LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Tietosuoja pilvipalveluissa

Case: LAMK

LAHDEN
AMMATTIKORKEAKOULU
Liiketalouden ala
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kevät 2016
Tomi Viitala

Lahden ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

VIITALA, TOMI:

Tietosuoja pilvipalveluissa
Case: LAMK

Tietojenkäsittelyn opinnäytetyö, 55 sivua, 2 liitesivua

Kevät 2016

TIIVISTELMÄ

Opinnäytetyössä selvitettiin organisaation tietojen tietosuojan varmistamista siirryttäessä käyttämään pilvipalvelupohjaisia ratkaisuja. Opinnäytetyö toteutettiin Lahden ammattikorkeakoululle keväällä 2016. Tavoitteena oli kartoittaa LAMKin käyttämät keinot ja toimintaperiaatteet, joilla se pyrkii varmistamaan tietojen tietosuojan, kun käyttöön otetaan pilvipalveluita.

Tutkimus oli laadullinen ja siinä käytettiin deduktiivista lähestymistapaa. Aineistoa tutkimukseen kerättiin sellaisten henkilöiden haastatteluilla, ketkä toimivat keskeisessä asemassa LAMKin siirtyessä pilvipalveluihin. Haastattelut toteutettiin puolistrukturoituina ja ne tallennettiin.

Tutkimustulosten mukaan organisaation tietojen tietosuojaa voidaan varmistaa monilla eri seikoilla. Tutkimuksessa selvisi, että henkilökunnan ohjeistaminen henkilötietojen käsittelyssä sekä esimerkiksi siinä, mitä tietoa pilvipalveluihin voi tallentaa, on yksi varmistuskeino suojata tietoa. Pääsyoikeuksia eri järjestelmiin ja palveluihin nähtiin hyväksi hallita henkilökohtaisilla käyttäjätunnuksilla ja salasanoilla. Luottamuksellisen tiedon lähettämistä sähköpostilla varmistetaan sähköpostin salauksella. Tutkimustulokset kertovat, että turvallista pilvipalveluiden käyttöä mobiililaitteilla toteutetaan laitteen tietoturva-asetuksilla ja että laitteet ovat etähallittavia.

Tutkimuksessa selvisi, että pilvipalveluiden tietosuojariskeihin varaudutaan tarpeen tullen riskikartoituksen tekemisellä ennen palvelun käyttöönottoa. Palveluntarjoajan kanssa koetaan myös tarpeelliseksi sopia, että tiedot säilytetään vain Euroopan alueella. Tämä sovitaan palveluntarjoajan ja asiakkaan välisessä palvelutasosopimuksessa (SLA). Lisäksi siinä sovitaan tärkeitä tietojen tietosuojaan liittyviä asioita, kuten mm. palveluntarjoajan ja asiakkaan vastuiden jakaminen, saatavuus ja vasteajat. Ulkopuolisen konsultointiavun käyttäminen eri osa-alueilla koettiin vahvistavan pilvipalveluiden sujuvaa käyttöönottoa, etenkin lainsäädäntöön liittyvissä asioissa.

Asiasanat: tietosuoja, pilvipalvelut, tietoturva, internet

Lahti University of Applied Sciences
Degree Programme in Information Technology

VIITALA, TOMI: Data Protection in Cloud Computing
CASE: LAMK

Bachelor's Thesis in Information Technology, 55 pages, 2 pages of appendices

Spring 2016

ABSTRACT

This thesis discusses how an organization can ensure data protection when starting to use cloud-based services. This thesis was conducted for Lahti University of Applied Sciences in spring 2016. The aim was to map the means and principles the University applies in order to ensure data protection when it transfers to cloud-based services.

This thesis is a qualitative study and applies a deductive research approach. Data was collected by interviewing the people who have been working in key positions when the University started using cloud-based services. The interviews were carried out as semi-structured interviews, and they were recorded.

According to the results, there are many ways to ensure data protection in an organization. One way to protect data is to instruct the staff how to handle personal details and give instructions on what kind of data is allowed to be saved in the organization's cloud. It was seen beneficial to control access rights into different systems and services with personal user identifications and passwords. Sending confidential data via email is secured with encryption. Finally, based on the results, when using cloud services on mobile devices, security is ensured according to the devices' security settings and by making sure the devices can be managed remotely.

The study found that, if necessary, an organization can prepare for security risks in cloud services by making a risk assessment prior to implementation. It is desirable to agree with the service provider that all data will be stored only in the European area. This will be agreed in Service Level Agreement between the provider and the client. In addition, the agreement includes topics related to data protection such as the division of responsibilities between the service provider and the client, and availability and response times. The use of external consultants was considered to strengthen an easy implementation of cloud services, especially regarding legal matters.

Keywords: data protection, cloud computing, data security, internet

SISÄLLYS

1 JOHDANTO

Yritysten toimintojen siirtyminen pilvipalveluihin on viime aikoina ollut kovassa nousussa. Suomen yrityksistä jopa yli puolet on siirtynyt pilvipalveluiden käyttäjiksi (Tilastokeskus 2014). Suosio selittyy monista hyödyistä, joita pilvipalvelut tarjoavat yrityksille. Pilvipalvelut mahdollistavat palvelujen ja tietojen vaivattoman käytön missä päin maailmaa tahansa. Palveluiden käyttö lisää kustannussäästöjä esimerkiksi IT-tuen tarpeen vähenemisellä ja lisäksi se on helppo ottaa käyttöön (Hanhirova 2011).

Ajatus siitä, että yrityksen tärkeää tietoa tallennetaan ”pilveen”, jonka konkreettista sijaintia ei välttämättä tiedä, saattaa herättää käyttäjissä epävarmuutta. Omassa sisäverkossa palomuurin takana toimiva palvelu ei ole juurikaan sen enempää suojattu. Pilvipalveluita tuottavat yrityksen ovat sen sijaan panostaneet tiedon turvaamiseen niin suurilla investoinneilla, että mikään yksittäinen organisaatio ei siihen yksin kykenisi.

Pilvipalveluiden käytön esteitä on aiemmin tutkittu ja tuloksista ilmenee, että mm. tiedon puute, tietoturvariskit ja epävarmuus oikeudellisissa kysymyksissä ovat keskeisiä huolenaiheita pilvipalveluiden käyttöönotossa (Tilastokeskus 2014).

Tämän kvalitatiivisen opinnäytetyön aiheena on ”Tietosuoja pilvipalveluissa”. Aihe on kiinnostava, koska tulevaisuudessa yhä useampi organisaatio tulee ottamaan käyttöönsä erilaisia pilvipalvelupohjaisia ratkaisuja. Tutkittava ilmiö on ”Organisaation tietosuojan varmistaminen”. Isoilla ja pienillä organisaatioilla on paljon suojattavaa tietoa, joiden päätyminen vääriin käsiin saattaa vahingoittaa yritystä ja sen mainetta. Suojattavia tietoja voivat olla esimerkiksi henkilötiedot, yrityksen strategiset suunnitelmat, toimintaan ja käyttökustannuksiin liittyvät tiedot sekä kaikki taloudellisiin asioihin liittyvät tiedot. Tässä opinnäytetyössä tutkitaan, millä keinoilla ja toimintaperiaatteilla Lahden ammattikorkeakoulun tietojen tietosuoja pyritään varmistamaan, kun siirrytään käyttämään pilvipalvelupohjaisia ratkaisuja. Tutkimukseen kerätään aineistoa henkilöiden haastatteluilla.

2 TUTKIMUSTEHTÄVÄ

2.1 Tutkimuskysymys ja tavoitteet

Tutkimuksen tutkimuskysymys on: **”Kuinka organisaation tietojen tietosuoja pyritään varmistamaan siirryttäessä pilvipalvelupohjaisiin ratkaisuihin?”** Tutkimuskysymyksen tyyppi on kuvaileva, millä saadaan selville ilmiön tiedot ja ominaisuudet.

Tutkimuksen tavoitteena on löytää LAMKin käyttämät keinot ja toimintaperiaatteet, joilla se pyrkii varmistamaan tietojen tietosuojauksen siirryttäessä käyttämään pilvipalvelupohjaisia ratkaisuja. Tutkimuksessa selvitetään, mitä tietosuojaan liittyviä asioita LAMKissa otetaan huomioon pilvipalvelu-siirtymäprosessissa ja minkälaisia tietosuojan turvaamiseen liittyviä päätöksiä siinä tehdään.

Tutkimus on rajattu käsittelemään tietojen tietosuojan varmistusta pilvipalveluihin siirtyessä, eikä tarkoituksena ole selvittää niinkään tietoturvaan liittyviä teknisiä ratkaisuja. Tutkimus suoritettiin toimeksiantona keväällä 2016.

2.2 Tutkimuksen taustat

LAMKiin ollaan perustamassa omaa tietohallintoa hiljattain aloittaneen tietohallintopäällikön johdolla. LAMK on ottamassa käyttöönsä Office365-pilvipalveluja, joten tutkimustyö on ajankohtainen.

Pilvipalveluihin siirtyessä yrityksen tärkeät tiedot saattavat olla toisen osapuolen hallinnassa, joten tietosuojaan liittyvät seikat prosessin aikana on syytä selvittää.

2.3 Tutkimusmenetelmät

Tutkimus noudattaa deduktiivista, eli teorialähtöistä lähestymistapaa. Kyseessä on teorialähtöinen tutkimus, kun tutkimusaineistoa analysoidaan

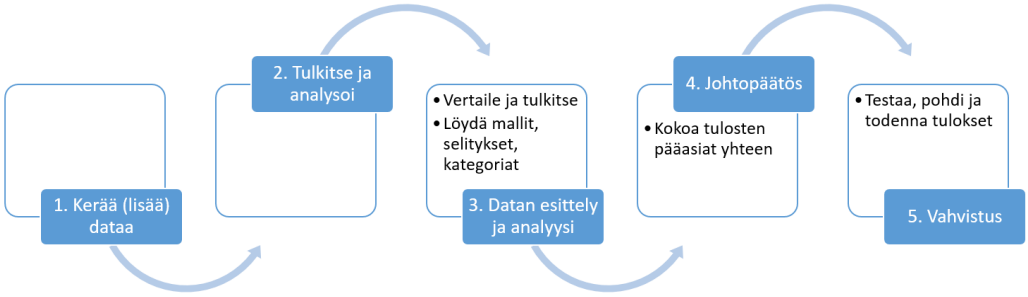
jo olemassa olevan teorian tai mallin mukaisesti. Aineiston analyysiin vaikuttaa siis valmis malli, ja tavoitteena on tämän ennestään tutun mallin tai teorian testaaminen uudessa tilanteessa. (Saaranen-Kauppinen & Puusniekka 2006a.) Tähän tutkimukseen soveltuu parhaiten deduktiivinen lähestymistapa, koska aiempi teoria edesauttaa haastattelun kysymysten muodostamisessa sekä aineiston analyysin tekemisessä. Teoriasta saatujen linjausten pohjalta tutkimusaineistosta on helpompi tehdä johtopääköksiä sekä antaa mahdollisia parannusehdotuksia toimeksiantajalle.

Tämä empiirinen tutkimus on laadullinen eli kvalitatiivinen, jossa kerättyä aineistoa verrataan teoriaan ja se toteutetaan case, eli tapaustutkimuksena. Tutkimusaineisto koostuu muutamien henkilöiden haastatteluista.

Empiirisessä tutkimuksessa tehdään konkreettisia havaintoja tutkimuskohteesta. Havaintojen jälkeen ne analysoidaan ja mitataan tutkimustulosten saamiseksi. (Jyväskylän yliopisto 2015a.) Opinnäytetyö toteutetaan tapaustutkimuksena, jonka keskeinen piirre on empiirinen tutkimus. Tämän vuoksi tutkimus on johdonmukaista toteuttaa empiirisenä.

Laadulliselle tutkimukselle on tunnusomaista pyrkiä ymmärtämään tutkittavaa ilmiötä. Päämääränä on selvittää ilmiön merkitys tai tarkoitus sekä saamaan kokonaisvaltainen ja syvä käsitys ilmiöstä. Menetelmän kuvaus tuottaa kuvailevaa ja selittävää aineistoa. Laadullisen tutkimuksen vaihtoehtona pidetään määrällistä tutkimusta eli kvantitatiivista tutkimusta. Siinä kohdetta kuvataan ja tulkitaan tilastojen ja numeroiden avulla. Tutkimuksien menetelmäsuuntauksien välistä eroa korostetaan usein, vaikka kumpaakin suuntausta voidaan käyttää samassa tutkimuksessa ja molemmilla on mahdollista selittää samoja tutkimuskohteita eri tavoin. (Jyväskylän yliopisto 2015b.) Tässä tutkimuksessa käytetään laadullista menetelmää, koska se soveltuu paremmin vastaamaan tutkimusongelmaan.

Laadullisen aineiston analyysiprosessi (KUVIO 1) alkaa aineiston keruusta, jonka jälkeen aineistoa tulkitaan ja analysoidaan. Tarvittaessa aineistoa kerätään lisää. Kun mallit, selitykset ja kategoriat on löydetty, esitellään aineisto ja analyysi. Johtopäätöksessä kootaan tulosten pääasiat yhteen, jonka jälkeen tutkimuksen tekijä testaa, pohtii ja todentaa tulokset vahvistamalla ne.



KUVIO 1. Laadullisen analyysin prosessi

Tapaustutkimukselle on tunnusomaista valita tutkimuskohteeksi yksittäinen tapaus, tilanne tai tapahtuma. Yksittäistapauksia tutkitaan niiden luontaisessa ympäristössään kuvailemalla yksityiskohtaisesti tutkittavaa ilmiötä. (Saaranen-Kauppinen & Puusniekka 2006b.) Sen tavoitteena on tuottaa tietystä tapauksesta yksityiskohtaista ja intensiivistä tietoa, joten se ei pyri yleistettävyyteen samanlaisin keinoin kuin survey-tutkimus (Jyväskylän yliopisto 2015c.) Tämä opinnäytetyö toteutetaan tapaustutkimuksena, koska sillä on tilausta ja siitä on hyötyä toimeksiantajalle.

Tutkimuksen teoriaosuudessa syvennytään erikseen tietosuojakäytäntöihin ja pilvipalveluihin sekä siihen, kuinka tietosuoja huomioidaan pilvipalveluissa. Näitä tarkastellaan kirjallisuuden ja aiemmin tehtyjen tutkimusten avulla. Tutkimuksessa käytetään tukena olemassa olevia teorioita, kuten millaisilla keinoilla tietosuojaa voidaan parantaa yrityksessä. Käytössä on myös teoriaa siitä, kuinka lainsäädäntö vaikuttaa henkilötietojen käsittelyssä sekä teoriaa henkilötietojen luovutuksista ja siirroista EU:ssa ja sen ulkopuolella. Lisäksi käytetään teorioita siitä, mitä

tietosuojaa vahvistavia seikkoja kannattaa ottaa huomioon pilvipalveluihin siirtyessä, tietoturvan rooli tietosuojan varmistamisessa ja tiedon suojaamisen varmistuskeinot pilvipalveluissa.

Tutkimusaineisto analysoidaan tutustumalla aineistoon huolellisesti. Nauhoitettu haastattelu litteroidaan tekstiksi, jonka jälkeen haastattelut luetaan läpi. Tämän jälkeen tekstistä merkataan ylös tärkeimmät havainnot fontin väriä muuttamalla.

2.4 Avainsanat

Tietosuoja

Yleensä tietosuojasta puhuttaessa tarkoitetaan ihmisen oikeutta omiin tietoihinsa. Tässä tutkimuksessa tietosuojalla tarkoitetaan sen lisäksi organisaation luottamuksellisten tietojen suojausta. Luottamuksellista tietoa on kaikkialla organisaatiossa. Tähän sisältyy mm. henkilötiedot, yrityksen strategiset suunnitelmat, toimintaan ja käyttökustannuksiin liittyvät tiedot ja kaikki taloudellisiin asioihin liittyvät tiedot.

Tietoturva

Syrjälän (2015) mukaan tietosuojan varmistamiseen liittyy osaltaan myös tietoturva. Tietoturvalla pyritään suojaamaan organisaation tärkeät tiedot ulkopuolisilta. Organisaation tietojen koskemattomuus voidaan taata tietoturvaan liittyvillä toimenpiteillä. Tietoturvaa voidaan arvioida sovellustietoturvan, datan suojauksen, salausavainten hallinnan, pääsynvalvonnan, lokien valvonnan, tunkeutumisen estämisen, tietoturva-standardien noudattamisen ja vaatimustenmukaisuuden näkökulmasta.

Pilvipalvelut

Pilvipalvelut ovat “pilvessä” tarjottavia palveluita. Tarkemmin kuvattuna ne ovat verkkopohjaista tiedonhallintaa, jossa tietokoneiden ohjelmistot, osa laitteistoa sekä kaikki tieto sijaitsevat verkossa, eikä käyttäjien tietokoneilla. Kaikki käyttäjän data on saatavilla verkon välityksellä

pilvestä, jonka tietokoneet ja mobiililaitteet osaavat ymmärtää. (Hanhirova 2011.)

Office365

Office365 on Microsoftin tarjoama pilvipalveluratkaisu. Sen tietty versio sisältää Office-ohjelmat työasemiin sekä selaimella käytettävään Office-ohjelmaan. (Arstila 2012.) Kattavimpaan palvelupakettiin sisältyy lisäksi mm. julkaisuohjelma Publisher, tiedostojen säilytys- ja jakopalvelu OneDrive, pikaviestintä- ja videoneuvotteluohjelma Skype for Business sekä sähköposti- ja kalenteriohjelma Exchange Online.

Lahden ammattikorkeakoulu

Lahden ammattikorkeakoulu on Päijät-Hämeessä toimiva monialainen ja kansainvälinen korkeakoulu. Henkilöstöä Lahden ammattikorkeakoulussa on noin 400 ja opiskelijoita yli 5000. Koulutusaloja ovat liiketalous, matkailu, muotoilu ja viestintä, musiikki, kuvataide, sosiaali- ja terveysala sekä tekniikka. (Lahden ammattikorkeakoulu 2016.)

3 TEOREETTINEN VIITEKEHYS

3.1 Tietosuoja

Perinteinen käsitys tietosuojasta on henkilötietolain ja erityislakien henkilötietojen käsittelyä koskevien vaatimusten huomioimista yksityisen henkilöiden yksityisyyden suojan ja oikeusturvan varmistamiseksi (Andreasson, Koivisto & Ylipartanen 2013, 14). Tietoja käsiteltäessä on aina huolehdittava sen lainmukaisesta käsittelystä. Viranomaisten tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi pitää huoli asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen vaatimasta saatavuudesta, käytettävyydestä, suojaamisesta sekä eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä. (Andreasson ym. 2013, 21.)

Tietosuojan huomioon ottamisen tarpeet ovat kasvaneet yrityksissä kerättävien henkilötietojen sekä niiden käsittelytapahtumien määrän kasvun myötä. Informaatioteknologia, tallentamiskapasiteetti ja tiedonsiirron menetelmät ovat kehittyneet viime vuosikymmeninä sellaista vauhtia, että yritykset ovat ottaneet käyttöön tietojärjestelmiä, joita ei ole aiemmin ollut edes mahdollista toteuttaa. (Salminen 2009, 18.)

Tämän kehittymisen myötä yrityksille on syntynyt henkilötiedoista tietovarantoja, jotka muodostavat useilla liiketoiminnan aloilla tietopääomaa. Tekniikka mahdollistaa yrityksille jatkuvasti uusia tietojen käsittelyyn perustuvia mahdollisuuksia, mutta samanaikaisesti tietojen käsittelyn ja yksityisyyden suojaamisen riskit ovat lisääntyneet. (Salminen 2009, 19.)

3.2 Tietosuojalainsäädäntö

Tietosuojalainsäädännön tarkoituksena on luoda henkilötietojaan luovuttaville henkilöille oikeuksia ja samanaikaisesti asettaa henkilötietoja käsitteleville yrityksille velvollisuuksia. Tietosuojalainsäädäntö ei siis suojaa tietoa, vaan henkilöä ja hänen oikeuksiaan omiin tietoihinsa.

Tämän lisäksi lainsäädännöllä on tarkoitus suojata yksilöä hänen henkilötietojensa vahingolliselta käytöltä. (Salminen 2009, 15.)

Informaatio- ja viestintäteknologioiden vauhdikas kehitys on vaikuttanut tietosuojalainsäädännön syntymiseen. Tietosuojaa koskevia kysymyksiä on alettu lainsäädännön avulla ratkomaan laajemmin vasta viime vuosikymmeninä. Tämän vuoksi lainsäädäntö on siis vielä varsin nuorta verrattuna moneen muuhun lainsäädännön alueeseen. Odotettavissa onkin, että tietosuojalainsäädännön vaikutus yritysten toiminnassa kasvaa edelleen sitä mukaan, kun yritykset ottavat uusia sähköisen liiketoiminnan teknologioita käyttöön ja asiakastietojen käsittelyn merkitys liiketoiminnassa kasvaa. (Salminen 2009, 19-20.)

Suomessa oikeus yksityisyyden suojaan on perusoikeus. Suomen perustuslain mukaan henkilötietojen suojasta säädetään lailla (Suomen perustuslaki 731/1999, 10 §). Perustuslaki sisältää näin ollen lainsäädäntö toimeksiannon, johon henkilötietolaki ja muu lainsäädäntö henkilötietojen suojaamisesta perustuu (Salminen 2009, 43). Seuraavat säännökset toteuttavat oikeutta yksityisyyden suojaan.

3.2.1 Henkilötietolaki

Henkilötietolaki on tärkein tietosuojaa koskeva laki Suomen lainsäädännössä. Laki tunnetaan yleislakina, ja sen tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä. (Salminen 2009, 45.) Lisäksi se on säädetty edistämään hyvän tietojenkäsittelytavan kehittämistä ja noudattamista (Tietosuojavaltuutetun toimisto 2013).

Lakia sovelletaan automaattiseen henkilötietojen käsittelyyn sekä muuhun henkilötietojen käsittelyyn silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. Jos kyseessä on yrityksiä tai yhteisöjä koskevien tietojen käsittelyä, ei henkilötietolakia sovelleta, ellei näihin rekistereihin kuulu myös henkilötietoja.

Henkilötietolaki on niin sanottu yleislaki suhteessa erityislainsäädäntöön. (Salminen 2009, 45.)

3.2.2 Julkisuuslaki

Julkisuuslain tehtävänä on erotella henkilörekisteristä tapahtuvan julkisten henkilötietojen nähtäväksi antaminen ja henkilötietojen luovuttaminen toisistaan (Tietosuojavaltuutetun toimisto 2014). Julkisuuslainsäädännön mukaan tieto on julkista, ellei se julkisuuslain tai muiden säädösten perusteella ole salassa pidettävää. Yksityisen palveluntuottajan toimiessa julkisen sektorin organisaation lukuun, palveluntuottajaa velvoittaa julkisuuslaki niiden toiminnassa syntyvien tietojen osalta, joissa rekisterinpitäjänä toimii julkishallinnon viranomainen. (Andreasson ym. 2013, 21-22).

3.2.3 EU:n tietosuojauudistus

EU:n uusi tietosuoja-asetus tulee korvaamaan vuonna 1995 annetun henkilötietodirektiivin. Tekniikan nopea kehitys ja globalisoituminen ovat tuoneet mukanaan uudenlaisia haasteita henkilötietojen varmistamiseen. Henkilötietoja kerätään nykyään kehittyneemmin, joten sitä on aikaisempaa vaikeampi havaita. Tämän kaltaisten haasteiden vuoksi EU:n on luotava johdonmukainen lähestymistapa, joka takaa, että yksilön tietosuojaa koskevaa perusoikeutta noudatetaan sekä EU:ssa että sen ulkopuolella. (Oikeusministeriö 2015.)

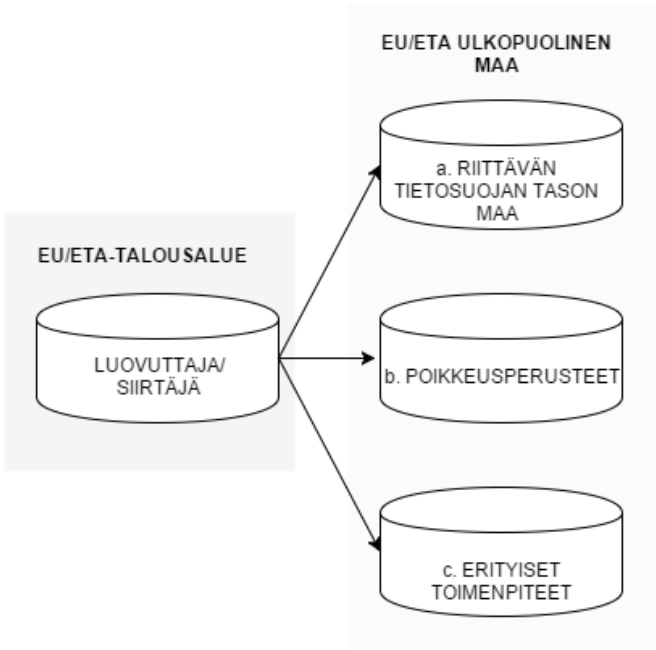
Ehdotuksen tavoitteena on luoda Euroopan unionille ajanmukainen, vahva, yhtenäinen ja kattava tietosuojakehys. Lisäksi tavoitteena on parantaa luottamusta online-palveluihin ja siten edistää EU:n digitaalista sisämarkkinoiden kehittämistä. Ehdotuksen tarkoituksena on nykyaikaistaa tietosuojadirektiivin periaatteet. Asetus sisältää säännöksiä mm. henkilötietojen käsittelyä koskevista periaatteista, käsittelyn lainmukaisuudesta, rekisteröiden suostumuksen edellytyksistä ja arkaluonteisten tietojen käsittelystä (Tietosuojavaltuutetun toimisto 2015a).

Tietosuojauudistuksen merkittävin vaikutus koskee kaikkia julkisyhteisöjä ja yrityksiä, jotka käsittelevät vuosittain yli 5 000 henkilön tietoja. Näiden tahojen olisi perustettava tietosuojavastaavan tehtävä uudistuksen toteutuessaan. Uuden säännöstelyn tavoite on ohjata yhteisöt ja yritykset ottamaan kokonaisvaltaisesti huomioon tietosuoja-asiat toimintansa suunnittelussa. (Andreasson 2015.)

3.3 Henkilötietojen luovutuksien ja siirtojen periaatteet EU:ssa ja ETA:ssa

EU:n sisällä ja Euroopan talousalueella voidaan tietoja liikuttaa vapaasti Euroopan unionin periaatteiden mukaisesti. Henkilötietoja voidaan siirtää vapaasti EU-maiden välillä, kuten se olisi mahdollista siirtää yhden jäsenmaan sisällä. Rekisterinpitäjä ei ole ilmoitusvelvollinen tietosuojavaltuutetulle siirrättäessä henkilötietoja esimerkiksi Suomesta toiseen EU-maahan tai Euroopan talousalueeseen. (Salminen 2009, 83–84)

Sähköisessä liiketoiminnassa palvelun tuotanto ja henkilötietojen käsittely on mahdollista siirtää maantieteellisesti myös muihin maihin. Monet palveluita tuottavat tietojärjestelmät saattavat sijaita useassa eri maassa ja henkilötietojen käsittely voi olla levittäytynyt monien eri oikeusjärjestysten alueille. EU:n ja ETA:n ulkopuoliset maat voidaan jakaa kolmeen osioon (KUVIO 2).



KUVIO 2. Henkilötietojen siirrot ja luovutukset EU/ETA-alueen ulkopuolelle (Salminen 2009, 88).

A. Riittävän tietosuojan maa

Henkilötietoja on mahdollista siirtää maihin, joissa taataan riittävä tietosuojan taso. EU:n komissio ylläpitää listaa niistä maista, jotka se katsoo riittävän tietosuojan tason vaatimukset täyttäviksi. Tämän kaltainen maa takaa noudattavansa riittävän tasokkaita tietosuojan periaatteita ja kunnioittavansa rekisteröityjen oikeuksia. Lisäksi kyseinen maa osoittaa, että sillä on riittävät valmiudet ja tehokkaat menetelmät niiden toteuttamiseksi. (Salminen 2009, 88.) EU:n komission mukaan riittävän tietosuojan maita ovat Australia, Canada, Guernsey, Havaiji, Hong Kong, Mansaari, Israel, Japani, Jersey, Uusi-Seelanti, Etelä-Korea, Taiwan ja Thaimaa (European Commission 2015).

Lokakuussa 2015 EU-tuomioistuin antoi päätöksen, jossa se on todennut Yhdysvaltalaisen Safe Harbor -järjestelmän pätemättömäksi (EU-tuomioistuin C-362/14). Tätä ennen Yhdysvallat oli turvallisen tietosuojan tason maa vain Safe Harbor -järjestelmän osalta. Safe Harbor -järjestelmä perustettiin yhdysvaltalaisia organisaatioita varten, jotka sitoutuivat noudattamaan Yhdysvaltojen kauppaministeriön ja komission hyväksymiä

yksityisyyden suojaa koskevia Safe Harbor -periaatteita. Järjestelmässä sovellettiin tehokkaan henkilötietojen suojan takaavaa lainsäädäntöä tai säännöstöä. (Tietosuojavaltuutetun toimisto 2015b.)

B. Poikkeusperusteet

Tietoja on mahdollista siirtää poikkeuksien perusteella myös maihin, joiden tietosuojan riittävää tasoa komissio ei ole todennut. Poikkeusperusteet ovat sallittuja tapauksissa, joissa rekisteröity on antanut suostumuksensa siirtoon tai siirto on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi. Siirto onnistuu myös, jos rekisterinpitäjä antaa sopimuslausekkein tai toisella tavoin riittävät takeet henkilöiden yksityisyyden ja oikeuksien suojasta. (Salminen 2009, 89.)

C. Riittävän tietoturvallisuuden takaavat erityiset toimenpiteet

Henkilötietoja voidaan siirtää erilaisilla mallisopimuksilla myös EU:n ja ETA-alueen ulkopuolisiin maihin, vaikka riittävää tietosuojan tasoa ei ole vahvistettu. Tällöin tietojen siirtäjä ja vastaanottaja tekevät keskenään sopimuksen, jossa rekisterinpitäjä asettaa tietojen vastaanottajalle velvollisuuksia. Ehtojen tulevat olla yhtenäiset Euroopan tietosuojalainsäädännön vaatimuksien kanssa ja sopimuksella on turvattava asetettujen ehtojen tehokas toteuttaminen. EU:n komissio on sallinut erityisiä mallisopimuslausekkeita, joita voidaan käyttää hyväksi riittävän tietosuojan tason turvaamiseksi. Mallisopimuksia hyödyntäen tietojen siirto on yksi tärkeimmistä tietojen siirron poikkeusperusteista. (Salminen 2009, 90.)

3.4 Pilvipalvelut

Salon (2010, 16) mukaan pilvipalveluista on olemassa runsaasti eri käsitteitä ja niitä syntyy koko ajan lisää. Hanhirovan (2011) määritelmän mukaan pilvipalvelut ovat “pilvessä” tarjottavia palveluita. Tarkemmin kuvattuna ne ovat verkkopohjaista tiedonhallintaa, jossa tietokoneiden ohjelmistot, osa laitteistoa sekä kaikki tieto sijaitsevat verkossa eikä

käyttäjien tietokoneilla. Kaikki käyttäjän data on saatavilla verkon välityksellä pilvestä, jonka tietokoneet ja mobiililaitteet osaavat ymmärtää. Nykyään pilvipalvelut täydentävät organisaation omia järjestelmiä tai jopa korvaavat ne täysin (Andreasson ym. 2013, 93).

National Institute of Standards and Technology (NIST) mukaan pilvipalveluiden viisi ominaispiirrettä ovat

- itsepalvelullisuus
- pääsy palveluihin eri päätelaitteilla
- resurssien yhteiskäyttö
- nopea joustavuus
- käytön tarkka mittaaminen.

Itsepalvelullisuudella tarkoitetaan, että IT-resursseja voidaan ottaa itse käyttöön ja lopettaa ilman tarvetta olla yhteydessä palveluntarjoajaan. Itsepalvelulla käyttäjä voi itse määrittää, milloin resursseja käyttää, mitä resursseja käyttää ja miten niitä käyttää. (Salo 2010, 17.)

Päätelaiteriippumaton palveluiden käyttö on mahdollista työasemalla, kannettavalla ja mobiililaitteella. Palveluiden resurssien hyödyntäminen onnistuu kaikkialla, missä on verkkoyhteys. (Salo 2010, 18.)

Resurssien yhteiskäyttö mahdollistaa palveluntarjoajalle korkean käyttöasteen, koska iso osa sen asiakkaista käyttää samaa laitteisto- ja ohjelmistokapasiteettia yhteisesti toisistaan tietämättä tai riippumatta. Lisäksi palveluntarjoaja voi mittakaava- ja skaalaetujen avulla pitää edullisia hintoja. Ylläpito on tehokasta yhteiskäytön vuoksi, mutta samalla se tuo mukanaan haasteita, kuten käyttäjien eristäminen toisistaan sekä mahdollisen asiakkaan häiriöllisen toiminnan rajaaminen siten, että se ei häiritse toisia käyttäjiä. (Salo 2010, 18.)

Pilvipalvelut ovat nopeasti joustavia palveluita, jotka skaalautuvat helposti ja nopeasti ylös- ja alaspäin. Asiakkaan näkökulmasta kapasiteettirajoitteita ei ole juuri lainkaan ja laskenta-, tallennus- ja

tietoliikennekapasiteetin lisääminen onnistuu tarpeen tullessa lähes saman tien. (Salo 2010, 18.)

Palveluiden resurssien käyttö on tarkan valvonnan ja mittauksen alaista. Asiakas maksaa vain siitä osuudesta, jota käyttää ja laskutus on saumattoman rehellistä. Asiakas ja palveluntarjoaja saavat palveluiden käytöstä tarvittaessa paljon yksityiskohtaista tietoa, joten asiakas voi huoletta luottaa laskutuksen oikeellisuuteen. (Salo 2010, 18.)

3.5 Pilvipalveluiden käyttöönotto

Toimialan luonne on yksi tekijä, joka asettaa omat rajoitteensa yrityksen siirtyessä pilvipalveluiden käyttäjäksi. Jos asiakkaat yrityksen toimialalla asettavat suuren painoarvon luotettavuudelle, ei asiakastietojen säilyttäminen tai prosessointi pilvipalveluissa tule kuuloonkaan. Lisäksi jos yrityksen toiminnan kannalta on kriittistä 100 %:n toimintavarmuus, ei palvelutasosopimus ole 99,99 %:n toimintavarmuudella riittävä. (Salo 2010, 74.)

Pilvipalveluihin voidaan laittaa joko a) dataa tai b) sovelluksia, toimintoja ja prosesseja. Pilvipalveluvaihtoehtoa kannattaa harkita tarkkaan, mitä liiketoimintakriittisempi, arkaluonteisempi ja yrityksen toiminnan jatkuvuudelle tärkeämpi resurssi on kyseessä. Myös lainsäädäntö saattaa estää pilvipalveluihin siirtymisen esimerkiksi asiakastietojen kohdalla. Siirtymisessä yritys voi listata datan, sovellukset, toiminnot ja prosessit tärkeysjärjestykseen tärkeimmästä vähiten tärkeisiin. Listauksen jälkeen yritys voi katsoa, mitkä tiedot, sovellukset, toiminnot ja prosessit ovat mahdottomia tai liian riskialttiita siirrettäväksi pilvipalveluihin. Listauksen vähiten riskialttiita osa-alueita yritys voi harkita pilvipalveluihin siirrettäväksi. Lisäksi yrityksen on verrattava tiedossa olevia etuja havaittuihin riskeihin ja aiheutuviin kustannuksiin. (Salo 2010, 75.)

Ennen siirtoa olisi hyvä tehdä myös riippuvaisuuksia esittävä *dependency mapping* -kaavio, koska todennäköisesti sovellusta tai datamassaa ei voida siirtää pilveen ilman muita toimenpiteitä. Sovellukselle on annettava

pilvessä käyttötarvetta vastaavat abstraktiot. Näitä ovat tietoliikenne, tallennus, tietokanta ja varmistaminen. (Heino 2010, 229.)

Yrityksen on hyvä tutkia markkinoita ja selvittää olemassa olevia pilvipalveluntarjoajia ja samalla pohtia, mihin pilvipalvelumalli yrityksen tapauksessa sopii ja mihin ei. Vaihtoehtoja on paljon ja niitä on vielä lisää tulossa. Salon (2010) mukaan palveluntarjoajaa valittaessa on hyvä pohtia mm;

- Mitä palveluita palveluntarjoajalla on saatavilla?
- Onko palveluntarjoajalla tarjota palvelutasopimusta? Sen mahdollinen sisältö?
- Minkälainen maine on palveluntarjoajalla?
- Miten suuri toimija palveluntarjoaja on markkinoilla liikevaihdollisesti ja asiakasmäärällisesti mitattuna?
- Uskottava toimintamalli palvelukatkos tilanteisiin?
- Kuinka kattavaa informaatiota palveluntarjoaja lupaa asiakkailleen toimintansa laadusta, suorituskyvystä ja häiriöistä tai katkoksista?

Palveluntarjoajaa valittaessa on hyvä huomioida, että isojen yritysten palvelut ovat todennäköisesti vakaalla pohjalla, eivätkä ne kaadu niin helposti kuin vasta toimintansa aloitteet yritykset (Salo 2010, 76). Suuret yritykset panostavat toimintaan todella tehokkaasti, koska yrityksen maine on epäonnistuessaan vaakalaudalla. Iso yritys pystyy myös tarjoamaan hyvää palvelua kilpailukykyiseen hintaan, koska sillä on potentiaalia rakentaa iso ja tehokas infrastruktuuri. Isoissa palveluympäristössä on kuitenkin riski, että yksittäisen asiakkaan tarpeet saattavat helposti hautautua massan alle. Suuressa ympäristössä on myös paljon eri tahoja tuottamassa ja käyttämässä palvelua, jonka vuoksi väärinkäytön tai tahattoman haitan aiheuttamisen riski kasvaa. Lisäksi suuri toimintaympäristö saattaa houkutella haitantekijöitä. (Viestintävirasto 2014, 15-16.)

Pienten palveluntarjoajien etuna on, että niiden kanssa voi usein neuvotella palveluun liittyvistä seikoista sekä räätälöidä itselle

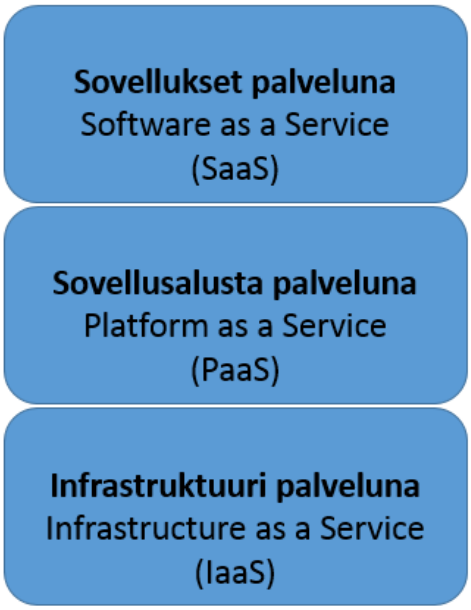
sopivamman palvelupaketin. Pienempi palveluntarjoaja saattaa olla myös valmis muokkaamaan halutunlaisen rajapinnan asiakkaan tietojärjestelmää varten. Jos kyseessä on paikallinen toimija, voi asiakas käydä mahdollisesti tarkistamassa palvelun fyysisen ympäristön. (Viestintävirasto 2014, 16.)

Palveluiden ja niissä olevan tiedon siirto ulkopuolisille tahoille aiheuttaa tietohallinto- ja tietoturva-asiantuntijoissa huolta niiden tietoturvallisuudesta. Andreassonin ym. (2013, 33) mukaan huoli on aiheellinen ja pakottaa organisaation tarkistamaan tietoturvakäytäntöjään sekä sopimuksien sisältöä. Tietoturvan ja tietosuojan toteuttamisessa on tarvittaessa käytettävä ulkopuolisten asiantuntijoiden apua.

Tietojärjestelmissä ja projekteissa tietoturvan ja tietosuojan vaatimusten toteuttaminen on hyvä tarkastaa eli auditoida ulkopuolisella asiantuntijataholla tai sisäisesti. Monesti palveluntarjoajien tietoturvatasoa on kuitenkin hyvin vaikea auditoida tai muuttaa. Yleensä, mikäli palvelua halutaan käyttää, on pakko hyväksyä toimittajan ratkaisu sellaisenaan. (Andreasson ym. 2013, 94.)

3.6 Pilvipalveluiden luokittelu

Pilvipalvelut on luokiteltu muutamaan päätyyppiin niiden teknisen toteutustavan perusteella. Toteutustavasta voidaan päätellä, minkälaisia tietojenkäsittelytehtäviä pilvipalvelusta saadaan ja kuinka niihin liitytään. (Heino 2010, 50.) Palveluarkkitehtuuri jaetaan kolmeen kerrokseen (KUVIO 3).



KUVIO 3. Pilvipalveluarkkitehtuurin kolme kerrosta (Salo 2010, 22).

Vuonna 2010 pilvipalvelumarkkinoiden suurin osa oli SaaS-palveluita 49 % osuudella. Toiseksi suurin osuus oli IaaS-palveluilla 38 % osuudella ja viimeisenä PaaS 13 % osuudella. Palvelualusta (PaaS) rakennetaan Infrastruktuurin (IaaS) päälle ja se luo taas pohjan sovelluksien rakentamiselle (SaaS). (Salo 2010, 22.)

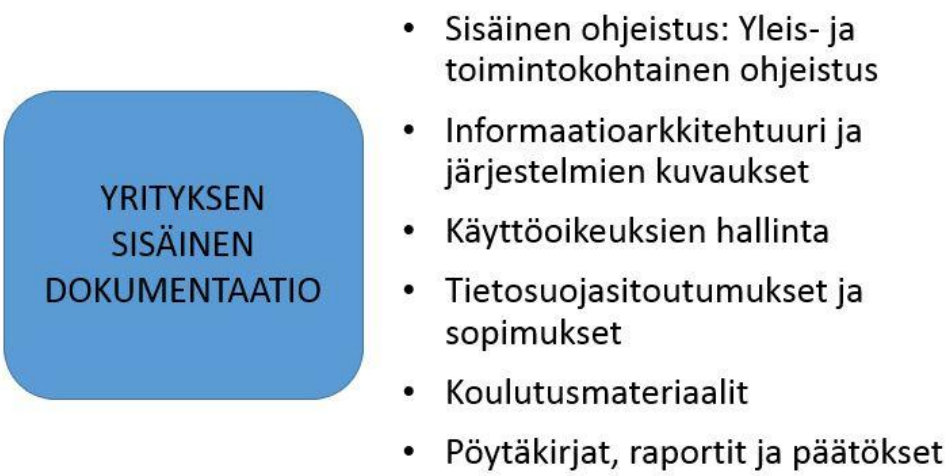
Palveluita käyttävän yrityksen kannalta katsottuna tärkeimpiä seikkoja ovat liiketoimintaprosessit, eivätkä ne mahdollistavat tekniikat. Pilvipalveluiden ja teknisten ratkaisujen arvo muodostuu niiden kyvystä mahdollistaa liiketoimintaprosessit ja tukea organisaation liiketoimintaa. PaaS- ja IaaS-ratkaisut sekä niiden päällä toimivat sovellukset eivät ole yrityksen kannalta kiinnostavia muutoin kuin liiketoiminnan mahdollistavina, sitä kannattavina ja kehittävinä toimintoina. Yritys on itse vastuussa liiketoimintaprosesseistaan tai vaihtoehtoisesti se voi ulkoistaa osan niistä yhteistyökumppaneilleen. Yrityksen ulkoistaessaan toimintojaan, löytää se pilvipalvelumarkkinoilta vaihtoehtoja sovelluksista sovellusalustoihin ja infrastruktuuriin. Yritys voi itse päättää, mistä tasosta se haluaa vastata itse ja minkä ulkoistaa. Tarvittaessa se voi ulkoistaa vaikka kokonaisen liiketoimintaprosessin, esimerkiksi maksuliikenteen. (Salo 2010, 24.)

Suurimmalla osalla yrityksistä tulee olemaan erilaisia järjestelmiä omassa omistuksessaan ja hallinnassaan ja näihin järjestelmiin pilvipalveluiden on kyettävä integroitumaan saumattomasti. Yrityksen on mitattava hankittujen palveluiden suorituskykyä ja luotettavuutta, koska se on sisäisen sekä ulkoisen laadunvarmistuksen ja palvelutason säilyttämisen kannalta tärkeää. Kokonaisuutta täytyy pystyä hallinnoimaan ja hankitut palvelut liittämään saumattomasti osaksi kokonaisuutta. Yritys vastaa itse omista liiketoimintaprosesseistaan ja niiden lopputuloksista omille asiakkailleen ja muille sidosryhmille, joten pilvipalvelumalleissa yrityksen on seurattava palveluntarjoajan palvelutasoa ja hinnoittelumenetelmiä. (Salo 2010, 24.)

3.7 Tietojen suojaamisen periaatteet yrityksessä

3.7.1 Tietosuojadokumentaatio

Tietosuoja-asioiden huomioiminen käytännön työssä onnistuu parhaiten, kun tietosuojadokumentaatio on kattava ja ohjeistus on selkeä. Jokainen joka käsittelee työssään henkilötietoja, tulee tuntea omiin tehtäviinsä liittyvät ohjeistukset ja yksityisyyden suojaamiseen liittyvät periaatteet. Salminen (2009, 129) lisäksi esittää, että tietosuoja-asioiden ja –ohjeistusten tuntemusta voidaan parantaa kouluttamalla henkilökuntaa. Hyvin laadittu tietosuojadokumentaatio on johdonmukainen kokonaisuus, joka kattaa koko organisaation henkilöstötietojen käsittelyn. Dokumentaatio voi sisältää esimerkiksi seuraavanlaisia yrityksen sisäisiä dokumentaatioita (KUVIO 4).



KUVIO 4. Tietosuojadokumentaatio ja ohjeistus – Yrityksen sisäinen dokumentaatio (Salminen 2009, 129).

Organisaation sisäisen dokumentaation ja ohjeistuksen tulee kattaa kaikki organisaatiossa tapahtuva henkilötietojen käsittely. Yleisohjeistukset ovat koko henkilötietojen käsittelyä koskevia yleisiä sääntöjä, jotka koskevat koko yrityksen henkilökuntaa. Toimintokohtaisten kuvausten ja ohjeistusten olisi hyvä olla käytännönläheisiä ja tarkkoja, jotta henkilötietojen käsittelijät suoriutuvat niitä avuksi käyttäen henkilötietojen käsittelytehtävistään. (Salminen 2009, 129–130.)

Henkilötietojen käsittelyn looginen informaatioarkkitehtuuri ja tietojärjestelmien kokonaisuudet olisi kuvattava siten, että liiketoiminnan prosessit ja tietojärjestelmät sisältävät henkilötietojen käsittelyn. Tämä mahdollistaa henkilötietojen käsittelyn kehittämisen ja hyvän kommunikoinnin, lisäksi se mahdollistaa toiminnan yksiselitteisen ohjeistamisen sekä tehtävien ja vastuiden jakamisen. (Salminen 2009, 130.)

Tietojärjestelmiä on mahdollista hallita käyttöoikeuksilla. Ne ovat tarpeen etenkin silloin, kun halutaan varmistaa, että henkilötietoihin pääsevät käsiksi vain niiden käsittelyyn oikeutetut henkilöt. Tämän lisäksi henkilötietojen valvontaa voidaan tehostaa käsittelijöiden tietosuoja- ja vaitiolositoumuksilla. (Salminen 2009, 130.)

Jos yrityksellä on henkilötietoihin liittyviä työtehtäviä, on yrityksen hyvä pitää huoli henkilökunnan riittävästä koulutuksesta. Koulutusmateriaalia laatiessa tulee ottaa huomioon, että tiedot ovat riittäviä tietosuojalainsäädännöstä ja henkilötietojen käsittelyn menettelystä yrityksessä. Tietosuojakoulutusta ja koulutusmateriaalia suunniteltaessa on hyvä ottaa huomioon myös uusien työntekijöiden perehdyttäminen. (Salminen 2009, 130.)

Yrityksen tietosuojatoiminnassa käsitellyt asiat ja tehdyt päätökset on syytä dokumentoida pöytäkirjoihin sekä raportoida niistä tietoa tarvitseville. Dokumentointi mahdollistaa päätösten tarkistamisen toiminnan kehittyessä. Tietosuoja-asiat kannattaa ottaa osaksi yrityksissä tapahtuvaa liiketoiminnan ja tietojärjestelmien kehittämisprojekteita. Näin toimien, tietosuojan vaatimukset dokumentoidaan jo liiketoiminnan ja tietojärjestelmien suunnitteluvaiheessa. Lisäksi tämä helpottaa projektin vaikutusten ennakoitavuutta yrityksen henkilötietojen käsittelyssä. (Salminen 2009, 130–131.)

Tietosuojatoimintaa ja -dokumentaatiota on hyvä tarkastella sopivin väliajoin. Tarkastuksissa on mahdollista tunnistaa ja priorisoida tietosuojatoiminnan kehittämisen tarpeita ja samalla voidaan päättää toimenpiteistä, kuinka tietosuojaa kehitetään. Lisäksi voidaan verrata, kuinka henkilötietoja käytännössä käsitellään verrattuna ohjeistuksiin. Toiminnan kehittyessä on hyvä tarkastaa, että suojadokumentaatio ja -ohjeistukset ovat pysyneet ajan tasalla. (Salminen 2009, 131.)

3.7.2 Identiteettien ja käyttövaltuuksien hallinta

Andreasson ym. (2013, 46) esittävät, että identiteettien ja käyttövaltuuksien hallinta käsittää toimintaprosessit, säännöt, organisaation ja välineet, joiden avulla kontrolloidaan tietojärjestelmien asianmukaista käyttöä. Yrityksen suunniteltaessa käyttövaltuuksien hallinnan periaatteita ja lähtökohtia, täytyy lähtökohtana olla asiaa koskeva lainsäädäntö sekä organisaation ohjeet ja määräykset. Käyttäjien

oikeuksia ja hallintaa määriteltäessä, on roolipohjaisuus yleensä hyvä ratkaisu. Ensin määritellään käyttäjäroolit ja sen jälkeen se, mihin toimintoihin näiden roolien haltijoilla on oikeudet. Jokaisella työntekijällä saa olla käyttöoikeudet vain sellaisiin tietoihin, jotka ovat todella tarpeen hänen työtehtävistään.

Joissakin organisaatioissa on riskinä, että käyttöoikeuksien hallinnan puutteellisuudesta johtuen kenelläkään ei ole välttämättä täydellistä kuvaa siitä, kuka pääsee järjestelmiin ja millä oikeuksilla. Tilanteessa on vaarana, että tilapäisetkin käyttäjät saavat pysyviä käyttöoikeuksia tai käyttäjille annetaan varmuuden vuoksi laajempia oikeuksia kuin heille edes kuuluu. (Andreasson ym. 2013, 46.)

3.8 Tietosuoja pilvipalveluissa

3.8.1 Internet ja sähköposti

Internet ja sähköposti ovat käteviä työkaluja sekä tiedon hakuun, että yhteydenpitoon. Sähköpostin ja internetin käyttö vaatii kuitenkin käyttäjältä huolellisuutta, sillä niissä ei itsessään ole oletuksena minkäänlaista suojausta, vaan tiedot liikkuvat salaamattomina julkisessa verkossa. Työpaikalla sähköposti ja internet on tarkoitettu pääsääntöisesti työkäyttöön. Työnantajan velvollisuus on pitää huoli, että työntekijöillä on tarvittaessa käytössään asianmukaiset työvälineet, kuten sähköpostin salaustuotteet. (Andreasson ym. 2013, 55.)

Asiakkaita koskeva tieto on aina luottamuksellista. Verkossa kuten esimerkiksi Facebookissa kirjoitettu voi päätyä julkiseksi, eikä sanojaan saa takaisin. On myös otettava huomioon, että vaikka kirjoittaisi kotikoneelta yksityishenkilönä, voidaan nimen perusteella helposti yhdistää työnantajaan. Lisäksi verkossa on paljon tahoja, jotka yrittävät kalastella organisaatioiden salaisuuksia, joten epävarmoissa tapauksissa kannattaa neuvoa kysyä esimieheltä. (Andreasson ym. 2013, 55.)

3.8.2 Mobiililaitteet

Älypuhelimet ja muut mukana kulkevat tietotekniset laitteet ovat entisestään yleistyneet kovaa vauhtia. Lisäksi erilaisten ajasta ja paikasta riippumattomien sovellusten ja palveluiden käyttö ovat huomattavasti yleistyneet. Nykyteknologia tarjoaa paljon uusia mahdollisuuksia, mutta sen varjopuolena on, että ne aiheuttavat riskejä ja muutostarpeita vanhentuneisiin järjestelmiin ja toimintatapoihin.

Mobiililaitteiden käyttöön ja niiden tietoturvariskien hallintaan vaikuttavat monet asiat. Sähköisten palveluiden laajentuminen, tietojärjestelmien etä- ja mobiilikäytön lisääntyminen sekä palvelutuotannon uudet menetelmät ovat muun muassa tällaisia tekijöitä. (Andreasson, Koivisto & Ylipartanen 2014, 91.) Etenkin älypuhelimet mahdollistavat arkipäiväisen urkinnan, sillä ne kulkevat aina mukana ja tallentavat nettiin jonkin vieraan maan palvelimelle sähköpostit, liitetiedostot ja wlan-verkkojen sekä nettipalveluiden salasanat (Järvinen, 2014, 292).

Sosiaalinen media ja muiden sovellusten käyttö tuo erityisiä haasteita, sillä niissä työ- ja siviilirooli ovat lähellä toisiaan. Kun käytössä on työnantajan tarjoama laite, tulee helposti houkutus tehdä laitteella työhön kuulumattomia asioita. Uudet pilvipalvelut mahdollistavat erilaisia tapoja hoitaa tiedonvälitystä ja sovellusten hajauttamista, mutta samanaikaisesti tietojen sijainti ja rajat maiden välillä hämärtyvät. Tämä aiheuttaa kysymyksen siitä, mitä tietoja palveluissa kannattaa käsitellä. (Andreasson ym. 2014, 91.)

Järvisen (2014, 294) mukaan älypuhelimien mukana tulevat pilvipalvelut ovat kaiken urkinnan perusta, mutta silti niitä on mahdotonta välttää. Jopa älypuhelimien perustoiminnot ovat kytketty palveluihin, jotka keräävät tietoa. Palveluihin liittyminen on vapaaehtoista, mutta käytännössä lupa on pakko antaa, jos puhelimella on tarkoitus jotakin tehdä. iOs-, Android- ja Windows -puhelimien käyttäjien sähköposti, työtiedostot, kalenterit, osoitekirjat, salasanat ja muut henkilökohtaiset tiedot tallentuvat pilveen automaattisesti.

Organisaatiot voivat halutessaan laatia ja toteuttaa ns. mobiilipolitiikan, joka luokitellaan yhdeksi riskienhallinnan osaksi. Sen tarkoituksena on määritellä ja ohjeistaa mobiililaitteiden käyttöä ja hallintaa. Lisäksi sillä pyritään selkiyttämään, yhtenäistämään, määrittelemään ja ohjeistamaan mobiililaitteiden turvalliseen käyttöön ja hallintaan liittyviä seikkoja ja toimintatapoja. Edellä mainitut asiat pyrkivät siten torjumaan tietoturvan ja tietosuojan ongelmia sekä pienentämään erilaisia uhkia. (Andreasson ym. 2014, 91–92.)

3.8.3 Tietoturva pilvipalveluissa

Järvinen (2014, 283-284) tähdentää, että vaikka monet pilvipalvelut mainostavat tietojen olevan turvassa niiden salauksen vuoksi, pystyy palveluntarjoajan henkilökunta lukemaan tiedot kuin salausta ei olisikaan. Lisäksi tiedot voidaan luovuttaa viranomaisille, mainostajille tai muulle ulkopuoliselle taholle. Salattuina tiedot ovat turvassa lähinnä vain ulkopuolista hakkeria vastaan. Jos ulkopuolinen hakkeri onnistuu murtautumaan pilven levyjärjestelmään, estää salaus tietojen luvattoman haltuunoton. Todennäköisempää on, että mahdollinen tietomurto tapahtuu palveluntarjoajan henkilökunnan avustuksella.

Pilvipalveluiden käyttäjän tulisi varmistaa, missä hänen tallentamansa tieto sijaitsee sen elinkaaren aikana. Tieto liikkuu tallennuspaikkojen välillä varmuuskopioinnin, palveluun liittyvän hallinnollisen toiminnan yhteydessä tai kun käyttäjä käsittelee sitä. Tiedon sijainti voi muuttua eri mantereiden välillä valon nopeudella ja se voi käydä matkansa varrella olevien tietoliikennelaitteiden välimuistissa.

Julkisuuteen tulleiden uutisointien mukaan eri maiden tiedustelupalvelut ovat kuunnelleet sekä mantereiden välistä tietoliikennettä että isoimpien palveluntarjoajien palvelinkeskusten välistä liikennöintiä. Jos tieto tai tietoliikenne ei ole salattu, se on helposti luettavissa kolmansien osapuolten toimesta. (Viestintävirasto 2014, 8.) Jotta tietojen tallentaminen pilveen olisi luotettavan turvallista, tulisi tietojen olla salattua ennen kuin se

siirretään pilvipalveluun. Salauksen avaimen pitäisi olla vain käyttäjän itsensä tiedossa. (Järvinen 2014, 284.)

Kun tietoa poistetaan tietojärjestelmistä perinteisin menetelmin, jää tieto yleensä kuitenkin talteen. Yleinen toimintamalli käyttöjärjestelmissä on, että kun tiedosto tai hakemisto poistetaan kiintolevyltä, itse tietoa ei poisteta, vaan ainoastaan tieto siitä pyyhitään pois järjestelmän kirjanpidosta. Tiedoston tai hakemiston varaama tila tallennusjärjestelmässä merkitään siis vapaaksi, jolloin järjestelmä voi käyttää tilaa muiden tietojen tallentamiseen. Poistettu tieto on kuitenkin luettavissa levyltä niin kauan, kunnes sen kohdalle levypinnalle kirjoitetaan muuta tietoa. Tiedon tuhoamisen voi varmistaa esimerkiksi erillisellä ohjelmistolla, joka ylikirjoittaa poistettavan tiedoston kohdan levypinnasta satunnaisilla merkeillä. (Viestintävirasto 2014, 8.)

Palveluiden käyttäjien on hyvä ottaa selville, kuinka asiakkaan tietoja sisältävä vanhentunut fyysinen laitteisto poistetaan käytöstä. Palveluntarjoajan vaihtoehdot ovat: laitteiston tietosisällön ylikirjoitus, mekaaninen tuhoaminen tai huonoin vaihtoehto, laite laitetaan suoraan kiertoon. (Viestintävirasto 2014, 8-9.) Pilvipalvelut ovat nyt ja tulevat jatkossa olemaan kompromissi mukavuuden ja turvallisuuden välillä, mutta suurimmaksi osaksi asiakkaat valitsevat lopulta mukavuuden. (Järvinen 2014, 284.)

3.8.4 Pilvipalvelujen riskit ja kustannukset

Pilvipalvelumalliin siirtymiseen on useita esteitä. Toimintamallin uutuuden vuoksi se aiheuttaa epävarmuutta potentiaaleissa asiakkaissa. Asiakkaan huoli turvallisuudesta, tehtyjen investointien loppuun hyödyntäminen ja yrityksen henkilökunnan osaaminen ovat epävarmuustekijöitä yrityksen näkökannalta. Pilvipalveluihin siirryttäessä on hyvä kartoittaa riskit, arvioida niiden toteutumisen todennäköisyys ja vahinkojen suuruus.

Kun riskit on listattu, on mietittävä kuinka riskien toteutumisen todennäköisyyttä voitaisiin minimoida ja kuinka niiden toteutumisesta

aiheutuneita vahinkoja voitaisiin pienentää. Vahinkoja voidaan pienentää perinteisellä vakuuttautumisella, mutta pilvipalveluiden kohdalla se on lähes mahdotonta. Vahingon sattuessa pitäisi osoittaa, että tietovuoto on todella tapahtunut, vaikka data sijaitsisi ympäri maailmaa olevissa palvelinkeskuksissa.

Lisäksi ongelmaksi muodostuu, kuinka osoittaa esimerkiksi liiketoimintaprosessin toimimattomuuden syy, kun ongelma voi olla pilvipalveluntarjoajassa, verkkoyhteyksiä tarjoavassa yrityksessä tai palveluita hyödyntävän yrityksen omassa päässä. Liiketoiminnassa kaikkia riskejä ei voida poistaa eli niiden toteutumisen todennäköisyyttä ja aiheutuneita vahinkoja ei saada nollatasolle. Kartoitus auttaa kuitenkin yritystä hahmottamaan riskit, arvioimaan niiden vaikutusta, varautumaan niihin ja ennaltaehkäisemään niitä. (Salo 2010, 72-73.)

3.8.5 Palvelutasosopimus (SLA – Service Level Agreement)

Palvelutasosopimuksella asiakas ja palveluntarjoaja sopivat palvelulle tietyn tason (Andreasson ym. 2014, 94). Sopimuksessa voidaan määritellä tarkemmin palveluihin liittyvät palvelutasotavoitteet ja yksilöidä palveluntarjoajan ja asiakkaan vastuut (Viestintävirasto 2014, 15). Tason toteuttamista voidaan valvoa erilaisilla mittareilla ja seurantapalavereilla. Palvelutasosopimuksissa voidaan määritellä sanktioita palveluntarjoajalle, jos tietty palvelutaso alittuu. Sanktiot ovat yleensä sidottu palvelusta maksettavaan korvaukseen, eikä haittaan, jota puutteellinen palvelu aiheuttaa yritykselle. (Andreasson ym. 2014, 94.) Viestintäviraston (2014, 15) mukaan palvelutasosopimuksen avulla määritettäviä tavoitteita voivat olla esimerkiksi:

- Kuinka suuren osan ajasta palvelun luvataan toimivan ja minkälaiset ovat vasteajat?
- Minkälaista käyttäjätukea on saatavilla ja millaiset vasteajat ovat arkisin, viikonloppuisin, päivällä, illalla ja yöllä?
- Missä yrityksen tietoa säilytetään ja mistä sitä ylläpidetään?

Erityisen tärkeä seikka sopimuksia tehdessä on huomioida tiedon hallintaan ja käsittelyoikeuteen liittyviä asioita. Jos yritys päättää säilyttää pilvessä muun tiedon lisäksi myös liikesalaisuuksia, on tärkeää varmistaa, että tietoihin pääsee vain ne henkilöt, joilla on oikeus niitä käsitellä. Käsittelyoikeuksien säilyminen organisaatiolla voidaan varmistaa sopimuksin. Tarvittaessa arkaluonteisen tai salassa pidettävän tiedon käsittelystä voidaan yrityksen ja palveluntarjoajan välille tehdä salassapitosopimus. (Viestintävirasto 2014, 7.)

Salminen (2009, 108-109) esittää, että toimeksiantajan tulee esimerkiksi vastata toimeksisaajan henkilötietojen käsittelystä kuten omasta toiminnastaan. On tärkeää varmistaa, että myös toimeksisaaja käsittelee henkilötietoja vastuullisesti. Henkilötietojen käsittelystä ei tarvitse välttämättä laatia erillistä sopimusta, mutta on huolehdittava, että tietosuoja-asiat on riittävästi huomioitu sopimuskokonaisuudessa, jolta palvelu tilataan.

Kun käyttäjät ymmärtävät tietosuojan pääperiaatteet, erityisesti määrittelyiden tarkoituksen, käyttörajoituksen ja turvallisuustakeen, on ryhdyttävä tekemään riskiarviointia kaikista sopivista pilvipalveluntarjoajista. Tällä tavalla tunnistetaan mahdolliset aukot tarjoajien ja omien vaatimusten välillä. Jokaiseen löydettyyn aukkoon tulisi sitten toteuttaa jokin sopiva hallintamenetelmä, jotta riskit vältettäisiin tai edes vähenisi. (Chang 2014.)

Sopimuksia tehtäessä on tärkeää dokumentoida huolellisesti ulkoistusprosessi, ostettavan palvelun sisältö ja palvelutaso. Kun sopimuskausi lähestyy loppuaan, voidaan dokumentoinnin avulla huomioida tarpeelliset asiat ennen uutta kilpailutusta tai mahdollista sopimuksen jatkamista. Sopimuksia tehtäessä on järkevää laatia sopimuspohjat yhteistyössä sopimusjuridiikkaan paneutuneen lakimiehen kanssa. Tämän lisäksi on suositeltavaa, että mukana on ostettavien palveluiden alan asiantuntijoita sekä rekisterinpitoon että tietoturvaan liittyvää ammattitaitoa. (Andreasson ym. 2014, 99.)

3.9 Aiemmat tutkimukset

Aleemin ja Sprottin (2013) mukaan suurimpia huolenaiheita organisaatioiden siirtyessä pilvipalveluihin ovat mm. turvallisuustekijät ja kyvyttömyys hallita palvelun saatavuutta. Velumadhava Rao & Selvamani (2015) olivat myös samaa mieltä siitä, että pilvipalveluissa on paljon turvallisuuteen liittyviä haasteita. Useimpien tutkimuksen mukaan tietojen salaaminen ennen pilvipalveluihin siirtymistä on tehokas keino estää tietovuotoa (Velumadhava Rao ym. 2015; Chang 2014).

Aleemin ym. (2013) tutkimuksessa kävi kuitenkin ilmi, että suurin osa IT-ammattilaisista eivät ole olleet tietoisia siitä, että jotkut palveluntarjoajat hallitsevat salausavaimia, joilla he pääsevät käsiksi asiakkaidensa tietoihin. Tämä on merkittävä turvallisuushuoli, ja tämä seikka on hyvä huomioida palvelutasosopimusta (SLA) laatiessa.

Changin (2014) mukaan on kuitenkin olemassa keinot, joilla voidaan ehkäistä salausavainten joutumista vääriin käsiin. Asiakkaiden käyttäessään vahvoja toimenpiteitä salatakseen henkilökohtaisia tietoja pilvipalveluissa, kuten salausalgoritmeja, vahvoja salasanoja ja kunnollista avainhallintaa, ovat he näillä toimenpiteillä kykeneviä säilyttämään korkean tietojen luottamuksellisuuden, sillä he ovat ainoa osapuoli, joka pystyy purkamaan tiedon salauksen.

Syrjälän (2015) mukaan pilvipalvelun tuottajan vastuulla on tarjota asiakkaalle sellainen mekanismi, jolla se voi vakuuttaa, että aineisto on tallennettu pilveen turvallisesti. Chang (2014) puolestaan toteaa, että käyttäjät ovat viime kädessä itse vastuussa henkilökohtaisten tietojen asianmukaisesta käsittelystä. Pilvipalveluiden hyödyntämisen päähaaste on siten etsiä keinot, kuinka huolehditaan ohjauksesta ja valvonnasta niin, että henkilökohtaisten tietojen hallinta säilyy käyttäjillä itsellään.

4 TUTKIMUSPROSESSI

4.1 Aineiston keruusuunnitelma

Aineistoa tähän tutkimukseen kerättiin niiden henkilöiden haastatteluilla, jotka ovat keskeisessä asemassa päättämässä LAMKin toimintaperiaatteista tietosuojaan ja pilvipalveluihin liittyvissä asioissa. Haastateltavia henkilöitä oli tarkoitus saada äskettäin perustetusta LAMKin omasta tietohallinnosta sekä Salpauksen tietohallinnosta, josta LAMK kirjoittamishetkellä ostaa tietohallinto ja IT-palveluita. Tavoitteena oli haastatella kahta tai kolmea henkilöä.

Alkuperäisen tutkimussuunnitelman mukaan haastatteluaineisto kerättäisiin teemahaastattelun avulla. Tämän tyyppinen haastattelu ei etene tarkkojen, yksityiskohtaisten kysymysten kautta, vaan väljemmin kohdentuen tiettyihin ennalta suunniteltuihin teemoihin. Teemahaastattelu on strukturoidumpi kuin avoin haastattelu, koska aihepiirin tutustumisen pohjalta valmistellut teemat ovat kaikille haastateltaville samoja. (Saaranen-Kauppinen & Puusniekka 2006c.)

Teoriaan tutustumisen aikana käsitys tietosuojan varmistamisesta pilvipalveluissa kasvoi, jonka vuoksi teemahaastattelusta luovuttiin ja se vaihdettiin puolistrukturoituun haastatteluun. Tällä haastattelutyypillä saadaan suoraviivaisemmat vastaukset esitettyihin kysymyksiin. Saaranen-Kauppisen & Puusniekan (2006c) mukaan puolistrukturoidusta haastattelusta ei ole olemassa täysin yhtenäistä määritystä. Puolistrukturoitu ja osittain avoin haastattelu sijoittuu täysin strukturoidun lomakehaastattelun ja teemahaastattelun väliin. Puolistrukturoidussa haastattelussa on tavanomaisesti mietitty teemat, mutta niiden lisäksi esitetään tarkkoja kysymyksiä, joista kaikki kysytään haastateltavilta. Osittain järjestetty haastattelu soveltuu parhaiten tilanteisiin, joissa halutaan tietoa juuri tietyistä asioista, eikä haastateltavalle jää kovin paljon vapauksia haastattelussa. Haastattelut tallennetaan puhelimen sanelin-ohjelmalla, jotta ne voidaan myöhemmin kuunnella ja analysoida.

4.2 Haastattelukysymykset

Haastattelun kysymykset (LIITE 1) on muodostettu aiheeseen liittyvän kirjallisuuden sekä aikaisempien tutkimusten pohjalta. Aiheeseen huolella tutustumisen jälkeen on helpompi määritellä sellaiset kysymykset, joilla saadaan parhaiten vastaus tutkimusongelmaan.

Ensimmäiseksi haastateltavilta kysytään taustatiedot, kuten koulutus ja työtehtävät. Tämän jälkeen haastateltavat kertovat oman käsityksen keskeisistä aiheeseen liittyvistä termeistä; tietosuoja ja tietoturva. Organisaation tietosuojakäytäntöön perehdytään seuraavilla kysymyksillä. Kysymyksissä pyritään saamaan selville LAMKin toimintaperiaatteet sekä haastateltavan oma mielipide samaan aiheeseen. Haastattelussa käydään lisäksi läpi mobiililaitteiden käyttöön liittyviä kysymyksiä, koska pilvipalvelut ovat käytettävissä myös mobiililaitteilla. Pilvipalveluihin liittyvissä kysymyksissä käydään läpi pilvipalveluihin siirtymisen taustoja. Kysymysten tarkoituksena on saada selville haastateltavien omat mielipiteet mm. pilvipalveluiden haasteista, riskeistä, sopimuksista ja lainsäädännöstä. Lisäksi kysymyksillä selvitetään, kuinka LAMKissa toimittiin aiemmin pilvipalveluihin siirtyessä.

4.3 Aineiston analyysi

Kvalitatiivisessa tutkimuksessa aineiston analyysi etenee seuraavien askeleiden mukaan: tunnista analyysin kohteet, kerää tutkimusaineisto, valmista aineisto analyysiin varten, kuvaile kohteet, kuvaile kohteet kokonaisuudessaan ja selitä kokonaisuus. Ensisijaisesti kerättyyn aineistoon tutustutaan huolella. Analyysin alkuvaiheessa pyritään havainnoimaan aineistosta tarpeelliset kohdat. Kerätyn aineiston analyysiprosessissa (KUVIO 6) nauhoitettu haastattelu on ensimmäiseksi litteroitava tekstiksi, joka tarkoittaa äänitallenteen kirjoittamista tekstimuotoon. Litteroitavasta tekstistä merkataan tärkeimmät havainnot ylös, jotta kysymyksiin saadaan tarkka vastaus. Tekstiä korostetaan fontin

väriä muuttamalla, jolloin kokonaistekstistä saadaan helposti poimittua hyödyllisimmät kohdat näkyville.

KUVIO 6. Kerätyn aineiston analyysiprosessi

Tutkimukseen liittyvät tiedostot järjestellään ja luokitellaan. Ne voidaan esimerkiksi luokitella päivämäärän mukaan, tiedostojen nimen tai id-numeron mukaan tai dokumentin tyypin mukaan.

5 TUTKIMUSAINEISTO

Tutkimusaineisto koostuu kolmen eri henkilön haastatteluista. Haastateltavat hankittiin tiedustelemalla sopivia ehdokkaita LAMKin tietohallintopäälliköltä. Haastatteluajat ja paikka sovittiin tietohallintopäällikön välityksellä. Yksi haastateltavista työskentelee LAMKin tietohallinnossa ja kaksi muuta Salpauksen tietohallinnossa, josta LAMK tällä hetkellä hankkii ison osan IT-palveluista. Salpauksen haastateltavat ovat olleet merkittävässä roolissa, kun LAMK on siirtynyt käyttämään pilvipalveluita.

Kaikkien kolmen henkilön vastaukset edustavat LAMKin kantaa ja suhtautumista haastatteluissa esitettyihin kysymyksiin. Haastattelut suoritettiin helmikuussa 2016 FellmanniCampuksen pienryhmätiloissa. Puolistrukturoitu haastattelu suoritettiin yksilöhaastatteluina ja kaikki haastattelut tallennettiin. Haastattelut kestivät kahdestakymmenestä minuutista neljäänkymmeneen minuuttiin.

5.1 Käsitteet ”tietoturva” ja ”tietosuoja”

Tietosuojaan liittyy lainsäädäntö, sovitut käytännöt kuinka tietoa suojataan, säännöt, kenelle tietoja luovutetaan, kuka saa katsella niitä ja sen elinkaaren hallinta. Tietoturvaan liittyy käytettävyys ja jatkuvuus. Tietoturvan tavoitteita on erityisesti luottamuksellisuus, eheys ja saatavuus. Tietoturva on organisaation tapa toimia, eli tietoturvan teknisillä ratkaisuilla hoidetaan tietosuojan luomat säännöt.

> *”Tietoturva, siinä on nämä perus kolme aspektia: käytettävyys, saatavuus ja jatkuvuus ja mitä näitä nyt tähän kuuluu. Tietosuoja menee enemmän ehkä tonne lakiosastolle enemmän, et sieltä enemmän Suomen laki ottaa ja EU-lait määrittää niitä asioita sinne puolelle. Sitten taas tietoturva organisaation oma tapa toimia näitten puitteessa, mutta ehkä tää tämmönen erovaisuus nään mikä niillä on.”* (H1)

> *”Tietoturva on sitten laaja käsite, tietoturvallisuus on oikeastaan sitä, että toimitaan niin, että tietojen luottamuksellisuus, eheys ja saatavuus toteutuu. Elikä se on niin sanotusti työtä ja sopimisia ja toimenpiteitä ja sen tavoitteena on tavallaan, että se tieto on eheää, että siinä tulee se CIA-kolmio. Tietoturva ei ole ne pelkästään, luottamuksellisuus, eheys ja saatavuus, vaan se tarkoittaa, että ne on sen tietoturvan tavoitteita. Elikä se on niin ku lopputulos.”* (H2)

> *”Mun mielestä erona voisi olla sellainen, että tietoturva on enemmänkin teknistä puolta, että siinä keskitytään suojaamaan asioita ja tietosuoja on taas enemmän sitten semmoinen hallinnollinen, jossa sovitaan käytäntöjä miten suojataan tiettyjä asioita. Mä oon ymmärtänyt vähän niin, että tietosuoja luo ne säännöt ja sitten tietotuvallisuuden teknisillä ratkaisuilla pyritään sitten hoitamaan ne asiat sillai fiksusti.”* (H3)

5.2 Yksityisyyden suojaaminen

Yksityisyyden suojaamisen periaatteet ja ohjeistukset hoidetaan esimerkiksi intranetin kautta, raportoimalla, puuttumalla väärinkäytöksiin ja antamalla tarvittaessa ohjeistusta. Henkilötietoja käsittelevillä henkilöillä on omat ohjeistukset. Tämän lisäksi opintohallinnossa on käytössä korkeakoulujen yhdessä muodostama tietosuojaohjeistus ja henkilöstöhallinnossa on tarkat säännökset henkilötietojen käsittelystä.

> *”Meillä on tota pyritty tiedottamaan näistä ja ohjeistamaan intranetin kautta ja sitten puuttumalla tällaiseen, jos havaitaan tietohallinnossa tai tuessa tai missä tahansa tämmöisiä väärinkäytöksiä ja semmosia asioita missä tietosuojaa joko tahallisesti tai tahattomasti poljetaan.”* (H1)

Virheiden välttämiseksi koulutusta olisi syytä lisätä jokaisen käyttäjän kohdalla. Julkisorganisaatiossa koulutukseen ei välttämättä panosteta niin paljon kun olisi tarvis. Tietoturva asioista vastuussa olevat käyvät riittävästi koulutuksessa. Sisäisellä perehdytyksellä kannattaisi kouluttaa peruskäyttäjiä.

> *”Mä väittäsin, että ei riittävästi ainakaan. Että kyllä toi on semmoinen tärkeä asia ja etenkin kun katotaan tulevaisuuteen. Mun mielestä toi henkilöstön kouluttaminen ja ihan joka ikisen kouluttaminen. Et ne kellä on sitten työtehtävis jotain henkilötietojen käsittelyä, ni niille vielä sitten vähän lisää, mutta toi on semmoinen toi koulutuspuoli. Että jos ajatellaan ihan tietoturvallisuutta, ni toi on se isoin riski minun mielestä, henkilöstö. Että siellä kun ei aina toimita hyvien tapojen mukaisesti ni sit sattuu ja tapahtuu.”* (H3)

Jokaisella henkilöllä on henkilökohtainen henkilötunnus ja sen salasana. Henkilökunnan tunnukset on sidottu tiettyihin lähdejärjestelmiin. Pääkäyttäjät varmistavat, kenelle antavat oikeuksia tiedostopalveluihin tai henkilöstöhallinnan järjestelmiin. Työsopimusta allekirjoittaessa sitoudutaan, että yrityksen asioita ei kerrota eteenpäin. Tehtävästä riippuen voidaan lisäksi kirjata erillinen vaitiolositoumus.

> *”Työsopimus on yksi asia missä määritellään asioita, ja sitten oikeastaan tehtävästä riippuen saatetaan kirjata enemmänkin ja tehdä vaikka erillinen vaitiolositoumus. Jokaisella henkilöllä on oma tiettyyn lähdejärjestelmään perustuva henkilökohtainen käyttäjätunnus ja siihen liittyvä salasana. Sen käyttäjätunnuksen olemassaolo on sidottu tavallaan niihin lähdejärjestelmiin. ”* (H2)

LAMKissa on käytössä Turvaposti niminen palvelu, jonka kautta on mahdollista lähettää turvallisesti arkaluontaisempaa sähköpostia. Vastaajien mukaan salausta pitäisi käyttää, jos materiaali ei ole julkista, tai sellaisessa tapauksessa, missä esimerkiksi kurssiarvosanoja tai Kela-

etuisuuksiin liittyvät päätökset voidaan yhdistää henkilökohtaisiin tietoihin. Perinteisessä sähköpostissa ei pitäisi lähettää mitään luottamuksellista tietoa.

> *”Sitä pitäisi käyttää kaikissa tapauksissa, jos organisaation tietosuojaperiaatteet niin vaatii. Periaatteessa niin, että kaikki materiaali mikä ei ole täysin julkista, pitäisi salata. Siellä tulee tietosuojalait vastaan, plus sitten organisaation omat tietoturvalinjaukset, että henkilötietoja koulutusorganisaatiossa kurssiarvosanoja yhdistettynä henkilön nimeen tai kotiosoitteita, puhelinnumeroita, tämän tyyppisiä mitkä voi yhdistää sitten luonnollisen henkilöön. Nämä kaikki on sellaista mitkä pitäisi salata.”* (H1)

Tietosuojaan liittyviä asioita voisi parantaa organisaatiossa esim. tiedottamisella ja varautumisella tulevaan EU:n tietosuoja-asetukseen.

> *”Sanotaan, että mun mielestä ne nyt hoidettu tavallaan organisaation nykyisen kyvykkyyden perusteella parhaalla mahdollisella tavalla. Aina on parannettavaa, ja sitä mukaan kun tavallaan tulee lisää tietoa ja tekniset edellytykset paranee, niin on paljon parannettavaa kyllä.”* (H2)

5.3 Mobiililaitteiden käyttö

LAMKissa ei ole määritelty varsinaista mobiilipolitiikkaa, mutta joitakin sääntöjä ja ohjeita löytyy. Mobiililaitteet ovat etähallittavia ja ne sisältävät tietyt tietoturva-asetukset.

> *”Kyllä mun mielestä jotakin asioita on yhteisesti sovittu ja kaiketi niin, että jos esimerkiksi henkilökunta haluaa sähköposteja lukee mobiililaitteella ni sinne tulee sitten tiettyjä asetuksia sähköpostipalvelimesta lukituskäytäntöjä sun muuta tämmöistä tulee, että vähän siihen suoja puoleen sitten ratkaisuja. Kyl mun mielest siitä on ihan hyvät ohjeistukset*

> *olemassa, että kuinka niitten laitteiden kanssa toimitaan ja montako laitetta per henkilö saa olla ja näin päin pois."* (H3)

5.4 Pilvipalvelut

Pilvipalveluissa on tulevaisuus ja niiden menestys kasvaa, ellei jotain todella massiivista katastrofia tapahdu. Ovat oikein hyviä hyvin toteutettuna ja ne tulevat yleistymään. Pilvipalveluissa on seikkoja joihin olisi syytä varautua, kuten ongelmallinen lainsäädäntö. Tietosuojan, tietoturvan ja ohjeistamisen lisääminen ja selkeiden pelisääntöjen tekemisellä varaudutaan yllätyksiin.

> *"Ihan takuuvarmasti yleistyy, siinä ei oo niin ku epäselvää. On se kuitenki varmaa aika monessa kohtaa niin paljon edullisempaa hankkia pilvestä tilaa kuin omaa konesaliin ostaa rautaa. Se on yksi asia ja totta kai sitten ne puolet että pääset siihen tietoon käsiksi ehkä helpommin ja näin. Mut kyl mä vähän sillain pelkään, että aika monessa paikassa voi levähtää käsille siinä vaiheessa kun tulee nää tietosuoja-asetukset vielä, niin jos ei ihmisiä kouluteta mitä sinne pilveen voi tallentaa ja tosiaan sellaset selkeet pelisäännöt, ni voi tulla kaikennäköistä yllätystä. Kyllä mä positiivisena näen kuitenki, että kaikki mikä helpottaa työntekoa tai muuta ni onhan ne tervetulleita ratkaisuita."* (H3)

Isojen toimijoiden pilvipalveluista on käytössä Office365, jonka varaan aiotaan tulevaisuudessa laskea vielä enemmän. Lisäksi käytetään Google apps for education ja Trello pilvipalveluita. Joidenkin käytössä on vielä lisäksi Asana & Slack –pilvipalvelut. Työasema- ja toimisto-ohjelmaympäristössä on ollut entuudestaan käytössä Microsoftin käyttöjärjestelmiä ja ohjelmia, joten Office365:een on siirrytty osittain niistä syistä. Lisäksi se on sopimusteknisesti helpoimmasta päästä hyväksyä.

> *"Office365 tulee sieltä Microsoft maailmasta, kun työasemaympäristö, toimisto-ohjelmaympäristö on Microsoft-*

> *merkkistä, niin silloin se on tällainen luonnollinen jatkumo että niitä samoja työkaluja pystyy käyttämään selain-pohjaisestikin. Käytettävyyden näkövinkkelistä nämä muut, ohjelmat Googlen, Trellon kaltaiset palvelut on hyvin helposti käytettäviä ja niihin ei tarvitse juurikaan opastaa henkilöstöä tai kouluttaa niiden käyttöön, kun käyttöliittymät on niin hyvin suunniteltu ja tehty."* (H1)

5.5 Pilvipalveluiden haasteet

Pilvipalvelut ovat teknisesti hyvin nopeasti käyttöönotettavissa ja niihin on voidaan integroida organisaation omat järjestelmät todella yksinkertaisesti ja helposti. Pilvipalveluihin siirtyminen on tuonut mukanaan joitakin lainopillisia sopimuspapereihin liittyviä ja yliheittoon liittyviä haasteita. Sopimusehdoista on lisäksi hankala neuvotella. Lisäksi loppukäyttäjät ovat olleet hämmästyneitä, kun esimerkiksi sähköpostiviestintään on tullut uusia ohjeistuksia. Haasteena on myös käyttäjien koulutus, liittyen esimerkiksi siihen, mitä tietoa sähköpostissa voi olla mukana.

> *"Ehkä isoin hankaluus on nää sopimuspaperien läpikäynti, koska ne on lakimiestekstiä, ne on tarkoituksella tehty hankalasti tulkittavaksi, se on ehkä se tietyllä lailla työläs osuus ja se vie aika paljon aikaa. Ja sitten siitä tulee vielä se, että niistä on hankala neuvotella. Eli mitä isompi toimija, sen vähemmän yksittäisellä asiakkaalla on mahdollisuus sopimuksen ehtoihin. Nyt syksyllä oli yksi haaste, tää niin ku Safe Harbor –sopimuksen raukeaminen. Taas täytyy sanoa, että tän O365-palvelun kansa ei sinänsä ollut ongelmaa, mutta sitten oli näitä pienempiä palveluntarjoajia, joilla ei nää mallisopimuslausekkeet ja muut ollut käytössä, vaan mitkä nojasi pelkästään siihen Safe Harbor –sopimukseen, niin ne olivat ongelmallisempia tapauksia."* (H2)

5.6 Tiedon tallentamisen periaatteet

LAMKilla ei ole voimassa olevaa sääntöä siitä, mitä pilveen voi laittaa ja mitä ei. Yleinen ohjeistus on kuitenkin tulossa. Ohjeistuksessa täytyy ottaa huomioon lainsäädäntö, jonka nojalla luokitteluohjeistuksia tehdään, etenkin julkisuuslaki määrittelee paljon salassa pidettäviä asioita. Luottamuksellisia asioita voidaan laittaa pilveen, jos palvelu arvioidaan riittävän turvalliseksi ja etenkin jos tiedon salaa ennen pilveen laittamista. Henkilötiedot, joissa voidaan yksilöidä joku ihminen tai muut salaiset asiat pilveen kuulu edes salattuna.

> *”Kyl mä nään niin, et henkilötiedot, kaikki tämmöiset tiedot missä voidaan yksilöidä joku ihminen, niin ne salassa pidettävää tietoa, niitä ei mun mielestä pilveen pitäis tallentaa. Ehkä ei edes salattuna. Pitäisin kyllä ihan omassa konesalissa. Tommosta luottamuksellista tietoa, keskeneräistä, suunnittelumateriaalia ni niitä vois ehkä olla salattuna ainakin, et se on semmoista vähän köykäsempää, mut kyl mä siinä sen rajottaisin. Ja tietysti nyt julkinen tieto, sehän nyt voi olla siellä, et ei haittaa.”* (H3)

Tieto pitäisi olla salattua etenkin tilanteessa, jos kyseessä on Suomen lakisääteisistä tietosuoja-asioista. Näitä ovat esimerkiksi sanalliset arvioinnit ja arkaluontoiset henkilötiedot. Salattavaa tietoa ammattikorkeapuolella ovat tutkimusdata tai business-kriittinen tieto. Lisäksi kaikki tiedot, joita kilpaileva organisaatio voi hyödyntää, on salattava, näitä ovat esimerkiksi liikesalaisuudet. Office 365 palvelussa yhteydet ovat https/ssl-salattuja, mutta salausavaimet ovat Microsoftin hallussa. Tietosuojalainsäädäntö ei huomioi, onko tieto salattua vai ei, vaikka salaamalla tieto on tallennettavissa pilvipalveluihin helpommin. Tieto on salattava omalla työasemalla, jonka jälkeen se voidaan siirtää pilveen.

> *”…Kyllähän nämä Office365-palvelut on sinänsä se yhteys jo salattu https/ssl –salattuja nämä yhteydet, että periaatteessa*

> *jos se tieto salataan siellä pilvipalveluissa tietyllä tavalla, niin sekin on vielä ok. Mutta jos sitä lähetetään ftp-yhteydellä tai http-yhteydellä, sähköpostin liitteenä, niin se on tietenkin sitten salattava työaseman päässä…"* (H2)

5.7 Pilvipalveluiden riskit

Yksi riski tulee lainsäädännöistä ja sopimuksista. Helposti voidaan päätyä tilanteeseen, jossa lakia rikotaan vahingossa. Esimerkiksi henkilötietoja saatetaan käsitellä väärässä tilanteessa, koska palveluntarjoaja on valittu huolimattomasti. Organisaatio voi olla myös tilanteessa, jossa se tulee liian riippuvaiseksi palveluntarjoajaan. Kun palveluntarjoajan palvelut lakkaavat, on organisaatio hankalassa tilanteessa, koska sen pitäisi saada tiedot palveluntarjoajalta takaisin ja varmistaa niiden poistaminen palveluntarjoajan laitteilta.

Monissa pilvipalveluissa saattaa jäädä epäselväksi, mitä tapahtuu tiedoille palvelun loppumisen jälkeen. Tietovuoto ja sitä kautta maineen menettäminen on suurin riski. Tietovuodon toteutuminen saattaisi johtua enemmin käyttäjän virheestä, kun esimerkiksi Microsoftin palvelimelle murtautumisen johdosta. Kalasteluviestit ovat yleisimpiä keinoja, joilla tietovuoto toteutuu.

> *"Tietovuoto. Suurin riski on ehkä maineen menettäminen jos puhutaan ammattikorkeesta niin opiskelijakato, tai se ei enää oo niin houkutteleva opiskelupaikkana tai työpaikkana, jos todetaan tämmöinen laajamittainen tietovuoto, jossa vaikka satojen tai tuhansien opiskelijoiden henkilötiedot on vuotanut jonnekin. Ehkä inhimillisen virheen takia tai muun toiminnan takia, kyllä nämä riskit kasvavat… Ehkä tällainen maineen menettämin on suurin riski. Kalasteluviestit ovat varmasti yleisimpiä, tavallaan se keino siihen, millä tavalla tällaiset vuodot ehkä toteutuu. Todennäköisesti on kalastelu, että joku antaa sitten johonkin hyvin naamioituun sähköpostiviestin*

> *perusteella omat verkkotunnuksensa vääriin käsiin. Niillä sitten saadaan tehtyä haittaa. Nämä ovat isoimmat riskit.”* (H1)

Kun LAMK siirtyi käyttämään Office 365:ta, käytiin riskeihin liittyviä keskusteluja ja pohdintoja yhdessä samankaltaisten organisaatioiden kanssa ammattikorkeakoulu verkostossa, mutta systemaattista riskikartoitusta ei tehty. Riskikartoituksessa olisi huomioitava sopimustekniset asiat, tiedon hallinnointiin liittyvät asiat ja saako tiedon ulos kun pilvipalveluiden käyttö lopetetaan. Lisäksi siinä olisi hyvä huomioida myös teknisiä kysymyksiä, kuten kuinka palvelu integroidaan omiin järjestelmiin sekä toimittajan palvelukuvausten ja palvelulupausten läpikäynti.

> *”Kyllä mun mielestä on ihan asiaa tommoinen. Oon sitä mieltä, että pitäis tehdä ihan kaikista palveluista kartoitus ja sitä kautta sitten ottaa ne riskit selville, ja sitten tietysti yrityksen oma asia on, että mikä riski hyväksytään, että ikinähän sitä ei saa kokonaan pois. Mutta riskejä saa aina pienennettyä.”* (H3)

5.8 Lainsäädännön vaikutus pilvipalveluissa

Organisaation pilvipalveluihin siirtymisprosessi alkaa lainsäädännöstä. LAMKin siirtyessä käyttämään Office365-palvelua, seurattiin yleistä ammattikorkeakoulujen linjausta. Microsoft on saanut EU mallilausekkeet, ja siirtymisen aikana oli voimassa Safe Harbor -sopimus. Palvelu katsottiin lainsäädännöllisesti turvalliseksi, koska mallilausekkeet pätevät siellä edelleenkin. Kun palvelua otettiin käyttöön, oli ehtona, että data säilyy fyysisesti Euroopassa olevilla palvelimilla.

Office 365:ssa on mahdollista tehdä myös niin, että välikätenä toimii joku suomalainen toimija. Silloin se pystyy takaamaan, että data on tallennettuna Suomessa sijaitsevaan konesaliin, jolloin siihen pätee suomalainen lainsäädäntö. Sopimuksen tekoon pitää panostaa, tarvittaessa lainoppineen kanssa.

> *”Kyllä ne vaikuttaa. Jos puhutaan tämmöisistä mitä koko organisaatio ajattelee käyttävänsä, niin se koko prosessi oikeastaan lähtee ehkä sieltä lainsäädännöstä, et onko tää mahdollisuus ottaa käyttöön ja miten siellä tää henkilötietojen elinkaaren hallinta esimerkiksi voidaan hoitaa..”* (H1)

5.9 Palveluntarjoajan ja asiakkaan väliset sopimukset

Palvelutasosopimuksessa eli SLA:ssa (*Service Level Agreement*) määritellään yleensä mm. vastuut, korvaukset ja sanktiot, missä tieto sijaitsee, saatavuus ja jos mahdollista niin palvelukerroksen vasteajat. Lisäksi olisi hyvä sopia tukeen liittyviä seikkoja, kuten tukiajat eli kuinka nopeasti ongelmiin puututaan, kuinka pitkiksi katkot voivat muodostua ja miten asiakas saa yhteyden tukeen sekä tukipyynnön käsittelyajat. Tiedon sijaitseminen on kuitenkin jossakin tapauksessa hankala määritellä.

Esimerkiksi Office 365 koostuu monesta eri osasesta, kuten Yammer, joka ei ole samalla tavalla integroitu siihen pakettiin kuin muut. Tämä saattaa aiheuttaa palvelukohtaisia poikkeuksia. Käyttötukea voidaan myös tarjota eri mantereella, kuin Euroopassa. Siinä tapauksessa tiedot käsitellään EU-alueen ulkopuolella, esimerkiksi Intiassa.

Nykyiset pilvipalvelut ovat sellaisia, että niissä palvelutasoon ei juuri voi vaikuttaa, eli ne tulevat sellaisenaan. Palvelut ovat monesti ainakin EU-tasolla samanlaisia, eikä neuvotteluvaraa niissä ole. Lisäpalveluina on mahdollista hankkia palveluntarjoajalta tai kolmannelta osapuolelta esim. varmistuspalveluita tai tietosuojan ja tietoturvan lisäystä. Pienet kotimaiset palveluntarjoajat ovat paremmin räätälöitävissä omiin tarpeisiin sopivammiksi.

> *”Yleensä siellä määritellään, tämmöinen yleinen sla-taso, mikä on sen palvelun saatavuus... Hyvä olisi, jos siellä pystyisi määrittelemään jollain lailla sen pilvipalvelun palvelukerroksen näitä vasteaikoja, eli kuinka hidas se voi käytännössä silti olla se pilvipalvelu... Sitten siinä pitää olla tavallaan nää tukiajat,*

> *kuinka nopeesti ongelmiin puututaan, tavallaan kuinka pitkiksi ne katkot voidavat muodostua, ja miten asiakas saa yhteyden näihin tukeen, onko siellä käytössä puhelinta, sähköpostia, jotain tiketöinti-järjestelmää ja mitkä ovat niiden käsittelyajat."* (H2)

5.10 Ulkopuolinen konsultointiapu

LAMKissa Office 365 palveluun siirtymisessä ja käyttöönoton jälkeen on käytetty konsultointiapua. Erityisesti IT- ja sopimuslakimiesten apua on tarvittu lausuntojen ja menettelytapa ohjeistuksien kanssa. Konsultoijan kanssa täytyy pitää huoli salassapito- tai vaitiolosopimuksesta, koska hän kuitenkin törmää tehtävässään organisaation tietoihin, tiedostoihin ja muihin tärkeisiin asioihin. Konsultoijan käyttäminen antaa tukea omalle toiminnalle, koska on paljon monimutkaisia asioita, joita konsultoijat ovat tehneet tai pohtineet entuudestaan muissakin yhteyksissä.

> *"Ilman muuta siis, mun mielestä toi on kuitenkin iso juttu… Pääsis sillai alkuun ja sais niin ku sellaset perusasiat kuntoon, niin mun mielestä siinä vaiheessa kannattaa käyttää. Puhutaan niin isosta kokonaisuudesta, että ilman muuta."* (H3)

Isojen toimijoiden kanssa on hyvin hankalaa sopia auditoinnista. Pelisäännöt on kuitenkin hyvä sopia firman sisällä useamman henkilön kanssa, vastasi yksi haastateltavista. Lisäksi tietosuojavastaava ja tietoturvaihmisillä on vahva rooli palveluun siirtyessä. LAMKin siirtyessä käyttämään Office 365 pilvipalvelua ei oltu käytetty asiantuntijaa, joka tarkistaisi eli auditoi tietoturvan ja tietosuojan vaatimusten toteuttamisen. Microsoftilla oli tuoreet dokumentit siitä, että tarkastuksia on tehty ulkopuolisten auditoijien toimesta Euroopassa oleviin konesaleihin.

> *"Näissä palveluissa mistä ollaan puhuttu, on kyllä auditointi dokumentaatiot sen verran tuoreita ja olemassa jo, että ei katsottu tarpeelliseksi että tarvitsee enää. Tähän oikeastaan pätee sama tarina, eli sitä on tässä*

ammattikorkeakouluverkostossa yhdessä käyty läpi näitä asioita. Ollaan saatu esimerkiksi Microsoftilta ihan tällainen kirjallinen dokumentaatio siitä, että tämä tieto pysyy Euroopan sisällä ja näin päin pois, niin erikseen ei ole tarvinnut tällaista isompaa auditointi-rumbaa käynnistää… Fyysinen puoli sieltä on katsottu ja prosessit ja muut jo kuntoon. Niistä löytyy dokumentit, niihin sitten luotettiin." (H1)

6 ANALYYSI

6.1 Käsitteet ”tietoturva” ja ”tietosuoja”

Ensimmäiseksi haastateltavilta kysyttiin keskeisistä aiheeseen liittyvistä käsitteistä. Kysymyksen taustalla oli saada selville henkilön oma näkemys kahdesta samantyylisestä, mutta eri asioita tarkoittavista käsitteistä. Haastateltavien vastaukset olivat samantyylisiä ja toisiaan täydentäviä. Tietoturva nähtiin liittyvän enemmän tekniseen puoleen, jolla pyritään toteuttamaan tietosuojaa.

6.2 Tietosuojakäytäntö

Toisessa osiossa kysyttiin organisaation tietosuojakäytäntöön liittyviä asioita. Tämän osion tarkoitus oli selvittää, kuinka organisaatiossa hoidetaan yksityisyyden suojaamisen periaatteet ja ohjeistukset.

LAMKissa ei ole käytössä koko organisaation kattavaa tietosuojadokumentaatiota. Tarkat ohjeistukset löytyvät kuitenkin henkilöiltä, jotka käsittelevät työtehtävissään henkilötietoja. LAMKissa yksityisyyden suojaamisen periaatteet pyritään hoitamaan tiedottamalla asioista intranetissä, raportoimalla sekä väärinkäytöksiin puuttumalla. Henkilökuntaa, jotka käsittelevät henkilötietoja työtehtävissään, ei vastaajien mukaan kouluteta riittävästi. Kaikki vastaajat olivat sitä mieltä, että henkilötietoja käsittelevien henkilöiden pitäisi saada lisäkoulutusta työtehtäviin liittyen.

Työntekijöiden käyttöoikeuksia jaetaan ja hallitaan monin tavoin. Haastateltavat kertoivat, että työntekijöiden käyttöoikeuksia jaetaan ja hallitaan henkilökohtaisella käyttäjätunnuksella ja salasanalla. Käyttäjätunnus on sidottu tiettyyn lähdejärjestelmään ja pääkäyttäjät ovat vastuussa oikeuksien antamisesta tiedostopalveluluihin ja henkilöstöhallinnan järjestelmiin. Työsopimuksessa sitoudutaan olemaan

kertomatta yrityksen asioita eteenpäin, lisäksi voidaan kirjata erillinen vaitiolositoumus.

Vastaajat kertoivat, että LAMKin ohjeistuksen mukaan mitään luottamuksellista tietoa ei pitäisi lähettää perinteisellä sähköpostilla. Salausta tulisi käyttää, jos materiaali ei ole julkista. Tämän vuoksi LAMKissa on käytössä sähköpostin salausmahdollisuus. Haastateltavilta kysyttiin myös omaa näkemystä siitä, onko tietosuojaan liittyvät asiat hoidettu LAMKissa hyvin ja voisiko jotain parantaa. Vastaajien mukaan LAMKissa on paljon parannettavaa tietosuojaan liittyvissä asioissa. Tiedottaminen, vastuuttaminen ja tulevaan EU tietosuoja-asetukseen varautuminen nähtiin tärkeimpinä.

LAMKissa mobiililaitteisiin on määritelty tietyt tietoturva-asetukset ja ne ovat etähallittavissa. Kokonaisvaltainen mobiilipolitiikka puuttuu LAMKista, mutta joitakin sääntöjä ja ohjeistuksia on määritelty.

6.3 Pilvipalvelut

Kolmannessa haastattelun osiossa kysyttiin pilvipalveluista ja sitä, minkälaisilla toimenpiteillä niiden käyttöönottoon oli valmistauduttu tai kuinka pitäisi valmistautua, jos siirtyminen tapahtuisi nyt tai lähitulevaisuudessa. Pilvipalveluiden tulevaisuus nähdään LAMKissa valoisana, ja niiden tarjoama hyöty nähdään kustannustehokkaana. Suosituin pilvipalvelu on Microsoftin tarjoama Office 365. Siihen on päädytty, koska sen toimittaja on entuudestaan tuttu ohjelmien ja käyttöjärjestelmien kautta, ja sillä on tukenaan ison organisaation resurssit. Vastaajien mukaan pilvipalveluihin siirtymisen suurimmat haasteet ovat olleet lainopillisia sopimuksiin liittyviä sekä loppukäyttäjien ohjeistamiseen liittyviä seikkoja.

LAMKissa ei ole voimassa olevaa sääntöä siitä, mitä pilveen voi tallentaa ja mitä ei. Ohjeistusta on kuitenkin tarvittaessa saatavilla ja yleinen ohjeistus on työn alla. Kahden vastaajan mukaan luottamuksellisia asioita voi pilveen laittaa, jos palvelu arvioidaan turvalliseksi ja etenkin jos tiedon

salaa ennen pilveen siirtämistä. Haastateltavilta kysyttiin, että missä tilanteessa tiedon pitäisi olla salattua ennen kuin sen siirtää pilveen. Vastauksien mukaan salaukseen täytyy turvautua etenkin tilanteessa, jos kyseessä on Suomen lakisääteisiä asioita tai esimerkiksi ammattikorkeakoulun tutkimusdataa ja liikesalaisuuksia. Haastateltavien mukaan tieto on salattava omalla työasemalla, ennen kuin sen siirtää pilveen. Arkaluontoisia henkilötietoja tai muita salaisia tietoja ei asioista päättävien mielestä pidä pilveen laittaa edes salattuna. LAMKissa ollaan tietoisia siitä, että vaikka Microsoftin palvelut ovat salattuja, ovat salausavaimet Microsoftin omassa hallussa.

Pilvipalveluihin siirtymistä ei nähdä täysin riskittömänä. Esille nousseita riskejä olivat tahaton lain rikkomisen mahdollisuus, riippuvaisuus palveluntarjoajaa kohtaan, tietovuodon mahdollisuus ja sitä kautta maineen menettäminen. Vastaajien mukaan pilvipalveluihin siirryttäessä LAMKissa nähdään tarpeelliseksi tehdä riskikartoitus ennen palveluun siirtymistä, vaikka Office 365:een siirtyessä sitä ei tehty. Keskusteluja ja pohdintoja kuitenkin käytiin ammattikorkeakoulu verkostossa.

Tärkeitä seikkoja riskikartoituksessa katsotaan olevan sopimustekniset ja tiedon hallinnointiin liittyvät asiat sekä saako tiedon ulos kun palvelu lopetetaan. Näiden lisäksi joitakin teknisiä kysymyksiä, kuten palvelun integrointiin liittyvät asiat olisi haastateltavien mukaan huomioitava riskikartoituksessa. Myös palvelukuvaukseen ja palvelulupauksiin tutustumista pidetään tärkeänä.

Pilvipalveluihin siirtyessä kysyttiin vastaajilta näkemystä eri lainsäädäntöjen vaikutusta tietosuojaan. Tietosuojaan liittyvät lainsäädännöt nähtiin merkittäväksi tekijäksi pilvipalveluihin siirtyessä. Office 365 palveluun siirtyessä Microsoft oli sitoutunut EU-mallilausekkeisiin ja Safe Harbor –sopimus oli vielä silloin voimassa sen aikaisilla ehdoilla. Lisäksi Microsoftilta on saatu kirjallinen dokumentaatio siitä, että tieto pysyy Euroopan sisällä.

Pilvipalveluihin siirryttäessä ammattikorkeakoulut sopivat keskeiset tietosuojan varmistamiseen liittyvät asiat palveluntarjoajan kanssa palvelutasosopimuksella (SLA). Tarpeelliseksi nähdään sopia mm. vastuut, korvaukset ja sanktiot, tiedon sijainti, saatavuus ja vasteajat. Näiden lisäksi vielä käyttötukeen liittyvät seikat olisi hyvä mainita sopimuksessa. Lisäksi ilmeni, että pilvipalveluiden palvelutasoon ei kuitenkaan juuri voi nykyään vaikuttaa, vaan peruspalvelut tulevat sellaisenaan.

Ulkopuolisen konsultointiavun käyttäminen koettiin hyvänä kaikkien vastaajien kesken. Tutkimustuloksista on nähtävissä, että LAMK on valmis käyttämään ulkopuolista konsultointiapua pilvipalveluihin siirtyessä, mikäli osaamista ei esimerkiksi lausuntojen ja ohjeistuksien kanssa itseltä löydy. Konsultointiavun käytössä on pidettävä huoli salassapito- tai vaitiolosopimuksesta, jotta ulkopuolinen henkilö ei pääse hyödyntämään yrityksen luottamuksellista tietoa. Aikaisimmin mainittuihin pilvipalveluihin siirtyessä ei ole ollut mahdollista selvittää auditoinnilla tietosuojan ja tietoturvan vaatimusten toteuttamista. Palveluntarjoajien ratkaisuita on kuitenkin tarkistettu säännöllisesti ulkopuolisten auditoijien toimesta, joista on olemassa tuoreet dokumentit.

7 JOHTOPÄÄTÖKSET

Tutkimuksen tavoitteena oli löytää organisaation käyttämät keinot ja toimintaperiaatteet, joilla se pyrkii varmistamaan tietojen tietosuojauksen, kun siirrytään käyttämään pilvipalvelupohjaisia ratkaisuja. Tarkoituksena oli kartoittaa, minkälaisin keinoin oppilaitoksessa oli varauduttu aiemmissa pilvipalveluiden käyttöönotossa sekä minkälaisin keinoin tietojen tietosuoja pyritään varmistamaan nykyisin.

Tutkimuskysymys oli: ”Kuinka organisaation tietojen tietosuoja pyritään varmistamaan siirryttäessä käyttämään pilvipalvelupohjaisia ratkaisuja?” Koska tietojen tietosuojan varmistamiseen liittyy monenlaisia eri tekijöitä, voidaan tähän kysymykseen vastata tarkastamalla tuloksia kokonaisuutena.

7.1 Tietojen suojaaminen

Tutkimustuloksista ilmeni, että ammattikorkeakouluissa ei ole käytössä tietosuojadokumentaatiota, joka koskisi koko organisaatiota. Tämä ei vastaa Salmisen (2009, 129) mukaan suositeltua käytäntöä. Yrityksellä olisi hyvä olla selkeät ja tarkat yleisohjeistukset, jotka koskisivat koko henkilökuntaa. Tällä tavalla voitaisiin varmistaa, että koko organisaation työntekijät noudattavat samoja ennalta määriteltyjä tietosuojauksen periaatteita. Tietosuojaan liittyvää tiedotusta on myös hyvä pitää yllä tasaisin väliajoin, jotta henkilökunta pysyy asiasta valveilla ja tahattomien väärinkäytöksien riski pienenee.

Henkilötietoja työtehtävissään käsitteleville henkilöille nähdään tarpeelliseksi järjestää lisäkoulutusta ammattikorkeakouluissa. Tästä voidaan päätellä, että koulutus nähdään tärkeänä sekä ymmärretään, että on riskialtista työskennellä luottamuksellisten tietojen parissa, jos pelisäännöt eivät ole kaikille täysin selvät. Ammattikorkeakouluissa käyttöoikeuksia jaetaan ja hallitaan käyttäjätunnuksella ja salasananalla. Lisäksi tietojen tietosuojaa pyritään varmistamaan vaitiolosopimuksilla. Edellä mainitut ovat vahvoja toimenpiteitä, joilla pyritään varmistamaan,

että käsiksi pääsevää tietoa ei käytetä vääriin tarkoituksiin. Käyttöoikeuksia on hyvä jakaa harkiten ja hallitusti, jotta liialliset oikeudet eivät kasvattaisi organisaation tietosuojariskiä.

Sähköposti liikkuu verkossa usein salaamattomana. Salaamattomuus on riskialtista etenkin silloin, jos sähköposti sisältää salaista luottamuksellista tietoa. Tuloksien mukaan ammattikorkeakouluissa on käytössä sähköpostin salausmahdollisuus. Tästä voidaan päätellä, että luottamuksellista tietoa varjellaan ammattikorkeakouluissa tarkasti. Lisäksi lakipykäliä noudatetaan tarkasti, eikä heillä ole varaa, eikä syytä niistä lähteä tinkimään. Ammattikorkeakouluissa toimitaan samassa linjassa teoriassa esitettyjen ohjeistuksien kanssa. Tuloksista ilmeni, että tietosuojaan liittyvissä asioissa on parantamisen varaa. Tiedottamista, vastuuttamista ja tulevaan EU tietosuoja-asetukseen varautumista pidettiin merkittävimpinä. Tuloksista voidaan päätellä, että henkilökunta on valveutunut ja heillä on katse tulevaisuudessa.

Pilvipalveluiden mobiilikäyttö lisää urkinnan riskejä, joten mobiililaitteet tuovat uusia haasteita turvalliseen pilvipalveluiden käyttöön. Ammattikorkeakoluissa mobiililaitteet ovat etähallittavia ja niihin on määritelty tietyt tietoturva-asetukset tietosuojan lisäämiseksi. On merkittävää huomata, että oppilaitoksissa on ymmärretty mobiililaitteiden tuoma lisäriski pilvipalveluiden käytössä.

Tuloksista tuli ilmi, että ammattikorkeakouluissa mobiililaitteisiin liittyviä ohjeistuksia ja sääntöjä on määritelty, mutta varsinainen mobiilipolitiikkaa puuttuu. Lisääntyvän mobiililaitteiden aikakautena voisi olla suotavaa laatia niiden käyttöön ja hallintaan liittyvät yhtenäiset toimintaperiaatteet, joilla pyritään vähentämään erilaisia riskejä (Andreasson ym. 2014, 91-92).

7.2 Pilvipalveluihin siirtyminen

Ammattikorkeakouluissa pilvipalvelut koetaan hyviksi ratkaisuiksi ja niitä otetaan käyttöön tulevaisuudessa yhä enemmän. Tutkimuksessa kävi myös ilmi, että pilvipalveluihin liittyvät riskit ja haasteet ovat

ammattikorkeakouluissa hyvin tiedossa. Haasteista riippumatta pilvipalveluiden tarjoama hyöty nähdään kiistattomana, koska niihin ollaan tulevaisuudessa siirtymässä enemmissä määrin. Ammattikorkeakouluissa ei ole tarkkaa määritelty, mitä pilveen voi tallentaa ja mitä ei. Joitakin linjauksia on tehty, kuten että luottamuksellista tietoa voi pilveen tallentaa, etenkin jos tieto on salattu ennen pilveen siirtämistä. Järvinen (2014, 284), Chang (2014) ja Velumadhava Rao ym. (2015) ovat myös sitä mieltä, että tietojen turvallinen tallentaminen pilveen voidaan varmistaa tietojen salauksella. Tuloksien mukaan arkaluontoista salaista tietoa ei ammattikorkeakouluissa pidä pilveen tallentaa edes salattuna. Tästä voidaan päätellä, että oppilaitoksissa on perehdytty tiedon suojauksen periaatteisiin, ja niissä pyritään toimiaan yleisten periaatteiden mukaan.

Tutkimustuloksista selvisi, että ammattikorkeakoulujen käyttämät Microsoftin pilvipalvelut ovat salattuja, mutta salausavaimet ovat kuitenkin Microsoftilla hallussa. Johtopäätöksenä voidaan todeta, että ammattikorkeakouluissa luotetaan palveluntarjoajiin ja että he toimivat sopimusten mukaan. Microsoft on iso tekijä pilvipalvelumarkkinoilla, joten heillä ei ole maineensa menettämisen vuoksi intressejä hyödyntää asiakkaidensa tietoja, vaikka he hallitsevat salausavaimia.

Tutkimuksessa kävi myös ilmi, että pilvipalveluihin liittyvät erilaiset riskit ovat hyvin tiedossa. Riskejä voidaan vähentää sopimuksen tekemisellä palveluntarjoajan kanssa, ja esimerkiksi sopia, että tiedot pysyisivät vähintäänkin EU-alueella. Office 365:een siirryttiin käyttämään ilman riskikartoituksen tekoa. Voidaan todeta, että Microsoft koetaan luotettavaksi ja turvalliseksi palvelujen tuottajaksi ammattikorkeakoulujen keskuudessa. Riskikartoitus koettiin tärkeäksi tehdä palveluntarjoajan kanssa ja siinä olisi hyvä huomioida mm. sopimustekniset ja tiedon hallinnointiin liittyvät seikat. Tästä voidaan päätellä, että pilvipalveluihin siirtymistä ei nähdä ammattikorkeakouluissa riskittömänä.

Erilaiset lainsäädännöt tiedettiin olevan suuressa roolissa pilvipalveluiden käyttöönotossa. Tulokset toivat esille, että ammattikorkeakoulut ovat

perehtyneet lainsäädännöllisiin seikkoihin pilvipalveluihin siirtyessä ja he ovat siten ymmärtäneet vaatia palveluntarjoajalta tietojen säilyttämistä Euroopassa. Palvelutasosopimuksessa nähtiin tärkeänä sopia palveluntarjoajan kanssa tietosuojan varmistamiseen liittyviä asioita, kuten esimerkiksi vastuut ja tiedon sijainti. Tuloksien mukaan ammattikorkeakoulut sopivat palvelutasosopimuksella juuri niitä tärkeitä asioita, jotka takaavat palvelulle halutun tason (Viestintävirasto 2014, 15).

Ulkopuolisen konsultointiavun käyttö nähtiin positiivisena. Ulkopuolisen avun käyttäminen on suotavaa, etenkin jos apua tarvitaan sellaisella osa-alueella, josta talon sisällä ei ole riittävää osaamista. Office 365:een siirtyessä erillistä auditointia ei tehty tietosuojan ja tietoturvan osalta, koska Microsoftilla oli näyttää siitä tuoreet asiakirjat. Pääteltävissä on, että ammattikorkeakoulut luottavat isoihin palveluntarjoajiin, koska heillä on resursseja sijoittaa tietoturvaan ja tietosuojaan, eikä heillä ole maineensa vuoksi varaa mennä sieltä, mistä aita on matalin.

Tämän tutkimuksen perusteella voidaan päätellä, että pilvipalveluihin siirryttäessä ammattikorkeakoulujen tietojen tietosuojaus pyritään varmistamaan varsin mallikelpoisesti teoriassa esitettyihin ohjeistuksiin nähden.

8 YHTEENVETO

Tämän tutkimuksen tarkoituksena oli selvittää, kuinka organisaatiot pyrkivät varmistamaan tietojen tietosuojauksen siirtyessä käyttämään pilvipalvelupohjaisia ratkaisuja. Tutkimus toteutettiin kvalitatiivisena tapaustutkimuksena Lahden ammattikorkeakoululle ja siinä käytettiin deduktiivista lähestymistapaa. Tutkimusaineisto kerättiin puolistrukturoidulla haastattelulla, joka litteroitiin tekstiksi analysointia varten.

Haastateltavina oli henkilöitä Salpauksesta, jotka ovat olleet keskeisessä asemassa organisaation pilvipalveluiden käyttöönotossa sekä yksi henkilö LAMKin tietohallinnosta. Tutkimusaineistosta tehtyjä tutkimustuloksia verrattiin kirjallisuudesta koostuvaan teoriaan ja aiempiin aiheeseen liittyviin tutkimustuloksiin.

8.1 Tietosuojan varmistaminen LAMKissa

Tämän tutkimuksen mukaan LAMKin tietojen tietosuojaukseen voidaan vaikuttaa monin eri tavoin, joten tutkimustuloksia on tarkasteltava kokonaisuudessaan. Tutkimuksessa esille tulleiden seikkojen mukaan tietosuojauksen varmistusta pyritään toteuttamaan mm. ohjeistamalla henkilöitä, jotka käsittelevät työtehtävissään henkilötietoja, tiedottamalla asioista intranetissä, raportoimalla ja väärinkäytöksiin puuttumalla. Työntekijöiden käyttöoikeuksia hallitaan henkilökohtaisilla käyttäjätunnuksilla ja salasanalla. Pääkäyttäjät ovat vastuussa antamistaan oikeuksista tiedostopalveluihin ja henkilöstöhallinnan järjestelmiin. LAMKin henkilökunta sitoutuu työsopimuksessa olemaan kertomatta yrityksen asioita eteenpäin.

LAMKin ohjeistuksen mukaan mitään luottamuksellista tietoa ei pitäisi lähettää perinteisellä sähköpostilla. Tähän tarkoitukseen LAMKilla on käytössä sähköpostin salausmahdollisuus. Mobiililaitteet ovat etähallittavia ja niissä on tietynlaiset tietoturva-asetukset tietosuojan turvaamiseksi.

Mobiililaitteiden turvalliseen käyttöön liittyvä ns. mobiilipolitiikka puuttuu LAMKista, mutta joitakin sääntöjä ja ohjeita on aiheesta määritelty.

8.2 LAMKin siirtyminen pilvipalveluiden käyttäjäksi

Pilvipalvelut koetaan myönteisenä asiana LAMKissa. Suurimmassa roolissa on Microsoftin Office 365 -palvelu. Palveluihin siirtymisen päähaasteet ovat sopimuksiin liittyvät lainopilliset haasteet sekä loppukäyttäjien ohjeistuksiin liittyvät haasteet. Pilvipalveluihin liittyvä yleinen ohjeistus on työn alla. Tämän vuoksi LAMKista ei löydy voimassa olevaa linjausta esimerkiksi siitä, mitä pilveen voi tallentaa ja mitä ei. Ohjeistusta on kuitenkin saatavilla tarpeen tullen. LAMKin ohjeistuksen mukaan luottamuksellista tietoa voi pilveen tallentaa, jos palvelu arvioidaan turvalliseksi ja jos tieto salataan ennen pilveen siirtoa. Arkaluontoisia henkilötietoja ja salaiseksi luokiteltavaa tietoa ei pilveen tule laittaa edes salattuna.

Pilvipalveluihin liittyvät riskit ovat LAMKilla tiedossa, ja riskikartoituksen tekeminen nähtiin tärkeänä uusiin palveluihin siirtyessä. Tietojen suojausta pilvipalveluissa on pyritty varmistamaan myös siten, että Microsoftin kanssa on sovittu tietojen säilyttämistä vain Euroopan alueella. Keskeinen väline tietojen tietosuojauksessa on palvelutasosopimuksen (SLA) tekeminen palveluntarjoajan ja asiakkaan välille. Siinä LAMKissa nähdään tärkeänä määritellä mm. palveluntarjoajan ja asiakkaan vastuiden jakaminen, korvaukset ja sanktiot, saatavuus, vasteajat sekä missä yrityksen tietoa säilytetään ja ylläpidetään.

Pilvipalveluihin siirtyessä tietojen tietosuojausta voidaan LAMKissa vahvistaa ulkopuolisella konsultointiavun käyttämisellä, mikäli talosta ei löydy tarvittavaa osaamista jollakin osa-alueella. Salassapito- tai vaitiolosopimus on kuitenkin hyvä laatia ulkopuolisen henkilön kanssa ennen toimeksiantoa. Lisäksi LAMK on valmis käyttämään omaa tai ulkopuolista asiantuntijaa, jonka tehtävänä olisi auditoida eli tarkistaa

palveluntarjoajan tietoturvan ja tietosuojan vaatimusten toteutuksen, jos se nähdään tarpeelliseksi.

Edellä mainitut toimenpiteet pyrkivät varmistamaan LAMKin tietojen tietosuojan pilvipalveluihin siirtyessä. Kokonaisuudessaan LAMK on hoitanut pilvipalveluihin siirtymisen huolella ja ammattitaidolla, kuten isolta organisaatiolta voisi olettaakin.

Tutkimuksen voisi jatkossa tehdä joillekin eri aloille, jotta voitaisiin verrata, poikkeavatko tapaustutkimusten tutkimustulokset keskenään eri alojen välillä. Tällä tavoin tutkimuksesta voisi hyötyä myös muiden alojen organisaatiot.

8.3 Reliabiliteetti

Reliabiliteetilla tarkoitetaan, kuinka luotettavasti ja toistettavasti käytetty mittari mittaa tiettyä ilmiötä. Yksi keino arvioida reliabiliteettia on tehdä toistomittauksia. (Tilastokeskus 2006a.) Tutkimuksen toistamisella pitäisi saada samat tulokset, vaikka tutkija vaihtuisi (Silius & Tervakari 2006). Tutkimuksen luotettavuutta pohdittaessa on otettava huomioon, millä tavalla tutkimuksen luonne ja tutkimusaihe ovat vaikuttaneet tutkimukseen osallistuneiden vastauksiin (Saaranen-Kauppinen & Puusniekka 2006d).

Tutkimusaineisto kerättiin tallentamalla haastattelu, josta se litteroitiin tekstiksi. Haastattelut kirjoitettiin tarkasti sanasta sanaan, joten haastateltavien vastaukset on huolella kirjoitettu siten, miten he kysymyksiin vastasivat. Tutkimuskysymykset olivat sellaisia, joihin haastateltavilla oli mahdollisuus vastata perustellen omin sanoin, eivätkä vastaukset olleet ennalta-arvattavissa. Haastattelurunko oli myös kaikilla haastateltavilla sama, joka lisää reliabiliteettia.

8.4 Validiteetti

Validiteetti kertoo, kuinka hyvin tutkimuksen mittausmenetelmä mittaa juuri sitä tutkittavan ilmiön ominaisuutta, mitä on tarkoituskin mitata

(Tilastokeskus 2006b). Validiteetilla ilmaistaan tutkimuksen pätevyyttä, eli onko se perusteellisesti tehty, ja ovatko siitä saadut tulokset ja päätelmät oikeita. Laadullisessa tutkimuksessa kyse on lähinnä uskottavuudesta ja vakuuttavuudesta. (Saaranen-Kauppinen & Puusniekka 2006e.)

Tutkimuksen tarkoitus oli etsiä niitä keinoja, joilla organisaatio pyrkii varmistamaan tietojen tietosuojauksen pilvipalveluihin siirtyessä. Haastateltavat olivat alansa asiantuntijoita, ja he ovat vaikuttaneet keskeisessä asemassa organisaation siirtyessä pilvipalveluihin. Haastattelun kysymykset muodostettiin kirjallisuudesta saatavan teorian pohjalta, joten kysymykset olivat ennalta tarkkaan mietitty. Kysymyksillä oli tarkoitus saada laaja-alainen näkemys LAMKin linjauksesta ja toimintaperiaatteista, joilla he pyrkivät varmistamaan tietojen tietosuojaa.

Aineistonkeruumenetelmänä haastattelu oli pätevä, koska siinä informaatio saadaan suoraan asianomaiselta. Haastattelutilanteessa haastateltava oli yksin haastattelijan kanssa, joten heillä on ollut vapaus vastata ilman kollegoiden tai muiden henkilöiden läsnäolon vaikutusta. Tutkimuksen johtopäätökset on tehty itsearviona vertaamalla tutkimustuloksia teoriaosuuteen.

8.5 Yleistettävyys

Tapaustutkimuksia ei ole tapana yleistää, mutta arvioinnissa voidaan pohtia tutkimustuloksia myös laajemmassa mittakaavassa. Voidaan esimerkiksi miettiä, kuinka saatuja tuloksia voitaisiin soveltaa jossain muualla tai kuinka yksittäistapauksen tuloksia voisi hyödyntää, jos samasta aiheesta ollaan tekemästä laajempia tutkimuksia (Saaranen-Kauppinen & Puusniekka 2006b.)

Vaikka tutkimus toteutettiin ns. single-case studyna, voidaan tutkimustulokset yleistää koskemaan monia ammattikorkeakouluja. Ammattikorkeakoulut toimivat opetus- ja kulttuuriministeriön alaisuudessa ja pilvipalveluihin siirtyessä asiaa oli pohdittu yhdessä muiden

ammattikorkeakoulujen kanssa, joten ammattikorkeakoulujen toimintaperiaatteet noudattavat yhtenäisiä linjauksia.

LÄHTEET

Aleem, A. & Sprott, C. R. 2013. Let me in the cloud: analysis of the benefit and risk assessment of cloud platform. Journal of Financial Crime [verkkolehti]. 20, 6-24 [Viitattu 27.1.2016]. Saatavissa: http://www.emeraldinsight.com/doi/abs/10.1108/13590791311287337#

Andreasson, A. 2015. Opi tietosuojaa. EU:n tuleva tietosuoja-asetus muuttaa kansalliset käytännöt [viitattu 27.10.2015]. Saatavissa: https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus

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

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 2. Helsinki: Tietosanoma.

Chang, H. 2014. Data Protection Regulation and Cloud Computing. The University of Hong Kong - Law and Technology Centre [viitattu 27.1.2016]. Saatavissa: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2610615

Arstila, A. 2012. Pilvipalvelut: Kymmenen kysymystä, joita et ole koskaan kehdannut kysyä. Sulava [viitattu 15.1.2016]. Saatavissa: http://www.sulava.com/2012/04/pilvipalvelut-kymmenen-kysymysta-joita-et-ole-koskaan-kehdannut-kysya/

European Commission 2015. Countries outside the EU (third countries) [viitattu 28.10.2015]. Saatavissa: http://ec.europa.eu/justice/data-protection/bodies/authorities/third-countries/index_en.htm

Hanhirova, A. 2011. Mitä pilvipalvelut ovat? Gapps [viitattu 15.1.2016]. Saatavissa: http://www.gapps.fi/mita-ovat-pilvipalvelut/

Heino, P. 2010. Pilvipalvelut. Helsinki: Talentum.

Jyväskylän yliopisto 2015a. Empiirinen tutkimus [viitattu 3.2.2016]. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/empiirinen-tutkimus

Jyväskylän yliopisto 2015b. Laadullinen tutkimus [viitattu 15.1.2016]. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus

Jyväskylän yliopisto 2015c. Tapaustutkimus [viitattu 3.2.2016]. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/tapaustutkimus

Järvinen, P. 2014. NSA: Näin meitä seurataan. Jyväskylä: Docendo.

Lahden ammattikorkeakoulu 2015. Organisaatio [viitattu 29.2.2016] Saatavissa: http://www.lamk.fi/lamk-oy/organisaatio/Sivut/default.aspx

Oikeusministeriö 2015. Euroopan unionin tietosuojalainsäädännön uudistaminen [viitattu 27.10.2015]. Saatavissa: http://www.oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/euroopanunionintietosuojalainsaadannonuudistaminen.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006a. KvaliMOTV – Aineisto- ja teorialähtöisyys. Tampere: Yhteiskuntatieteellinen tietoarkisto [viitattu 3.2.2016]. Saatavissa: http://www.fsd.uta.fi/menetelmaopetus/kvali/L2_3_2_3.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006b. KvaliMOTV - Tapaustutkimus. Tampere: Yhteiskuntatieteellinen tietoarkisto [viitattu 3.2.2016]. Saatavissa: http://www.fsd.uta.fi/menetelmaopetus/kvali/L5_5.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006c. KvaliMOTV - Strukturoitu ja puolistrukturoitu haastattelu. Tampere:

Yhteiskuntatieteellinen tietoarkisto [viitattu 15.1.2016]. Saatavissa: http://www.fsd.uta.fi/menetelmaopetus/kvali/L6_3_3.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006d. KvaliMOTV - Reliabiteetti. Tampere: Yhteiskuntatieteellinen tietoarkisto [viitattu 10.2.2016]. Saatavissa: http://www.fsd.uta.fi/menetelmaopetus/kvali/L3_3_2.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006e. KvaliMOTV - Validiteetti. Tampere: Yhteiskuntatieteellinen tietoarkisto [viitattu 10.2.2016]. Saatavissa: http://www.fsd.uta.fi/menetelmaopetus/kvali/L3_3_1.html

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

Salo, I. 2010. Cloud computing – Palvelut verkossa. Jyväskylä: WSOYpro Oy.

Syrjälä, J. 2015. Pilvipalveluiden tietosuojan varmistaminen. Tampereen teknillinen yliopisto [viitattu 27.11.2015]. Diplomityö. Saatavissa: http://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/23002/syrjala.pdf

Silius, K. & Tervakari, A-M. 2006. Tampereen teknillinen yliopisto. Kvalitatiiviset tutkimusmenetelmät [viitattu 19.2.2016]. Saatavissa: http://matwww.ee.tut.fi/hmopetus/kval-tutk/2005/luennot2005/liitteet/kvalit070306.pdf

Tietosuojavaltuutetun toimisto 2013. Henkilötietolaki [viitattu 27.10.2015]. Saatavissa: http://www.tietosuoja.fi/fi/index/lait/Henkilotietolaki.html

Tietosuojavaltuutetun toimisto 2014. Julkisuuslaki [viitattu 27.10.2015]. Saatavissa: http://www.tietosuoja.fi/fi/index/lait/julkisuuslaki.html

Tietosuojavaltuutetun toimisto 2015a. EU:n tietosuojauudistus [viitattu 27.10.2015]. Saatavissa: http://www.tietosuoja.fi/fi/index/lait/euntietosuojauudistus.html

Tietosuojavaltuutetun toimisto 2015b. Henkilötietojen ulkomaille luovutus [viitattu 28.10.2015]. Saatavissa: http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/ilmoitusvelvollisuus/henkilotietojenulkomailleluovutus.html

Tilastokeskus 2006a. Käsitteet ja määritelmät: Reliabiliteetti [viitattu 10.2.2016]. Saatavissa: http://www.stat.fi/meta/kas/reliabiliteetti.html

Tilastokeskus 2006b. Käsitteet ja määritelmät: Validiteetti [viitattu 10.2.2016]. Saatavissa: http://www.stat.fi/meta/kas/validiteetti.html

Tilastokeskus 2014. Tietotekniikan käyttö yrityksissä [viitattu 15.1.2016]. Saatavissa: http://www.stat.fi/til/icte/2014/icte_2014_2014-11-25_fi.pdf

Velumadhava Rao, R. & Selvamani, K. 2015. Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science [verkkolehti]. 48, 204-209 [Viitattu 27.1.2016]. Saatavissa: http://www.sciencedirect.com/science/article/pii/S1877050915006808

Viestintävirasto 2014. Pilvipalveluiden turvallisuus [verkkodokumentti]. Helsinki [viitattu 4.11.2015]. Saatavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf

LIITTEET

LIITE 1: Haastattelurunko

1. **Haastateltavan tenttaus**
   - Nimi?
   - Minkälainen koulutus sinulla on?
   - Mitä teet työksesi?
   - Mitä käsiteet ”tietosuoja” ja ”tietoturva” mielestäsi sisältää?
2. **Tietosuojakäytäntö**
   - Millaisilla toimenpiteillä yksityisyyden suojaamisen periaatteet ja ohjeistukset hoidetaan LAMKIssa?
     - Pidetäänkö LAMKissa yllä tietosuojadokumentaatiota, joka kattaa organisaation henkilöstötietojen käsittelyn periaatteet?
     - Ohjeistetaanko ja koulutetaanko henkilökuntaa, jotka käsittelevät henkilötietoja työtehtävissään?
       - Miten?
     - Miten työntekijöiden käyttöoikeuksia jaetaan ja hallitaan? (esim. tietosuoja- ja vaitiolositoumukset, toimintaperiaatteet)
   - Mitä mieltä olet sähköpostiviestin salauksesta? Koska sitä pitäisi käyttää?
   - Onko tietosuojaan liittyvät asiat mielestäsi hoidettu hyvin? Voisiko jotain parantaa?

   Mobiililaitteiden käyttö
   - Onko LAMKissa määritelty ns. mobiilipolitiikkaa, jossa pyritään selkiyttämään, yhtenäistämään, määrittelemään ja ohjeistamaan mobiililaitteiden käyttöön liittyviä asioita ja toimintatapoja?
     - Jos on, mitä se sisältää?
3. **Pilvipalvelut**
   - Mitä mieltä olet pilvipalveluista ja millaisena näet niiden tulevaisuuden?
   - Mitä pilvipalveluita LAMKilla on käytössä?
   - Miten ja miksi juuri näihin palveluihin on päädytty?
   - Millaisia haasteita on tullut vastaan käyttöönotossa?
   - Millaista tietoa pilvipalvelimelle voi mielestäsi laittaa ja mitä ei?
   - Missä tilanteessa tiedon pitäisi olla salattua ennen sen siirtämistä pilveen?
   - Millaisia riskejä pilvipalveluihin siirtyminen mielestäsi tuo ja niiden todennäköisyys?
   - Miten tietosuojaan liittyvät eri lainsäädännöt vaikuttavat palveluiden käyttöönotossa? (esim. Henkilötietolaki, työelämän tietosuojalaki, henkilötietojen luovutus EU/muu maailma ym.)
   - Koetko riskikartoituksen tekemisen tarpeelliseksi palveluun siirtyessä?
     - Mitä siinä kannattaa mielestäsi huomioida?
   - Mitä keskeisiä asioita palvelutasosopimuksessa (SLA) kannattaa mielestäsi määritellä?
   - Mitä mieltä olet ulkopuolisesta konsultointiavusta pilvipalveluiden käyttöönoton yhteydestä?

- Pilvipalveluihin siirtyessä, koetko tarpeelliseksi käyttää talon omaa tai ulkopuolista asiantuntijaa, joka tarkistaisi eli auditoi tietoturvan ja tietosuojan vaatimusten toteuttamisen? Miksi?