HAAGA-HELIA
ammattikorkeakoulu

Tietosuoja pilvipalveluissa

Anne Hankosalo

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
7.5.2014

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

7.5.2014

Tietojenkäsittelyn koulutusohjelma

Tekijä tai tekijät Anne Hankosalo	**Ryhmätunnus tai aloitusvuosi** 2012
Raportin nimi Tietosuoja pilvipalveluissa	**Sivu- ja liitesivumäärä** 40 + 0
Opettajat tai ohjaajat Outi Valkki	

Pilvipalvelut ovat nousseet varteenotettavaksi vaihtoehdoksi tuottaa yrityksen tietoteknisiä ratkaisuja. Pilvipalveluissa yrityksen tieto luovutetaan ulkopuolisen käsiin, jolloin syntyy tarve miettiä yrityksen tietoturvaa ja tietosuojaa uudesta näkökulmasta. Tietosuojaan liittyy monia tuntemattomia kysymyksiä, joita tulisi pohtia ennen pilvipalveluun ulkoistamista.

Opinnäytetyössäni tarkastellaan niitä tietosuojaan liittyviä kysymyksiä, joita tulisi huomioida ulkoistuksissa pilvipalveluun. Tietosuojaa tarkastellaan oikeudellisesta ja teknisestä näkökulmasta. Oikeudellisen ja teknisen näkökulman kautta tuodaan esille ne seikat, joihin tietohallinnon tulisi keskittyä pilvipalveluun ulkoistuksessaan.

Aluksi opinnäytetyössä määritetään, mitä pilvipalveluilla tarkoitetaan. Tämän jälkeen käydään läpi niitä teknisiä kysymyksiä, joita vähintään tulee huomioida ja vaatia turvallisessa pilvipalvelussa. Seuraavaksi esitellään tietosuojan kannalta olennaisin lainsäädäntö ja kansainväliset sopimukset. Lopuksi tuodaan esille vähimmäisvaatimuksia, joita on hyvä huomioida pilvipalvelua hankittaessa, jotta yrityksen tietosuojan taso säilyy halutun tasoisena.

Opinnäytetyön tarkoituksena on tuottaa monipuolinen raportti, jota voidaan hyödyntää mietittäessä tietosuojan ongelmia ulkoistettaessa tietoteknisiä palveluja pilvipalveluun.

Asiasanat
pilvipalvelut, tietosuoja, auditointi, sopimukset, riskienhallinta

HAAGA-HELIA
University of Applied Sciences

Abstract

May 2014

Degree Programme in Business Information Technology

Authors Anne Hankosalo	**Group or year of entry** 2012
The title of thesis Privacy in Cloud Computing	**Number of pages and appendices** 40+0
Supervisor(s) Outi Valkki	

Cloud computing has become a viable alternative to manage company's IT services. In the cloud services companies' data is located outside of the organization's control, this creates a need to consider information security and data privacy from different perspective. Data privacy contains many unknown questions which should be thought before outsourcing business to cloud services.

My thesis examines those data privacy issues that need to be taken into account when making decision to outsource to cloud. Data privacy has been observed from legal and technical point of view. Combination of the technical and the legal perspective will introduce those facts which IT management should be focused regarding outsource.

At the beginning my thesis defines the meaning of cloud services. Secondly thesis goes through technical questions which are to be considered and demanded at least in safe cloud service. After that thesis introduces most relevant legislation and international agreements. Finally thesis brings out the minimum demand which maintains companies specified security level before data is outsourced to cloud computing services.

The purpose is to provide comprehensive report which can be exploited while considering the data privacy issues in the outsourcing IT services to cloud computing services.

Key words
cloud computing, data protection, audit, agreements, risk management

Sisällys

1 Johdanto 1

2 Pilvipalvelut 3

2.1 Pilvipalveluiden ominaisuudet 4

2.2 Pilvipalvelumallit 5

2.3 Käyttöönottomallit 7

3 Pilvipalveluiden tietoturvallisuus 9

3.1 Yleinen tietoturva 10

3.2 Tiedon saatavuus 12

3.3 Kolmas osapuoli 13

3.4 Tietoturvastandardit 15

4 Tietosuoja ja lainsäädäntö 17

4.1 Yksityisyyden suoja 17

4.2 Tietosuoja Suomen lainsäädännössä 18

4.3 Kansainväliset sopimukset 22

5 Tietosuojan huomioiminen ulkoistuksissa 25

5.1 Sopimustyypit 25

5.2 Palvelutasosopimus (SLA) 26

5.3 Auditointi 27

5.4 Riskinhallinta 29

6 Yhteenveto 31

6.1 Oma oppiminen 32

7 Lähteet 34

1 Johdanto

Aiheenani on pilvipalveluiden tietosuoja ja sen rooli pilvipalveluiden turvallisessa hankinnassa. Tarkoituksenani on selvittää, kuinka tietosuoja tulee huomioida ulkoistuksissa pilveen ja kuinka auditoinnin mahdollisuutta voidaan hyödyntää. Kiinnostavia asioita ovat pilvipalvelujen tekniset vaatimukset, tietosuojan määrittely sopimuksissa ja lainsäädännön tuomat vähimmäisvaatimukset.

Pilvipalvelu on uusi käsite, jonka suosiota ovat lisänneet mobiililaitteet, riippumattomuus, joustavuus ja kustannustehokkuus. Pilvipalvelut ovat nousseet vaihtoehdoksi tiedonhallintaan ja tietoteknisten palveluiden tuottamiseen. Keskustelu pilvipalveluiden tietosuojasta kulkee rinnakkainen yritysten ulkoistaessa it-palvelujaan pilvipalveluihin. Suurimmat yritykset toimivat pilvessä, mutta potentiaalia on vielä käyttämättä runsaasti. Sensitiivisen tiedon siirtämisessä pilvipalveluun ollaan edelleen varoivaisia.

Tietoturva ja tietosuoja ovat vaikeita kysymyksiä ja ne aiheuttavat epävarmuutta ulkoistuksiin, mutta edullinen hinta houkuttaa. Pilvipalvelussa tallennetun tiedon hallinta on siirtynyt palveluntarjoajalle, mistä syystä sen yksityisyyden käsitys poikkeaa perinteisestä yksityisyyden määritelmästä suljetussa konesaliympäristössä. Tietoturvaongelmat ovat kuitenkin pääasiassa samoja, mutta niiden vaikutukset huomattavasti suurempia ja laajempia.

Pilvipalvelujen tietosuojaa mietittäessä on huomioitava sen hajautettu luonne ja globaalius. Tietosuojan turvaamiseksi täytyy palvelua ajatella Suomen tai Suomen lainsäädännön näkökulmaa laajemmin. Hajautus aiheuttaa sen, että tieto voi liikkua hetkessä toisella puolelle maapalloa ja toisenlaisen lainsäädännön piiriin. Lainsäädännöllä pyritään rajaamaan tiedon vapaata liikuteltavuutta ja säätelemään riittävästä turvallisuuden tasosta. Lainsäädäntö muuttuu kuitenkin hitaasti ja sen valvonta on haastavaa.

Pilvipalvelujen käyttöönotossa tiedon säilyvyys tulee turvata siten, että se pysyy vain organisaation hallussa. Mahdolliset ongelmat tietosuojassa kohdistuvat yrityksen liiketoimintaan ja voivat aiheuttaa tappioita liiketoiminnalle. Ongelmat ovat globaaleja ja valtioiden rajat ylittäviä, eikä niihin ole olemassa yksiselitteisiä ratkaisuja. Ongelmallisin

tilanne syntyy silloin, kun pilvipalvelu myydään, eikä sitä suojaa EU:n sääntelemät tietosuojamääräykset.

Tietosuojaa voidaan turvata lainsäädännön ohella erilaisin sopimuksin ja siinä määritellä tietoturvan ja tietosuojan vaatimukset. Julkiset palveluntarjoajat tarjoavat samoja vakiopohjaisia sopimuksia asiakkailleen. Asiakkaan voi olla vaikea arvioida sopimuksen sisältöä ja sen riittävyyttä omiin tarkoituksiinsa. Palveluntarjoajat tarjoavat myös sopimuksia, joissa he siirtävät vastuun asiakkaalle. Asiakkaan näkökulmasta tämä ei ole hyvä vaihtoehto. Yksilöllisellä sopimuksella voidaan määritellä tarkemmin tietosuojan ja tietoturvan tasosta sekä mahdollisuudesta auditointiin.

Pilvipalveluja tarjoava taho määrittelee oman palvelunsa turvallisuuden, tiedon yksityisyyden ja tallennetun tiedon omistuksen. Asiakkaalla on rajalliset mahdollisuudet tarkastaa palvelun luotettavuutta ja tekninen toimivuus. Palvelun teknistä luotettavuutta voitaisiin palveluissa parantaa standardoinnilla ja auditoinnilla. Palvelun teknisestä toimivuudesta ja toiminnasta ei kuitenkaan täysin voi varmistua.

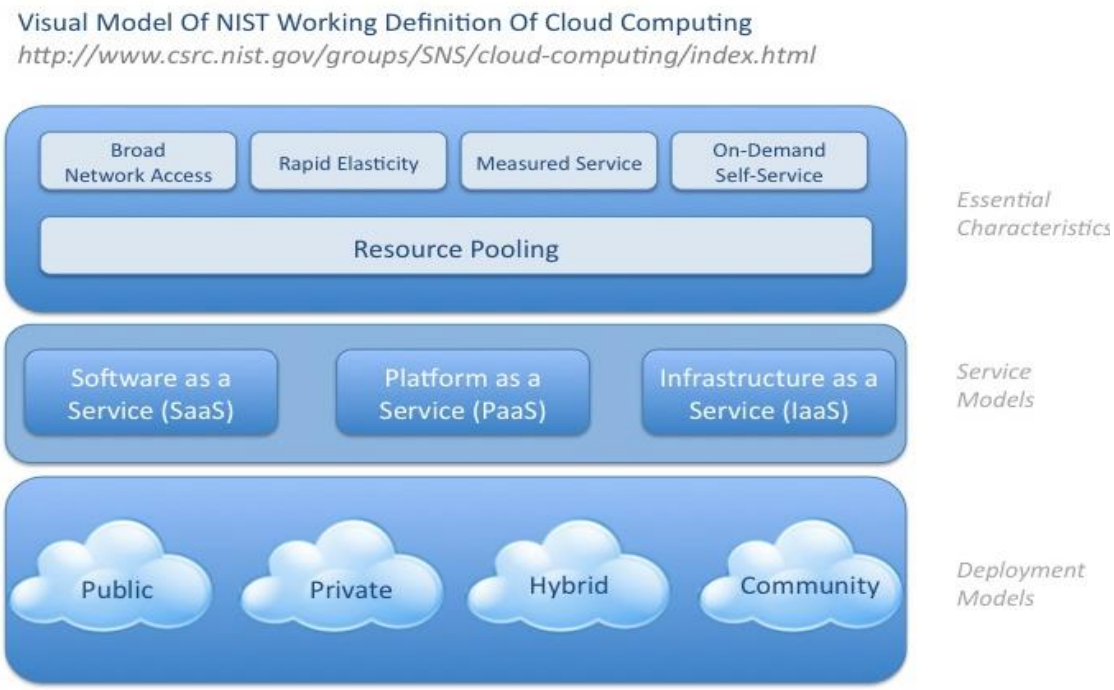
Opinnäytetyössäni esittelen pilvipalveluiden tietosuojaan liittyvää lainsäädäntöä, pilvipalveluiden tietoturvahaasteita ja kuinka näistä voi varmistua. Lainsäädäntöä käsitellään Suomessa toimivien pilvipalveluiden ja eri pilvityyppejä erottelematta. Näkökulmana ovat käytetty yksityistä organisaatiota ja julkisen sektorin sekä salassa pidettävien tai arkaluonteisten tietojen käsittelyn erityispiirteet on jätetty huomioimatta.

2 Pilvipalvelut

Pilvipalvelulla tarkoitetaan kaikkia niitä kaupallisia toimijoita, jotka tarjoavat palvelujaan ja kapasiteettia verkon yli paikasta riippumatta. (Voorsluys, Broberg, & Buyya 2011, 3-4.) Pilvipalvelu on koko se kokonaisuus, jossa palvelut toimivat ja joka koostuu laitteistosta, tietoverkosta, tietovarastosta, palvelusta ja käyttöliittymästä. Yhteistä eri määritelmillä pilvipalveluista on, että sen laskutus tapahtuu käytön mukaan, palvelu on skaalautuva, käyttöliittymä toimii itsepalveluna ja resurssit ovat hajautetut ja virtualisoitu (Voorsluys, Broberg & Buyya 2011, 4). Pilvipalveluiden tuomia hyötyjä verrattuna perinteisiin konesalipalveluihin ovat skaalautuvuus, käytettävyys ja kustannustehokkuus. (Bauer & Randee 2012, 14-15.)

Pilvipalveluilla ei ole olemassa yhtä hyväksyttyä määritelmää, mutta yksi käytetyin ja tunnetuin on NIST:n määritelmä (Salo 2010, 16). NIST (US National Institute of Standards and Technology) on kuvannut pilvipalvelut ja pitäydyn pilvipalveluiden luokittelussa NIST:n määritelmässä, joka on esitetty kuviossa 1. NIST:n mukaan pilvipalveluita on olemassa erityyppisiä, kuten SaaS (Software as a Service, sovelluksia palveluna), PaaS (Platform as a Service, sovellusalusta palveluna) ja IaaS (Infrastructure as a Service, infrastruktuuri palveluna). Pilvipalvelut luokitellaan lisäksi yksityisiin, julkisiin, yhteisöllisiin ja hybridimallin pilviin. (Mell ja Grance, 2011).

Pilvipalvelun ontologian mukaan palvelu kuuluu johonkin viidestä kerroksesta, joita ovat: sovellukset, sovellusympäristöt, sovellusarkkitehtuuri, sovellusydin ja laitteisto. Pilvipalveluiden ontologian ymmärtäminen auttaa hahmottamaan eri pilvikomponenttien välisiä suhteita ja erottamaan eri pilvityypit toisistaan. Samalla ymmärtää paremmin pilven ominaisuudet, kuten laajennettavuuden, joustavuuden, saatavuuden, optimoinnin ja kustannustehokkuuden. Ontologioita ymmärtämällä pilvestä saa enemmän irti. (Youseffin, Butricon ja Da Silvan, 2008).



Kuvio 1. NIST:n pilvipalveluiden määritelmä (National Institute of Standards and Technology 2012).

2.1 Pilvipalveluiden ominaisuudet

NIST:n määritelmän mukaan pilvipalvelulla on viisi erilaista ominaisuutta (Essential Characteristics), joiden avulla voidaan määritellä pilvipalveluihin kuuluvia palveluita. Näitä ominaisuuksia ovat On-demand itsepalvelu, avoin verkkoon pääsy, resurssien yhteiskäyttö, nopea joustavuus ja käytön tarkka mittaaminen. (Mell ja Grance, 2011).

On-demand itsepalvelulla (On-demand self-service) tarkoitetaan sellaista automaattista tietoteknistä palvelua, jossa asiakas voi ostaa käyttöönsä palvelin aikaa ja tallennus kapasiteettia tarpeen mukaan. Palvelu tulee saada käyttöön automaattisesti ilman vuorovaikutteista ihmiskontaktia. (Mell ja Grance, 2011).

Avoin verkkoon pääsy (Broad network access) pilvipalvelussa tarkoittaa sitä, että palvelu on saavutettavissa internetin välityksellä standardoiduilla menetelmillä ja päätelaite riippumattomasti. Palvelun tulee olla saavutettavissa riippumatta siitä, mitä päätelaitetta

ja käyttöjärjestelmää asiakas käyttää, kunhan hänellä on käytössään toimiva internet yhteys. (Mell ja Grance, 2011)

Resurssien yhteiskäytöllä (Resource pooling) pilvipalvelu jakaa tarjoamansa resurssit asiakkailleen heidän tarpeensa mukaan. Yhteiskäyttö resursseilla tarkoitetaan levytilaa, laskentatehoa, muistia ja verkon kaistanleveyttä. Resursseilla voi olla erilaiset fyysiset ja virtuaaliset sijainnit, jotka vaihtuvat dynaamisesti asiakkaan tarpeiden mukaan. Pilvipalvelun resurssit ovat riippumattomia sijainnista eikä asiakas voi vaikuttaa tarkkaan resurssin sijaintin. Poikkeuksena ovat korkeamman tason palvelut, joista asiakas voi saada tietoonsa maan, alueen tai palvelinkeskuksen. (Mell ja Grance, 2011).

Nopea joustavuus (Rapid elasticity) palvelussa näyttäytyy asiakkaalle rajattomana resurssina, joka on käytettävissä ajasta riippumattomasti ja riittävän suurena. Nopea joustavuus saavutetaan vastaamalla kysyntään vapauttamalla ja käyttöön ottamalla resursseja joustavasti, myös automaattisesti. (Mell ja Grance, 2011).

Käytön tarkalla mittaamisella (Measured service) pilvipalveluissa voidaan seurata, valvoa ja raportoida resurssien käyttöä. Mitattavia resursseja ovat kaistanleveys, aktiiviset käyttäjätilit ja tallennukset. Mittaustuloksia hyödyntämällä pilvipalvelut kontrolloivat ja optimoivat palvelunsa käyttöä automaattisesti. Palveluntarjoajan lisäksi mittaustulokset ovat myös asiakkaan käytettävissä ja niiden tarkoituksen on lisätä palvelun läpinäkyvyyttä. (Mell ja Grance, 2011).

2.2 Pilvipalvelumallit

Pilvipalveluiden ominaispiiteiden lisäksi NIST on määritellyt pilvipalvelumallit (Service Models). Näitä ovat SaaS, PaaS ja IaaS (Mell ja Grance 2011, 2-3).

Sovelluksia palveluna (SaaS, Software as a Service) palvelussa asiakkaalla on päätelaitteen internetyhteyden kautta käytettävissä jokin pilvipalvelu. Pilvipalvelu tarjoaa koko palvelun ja asiakkaalla on käytössään koko palvelun tarjoaman infrastruktuuri. Tarjottavia yhteiskäyttöisiä resursseja voivat olla sovellusten lisäksi palvelinkapasiteetti, käyttöjärjestelmät ja tietokannat. Pilvipalvelun tarjoaja vastaa koko palvelun ylläpidosta ja

asiakas maksaa vain palvelun käytöstä. (Mell ja Grance 2011, 2). SaaS-palvelut ovat suosituin pilvipalvelumalli ja omaa heikoimman tietosuojan. Ontologian mukaan SaaS-palvelut toimivat sovelluskerroksella ja ovat näkyvin palvelu käyttäjille (Youseff, Butrico ja Da Silva 2008, 3).

Sovellusalusta palveluna (PaaS, Platform as a Service) mallissa asiakas ostaa käyttöönsä pilvipalvelulta alustan, jonka avulla hän voi ylläpitää omia sovelluksiaan. Pilvipalvelu hallitsee tarjoamansa infrastruktuurin eikä asiakas osallistu sen hallintaan. Asiakas hallitsee kuitenkin omia sovelluksiaan ja mahdollisesti hänellä on mahdollisuus hallinnoida hosting-palvelun kokoonpanoasetuksia. (Mell ja Grance 2011, 2-3). PaaS-palvelussa asiakas on riippuvainen palveluntarjoajasta, mikä heikentää sovellusten tietosuojaa. Palvelun hallinta vaatii teknistä osaamista myös asiakkaalta. Paas-palvelut toimivat sovellusympäristöt -kerroksella, jota käyttävät pääasiassa sovelluskehittäjät API-rajapintojen kautta. (Youseff, Butrico ja Da Silva 4, 2008).

Infrastruktuuri palveluna (IaaS, Infrastructure as a Service) mallissa asiakas ostaa käyttöönsä palveluntarjoajan infrastruktuurin resurssit käyttöönsä. Palvelun tarjoamassa suoritusympäristössä asiakas voi pyörittää sovellusten lisäksi käyttöjärjestelmää tai virtuaalikonetta. Tarjottavat palvelu on virtualisoituja ja skaalautuvia käytetyn tarpeen mukaan. Palveluntarjoajan tarjoaa asiakkaan käyttöön suoritusympäristön, mutta hallinnoi tarjoamaansa infrastruktuuria. (Mell ja Grance 2011, 2-3). IaaS-palvelussa asiakkaalle on myös riippuvuussuhde palveluntarjoajaa, mikä heikentää tietosuojaa. Palvelun hallinta vaatii teknistä osaamista myös asiakkaalta. IaaS-palvelut toimivat sovellusarkkitehtuurikerroksella, joka tarjoavat laskentaresursseja, tiedon tallennusta ja viestintää (Youseffin, Butricon ja Da Silvan 2008, 5). IaaS-palveluihin voidaan lukea myös laitteistokerroksella toimivat HaaS-palvelut (Bauer, A. ja Adams, R. 2012, 10). Niiden asiakkaat ovat pääasiassa suuria yrityksiä, jotka tarvitsevat vuokrattavia laitteistoja. Lisäksi pilveen kuuluu ohjelmistoydin-kerros, joka tarjoaa pilvipalveluja tarjoaville palvelimille ohjelmistopalveluja. (Youseff, Butrico ja Da Silva 2008, 5).

2.3 Käyttöönottomallit

NIST määrittelee lisäksi neljä eri käyttöönottomallia pilvipalveluille (Deployment Models). Näitä ovat yksityinen pilvipalvelu, julkinen pilvipalvelu, yhteisöllinen pilvipalvelu ja hybridi pilvipalvelu (Mell ja Grance 2011, 3). Käyttöönottomallien luokitus tapahtuu niiden omistajuuden mukaan ja, kuinka paljon vastuuta on pilvipalveluntarjoajalla.

Yksityisessä pilvipalvelussa (Private cloud) kaikki resurssit ovat yrityksen yksinomaisessa käytössä. Palvelu voi olla yrityksen omassa hallinnassa ja omistuksessa tai vuokrattu ja kolmannen osapuolen hallinnoima. Se voi myös sijaita yrityksen omissa tiloissa tai ulkoistettuna kolmannelle osapuolelle. (Mell ja Grance 2011, 3). Tietosuojan kannalta tämä on kaikkein turvallisen ratkaisu, mutta ei välttämättä tuo kaikkein suurinta kustannussäästöä, jota pilvipalvelulla usein tavoitellaan.

Julkinen pilvi (Public cloud) lienee kaikkein tunnetuin pilven käyttömalli, koska se on kaikkien saavutettavissa vapaasti. Julkinen pilvipalvelu sijaitsee aina palveluntarjoajan tiloissa. Julkisen pilven omistajuus on palveluntarjoajalla ja palveluntarjoajana voi olla periaatteessa kuka tahansa. (Mell ja Grance 2011, 3). Tietosuojan näkökulmasta julkinen pilven tietosuoja on kaikkein arvaamattomin, koska se on vain palveluntarjoajan tiedossa ja hallinnassa.

Yhteisöllinen pilvi (Community cloud) on usean eri organisaation yksinomaisessa ja jossakin erityisessä käytössä, joka voi liittyä turvallisuuteen, politiikkaan tai yhteiseen päämäärään. Sen omistajuus ja hallinta voi olla joko kaikilla organisaatioilla, vain yhdellä näistä, kolmannella osapuolella tai jollakin näiden yhdistelmistä. (Mell ja Grance 2011, 3). Tietosuojan kannalta tämä on suhteellisen hyvä vaihtoehto, koska pilvi on vain sen tietyn yhteisön käytössä. Kustannukset ja turvallisuus riippuvat yhteisön koosta.

Hybridipilvi (Hybrid cloud) on nimensä mukaisesti yhdistelmä kahdesta tai useammasta edellisistä palvelumalleista. Hybridipilvessä jokainen palvelumalli säilyy kuitenkin itsenäisenä kokonaisuutena, mutta helposti toisiin yhdistettävänä. Yhdistämisessä käytetään standardoitua ja patentoitua tekniikka, joka mahdollistaa tiedon ja sovellusten su-

juvan siirrettävyyden ja käyttöönoton. (Mell ja Grance 2011, 3). Hybridipilven tietosuojan taso riippuu käytetystä tekniikasta ja omistajuudesta.

3 Pilvipalveluiden tietoturvallisuus

Pilvipalveluiden tekninen turvallisuus on avainasemassa tietojen suojaamisessa ja yksityisyyden turvaamisessa. Tietoturvallisuutta käsitellään tässä ensisijaisesti tietosuojan näkökulmasta. Tietosuoja ja tietoturva eivät ole käsitteinä toistensa synonyymejä ja ne on syytä pitää erillään. Tietosuojalla suojataan palvelun käyttäjää, kun taas tietoturvalla suojataan palveluun tallennettua itse tietoa. (Järvinen 2010, 15).

Yleisesti tietoturvan osa-alueiksi määritellään kolme osa-aluetta, joita ovat luottamus, käytettävyys ja tiedon eheys. Klassista tietoturvan määritelmä riittämätön, koska se ei huomioi tiedon tuottajan ja omistajan identiteettiä. Kuviossa 2 kuvatussa laajennetussa määritelmässä on viisi osa-aluetta: luottamus, käytettävyys, eheys, kiistämättömyys ja pääsynvalvonta. (Hakala, Vainio ja Vuorinen 2006, 4-5). Laajennettu tietotuvan määritelmä pätee myös pilvipalveluissa, mutta osa-alueet painottuvat hieman toisin.

Kuvio 2. Tietoturvallisuuden osatekijät (Hakala, Vainio ja Vuorinen 2006, 6)

Pilvipalveluiden teknistä turvallisuutta on määritelty monella tavalla, mutta mitään niistä ei ole toistaiseksi standardoitu. CSA eli Cloud Security Alliance on määritellyt pilvipalveluiden turvallisuutta ja yksityisyyttä 14 kohdan mukaisesti (Cloud Security Alliance 2011). Tutkimuslaitos Forresterin luokituksen mukaan pilvipalveluiden turvallisuuden osa-alueita ovat turvallisuus ja yksityisyys, asetuksien ja standardien mukaisuus sekä lakeihin ja sopimuksiin liittyvät seikat (Wang, Penn ja Viglianti 2009).

Pilviteknologioissa tietoturvakysymykset voidaan jakaa kolmeen eri kategoriaan: yleiseen turvallisuuteen, saatavuuteen ja palveluntarjoajaan. Käsittelen tietosuojaan liittyviä tietoturvahaasteita näiden kolmen kategorian mukaisesti, jotka ovat suurimpia tietoturvan huolenaiheita pilvipalveluiden asiakkailla. Tämä jaottelu korreloi suoraan klassista tietoturvamääritelmää, mutta painottuu toisin. Tietoturvaongelmat ovat pilvipalveluissa samat kuin ennenkin, mutta ne esiintyvät hieman erilaisessa muodossa (Chow, Golle, Jakobsson, Shi, Staddon, Masuoka ja Molina, 2009, 85-90). Tietoturvamääritelmän lisäksi esitellään yleisimpiä pilvipalveluissa käytettyjä tietoturvastandardeja.

3.1 Yleinen tietoturva

Yleisen tietoturvan tavoitteena on varmistaa, että asiakkaan tallentama tieto säilyy sellaisenaan ilman, että ulkopuolinen taho pääsee sitä muuttamaan tai tuhoamaan. Yleisen tietoturvan kategoriaan pilvipalveluissa määritellään kuuluvaksi tiedon eheys ja oikeellisuuden turvaaminen sekä palvelun suojaaminen ulkopuolisilta tunkeutujilta ja hyökkäyksiltä. (Chow, Golle, Jakobsson, Shi, Staddon, Masuoka ja Molina, 2009, 85-90).

Tiedon eheys tarkoittaa sitä, että tieto pysyy koskemattoman, muuttumattomana, eikä sisällä virheitä. Tiedon koskemattomuus on pilvipalvelun tietosuojan kannalta olennainen asia. Tallentaessaan tietonsa palveluun asiakas luottaa siihen, että hänen tallennuksensa säilyvät koskemattomina. Ulkopuoliset eivät saa päästä tarkkailemaan tietoa palvelun sisällä, eikä sen ulkopuolelta. Siihen liittyy tiedon turvallinen tallentaminen ja tietoliikenteen suojaaminen. (Petkoviç ja Jonker 2007, 95-96).

Palvelin on avainasemassa tiedon eheyden turvaamisessa ja samalla tietosuojan säilymisessä. Palvelimen tai palvelimien tulee toimia luotettavasti ja turvallisesti suoritettaessa tietokanta kyselyitä, mutta se ei kuitenkaan saa nähdä tiedon sisältöä. Tallennettu tieto tulee olla yksiselitteisesti eroteltu muiden asiakkaiden materiaalista ja rajapinnat palveluun määritelty huolella. (Samarati ja De Capitani di Vimercati 2010).

Tiedon on säilyttävä eheänä palvelimelta tehtävien tietokantakyselyjen ja transaktioiden aikana, mutta myös suorituksen loputtuakin. Järjestelmään tunkeutujat pyrkivät hyödyntämään tietokantakyselyiden haavoittuvuuksia SQL-injektion avulla toteutetuissa tunkeutumisessa. (Petkoviç ja Jonker 2007, 97). Tietotulvan aikaansaamana pilvipalvelut ovat nousseet merkittäväksi tietovarastoksi, mistä johtuen tietokannat ja niistä tehtävät kyselyt ovat kokeneet oman murroksensa siirryttäessä big dataan (Lu, Guo, Xu, Zhao, Peng ja Yang 2013, 1066).

Pilvipalveluihin kohdistuu laaja joukko erilaisia hyökkäyksiä ja tiedon kalastelua. Pilvipalveluiden haavoittuvuudet eivät poikkea juurikaan perinteisistä haavoittuvuuksista. Pilvipalvelun tietovuodolla on vain huomattavasti laajempi merkitys, kuin perinteisen it-frastruktuurin vuodolla. (Chow, Golle, Jakobsson, Shi, Staddon, Masuoka ja Molina, 2009, 85-90). ISO 27005 määrittelee haavoittuvuuden heikkoudeksi, jota ulkopuolinen osapuoli käyttää vahingoittaakseen organisaatiota. Erityisesti pilveen kohdistuviksi haavoittuvuuksia voidaan lukea sellaiset haavoittuvuudet, jotka johtuvat pilviteknologista. (Grobauer, Walloschek ja StöckerStöcker 2011, 50).

Pilvihaavoittuvuudet voidaan jaotella neljään eri kategoriaan. Pilvihaavoittuvuuksiksi luetaan sellaiset haavoittuvuudet, jotka pohjautuvat pilviteknologian ytimeen, kuten virtuaalikoneen haavoittuvuudet, kaappaukset ja vanhentunut tai heikko salaus. Toiseksi ne voivat perustua johonkin NIST:n määrittelemistä pilvityypeistä, kuten pääsynhallintaan tunkeutuminen, internet protokollaan kohdistuvat heikkoudet, heikkoudet tietojen palautuksessa tai palvelun mittaamisen ja laskutuksen heikkoudet. Kolmanneksi haavoittuvuuksia ovat pilven pääsynhallinnan heikkoudet silloin, kun ne erityisesti johtuvat pilviteknologiasta. Ja viimeiseksi uusimman teknologian tietoturva-aukkoja hyödyntävät hyökkäykset ja heikot käyttäjän todennukset. (Grobauer, Walloschek ja StöckerStöcker 2011, 52-54). Tietojen kalastelua on noussut yhdeksi yleisimmäksi haavoittuvuudeksi etenkin pankkijärjestelmissä, mutta samalla myös muissa verkkopalveluissakin (Andersson 2008, 60).

Pilvipalveluiden yleiseen turvallisuuteen liittyy myös pääsynhallinta. Sillä pyritään varmistamaan, että tiedon käyttäjällä on siihen yksiselitteinen oikeus ja toisaalta tallennet-

tava tieto on luotettavaa ja sallittua. Pääsynhallinnalla estetään ulkopuolisten pääsy tietoihin ja pyritään turvaamaan tallennetun tiedon säilyminen palvelussa muuttumattomana. (Goodrich ja Tamassia 2011, 4-5).

Tiedon luottamuksellisuuden turvaamiseksi on olemassa erilaisia salausmenetelmiä, joiden turvallisuudesta on esitetty kriittisiäkin näkemyksiä. Pilvipalveluissa toteutetaan todennus ja valtuutus usein Public Key -infrastruktuurin ja X.509 SSL -sertifikaatin avulla (Youseff, Butrico ja Da Silva 2008, 1-10). Kriittinen virhe pilvipalvelun tietoturvassa voi olla liiallinen luottamisen salausmenetelmiin ja vanhentuneiden ohjelmistojen käyttäminen. Uudet salausmenetelmät puretaan melko nopeasti, eivätkä ne enää tulevaisuudessa välttämättä takaa riittävää tietoturvaa. (Parakh ja Kak 1999, 3323–3331.)

3.2 Tiedon saatavuus

Pilvipalveluiden etuna on hyvä saavutettavuus ja se on tärkeä osa-alue ylläpitää eriomaisena. Pilvipalvelut ovat hajautettuja järjestelmiä, jolloin tallennettu tieto on hajautettuna useille eri palvelimille ja mahdollisesti useille eri mantereilla. Hajauttamalla tallennettu tieto aikaan saadaan hyvä saatavuus ja virheensietokyky, eikä yhden palvelimen rikkoutuminen lamauta koko palvelua. Tiedon saatavuus eli käytettävyys turvaa sen, että pilvipalvelun asiakkaan tallentama tieto on hänen käytössään aina tarvittaessa (Paananen 2005, 388).

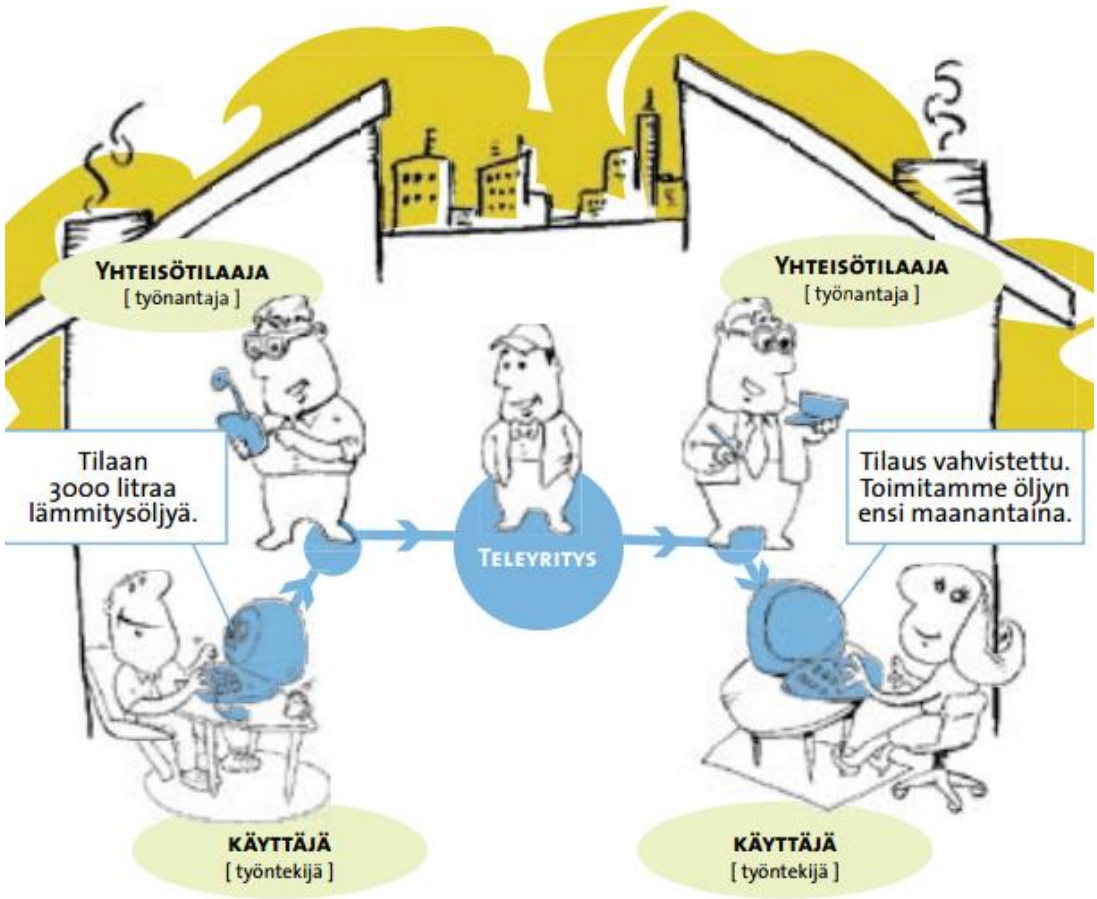
Tiedon saatavuuden turvaamiksi pilvipalvelun tulee rakentaa infrastruktuurinsa skaalautuvaksi. Palvelun toimivuus ja saatavuus eivät saa kärsiä tietoliikenne- tai sähkökatkosta tai palvelimen rikkoontumisesta. Pilvipalveluun täytyy pystyä tekemään muutoksia katkaisematta koko palvelua tai ainakin hyvin vähäisillä katkoilla. Asiakkaan tiedon säilyvyys on turvattava niissäkin tilanteissa, joissa palveluun tulee katkoja. Hyvin toimivalla pilvipalvelulla tulee olla riittävä kapasiteetti, että se kestää suuremmatkin palvelunestohyökkäykset ja pystyy turvamaan asiakkaan tietosuojan sekä sujuvan ja turvallisen tietoliikenteen palveluun. (Goodrich ja Tamassia 2011, 8-9)

Tiedon saatavuuteen liittyy myös kysymykset palvelun elinkaaresta ja tiedon säilymisestä palveluntarjoajan lopettaessa toimintansa. Tiedon tulee olla myös sellaisessa muodossa, että asiakas voi sen ongelmitta siirtää toiselle palveluntarjoajalle. Tiedon saatavuuden pysyvyydestä voidaan määritellä sopimuksin ja siihen asetetuin sanktioin. (Youseff, Butrico ja Da Silva 2008, 1-10).

3.3 Kolmas osapuoli

Otettaessa käyttöön pilvipalvelua asiakas siirtää tietonsa ulkopuoliselle taholla ja luovuttaa tietojen hallinnan oman kontrollinsa ulottumattomiin. Läpinäkyvyyden puute ja kontrollinen menetys aiheuttavat tietoturvaongelmia ja epävarmuutta. Palvelun huolellinen suunnittelu on tae tietoturvalliselle palvelulle ja sen skaalautuvuudelle. (Chow, Golle, Jakobsson, Shi, Staddon, Masuoka ja Molina, 2009, 86).

Kolmannella osapuolella tarkoitetaan pilvipalveluissa pilvipalvelun tarjoajaa. Kaksi muuta osapuolta ovat pilvipalvelun asiakas, joka tarjoaa pilviohjelmistoja ja loppukäyttäjä. (Sakr ja Liu 2012, 360-362). Kolmatta osapuolta voi hahmottaa rooliajattelun mukaisesti, mikä auttaa hahmottamaan toimijan lainsäädännöllisiä velvoitteita. Lainsäädännössä määriteltyjä rooleja ovat viestinnän osapuoli, yhteisötilaaja, teleyritys, lisäarvopalvelun tarjoaja ja tietoyhteiskunnan palvelujen tarjoaja. Alihankinnan roolia ei ole erikseen lainsäädännössä määritetty. Roolit eivät ole staattisia ja toimijalla voi olla kaksoisroolikin. (Innanen ja Saarimäki 2012, 48-49). Kuviossa 3 on esitetty roolien suhteet toisiinsa. Teleyritys on vastaa pilvipalvelun tarjoajaa, yhteisötilaaja pilvipalvelun asiakasta ja käyttäjä loppukäyttäjää.



Kuvio 3. Pilvipalveluiden roolit. (Liikenne- ja viestintäministeri, Tietosuojavaltuutetun toimisto ja Viestintävirasto, 4).

Suomen lainsäädännöllä voidaan velvoittaa vain Viestintäviraston vaikutuspiirissä tietyssä roolissa olevia palveluntarjoajia. Useassa eri laissa ja säännöksissä asetetaan velvoitteita eri toimijoiden toiminnasta ja tietoturvasta. Ensiarvoisen tärkeää on hahmottaa toimijan rooli velvoitteiden tunnistamiseksi. (Innanen ja Saarimäki 2012, 47-48). Tiedon hallintaan liittyvistä kysymyksistä määritellään lain hengessä toimivien pilvipalveluiden sopimusehdoissa.

Kolmannen osapuolen läpinäkyvyyden puute aiheuttaa epävarmuutta tallennettuja tietojen käsittelystä. Asiakas olettaa tietonsa luovuttaessaan, että hänen tallentamansa tieto säilyy muuttumattomana ja maantieteellisesti sovitussa sijainnissa. Läpinäkyvyyden ongelmana ovat varmuuden saaminen tallennetun tiedon luotettavasta käsittelystä ja hei-

kot mahdollisuudet varmistua tietojen tallennuksesta. Asiakkaalla on mahdollisuudet päästä tarkastamaan tallentamiaan tietoja vain dokumentaatiosta ja manuaaliselle auditoinnilla. (Chow, Golle, Jakobsson, Shi, Staddon, Masuoka ja Molina, 2009, 87). Tietoturvahaasteeksi voi muodostua myös lukkiutuminen palveluntarjoajaan. Pilviympäristöt ovat standardoimattomia, mistä johtuen palveluntarjoajan vaihto ei aina onnistu, koska toimintaympäristöt eivät ole yhteensopivia. Tähän ongelmaan auttaisi palveluiden standardointi (Salo 2010, 110-114).

Kolmannen osapuolen läpinäkyvyyden puutteeseen vaikuttaa myös alihankinta, koska alihankintaketjut voivat olla pitkiä. Toimittajien rooleja ja vastuita voi asiakkaan olla vaikea tunnistaa. (Chow, Golle, Jakobsson, Shi, Staddon, Masuoka ja Molina, 2009, 88). Suomen lainsäädännön piirissä alihankinta ei kuitenkaan vaikuta teleyrityksen, eikä yhteisötilaajan vastuisiin ja velvollisuuksiin. Teleyrityksellä säilyy vastuu palvelun tietoturvasta ja yhteisötilaajalla käyttäjätietojen tietoturvasta. (Innanen ja Saarimäki 2012, 62).

3.4 Tietoturvastandardit

Tietoturvastandardeilla voidaan määritellä palvelun turvallisuutta, laatua ja teknisiä standardeja. Standardit tuovat luotettavuutta palveluille ja niillä taataan asiakkaalle tietty turvallisuuden taso palvelussa. Tietoturvastandardeja on olemassa paljon, mutta varsinaisesti pilvipalveluiden turvallisuuteen ja toimintaan kohdistuvia yleisiä standardeja ei vielä ole. Pilvipalveluissa on kuitenkin käytössä eri osa-alueilla erilaisia standardeja, vaikka ne eivät ole suoraan suunnattu pilvipalveluille. (Chemerkin 2013, 55-60). Tässä esitellään yleisimpiä pilvipalveluissa käytettäviä standardeja.

Cloud Security Alliancen eli CSA:n tavoitteena on määritellä standardi pilvipalveluihin ja opastaa palveluita turvallisemman pilvipalvelun pariin. CSA on tuottanut Security Guidance for Critical Areas of Focus in Cloud Computing -oppaan, jossa käsitellään laajasti pilvipalveluiden tietoturvaa. Oppaassa käsitellään pilvipalveluiden tietoturvaa tiedon ja tiedon prosessoinnin näkökulmasta. Siinä on yhteensä 14 eri kohtaa pilvipalveluiden turvaamiseksi. Oppaan tavoitteena on minimoida tietoturvariskit, jotka syntyvät tietoa liikuteltaessa ja käsiteltäessä pilvipalvelussa. (Cloud Security Alliance 2011, .)

Maksukorttialan tietoturvastandardi (PCI Data Security Standard PCI DSS**)** on yksi pilvipalveluissa käytettävistä standardeista. PCI DSS on käytössä maksukorttimaksuissa ja sillä määritellään maksukortin käyttäjien tietoturvaa maailmanlaajuisesti. Standardin avulla pyritään saavuttamaan yhtenäinen tietoturvakäytäntö kaikkien standardia käyttävien maksukorttiyhtiöiden kesken. Standardi asettaa minimivaatimukset palveluntarjoajan teknisille ja operatiivisille vaatimuksille, ja sen avulla pystytään turvaaman kortin haltioiden turvallinen maksaminen verkkopalveluissa. (PCI Security Standards Council, 2013)

ISO 2700 -standardisarja on toinen pilvipalveluissa käytettävistä merkittävistä standardeista. Standardisarja on kehitetty parantamaan yritysten kykyä hallita tietoturvallisuutta, sen riskejä ja valvontaa (Evans, Tsohou, Tryfonas ja Morgan 2010, 1-6.). Sarjassa on 7 julkaistua standardia ja kaksi kehitteillä olevaa. Sen suosituimpia standardeja ovat ISO 27001 ja ISO 27002 – standardit. ISO 27001 sisältää tietosuojan hallintajärjestelmien sertifioinnin ja se määrittää tietoturvan teknisen turvallisuuden vaatimukset, kuten dokumentoinnin, implementoinnin, käytön, monitoroinnin, arvioimisen, ylläpidon ja kehittämisen vaatimukset. ISO 27002 vastaavasti asettaa vaatimukset yleisiä ohjeita tietoturvallisuuden hallintaan. (Evans, Tsohou, Tryfonas ja Morgan 2010, 1-6.)

Yhdysvalloilla on käytössään useita omia valvontajärjestelmiään ja asetuksiaan, jotka vaikuttavat julkisten pilvipalveluiden toimintaan. Yksi Yhdysvaltojen oma säännös on **SOX**, eli Sarbanes-Oxley Act. Sillä määritellään kaikkien pörssiin listautuneiden yritysten toimintaa. Pörssiin listautuneiden pilvipalveluille se merkitsee esimerkiksi tiettyä tasoa läpinäkyvyydessä ja vastuullisuutta toiminnassa. SOX-vaatimukset on kuvattu erikseen SAS70-standardissa. (Goorich ja Tamassia 2011, 459.)

SAS70-standardi (Statement on Auditing Standards (SAS) No. 70) on American Institute of Certified Public Accountantsin (AICPA) auditointistandardi ja se on tarkoitettu palveluorganisaatioille. Standardi määrittelee vaatimukset tietosuojan auditoinnille eli riippumattoman ulkopuolisen tarkastukselle. Auditoinnissa tarkastetaan palvelun suojausmenetelmien vaatimustenmukaisuus ja niiden tehokkuus. Standardi tuo turvaa sitä käyttävien palveluiden tietosuojaan. (Aicpa 2014.)

4 Tietosuoja ja lainsäädäntö

Lainsäädäntö luo pohjan pilvipalveluiden tietosuojalle ja yksityisyyden turvaamiselle. Suomessa tietosuojalainsäädäntö syntyi automaattisen tietojenkäsittelyn myötä ja pohjautuu Euroopan unionin tietosuojasäädöksiin. Lain synnyn taustalla oli pelko yksityisyyden häviämisestä ja sen tarkoituksena oli suojata yksityisyyden suojan lisäksi oikeusturvaa ja demokraattisuutta. (Wallin ja Nurmi 1990, 1). Suomen lainsäädännöissä pilvipalveluihin sovellettava laki sisältyy useisiin eri lakeihin, joita sovelletaan tilanteen mukaan (OM, 1989). Pilvipalveluiden kohdalla lainsäädäntö on monitulkintainen ja haastava osittain siksi, että kokonaiskuvaa on vaikea hahmottaa ja se on laajalle hajautettu (Innanen ja Saarimäki 2012, 1). Lain soveltamisalaa ovat yleiset viestintäverkot, joilla tarkoitetaan palveluja, joiden käyttäjäkuntaa ei ole ennalta rajattu (Helopuro, Perttula ja Ristola 2009, 1).

Laintulkinnan kannalta pilvipalveluita on kolmenlaisia: kokonaan Suomessa ylläpidettävät palvelut, osittain Suomessa ylläpidettävät palvelut ja kokonaan ulkomaiset palvelut (Saarimäki 2013). Tässä työssä keskitytään tarkastelemaan Suomessa toimivia pilvipalveluita ja niihin sovellettavaa lainsäädäntöä ja kansainvälisiä sopimuksia. Pilvipalveluihin liittyvä lainsäädäntö on muutosvaiheessa ja Euroopan komissio valmistelee tietosuojalainsäädännön uudistamista (Innanen ja Saarimäki 2012, XVII). Uudistuksen tavoitteena on luoda yhtenäinen ja kattava lainsäädäntö Euroopan Unionille, joka parantaa online-palveluiden tietoturvaa. (Oikeusministeriö, 2014)

4.1 Yksityisyyden suoja

Tietosuoja on yksityisyyden turvaamista henkilötietojen käsittelyssä lainsäädännön keinoin. Tietosuojaa määritellään etenkin henkilötietolailla, mutta yksityisyyden suojaa ei ole kuitenkaan määritelty tarkasti lainsäädännössä. Tietosuojaa turvataan tietoturvalla, jonka tarkoituksena on suojata yksityisyyttä ja oikeusturvaa. (Mäenpää 2008, 34). Lainsäädäntö asettaa vähimmäisvaatimukset, mutta yksityisyys koetaan usein laajemmaksi asiaksi kuin, mitä lainsäädäntö määrittää.

Monelta osin yksityisyyden suojassa on kyseessä moraalisesta kysymyksestä, jota lainsäädäntö omalta osaltaan sääntelee. (Nyyssölä 2001, 16-17). Suomen lainsäädännössä yksityisyyden suojaa määrittävät EU:n perusoikeuskirjan 7 artikla, Euroopan Ihmisoikeussopimuksen 8 artikla ja Perustuslain 10§:n mukaisesti sekä kansainvälisten sopimusten pohjalta. Suomen kansalaisella yksityisyyden suoja on perusoikeus, joka muodostuu ihmisen syntyessä samalla kuin oikeuskelpoisuuskin. (Ojanen 2009, 21).

Seuraavaksi esitellään pääpiirteet Suomessa käytettävästä lainsäädännöstä, sekä sovellettavista kansainvälisistä sopimuksista. Kansainvälisissä sopimuksissa pääpaino on EU-maissa ja Yhdysvalloissa, joissa sijaitsevat Suomen suosituimmat pilvipalvelut. EU:n ulkopuolisissa maissa oikeudet ovat erilaiset ja tietojen käsittelyä on säännelty hyvin eri tavalla. EU:n ulkopuolisiin maihin tallennettua tietoa ei saa siirtää ilman laillista perustetta ja vakuutusta saman tietoturvatason säilymisestä (Smith, Bird ja Bird 2007, 689).

4.2 Tietosuoja Suomen lainsäädännössä

Perustuslain 10§:ssä määritellään yksityisyyden suoja, joka on perustana muussa kansallisessa lainsäädännössä EU-lainsäädännön ohella. Se turvaa yksityiselämän, kunnian ja kotirauhan. (Helopuro, Perttula ja Ristola 2009, 267). Merkittävimpiä lakeja tietosuojan kannalta ovat henkilötietolaki (523/1999), laki yksityisyyden suojasta työelämässä (759/2004), sähköisen viestinnän tietosuojalaki (516/2004) ja tekijänoikeuslaki (404/1961). EU on vaikuttanut näiden kaikkien lakien sisältöön merkittävästi omalla lainsäädännöllään. Tämä takaa sen, että EU:n alueella on yhtenäinen lainsäädäntö tietosuojan käsittelyssä.

Henkilötietolaki määrittää (523/1999) Suomessa henkilötietojen suojasta, mutta samalla myös salassapitosäännöksillä henkilöä koskevien tietojen suojasta (Mäenpää 2008, 291). Henkilötietolain pohjana on ollut tietosuojadirektiivi (95/46/EY) (Vanto 2011, 12) ja se takaa tietojen vapaan liikkuvuuden EU:n sisällä mukaan lukien ETA-maat (Vanto 2011, 84).

Henkilötietolain periaatteena on määritellä henkilötietojen käsittelyn tarkoitus, turvata yksityiselämän suoja ja ohjata hyvään tietojenkäsittelytapaan (Vanto 2011, 18). Henkilö-

tietolaki on yleislaki ja sitä sovelletaan, ellei muussa laissa toisin todeta. Henkilötietolaki sisältää yleisvelvoitteet, joita palvelunylläpitäjän tulee noudattaa käsitellessään rekisteröityjä henkilötietoja.

Laissa määritellään henkilötietojen käsittelyyn liittyvistä oikeuksista, sanktioista, seuraamuksista ja sovellettavasta valvontajärjestelmästä. (Innanen ja Saarimäki 2012, 43-44). Henkilötietolakia sovelletaan rekisterinpitäjään, jonka toimipaikka on Suomessa tai Suomen lainsäädännön piirissä. Lakia sovelletaan myös rekisterinpitäjiin joiden henkilötietojen käsittelyyn käyttämä konesali sijaitsee Suomessa. (Hon, Hörnle ja Millard 2012, 8).

Henkilötietolakiin sisältyy rekisterinpitäjän huolellisuusvelvoite, mikä siirtyy ulkoistetun tietohallintopalvelun tarjoajalle rekisterinpitäjän lukuun toimittaessa. Huolellisuusvelvoite edellyttää, että tietojärjestelmä tulee alusta pitäen suunnitella huomioiden henkilötietojen käsittely. Teknisissä ratkaisuissa on otettu huomioon kaikki henkilötietojen käsittelyvaiheet keräämisestä poistamiseen. (Vanto 2011, 39-44). Hänellä on myös ilmoitusvelvollisuus henkilötietojen automaattisesti käsittelystä tietosuojavaltuutetulle rekisteriselosteella (Tietosuojavaltuutettu 2010, 5).

Henkilötietolaissa määritellään rekisteröidyn käyttäjän oikeudet rekisterinylläpitäjän velvollisuuksien lisäksi. Rekisterinpitäjän tulee määritellä rekisterin käyttötarkoitus, käyttötarkoituksensidonnaisuudet sekä henkilötietoja saa käsitellä vain rekisteröivän suostumuksella. Lakiin sisältyy rekisteröitävän tietojen tarkastusoikeus ja tiedonsaantioikeus. Lain hengen mukaisesti jokaisen Suomessa rekisteriä pitävän tulee täyttää lain asettamat velvollisuudet ja toisaalta tukea käyttäjän oikeuksia. (Vanto 2011, 39-44, 138).

Henkilötietolakiin sisältyy myös säännökset tietojen siirtämisestä EU/ETA-alueen ulkopuolelle kolmansiin maihin. Laki määrittää, että vain sellaisia tietoja voi siirtää EU/ETA-alueen ulkopuolella, joita on käsitelty Suomessa lain mukaisesti. Siirto onnistuu tämän lisäksi vain, jos tiedoille voidaan taata riittävä tietosuojan taso siirron kohteena olevassa maassa. Tämä tarkoittaa sitä, että tietosuojan tason tulee olla vähintään sama, kuin tiedoilla oli ennen siirtoa. Tämän lisäksi siirron kohteena olevassa maassa pitää olla EU-komission hyväksymä riittävä tietosuojan taso. Siirto ei koske pelkästään

konkreettisen tiedon siirtämistä, vaan myös tiedon käsittelyä monikansallisen konsernin sisällä. (Vanto 2011, 84-85)

Pilvipalveluiden käyttöönottoon liittyen olennainen lainsäädäntö on **laki viranomaisten toiminnan julkisuudesta** (621/1999), johon sisältyy julkisuusperiaate. Tietoverkkojen kannalta olennaista tässä lainsäädännössä yksityisyyden näkökulmasta on lain salassapitoperusteet. Salassapito rajoittaa asiakirjan julkisuutta ja se on poikkeus julkisuuden pääsääntöön. Yleisesti salassapito tunnetaan vaitiolovelvollisuutena ja siihen liittyy vahinkoedellytyslauseke. (Neuvonen 2013, 152-153). Salassapito voi perustua laintasoisen säädöksen lisäksi lain nojalla annettuun viranomaisen määräykseen. Salassapitoperusteet voidaan luokitella niiden suojaaman salassapitointressin mukaan. Salassapitoperusteita ovat henkilökohtaista ja yksityistä intressiä suojaavat perusteet, yleistä etua ja julkisyhteisön intressiä suojaavat perusteet. (Mäenpää 2008, 284).

Tietoverkkojen tietosuojasta säädetään **sähköisen viestinnän tietosuojalaissa** (516/2004), joka perustuu direktiiviin sähköisen viestinnän tietosuojasta (2002/58/EY) (Neuvonen 2013, 137). Laki on yleislaki, mutta erityislaki suhteessa henkilötietojen käsittelyyn (Helopuro, Perttula ja Ristola 2009, 13). Sähköisen viestinnän tietosuojalain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuus, tietoturvallisuus ja varmistaa yksityisyyden suojan toteutuminen sähköisessä viestinnässä (Helopuro, Perttula ja Ristola 2009, 29-30). Laki kattaa tunnistetietojen lisäksi viestien sisällön ja niiden luottamuksellisuuden (Neuvonen 2013, 173).

Pilvipalvelun ylläpitäjä voi tallentaa käyttäjästä henkilötietojen lisäksi paikkatietoja sekä netin käyttötietoja ja tarkastella niitä evästeiden avulla. Evästeiden käytöstä tulee ilmoittaa palvelun käyttäjälle selkeästi ja ymmärrettävästi. Evästeiden käytön sääntely vastaa suoraan sähköisen viestinnän tietosuojadirektiivin sääntelyä ja sitä on kritisoitu. (Helopuro, Perttula ja Ristola 2009, 234). Laissa määritellään lisäksi käyttäjän ja poliisin tiedonsaantioikeudesta sekä suoramarkkinoinnista. Poliisin tiedonsaantioikeus on merkittävä silloin, kun pilvipalvelussa epäillään tapahtuneen rikos, ja sen selvittämiseksi tarvitaan sähköisiä tunnistetietoja. (Helopuro, Perttula ja Ristola 2009, 291).
Sähköisen viestinnän tietosuojalakiin sisältyy lisäksi viestinnän valvontajärjestelmä. Lain 30§:n mukaan liikenne- ja viestintäministeriö valvoo ja ohjaa lain toteutumista. Käytän-

nön valvonta jakautuu Viestintäviraston ja tietovaltuutetun välillä. Heidän vastuunsa on määritelty laissa. Valvovilla viranomaisilla on tiedonsaantioikeuden lisäksi käytettävissään pakkokeinoja. (Helopuro, Perttula ja Ristola 2009, 295-303).

Turvaa henkilötietojen käsittelyyn pilvipalveluissa tuo myös **laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista** (617/2009). Lain tavoitteena on, että palveluntarjoaja takaa palvelussaan tietoturvan ja yksityisyyden suojan toteutumisen silloin, kun hänellä on käytössään vahva sähköinen tunnistaminen tai sähköinen allekirjoitus. Laki tuo myös palveluntarjoajalla turvaa siinä, että se voi luottaa palvelua käyttävän henkilön olevan juuri se, joka hän väittää olevansa. (Innanen ja Saarimäki 2012, 45). Viestintävirasto pitää yllä listaa palveluntarjoajista, jotka käyttävät lain edellyttämät vaatimukset. Vahvaksi tunnistautumiseksi luetaan pankkien verkkopankkitunnukset, Väestörekisterikeskuksen kansalaisvarmenne ja teleyritysten mobiilivarmenteet. (Viestintävirasto 2013).

Tekijänoikeuslaki liittyy pilvipalveluiden yksityisyyden suojaan immateriaalioikeuksien turvaamiseksi. (404/1961). Immateriaalioikeudet syntyvät aina luonnollisille henkilöille teoksen synty hetkellä ja ne ovat kansallisoikeuksia. (Haarman ja Maisala 2007, 5). Pilvipalveluihin immateriaalioikeudet liittyvät erityisesti kuvatallenteiden takia. Pilvipalveluihin liittyy tekijänoikeuksien osalta välittäjän eli pilvipalvelun tarjoajan vastuuvapaussääntely sekä lähdemaaperiaate. Lähdemaaperiaate määrittää sen, että vastuu määräytyy sen maan mukaan, missä palvelua tarjotaan. (Oesch, Heiskanen ja Hyyrynen 2008, 117-131).

Yksityisyyden suoja tekijänoikeuksiin liittyy erityisesti tekijänoikeuksien rajoitusten takia. Oleellisia tekijänoikeuksien rajoituksia pilvipalveluissa ovat yksityiselämän suoja ja sananvapaus. (Haarman ja Mansala 2007, 45). Tunnistettava valokuva katsotaan olevan henkilötieto. Yksityiselämää levittävän tiedon levittäminen ja kunnianloukkaus ovat kriminalisoitu rikoslaissa, jossa niistä on sääntely rangaistavuus (Tietosuojavaltuutetun toimisto 2010). Yksityishenkilöä kuvattaessa joudutaan arvioimaan, kuuluuko kuvaaminen sananvapauden suojan piiriin vai rikkooko oikeudeton kuvaaminen kotirauhaa (Neuvonen 2013, 299-301). Luvattomasti kuvatun kuvan julkaiseminen rikkoo yksityi-

syyttä, mikäli se on otettu kotirauhan piirissä tai julkisessa tilassa kuvattu kuva sisältää yksityisyyteen liittyvää tietoa (Pesonen 2011, 70).

Suomessa ei ole säädetty erityissääntelyä henkilöstä otettuun omaan kuvaan, mutta kuvan kohteella on tiettyjä oikeuksia, joita on käsitelty KKO:n päätöksissä (Neuvonen 2013, 303). Pääasialliset oikeudet ovat kuitenkin tekijänoikeuden haltijalla eli valokuvan ottajalla. Oikeus antaa hänelle yksinoikeuden päättää teoksen hyväksikäytöstä (Oesch, Heiskanen ja Hyyrynen 2008, 4). Yksinoikeus antaa oikeuden hyödyntää teosta taloudellisesti, mutta samalla se antaa kielto-oikeuden (Haarmann ja Mansala 2007, 4). Tekijän oikeuden haltija voi vaatia teoksen poistoa tietoverkosta, mikäli se on julkaistu luvattomasti (Pesonen 2011, 126).

4.3 Kansainväliset sopimukset

Kansallisen lainsäädännön lisäksi Suomessa toimivien pilvipalveluiden tietosuojan käsittelyyn vaikuttavat myös kansainväliset sopimukset ja komission päätökset. Näitä sopimuksia ovat Safe Harbor -järjestelmä, EU:n mallislausekkeet, maksukorttialan tietoturvastandardi PCI-DSS, Euroopan neuvoston tietosuojasopimuksessa, OECD:n julkaisemat turvallisuusperiaatteet ja Sarbanes-Oxley Act.

Safe Harbor -järjestelmä on yksi Euroopan yhteisöjen komission päätöksellä (2000/520/EY) määritelty järjestelmä, minkä tarkoituksena on turvata riittävä tietosuoja henkilötietojen siirroissa Yhdysvaltoihin sijoittautuneille organisaatioille Safe (Harbor Framework 2012). Komission päätös (2000/520/EY) on jäsenvaltioita velvoittava.

EU-komissio on todennut, ettei Yhdysvaltojen tietosuojan taso ole riittävä tietojen siirtämiseen. Tämä on aiheuttanut hankaluuksia EU:n ja Yhdysvaltojen väliselle kaupankäynnille. Safe Harbor – järjestelmä on ratkaisu ongelmaan ja sitä hallinnoi Yhdysvaltain kauppaministeriö. Safe Harbor -järjestelmässä määritellään tietojen siirtämisestä yhdysvaltalaisen yhtiön haltuun ja sen edellytyksenä on, että henkilötietolain säännöksiä noudatetaan ennen tietojen siirtämistä. (Valto 2011, 86). Euroopan komissio on tehnyt 27.11.2013 päätöksen laittaa järjestelmän koeajalle ja vaatii Yhdysvalloilta selvityksen sen toimista (European Commission 2013).

Järjestelmää noudattavan yhtiön on huolehdittava henkilötietojen suojaamisesta ja varmistettava seitsemän eri tietosuojaperiaatteen noudattaminen. Periaatteiden mukaisesti järjestelmää noudattavan yhtiön on pyydettävä yksiselitteinen suostumus tietojen keräämiselle. Yhtiön on ilmoitettava vähintään, mitä tietoja kerätään, miksi ja mihin maahan. Rekisterissä olevalle yksityishenkilölle on tarjottava mahdollisuus tarkastaa tietonsa ja muuttaa tai poistaa virheellisiä tietoja. Lisäksi heidän on tarjottava yksityishenkilölle mahdollisuus valita, voiko tietoja luovuttaa kolmannelle osapuolelle tai käyttää tietoja muuhun, kuin alun perin ilmoitettuun tarkoitukseen. (US Department of Commerce 2000).

Tietosuojan turvaamisen kannalta on olennaista, että yhtiö on sitoutunut noudattamaan Yhdysvaltojen kauppaministeriön (US Department of Commerce) ja komission hyväksymiä yksityisyyden suojaa koskevia Safe harbor – periaatteita. Lisäksi velvoitteena on periaatteiden täytäntöön panemiseksi noudattaa Yhdysvaltain hallituksen 21.7.2000 laatimia tavallisimpien kysymysten ohjetta (Frequently Asked Questions, FAQs). Yhdysvaltain kauppaministeriö ylläpitää rekisteriä yhtiöstä, jotka noudattavat Safe Harbor -periaatetta tai joidenkin osallistumien järjestelmään on päättymässä. (Tietosuojavaltuutettu).

Safe Harbor järjestelmän lisäksi komissio on henkilötietosuojadirektiivin mukaisesti hyväksynyt **mallisopimuslausekkeita** (EU Standard Contractual Clause), jotka mahdollistavat tietojen siirron EU-alueen ulkopuolelle. Mallisopimuslausekkeet koskevat EU/ETA-alueen palveluntarjoajia, eivätkä jäsenvaltiot voi kieltää niiden käyttöä tietojen siirrossa. Mallilausekkeita on kolmenlaisia ja ne niiden tavoitteena on taata riittävä tietosuoja siirrettäessä tietoja EU/ETA-alueen ulkopuolelle sekä helpottaa turvallista tietojen siirtoa maailmanlaajuisesti. Mallilausekkeiden mukaisista henkilötietojen siirroista ei tarvitse ilmoittaa tietosuojavaltuutetulla. (Tietosuojavaltuutettu).

Julkisten pilvipalveluiden yksityisyyden suojaan vaikuttaa myös maksukorttialan sopimukset. Useissa pilvipalveluissa on mahdollisuus maksukorttimaksuihin, joiden käytön tietoturvaa varten on kehitetty **maksukorttialan tietoturvastandardi** (PCI DSS) (PCI Data Security Standard 2010). PCI DSS-standardi määrittää vähimmäisvaatimukset

maksukorttien tietosuojalla ja sitä sovelletaan kaikkiin toimijoihin, jotka käsittelevät maksukortin haltijan tietoja. Standardin tavoitteena on ylläpitää maailmanlaajuisesti yhtenäisiä teknisiä ja operatiivisia tietoturvakäytäntöjä ja määrittää vähimmäisvaatimukset tietojen turvaamiselle. Standardia hallinnoi riippumaton The PCI Security Standards Council ja siinä on mukana kaikki merkittävimmät maksukorttiyhtiöt. (PCI Data Security Standard 2010).

Tietosuojasta automaattisessa tietojenkäsittelyssä on määritelty lisäksi **Euroopan neuvoston tietosuojasopimuksessa** ja **OECD**:n (Organization for Economic Cooperation and Development) suositus yksityisyyden suojaamisesta, jotka ovat vanhimpia sopimuksia, joissa on käsitelty tietosuojaa tietojenkäsittelyssä. OECD on alun perin määritellyt turvallisuusperiaatteet vuonna 1992. Turvallisuusperiaatteet sisältävät 9 eri kohtaan ja niitä on uudistettu sittemmin. (Valtiovarainministeriö, 2002).

OECD on turvallisuusperiaatteiden lisäksi laatinut vuonna 1980 ohjeet yksityisyyden suojasta ja 1997 salauspolitiikan periaatteet. (Valtionvarainministeriö 2002, 9-11). Vahti-ohjeen mukaisesti Suomen valtionhallinnossa noudatetaan OECD:n turvallisuusperiaatteita (VAHTI 2/2004 2004, 16).

5 Tietosuojan huomioiminen ulkoistuksissa

Pilvipalvelun tietosuoja huomioidaan pilvipalveluun ulkoistettaessa tehtävissä sopimuksissa. Henkilötietolaki edellyttää myös kirjallista sopimista, mikäli henkilörekisteri luovutetaan jollekin ulkopuoliselle osapuolelle. (Laaksonen, Nevasalo ja Tomula 2006, 243). Seuraavaksi esitellään niitä sopimusoikeudellisia kysymyksiä, joita tulisi vähintään huomioida. Lisäksi perehdytään auditointiin ja riskienhallintaan, joilla voidaan varmistua tietosuojan tasosta.

5.1 Sopimustyypit

Pilvipalvelun asiakas luovuttaa tallentamansa tiedot yrityksen ulkopuolisen palvelun hallintaan. Näiden tietojen hallinnasta määritellään pilvipalvelun sopimusehdoissa. Lainsäädäntö asettaa reunaehdot, mitä sopimusehtojen tulee sisältää ja kuinka palvelun tulee käsitellä tallennettua tietoa. Sensitiivisintä tallennettua tietoa ovat henkilötiedot, joista määritellään laissakin. Sopimustyyppejä ovat vakiosopimus ja yksilöllisesti laadittu sopimus, mutta rajanveto näiden välillä on liukuva (Wilhelmsson 2008, 35).

Julkisten pilvipalveluiden sopimukset ovat sähköisiä sopimuksia ja niiden määrä on kasvanut nopeasti. Sähköisen sopimuksen linkin takaa löytyvät sopimusehdot muistuttavat muodoltaan perinteistä vakiosopimustyyppiä, jossa ehdot on sijoitettu paperisen lomakkeen taakse. (Wilhelmsson 2008, 70).

Vakioehdot ovat yksipuolisesti laadittuja vakioehtoja, joita käytetään useissa yksittäisissä sopimuksissa. Ne on laadittu ennalta myöhemmin solmittavia sopimuksia varten ja niitä käytetään usean sopimuskumppanin kanssa (Wilhelmsson 2008, 36–37). Vakiosopimuksiin liittyy yllättäviä ja ankaria ehtoja, sekä elinkeinon harjoittajan informaatiovelvollisuus (Wilhelmsson 2008, 92–93). Näiden tulkinta on kuitenkin epämääräistä ja tapauskohtaista (Wilhelmsson 2008, 95). Isompien sopimuskokonaisuuksien kohdalla voi olla mahdollista neuvotella vakioehdoistakin (Bradshaw 2010, 2).

Tietosuojavaltuutettu ja tietosuojatyöryhmä ovat laatineet ohjeistuksia sopimuksien tekoon. IT-alalla on myös yleisesti käytössä IT2010 -sopimusehdot, jotka ovat IT-alan vakioehdot. Ohjeistus on tehty helpottamaan osapuolten välistä sopimista ja kustannusten alentamiseksi. IT2010 -sopimusehdot ovat laatineet yhdessä Keskuskauppakamari, Ohjelmistoyrittäjät ry, Suomen Osto- ja logistiikkayhdistys LOGY ry, Teknologiateollisuus ry ja Tietotekniikkaliitto ry vuosina 2009–2010 ja ne korvasit aiemmat ehdot. (Erlund, Lindfors, Salminen ja Turunen 2011, 31)

ICT-alan sopimukset ovat tyypillisesti monimutkaisia kokonaisuuksia, joissa asiakkaan on oltava valveutunut. Sopimuksissa määritellään tyypillisesti palvelukokonaisuudesta, sopimuksen kestosta ja hinnasta. Tietosuojan kannalta olennaista on sopia henkilötietojen käsittelystä. Ulkoistettava kohde on hyvä yksilöidä ja määritellä tarkasti, mitä luovutetaan. Sopimuksessa määritellään lisäksi tietojen siirron rajoituksista kolmansiin maihin, alihankinta ketjutuksista ja auditoinnista. IT2010 ETP -erityisehdoissa määritellään tarkemmin kysymyksiä liittyen tietoverkkojen välityksellä toimitettavista palveluista (Erlund, Lindfors, Salminen ja Turunen 2011, 351–400).

Tyypillisesti sopimuksessa käsitellään tietojenkäsittelyn rajoituksista ja lainvelvoitettavuudesta. Tähän liittyy myös vastuut, vahingonkorvaus velvoitteet ja mahdollisissa ongelmatapauksissa käytettävä lainsäädäntöalue. Olennaista on sopia myös sopimuksen päättämisen toimenpiteistä, kuten tallennettujen tietojen siirrosta toiselle palveluntarjoajalle tai palveluntarjoajan konkurssista. (Erlund, Lindfors, Salminen ja Turunen 2011, 394–395).

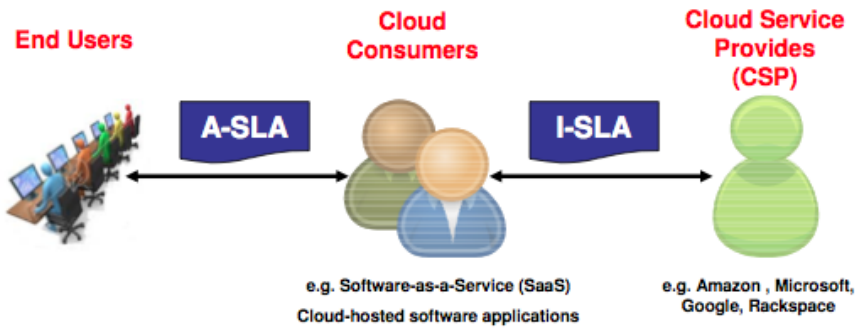
5.2 Palvelutasosopimus (SLA)

SLA-palvelutasosopimuksella (SLA, Service Level Agreement) ja Qos-laatulupauksilla turvataan pilvipalvelun tietosuojaa. Sillä on suuri merkitys luotettavuuden ja saatavuuden todentamisessa asiakkaalle. (Salo 2010, 112). Tyypillisesti SLA-palvelutasopimus on liitteenä osana palvelusopimusta (Erlund, Lindfors, Salminen ja Turunen 2011, 352).

Palvelutasosopimus on tärkeä työväline määriteltäessä pilvipalvelun tarjoajan ja asiakkaan välisiä suhteita. Siinä määritellään palvelun sisällöstä ja tasoista, kuten kuinka pil-

vipalvelun tulee toimia, vasteaikoja, suoritustehoja ja sanktiota. (Wang, Wu, Zhang, Ding, Zhou ja Pei 2011, 1131). Palvelutasosopimus on myös hyvä väline tietoturvariskien määrittelyyn (Li, Xu, Li ja Zhang 2011, 221). Palveluntarjoajasta riippuen palvelutasosopimuksen sisältö voi olla hyvinkin erilainen. Tästä syystä asiakkaan voi olla vaikea verrata palveluntarjoajia ja luotettavan palveluntarjoajan valinta voi olla haastavaa. (Wang, Wu, Zhang, Ding, ja Pei 2011, 1131).

SLA on toimijan ja asiakkaan välinen sopimus. Pilvipalveluissa SLA:n suhteen on omat ongelmansa. Ongelmia aiheuttavat pilven kapasiteetin käytön suuri vaihtelevuus, sekä kolme toimija osapuolta. Osapuolet on kuvattu kuviossa 4 ja ne ovat pilvipalvelun palveluntarjoaja, pilvipalvelun asiakas sekä loppukäyttäjä. Pilvipalveluissa on palvelutasosopimukset ovat osapuolten välillä. Sopimuksia on pilvipalvelun tarjoajan ja sen asiakaan välillä sekä pilvipalvelun asiakkaan ja loppukäyttäjän välillä.. Sopimusten vastuiden välillä syntyy helposti ristiriitatilanteita ja kapasiteetti ongelmia, joista toinen osapuoli voi joutua korvausvelvolliseksi. (Sakr ja Liu 2012, 360–362).



Kuvio 4: Palvelutasosopimuksen osapuolet (Sakr ja Liu 2012, 362).

5.3 Auditointi

Auditoinnissa luotettava ulkopuolinen taho tarkastaa palvelun turvallisuuden ja toiminnan. Auditoinnilla voitaisiin parantaa pilvipalveluiden läpinäkyvyyttä, mikä luotettavuutta (Chow, Golle, Jakobsson, Shi, Staddon, Masuoka ja Molina 2009, 85–90). Hyvään yrityskulttuurin ja tietoturvan hallintaan sisältyy auditointi, jonka periaatteita on määri-

telty myös Cloud Security Alliancen ohjeistuksessakin (Cloud Security Alliance 2011, 47).

Auditoinnissa on hyvä noudattaa riittäviä tietoturvastandardeja, suosituksia ja vaatimuksia. Tunnetuin auditointistandardi on AICPA:n (American Institute of Certified Public Accountants) SAS 70-standardi, joka määrittelee suuntaviivat sisäiselle valvonnalle, joka on tietyissä tapauksissa jopa pakolinen (Laaksonen, Nevasalo ja Tomula 2006, 242). Muita standardeja ovat HIPPA (Health Insurance Portability and Accountability A), PA-DSS (The Payment Application Data Security Standard), ISO/EIC 27001 ja Cobit. Lisäksi Yhdysvalloissa on useita omia standardeja ja lakeja, joilla valvotaan ja kontrolloidaan yhdysvalloissa toimivien pilvipalveluiden toimintaa. Suomessa on valtiohallinnan määrittelemät Vahti-ohjeet, Katakri-kriteeristö ja tietoturvatasot. Varsinaisina pilvipalvelun auditointikriteereitä ei vielä ole kuitenkaan olemassa (Rehman ja Islam 2011, 143).

Katakri on valtionhallinnon kansallinen turvallisuusauditointikriteeristö. Sen tarkoituksena on yhtenäistää viranomaistoimintoja kansallisesti sekä auttaa yrityksiä ja muita yhteisöjä turvallisuustyössä. Turvallisuusauditointikriteeristö jakautuu neljään osaan, joita ovat hallinnollinen turvallisuus (turvallisuusjohtaminen), henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Osiot eivät ole itsenäisiä kokonaisuuksia, vaan ne kaikki on huomioitava auditoinnissa. Kriteeristö sisältää viranomaisohjeiden ohella erilliset suositukset elinkeinoelämän turvallisuuskäytänteistä. Elinkeinoelämän suositukset valmistavat yrityksen vastaamaan viranomaisvaatimuksia, vaikka ne muutoin eivät ole vaatimuksena. (Puolustusminiteriö 2011, 3-4).

Valtionhallinnolla on käytössä myös Vahti-ohjeet 3/2012 Teknisen ICT-ympäristön tietoturvataso-ohje ja 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Näissä ohjeissa määritellään teknisten tietoturvatasojen toteuttamisesta ja viitataan Katakri-kriteeristöön. Ohje on ICT-palvelujen kilpailutukseen liittyviä tietoturvanäkökulmia ja teknisen tietotekniikkaympäristön vaatimusten kuvauksia. Ohje sisältää apuvälineitä ICT-palvelujen tuottamiseen ja hankintaan, koska valtionhallinnon organisaatioiden tietoturvallisuustasojen vaatimukset koskevat sisäisten

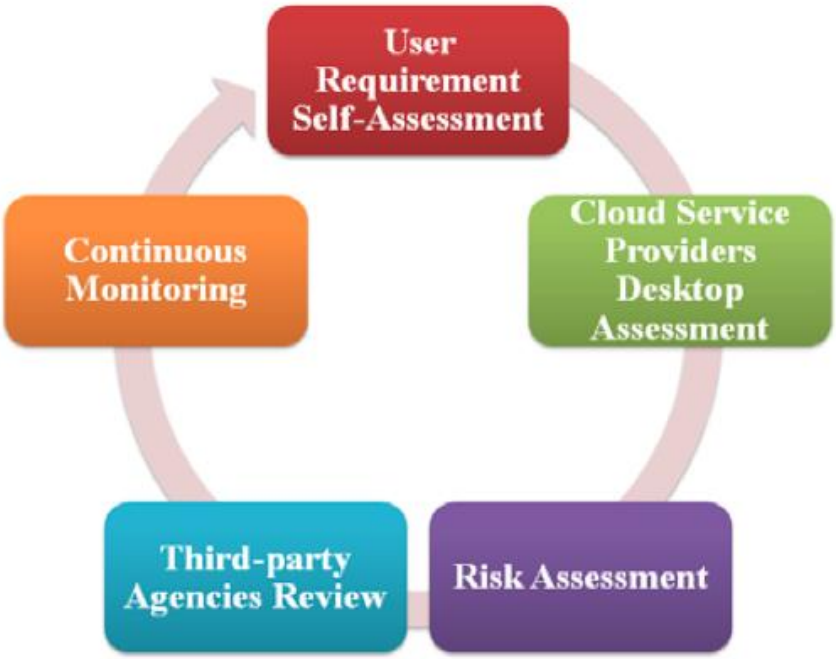
palveluntoimittajien lisäksi ulkoisia palvelutoimittajia. (Valtiovarainministeriö 2012, 11–12, 28).

5.4 Riskinhallinta

Pilvipalvelun palveluntarjoajan riskienhallinnalla on omalta osaltaan merkittävä rooli tietosuojan turvaamisessa ja sen mittaamisessa. Riskienhallinnalla palveluntarjoaja pystyy ennakoimaan mahdolliset tulevat riskit ja mahdollisesti ennaltaehkäisemään ne. Riskienhallinnalla pyritään kartoittamaan toimivat tekniset ratkaisut, kuten myös sopimusoikeudelliset periaatteet ja lainmukaisuus. Parhaillaan kunnollinen riskienhallinta takaa pilvipalvelun asiakkaalle turvallisen ympäristön, jossa hänen tallentamansa tieto on kunnolla suojattu. Riskienhallinnasta sovitaan osapuolien kesken palvelutasosopimuksella (Kirkham, Djemame, Kiran, Jiang, Armstrong, Kousiouris, Vafiadis ja Evangelinou 2012, 156).

Pilvipalvelun riskienhallinta ei rajoitu kuitenkaan pelkästään palveluntarjoajan riskienhallintaan, vaan myös asiakaan omaan riskienhallintaan. Riskienhallinnassa hyvin laadittu palvelutasosopimus on tärkeä asiakkaan tietoturvan tuoja pilvipalveluissa (Morin, Aubert, Gateau 2012, 5509). Hyvin suunnitellulla riskienhallinnalla voidaan varmistaa, että tieto on turvattua ja saatavilla (Zhang, Wuwong, Li ja Zhang 2010, 1328). Hyvällä riskienhallinnalla suunnittelulla pystytään turvaamaan se, ettei sensitiivisenkään tiedon ulkoistamisessa tule ongelmia (Samarati ja De Capitani di Vimercati 2010, 12).

Perinteisesti riskienhallinnassa on käytössä tietoturvamenetelmiä, parhaita käytäntöjä ja tietoturvaohjelmistoja sekä laitteistoja. Pilvipalveluissa tilanne on kuitenkin toisenlainen. Perinteisesti ajateltu tietoturva on asiakkaan ulottumattomissa palveluntarjoajan hallinnassa. Pilvipalveluissa riskienhallinnan tulee keskittyä myös pilvipalvelun asiakkaan ja loppukäyttäjän luottamuksen turvaamiseen. Tämän turvaamiseksi pilvipalveluiden riskienhallinnassa voidaan käyttää seuraavia kuviossa 5 kuvattuja periaatteita: käyttäjävaatimusten itsearviointi, pilvipalveluntarjoajan käytäntöjen arviointi, pilvipalvelun tuottajan riskiarviointi, kolmannen osapuolen validointi ja jatkuva seuranta. Näiden avulla on helpompi ymmärtää pilvipalveluiden monimutkaisuutta useiden toimijoiden kesken. (Xie, Peng, Zhao, Chen, Wang ja Huo 2012, 476–480).



Kuvio 5: Pilvipalveluiden riskienhallinnan periaatteet (Xie, Peng, Zhao, Chen, Wang ja Huo 2012, 477).

Yritykset käyttävät paljon aikaa riskianalyyseissä verkon suojaamiseen, palomuureihin ja ulkopuolisten tunkeutujien torjuntaan. Enemmän tulisi kuitenkin kiinnittää huomioita tietosuojanäkökulmaan, koska periteinen tietoturva on pilvipalveluissa asiakkaan ulottumattomissa. Riskianalyysissä tulisi huomioida ainakin tiedon luottamuksellisuuteen, eheyteen, auditoitavuuteen, käytettävyyteen, monitoimijaympäristön luottamuksellisuuteen ja auditoitavuuteen. Näiden osa-alueiden tarkastelun etuna on, että asiakkaat, toimijat ja muut pilvipalvelun osapuolet tulevat kaikki huomioiduksi. Tämäkään ei kata kaikkia mahdollisia riskejä, mutta auttaa laajentamaan näkökulmaa. (Khan, Oriol, Kiran, Jiang ja Djemane 2012, 125).

6 Yhteenveto

Työn tavoitteena oli selvittää, kuinka tietosuoja tulisi huomioida it-palveluja ulkoistettaessa pilvipalveluihin ja kuinka auditoinnilla voidaan varmistaa tietosuojan taso. Pilvipalvelun hankinnassa on useita tietosuojaan liittyviä kysymyksiä, joita yrityksen on syytä pohtia ennen pilvipalvelun käyttöönottoa. Tekniset vaatimukset ja hinta eivät pelkästään riitä määrityksiksi pilvipalvelua hankittaessa, vaan yrityksen on syytä määrittää oma suhtautumisensa myös tietosuojaan. Tietosuojaa ei tulisi nähdä vain ylimääräisenä kustannuksena hankinnassa.

Pilvipalvelun kolme osapuolta tuovat epävarmuuden ja eron perinteiseen tietoturvaan. Epävarmuutta lisää läpinäkyvyyden puute palveluntarjoajan toimintaan, sekä mahdottomuus varmistua palvelun tasosta tai palveluntarjoajan motiiveista. Pilvipalvelu on suhteellisen helppo ja nopea pystyttää. Palvelun rakenteen suunnittelu jää helposti vähälle huomiolle, eikä riskienhallintaan kiinnitetä riittävää huomiota. Julkisissa pilvipalveluissa tämä on kaikkien helpoimmin havaittavissa. Näissä palveluissa käyttäjämäärät ovat kasvaneet nopeasti heti alussa, eikä palvelua ole alun perin suunniteltu niin suurille käyttäjämäärille.

Suomen suosituimmat pilvipalvelut ovat EU:n ulkopuolisia yhtiötä ja useimmiten Yhdysvaltalaisia yhtiöitä. Yhdysvaltojen tietosuoja ei ole Euroopan Unionin määritelmän mukaan riittävä ja siellä tietosuojaa käsitellään hyvin eri tavalla kuin EU:ssa ja Suomessa. Tästä syystä kansainvälisillä sopimuksilla, kuten Safe Harbor -menetelmällä on merkittävä rooli yhtiöiden toimiessa EU-alueella.

Tutkielmassa esitellyt standardit eivät ole ainoita, joilla voidaan taata palvelun tietoturvallisuutta. Niiden olemassa ololla voidaan kuitenkin varmistua palvelun luotettavuudesta. Standardien puute voi kuvastaa sitä, että palvelussa ei ole huomioitu kaikkia tietosuojaan vaikuttavia turvallisuustekijöitä.

Sopimusoikeudellisesti julkisen pilvipalvelun käyttäjät ovat heikommassa asemassa kuin muiden pilvityyppien asiakkaat. Huolellisesti laadittu ulkoistussopimuksen ja vastuiden

määrittäminen auttavat turvaamaan tietosuojaa. Sopimuksen sisältö, tyyppi ja sanktiot on syytä miettiä tarkkaan ja tarvittaessa käytettävä lakimieskonsultaatiota. Hankittaessa pilvipalvelua on syytä tutustua palvelun sopimusehtoihin huolella.

Kokonaisuutena tunnettujen pilvipalveluiden tietosuoja on hyvissä kantimissa ja ne ovat turvallisia käyttää. Tietosuojapuutteet tulevat julkisuuteen nopeasti, mikä auttaa ylläpitämään riittävää tasoa pilvipalveluiden tietosuojassa. Asiakkaan vastuulle jää valinta pilvipalveluiden tuottajasta ja sen luotettavuuden varmistamisesta.

6.1 Oma oppiminen

Työn aiheen valinta perustui vahvaan omaan kiinnostukseen pilvipalveluiden tietosuojasta. Osaamista aihealueesta olen kasvattanut opintojen aikana, joten työhön orientoituminen oli helppoa. Työn aloittaminen oli tästä syystä nopeaa ja sain raportin rungon tehtyä melko lyhyessä ajassa loppuvuodesta 2013. Työn loppuun saattaminen ja viimeistely venyivät muiden opiskelukiireiden takia kevääseen 2014.

Raporttia kirjoittaessani tietosuojalainsäädäntö on murrosvaiheessa ja Euroopan unioni on uudistamassa kattavasti tietosuojasääntelyään. Julkinen keskustelu tietosuojasta on kasvanut, mitä on ollut mielenkiintoista seurata opinnäytetyöprosessin aikana. Työn edetessä oma osaamiseni syventyi huomattavasti erityisesti henkilötietolain osalta ja opin tulkitsemaan paremmin Euroopan unionin säännöksiä. Samalla opin ymmärtämään syvällisemmin Safe Harbor -järjestelmä ja sen puutteita. Työn edetessä hämmästyin, kuinka välinpitämätön Yhdysvaltojen hallinto ja yritykset ovat Euroopan Unionin tietosuojasäännöksiä ja Safe Harbor -järjestelmää kohtaan.

Opinnäytetyön ja raportin kirjoittaminen oli minulle ennestään tuttua, kuten myös lähteiden käyttö ja hankinta. Suuri etu lähteitä etsiessäni oli Helsingin Yliopiston tieteellisten artikkeleiden tietokannat, joista löytyi runsaasti tieteellisiä julkaisuja lainsäädännöstä ja pilvipalveluiden teknisestä turvaamisesta. Haaga-Helian kirjaston tarjonta yllätti positiivisesti, mistä löytyi kattavasti lähdeteoksia pilvipalveluista ja sopimusoikeudesta.

Haaga-Helian puolelta opinnäytetyöprosessi oli selkeästi ohjeistettu ja ohjattu. Prosessissa sai riittävästi tukea ja ohjausta, mutta samalla myös vapautta. Prosessissa on huomioitu hyvin aikuisopiskelijat ja työn tekeminen on tehty joustavaksi ja sujuvaksi.

7 Lähteet

Aicpa, 2014, SAS 70 overview. Luettavissa: http://sas70.com/sas70_overview.html. Luettu 4.5.2014

Anderson, R., 2008, Security Engineering. Wiley Publishing, Indiana, Yhdysvallat.

Bauer, E., Randee, A., 2012, Reliability and availability of Cloud Computing, Institute of Electrical and Electronics Engineers. John Wiley & Sons., New Jersey.

Bradshaw, S., Millard, C. ja Walden, I. Contracts for Clouds: Comparsison and Analysis of the Terms and Conditions of Cloud Computing Services. Queen Mary School of Law Legal Studies Research Paper No. 63/2010.
Luettavissa: http://ssrn.com/abstract=1662374.
Luettu 4.5.2014.

Buyya, R., Broberg, J., Goscinski, A., 2011, Cloug Computing – Principles and Paradigms, John Wiley & Sons, Inc., New Jersey.

Chemerkin, Y. 2013, Limitations of Security Standards against Public Clouds. Russian State University for the Humanities, Moskava, Venäjä.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. ja Molina, J., 2009, Controlling data in the cloud: outsourcing computation without outsourcing control. Proceedings of the ACM Workshop on Cloud Computing Security, Chicago.

Cloud Security Alliance, 2011 Security guidance for critical areas of focus in cloud computing. Luettavissa: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf. Luettu 15.9.2013.

Doelitzscher, F., Fischer, C., Moskal, D., Reich, C., Knahl, M. ja Clarke, N., 2012, Validating Cloud Infrastructure Changes By Cloud Audits. Furtwangen University - Cloud Research Lab, Saksa, 2012 IEEE Eighth World Congress on Services.

Erlund, K., Lindfors, A., Salminen, J. Ja Turunen, J., 2011, IT2010 käytännön käsikirja. Bookwell, Helsinki.

European Commission Decision 26.7.2000 2000/520/EC.
25.8.2000, Euroopan yhteisöjen virallinen lehti.

European Commission – MEMO/13/1059, 27.11.2013
Luettavissa: http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm. Luettu 27.11.2013.

Evans, R., Tsohou, A., Tryfonas, T. ja Morgan, T. 2010, Engineering secure systems with ISO 26702 and 27001. 5th International Conference on System of Systems Engineering (SoSE), Loughborough University, UK.

Goodrich, M., Tamassia, R. 2011, Introduction to Computer Security. Pearson, Boston, Yhdysvallat.

Grobauer, B., Walloschek, T. ja Stöcker, E., 2001, Understanding Cloud Computing Vulnerabilities. IEEE Computer and reliability societies maaliskuu/huhtikuu 2011.

Haarman, P-L ja Maisala, M-L, 2007, Immateriaalioikeuden perusteet. Talentum, Helsinki.

Hakala, M., Vainio, M. ja Vuorinen, O., 2006, Tietoturvallisuuden käsikirja, WS Bookwell, Porvoo.

Helopuro, S., Perttula, J., Ristola, J., 2009, Sähköisen viestinnän tietosuoja. Talentum, Helsinki.

Hemmo, M., 2006, Sopimusoikeuden oppikirja. Talentum, Helsinki.

Henkilötietolaki 523/1999.

Horn, K., Hörnle, J. ja Millard, C., 2012, Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data

Protection Law?. The Cloud of Unknowing, Part 3, Queen Mary University of London. Lontoo, Yhdistynyt Kuningaskunta.

Innanen, A. ja Saarimäki J., 2012, Internetoikeus. Edita, Helsinki.

Järvinen, P. 2010, Yksityisyys: Turvaa digitaalinen kotirauhasi. WSOYpro, Jyväskylä.

Katakri II, 2011, Kansallinen turvallisuusauditointikriteeristö. Puolustusministeriö.

Khan, A., Oriol, M., Kiran, M. Jiang, M. ja Djemame, K., 2012, Security Risks and their Management in Cloud Computing. 2012 IEEE 4th International Conference on Cloud Computing Technology and Science.

Kirkham, T., Djemame, K., Kiran, M., Jiang, M., Armstrong, D., Kousiouris, G., Vafiadis, G. ja Evangelinou, A., 2012, Risk Based SLA
Lu, T., Guo, X., Xu, B., Zhao, L., Peng, Y. ja Yang, H., 2013, Next Big Thing in Big Data: the Security of the ICT Supply Chain. IEEE Computer society.

Management in Clouds - A legal perspective. The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012).

Kleemola, M. Ja Tervo-Pellikka, R., 1998, Tietosuoja – Vaatimukset verkottuvassa tietojärjestelmässä. Suomen ATK-kustannus, Espoo.

Koivunen, E. 2011, Normit ja muut viitekehykset. Vahti-ohje.

Laaksonen, M., Nevasalo, T. ja Tomula, K., 2006, Yrityksen tietoturvakäsikirja. Edita Pubslishing, Helsinki.

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009.

Lamberg, A., Mäkelä, Y. ja Terämaa, J., 1992, Tietoverkon oikeudelliset kysymyset. Liikenneministeriön julkaisuja 15/92, Helsinki.

Li, L. Xu, L., Li, J., Zhang, C., 2011, Study on the Third-party Audit in Cloud Storage Service. School of Computer Science and Technology University of Science and Technology of China, International Conference on Cloud and Service Computing.

Liikenne- ja viestintäministeriö, Tietosuojavaltuutetun toimisto ja Viestintävirasto, Sähköisen viestinnän tietosuojalaki -esite.

Mell, P. & Grance, T., 2011, The NIST Definition of Cloud Computing. Recommendation of the National Institute of Standards and Technology, National Institute of Strandards and Technology U.S. Department of Commerce.

Morin, J-H., Aubert, J. ja Gateau, B., 2012, Towards Cloud Computing SLA Risk Management: Issues and Challenges. 2012 45th Hawaii International Conference on System Sciences.

Mäenpää, O., 2008, Julkisuusperiaate. WSOY, Helsinki.

Neuvonen, R., 2013, Viestintä- ja informaatio-oikeuden perusteet. Lakimiesliiton kustannus, Helsinki.

Nyyssölä, M, 2001, Yksityisyyden suoja työsuhteessa. WS Bookwell, Porvoo

Oeshc, R., Heiskanen, H. ja Hyyrynen, O. (toim.), 2008, Tekijänoikeus ja digitaalitalous. WSOYpro, Helsinki.

Oikeusministeriön tiedote 18.2.2014.

http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/euroopanunionintietosuojalainsaadannonuudistaminen.html. Luettu 19.4.2014.

Ojanen, T., 2007, EU-oikeuden perusteita. Edita, Helsinki.

Ojanen, T., 2009, Johdatus perus- ja ihmiesoikeusjuridiikkaan. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut, Yliopistopaino, Helsinki.

Paananen, J., 2005, Tietotekniikan peruskirja. Docendo Oy, Jyväskylä.

Parakh, A, Kak S, 2009, Online data storage using implicit security. Information Sciences, Computer Science Department, Oklahoma State University, USA.

Pesonen, P, 2011, Viestintäoikeuden käsikirja. Edista Publishing, Helsinki.

Petković, M., Jonker, W., 2007, Security, Privacy and Trust in Modern Data Management. Springer, Berlin.

PCI Data Security Standard, PCI Security Standards Council, 2010
Luettavissa: https://www.pcisecuritystandards.org/index.php. Luettu 20.10.2013.

Rehman, I., ja Islam, H., Cloud Computing Security Auditing. Next Generation Information Technology (ICNIT), The 2nd International Conference on, IEEE.

Sakr, S. ja Liu, A., 2012, SLA-Based and Consumer-Centric Dynamic Provisioning for Cloud Databases. 2012 IEEE Fifth International Conference on Cloud Computing, IEEE Computer Society.

Salo, I, 2010, Cloud computing palvelut verkossa. Bookwell, Porvoo.

Samarati, P. ja De Capitani di Vimercati, S., 2010, Data protection in outsourcing scenarios: issues and directions. In Proceedings of the 5th ACM Symposium on infor-

mation, Computer and Communications Security (ASIACCS), Beijing, China, ACM, New York.

Safe Harbor Framework, The U.S. Department of Commerce 11.4.2012

Sähköisen viestinnän tietosuojalaki 16.6.2004/516.

Suomen Perustuslaki 11.6.1999/731.

Tekijänoikeuslaki 8.7.1961/404.

Tietosuojavaltuutetun toimisto, Valokuva ja yksityisyyden suoja henkilötietolain kannalta. Tietosuoja.fi 27.7.2010.
http://www.tietosuoja.fi/uploads/qw2kuu7_1.pdf
Luettu 2.5.2014.

Tietosuojavaltuutetun toimisto, Henkilötietolain mukainen ilmoitusvelvollisuus. Tietosuoja.fi 27.7.2010.
http://www.tietosuoja.fi/uploads/068sox3cia0ww.pdf
Luettu 2.5.2014

Valtiovarainministeriö, 2002, OECD:n suositus, Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet. Luettavissa:
https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/24335_fi.pdf
Luettu 25.4.2014

Valtiovarainministeriö julkaisu 2004, Vahti 4/2004 - Tietoturvallisuus ja tulosohjaus. Edita Prima Oy, Helsinki.

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

Wallin, A-R ja Nurmi, P, 1988, Tietosuoja-lainsäädäntö. Lakimiesliiton kustannus, Helsinki

Wang, C., Penn J. ja Viglianti A., 2009, How Secure Is Your cloud? A Close Look At Cloud Computing Security Issues. Forrester Research Inc.

Vahti-ohje 3/2012, Teknisen ICT- ympäristön tietoturva- taso-ohje, Valtionhallinnon tietoturvallisuuden johtoryhmä, Ympäristöministeriö.

Viestintävirasto 2013, Vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne. Luettavissa: https://www.viestintavirasto.fi/tietoturva/sahkoinentunnistaminenjaallekirjoitus.html Luettu 4.5.2012.

Xie, F., Peng, Y., Zhao, W., Chen, D., Wang, X. ja Huo, X., 2012, A risk management framework for cloud computing. Proceedings of IEEE CCIS2012

Youseff, L., Butrico, M. ja Da Silva, D., 2008, Toward a Unified Ontology of Cloud Computing. In Proceedings of Grid Computing Environments Workshop, Texas, USA.

Zhang, X., Wuwong, N., Li, H. ja Zhang, X., 2010, Information Security Risk Management Framework for the Cloud Computing Environments, 10th IEEE International Conference on Computer and Information Technology, IEEE Computer Society.