiseen se ei periaatteiltaan tuo suurta muutosta, mutta joiltakin osin tarkentaa tai täsmentää tietoturvaan liittyviä asioita. Kuten henkilötietolaista, myös ehdotetusta asetuksesta on luettavissa suhteellisuusperiaate henkilötietojen suojaamisessa. Henkilötietolain suhteellisuusperiaatteeseen siinä on kuitenkin pieni poikkeus. Kun henkilötietolain mukaan tietojen suojaamisessa voidaan ottaa huomioon käytettävissä olevat tekniset keinot, niin ehdotuksessa huomioon otetaan uusin tekniikka. Siten tietoturvaa toteuttaessa ei voida turvautua jo vanhentuneisiin keinoihin, vaikka ne ehkä joissakin tapauksissa voisi toimiakin. (Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta 2012, 62.)

Yksi yrityksen toiminnassa näkyvimmistä tietoturva-asioihin liittyvistä muutoksista on tietosuojavastaavan nimeäminen. Ehdotetun tietosuoja-asetuksen 35 artiklan kohdan 1 mukaan tietosuojavastaava täytyisi nimetä tietojen käsittelyä suorittavaan viranomaiseen ja julkishallinnon elimeen sekä vähintään 250 henkeä työllistävään yritykseen. Tietosuojavastaava täytyisi nimetä myös tätä pienempään yritykseen, jos sen keskeiset tehtävät vaativat rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. (Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta 2012, 67.)

Tietosuojavastaavalta edellytetään riittävää ammattipätevyyttä ja erityisesti tietosuojalainsäädännön ja alan käytänteiden erityisasiantuntemusta. Lisäksi tietosuojavastaavalta vaaditaan valmiuksia hoitaa sille tarkoitetut tehtävät. Näitä ovat esimerkiksi neuvonta asetuksen mukaisten velvollisuuksien hoitamisessa, asetuksen säännösten noudattamisen seuraaminen (muun muassa tietoturva-asioissa) ja valvontaviranomaisen yhteyspisteenä toimiminen. Tietosuojavastaavalta vaadittavan erityisasiantuntemuksen tason määrittelevät henkilötietojen käsittelyn laajuus ja tietojen vaatima suoja. Tietosuojavastaava nimetään aina kahdeksi vuodeksi kerrallaan. Sama henkilö voidaan nimetä tehtävään myös uudelleen. (Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta 2012, 68–69.)

Toinen merkittävä muutos vielä voimassa olevaan henkilötietolakiin nähden on rekisterinpitäjän velvollisuuksien laajentaminen myös henkilötietojen käsittelijään. Asetuksen mukaan henkilötietojen käsittelijä voi olla luonnollinen tai oikeushenkilö, viranomainen tai virasto, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Muun muassa ehdotuksen 30 artikla velvoittaa rekisterinpitäjän ohella myös henkilötietojen käsittelijää toteuttamaan tarvittavat tietoturvatoimet tietojenkäsittelyn turvallisuuden varmistamiseksi. (Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta 2012, 11, 44.)

Ehdotus tuo mukanaan myös toisen velvollisuuden laajentamisen. Nykyiseen sähköisen viestinnän tietosuojadirektiivin 2002/58/EY 4 artiklan 3 kohtaan perustuva ilmoitusvelvollisuus tietoturvaloukkauksista laajenee kaikkia rekisterinpitäjiä koskevaksi. (Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta 2012, 11.) Säännökset ilmoitusvelvollisuudesta ovat lähinnä yksilön turvaksi. Riittävän nopeat ja tehokkaat toimet tietoturvaloukkauksen yhteydessä vähentävät huomattavasti yksilölle koituvia taloudellisia menetyksiä ja sosiaalisia haittoja. Sen vuoksi ehdotuksen 31 artiklan kohdan 1 mukaan rekisterinpitäjän olisi ilmoitettava tietoturvaloukkauksesta valvontaviranomaiselle mahdollisimman nopeasti 24 tunnin kuluessa. Heti tämän ilmoituk-

sen jälkeen tietoturvaloukkauksesta on ilmoitettava kaikille niille henkilöille, joiden henkilötietoihin tietoturvaloukkaus voi vaikuttaa haitallisesti. Tietoturvaloukkaus vaikuttaa rekisteröidyn henkilötietoihin tai yksityisyyteen haitallisesti, jos se voi johtaa esimerkiksi henkilötietovarkauteen tai -petokseen tai jos siitä voi aiheutua fyysistä haittaa tai huomattavan vakavaa nöyryytystä. Myös rekisteröidyn maineelle mahdollisesti aiheutuva haitta on perusteltu syy ilmoittaa tietoturvaloukkauksesta rekisteröidylle. (Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta 2012, 29.)

Kansalaisen kannalta merkittävä muutos on oikeus tulla unohdetuksi. Sen perusteella jokainen voi pyytää tietojensa poistamisen heti, kun tietojen säilyttämiselle ei ole perusteltua syytä. Myös suostumuksen perusteella tapahtuvaan tietojen käsittelyyn tarvittaisiin uudistuksen myötä aina nimenomainen suostumus. Tänä päivänä usein vain oletetaan henkilön antaneen suostumuksensa, mutta uudistuksen myötä se ei enää voisi olla mahdollista. Kolmas merkittävä uudistus kansalaisen näkökulmasta on rekisterin pitäjän velvollisuus tiedottaa tapahtuneesta tietojen katoamisesta, varastamisesta tai käsittelystä mahdollisimman nopeasti, viimeistää 24 tunnin kuluttua. Näin yksilöllä on paremmat mahdollisuudet toimia nopeasti itse mahdollisten tietojen vääriin käsiin joutumisen haittoja vastaan. (Reding 2013.)

Euroopan Unionin Komissio haluaa varmistaa, että asetuksen säännöksiä varmasti noudatetaan. Asetuksen myötä tietosuojavaltuutettu voi määrätä tehokkaita, oikeasuhteisia ja varoittavia hallinnollisia seuraamuksia asetuksen säännösten rikkomisesta. Hallinnollisen sakon suuruus määräytyy sääntörikkomuksen luonteen, vakavuuden ja keston sekä tahallisuuden mukaan. Aiemmat rikkomukset ja tietoturvan laiminlyönti ovat raskauttavia seikkoja. Ensikertalainen voi selvitä pelkällä huomautuksella, jos henkilötietojen käsittely on lähes merkityksetöntä. Käytännössä tämä tarkoittaa sitä, ettei luonnollisen henkilön suorittamalla henkilötietojen käsittelyllä ole kaupallista intressiä tai alle 250 hengen yrityksessä henkilötietojen käsittely on pelkkä aputoiminto. (Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta 2012, 94.)

4 Tietosuoja ja tietoturva yrityksissä

Asiakastietojen keruun ja käsittelyn lisääntyminen uudenlaisten ja tehokkaiden menetelmien myötä on kasvattanut valtavia tietovarastoja. Usein henkilötietojen käsittely on keskeisessä asemassa niin julkisella kuin yksityisellä sektorillakin. Joillakin yrityksillä liiketoiminta jopa perustuu henkilötietojen käsittelyyn, ja asiakastiedoilla ja asiakkuuksilla on yrityksille usein merkittävä taloudellinen arvo. Verkossa liikkuvan tiedon määrän kasvaessa ovat erilaiset tietomurrot, vakoilut ja tietojen kalastelut lisääntyneet huimasti. Tämä kehitys asettaa toimijoille uusia haasteita niin tietosuojasta kuin tietoturvastakin huolehtimiselle. (Salminen 2009, 18–22.) Tässä luvussa tarkastellaan tietosuojan ja tietoturvan haasteita ja niihin vastaamista yrityksissä ja organisaatioissa.

4.1 Tietosuojan merkitys yrityksille

Yrityksissä ei tunneta tietosuojalainsäädäntöä kovinkaan hyvin. Muun muassa Eurobarometri 2008 kertoo, että rekisterinpitäjien oman näkemyksensä mukaan Suomessa vain murto-osa (2 %) tuntee tietosuojalainsäädännön hyvin ja vajaa puolet (48 %) melko hyvin. Puolet (50 %) rekisterinpitäjistä katsoo, että tuntee tietosuojalainsäädännön huonosti. (Data Protection in the European Union - Data controllers' perceptions - Analytical Report 2008, 9.) Myös Tietosuojavaltuutetun 2011 tekemä selvitys antaa samansuuntaisia viitteitä. Sen mukaan suurin osa tietomurron kohteiksi joutuneista yrityksistä ei tiedä, miten lainsäädäntö vaatii suojaamaan henkilötietoja. (Tietosuojavaltuutettu vaatii yrityksiä panostamaan tietoturvaan 2012.)

Tietosuoja koetaan PK–yrityksissä myös raskaaksi ja hallinnollisia kuluja lisääväksi. Tietosuojasäädökset ovat yksi yrityksen taloutta eniten rasittavista säädöksistä. (Komissio haluaa helpottaa pk-yritysten toimintaa keventämällä kymmentä eniten hallinnollista rasitusta aiheuttavaa EU:n säädöstä 2013.) Yrityksissä ei myöskään olla perillä tietosuojalainsäädännön uudistumisesta ja muuttumisesta. Tämä käy ilmi tie-

toturvayhtiö Trusteqin tekemästä selvityksestä, jonka mukaan vain puolet suomalaisista yrityksistä on tietoisia lähiaikoina tapahtuvasta muutoksesta. (Mikkonen 2013.)

Tietosuoja ja siitä huolehtiminen on kuitenkin tärkeää yrityksen toiminnan jatkuvuuden kannalta. Mahdolliset tietosuojan ja yksityisyyden loukkaukset tulevat nopeasti julkisuuteen median kautta. Julkisen keskustelun myötä yksilön tietoisuus oikeudesta omaan yksityisyyteensä on lisääntynyt. Se on myös saanut yksilöt arvostamaan tietosuojaa aiempaa enemmän. Yrityksen hitaasti ansaitsema luottamus saattaa romahtaa hetkessä julkisuuteen tulleen tietosuojaloukkauksen myötä. Kertaalleen menetetty maine ja luottamus on vaikeaa saada takaisin, ja pahimmillaan tietosuojaloukkauksen julkitulo voi lamaannuttaa koko liiketoiminnan. (Salminen 2009, 20–22, 122.)

Ihmiset asioivat mieluummin luotettavaksi koetuissa yrityksissä, vaikkei se olisikaan edullisin vaihtoehto. Eurobarometrin 2011 mukaan kansalaiset ovat huolissaan tietosuojastaan, mutta luottavat enemmän organisaatioihin, joissa on tietosuojavaltuutettu (Special eurobarometer 359 - Attitudes on Data Protection and Electronic Identity in the European Union 2011, 2–3).

Yrityksen vastuullisuus tietosuojassa on osa hyvää asiakaspalvelua etenkin niissä yrityksissä, joissa liiketoiminta perustuu henkilötietojen käsittelyyn. Hyvin hoidettu tietosuoja parantaa asiakkaiden kokemusta yrityksestä ja lisää luottamusta yritystä kohtaan. Voidaan siis sanoa, että tietosuojan huomioiminen liiketoiminnassa vaikuttaa yrityksen kilpailukykyyn ja on asianmukaisesti hoidettuna yritykselle kilpailuetu. (Salminen 2009, 18–22.)

Tietosuoja on myös lakisääteinen velvollisuus. Se velvoittaa yrityksiä huolehtimaan henkilötietojen lainmukaisesta käsittelystä. Rekisterinpitäjänä yritys on vastuussa siitä, että rekisteritoiminnot ja näihin toimintoihin käytettävät tietojärjestelmät vastaavat lainsäädäntöä. Rekisterinpitäjän vastuulla on myös henkilöstön kouluttaminen, ohjeistaminen ja asianmukaisten määräysten antaminen henkilötietojen käsittelyyn. Jokainen henkilötietoja käsittelevä on vastuussa käsittelyn lainmukaisuudesta. Esimerkiksi vaitiolovelvollisuus koskee jokaista henkilötietoja käsittelevää. Yrityksen tai organisaation päättävät elimet tai henkilöt vastaavat kuitenkin viimekädessä siitä,

että annettuja ohjeita ja määräyksiä noudatetaan. Havaittuun säännösten ja määräysten sekä ohjeiden vastaiseen henkilötietojen käsittelyyn täytyy johdon puuttua välittömästi. (Henkilötietolain seuraamusjärjestelmä 2010, 3, 5.)

Tietosuojan laiminlyönti voi johtaa henkilötietolain (22.4.1999/523) 47 § ja 48 §:n mukaisesti korvausvelvollisuuteen sekä mahdollisesti myös rikosoikeudelliseen vastuuseen. Esimerkiksi vaitiolovelvollisuuden rikkomisesta voi saada sakkoa tai enintään vuoden vankeusrangaistuksen (Henkilötietolain seuraamusjärjestelmä 2010, 3). Tai jos rekisterinpitäjän rekisteristä joutuu tietoja sivullisen käsiin, selvitetään myös rekisterin suojaamisvelvoitteen toteutuminen. Puutteellisesti toteutettu suojaaminen tai suojaamisvelvoitteen laiminlyöminen voi tarkoittaa, että kyseessä on henkilörekisteririkos. (Voutilainen 2012, 319.)

Henkilötietolain (22.4.1999/523) 47 §:n mukaan rekisterinpitäjä on velvollinen korvaamaan rekisteröidylle tai muulle henkilölle henkilötietolain vastaisesta henkilötietojen käsittelystä aiheutuneen taloudellisen ja muun vahingon. Myös asianosaisen kärsimys on korvattava. (Henkilötietolain seuraamusjärjestelmä 2010, 4.) Vahingonkorvausvastuu on niin sanottua ankaraa vastuuta. Siten vastuun syntyminen ei edellytä tahallisuutta tai edes huolimattomuutta, vaan henkilötietojen lainvastaisesta käsittelystä syntynyt vahinko on aina korvattava asianosaiselle henkilölle. Edellytyksenä on, että asianosainen pystyy osoittamaan, että vahinko on tapahtunut yrityksen toiminnasta. (Salminen 2009, 121.)

4.2 Yritysten yleisimmät tietosuoja- ja tietoturvauhat

Yritykset kohtaavat erilaisia tietosuojaa uhkaavia tekijöitä ja tilanteita jopa päivittäin. Henkilötietojen joutuessa vääriin käsiin, on tietojen kohteen yksityisyys ja tietosuoja vaarassa. Samalla se aiheuttaa haittaa myös tietojen suojaamisesta vastuussa olleelle organisaatiolle. (Tietovuodot 2011.) Useiden tutkimusten mukaan tietoturvaosaaminen on PK -yrityksissä ollut puutteellista ja kiinnostus tietoturvaa kohtaan vähäistä. Vaikka yrityksissä myönnetään, että tietoturva on liiketoiminnan elinehto, ei sen toteuttamiseen ole riittävästi panostettu (Hulkko 2012). Asenteet ovat olleet suurim-

pana esteenä tietoturvalle. Uhkakuvia ei oteta todesta eikä suojausta nähdä tarpeellisena. Tietoturvayhtiö Symantecin 2010 julkaiseman tutkimuksen mukaan lisääntyneet tietoturvahyökkäykset ovat kuitenkin saaneet PK -yritykset kiinnostumaan tietoturvasta. (Symantec 2010 SMB Information Protection Survey Global Data 2010, 5–6.)

Tietotekniikan liitto ry:n, Symantecin ja Rittalin vuonna 2007 julkaiseman tutkimuksen mukaan tietoturvauhat on jaettavissa kolmeen ryhmään. Ensimmäisen ryhmän uhat kohdistuvat verkkotietoturvaan ja IT-järjestelmiin. Niitä uhkaavat niin huomaamattomasti leviävät haittaohjelmat kuin roskapostit ja muut verkon yli tapahtuvat hyökkäyksetkin. Myös laitteisto- ja ohjelmistoviat kuuluvat tutkimuksen mukaan tähän ryhmään. Toisen ryhmän muodostavat fyysiset uhat, kuten tulipalot ja onnettomuudet. Tutkimus sisällyttää myös salakuuntelun ja teknisin keinoin tapahtuvan tietojen keräämisen tähän ryhmään. Kolmantena, muttei suinkaan vähäisimpänä ryhmänä, ovat henkilöstöstä johtuvat riskit. Henkilöstö aiheuttaa vahinkoa tahallaan tai tahattomasti. Usein suurimpana ongelmana ovat henkilöstön tietämättömyys ja osaamattomuus. (Mäki 2007.)

Henkilöstöriskit

Henkilöstö on tiedostettu suurimmaksi tietoturvaa uhkaavaksi tekijäksi organisaatioissa. Henkilöstö tallentaa, muokkaa, välittää ja muutoinkin käsittelee tietoja. Myös tietovarastojen ja -järjestelmien ylläpito on ihmisten vastuulla. Näissä tietojen käsittelyn eri vaiheissa ja tilanteissa huolimattomuus, virheet, osaamattomuus tai tahallisesti aiheutetut vahingot uhkaavat tietoturvaa ja siten myös tietosuojaa. (Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008, 11–12.)

Henkilöstön osaamattomuus ja huolimattomuus aiheuttaa usein riskitilanteita. Tekniikan kehittymisen myötä tietojen käsittely ja säilyttäminen tapahtuu yhä useammin sähköisesti. Samalla myös käytettävät laitteet ja menetelmät kehittyvät. Puhelimet eivät ole enää vain soittamista ja vastaamista varten, vaan niillä voidaan päästä tietojärjestelmiin ja -verkkoihin. Puhelimen rinnalle on tullut myös muita tietojen käsittelyyn pystyviä kannettavia laitteita. Tietojen käsittelyyn tulee uusia, entistä monipuoli-

sempia ja tehokkaampia ohjelmistoja, jotka voivat tuottaa tietojen käsittelijöille vaikeuksia. Käytössä tapahtuvat inhimilliset virheet ja tietosuojaohjeiden laiminlyönnit voivat johtaa haittaohjelmien pääsyyn tietokoneelle ja tietosuojaloukkauksiin. Etenkin kannettavien laitteiden suojaaminen ja tietoturvaohjelmistojen päivitykset unohtuvat helposti. Henkilöstön huolimattomuuden vuoksi kannettavia laitteita myös katoaa, jolloin niiden sisältämät tiedot voivat joutua vääriin käsiin tai löytäjällä voi olla vaikka suora pääsy yrityksen tietojärjestelmiin. Erityisesti suojaamattomien kannettavien laitteiden katoaminen onkin yksi PK-yritysten huolenaihe (Symantec 2010 SMB Information Protection Survey Global Data 2010, 5–6).

Tietosuojauhkaksi täytyy ymmärtää myös yrityksestä pois lähtevä henkilöstö. Etenkin riitatilanteessa eroava tai irtisanottu työntekijä saattaa olla halukas kostamaan tai ottamaan vielä viimeisen hyödyn irti työpaikastaan. Yritysten rikosturvallisuus 2012: Riskit ja niiden hallinta (2012, 25–26) selvityksen mukaan keskimäärin joka kymmenessä (12 %) yrityksestä pois lähtevä työntekijä on kopioinut yrityksen tietoja mukaansa. Selvitys ei kerro, kuinka suuri osa kopioiduista tiedoista sisältää henkilötietoja, jolloin tietojen kopioiminen luvatta vaarantaa suoraan yksilön tietosuojan. Ongelma on yleisempi suurissa yrityksissä, joissa yli viidesosa (22 %) kopioi tietoja mukaansa työsuhteen päättyessä. Tietoja ei tarvitse kopioida, jos poislähtevän työntekijän oikeuksia päästä yrityksen tietoihin ei muisteta poistaa.

Henkilöstön uteliaisuus koituu toisinaan yksilön tietosuojaa vaarantavaksi tekijäksi. Mediassa on ollut esillä useita tietosuojaloukkaustapauksia etenkin terveydenhuoltoalalta. Näissä tapauksissa henkilöstö on urkkinut luvatta asiakkaan potilastietoja. (Eronen 2012.) Urkintatapaukset ovat olleet kasvussa, vaikka kiinnijäämisriski on aiempaa suurempi kehittyneen teknologian vuoksi. Yleensä urkkija itse myös tietää tekevänsä väärin. (Airola, O 2013.) Tietoja voivat urkkia myös ulkopuoliset. Ei ole aivan tavatonta, että verkosta löytyvän tiedon avulla tekeydytään toiseksi henkilöksi. Näitä tietoja ja henkilöstön hyväuskoisuutta hyväksi käyttäen tietoja joutuu vääriin käsiin (Vuoden 2010 merkittävimmät tietoturvariskit 2010.)

Muut riskit

Eri-ikäisillä ja -kokoisilla yrityksillä on toimialasta riippuen hieman erilaisia tietosuojaan liittyviä haasteita. Yrityksen toiminta voi jo sinällään sisältää tietosuojaa uhkaavia riskejä. Ajasta ja paikasta riippumaton työ on lisääntynyt, palveluita ulkoistetaan ja monia sovelluksia käytetään pilvipalveluina. Myös yhteistyö toisten yritysten kanssa voi olla riski tietosuojalle. Suurilla yrityksillä tietosuoja-asiat ja -käytänteet voivat olla paremmin ymmärrettyjä. Suuret yritykset ovat kuitenkin paremmin tunnettuja ja saattavat siksi joutua kohdistettujen hyökkäysten kohteiksi. (Yritysten rikosturvallisuus 2012: Riskit ja niiden hallinta 2012, 23–25.)

Nuorissa yrityksissä keskitytään enemmän liiketoiminnan käynnistämiseen, eikä tietojen suojaamineen ole niin paljoa resursseja käytettävissä. Kustannuksista säästämiseksi turvaudutaan usein ilmaispalveluihin, kuten Googlen kalenteriin ja sähköpostiin tai tiedostojen tallentamiseen Dropboxiin. Amerikkalaisina palveluina ne eivät takaa Suomen lainsäädännön edellyttämää tietosuojaa ja muun muassa mainitut palvelut ovat Yhdysvaltojen kansallisen turvallisuusviraston (NSA) seurannan piirissä. (Lappalainen 2013, 9.)

Liiketoiminnassa runsaasti lisääntyneen tiedon määrä johtaa helposti tietosuojaa uhkaaviin tilanteisiin. Tietojen varastointitarve sekä pyrkimys kustannussäästöihin ja tehokkuuteen voi johtaa joidenkin toimien ulkoistamistarpeeseen. Esimerkiksi IT-ylläpidon, talouspalveluiden tai asiakasrekisterin ulkoistaminen voi olla liiketoiminnan kannalta edullinen ja houkutteleva ratkaisu. Henkilötietojen käsittelyn ulkoistaminen etenkin Suomen ulkopuolelle vaatii ulkoistavalta organisaatiolta tarkkuutta ja huolellisuutta, jotta rekisteröityjen yksityisyyden suoja on turvattu. Ulkoistamisen tietoturvan hallinta onkin yksi merkittävä yrityksen tietoturvan hallinnan osa. (Laaksonen ym. 2006, 239.)

Ajasta ja paikasta riippumaton työ on lisännyt suosiotaan. Yhä useammassa yrityksessä työt seuraavat työntekijän mukana kotiin tai vapaa-ajalle. Tämä on mahdollista kannettavan tietotekniikan sekä pilvipalveluissa kaikkialla käytettävissä olevien tietojen ja sovellusten turvin. (Rousku 2013, 12.) Tällainen työskentely on lisännyt tie-

tosuojaan liittyvien riskien määrää. Muun muassa liikkuvassa työssä suosittujen kannettavien laitteiden tietoturva on usein heikosti toteutettu, jolloin virukset ja haittaohjelmat pääsevät helposti laitteeseen. Sen vuoksi verkkorikolliset ovat yhä kiinnostuneempia kannettavista laitteista. (Vuoden 2010 merkittävimmät tietoturvariskit 2010.) Viestinnässä ja verkkotyöskentelyssä saatetaan käyttää avoimia, suojaamattomia verkkoyhteyksiä. (Liikkuva työ: Liikkuvan työn tietoturva n.d., 1.)

Liiketoiminnan ja tietojärjestelmien kehittäminen organisaatiossa sisältää myös tietosuojariskejä. Valittaessa uusia järjestelmiä tai palveluntarjoajia on pyrittävä huolehtimaan, että järjestelmät täyttävät tietoturvallisuuden osalta lainvaatimukset. (Salminen 2009, 123.) Erilaiset paikasta riippumattomat verkon kautta käytettävät pilvipalvelut kasvattavat suosiotaan myös henkilötietojen käsittelyssä. Yrityksen ei tarvitse tallentaa tietoa yrityksen tietokoneille, ja verkossa olevat ohjelmistot ja tiedot ovat missä tahansa helposti niiden saatavilla, jotka niitä tarvitsevat. Pilvipalveluissa tiedon tallennuspaikka voi samalla palveluntarjoajalla vaihdella maasta toiseen. Tämä sisältää tietosuoja- ja tietoturvariskejä erityisesti silloin, kun tietojen tallennuspaikka sijaitsee Euroopan Unionin tai Euroopan talousalueen ulkopuolella. Sovellettavat lait valikoituvat tietojen tallennusmaan mukaan, jolloin yksityisyyden suoja voi olla heikommin turvattu kuin Suomen lainsäädäntö edellyttäisi. Sovellettavaksi tulevasta lainsäädännöstä voidaan yleensä sopia erikseen. (Castrén 2013.)

5 Tutkimuksen lähtökohdat ja toteutus

Tutkimus sai alkunsa projektityön jatkumona samalle toimeksiantajalle. Projektin sisältöä suunniteltaessa tuli ilmi useita tutkittavia aiheita ja ideoita. Aluksi opinnäytetyön aiheeksi valikoitui tietoturvalainsäädännön tunteminen jyväskyläläisten toimijoiden keskuudessa. Tietoturvalainsäädännön laajuuden vuoksi aihe rajattiin koskemaan vain asiakkaiden tietojen suojaamista. Tässä tutkimuksessa tarkasteltiin jyväskyläläisten toimijoiden tietämystä tietosuojalainsäädännön tietojen suojaamisvelvoitteista ja sen vaikutusta tietoturvasta huolehtimiseen. Tulosten myötä oli tarkoitus saada viitteitä siitä, voidaanko lainsäädännön korostamisen kautta motivoida

toimijoita huolehtimaan tietoturvasta ja onko tietoturvakoulutuksessa siten tarpeen korostaa lain vaatimuksia. Vastauksia haettiin seuraaviin kysymyksiin:

- Miten hyvin organisaatioissa tunnetaan henkilöasiakkaiden kannalta merkittävien tietosuojasäännösten tietojen suojaamisvelvoitteet syksyllä 2013?
- Vaikuttaako tietojen suojaamisvelvoitteiden tunteminen halukkuuteen huolehtia tietoturvasta?

Tutkimuksen teoriaviitekehys muodostui tietosuojalainsäädännön tietoturvavelvoitteista ja sen edellyttämistä käytännön ratkaisuista esimerkkien muodossa. Teoriaosuudessa on selvitetty myös yritysten merkittävimmät tietosuojaa uhkaavat riskit.

Tutkimus suoritettiin syksyllä 2013, jolloin Jyväskylässä on toimipaikka 7298:lla liiketoiminnastaan arvolisäverovelvollisella ja työnantajina toimivalla toimijalla. Luvussa ovat mukana myös liikevoittoa tavoittelemattomat yhdistykset, mutta ei työnantajina olevia kotitalouksia. (Taulukot tilastossa: Toimipaikkalaskuri 2013.)

Tutkimuksen aineisto kerättiin verkkokyselyn avulla satunnaisotannalla valikoituneiden Jyväskylässä toimivien yksityisten ja julkisen sektorin toimijoilta. Kolmiosaisen kyselyn kysymykset laadittiin teoriaperustan pohjalta. Kyselyssä kysyttiin taustatietoja ja mitattiin tietosuojatietämystä sekä tietoturvatoimien kattavuutta. Kysymykset olivat enimmäkseen strukturoituja monivalintakysymyksiä, joissa olivat valmiit vastausvaihtoehdot. Muutamaan kysymykseen lisättiin vastaajalle mahdollisuus lisätä oma vaihtoehtonsa. Ennen kyselyn julkaisemista kyselylomakkeen sisältö ja rakenne hyväksytettiin ohjaavalla opettajalla sekä toimeksiantajalla. Kyselylomake myös testattiin ennen julkaisemista. Aineisto analysoitiin pääasiassa kvantitatiivisia menetelmiä käyttäen. Avoimen kysymyksen osalta vastauksia analysoitiin kvalitatiivisin menetelmin. Seuraavaksi käydään tarkemmin läpi tutkimusmenetelmän valintaa, tutkimusaineistoa ja sen keruutapaa, käsittelyä ja analysointia.

5.1 Tutkimusmenetelmät

Kvantitatiivista eli määrällistä tutkimusmenetelmää käytetään, kun ilmiö tunnetaan ja halutaan kuvailla numeerisesti asioita tai niiden välistä suhdetta. Esimerkiksi, kun halutaan selvittää, miten paljon jokin asia vaikuttaa toiseen asiaan. Määrällinen tutkimus ei ole kiinnostunut poikkeavuuksista vaan pyrkii yleistämään. Tavoitteena on esimerkiksi löytää syy-seuraus -suhde ja yleistää, miksi näin on. (Vilkka 2005, 49–50.)

Tässä opinnäytetyössä käytetään kvantitatiivista tutkimusmenetelmää. Kvantitatiivinen tutkimus sopii tutkimukseen, jossa vertaillaan tietosuojatietämystä erilaisten yritysten välillä ja etsitään mahdollista yhteyttä lainsäädännön tuntemisen ja sen vaatimusten täyttämisen välillä. Kvantitatiivisin tutkimusmenetelmin pyritään yleistämään, onko tietosuojalainsäädännön asettamien tietojen suojaamisvaatimusten tuntemisella yhteyttä tietoturvan huolehtimishalukkuuteen. Vaikka kyselystä saadaan myös kvalitatiivista aineistoa, on tutkimusote kvantitatiivinen. Kvalitatiivisessa tutkimusotteessa aineiston keruu tapahtuu yleensä haastattelemalla. Tässä tutkimuksessa havaintoaineisto kerätään verkkokyselyllä. Aineistoa analysoitiin pääosin kvantitatiivisin menetelmin, mutta myös kvalitatiivista tutkimusotetta hyödyntäen.

5.2 Tutkimusaineiston keruu ja analysointi

Tutkimus toteutettiin kyselytutkimuksena, jolloin havaintoaineiston keruu tapahtui kyselylomakkeen avulla. Kohderyhmänä olivat Jyväskylässä toimivat yritykset ja organisaatiot, joita oli reilut 7000 toimijaa. Lähes kaikki (99,8 % Jyväskylän toimijoista on PK-yrityksiä eli alle 250 henkilöä työllistäviä yrityksiä). Kaikista yrityksistä selvästi eniten (90 %) on 0–9 hengen mikroyrityksiä. Pieniä 10–49 henkilön yrityksiä on vajaa kymmenesosa (8,7 %). Henkilöstömäärän kasvaessa yritysten lukumäärä vähenee. Keskisuurten (50–249 henkilön) sekä suurten (yli 250 henkilön) yritysten osuus kaikista yrityksistä on yhteensäkin vain murto-osa (1,5 %). Päätoimialoista suurimpana ryhmänä oli tukku ja vähittäiskauppa, johon sisältyy moottoriajoneuvojen ja moottoripyörien korjaus. Toimialan osuus oli viidennes kaikista toimijoista (18 %). Suurin osa

yrityksistä on yksityisessä omistuksessa, mutta Jyväskylässä on myös kunnan ja valtion alaisia toimijoita. (Taulukot tilastossa: Toimipaikkalaskuri 2013.)

Tutkittavien joukko oli melko suuri, mutta verkkokysely mahdollistaa kokonaistutkimuksen suhteellisen suurestakin perusjoukosta. Ongelmana tämän tutkimuksen osalta oli kuitenkin kaikkien yritysten sähköpostiosoitteiden saatavuus sekä osoitetietojen hakemisen hitaus. Sen vuoksi päädyttiin otostutkimukseen. Tutkimukseen valittiin 1000 tutkittavaa Kauppalehden yritysrekisteristä yksinkertaisella satunnaisotannalla.

Tutkimusaineisto kerättiin verkossa vastattavalla kyselylomakkeella. Verkkokyselyä puolsivat ajan säästäminen ja virheitten minimointi vastausten tallentamisessa. Verkkolomakkeen vastaukset tallentuivat suoraan tietojärjestelmään, jolloin virhealtis tietojen syöttövaihe jäi kokonaan pois. Lisäksi verkkokysely on edullinen toteuttaa, kun tulostus- ja postituskustannukset jäävät pois. Kyselyn toteuttaminen internetissä on myös vastaajalle eduksi. Vastaaminen tapahtuu anonyymisti ja silloin, kun se vastaajalle parhaiten sopii.

Mittarit ja muuttujat

Kyselytutkimuksessa mittareita ovat kyselyn kysymykset ja väittämät, joilla tutkittavaa ilmiötä pyritään mittaamaan. Mittarit voi rakentaa itse tai tutkimuksessa soveltaa valmiita mittareita, joiden toimivuus omaan tutkimukseen on varmistettava. Mittareiden valinnassa ja rakentamisessa on syytä olla erityisen huolellinen, sillä tehtyjä virheitä ei voida enää korjata analyysimenetelmillä, ja sillä on vaikutuksensa myös tutkimuksen johtopäätösten luotettavuuteen. (Vehkalahti 2008, 17.)

Kruger ja Kearney (2005, 3–4) ovat kehittäneet tietoturvatietoisuuden mittaukseen soveltuvan menetelmän, jossa hyödynnetään sosiaalipsykologiaa. Siinä arvioitavana ovat ihmisen tunteet, tiedot ja käyttäytyminen, jotka kaikki vaikuttavat ihmisen toimintaan eri asioiden suhteen. Kruger ja Kearney katsoivat, että tietoturvatietoisuutta voidaan mitata tietämystä, asenteita ja käyttäytymistä mittaamalla. He käyttivät tietämyksen ja asenteiden mittaamiseen valintakysymystä, jossa vastausvaihtoehtoina olivat: tosi, epätosi ja en tiedä. Käyttäytymisen mittaamisessa vastausvaihtoehdot

olivat: tosi ja epätosi. He keskittyivät mittaamaan tietämystä, asenteita ja käyttäytymistä kuudelta eri osa-alueelta käyttäen analysoinnissa painotettuja keskiarvoja. Tietämyksen tason määrittelyssä asteikkona oli 0 - 100 % ja tuloksia tulkittiin kolmiportaisella asteikolla.

Tässä tutkimuksessa tutkittiin tietojen suojaamisvelvoitteiden tietämystä ja sen vaikutusta tietoturvasta huolehtimiseen Krugerin ja Kearneyn (2005) mallia hyödyntäen. Mallia on käytetty hieman soveltaen, ja asenteiden mittaaminen oli vähäistä. Asenteita mittaamalla saataisiin tietoa siitä, miten ihmiset suhtautuvat oppimaansa tai tietämäänsä. Tässä tutkimuksessa kuitenkin pyrittiin selvittämään mahdollinen yhteys tietojensuojaamisvelvoitteiden tuntemisen ja käytettyjen tietoturvatoimien välillä. Vaikka asenteet vaikuttavat siihen, miten tietämys lopulta vaikuttaa käyttäytymiseen, ei sen laajamittaisella mittaamisella saataisi tässä tutkimuksessa merkittävää lisätietoa.

Haasteita kyselyn laatimiselle asettivat alati lisääntyvien kyselyiden aiheuttama vastastausväsymys. Sen vuoksi huomiota kiinnitettiin vastaamisen helppouteen ja kyselyn pituuteen. Kysymysten määrä pyrittiin pitämään mahdollisimman vähäisenä, mutta kysymykset kuitenkin riittävän tarkkoina, jotta vastauksista voitaisiin tehdä päteviä johtopäätöksiä. Kysymykset pyrittiin jättämään lyhyiksi niiden selkeyden kuitenkaan kärsimättä.

Kysely laadittiin teorian pohjalta kolmiosaiseksi. Ensimmäisessä osassa kysyttiin taustatietoja, toinen osa mittasi tietämystä tietosuojalainsäädännön suojaamisvelvoitteista, ja kolmannessa osassa kysyttiin käytössä olevista tietoturvatoimenpiteistä. Tietosuojatietämystä mittaavissa kysymyksissä käytettiin strukturoituja kysymyksiä. Toisin kuin Krugerin ja Kearneyn (2005) mallissa suurin osa kysymyksistä oli monivalintakysymyksiä. Monivalintakysymysten vastausvaihtoehdot voidaan tulkita niin, että valittu vaihtoehto tarkoittaa kyllä-vastausta ja valitsematta jättäminen tarkoittaa ei-vastausta. Näin vastausvaihtoehdoista jäi pois ”en tiedä” -vaihtoehto.

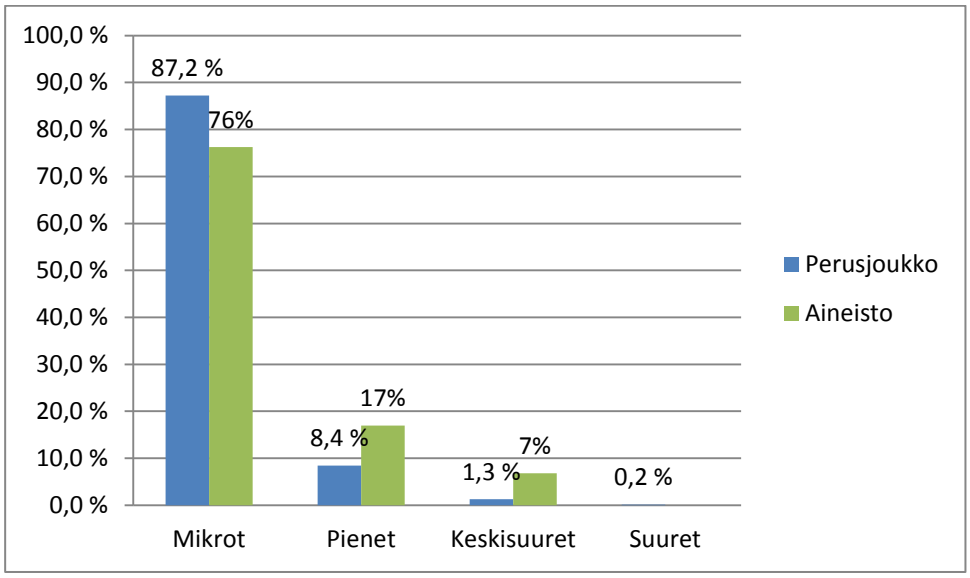
Tietoturvaan panostamista mitattiin käytössä olevien menetelmien määrää ja laatua mittaamalla. Myös näitä kysyttiin strukturoiduilla kysymyksillä. Kahdessa kysymyk-

sessä käytettiin strukturoidun ja avoimen kysymyksen yhdistelmää. Näin vastaajalle annettiin mahdollisuus lisätä vastausvaihtoehtoihin sellainenkin vaihtoehto, joka mahdollisesti puuttui. Kyselyn lopussa oli avoin kysymys, jossa vastaajalla oli mahdollisuus vielä täsmentää jotain vastausta ja kertoa vapaalla sanalla tietojen suojaamisvelvoitteen vaikutuksesta yrityksen tietoturvatoimiin. Kyselystä saatiin sekä kvantitatiivista että kvalitatiivista aineistoa.

Aineisto, sen käsittely ja analysointi

Tutkimuksen aineisto kerättiin 1.11. – 14.11.2013 verkkokyselyllä, joka toteutettiin Webropol-sovelluksella. Kutsu tutkimukseen lähetettiin sähköpostilla 1000:lle otokseen valikoituneelle jyväskyläläiselle toimijalle. Mukaan liitettiin saatekirje (liite 2). Heistä kolme ilmoitti, ettei osallistu tutkimukseen ja kaksi ilmoitti, että on lopettanut liiketoimintansa tai työskentelynsä yrityksessä, jolle sähköpostiosoite kuului. Kutsuista 263 ei mennyt perille. Luultavasti sähköpostiosoite ei ollut enää käytössä. Siten netto-otokseksi tuli 732 toimijaa.

Vastausaikaa annettiin ensin viikko. Vastauksia kerääntyi ensimmäisellä kierroksella 35 kappaletta. Ensimmäiseen kutsuun vastaamatta jättäneille lähetettiin uusintapyyntö saatekirjeen kera (liite 3). Uusintapyyntöä ei lähetetty heille, jotka olivat aiemmin ilmoittaneet kieltäytyvänsä tutkimuksesta. Uusintapyynnön jälkeen tuli vielä 31 vastausta. Tutkimukseen osallistui lopulta 66 toimijaa. Palautusprosentiksi muodostui 9 % suhteutettuna netto-otokseen. Aineistosta poistettiin ne vastaukset, joissa ilmoitettiin, ettei käytössä ole henkilörekisteriä eikä työtehtävät sisällä henkilötietojen käsittelyä. Aineistoon kulumattomien vastausten poiston jälkeen vastauksia jäi 59 kappaletta, jolloin vastausprosentiksi jäi 8 % ja kadoksi tuli 92 %. Tulosta voidaan pitää heikkona, vaikkakin nykyisiin vastausprosentteihin nähden aineistoa kertyi yllättävän hyvin.



Kuvio 3. Perusjoukon ja aineiston jakautuminen

Kuviosta 3 nähdään, ettei aineisto ole sisäiseltä rakenteeltaan kovin edustava. Mikroyritykset ovat aineistossa hieman aliedustettuina, kun taas pienten ja keskisuurten yritysten osuus on tutkimusaineistossa perusjoukkoa selvästi suurempi. Perusjoukossa suuria yrityksiä on vain murto-osa. Tutkimuksessa niitä ei ole mukana yhtään.

Aineisto poikkeaa selvästi perusjoukosta myös toimialojen suhteen. Perusjoukossa suurinta päätoimialaa viidenneksen osuudellaan (18 %) edustaa tukku- ja vähittäiskauppa, johon sisältyvät moottoriajoneuvojen ja moottoripyörien korjaus. Aineistossa kyseinen toimiala oli erittäin heikosti (3,4 %) edustettuna. Perusjoukossa muu palvelutoiminta kattoi kymmenyksen (10 %) kaikista toimialoista. Aineistoin päätoimialoista se kahmaisi viidenneksen (17 %) ja oli siten selvästi yliedustettuna perusjoukkoon nähden. Myös terveyspalvelut ovat aineistossa selvästi yliedustettuina. Perusjoukossa toimialan osuus on kahdeskymmenesosa (5 %), kun aineistossa se on viidennes (14 %). Muiden toimialojen kohdalla erot eivät olleet yhtä selkeät.

Vastaukset tallentuivat suoraan tilastollisin menetelmin käsiteltävään muotoon, mutta koska Webropol-sovellus ei ole kovinkaan monipuolinen, käytettiin tarkemmassa analysoinnissa Aki Taanilan laatimaa Excelin apuohjelmaa Tilastoapua. Lisäksi analysoinnissa käytettiin SPSS -tilasto-ohjelmaa. Taanilan Tilastoapu oli vapaasti ladatta-

vissa internetistä. Muuttujia muodostui yhteensä 77 kappaletta, joista taustamuuttujia oli seitsemän. Aluksi aineisto käytiin läpi tarkastelemalla frekvenssijakaumia eli suoria jakaumia.

Kyselyn avulla saatua aineistoa analysoitiin tilastollisin menetelmin. Kyselyssä oli yksi avoin kysymys, jonka vastausten analysoinnissa käytettiin kvalitatiivista sisältöanalyysiä. Tutkimuskysymyksiin haettiin vastauksia käyttämällä yhteenvetotaulukoita ja ristiintaulukointia. Yksittäisten muuttujien arvojen vaihtelua tarkasteltiin yhteenvetotaulukoiden ja frekvenssijakaumien avulla. Ryhmien välisiä eroja ja riippuvuuksia etsittiin ristiintaulukointien avulla.

Tietosuojatietämystä tarkasteltiin muodostamalla sitä mittaavista muuttujista summamuuttuja ja koodaamalla muuttujat niin, että mitä lähempänä muuttujien keskiarvo on arvoa 3, sen suurempi on tietämys. Tietämystason arvioinnissa käytettiin Krugerin ja Kearneyn (2005, 6) määrittelemää kolmiportaista asteikkoa, jossa tietämystaso on:

- hyvä, kun tulos 80 - 100 %
- kohtalainen, kun tulos on 60 - 79 %
- heikko, kun tulos on alle 60 %

Keskiarvolukuina tarkasteltuna tietämystaso on:

- hyvä, kun keskiarvo on 2,4 - 3,0
- kohtalainen, kun keskiarvo on 1,8 - 2,39
- heikko, kun keskiarvo on alle 1,8.

Aineistoon muodostettiin uusi muuttuja ”Tietämystaso”, jota käytettiin ristiintaulukoinnissa etsittäessä eroavaisuuksia eri tietämystasojen välillä käytettyjen tietoturvatoimien suhteen. Muuttujan arvoiksi annettiin 1, 2 ja 3. Arvo 1 vastasi heikkoa tietämystasoa, 2 kohtalaista ja 3 hyvää tietämystasoa. Vastaukset luokiteltiin tietämystason mittaamisesta saatujen keskiarvojen mukaan edellä mainittuihin luokkiin.

Tutkijan olettamus oli, että isommissa yrityksissä lainsäädännön velvoitteet ovat paremmin tunnetut ja myös tietoturvasta huolehtiminen on monipuolisempaa ja siihen on haluttu panostaa tehokkaammin. Vastaukset luokiteltiin yritysten koon mukaan neljään ryhmään (mikro-, pienet, keskisuuret ja suuret yritykset) ja verrattiin ristiintaulukoinnin avulla tietosuojatietämyksestä saatuja keskiarvoja kokoluokkien välillä. Näin etsittiin ryhmien välisiä eroja tietosuojatietämyksessä ja tietoturvakeinojen ja -menetelmien käytössä. Toimialojen välisiä eroja tietämyksessä tarkasteltiin ristiintaulukointia hyväksi käyttäen.

5.3 Tutkimuksen luotettavuuden arviointi

Kvantitatiivisen tutkimuksen luotattavuutta arvioidaan reliabiliteetin ja validiteetin kautta. Tutkimuksen validiteettia voidaan pitää hyvänä, kun tutkimuksen kohderyhmä on oikea ja kysymykset ovat oikein valittu tai rakennettu. Reliabiliteetti on onnistunut, kun tutkimukset tulokset eivät ole sattumanvaraisia, vaan toistamalla tutkimus saataisiin samat tulokset. (Kananen 2010, 128.)

Validiteettia voidaan tarkastella ulkoisen validiteetin ja sisältövaliditeetin kannalta. Määrällisessä tutkimuksessa pyritään yleistämään. Ulkoinen validiteetti mittaa tutkimustulosten yleistettävyyttä eli sitä, ovatko tutkimustulokset yleistettävissä koko populaatiota koskevaksi. Tällöin tutkittavista saatujen tutkimustulosten täytyy vastata koko populaatiota. (Kananen 2010, 129.)

Tässä tutkimuksessa käytettiin otantamenetelmänä yksinkertaista satunnaisotantaa. Kaikilla ei ollut sähköpostiosoitetta Kauppalehden yritysrekisterissä, joten tosiasiassa otokseen valikoituivat vain sähköpostiosoitteen rekisteriin ilmoittaneet. Tämän vuoksi otantakehikko poikkeaa perusjoukosta ja otos on näin ollen vino. Sähköpostiosoitteensa ilmoittamatta jättäneiden joukossa ovat perusjoukkoon kuulumattomia muun muassa omaa metsää metsäyhtiölle myyviä yksityishenkilöitä. Näitä ei otokseen valittu. Myös monet taksi- ja kuorma-autoyrittäjät sekä parturi-kampaamo ja terveyspalvelu-yrittäjät eivät ole ilmoittaneet sähköpostiosoitettaan. Otokseen valikoitui tutkit-

tavia edellä mainituilta toimialoilta, mutta sähköpostiosoitteiden puuttumisen vuoksi vähemmän kuin muutoin olisi valikoitunut.

Tutkimustulosten yleistettävyyden kannalta otoskoolla on oma merkityksensä. Pieni otos voi antaa hyvinkin paljon perusjoukosta poikkeavia tuloksia, eikä tuloksia voida yleistää perusjoukkoon. Vastaajien määrä jäi niin vähäiseksi, ettei tuloksia voida varauksetta yleistää koko perusjoukkoa koskevaksi. Etenkin julkisen sektorin osalta tulokset voivat vaihdella suurestikin perusjoukon kanssa.

Kuten aiemmin todettiin, poikkeaa vastanneiden joukko jonkin verran koko populaatiosta. Erot olivat suurimmat toimialojen kohdalla. Poikkeamaa oli hieman myös yrityskokojen suhteen. Pienet ja keskisuuret toimijat olivat havaintoaineistossa hieman yliedustettuina. Myöskään tältä osin tutkimuksen tuloksia ei voida varauksetta yleistää koko populaatiota koskevaksi.

Sisältövaliditeetti tarkastelee käytettyjen mittareiden oikeellisuutta eli sitä, onko kysytty oikeita asioita. Kyselytutkimuksessa mittareiden eli kyselyn kysymysten onnistuminen vaikuttaa paljon tutkimuksen luotettavuuteen. Kysymykset pitäisi rakentaa niin, että niillä saadaan vastaus tutkimusongelmaan. Väärin valitut mittarit eivät voi antaa oikeanlaista tietoa, jolloin tutkimuksen luotettavuus kärsii. (Vehkalahti 2008, 17.)

Kysymykset laadittiin niin, että tuloksista kävisi ilmi se, miten hyvin lain velvoitteet tietojen suojaamisesta tiedetään sekä miten tehokkaasti tietojen suojaamiseen on haluttu panostaa. Tietämyksen mittaamiseen sopivat hyvin strukturoidut kysymykset, joita kyselyn kysymykset enimmäkseen ovat (Taanila 2012, 23). Tietosuojatietämystä mittaavat kysymykset on johdettu teoriapohjasta, joka perustuu tietosuojalainsäädäntöön. Näin kysymyksillä saatiin mitattua, miten hyvin tietosuojalainsäädännön tietojen suojaamisvelvoitteet tiedetään.

Tosiasioiden mittaamiseen sopivat hyvin myös strukturoidut kysymykset, joita tietoturvakysymykset suurelta osaltaan ovatkin (Taanila 2012, 22). Valmiit vastausvaihtoehdot saattavat kuitenkin jättää käytössä olevista tietoturvakeinoista ja menetelmistä jotain havaintoaineiston ulkopuolelle. Sen vuoksi käytössä olevia tietoturvamene-

telmiä koskeva kysymys on toteutettu strukturoidun ja avoimen kysymyksen yhdistelmänä, jossa valmiiden vastausvaihtoehtojen jälkeen on yksi avoin kysymys. Myös kysymyksessä tietoturvamenetelmien valintaan vaikuttaneista tekijöistä on sisällytetty vastaajalle mahdollisuus lisätä listan ulkopuolinen tekijä.

Tietoturvaan panostamista mitattiin siihen käytettävien menetelmien ja keinojen monipuolisuudella. Tietoturvaan panostamista olisi voinut mitata myös siihen käytettyä rahamäärää mittaamalla. Se ei kuitenkaan antaisi kovinkaan hyvää käsitystä siitä, miten tehokkaasti tai laajasti tietoturvaan on haluttu panostaa. Tietoturvatasoa voidaan nostaa myös hyvin edullisin ja jopa maksuttomin keinoin.

Kysymykset hyväksytettiin sekä toimeksiantajalla että ohjaavalla opettajalla, jotka arvioivat myös lomakkeen toimivuutta ja sen tarkoituksenmukaisuutta. Valmis kysely esitestattiin. Esitestauksella varmistettiin kysymysten ymmärrettävyys ja toimivuus sekä minimoitiin mahdolliset väärinkäsitykset. Kyselyn lopussa oli avoin kysymys, jossa vastaajalla oli mahdollisuus tarkentaa vastauksia. Sen tarkoituksena oli parantaa havaintoaineiston luotettavuutta.

Reliabiliteetti tarkoittaa tutkimustulosten pysyvyyttä eli sitä, että tuloksissa ei ole sattuman mahdollisuutta. Toistamalla tutkimus samanlaisissa oloissa, voidaan tulosten sattumanvaraisuus sulkea pois, jos tulokset olisivat samanlaiset kuin edelliset tulokset. Silloin voidaan sanoa, että reliabiliteetti on kunnossa. (Kananen 2010, 128–129.)

Kysymysten ja kyselylomakkeen esitestauksella pyrittiin varmistamaan kysymysten ymmärrettävyys ja selkeys. Kysymyslomakkeessa annettiin selvät vastausohjeet, joilla pyrittiin varmistamaan, että kyselyyn vastaaminen olisi helpompaa ja että kaikki ymmärtäisivät vastaamisen samalla tavalla.

Koska kysely suoritettiin verkkokyselynä, ei tutkijan läsnäolo voinut vaikuttaa vastauksiin. Toisaalta tutkittava pystyi vastamaan kyselyyn yksin, jolloin hän on voinut etsiä tietoa internetistä. Sen vuoksi tietosuojatietämyksen osalta tulokset voivat näyttää todellisuutta paremmilta. Toisaalta vastaaminen anonyyminä rohkaisee vastaamaan rehellisemmin. Kyselyn aihe oli hyvin ajankohtainen ja ehkä jopa arka. On hyvin

mahdollista, että vastaajat ovat kyselyn edetessä alkaneet pitää jo kysyttyjä asioita tärkeinä toiminnassaan. Se on voinut vaikuttaa vastauksiin kysymyksessä, jossa vastaajia pyydettiin arvioimaan tiettyjen asioiden merkitystä heidän tietoturvatoimien valintaan.

Tutkimuksen luotettavuutta lisää riittävän suuri havaintoyksiköiden määrä. Riittävän suuren havaintoaineiston kerääminen on erittäin haastavaa lisääntyneiden kyselyiden aiheuttaman vastausväsymyksen vuoksi. Kysely pyrittiin laatimaan helposti vastattavaksi ja ymmärrettäväksi. Vastaajia pyrittiin motivoimaan vastaamisesta saatavalla hyödyllä ja korostamalla vastaajien tärkeää roolia tutkimuksen onnistumisessa. Kaikesta huolimatta vastausprosentti jäi niin alhaiseksi, ettei tutkimuksen tuloksia voida pitää kovinkaan luotettavina koko populaation suhteen. Tulokset pätevät kuitenkin tutkimukseen osallistuneiden joukossa.

Toistettavuus lähitulevaisuudessa toisi ehkä samansuuntaisia tuloksia. On kuitenkin mahdollista, että kysely on herättänyt tutkittavia pohtimaan asioita. Se on saattanut lisätä tutkittavien tietämystä ja vaikuttaa myös toimintaan. Joka tapauksessa lähivuosina tietosuojalainsäädäntö on uudistumassa, ja se tuo joitakin muutoksia tietojen suojaamisvelvoitteisiin liittyen. Uudistuvan tietosuojalainsäädännön laajempia tietoturvavaatimuksia ei kyselyssä voitu huomioida, koska ne eivät ole vielä voimassa. Myös yhteiskunta, liiketoimintaympäristö ja käsitys yksityisyydestä muuttuu koko ajan. Tietoturvaa ja -suojaa uhkaavia uusia tekijöitä saattaa myös ilmetä. Tekniikan kehittyessä tietoturvakeinot ja menetelmätkin muuttuvat. Muuttuva Toimintaympäristön muutos, kasvava tietoisuus yksityisyydestä sekä lisääntyvät tietosuoja- ja tietoturvaloukkaukset tulevat todennäköisesti lisäämään toimijoiden halua kehittää toimintaansa paremmin ajan haasteita vastaavaksi. Pidemmällä aikavälillä toistettuna tutkimus todennäköisesti antaisi aivan toisenlaisia tuloksia.

6 Tulokset

Tässä tutkimuksessa oli tarkoitus selvittää, miten hyvin jyväskyläläiset toimijat tuntevat henkilöasiakkaiden kannalta merkittävien tietosuojasäännösten tietojen suojaa-

misvelvoitteet. Selvitettävänä oli myös se, vaikuttaako tietojen suojaamisvelvoitteiden tunteminen halukkuuteen huolehtia tietoturvasta. Tutkimustuloksilla pyritään löytämään vastaukset edellä mainittuihin kysymyksiin sekä vastaamaan tutkimusongelmaan: Voidaanko tietoturvahalukkuuteen motivoida lainsäädännön tuntemusta lisäämällä? Siten saadaan käsitys siitä, onko koulutuksissa tarvetta korostaa enemmän lainsäädännöstä lähteviä tietojen suojaamisvelvoitteita.

Tutkimustuloksia käsitellään neljässä alaluvussa. Ensimmäisessä alaluvussa käydään läpi vastaajien taustatietoja, joiden perusteella muita tuloksia tarkastellaan. Toisessa alaluvussa selvitetään tutkimustulokset vastaajien tietosuojatietämyksestä ja sen tasosta. Kolmas alaluku käsittelee toimijoiden käyttämiä tietoturvatoimia, ja neljäs alaluku kertoo lainsäädännön sekä muiden seikkojen vaikutuksista tietoturvatoimiin. Tulosten selvittämisessä käytetään jonkin verran graafisia kuvioita, koska kuviot selittävät pitkälti itse itseään ja antavat useimmille lukijoille tuloksista taulukkoa nopeammin ymmärrettävän kuvan. Aivan kaikkia lukujen taakse kätkeytyviä asioita ei pyritä kirjoittamaan auki, koska se voisi nopeasti tehdä tekstistä raskaslukuisen ja pitkän. Neljännessä alaluvussa arvioidaan tutkimuksen luotettavuutta. Kysymykset ovat kokonaisuudessaan liitteessä 1.

6.1 Vastaajien taustatiedot

Kyselyn ensimmäisessä osassa kysyttiin vastaajien taustatietoja. Taustatietojen avulla haluttiin selvittää, miten hyvin otos vastaa populaatiota ja että vastaaja kuuluu varmasti tutkittavien joukkoon. Taustatietoja tarvittiin myös tulosten vertailuun eri vastaajaryhmien kesken.

Kyselyyn osallistui 66 jyväskyläläisen toimijan edustajaa. Kaikista vastaajista seitsemällä (11 %) ei ollut käytössä henkilörekisteriä eivätkä työtehtävät sisältäneet henkilötietojen käsittelyä, joten heidän vastauksiaan ei ole huomioitu kyselyn tuloksissa. Lopullinen aineisto muodostui 59 vastaajan vastauksista. Näitä vastaajia käsitellään tästä eteenpäin tutkimukseen osallistuneina. Heistä valtaosa oli yksityiseltä sektorilta (97 %), julkisen sektorin edustajia oli vain murto-osa (3 %). Vastaajia oli 18 toimialal-

ta, joista suurimpana muu palvelutoiminta viidenneksen osuudella (17 %). Taulukosta 1 nähdään vastaajien jakautuminen toimijoiden kokoluokkien suhteen. Kokoluokittelussa on käytetty Euroopan Unionin yrityskoon määritelmiä henkilöluvun mukaan, mutta ei ole huomioitu liikevaihtoa.

Taulukko 1. Vastaajat toimijan koon mukaan

N	59
	%
Mikro	76
Pieni	17
Keskisuuri	7
Suuri	0
Yhteensä	100,0

Mikroyrityksiä oli selvästi eniten. Kolme neljästä (76 %) tutkimukseen osallistuneesta edusti 0-9 hengen mikroyritystä. Kokoluokan kasvaessa tutkimukseen osallistuneiden määrä vähenee ja suuria yli 249 hengen yrityksiä ei ole tutkimuksessa mukana lainkaan (0 %). Kuten jo aiemmin aineiston kuvailussa selvisi, ovat mikroyritykset aliedustettuina, kun taas pienet ja keskisuuret yritykset ovat selvästi yliedustettuina.

6.2 Lainsäädännön tunteminen organisaatioissa

Kun halutaan selvittää toimijoiden tietotaso lainsäädännön tietojen suojaamisvelvoitteiden osalta, on luonnollista selvittää, miten paljon tutkittavat siitä tietävät. Tietosuojalainsäädännön tietojen suojaamisvelvoitteitten tuntemusta kysyttiin kysymyksillä, jotka koskivat tietojen suojaamisen yleisiä periaatteita ja vastuukysymyksiä. Kyselylomakkeella kysymykset oli muotoiltu väittämiksi, joihin täytyi valita yksi tai useampi sopiva vastausvaihtoehto.

Tietosuojakysymysten avulla kartoitettiin vastaajien tietotasoa kolmiportaiselle asteikolle jaettuna. Tuloksia käsiteltiin keskiarvolukuina, jossa maksimiarvo oli 3. Arvo 2,4 on hyvän tietotason alaraja ja 1,8 kohtalaisen alaraja. Sen alapuolelle jää heikko tietotaso. Tietosuojatietämystä kuvaavissa kuvioissa on merkitty punaisin viivoin tietotasojen raja-arvot hahmottamisen helpottamiseksi. Tietotasoja tarkastellaan toimijoiden kokoluokittain.

Tietoturvatoimien laajuuden ja tehokkuuden arviointi

Tietoturvatoimia ei tarvitse toteuttaa täydellä volyymilla, vaan lainsäädäntö määrittelee lähtökohdat ja perusteet, joiden mukaan toimijat voivat arvioida käytettävien tarpeellisten tietoturvatoimien laajuutta ja tehokkuutta. Arvioinnissa voidaan ottaa huomioon esiintyvät seikat eli käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, suojattavien tietojen laatu ja määrä, suojattavien tietojen ikä sekä tietojen merkitys yksityisyyden suojan kannalta. (L 22.4.1999/523, 38 §.)

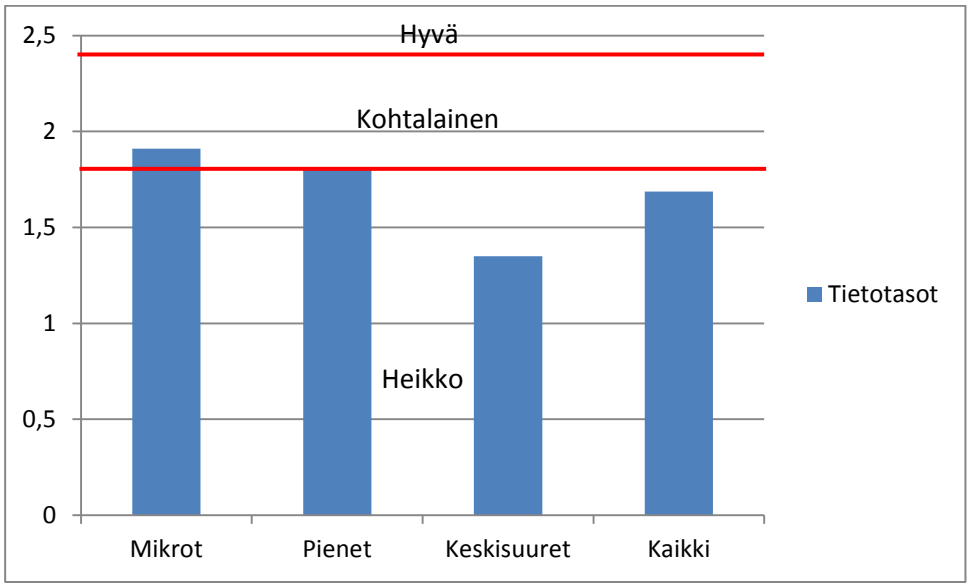
Tietoturvatoimien laajuuden ja tehokkuuden arviointiin vaikuttavista seikoista kysyttiin väittämäksi muotoillulla kysymyksellä, johon piti valita kaikki väittämään sopivat vaihtoehdot. Taulukosta 2 ilmenee, miten suuri osa eri kokoluokkien vastaajista oli pitänyt mainittua seikkaa tietoturvatoimien laajuutta ja tehokkuutta arvioitaessa vaikuttavana asiana. Taulukon viimeisessä sarakkeessa on prosenttiosuudet kaikista vastaajista yhteensä.

Taulukko 2. Tietoturvatoimien laajuuden ja tehokkuuden arvioimiseen vaikuttavat seikat

Toimijan koko	Mikrot	Pienet	Keskisuuret	Kaikki
N	45	10	4	59
	%	%	%	%
Käytettävissä olevat tekniset mahdollisuudet	78	90	25	76
Toimenpiteiden aiheuttamat kustannukset	51	40	25	48
Suojattavien tietojen laatu ja määrä	80	60	50	75
Suojattavien tietojen ikä	29	30	25	29
Tietojen merkitys yksityisyydelle	80	80	100	81

Tietoturvatoimien laajuuden ja tehokkuuden arvioimisessa huomioon otettavista seikoista parhaiten tiedettiin tietojen merkitys yksityisyyden suojan kannalta. Neljä viidestä (81 %) vastaajasta piti sitä harkintaan vaikuttavana seikkana. Suojattavien tietojen ikä oli tuntemattomin huomioon otettava tekijä. Vain vajaa kolmannes (29 %) kaikista vastaajista katsoi sen vaikuttavan tietoturvatoimien valinnassa. Toimijoiden kokoluokkien välillä oli havaittavissa joitakin eroja. Ero oli selvin käytettävissä olevien teknisten mahdollisuuksien kohdalla. Keskisuurista toimijoista vain neljännes (25 %) piti sitä harkinnassa huomioon otettavana seikkana, kun lähes kaikki (90 %) pienet toimijat pitivät seikkaa harkinnassa vaikuttavana. Selvä ero selittynee keskisuurten yritysten vähäisellä esiintyvyydellä tutkimusaineistossa, jolloin yksittäisen vastauksen vaikutus on suurempi.

Kuviosta 4 selviää toimijoiden tietotasot tietoturvatoimien laajuuden ja tehokkuuden arvioinnissa huomioon otettavista seikoista keskiarvolukuina kokoluokittain sekä yhteensä.



Kuvio 4. Tietotasot tietoturvatoimien laajuuden ja tehokkuuden arvioinnista

Yleisesti ottaen tietoturvatoimien laajuuden ja tehokkuuden arvioimisessa huomioon otettavista seikoista tiedettiin kohtalaisesti (1,69). Parhaiten arvioinnissa huomioon otettavat seikat tunnettiin mikroyrityksissä, jonka tietotaso oli kohtalainen (1,91) kuten myös pienten yritysten tietämystaso (1,8). Heikoimmin nämä seikat tunnettiin keskisuurissa yrityksissä, jonka tietämystaso jäi heikoksi (1,35).

Arkaluontoisten tietojen suojaaminen

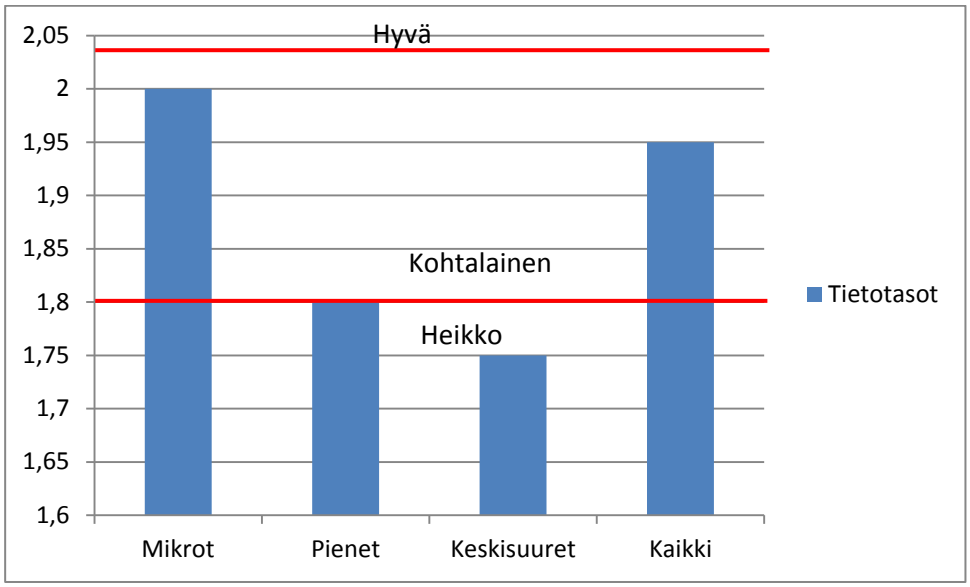
Arkaluontoisten tietojen suojaaminen vaatii enemmän huomiota kuin tavallisten tietojen, eikä taloudellisten resurssien puute saa olla esteenä tietojen suojaamiselle. (Voutilainen 2012, 318). Arkaluontoisten tietojen suojaamisesta kysyttiin väittämällä, johon annettiin kaksi oikeaa ja yksi väärä vastausvaihtoehto. Väittämä oli: Hyvin arkaluontoisten tietojen suojaaminen. Vastausvaihtoehdot: vaatii erityistä huolellisuutta, saa rasittaa yrityksen tai organisaation taloutta ja ei poikkea muiden tietojen suojaamisesta.

Taulukko 3. Arkaluontoisten tietojen suojaaminen

Toimijan kokoluokka	Mikrot	Pienet	Keskisuuret	Kaikki
N	45	10	4	59
	%	%	%	%
vaatii erityistä huolellisuutta	89	90	75	88
saa rasittaa yrityksen tai organisaation taloutta	29	10	25	25
poikkea muiden tietojen suojaamisesta	82	80	75	81

Taulukosta 3 voidaan tarkastella, miten hyvin arkaluontoisten tietojen suojaaminen on ymmärretty. Siitä ilmenee, että lähes kaikki (89 %) ovat tietoisia arkaluontoisten tietojen suojaamisen huolellisuusvaatimuksesta, mutta vain neljännes tiesi, etteivät taloudelliset resurssit saa rajoittaa arkaluontoisten tietojen suojaamista. Suurin osa (81 %) oli myös tiedostanut, että arkaluontoisten tietojen suojaaminen poikkeaa tavallisten tietojen suojaamisesta. Jopa viidesosa vastaajista arveli, ettei arkaluontoisten tietojen suojaaminen poikkea mitenkään tavallisten tietojen suojaamisesta.

Toimijoiden kokoluokkien välillä ei ole suuria eroja, mutta arkaluontoisten tietojen suojaamisen mahdollinen taloudellinen rasittavuus oli pienten toimijoiden keskuudessa hieman muita heikommin tunnettu. Heistä vain kymmenesosa (10 %) tiesi, että arkaluontoisten tietojen suojaaminen ei saa jäädä tarvittavaa tietoturvatasoa heikommaksi taloudellisten syiden vuoksi. Keskisuuret toimijat tiesivät tämän vain hieman paremmin, sillä vain neljännes (25 %) oli siitä perillä. Pienten toimijoiden keskuudessa lähes kolmannes (29 %) oli asiasta tietoinen.



Kuvio 5. Tietotasot arkaluontoisten tietojen suojaamisessa

Kuviosta 5 näkee selvästi tietotasojen erot erikokoisten toimijoiden välillä. Mikroyritykset olivat muihin kokoluokkiin nähden parhaiten perillä arkaluontoisten tietojen suojaamisen vaatimuksista jääden kuitenkin vielä niukasti kohtalaiselle tasolle (2,00). Pienet yritykset saavuttivat juuri ja juuri kohtalaisen tietotason (1,8), mutta keskisuuret yritykset jäivät tietotasossa heikoksi (1,75). Tietotaso arkaluontoisten tietojen suojaaminen jäi toimijoiden keskuudessa kohtalaiselle tasolle keskiarvoluvun ollessa 1,95.

Rekisterinomistajan vastuut

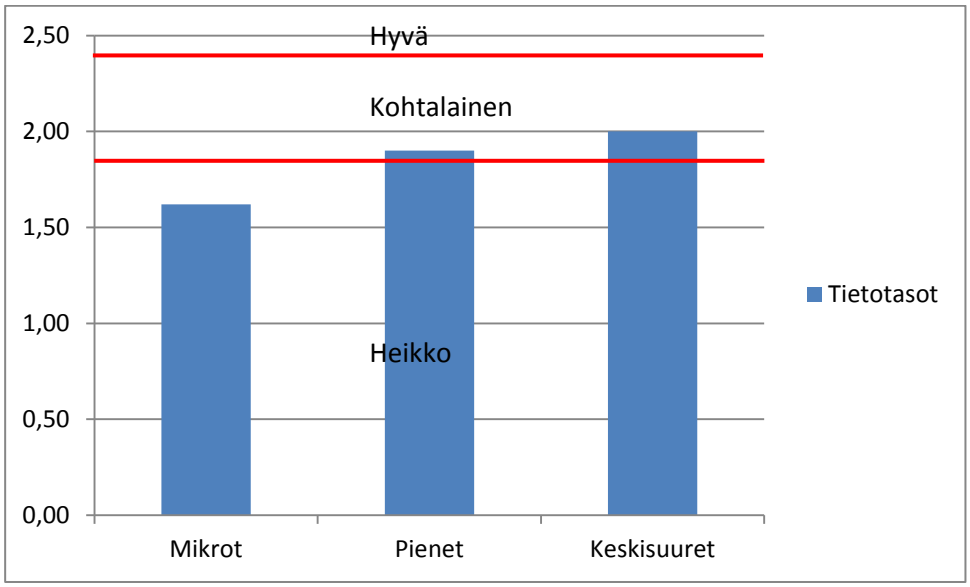
Vastuu henkilötietojen käsittelyn lainmukaisuudesta ja suojaamisesta henkilötietojen käsittelystä on aina rekisterinomistajalla. Ulkoistamistilanteissa palveluntarjoajan on annettava riittävät takeet siitä, että henkilötietoja käsitellään ja suojataan lain vaatimusten mukaisesti. Pakottavista lainsäännöksistä ei voida poiketa sopimuksin, mutta sopimuksissa on hyvä selventää kunkin tahon vastuut ja velvollisuudet. (Voutilainen 2012, 318–319.) Näistä kysyttiin väittämällä: Vastuu henkilötietojen käsittelyn lainmukaisuudesta ja suojaamisesta ulkoistamistilanteessa. Siihen annettiin kaksi oikeaa

ja yksi väärä vastausvaihtoehto: on rekisterin omistajalla, on palvelun tarjoajalla ja voidaan sopia rekisterinpitäjän ja palveluntarjoajan välillä kirjallisella sopimuksella.

Taulukko 4. Vastuut tietojen käsittelyn lainmukaisuudesta ja tietojen suojaamisesta henkilötietojen käsittelyn ulkoistamistilanteessa

Kokoluokka	Mikrot	Pienet	Keskisuuret	Kaikki
N	45	10	4	59
	%	%	%	%
On rekisterin omistajalla	62	70	75	64
On palveluntarjoajalla	33	50	25	36
Voidaan sopia kirjallisella sopimuksella	33	30	0	31

Kuten taulukosta 4 voi nähdä, henkilötietojen käsittelyn ulkoistamistilanteessa vastuuta tietojen käsittelyn lain mukaisuudesta ja tietojen suojaamisesta ei oikein mielletty palveluntarjoajalle. Vain noin kolmannes (36 %) kaikista vastaajista katsoi palveluntarjoajan olevan omalta osaltaan vastuussa henkilötietojen käsittelyn lainmukaisuudesta ja suojaamisesta. Rekisterinomistajan vastuu oli paremmin ymmärretty, ja kaikista vastaajista yli puolet (64 %) piti rekisterin omistajaa vastuullisena. Vajaa kolmannes (31 %) uskoi myös, että vastuut voidaan jakaa rekisterinpitäjän ja palveluntarjoajan välillä kirjallisella sopimuksella. Yritysten kokoluokkien välillä oli eroavaisuutta sopimusta koskevassa tilanteessa. Keskisuurista toimijoista ei yksikään väittänyt, että vastuista voisi sopia kirjallisella sopimuksella, kun pienistä ja mikroyrityksistä kolmannes (30 % ja 33 %) uskoi vastuun jakamiseen sopimuksin.



Kuvio 6. Tietotasot henkilötietojen ulkoistamisen vastuista

Kuviosta 6 huomaa, että tietotasot olivat toimijoiden kokoluokkien välillä hyvin tasaiset. Mikroyrityksissä oltiin heikoiten perillä siitä, kuka vastaa henkilötietojen käsittelyn lainmukaisuudesta ja tietojen suojaamisesta henkilötietojen käsittelyn ulkoistamistilanteissa. Mikroyritykset jäivät tietotason suhteen heikolle tasolle (1,62). Pienet ja keskisuuret yritykset tunsivat vastuut vain hieman mikroyrityksiä paremmin. Molemmat jäivät selvästi kohtalaiselle tasolle (1,9 ja 2.0)

Tietämystä rekisterinpitäjän vastuista kysyttiin myös kahdella väittämäpatteristolla. Ensimmäinen koski rekisterinpitäjän vastuuta tietojen joutuessa eri syistä ulkopuolisten käsiin. Rekisterinpitäjän vastuusta kysyttiin, kun

- henkilörekisteri on joutunut tietomurron kohteeksi
- henkilörekisteri on joutunut varastetuksi
- henkilörekisteri on varastettu palveluntarjoajan koneelta
- henkilörekisteri on epähuomiossa jäänyt sivullisen ulottuville, minkä seurauksena sivullinen kopioi tiedot itselleen
- työntekijä on luovuttanut tietoja rekisteröidyksi tekeytyneelle sivulliselle

- työntekijä hukkaa henkilötietoja sisältäneen sähköisen laitteen (esim. puhelin, kannettava tietokone, tablet-tietokone jne.)
- henkilötietoja käsitellään suojaamatonta verkkoa hyväksikäyttäen ja sivullinen tahallisesti skannaa tiedot.

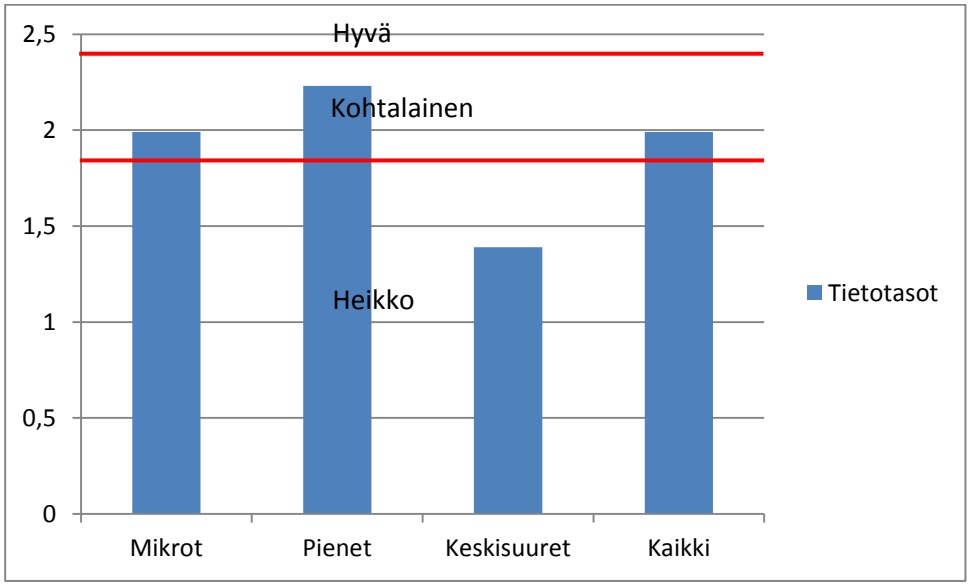
Taulukko 5. Rekisterinpitäjän vastuu henkilötiedoista eri tilanteissa

Kokoluokat	Mikrot	Pienet	Keskisuuret	Kaikki
N	45	10	4	59
	%	%	%	%
Tietomurto henkilörekisteriin	53	60	75	56 %
Henkilörekisteri on joutunut varastetuksi	53	60	25	53 %
Henkilörekisteri on varastettu palveluntarjoajan koneelta	38	50	25	39 %
Henkilörekisteri on jäänyt sivullisen ulottuville	87	100	25	85 %
Tietoja on luovutettu rekisteröidyksi tekeytyneelle sivulliselle	71	85	75	73 %
Työntekijä hukkaa henkilötietoja sisältäneen laitteen	76	80	50	75 %
Henkilötietoja käsitellään suojaamatonta verkkoa hyväksikäyttäen	87	90	50	85 %

Taulukosta 5 selviää, että kaikkien toimijoiden keskuudessa tunnettiin rekisterinpitäjän vastuu parhaiten tilanteissa, joissa henkilörekisteri on epähuomiossa jäänyt sivullisen ulottuville tai kun henkilötietoja käsitellään suojaamatonta verkkoa hyväksi käyttäen. Vastaajista lähes kaikki (85 %) olivat ymmärtäneet rekisterinpitäjän vastuulliseksi näissä tilanteissa. Heikoiten oli tunnistettu rekisterinpitäjän vastuu henkilörekisterin jouduttua varastetuksi palveluntarjoajalta. Tällöin vain vajaa puolet (39 %) katsoi vastuun henkilötietojen joutumisesta vääriin käsiin olevan rekisterinpitäjällä.

Tutkimuksen tuloksissa näkyy huomattavia eroja keskisuurten ja pienten yritysten välillä. Erityisesti rekisterinomistajan vastuu tilanteessa, kun henkilörekisteri jää sivullisen ulottuville vahingossa, oli keskisuurissa yrityksissä hämmästyttävän epäselvää. Vain neljännes (25 %) tiesi vastuun olevan tuolloin rekisterinomistajalla. Pienissä yrityksissä sen sijaan se oli kaikille (100 %) täysin selvä asia. Samansuuntaisia tuloksia saatiin myös tilanteissa, joissa henkilörekisteri oli joutunut varastetuksi joko omalta

tai palveluntarjoajan koneelta. Omalta koneelta varastettujen tietojen osalta pienistä yrityksistä yli puolet (60 %) katsoi rekisterinomistajan vastuulliseksi, kun taas keskisuurista vain neljännes (25 %). Samoin, kun henkilörekisteri varastetaan palveluntarjoajan koneelta, pienistä yrityksistä puolet (50 %) piti rekisterinomistajaa vastuullisena tietojen joutumisesta vääriin käsiin. Keskisuurissa yrityksissä vain neljännes (25 %). Suuret erot selittyvät aineiston pienellä koolla, jolloin yksittäisen vastaajan vaikutus tuloksiin on merkittävämpi.



Kuvio 7. Tietotasot rekisterinpitäjän vastuista

Tietotasot ja niiden erot rekisterinomistajan vastuusta tietojen joutuessa vääriin käsiin eri tilanteissa selviävät kuviosta 7. Tutkimuksen tuloksista tuli ilmi, että pienissä yrityksissä rekisterinomistajan vastuut olivat parhaiten tunnetut ja tietotaso oli lähes hyvä (2,23). Keskisuurten yritysten tietotaso jäi selvästi heikoksi (1,39). Kaikkien toimijoiden keskimääräinen tulos oli kohtalainen tietotaso (1,99).

Toisessa vastuista kysyvässä patteristossa kysyttiin rekisterinpitäjän vastuuta tietojen muuttumisesta, tuhoutumisesta tai katoamisesta eri tilanteissa. Rekisterinpitäjän vastuusta kysyttiin, kun:

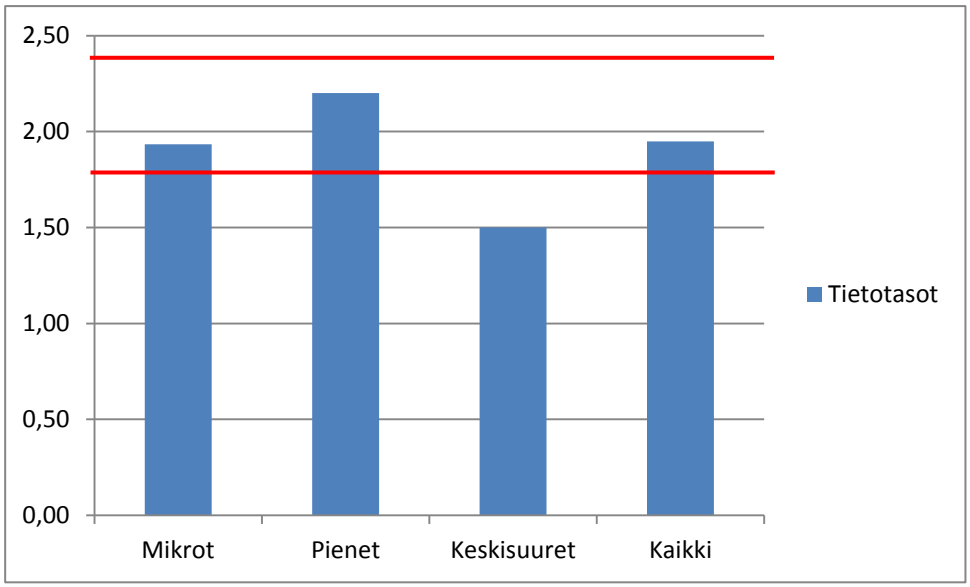
- henkilörekisteri on joutunut tietomurron kohteeksi palvelun tarjoajan palvelimella tai koneella
- henkilörekisteri on epähuomiossa jäänyt sivullisen ulottuville, minkä seurauksena sivullinen on käsitellyt tietoja
- työntekijä on vahingossa käsitellyt tietoja
- työntekijä, jolla ei ole oikeutta käsitellä henkilötietoja, käsittelee kuitenkin niitä
- henkilötietoja käsitellään suojaamatonta verkkoa hyväksi käyttäen ja ulkopuolinen pääsee siten käsittelemään tietoja
- henkilötietoja sisältävä järjestelmä tuhoutuu tulipalossa.

Taulukko 4. Rekisterinpitäjän vastuu henkilötietojen tuhoutumisesta, katoamisesta tai muuttumisesta

Kokoluokat	Mikrot	Pienet	Keskisuuret	Kaikki
N	45	10	4	59
	%	%	%	%
Tietomurto palvelun tarjoajan palvelimelle tai koneelle	40	60	75	46 %
Henkilörekisteri on epähuomiossa jäänyt sivullisen ulottuville	82	90	50	81 %
Työntekijä on vahingossa tuhonnut, kadottanut tai muuttanut tietoja	64	90	50	68 %
Työntekijä, jolla ei ole oikeutta käsitellä henkilötietoja, käsittelee kuitenkin niitä.	96	80	50	75 %
Henkilötietoja käsitellään suojaamattomassa verkossa	89	80	50	85 %
Henkilötietoja sisältävä järjestelmä tuhoutuu tulipalossa	36	40	25	36 %

Kuten taulukosta 4 havaitaan, kaikkien toimijoiden keskuudessa rekisterinpitäjä tunnistettiin parhaiten vastuulliseksi tietojen muuttumisesta, tuhoutumisesta tai katoamisesta, kun tietoja käsitellään suojaamattomassa verkossa. Lähes kaikki (85 %)vastaajat pitivät silloin rekisterinpitäjää vastuullisena. Heikoimmin tunnistettiin rekisterinpitäjän vastuu, jos tiedot tuhoutuvat tulipalossa. Vain kolmannes (36 %) vastaajista katsoivat rekisterinpitäjän olevan tuolloin vastuussa. Lähes kaikki (90 %) pienet toimijat tiedostivat rekisterinpitäjä vastuulliseksi tietojen tuhoutumisesta, katoami-

sesta ja muuttumisesta, jos työntekijä oli vahingossa käsitellyt tietoja kohtalokkain seurauksin tai henkilörekisteri oli jäänyt sivullisen ulottuville. Ero on huomattava keskisuuriin toimijoihin nähden, joista vain puolet (50 %) tunnisti rekisterinpitäjä vastuut näissä tilanteissa. Suuri ero kokoluokkien välillä selittyy keskisuurten toimijoiden vähäisellä esiintymisellä aineistossa, jolloin yksittäisen vastaajan vaikutus tuloksiin on suuri.



Kuvio 8. Tietotasot henkilötietojen tuhoutumisesta, muuttumisesta ja katoamisesta

Rekisterinpitäjän vastuut henkilötietojen muuttumisesta, tuhoutumisesta tai katoamisesta olivat yleisesti ottaen kohtalaisesti tunnettuja (1,95) kaikkien toimijoiden keskuudessa. Toimijoiden kokoluokkien välillä oli havaittavissa pientä vaihtelua tietotasoissa rekisterinpitäjän vastuista tietojen tuhoutuessa, kadotessa ja muuttuessa eri tilanteissa. Joukon paras tietotaso oli pienillä toimijoilla sen kuitenkin jäädessä kohtalaiseksi (2,20). Vain keskisuurten toimijoiden tietotaso jäi heikolle tasolle (1,50).

Julkisen sektorin tietosuojavaatimukset

Julkisen sektorin edustajilta kysyttiin kolme ylimääräistä, vain julkishallintoon liittyvää, tietosuojakysymystä. Kysymykset koskivat tietoturvallisuuden perustason vaatimukset täyttävää tietojenkäsittely-ympäristöä, asiakirjojen ja tietojärjestelmien suojaamista ja hyvän tiedonhallintatavan vaatimuksista.

Tietoturvallisuuden perustason vaatimukset tunnettiin melko hyvin. Yli puolet (68 %) tiesi, että perustason vaatimukset täyttävää tiedonkäsittely-ympäristö on viranomaisen määriteltävissä tietoturvallisuusasetuksen antamien ohjeiden mukaisesti.

Viranomaisten asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suojan, eheyden ja laadun turvaamiseen liittyvät vaatimukset tiedettiin yleisesti ottaen heikosti (keskiarvoluku 1). Parhaiten oli tiedetty, että tietojen suojaamisen täytyy tapahtua asianmukaisin menettelytavoin. Kaikki (100 %) viranomaisen edustajat tiesivät sen. Kukaan (0 %) ei tiennyt, että tietojen suojaamisessa otetaan huomioon tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvatoimenpiteistä aiheutuvat kustannukset.

Hyvän tiedonhallinnan toteuttamisen edellytykset olivat edellisiä paremmin tunnetut. Kaikki (100 %, n=3) tiesivät, että hyvän tiedonhallintatavan toteuttaminen edellyttää tiedonhallinnan suunnittelua. Tietojen suojaamisvaatimus oli vastaajille tuntemattomin. Vain kolmannekselle (33 %) vastaajista se oli tuttu.

Kaiken kaikkiaan tietotaso viranomaisille osoitetuissa kysymyksissä jäi vain niukasti heikolle tasolle (1,7). Tässä täytyy ottaa huomioon, että viranomaisen edustajien joukko oli todella pieni ja ettei tuloksia voi tältä osin mitenkään yleistää perusjoukkoon kuuluviin viranomaisiin. Tulokset pätevät vain tutkimuksen osallistuneiden joukossa.

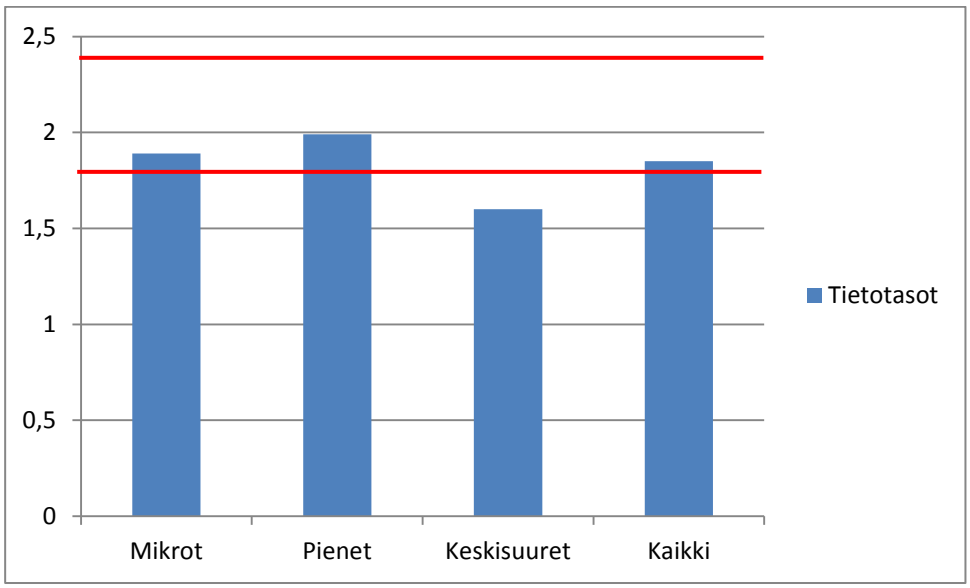
Yhteenveto tietotasoista

Tietotasoa kuvaava keskiarvo vaihteli yksittäisten vastaajien osalta 0,625 – 2,875 välillä eli tietotasot olivat heikosta hyvään. Vastaukset luokiteltiin keskiarvoluvun mukaan kolmelle tietotasolle (taulukko 6).

Taulukko 6. Tietosuojatiedon tasot

	n = 59 %
Heikko	32
Kohtalainen	44
Hyvä	24
Yhteensä	100

Kuten taulukosta selviää, neljännes (24 %) vastaajista omasi hyvän tietotason tietojen suojaamiseen ja rekisterinpitäjän vastuisiin liittyvissä kysymyksissä. Liki puolella (44 %) vastaajista tietotaso oli kohtalainen, ja kolmanneksella (32 %) se oli heikko.



Kuvio 9. Tietotasot keskiarvolukuina kokoluokittain

Kuviossa 9 tarkastellaan toimijoiden tietotason keskiarvolukuja kokoluokittain. Siitä näkee hyvin, että tietosuojalainsäädännön tietojen suojaamisvelvoitteiden ja rekisterinpitäjän vastuiden osalta ei lainsäädäntö ole kovin hyvin tunnettu. Kaikkien toimijoiden keskiarvo ylsi vain hieman kohtalaisen raja-arvon (1,8) yläpuolelle (1,85). Toimijoiden kokoluokkien välillä ei ole kovin merkittäviä eroja tietotasoissa. Mikro- ja pienet toimijat ylsivät juuri ja juuri kohtalaiselle (1,89 ja 1,99) tietotasolle, mutta keskisuuret toimijat jäivät heikolle tietotasolle (1,6). Toisin kuin tutkija alun perin arvioi, ei toimijan kokoluokalla ole juurikaan merkitystä tietosuojaosaamisessa.

Taulukko 7. Tietosuoja- ja tietoturvakoulutus sekä menettelytavat

	Heikko	Kohtalainen	Hyvä	Kaikki
N	19	26	14	59
	%	%	%	%
Tietosuojakoulutus	37	23	43	32 %
Tietosuojamenettelytavat	47	54	64	54 %
Tietoturvakoulutus	32	15	43	22 %
Tietoturvamenettelytavat	53	46	71	54 %

Taulukosta 7 voidaan nähdä tietosuoja- ja tietoturvakoulutusten vaikutus tietosuojatietämisen tasoon. Kaikista toimijoista kolmasosassa (32 %) oli järjestänyt tietosuojakoulutusta ja viidesosa (22 %) tietoturvakoulutusta. Tietosuojaan ja tietoturvaan liittyvät menettelytavat ja ohjeet oli noin puolella (54 %) toimijoista. Hyvään tietotasoon yltäneiden joukossa oli järjestetty selvästi enemmän koulutusta tietosuojasta ja tietoturvasta kuin heikon ja kohtalaisen tietotason joukoissa. Hyvän tietotason joukossa edellä mainittuja koulutuksia oli järjestetty melkein puolilla (43 %) toimijoista, kun taas heikon tietotason joukossa noin kolmasosassa oli järjestetty koulutusta tietosuojasta (37 %) tai tietoturvasta (32 %). Erot ovat selvät myös menettelytapojen ja ohjeistusten osalta.

6.3 Toimijoiden tietoturvatoimet

Kyselyn kolmasosa mittasi toimijoiden panostusta tietoturvaan käytettävien menetelmien laatua ja määrää tarkastelemalla. Tietoturva-asioista kysyttiin 11 kysymyksellä. Kysymyksillä pyrittiin saamaan selko, miten toimijat ovat huolehtineet tietoturvan eri osa-alueista. Kysymykset esitettiin väittämiksi muotoiltuina, ja vastausvaihtoehdoista täytyi tilanteesta riippuen valita yksi tai useampi väittämään sopiva vastaus.

Aluksi kysyttiin perustason tietoturvatoimista eli salasanojen ja käyttöoikeuksien jakamisesta työtehtävien mukaan. Niiden käyttöä tarkastellaan taulukossa 8.

Taulukko 8. Salasanojen ja käyttöoikeuksien käyttäminen tietotasoittain

Tietotaso	Heikko	Kohtalainen	Hyvä	Kaikki
n	19	25	13	59
	%	%	%	%
Salasanat ja käyttäjätunnukset	100	92	93	95
Käyttöoikeudet tehtävien mukaan	74	100	85	85

Taulukosta 8 nähdään, että käyttäjätunnukset ja salasanat olivat käytössä lähes kaikilla (95 %) vastaajilla, ja noin kahdeksalla kymmenestä (85 %) myös käyttöoikeudet oli jaettu työtehtävien mukaan. Käyttöoikeuksien rajaamisen vähyyttä salasanojen käyttöön verrattuna selittänee se, että pienissä yrityksissä oli mukana yhden hengen yrityksiä, joissa käyttöoikeuksia ei ole ollut tarpeen rajata. Mielenkiintoista oli, että tietojen suojaamisvelvoitteissa heikoimman tietotason saaneet käyttävät kaikki (100 %) salasanoja ja käyttäjätunnuksia koneille ja järjestelmiin kirjautumisessa. Tietotason parantuessa niiden käyttö oli vähäisempää. Käyttöoikeuksien jakamisessa työtehtävien mukaan ei samanlaista suuntausta ollut havaittavissa. Kaikki (100 %) kohtalaisen tietotason omaavat toimijat jakoivat järjestelmien käyttöoikeudet työtehtävien mukaan, kun heikon tietotason toimijoista vain kolme neljäsosaa (74 %).

Henkilötietoja sisältävien koneiden ja järjestelmien suojaamista tarkasteltiin paitsi kokonaisuutena, myös vastaajien tietosuojaosaamisen mukaisten tietotasoluokkien mukaan (taulukko 9). Näin voitiin nähdä, löytyykö eri tietotason omaavien ryhmien välillä eroja.

Taulukko 9. Henkilötietoja sisältävien koneiden ja järjestelmien suojaaminen

Tietotaso	Heikko	Kohtalainen	Hyvä	Kaikki
N	19	26	14	59
	%	%	%	%
Palomuurilla	100 %	96 %	100 %	98 %
Virustorjuntaohjelmalla	100 %	100 %	86 %	97 %
Salasanalla	95 %	88 %	93 %	92 %
Tunkeutumisen havaitsemisjärjestelmällä	37 %	23 %	29 %	29 %
Tietoja käsittelevät henkilöt tunnistetaan jälkikäteen	21 %	31 %	29 %	27 %
Laittomasta järjestelmään tunkeutumisesta ilmoitus rekisterinpitäjälle	11 %	12 %	0 %	8 %
Jotenkin muuten	5 %	8 %	14 %	8 %

Tutkimuksen tuloksista selvisi, että perustason suojausmenetelmät olivat yleisesti käytössä. Lähes kaikilla oli palomuuri (98 %) ja virustorjuntaohjelmat (97 %) käytössään. Myös salasanoja käytettiin koneiden ja järjestelmien suojaamiseen melko hyvin. Lähes kaikki (92 %) vastaajat kertoivat suojaavansa henkilötietoja sisältävät koneet ja järjestelmät salasanoin. Monimutkaisempiin menetelmiin mentäessä suojausmenetelmien käyttö vähenee huomattavasti. Menetelmä, joka ilmoittaa rekisterinpitäjälle laittomasta tunkeutumisesta, oli käytössä vajaalla kymmenesosalla (8 %).

Tietotason mukaisten luokkien välillä on pieniä, mutta mielenkiintoisia eroja erityisesti heikon ja hyvän tason välillä. Perustason suojausmenetelmien käytössä oli vain pieniä eroavaisuuksia, mutta vaativampaan suuntaan mentäessä erot hieman kasvoivat heikon tietotasoluokan hyväksi. Reilu kolmannes (37 %) heikon tietotason saaneista toimijoista käytti tunkeutumisen havaitsemisjärjestelmää, kun taas hyvälle tasolle yltäneistä se oli vain hieman yli neljänneksellä (29 %) käytössä. Ero oli edellistä suurempi, kun kyseessä oli menetelmä, joka ilmoittaa rekisterinpitäjälle laittomas-

ta järjestelmään tunkeutumisesta. Heikontietotason luokassa tällainen menetelmä oli käytössä noin kymmenesosalla (11 %), kun taas hyvän tietotasonluokassa ei kenelläkään (0 %). Eroa saattaa selittää se, että hyvän tietotasonluokassa tiedettiin paremmin lainsäädännön vähimmäisvaatimukset, jolloin tietoturvatoimet sovitettiin sen mukaisiksi ja vältettiin turhan tehokkaiden toimien käyttö, ja heikomman tietotason ryhmässä käytettiin tehokkaampia menetelmiä kaiken varalta. Selitystä voisi hakea myös arkaluontoisten tietojen vaatimasta huolellisemmasta suojaamisesta.

Taulukko 10. Arkaluontoisia tietoja sisältävien rekisterien esiintyvyys eri tietotasojen joukossa

Tietotaso	Heikko	Kohtalainen	Hyvä	Kaikki
N	19	26	14	59
	%	%	%	%
Kyllä	16	19	29	20
Ei	84	81	71	80
Yhteensä	100	100	100	100

Taulukosta ilmenee kuitenkin, että hyvän tietotason omaavassa luokassa on henkilörekisteriin tallennettu muita enemmän arkaluontoisia henkilötietoja, joten siitä ei löydy selitystä eroille henkilötietoja sisältävien koneiden ja järjestelmien suojauksessa.

Kulun- ja kameravalvonnalla voidaan nostaa fyysisen tietoturvan tasoa silloin, kun edellytetään tehokkaampaa tietoturvaa. Jokainen toimija joutuu itse arvioimaan tarvittavan taso huomioiden tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, suojattavien tietojen laadun ja määrän, suojattavien tietojen iän sekä tietojen merkityksen yksityisyyden suojan kannalta. (Laaksonen ym. 2006, 51.) Taulukossa 11 on tarkasteltu kulun- ja kameravalvonnan käyttöä yleisesti sekä tietosuojatietämisen mukaan jaotelluissa luokissa.

Taulukko 11. Kulun- ja kameravalvonta

	Heikko	Kohtalainen	Hyvä	Kaikki
N	19	26	14	59
	%	%	%	%
Kulunvalvonta, mutta ei tietoturvan vuoksi	16	19	14	17
Kulunvalvonta tietoturvallisuuden vuoksi	16	12	14	14
Kameravalvonta, mutta ei tietoturvan vuoksi	11	8	0	7
Kameravalvonta tietoturvallisuuden vuoksi	32	23	21	25

Tutkimuksesta selvisi, että kulunvalvonta oli noin kolmasosalla (31 %) ja kameravalvonta niin ikään kolmasosalla (32 %) käytössä. Kulunvalvontaa käytettiin tietoturvan vuoksi reilulla kymmenesosalla (14 %), mikä oli hieman vähemmän kuin kulunvalvonnan käyttö muun syyn vuoksi. Kameravalvonnan osalta tilanne oli toisin päin. Sitä käytettiin selvästi enemmän tietoturvallisuuden kuin muiden syiden vuoksi. Jopa neljännes (25 %) kaikista toimijoista käytti kameravalvontaa tietoturvasyistä.

Taulukosta voidaan nähdä, että heikon tietotason luokassa kameravalvontaa käytettiin suhteessa enemmän kuin muissa luokissa. Heistä jopa kolmasosa (32 %) oli valinnut kameravalvonnan muun muassa tietoturvan tason nostamiseksi, kun hyvän tietotason joukossa se oli vain viidesosalla (21 %). Tämä oli samassa linjassa tässä tutkimuksessa aiemmin esiteltyjen tietoturvatoimien valintaa koskevien tulosten kanssa. Myös niistä ilmeni, että heikon tietosuojatietämisen joukko käytti tehokkaampia tietoturvamenetelmiä.

Asiakasrekisterin sijainnista kysyttiin väittämällä: asiakastietoja sisältävä henkilörekisteri on tallennettu. Vastausvaihtoehdoista täytyi valita vain yksi toimipaikan tilanteeseen sopiva vaihtoehto. Vaihtoehdot olivat: omalle tai palveluntarjoajan palvelimelle; tietokoneelle, joka on vain toimipaikan työntekijöiden käytössä; tietokoneelle, jota voivat käyttää myös muutkin kuin toimipaikan työntekijät (esimerkiksi perheenjäsenet tai ystävät). Kysymyksestä saadut tulokset esitetään taulukossa 12 toimijoiden tietosuojatietotasojen mukaisesti luokiteltuina sekä kaikki yhteensä.

Taulukko 12. Henkilörekisterin tallennuspaikka

Tietotaso	Heikko	Kohtalainen	Hyvä	Kaikki
N	19	26	14	59
	%	%	%	%
Palvelimelle	42 %	65 %	36 %	51 %
Toimipaikan koneelle	58 %	31 %	64 %	47 %
Yhteisessä käytössä olevalle koneelle	0 %	4 %	0 %	2 %

Tutkimuksesta selvisi, että toimijat pyrkivät pitämään henkilörekisterin ulkopuolisten ulottumattomissa. Vain murto-osa (2 %) oli tallentanut henkilörekisterin koneelle, jota voivat ulkopuolisetkin käyttää. Noin puolella (51 %) rekisteri oli tallennettu palvelimelle tai koneelle, joka oli vain toimipaikan käytössä (47 %). Kohtalaisen tietotason ryhmästä kaksi kolmasosaa käytti tallennuspaikkana joko omaa tai palveluntarjoajan palvelinta, kun taas heikon ja hyvän tietotason ryhmissä kahdella kolmasosalla (58 % ja 64 %) tallennuspaikkana oli toimipaikan tietokone.

Toimipakassa voidaan parantaa tietoturvallisuutta muun muassa määrittelemällä ja ohjeistamalla, mitä ohjelmia tietokoneille tai puhelimille ja muille kannettaville laitteille saa asentaa tai millä verkkosivuilla ei saa vierailla toimipaikan tietovälineillä. (Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 69.) Taulukosta 13 selviää, miten toimipaikoissa on käytetty edellä mainittuja keinoja tietoturvallisuuden parantamiseksi.

Taulukko 13. Verkon ja koneiden käytöstä annetut ohjeet

	Heikko	Kohtalainen	Hyvä	Kaikki
N	19	26	14	59
	%	%	%	%
Mitä saa asentaa	53 %	38 %	50 %	46 %
Millä sivustoilla saa vierailla	26 %	27 %	7 %	22 %
Oman harkinnan varassa	42 %	35 %	50 %	41 %

Taulukosta 13 voidaan nähdä, että lähes puolet (46 %) oli määritellyt, mitä ohjelmia toimipaikan tietolaitteille saa asentaa, ja viidennes (22 %), millä sivustoilla saa internetissä vierailla. Mielenkiintoista oli, että tietosuojatietämisessä hyvään tasoon yltäneillä puolella (50 %) oli täysin oman harkinnan varassa, mitä koneille saa asentaa ja millä sivustoilla vierailla. Heikon tietotason ryhmässä ohjelmien asentaminen ja verkossa liikkuminen oli vajaalla puolella (42 %) oman harkinnan varassa ja kohtalaisen tietotason saavuttaneilla vain noin kolmasosa (35 %) luotti omaan harkintaan näissä asioissa. Tietoturva- ja tietosuojatietoisuuden ollessa korkealla tasolla voidaan oman harkinnan varaan jättääkin paljon, kuten eräs vastaus osoittaa:

> *Pienyrityksenkin on noudatettava hyviä toimintatapoja ja tarkkaavaisuutta puhtaan tietoliikenteen ja turvallisen tietojen varastoinnin ja käytön varmistamiseksi ja mahdollisuuksien mukaan eriytettävä yritys- ja yksityistietojen käsittely ja viihdesurffailu toisistaan.*

Tietoaineiston luokittelemisella voidaan suhteellisen helposti selvittää tarvittavien tietoturvatoimien laajuus ja tehokkuus, jolloin voidaan helpommin suhteuttaa tietoturvatoimet aineiston tarvitsemaan suojaukseen. (Laaksonen ym. 2006, 67.) Luokittelu ei kuitenkaan näytä olevat kovin yleisesti käytössä toimijoiden keskuudessa (taulukko 14).

Taulukko 14. Tietoaineiston luokittelu eri tietotasoilla

	Heikko	Kohtalainen	Hyvä	Kaikki
N	19	26	14	59
	%	%	%	%
Kyllä	32	31	29	31
Ei	32	62	50	49
En tiedä	37	8	21	20

Tutkimuksen tuloksista ilmeni, että vain kolmasosa kaikista toimijoista luokittelee tietoaineistonsa. Puolet (49 %) ei luokittele ja viidesosa ei tiedä, luokitellaanko tietoaineistoa. Tietotasojen välillä oli vain merkityksettömiä eroja. Sen perusteella aineiston luokittelu ei ole vaikuttanut arviointiin tietoturvamenetelmiä määriteltäessä.

Varmuuskopioinnilla toteutetaan tietoaineistoturvallisuutta. Henkilörekisterin säännönmukaisen varmuuskopioinnin avulla voitaisiin palauttaa toimipaikan tietokyky suhteellisen helposti sen jälkeen, kun toiminnan kannalta tärkeä henkilörekisteri jostain syystä tuhoutuu tai tiedot muuttuvat. (Laaksonen ym. 2006, 67.)

Taulukko 15. Henkilötietoja sisältävän rekisterin varmuuskopiointi

	Heikko	Kohtalainen	Hyvä	Kaikki
N	19	26	14	59
	%	%	%	%
Varmuuskopioidaan itse	74	42	64	58
Palvelimen ylläpitäjän toimesta	21	42	36	34
Ei varmuuskopioida	5	15	0	9

Taulukossa 15 tarkastellaan toimijoiden tapaa huolehtia varmuuskopioinnista. Tutkimuksesta selvisi, että suurin osa (58 %) varmuuskopioi henkilörekisterin tiedot itse, kun taas noin kolmannes jättää sen palvelimen ylläpitäjän hoidettavaksi. Hieman huolestuttavaa oli, että kymmenesosa (9 %) jättää varmuuskopioimatta henkilörekisterinsä tiedot. Tietotasojen välisistä eroista huomataan, että tietotasoltaan hyvässä ryhmässä tietoja ei jätetä varmuuskopioimatta, kun taas kohtalaisen tietotason ryhmässä jopa reilu kymmenesosa (15 %) jättää varmuuskopioinnin kokonaan välistä.

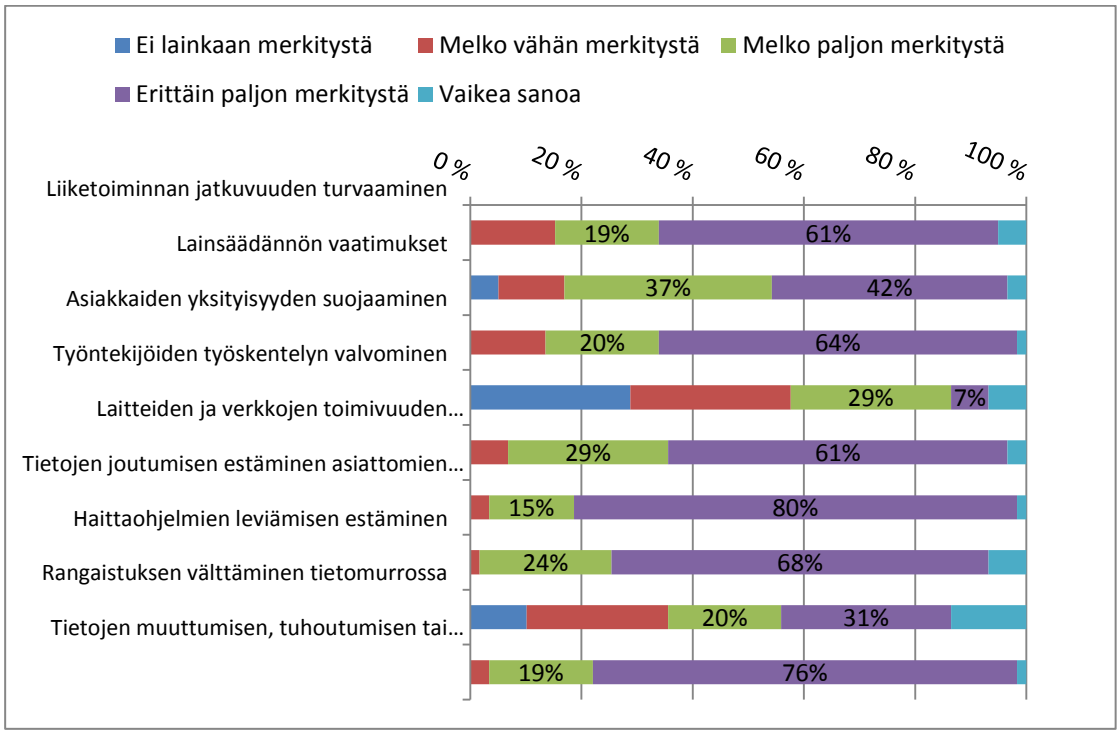
6.4 Lainsäädännön vaikutus toimipaikan tietoturvatoteutukseen

Kyselyn aiemmilla kysymyksillä haettiin vastausta siihen, miten paljon tietosuojalainsäädännön tietojen suojaamisvelvoitteiden ja rekisterinpitäjän vastuiden tunteminen vaikuttaa tietoturvasta huolehtimiseen. Tähän mennessä saadut tulokset osoittivat, ettei lainsäädännön tunteminen lisää tietoturvatoimien monipuolista käyttöä. Aiemmista kysymyksistä saatuja tuloksia haluttiin vahvistaa vielä kysymyksellä, jossa vastaajat saivat arvioida tiettyjen asioiden merkitystä toimipaikkansa käytössä olevien tietoturvatoimien valintaan. Kysymys oli: arvioikaa seuraavien asioiden merkitystä toimipaikassanne valittujen tietoturvatoimien (esim. virustorjunta, palomuuri, kulun-

valvonta, tietoturvaohjeistus) valintaan. Arviointiasteikkona käytettiin: Ei lainkaan merkitystä, Melko vähän merkitystä, Melko paljon merkitystä, Erittäin paljon merkitystä ja Vaikea sanoa. Arvioitavat asiat olivat:

- Liiketoiminnan jatkuvuuden turvaaminen
- Lainsäädännön vaatimukset tietojen suojaamisesta
- Asiakkaiden yksityisyyden suojaaminen
- Työntekijöiden työskentelyn valvominen
- Laitteiden ja verkkojen toimivuuden varmistaminen
- Tietojen joutumisen estäminen asiattomien käsiin
- Haittaohjelmien leviämisen estäminen
- Rangaistuksen välttäminen esimerkiksi tietomurron tapahduttua
- Tietojen muuttumisen, tuhoutumisen tai katoamisen estäminen
- Muu. Mikä?

Kysymyksen tulokset esitetään 100-prosenttisesti pinottuina pylväinä kuviossa 10. Vastauksista näytetään tarkat prosenttiosuudet vain tulosten kannalta merkityksellisimmissä palkeissa: Erittäin paljon merkitystä ja Melko paljon merkitystä. Muut arvopisteet jätetään näyttämättä, jotta luettavuus säilyy.



Kuvio 10. Tietoturvatoimien valintaan vaikuttavat asiat

Kun vastaajia pyydettiin arvioimaan, miten paljon tietyt seikat olivat vaikuttaneet toimipaikan tietoturvatoimien valintaan, eivät lainsäädännön vaatimukset olleet kovinkaan merkittävässä asemassa. Vain neljä kymmenestä (42 %) vastaajasta piti lainsäädännön vaatimuksia merkittävänä syynä tietoturvamenetelmien valintaan. Kuitenkin asiakkaiden yksityisyyden suojaaminen oli suurimmalla osalla (64 %) yksi erittäin merkittävä seikka ja viidesosalla (20 %) melko merkittävä seikka tietoturvamenetelmiä valittaessa. Samoin tietojen tuhoutumisen, katoamisen, muuttumisen estäminen oli kahdeksalle kymmenestä vastaajasta (80 %) erittäin merkittävä syy ja viidesosalle (19 %) melko merkittävä syy tietoturvatoimien valinnassa. Tietoturvalla haluttiin estää asiattomien pääsy tietoihin, mikä oli hyvin suurelle osalla (80 %) erittäin merkittävä syy tietoturvamenetelmien valinnassa. (Kuvio 10.)

Tuloksista voidaan selvästi nähdä, että lainsäädännön tietojen suojaamisvelvoitteiden tuntemisella tai sen vaatimuksilla ei ole juurikaan vaikutusta toimijoidentietoturvasta huolehtimiseen. Silti tietoturvatoimin pyritään samaan, mihin tietosuojalain-

säädäntökin pyrkii eli yksityisyyden suojaamiseen. Lainsäädännön tavoin toimijatkin ovat halunneet varmistaa, etteivät tiedot tuhoudu, katoa tai muutu eivätkä asiattomat pääse käsiksi tietoihin. Näin yksilön tietosuoja ja yksityisyys halutaan turvata, ja kuten eräs vastaaja osoittaa, on tietoturvallisuus ymmärretty liiketoiminnan kannalta tärkeäksi: *”Tietoturva-asiat ovat kuitenkin yrityksen toiminnan kannalta erittäin tärkeitä.”*

Vastaukset edelliseen kysymykseen vahvistivat tutkimuksesta saatuja tuloksia. Tuloksista voidaan nähdä, että tietoturvamenetelmän olivat monipuolisempia tietosuojatiedoiltaan heikossa ryhmässä kuin hyvässä ryhmässä. Tutkimuksen mukaan tietosuojaosaaminen ei tarkoita laajempaa tietoturvatoimien käyttöä, vaan lähinnä hillitympää menetelmien valintaa. Tuloksista voisi karkeasti päätellä, että tietosuojaosaaminen auttaa paremmin mitoittamaan tietoturvamenetelmät suojattaviin tietoihin nähden. Oikean tiedon puuttuessa halutaan ehkä enemmän varmistella, että tietoturvatoimet ovat riittävät. On hienoa, että tietoturvasta halutaan huolehtia tehokkaasti, mutta turhan resurssien tuhlaamisen välttämiseksi tarvitaan kykyä arvioida ja mitoittaa riittävä tietosuojan taso oikein.

7 Pohdinta

Tutkimuksen tavoitteena oli selvittää, vaikuttaako tietosuojalainsäädännön tietojensuojaamisvelvoitteiden tunteminen tietoturvasta huolehtimiseen. Tähän pyrittiin löytämään vastauksia kartoittamalla vastaajien tietosuojatietämisen tasoa ja eri tietotasoa edustavien käyttäjien tietoturvamenetelmien kattavuutta ja tehokkuutta. Tutkimus toteutettiin verkkokyselynä ja tutkimusmenetelmänä oli kvantitatiivinen tutkimusmenetelmä. Tarkoitus oli saada myös viitteitä siitä, voidaanko lain tietojensuojaamisvaatimusten korostamisella motivoida huolehtimaan tietoturvasta.

Tietosuojalainsäädännön vaatimukset tietoturvalle tunnettiin kohtalaisesti. Tietämisen tasoa voidaan nostaa tietoturva- ja tietosuojakoulutuksilla sekä tietoturvasta ja tietosuojasta laadituilla menettelytavoilla ja ohjeilla. Korkea tietosuojatietämisen taso ei kuitenkaan tarkoittanut monipuolisempaa tietoturvamenetelmien käyttöä

eikä se lisännyt halua huolehtia tietoturvasta muita enempää. Velvoitteiden tunteminen näytti kuitenkin lisäävän kykyä mitoittaa oikein tietoturvatoimet tarvittavaan turvallisuustasoon nähden. Tietoturvaan motivoivat muut syyt kuin tietoisuus lainsäädännön vaatimuksista. Asiakkaiden yksityisyyden suojaaminen ja tietojen tuhoutumisen, katoamisen ja muuttumisen estäminen olivat liiketoiminnan jatkuvuuden turvaamisen lisäksi merkittävimmät syyt huolehtia tietoturvasta.

Tuloksista voitiin havaita, että kaikkien tutkimukseen osallistuneiden keskimääräinen tietosuojaosaaminen saavutti juuri ja juuri kohtalaisen tason. Noin kolmannes (32 %) kaikista vastaajista jäi heikolle tasolle ja kohtalaiselle tasolle vajaa puolet (44 %) vastaajista. Hyvään tietotasoon ylsi vain noin kolmannes (34 %) kaikista vastaajista. Tulos oli hieman parempi kuin tietosuojavaltuutetun 2012 tekemässä tarkastuksessa, jossa yli puolet yrittäjistä ei tiennyt, mitä lainsäädäntö edellyttää tietoturvalta (Tietosuojavaltuutettu vaatii yrityksiä panostamaan tietoturvaan 2012). Siihen nähden tietosuojaosaamisen taso näyttäisi nousseen.

Laaksonen ja muut (2006, 19–20) ovat todenneet, ettei yrityksissä ymmärretä, että tietoturvallisuuden tasoa voidaan nostaa helposti myös organisatorisin keinoin. Tässä tutkimuksessa havaittiin kuitenkin, että organisatorisina keinoina tietosuojasta ja tietoturvasta laaditut menettelytavat ja ohjeistukset olivat hyvän tietosuojatason joukossa melko yleisiä. Menettelytavat ja ohjeistukset olivat myös tietosuojatietämisessä heikosti menestyneillä toimijoilla käytössä, mutta harvemmin. Tutkimuksen tuloksista voidaan päätellä, että tietosuoja- ja tietoturvakoulutuksella sekä myös tietoturvaan ja tietosuojaan liittyvillä menettelytavoilla ja ohjeistuksilla voidaan nostaa tietosuojatietämisen tasoa.

Näyttää kuitenkin siltä, ettei tietosuojaosaaminen vaikuta tietoturvasta huolehtimiseen niin kuin tutkija oli olettanut. Osaaminen ei suinkaan lisännyt käytettävien tietoturvamenetelmien käyttöä, vaan päinvastoin menetelmiä käytettiin hillitymmin. Heikon tietotason joukossa oli vastaavasti käytetty teknisesti monipuolisempia tietoturvakeinoja. Vaikuttaisi siltä, että tietoisuus lainsäädännön velvoitteista auttaa paremmin arvioimaan tarvittavan tietoturvallisuuden tason. Kun lain vaatimukset ovat tuntemattomat, halutaan varmistaa, että valitut menetelmät ovat varmasti riittävät.

Tutkimus osoittaa, että jyväskyläläiset toimijat huolehtivat tietoturvasta heikosta lainvelvoitteiden tuntemisesta huolimatta. Tämä poikkeaa selvästi aikaisemmista tutkimuksista. Tietosuojavastaavan kesällä 2012 tekemä selvitys osoittaa, etteivät lainsäädännön vaatimuksista tietämättömät toimijat huolehtineet riittävästä tietoturvasta. (Tietosuojavaltuutettu vaatii yrityksiä panostamaan tietoturvaan 2012.) Tietoturvasta huolehtiminen oli sivuutettu usein myös asenteiden takia, sillä toimijat eivät olleet suhtautuneet vakavasti olemassa oleviin tietoturvauhkiin (Hulkko 2012).

On mielenkiintoista, että vastaajat eivät tunteneet kovinkaan hyvin lainsäädännön tietojen suojaamisvelvoitteita eivätkä rekisterinpitäjän vastuita, mutta panostivat silti tietoturvaan monipuolisesti ja tehokkaasti. Tietoturvasta huolehtimishalukkuuden muutoksessa voi olla kyse Tietoturvayhtiö Symantecin vuonna 2010 tutkimuksessaan havaitsemasta ilmiöstä. Tietomurrot ja vakoilutapaukset ovat kasvattaneet yksityisyyden ja sen suojaamisen merkitystä yrityksissä. Sen vuoksi yritykset ovat aiempaa halukkaampia huolehtimaan tietoturvasta. (Symantec 2010 SMB Information Protection Survey Global Data 2010, 5–6.) Tutkimuksen tulokset vahvistavat tätä käsitystä. Lisääntynyt varovaisuus tuli ilmi myös tutkimukseen osallistumatta jättäneiden viesteistä. Niistä heijastui aito huoli tietojen joutumisesta vääriin käsiin, ja vastaamatta jättäminen oli nähty yhtenä tietoturvatoimena.

Asiakkaan yksityisyyden suojaaminen ja tietojen tuhoutumisen, muuttumisen ja katoamisen estäminen olivat liiketoiminnan jatkuvuuden turvaamisen lisäksi tärkeimpiä syitä huolehtia tietoturvasta. Ne olivat juuri niitä samoja asioita, joita tietosuojalainsäädännölläkin tavoitellaan. Lainsäädännön velvoitteiden toteuttaminen ei kuitenkaan ollut kovinkaan merkittävä syy tietoturvamenetelmien valintaan. Toimijat ovat ehkä oivaltaneet saman, minkä Salminenkin (2009) on todennut; asiakkaan yksityisyydestä huolehtiminen vaikuttaa kilpailukykyyn ja on yhteydessä myös liiketoiminnan jatkuvuuteen. Pahimmillaan tietosuojaloukkauksen julkitulo voi lamaannuttaa koko liiketoiminnan. (Salminen 2009, 22.) Saattaa olla myös, että kyselyn aihe ja kysymykset ovat vaikuttaneet siihen, miten merkittävinä vastaajat pitivät kyselyssä aiemmin kysyttyjä asioita.

Tietosuojatietämyksen lisääminen ei näyttäisi motivoivan tietoturvahalukkuuteen. Lain vaatimuksista paremmin perillä olevat toimijat eivät panosta muita enempää monipuolisten teknisten tietoturvamenetelmien käyttöön mutta osaavat paremmin arvioida tarvittavan tietoturvallisuuden tason ja suhteuttaa käytettävät tietoturvamenetelmät tarpeeseen. Tutkimuksen tulosten perusteella tietosuojalainsäädännön vaatimusten selvittäminen riskien arviointi -opastuksen lisänä olisi tietoturvakoulutuksissa tarpeen. Sen myötä toimijat osaisivat paremmin optimoida tietoturvatoimenpiteensä. Työskentelyyn tulisi enemmän joustavuutta ja sujuvuutta, kun tarpeettoman raskaat tietoturvamenetelmät jäisivät pois, mutta tietojen suojaamistaso kyettäisiin kuitenkin varmistamaan. Kun oikein mitoitettua tietoturvaa ei koeta liian raskaaksi eikä tietoturvamenetelmiä yritetä kiertää, tietojen suojaustasosta huolehditaan jopa paremmin. Tietoturvatoimien optimointitaito tuo onnistuessaan myös kustannussäästöjä toimijoille.

Tietosuojalainsäädäntö edellyttää myös organisatoristen menetelmien, esimerkiksi menettelytapojen ja ohjeistusten, käyttöä (L 22.4.1999/523, 32.1 §). Jotta yrityksissä voidaan laatia toimivat ja lainsäädännön vaatimusten mukaiset menettelytavat ja ohjeistukset, täytyy tietää, mitä lainsäädäntö tietojen suojaamiseksi edellyttää. Kuten tutkimus osoitti, koulutuksella voidaan lisätä tietosuojaosaamista. Osaamisen lisääntyessä yrityksissä pystytään laatimaan toimivat ja omaan tarpeeseen sopivat ohjeistukset, mikä selvästi parantaa tietoturvallisuutta.

Tulosten perusteella voidaan nähdä, missä asioissa tarvitaan enemmän koulutusta ja mitkä asiat on jo tiedostettu. Tulokset hyödyntävät paitsi koulutusten järjestäjiä myös koulutusta saavia toimijoita. Tekniset tietoturvamenetelmät olivat toimijoiden keskuudessa melko hyvin tunnetut ja käytetyt. Puutteita oli lähinnä tarvittavan turvallisuustason määrittelyssä ja sitä tukevassa toiminnassa sekä tietosuojaosaamisessa.

Tutkimuksen aiheen valinta oli onnistunut. Se oli mielenkiintoinen ja erittäin ajankohtainen, mikä antoi hyvän lähtökohdan työn onnistumiselle. Tutkimusmenetelmäksi valittu kyselytutkimus sopi tutkimukseen hyvin, kun haluttiin saada kokonaiskuva tietosuojatietämisen ja tietoturvan tasosta Jyväskylässä. Toisaalta olisi ollut mielen-

kiintoista tietää, olisiko toisenlaisella tutkimusmenetelmällä saatu samansuuntaisia tuloksia. Käyttämällä toista tutkimusmenetelmää olisi voitu saada myös sellaista tietoa, mitä verkossa toteutetulla kyselytutkimuksella ei voitu saada.

Kyselyn laatiminen oli haastavaa. Pitkiin ja yksityiskohtaisiin kyselyihin ei vastata, mutta pätevien tulosten saamiseksi tarvittiin riittävän tarkkoja tietoja tutkittavasta ilmiöstä. Kysely pyrittiin laatimaan helpoksi, ymmärrettäväksi ja nopeasti vastattavaksi, mutta toisaalta myös riittävän tarkaksi. Kyselyn laatiminen onnistui hyvin. Tutkimusaineistosta saatiin vastaukset tutkimuskysymyksiin ja tutkimusongelmaan. Tutkimuksen tuloksista johdettuja päätelmiä ei voida kuitenkaan yleistää koko populaatiota koskevaksi. Tulokset pätevät vain kyselyyn vastanneiden joukossa, sillä aineisto jäi harmillisen pieneksi. Etenkin viranomaisten edustus jäi todella vähäiseksi, eikä tutkimuksen tuloksia siltä osin voi yleistää perusjoukon viranomaisiin. Jotta viranomaisten osalta saataisiin päteviä tutkimustuloksia, olisi parasta kohdistaa heille täysin oma tutkimus.

Yksi syy pieneen aineistoon on kyselyiden huima lisääntyminen, mikä on osaltaan aiheuttanut vastausväsymystä. Vastaajia pyrittiin motivoimaan korostamalla saatekirjeissä osallistumisen tärkeyttä sekä vastaajan mahdollisuutta osallistua tärkeään tietoturvallisuuden kehittämistyöhön. Näistä sanallisista motivointikeinoista huolimatta vastausprosentti jäi hyvin alhaiseksi (8 %). Vastaamishalukkuutta olisi voitu yrittää lisätä sillä, että tutkimukseen kutsujana olisi ollut myös toimeksiantajan edustaja, sillä tuntemattoman opiskelijan nimi ei välttämättä vakuuta vastaajaa tutkimuksen tärkeydestä tai aitoudesta.

Otoskokoa kasvattamalla olisi voitu saada kattavampi aineisto. Tutkija kuitenkin luopui siitä aikeesta sen vaatiman suuren työmäärän vuoksi. Tietolähteeksi ensin valittu JYKESin yritysrekisteri ei sisältänyt kaikkien jyväskyläläisten yritysten tietoja, tai ne olivat puutteellisia, ja rekisteriksi vaihdettiin Kauppalehden yritysrekisteri. Se sisälsi kaikkien Jyväskylässä toimivien, mutta myös lopettaneiden, selvitystilassa ja konkurssissa olevien tiedot. Yritysten tiedot täytyi käydä läpi yksitellen, mikä oli erittäin hidasta. Kaikilta aktiivisilta yrityksiltä ei myöskään löytynyt tietoa sähköpostiosoitteesta. Edellä mainittujen seikkojen vuoksi otostutkimus osoittautui kokonaistutkimusta

järkevämmäksi vaihtoehdoksi. Otoksen valintaan käytettiin satunnaisotantaa. Ahkeralla tietojen läpikäymisellä viikon aikana saatiin 1000 sähköpostiosoitetta, joihin kutsu tutkimukseen päätettiin lähettää. Pienemmällä vaivannäöllä, mutta taloudellisin kustannuksin, olisi Tilastokeskukselta voinut tilata helposti käsiteltävän listauksen jyväskyläläisistä toimijoista, jolloin tutkimus olisi voitu suorittaa laajempana. Tutkijan taloudelliset resurssit eivät antaneet siihen kuitenkaan mahdollisuutta.

Aineiston analysointi oli hyvin mielenkiintoista. Kysely toteutettiin Webropol-sovelluksella, jossa oli kuitenkin varsin rajalliset analysointimahdollisuudet. Analysoinnissa käytettiin myös SPSS -ohjelmaa sekä Aki Taanilan tekemää Tilastoapu-ohjelmaa. Analysointivaiheessa aineiston sisältö avautui tutkijalle kokonaisuudessaan ja tulosten raportoinnista ja tulkinnasta tuli hyvin mielenkiintoinen osa koko opinnäytetyöprosessia. Tutkimus antoi osin poikkeavia tuloksia teoriaosuuteen ja aiempaan tutkimukseen nähden, toisaalta teoria tuki hyvin saatuja tuloksia. Tutkimuksen tuloksissa havaittu kehitys tietoturvasta huolehtimisessa tuli hyvin esiin myös teoriassa.

Opinnäytetyöprosessi oli mielenkiintoinen, haastava ja hyvin opettavainen. Tutkijan tietosuojaosaaminen syventyi todella paljon prosessin aikana. Tietoturvan merkityksen ymmärtäminen lisääntyi myös huomattavasti. Tutkija sai myös uusia näkökulmia tietoturva-asioihin. Prosessi toi myös hyvän käsityksen tutkimuksen tekemisestä. Tutkimusprosessin eri vaiheet konkretisoituivat, ja niiden merkitys tutkimuksen onnistumiselle ja tulosten luotettavuudelle ja yleistettävyydelle tuli ymmärretyksi.

Tutkimustuloksia analysoitaessa havaittiin tietoturvakoulutukseen liittyvä ongelma pienyrityksissä. Yhden ja kahden hengen yrityksissä ei nähdä mielekkääksi järjestää koulutuksia vaan tiedon hakeminen on pitkälti oman aktiivisuuden ja halun varassa. Eräs tutkimukseen osallistunut kertoo omana kokemuksenaan:

> *..että jos työntekijöitä ei ole kuin yksi, niin yrityksen sisäisiä koulutuksia on turha järjestää - se että yksityisyrittäjä ainoana työntekijänä sanoo järjestäneensä yrityksen sisäisen IT-koulutuksen sen jälkeen kun on lukenut vaikkapa Tietokone-lehden, menee termeillä kikkailun puolelle..*

Tutkimuksen myötä heräsikin kysymys: Millaiset mahdollisuudet pienyrittäjillä on kehittää tietosuoja- ja tietoturvaosaamistaan?

Myös tietosuojalainsäädäntö on uudistumassa tuoden joitakin uusia velvoitteita myös pienille toimijoille. Lisäksi tietosuojan laiminlyönnit tulevat olemaan ankarasti sanktioituja. Vaikka tällä hetkellä henkilötietojen suojaamisessa pärjää hyvin pelkällä maalaisjärjellä ja terveellä harkinnalla, voi koulutus uudistuvan lainsäädännön tuomista uusista velvoitteista olla kaikille toimijoille tarpeen.

Tutkimuksen tuloksissa oli myös mielenkiintoinen yllätys. Vaikuttaisi siltä, että lain velvoitteista tietoiset osasivat optimoida tietoturvatoimensa muita paremmin. Koska tutkimusaineisto jäi varsin suppeaksi, olisi mielenkiintoista tutkia tarkemmin, että onko asia todella näin. Osaavatko tietosuojalainsäädännön paremmin tuntevat mitoittaa tietoturvatoimensa oikein, kun toiset tuhlaavat resurssejaan ylimitoitettuun tietoturvaan? Halutaanko tiedon puuttuessa enemmän varmistella, että tietoturvatoimet ovat riittävät?

Lopuksi voidaan vielä todeta, että tutkimuksen tulokset huojentavat mieltä. Vaikka tietosuojalainsäädäntö onkin jyväskyläläisille toimijoille suhteellisen tuntematonta, he huolehtivat silti hyvin yrityksensä tietoturvasta, koska asiakkaiden yksityisyys on heille tärkeää.

Lähteet

A 12.11.1999/1030. Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta. Viitattu 17.8.2013. Http://www.finlex.fi, ajantasainen lainsäädäntö.

Airola, O. 2013. Kymmenen uutiset. MTV3 19.1.2013.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2013. Tietosuojavastaavan käsikirja. Helsinki. Tietosanoma.

Castrén, K. 2013. Palkkatoimisto muutti pilveen. Artikkeli tietosuojalehden verkkosivuilta. Julkaistu Tietosuojalehdessä 2/2013. Viitattu xx. Http://www.tietosuojalehti.fi/index.php?mid=2&pid=32&aid=3098#.UeOYW430H4Y

Data Protection in the European Union - Data controllers' perceptions - Analytical Report. 2008. Euroopan Komissio. Viitattu 7.8.2013. Http://ec.europa.eu/public_opinion/, Flash EB, 239-225.

Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta. 2012. Ehdotus yleiseksi tietosuoja-asetukseksi. Viitattu 21.8.2013. Http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fi.pdf.

Erityislainsäädäntö. N.d. Tietosuojavaltuutetun toimiston sivusto. Viitattu 5.8.2013. Http://www.tietosuoja.fi/, Lait.

Eronen, H. 2012. Hoitotietojen väärinkäytökset ja siitä aiheutuvat seuraukset. Viitattu 21.7.2013. Http://www.kuntamarkkinat.fi/, Luentoaineistoja, Luentoaineistoja 2012, Sosiaali- ja terveys.

EU:n tietosuojauudistuksen tavoitteena vahvistaa yksilön oikeutta valvoa henkilötietojaan. 2012. Oikeusministeriön sivustolla 12.4.2012 julkaistu uutinen. Viitattu 21.8.2013. Http://oikeusministerio.fi/fi/, Ajankohtaista, Uutiset, 2012.

Euroopan unionin tietosuojalainsäädännön uudistaminen 2013. Viitattu 21.8.2013.Http://oikeusministerio.fi/fi/, Valmisteilla, Lakihankkeet, Informaatio-oikeus.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä. Docendo Finland.

HE 96/1998. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi. Viitattu 23.8.2013. Http://www.finlex.fi, Hallituksen esitykset.

Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset. 2010. Tietosuojavaltuutetun toimiston antama opas. Viitattu 15.7.2013. Http://www.tietosuoja.fi/ oppaat.

Henkilötietolain seuraamusjärjestelmä 2010. Tietosuojavaltuutetun toimiston opas. Viitattu 3.7.2013. Http://www.tietosuoja.fi/, Oppaat.

Henkilötietolaki. N.d. Viitattu 17.7.2013. Http://www.tietosuoja.fi/, Lait.

Hulkko, K. 2012. Tietoturva on liiketoiminnan elinehto - teot puuttuvat. Artikkeli. Suomenkuvalehti verkkosivuilla. Viitattu 8.8.2013. Http://suomenkuvalehti.fi/jutut/kotimaa/tietoturva-on-liiketoiminnan-elinehto-teot-puuttuvat. Jutut, Kotimaa.

Innanen, A. & Saarimäki, J. 2012. Internetoikeus. 2. uudistettu painos. Helsinki. Edita publishing.

Jabe, M. 2011. Liian moni pomo on pihalla tietosuojasta. Artikkeli julkaistu Fakta lehdessä 26.10.2011. 10/10 nroa. Helsinki. Talentum Media.

JYVSECTEC. N.d. JYVCESTEC-projektin verkkosivut. http://jyvsectec.fi/.

Komissio haluaa helpottaa pk-yritysten toimintaa keventämällä kymmentä eniten hallinnollista rasitusta aiheuttavaa EU:n säädöstä. 2013. Viitattu 7.8.2013. Http://europa.eu/rapid/press-release_IP-13-188_fi.htm.

Korhonen, R. 2010. Oikeusjärjestys: Sähköinen asiointi ja viestintä. 7.täydennetty painos. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 55. ISSN 0788-7604.

Koskinen, S., Alapuranen, L., Heino, A-M & Lehtonen, L. 2012.Henkilötietojen käsittely työelämässä. Helsinki. Edita Publishing.

Kruger, H.A. & Kearney, W.D. 2005. Measuring information security awareness: A West Africa gold mining environment case study. Viitattu 29.10.2013. Http://icsa.cs.up.ac.za/issa/2005/TOC_Paper.htm.

L 11.6.1999/731. Suomen perustuslaki. Viitattu 2.8.2013. Http://www.finlex.fi, ajantasainen lainsäädäntö.

L 13.8.2004/759. Laki yksityisyyden suojasta työelämässä. Viitattu 4.8.2013.. Http://www.finlex.fi, ajantasainen lainsäädäntö.

L 16.6.2004/516. Sähköisen viestinnän tietosuojalaki. Viitattu 4.8.2013.. Http://www.finlex.fi, ajantasainen lainsäädäntö.

L 21.5.1999/621. Lain viranomaisten toiminnan julkisuudesta. Viitattu 21.8.2013. Http://www.finlex.fi, ajantasainen lainsäädäntö.

L 22.4.1999/523. Henkilötietolaki. Viitattu 17.6.2013. Http://www.finlex.fi, ajantasainen lainsäädäntö.

Laadi tietotilinpäätös. 2012. Viitattu 19.8.2013. Http://www.tietosuoja.fi/, Oppaat.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja: Ohjeistus, toteutus ja lainsäädäntö. Helsinki. Edita Publishin.

Lappalainen, E. 2013. Pienet yritykset alttiimpia urkinnalle. Artikkeli Talouselämä – lehden verkkosivuilla 14.6.2013 s.9. . Viitattu 21.6.2013.Http://www.talouselama.fi/uutiset/pienet+yritykset+alttiimpia+urkinnalle++ilmaispalvelut+ovat+kaksiterainen+miekka/a2190218?s=r

Liikkuva työ: Liikkuvan työn tietoturva. N.d. Viitattu 17.7.2013. Http://www.tietoturvaopas.fi/, Yrityksen tietoturvaopas.

Mikkonen, T. 2013. Trusteqin 22.5.2013 antama lehdistötiedote tekemästään kyselystä. Viitattu 7.8.2013. Http://www.trusteq.com/site/assets/files/1262/trusteq_tutkimustiedote.pdf.

Mäki, M. 2007. Työntekijä pahin tietoturvauhka pk-yrityksessä. Artikkeli tietotekniikkaliitto Ry:n verkkosivuilla Pk-tietoturvatutkimuksen tuloksista. Viitattu 27.7.2013. Http://www.ttlry.fi/, Tutkimukset ja tuotteet, Tutkimus ja tilastot, Pk-tietoturvatutkimus.

Nykänen, K. 2011. Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Väitöskirja. ISBN 978-951-42-9571-3. Viitattu 17.6.2013. Http://herkules.oulu.fi/isbn9789514295713/isbn9789514295713.pdf.

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. 2010. VAHTI 2/2010. Viitattu 27.7.2013. Https://www.vahtiohje.fi/web/guest, 2010.

Pekkala, M. 2012. Tietoturvallisuudenhallintajärjestelmän luominen pk-yrityksissä. Tutkielma.Viitattu 27.8.2013. https://aaltopro.aalto.fi/fi/, Koulutus, Koulutushaku, Turvallisuus, Tutkielmia.

Penttilä, T. 2012. Ulkoistaminen ja henkilötiedot. Diaesitys henkilötietojen ulkoistamisesta. Viitattu 30.68.2013. Http://www.slideshare.net/Sonera/tietoturva-2013-titta-penttil-esitys-teliasonera.

Reding, V. 2013. Tietosuojauudistuksen nykytilanne. Euroopan komission tiedote. Annettu Brysselissä 28. tammikuuta 2013. Viitattu 21.8.2013. Http://europa.eu/rapid/press-release_MEMO-13-39_fi.htm

Rosendahl, M. 2003. Tietoturva palvelee kaikkia - on jokaisen vastuulla. Helsingin yliopiston atk-osaston tiedotuslehti 1/2003. Viitattu 10.6.2013 Http://www.helsinki.fi/, Atk, Lehdet, 103.

Rousku, K. 2013. Näitä älä unohda! Tietoviikko 28.3.2013 s.12.

Saako henkilötietoja lähettää sähköpostilla salaamattomana? 2008. Tietosuojavaltuutetun ratkaisu. Tietosuojavaltuutetun toimisto. Viitattu 28.6.2013. Http://www.tietosuoja.fi, Ratkaisut, Työelämä.

Saako henkilötietoja lähettää sähköpostilla salaamattomana? 2008.Tietosuojavaltuutetun kannanotto. Viitattu 12.7.2013. Http://www.tietosuoja.fi/, Ratkaisut, Työelämä.

Saarenpää, A. 2011. Oikeusjärjestys osa 1: Henkilö- ja persoonallisuusoikeus. 7.täydennetty painos. Lapin yliopiston oikeustieteellisiä julkaisuja.

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

Sanastoa.N.d. Tietosuojavaltuutetun sivuston tietosuojasanastoa. Viitattu 22.8.2013. http://www.tietosuoja.fi/.

Special eurobarometer 359 - attitudes on data protection and electronic identity in the european union. 2011.Viitattu. 23.9.2013. Http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Suomen kyberturvallisuusstrategia ja taustamuistio. 2013. Turvallisuuskomitean sihteeristö.Valtioneuvoston periaatepäätös 24.1.2013. Viitattu 30.6.2013. Http://www.yhteiskunnanturvallisuus.fi/, Materiaalit.

Symantec 2010 SMB Information Protection Survey Global Data. 2010. Viitattu 22.7.2013. Http://www.symantec.com/, About Symantec, News Room, Media Resources, Press Kits, Symantec Study: SMBs are Getting Serious about Information Protection.

Taulukot tilastossa: Toimipaikkalaskuri 2013.Tilastokeskuksen toimipaikkalaskuri. Http://www.stat.fi/index.html/, Tuotteet ja palvelut, Tilastotietokannat, T Rekisteri- ja arkistopalvelut Yritysrekisteri, Toimipaikkalaskuri.

Tietosuojavaltuutettu vaatii yrityksiä panostamaan tietoturvaan. 2012. Tietosuojavaltuutetun antama lehdistötiedote. Julkaistu 10.10.2012 tietosuojavaltuutetun toimiston verkkosivuilla. Viitattu 2.6.2013. Http://www.tietosuoja.fi, Ajankohtaista.

Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. 2007. Viitattu 8.8.2013. Https://www.vahtiohje.fi/, 2007.

Tietoturvallisuusasetus. 2012. Valtionvarainministeriön julkaisema esite tietoturvallisuusasetuksesta. Http://www.vm.fi/, Julkaisut ja asiakirjat, Muut asiakirjat, 2012, Tietoturvallisuusasetus-esite.

Tietovuodot. 2011. Tietosuojavaltuutetun sivustolta ajankohtaista tietoa. Viitattu 7.8.2013. Http://www.tietosuoja.fi/, Ajankohtaista, Vuoden 2011 uutisia.

Työelämän tietosuojalaki. N.d. Tietoa työelämän tietosuojalaista Tietosuojavaltuutetun toimiston sivuilta. Viitattu 27.7.2013. Http://www.tietosuoja.fi/, Lait.

Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. 2008. Viitattu 5.9.2013. Http://www.vm.fi/vm/fi/01_etusivu/, Julkaisut ja asiakirjat, Julkaisut, Valtionhallinnon tietoturvallisuus, 2008.

Täsmennystä henkilötiedon määritelmään. 2007. Tietosuojavaltuutetun tiedote. Viitattu 12.6.2013. http://www.tietosuoja.fi, Ajankohtaista, 2007.

Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. 2004. Viitattu 28.8.2013. Https://www.vahtiohje.fi/web/guest, 2004.

Valtionhallinnon tietoturvakäsitteistö. 2004. Valtiovarainministeriön julkaisu. Viitattu 37.6.2013. Http://www.vm.fi/vm/fi/01_etusivu/, Julkaisut ja asiakirjat, Julkaisut, Valtionhallinnon tietoturvallisuus, 2003.

Vanto, J. 2011. Henkilötietolaki käytännössä. 1. painos. Helsinki. WSOYpro.

Vehkalahti, K.2008. Kyselytutkimuksen mittarit ja menetelmät. Helsinki. Kustannusosakeyhtiö Tammi.

Vilkka, H. 2005. Tutki ja kehitä. Helsinki. Kustannusosakeyhtiö Tammi.

Voutilainen, T. 2012, Oikeus tietoon: informaatio-oikeuden perusteet. Helsinki. Edita Publishing.

Vuoden 2010 merkittävimmät tietoturvariskit. 2010. Stonesoft.Viitattu 22.7.2013. Http://www.stonesoft.com/,company, press & media, releases, suomeksi, 2010.

Yritysten rikosturvallisuus 2012: Riskit ja niiden hallinta. 2012. Viitattu 24.7.2013. Http://kauppakamari.fi/, Mitä teemme?, Koulutus, julkaisut ja tapahtumat, Julkaisut, Rikosturvallisuus.

Liitteet

Liite 1. Kyselyn kysymykset

Olet vastaamassa tietosuojatutkimukseen liittyvään kyselyyn. Tutkimus on täysin luottamuksellinen. Vastaaminen tapahtuu anonyymisti eikä vastauksista tai tutkimuksen tuloksista voida tunnistaa yksittäistä vastaajaa

Vastausohjeet ovat jokaisen aihealueen alussa. Vastaaminen vie aikaa noin 10 minuuttia. Alla olevasta palkista voit seurata kyselyn etenemistä

Taustakysymykset

Taustatietoja kysytään vain vastausten tilastollista käsittelyä varten.

Mitä toimialaa toimipaikkanne edustaa?

- Maatalous, metsätalous ja kalatalous
- Kaivostoiminta ja louhinta
- Teollisuus
- Sähkö-, kaasu- ja lämpöhuolto, jäähdytysliiketoiminta
- Vesihuolto, viemäri- ja jätevesihuolto, jätehuolto ja muu ympäristön puhtaanapito
- Rakentaminen
- Tukku- ja vähittäiskauppa; moottoriajoneuvojen ja moottoripyörien korjaus
- Kuljetus ja varastointi
- Majoitus- ja ravitsemistoiminta
- Informaatio ja viestintä
- Rahoitus- ja vakuutustoiminta
- Kiinteistöalan toiminta
- Ammatillinen, tieteellinen ja tekninen toiminta
- Hallinto- ja tukipalvelutoiminta
- Julkinen hallinto ja maanpuolustus; pakollinen sosiaalivakuutus Koulutus
- Terveys- ja sosiaalipalvelut
- Taiteet, viihde ja virkistys
- Muu palvelutoiminta
- Kansainvälisten organisaatioiden ja toimielinten toiminta
- Toimiala tuntematon

Sektori, jota toimipaikkanne edustaa:

- Kunta- tai kuntayhtymä
- Valtio
- Yksityinen yritys

Toimipaikkanne henkilöstön kokonaismäärä:

- 0-4
- 5-9
- 10-19
- 20-49
- 50-99
- 100-249
- 250 tai enemmän

Mikä on asemanne toimipaikassanne?

- Työntekijä
- Luottamusmies
- Työsuojeluvaltuutettu
- Tietoturvavastaava
- Muu henkilöstön valitsema edustaja
- Henkilöstöjohtaja tai muu päällikkö, toimitusjohtaja
- Muu. Mikä?

Sisältävätkö työtehtävänne henkilötietojen käsittelyä?

- Kyllä
- Ei

Onko toimipaikallanne henkilörekisteri asiakastiedoista?

- Kyllä
- Ei

Sisältääkö henkilörekisteri myös arkaluonteisia henkilötietoja, kuten esimerkiksi henkilön terveydentilaa, sosiaalihuollon tarvetta, perhesuhteita tai ammattiliittoon kuulumista kuvaavia tietoja?

- Kyllä
- Ei

Tietosuojakysymykset

Valitkaa seuraavissa tietosuojaa koskevissa kysymyksissä yksi tai useampi mielestänne oikea vaihtoehto.

Käytettävien tietoturvatoimien laajuutta ja tehokkuutta arvioidessa voidaan ottaa huomioon muun muassa:

- käytettävissä olevat tekniset mahdollisuudet
- toimenpiteiden aiheuttamat kustannukset
- suojattavien tietojen laatu ja määrä
- suojattavien tietojen ikä
- Tietojen merkitys yksityisyyden suojan kannalta

Hyvin arkaluontoisten tietojen suojaaminen

- vaatii erityistä huolellisuutta
- saa rasittaa yrityksen tai organisaation taloutta
- ei poikkea muiden tietojen suojaamisesta

Vastuu henkilötietojen käsittelyn lainmukaisuudesta ja suojaamisesta ulkoistamistilanteessa

- on rekisterin omistajalla.
- on palvelun tarjoajalla.
- voidaan sopia rekisterinpitäjän ja palveluntarjoajan välillä kirjallisella sopimuksella.

Yritys tai organisaatio on rekisterinpitäjänä vastuussa tietojen joutumisesta vääriin käsiin, jos

- henkilörekisteri on joutunut tietomurron kohteeksi.
- henkilörekisteri on joutunut varastetuksi.
- henkilörekisteri on varastettu palveluntarjoajan koneelta.
- henkilörekisteri on epähuomiossa jäänyt sivullisen ulottuville, minkä seurauksena sivullinen kopioi tiedot itselleen.
- työntekijä on luovuttanut tietoja rekisteröidyksi tekeytyneelle sivulliselle.
- työntekijä hukkaa henkilötietoja sisältäneen sähköisen laitteen (esim. puhelin, kannettava tietokone, tablet-tietokone jne.).
- henkilötietoja käsitellään suojaamatonta verkkoa hyväksikäyttäen ja sivullinen tahallisesti skannaa tiedot.

Yritys tai organisaatio on rekisterinpitäjänä vastuussa henkilötietojen muuttumisesta, tuhoutumisesta tai katoamisesta, jos

- henkilörekisteri on joutunut tietomurron kohteeksi palvelun tarjoajan palvelimella tai koneella.
- henkilörekisteri on epähuomiossa jäänyt sivullisen ulottuville, minkä seurauksena sivullinen on käsitellyt tietoja.
- työntekijä on vahingossa käsitellyt tietoja.
- työntekijä, jolla ei ole oikeutta käsitellä henkilötietoja, käsittelee kuitenkin niitä.
- henkilötietoja käsitellään suojaamatonta verkkoa hyväksikäyttäen ja ulkopuolinen pääsee siten käsittelemään tietoja.
- henkilötietoja sisältävä järjestelmä tuhoutuu tulipalossa.

Viranomaisten on toteutettava ja ylläpidettävä vähintään tietoturvallisuuden perustason vaatimukset täyttävää tiedonkäsittely-ympäristöä, joka on

- laissa tarkasti määritelty.
- on viranomaisen itsensä vapaasti määriteltävissä.
- on viranomaisen määriteltävissä tietoturvallisuusasetuksen antamien ohjeiden mukaisesti.

Lain mukaan viranomaisten on turvattava asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu

- asianmukaisin menettelytavoin
- tietoturvajärjestelyin
- kaikin mahdollisin keinoin
- tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvatoimenpiteistä aiheutuvat kustannukset huomioiden

Hyvän tiedonhallintatavan toteuttaminen edellyttää

- tiedonhallinnan suunnittelua
- tietojen suojaamista
- henkilöstön perehdyttämistä

Tietoturvakysymykset

Valitkaa seuraavissa tietoturvaa koskevissa kysymyksissä yksi tai useampi toimipaikkaanne kuvaava vaihtoehto.

Toimipaikassanne käytetään käyttäjätunnuksia ja salasanoja järjestelmään tai tietokoneelle pääsemiseksi.

- Kyllä
- Ei
- En tiedä

Järjestelmän käyttöoikeudet ovat jaettu kunkin työtehtävien mukaan.

- Kyllä
- Ei
- En tiedä

Henkilötietoja sisältävät järjestelmät ja/tai tietokoneet ovat suojattu

- palomuurilla
- virustorjuntaohjelmalla

- salasanalla
- tunkeutumisen havaitsemisjärjestelmällä
- niin, että jälkikäteenkin voidaan yksilöidä ja tunnistaa henkilötietoja käsittelevät henkilöt
- niin, että laittomasta järjestelmään tunkeutumisesta tulee ilmoitus rekisterinpitäjälle
- Jotenkin muuten, miten?
- Järjestelmiä ja/ tai tietokoneita ei ole suojattu mitenkään.

Toimipaikassa

- käytetään kulunvalvontaa muun muassa nostamaan tietoturvallisuuden tasoa.
- käytetään kulunvalvontaa muuhun, muttei tietoturvallisuuden vuoksi.
- ei ole kulunvalvontaa.

Toimipaikassa

- käytetään kameravalvontaa muun muassa nostamaan tietoturvallisuuden tasoa.
- käytetään kameravalvontaa muuhun, muttei tietoturvallisuuden vuoksi.
- ei ole kameravalvontaa.

Toimipaikassa

- on järjestetty koulutusta tietosuojasta.
- on määritelty tietosuojaan liittyvät toiminta- ja menettelytavat.
- ei ole järjestetty koulutusta tietosuojasta eikä ole määritelty tietosuojaan liittyviä toiminta- ja menettelytapoja.

Toimipaikassa

- on järjestetty tietoturvakoulutusta.
- on määritelty tietoturvallisuuteen liittyvät toiminta- ja menettelytavat.
- ei ole järjestetty tietoturvakoulutusta eikä ole määritelty tietoturvallisuuteen liittyviä toiminta- ja menettelytapoja.

Asiakastietoja sisältävä henkilörekisteri on tallennettu

- omalle tai palveluntarjoajan palvelimelle.
- tietokoneelle, joka on vain toimipaikan työntekijöiden käytössä.
- tietokoneelle, jota voivat käyttää myös muutkin kuin toimipaikan työntekijät (esimerkiksi perheenjäsenet tai ystävät).

Toimipaikassa on

- määritelty, mitä ohjelmia tietokoneille tai puhelimille ja muille kannettaville laitteille saa asentaa.
- määritelty, millä verkkosivuilla ei saa vierailla toimipaikan tietovälineillä (tietokoneet, kannettavat, puhelimet yms).
- internetin käyttö ja ohjelmien asentaminen jokaisen oman harkinnan varassa.

Toimipaikan tietoaineisto on luokiteltu tietoturvan toteuttamistarpeen arvioimiseksi.

- Kyllä
- Ei
- En tiedä

Tietoaineisto henkilötiedot mukaan lukien pääsääntöisesti

- varmuuskopioidaan itse.
- varmuuskopioidaan tietojen tallennuspaikan palveluntarjoajan (palvelimen ylläpitäjä) toimesta.
- jätetään varmuuskopioimatta.

Arvioikaa seuraavien asioiden merkitystä toimipaikassanne valittujen tietoturvatoimien (esim. virustorjunta, palomuuri, kulunvalvonta, tietoturvaohjeistus) valintaan.

(Ei lainkaan merkitystä, Melko vähän merkitystä, Melko paljon merkitystä, Erittäin paljon merkitystä, Vaikea sanoa)

- Liiketoiminnan jatkuvuuden turvaaminen
- Lainsäädännön vaatimukset tietojen suojaamisesta

- Asiakkaiden yksityisyyden suojaaminen
- Työntekijöiden työskentelyn valvominen
- Laitteiden ja verkkojen toimivuuden varmistaminen
- Tietojen joutumisen estäminen asiattomien käsiin
- Haittaohjelmien leviämisen estäminen
- Rangaistuksen välttäminen esimerkiksi tietomurron tapahduttua
- Tietojen muuttumisen, tuhoutumisen tai katoamisen estäminen
- Muu. Mikä?

Kertokaa lyhyesti, millaisena näette tietosuojalainsäädännön tietojen suojaamis-velvoitteen yhteyden tietoturvaan ja siitä huolehtimiseen teidän toimipaikassanne.

Liite 2. Saatekirje

Hei,

Teknologian kehityksen myötä kyberturvallisuuden merkitys yhteiskunnassamme on korostunut. Samalla yksityisyyden suoja ja tietosuoja ovat tulleet entistä tärkeämmiksi. Tietojen käsittelyn siirtyminen sähköiseen ympäristöön tuo uudenlaisia uhkia, jotka ovat aiempaa vaarallisempia yksilön tietosuojalle ja yrityksille. Suojautuminen näitä uhkia vastaan vaatii jatkuvaa kehitystä. Jyväskylä on valittu vetovastuuseen Työ- ja elinkeinoministeriön INKA-ohjelmaan kyberturvallisuuden kehittämisessä. Jyväskylä Security Technology -hanke eli JYVSECTEC on omalta osaltaan mukana tässä kyberturvallisuuden kehittämistyössä.

Pyydämme Teitä osallistumaan JYVSECTEC:in toimeksiannosta toteutettavaan tietosuojaa ja tietoturvaa koskevaan tutkimukseen. Tutkimus tehdään opinnäytetyönä. Vastaajan olisi hyvä olla toimipaikan tietosuoja- ja tietoturva-asioista vastaava tai päättävä henkilö. Tutkimuksen onnistumiseksi on tärkeää, että vastaatte kyselyyn. Tutkimuksen tulokset tullaan julkaisemaan loppuvuoden aikana.

Alla olevasta linkistä avautuva kyselylomake on lähetetty otokseen valituille 1000 toimijalle julkisella ja yksityisellä sektorilla. Tutkimuksen kohteena olevat toimipaikat on poimittu Kauppalehden yritysrekistereistä satunnaisotannalla. **Kaikkia antamianne tietoja käsitellään ehdottoman luottamuksellisesti.** Kyselyyn vastaaminen tapahtuu anonyymisti eikä vastauksista voida tunnistaa yksittäistä toimipaikkaa tai henkilöä. Tutkimuksen tulokset esitetään myös niin, ettei tutkimukseen osallistuvia toimipaikkoja ja henkilöitä voida tunnistaa. Kerättävää aineistoa käytetään vain tutkimustarkoituksiin.

Lisätietoja tutkimuksesta antaa Kirsi Heimonen. Pyydämme teitä vastaamaan kyselyyn **8.11. mennessä**. Toivomme, että tutkimus on teillekin tärkeä ja haluatte vaikuttaa osaltanne sen onnistumiseen.

Kiitämme yhteistyöstä ja arvokkaasta tutkimusavustanne!

Jyväskylässä lokakuussa 2013

Kirsi Heimonen

Liite 3. Muistutuskirje

Hei!

Saitte viikko sitten kutsun JYVSECTEC:in toimeksiannosta tehtävään tietosuojaa ja tietoturvaa koskevaan tutkimukseen. Tutkimus toteutetaan opinnäytetyönä. Mikäli ette ole vielä vastanneet kyselyyn, pyydämme teitä vastaamaan mahdollisimman pian. Jos olette jo vastanneet, kiitämme teitä arvokkaasta avustanne!

Osallistumalla tutkimukseen olette avuksi tietoturvallisuuden kehittämistyössä. Luotettavien tutkimustulosten saamiseksi jokaisen vastaus on tärkeä! Vastaaminen tapahtuu anonyymisti eikä vastauksista voida tunnistaa yksittäistä toimipaikkaa tai henkilöä. Vastaamalla mahdollisimman pian, voitte vaikuttaa tutkimuksen tuloksiin. Toivomme vastaustanne kuitenkin viimeistään torstaihin 14.11.2013 mennessä. Vastaamaan pääsette alla olevasta linkistä.

Lisätietoja tutkimuksesta ja kyselystä antaa tarvittaessa Kirsi Heimonen. Kiitämme yhteistyöstä ja arvokkaasta tutkimusavustanne!

Jyväskylässä marraskuussa 2013

Kirsi Heimonen
Oikeustradenomiopiskelija
JAMK