VAASAN YLIOPISTO

KAUPPATIETEELLINEN TIEDEKUNTA

TALOUSOIKEUS

Pasi Laasala

TERVEYDENHUOLTOALAN OHJELMISTOSOVELLUKSEN SOPIMUKSELLINEN TIETOTURVARISKIEN HALLINTA PILVIPALVELUYMPÄRISTÖSSÄ

Talousoikeuden

Pro gradu -
tutkielma

VAASA 2018

SISÄLLYSLUETTELO SIVU

VAASAN YLIOPISTO

Kauppatieteellinen tiedekunta
Tekijä: Pasi Laasala
Tutkielman nimi: Terveydenhuoltoalan ohjelmistosovelluksen sopimuksellinen tietoturvariskien hallinta pilvipalveluympäristössä
Ohjaaja: Mika Kärkkäinen
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Strateginen talousoikeus
Koulutusohjelma: Talousoikeus
Aloitusvuosi: 2012
Valmistumisvuosi: 2018 **Sivumäärä:** 95

TIIVISTELMÄ

Pilvipalvelut yleistyvät nopeaa vauhtia yritysten käytössä. Palvelun käyttöön otosta on yrityksille useita hyötyjä. Se esimerkiksi mahdollistaa käyttöönottomallista riippuen sovelluksen käytön mistä tahansa internet yhteyden mahdollistavasta päätelaitteesta, laitteisto ja sovellus ovat aina käyttökunnossa sekä tietojen varmuuskopiointi ja suojaus on ajan tasalla palveluntoimittajan vastatessa niistä. Ulkopuolisen palveluntoimittajan vastatessa yritykselle arvokkaasta tiedosta, se aiheuttaa kuitenkin enemmän pohtimista yrityksessä tietoturvan sekä tiedon asianmukaisen säilytyksen varmistamisesta. Tietoturvariskit voivat liittyä henkilöstöturvallisuuteen, fyysiseen- ja laitteistoturvallisuuteen, tietoliikenneturvallisuuteen, ohjelmistoturvallisuuteen tai käyttöturvallisuuteen.

Myös terveydenhuoltoalan yritykset ovat alkaneet hyödyntämään pilvipalveluympäristöä asiakas- ja potilastietojen säilytys- ja käsittelyalustana. Koska yritysten käsittelemä tieto sisältää henkilö- sekä jopa arkaluonteisia sairaustietoja, tulee tietoturvan varmistaminen vielä tavallistakin oleellisemmaksi seikaksi. Yrityksen jonka toimipaikka sijaitsee Suomen alueella, tulee pilvipalveluita koskevissa juridisissa kysymyksissä soveltaa Suomen voimassaolevaa tietosuojalainsäädäntöä. Koska pilvipalveluissa palvelin, jolla yrityksen tietoja säilytetään voi periaatteessa sijaita missä päin maailmaa tahansa, on tietosuojan varmistamiseksi yrityksen oltava selvillä palvelimen sijainnista. Terveydenhuoltoalan yrityksissä henkilötietoja käsiteltäessä tietoja ei saa siirtää muutamia poikkeuksia lukuun ottamatta EU/ETA maiden ulkopuolisiin valtioihin.

Jotta, yritys pystyisi varmistamaan mahdollisimman hyvän tietoturvan, sen tulisi varmistua hyvästä tiedonhallintatavasta. Keskeistä on tiedon laadun säilyttäminen, tiedon saatavuus, eheys sekä tiedon suojaaminen. Laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä on säädetty ohjelmistovalmistajan yleisistä velvollisuuksista. Pilvipalveluasiakkaan vastuista on säädetty henkilötietolaissa. Pilvipalveluntoimittajan vastuuta ohjaa lähinnä lainsäädäntö, pilvipalvelusopimus sekä millä pilvipalveluntasolla toimitaan.

AVAINSANAT: Pilvipalvelu, henkilötiedot, tietoturva, pilvipalvelusopimus

1. JOHDANTO

1.1. Tutkimuskohteen kuvaus

Erilaiset tietokoneohjelmat ja niiden ohjelmistot ovat oleellinen osa meidän päivittäistä elämäämme. Aina ei tule ajatelleeksi, että kun käytämme jotain sähköistä laitetta, sen toiminnan taustalla on useimmiten ohjelmisto joka mahdollistaa laitteen toiminnan siten kun sen kuuluu. Ohjelmisto voi olla myös apuväline helpottamaan työtämme. Esimerkiksi hammaslääkärin suorittaessa asiakkaan suuntutkimusta, hän merkitsee sitä varten suunniteltuun ja valmistettuun ohjelmaan kaikki oleelliset löydökset, jotka tallentuvat sinne myös jatkossa hyödynnettäviksi tiedoiksi. Asiakkaan hammaskartat, sekä kaikki muu tarvittava terveystieto löytyy samasta ohjelmistosta. Hammaslääkärin ohjelmistoon merkitsemien tietojen pohjalta tapahtuu sitten myös lopuksi asiakkaan laskutus, jonka vastaanottovirkailija laskuttaa käynnin päätteeksi. Myöhemmillä käynneillä hammaslääkäri löytää ohjelmasta asiakkaan tiedot, joiden pohjalta hän pääsee heti tekemään omaa työtään tehokkaasti eli hoitamaan asiakkaan suun terveyttä. Ohjelmisto saattaa myös mahdollistaa sen, että myöhemmin kotona asiakas voi tarkastella omassa henkilökohtaisessa näkymässään, mitä hänelle on vastaanotolla tehty, ja mitä jatkossa tullaan tekemään.

Ohjelmistoliiketoiminnan kehittyminen alkoi 1960-luvun loppupuolella. Tällöin se alkoi kehittyä omaksi teollisuudenalakseen erillään laitekaupasta. IBM, joka oli laitekaupan markkinajohtaja, päätti eriyttää ohjelmistot laitekaupasta. Heti jo ohjelmistoliiketoiminnan alkumetreillä otettiin käyttöön erilaisia lisensointimalleja. Alkuun käytössä olivat kertarojalti sekä toimipistekohtainen rojalti. Lisenssisopimukset määrittelivät jo tuolloin varsin tarkasti ohjelmistojen käyttöoikeudet. Alkuun pääpainon ollessa liikesalaisuudessa sekä sopimusoikeudellisissa kysymyksissä. Ohjelmistojen tekijänoikeudellinen lisensointi alkoi yleistyä myöhemmin 1970-luvun loppupuolella, kun tietokoneet tulivat lähemmäksi tavallista kuluttaja-asiakasta. Uusilla massamarkkinoilla tarvittiin joustavampia ja aiempaa yksinkertaisempia lisensointimalleja. Ohjelmistoja alettiin myydä ainoastaan konekielisessä muodossa, jolla saatiin salassapito järjestettyä, sekä sopimuksiin lisättiin ”shrink-wrap”-lisenssisopimukset. Ohjelmistojen lisensointiin ei ole koskaan ollut yhtä yksittäistä mallia.[1]

[1] Välimäki 2009: 143 – 145.

Jo alkuvaiheessa tehtiin sopimuksia, joissa tekijä luopuu osasta lain suomista oikeuksistaan. Ohjelmistoliiketoiminnassa ohjelmistojen tekijöiden ongelma on ollut julkaisuprosessi, joissa kaupallinen julkaisija on ottanut suuren osan myyntituloista. Tämän vuoksi alkuvaiheessa kaikkein menestyksekkäimmäksi lisensointimalliksi nousi kokeilu versiot eli ”shareware”, joilla silloin kallis ja monimutkainen julkaisuprosessi pystyttiin ohittamaan. Kokeilu version avulla käyttäjä pääsi tutustumaan ohjelmistoon ja mikäli totesi sen käyttökelpoiseksi, tekijä myi suoraan loppukäyttäjälle täyden version käyttöoikeuden. Aiemmin ohjelmistot myytiin fyysisesti esimerkiksi levykkeellä. Fyysiseen kopioon perustuva jakelumalli ei kuitenkaan ole kaikkein tehokkain ja internetin keksimisen jälkeen ohjelmistojen myynti verkon välityksellä alkoi yleistyä. Nykyisin ohjelmistonvalmista voi ottaa palveluntoimittajan roolin ja sen lisäksi, että asiakas voi ostaa ja kopioida ohjelmiston verkon kautta hän voi ostaa tuotteen tai siihen olevan oheispalvelun verkon välityksellä. Myös ohjelmiston ylläpito, korjaukset sekä päivitysmahdollisuudet ovat olleet parantamassa ohjelmistojen käyttömukavuutta. Ohjelmiston säilytyspaikka sijaitsee nykyisin yhä useammin pilvipalveluympäristössä, jolloin sekä yksityiset ihmiset, että yritykset ovat joutuneet pohtimaan asiaa eri kantilta. Yritykselle tai yksittäiselle ihmiselle tärkeät tiedot eivät enää olekaan tallessa työpöydän alla olevassa tietokoneessa vaan ovat talletettuna konesaliin jonnekin kauas, jonka sijaintia emme useimmiten edes tiedä. [2]

Eri toimialoilla ohjelmistojen merkitys työssä korostuu eri tavoin. Jollain toimialoilla työtä tehdään täysin ohjelmiston avulla, kun taas toisilla toimialoilla esimerkiksi kädentaitojen merkitys korostuu ja ohjelmisto on esimerkiksi asiakasrekisterin ja laskutuksen apuna. Myös erilaiset tiedot, joita ohjelmistoihin tallennetaan vaihtelevat toimialasta ja ohjelmistosta riippuen. Voi olla, että joissain tapauksissa mikäli tiedot jostain syystä kadotettaisiin, merkitys yritykselle ei olisi välttämättä suuri. Toisessa tapauksessa taas, tietojen katoaminen tai vääriin käsiin joutuminen olisi suuri katastrofi, kuten esimerkiksi asiakkaan henkilökohtaisten terveystietojen vuotaminen.

Sekä yksityiselle että yrityskäyttäjälle tietoturva on tärkeä asia. Tuskin kukaan yksityinen tietokoneen käyttäjä haluaa, että hänen henkilökohtaiset kirjoittamansa tekstit, valokuvat tai videot joutuvat toisten käyttäjien haltuun. Yrityskäyttäjälle se, että tiedot päätyvät kilpailijan tai jonkun muun luvattoman käyttäjän haltuun saattaa olla suuri liiketaloudellinen riski. Tämän vuoksi tietokoneiden käyttäjät pyrkivät turvaamaan oman tieto-omaisuutensa erilaisilla menetelmillä, kuten esimerkiksi salasanoilla, palomuureilla ja virustorjuntaohjelmilla. Perinteisesti informaatio tallennetaan

[2] Välimäki 2009: 145 – 146.

kovalevylle, joka sijaitsee joko koneessa itsessään kiinteästi tai sitten irrallisena informaation tallennus välineenä. Nämäkin ovat riskialttiita esimerkiksi vaurioitumisille ja katoamiselle. Yksityisellä tai yrityskäyttäjällä tulisikin olla suunniteltuna järjestelmä, jolla hän saa säännöllisesti varmuuskopioitua informaatio-omaisuutensa, mikäli alkuperäiselle tallennusvälineelle sattuu jokin vahinko. Yhdysvalloissa vuosittain katoaa lentoasemilla yli 12 000 kannettavaa tietokonetta. Läheskään kaikissa ei varmastikaan ole suojattu kovalevyä siten, että ulkopuolinen ei pääsisi tietoihin käsiksi. Tämä saattaa olla etenkin yrityskäyttäjälle suuri vahinko.[3]

Ohjelmiston sijaitessa pilvipalvelussa, se asettaa tietosuojalle ja tietoturvalle isoja vaatimuksia. Eu:n tietoturvavirasto on varoittanut julkaisemassaan raportissa, että verkkorikolliset ottavat tulevaisuudessa pilven maalitaulukseen. Pilvipalvelut ovat valtavan kokoisia datavarastoja ja sellaisenaan kiinnostavia kohteita rikollisille. Raportin mukaan pilvikonesalin virtualisoidut palvelimet ovat samalla tavoin alttiita rikollisten iskuille, kuin fyysisetkin palvelimet. [4] Yritys, joka käyttää ohjelmistoa esimerkiksi henkilö- ja potilastietojen keräämiseen, täytyy pohtia jo ohjelmistoa tilatessaan tietosuoja ja –turva asioita. Suurin vastuu tietosuojavuodoissa on pilvipalveluasiakkaalla, mutta on tärkeää ohjelmiston valmistajankin osalta tehdä kaikki voitava tietoturva-asioiden turvaamiseksi. Tämän vuoksi on ohjelmistoyrityksen riskienhallinnan kannalta välttämätöntä varautua mahdollisiin ongelmatilanteisiin ennakolta. Ohjelmistoyritysten on vaikea kattaa yrityksen päivittäisessä toiminnassaan syntyneitä toiminnallisia riskejä vakuutuksin, tai ainakin se on hyvin kallista. Tämän vuoksi sopimusoikeuden keinot ovat tärkeä työkalu ohjelmistoalan yritysten riskienhallintaan. Tietokoneohjelmiston toimitussopimus on sinänsä poikkeuksellinen sopimustyyppi, että ohjelmiston toimittaja ei yleensä ota mitään vastuuta ohjelmiston toimivuudesta tai sen seurauksista ohjelmiston loppukäyttäjälle. [5]

Käsiteltäessä suurta määrää jopa salassa pidettävää ja arkaluonteista tietoa, nousee hyvä tiedonhallintatapa keskeiseen asemaan. Hyvän tiedonhallintatavan keskeisiä seikkoja ovat tiedon laadun säilyttäminen, asiakirjojen ja tiedon saatavuuden turvaaminen, käytettävyys, tiedon eheys sekä suojaaminen eri riskeiltä. Etenkin pilvipalveluasiakkaan

[3] Velte & Velte & Elsenpeter 2010: 38.

[4] Saarenpää 2014: 44 – 47.

[5] Välimäki & Laine, 2004.

tulee huolehtia, että kaikessa toiminnassaan huomio hyvän tiedonhallintatavan periaatteet. [6]

Riskienhallinta on nykypäivänä yritykselle tai yhteisölle yksi tärkeistä liiketoimintaa turvaavista asioista. On tärkeää varautua ennakolta tilanteisiin, jotka voisivat uhata ja pahimmassa tapauksessa lamauttaa jopa lopullisesti yrityksen tai yhteisön liiketoiminnan. Kartoittamalla ennakolta asiat joista riskejä voi aiheutua, sekä pyrkimällä ennakolta suojaamaan toimintaansa kaikin mahdollisin keinoin, voidaan pitää riskitilanteista aiheutuvat vahingot mahdollisimman pieninä. Sopimuksellisella riskienhallinnalla tarkoitetaan sitä, että pyritään esimerkiksi ennalta laadituin sopimuksin rajoittamaan korvausvastuut vahinkotilanteissa mahdollisimman pieneksi. Ennalta laadituin sopimuksin, voidaan myös pyrkiä rajoittamaan esimerkiksi tietoturvariskien mahdollisuutta, asettamalla riittävän selkeät ja korkeat sanktiot, mikäli on huolimattomalla toiminnallaan aiheuttamassa tietototurvariskin. [7]

Terveydenhuollon ja sairaanhoidon alalla on käytössä ohjelmistoja joihin tallennetaan asiakkaan tai potilaan henkilö – ja sairaustietoja. Näiden tietojen katoaminen tai vuotaminen vääriin käsiin olisi suuri ongelma. Tämän vuoksi ohjelmistovalmistajat ovat kehittäneet erilaisia varmennuksia, jotta tietoihin pääsisi käsiksi vain niihin oikeutetut henkilöt. Asiakkaan tai potilaan ollessa hoidossa on tärkeää, että tiedot saadaan nopeasti ja luotettavasti niitä tarvitseville. Tärkeää on myös, että tietoihin eivät pääse käsiksi ne jotka eivät ole siihen oikeutettuja. Tietojen toimitusvarmuus on myös oleellinen seikka arvioitaessa ohjelmiston toimivuutta käytännössä. Tiedot pitäisi olla käytettävissä siellä missä niitä tarvitaan, jotta informaation hyödyntäminen olisi optimaalista.

Yritykset ja organisaatiot tarvitsevat tietotekniikkaa ja sen mahdollistavia palveluita toiminnassaan. Tämä on tehnyt niistä entistä haavoittuvampia turvallisuutta uhkaaville tekijöille. Yksityisten ja julkisten organisaatioiden verkkoja on yhdistetty keskenään, tietojenkäsittelyä on hajautettu sekä palveluita ulkoistettu. Nämä tekijät ovat heikentäneet organisaatioiden mahdollisuuksia valvoa tietoturvallisuuttaan tehokkaasti. Erilaisilla teknisillä seikoilla saadaan parannettua tietojen koskemattomuutta, mutta kuitenkin silläkin on rajansa ja teknisiä ratkaisuja onkin tuettava erilaisilla hallinnollisilla toimenpiteillä. Näitä toimenpiteitä ovat esimerkiksi yritysten

[6] Mäenpää 2008: 163 – 170.

[7] Suominen 2003: 72 – 73.

toimintatapojen muuttaminen, turvaohjeiden laatiminen, henkilöstön kouluttaminen, toiminnan vakuuttaminen sekä erilaisilla juridisilla keinoilla suojaaminen. [8]

Yhä useampi tietokoneen käyttäjä käyttää pilvipalveluita tiedon tallennuspaikkana. Osa käyttäjistä ei itse ehkä tietoisesti ajattele käyttävänsä pilvipalveluita, kun tallentaa esimerkiksi valokuvia sosiaalisen median, kuten esimerkiksi Facebookin sivuille ystäviensä nähtäväksi. Monet yksityiset tietokoneen käyttäjät tallentavat tiedostojaan, valokuviaan tai videoitaan jo pilviympäristöön sitä varten hankkimaansa palveluun. Pilvipalvelut myös yritysten käytössä ovat viime vuosina lisääntyneet. Hammaslääkäriketju jolla on useita asemia, tarvitsee jokaisella vastaanotolla ohjelmiston joka on helpottamassa hammasalan asiantuntijoiden työtä. Asiakkaasta ohjelmistoon tallennetut tiedot tulee olla käytettävissä kaikilla ketjun vastaanotoilla, jotta asiakkaan tehokas hoito voidaan mahdollistaa. Tällöin asiakas pystyy valitsemaan ketjun kaikista ammattilaisista juuri sen, jonka asiantuntemusta hän tarvitsee sillä hetkellä. Useinkaan, eivät kaikki tarvittavat ammattilaiset pidä vastaanottoa juuri sillä hammaslääkäriasemalla. Hammasalan ammattilaiset eivät kuitenkaan välttämättä ajattele tai tiedä, että tiedot joita he ohjelmistoon hoitoa toteuttaessaan tallentavat, tallentuu usein nykyään pilvipalveluun.

Pilvipalvelut tarkoittavat, että yritys hankkii verkon välityksellä palveluntoimittajan IT-resursseja. Tällöin yrityksen käytössä on lähes rajattomasti laskentatehoa, ilman että yrityksen täytyy sitoa siihen mittavia pääomainvestointeja. Pilvipalveluiden avulla pienemmätkin yritykset tavoittavat suurempia markkinoita pienemmillä kustannuksilla. [9] Yritys voi hankkia käyttöönsä esimerkiksi palvelimen, joka sijaitsee palveluntoimittajan konesalissa tai ohjelmiston, joka on konkreettisesti palveluntoimittajan palvelimella. Palveluntoimittaja vastaa ja huolehtii ohjelman toimivuudesta sekä yleensä myös varmuuskopioinneista ja virussuojauksista sekä muista ohjelmiston turvalliseen ja luotettavaan käyttöön vaikuttavista seikoista. Yritys, joka on palveluntoimittajalta nämä palvelut hankkinut, pääsee ohjelmistoon käsiksi mistä tahansa laitteelta josta on pääsy internet- verkkoon. Pilvitoimintamallissa on perimmältään kyse yritysten kannalta taloudellisuudesta sekä kyvystä mukautua muutoksiin. [10]

[8] Suominen 2003: 79.

[9] Komission tiedonanto pilvipalveluiden potentiaalisesta käytöstä Euroopassa, KOM 2012, 529 lopullinen.

[10] Heino 2010: 20 – 22.

Pilvipalvelua harkitessaan yrityksen on ensin päätettävä, mikä käyttöönottomalli soveltuu sille parhaiten. Näitä ovat public cloud, private cloud, hybrid cloud sekä intercloud. Tämän jälkeen yritys voi hankkia pilvipalveluntoimittajalta pilvipalvelun kolmesta eri palvelumallista joita ovat Saas, Paas tai Iaas. Palvelumallit eroavat niiden toteutustavan perusteella. Millaisen pilvipalvelun yritys pilvipalveluntoimittajalta hankkii, riippuu yrityksen tarpeista sekä tarvittavista resursseista tiedonhallintakapasiteetin suhteen. [11]

Pilvipalveluiden käyttö tuo yritykselle useita juridisia haasteita. Ongelmana on, että nykyinen lainsäädäntö on hankalasti sovellettavissa pilvipalveluihin. Palveluiden käytössä esiin nousevat etenkin pilvipalveluiden tietosuojaa sekä tietoturvaa koskevat seikat. Tärkeitä pohdittavia asioita ovat myös sopimusoikeudelliset vastuut sekä liikesalaisuuksien suojaa koskevat kysymykset. Yrityksen, jonka toimipaikka on Suomen alueella, pilvipalveluita koskevissa juridisissa kysymyksissä sovelletaan Suomen tietosuojalainsäädäntöä. Suomessa tietosuoja on perustuslaillinen oikeus, joka pohjaa perustuslain 7 ja 10 §:ään. Perustuslaissa 7 §:ssä säädetään oikeudesta henkilökohtaiseen vapauteen ja koskemattomuuteen. Yksityiselämän suojasta säädetään perustuslain 10 §:ssä. Siinä mainitaan että,

> *”kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton”.* [12]

Lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) mukaan, tarkoituksena on edistää sähköisiä palveluita sekä niiden tietosuojaa ja tietoturvaa. [13] Pilvipalveluidentoimittajan on rakennettava palvelunsa siten, että palvelunasiakas voi luottaa tietoturvan ja yksityisyyden suojan säilyvän koskemattomana. Vastaavasti palveluntoimittajan on voitava luottaa siihen, että pilvipalveluasiakas on se joka väittää olevansa. Henkilötietolain (523/1999) tarkoituksena, on

> *”toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista”.* [14]

[11] Heino 2010:56 – 57.

[12] Järvinen 2012: 6 – 7.

[13] HE 125/2003

[14] Järvinen 2012: 6-7.

Pilvipalveluissa palvelin, jolle tiedot on tallennettu saattaa sijaita missä päin maailmaa tahansa. Toimialoilla, joilla on säädetty missä tallennetut tiedot voivat sijaita, tällä voi olla iso merkitys. Esimerkiksi pilvipalvelunasiakkaan, joka tallentaa rekisteriinsä asiakkaiden tai potilaiden henkilötietoja tulee olla selvillä missä palvelin sijaitsee. Henkilötietolain mukaan henkilötietoja ei saa siirtää muutamia poikkeuksia lukuun ottamatta EU/ETA maiden ulkopuolisiin valtioihin.

Pilvipalveluympäristössä toimittaessa tietoturvariskit ovat merkittävä huomioitava seikka. Tietoturvariskit on luokiteltu eri riskitekijöihin joita ovat henkilöstöturvallisuus, fyysinen- ja laitteistoturvallisuus, tietoliikenneturvallisuus, ohjelmistoturvallisuus sekä käyttöturvallisuus. Yrityksen hankkiessa ohjelmiston sekä käyttäessään sitä pilviympäristössä sen täytyy pohtia eri riskitekijöitä sekä arvioida niiden vaikutusta yrityksen tietoturvallisuuden kannalta. [15]

Keväällä 2016 Euroopan parlamentti sekä neuvosto julkaisivat yleisen tietosuoja-asetuksen (2016/679 EU). Tällä asetuksella kumotaan EU:n aiemmin julkaisema henkilötietodirektiivi (95/46/EY), joka on Suomessa laitettu voimaan henkilötietolailla (523/1999). Tämä tietosuoja-asetus tulee voimaan tänä keväänä 25.5.2018 kahden vuoden siirtymäajan jälkeen, ja asetus jättääkin kansallisille lainsäätäjille jonkun verran liikkumatilaa asetuksen täsmentämiseen sekä täydentämiseen. Suomessa Oikeusministeriö asetti työryhmän pohtimaan sekä valmistelemaan lainsäädäntöehdotusta liikkumatilan käytöstä. Työryhmä ehdottaa, että nykyinen henkilötietolaki kumotaan, ja säädetään uusi tietosuojalaki, jonka tarkoituksena on täydentää sekä täsmentää yleistä tietosuoja-asetusta. Tämän lain pitäisi tulla myös voimaan 25.5.2018. Terveydenhuoltoalan sovellusten käyttöön liittyvään henkilötietojen turvaan, nykyisillä muutoksilla ei ole suurta merkitystä. Henkilötietojen säilytys ja käyttö on jo ennestään varsin vahvasti säädeltyä. Pilvipalveluiden yleistyminen myös terveys- ja sosiaalipuolen ohjelmistoissa asettaa tietenkin vaatimuksia tietovarastojen säilytyspaikalle sekä tietojen yleiselle käsittelylle.

Pilvipalveluympäristössä toimiessa pilvipalvelusopimus on yleisimmin käytetty sopimustyyppi. Kuten usein IT-alan sopimuksissa, myös pilvipalveluympäristössä käytetään usein vakiosopimusehtoja. IT2015 yleiset sopimusehdot ja erityisehdot pilvipalveluympäristöön sekä JIT2015 vakiosopimusehdot ovat yleisimmin Suomessa käytetyt riippumattoman toimesta laaditut vakiosopimus ehdot. Lisäksi monilla ohjelmistovalmistajilla saattaa olla käytössään itse yksilöllisesti laaditut sopimusehdot,

[15] Paavilainen 1998: 26.

jotka kyllä useimmiten pohjautuvat IT- ja JIT sopimusehtoihin. [16] Vakiosopimusehdoissa on jo ennalta tarkoin pohdittu yleisimpiä pilvipalveluihin liittyviä ongelmia, ja luotu niiden pohjalta yleiset- sekä erityissopimusehdot. Kuitenkin, yritysten tai organisaatioiden on tärkeää tutustua tarkoin näihin sopimusehtoihin ja tarvittaessa täydentää niitä omin yksilöllisin ehdoin, mikäli se sopimusneuvotteluissa on mahdollista.

1.2. Tutkimusongelma ja aiheen rajaus

Tässä pro gradu tutkielmassa tarkoituksenani on tutkia ohjelmistovalmistajan, pilvipalveluasiakkaan sekä pilvipalveluntoimittajan vastuuta ja velvollisuuksia sekä riskien hallinnan keinoja mahdollisten tietoturvariskien kannalta pilvipalveluissa. Tarkoituksena on myös selvittää kuinka ennakolta pilvipalvelusopimuksen avulla pystytään suojautumaan mahdollisiin tietoturvaa uhkaaviin tilanteisiin terveydenhuolto-alan ohjelmistoa käytettäessä pilviympäristössä. Viime aikoina on markkinoille tullut terveyden – ja sairaanhoidon sektorille suunnattuja ohjelmistoja, jotka toimivat pilviympäristössä. Näin ollen yhä enenevässä määrin asiakas – ja potilastietoja tallennetaan pilveen. Yritysten ja eri organisaatioiden täytyy jo ennakolta varautua erilaisiin riskeihin, joita tietoturvan vaarantuminen saattaa olla aiheuttamassa. Näillä riskeillä saattaa olla hyvin merkittävät vaikutukset yrityksen tai organisaation toiminnalle.

Tutkielmassa en käsittele kaikkia ohjelmistotuotannossa esiin tulevia riskejä, riskien hallinnan keinoja enkä ohjelmistovalmistajan vastuita, vaan keskityn pilvipalveluiden kannalta oleellisimpiin riskitekijöihin sekä riskien hallintakeinoihin. Näistä esiin nousevat erityisesti tietoturvariskit ja niihin suojautuminen.

1.3. Tutkimuksen lähteet

Käytän tässä tutkielmassa lähteinä oikeustieteellistä kirjallisuutta. Tärkeimpinä lähteinä ovat Petteri Heinon *Pilvipalvelut – cloud computing,* Jouni Paavilaisen *tietoturva*, Rauno Korhosen *Perusrekisterit ja tietosuoja*, Arto Ylipartasen *Tietosuoja terveydenhuollossa, potilaan asema ja oikeudet henkilötietojen käsittelyssä,* Soile Pohjosen toimittama *Ennakoiva sopiminen, Liiketoimien suunnittelu, toteuttaminen ja*

[16] Erlund, Lindfors, Salminen & Turunen 2016: 31 – 37.

riskien hallinta, sekä Erlundin, Lindforsin, Salmisen ja Turusen *IT 2015 käytännön käsikirja.* Lisäksi tutkielmassa on käytetty lähteinä oikeustieteellisiä artikkeleita ja Oikeusministeriön mietintöä koskien EU:n yleisen tietosuoja-asetuksen täytäntöönpanoa.

1.4. Tutkimuksen rakenne

Johdantokappaleen jälkeen toisessa kappaleessa tarkastelen ensin pilvipalvelua yrityksen toimintaympäristönä. Seikka, että yritys säilyttää sille oleellisesti tärkeää tieto-omaisuutta toisen yrityksen hallinnoimilla laitteilla sekä sen tiloissa tekee toimintaympäristöstä ehkä hieman uudenlaisen ja asettaa yritysten väliselle luottamukselle sekä tietoturvallisuudelle uudenlaisia haasteita. Tämän jälkeen tarkastelen ohjelmistotoimituksen eri tietoturvariskejä pilvipalveluympäristössä toimittaessa. Pilvipalvelut lisääntyvät yritysten käytössä jatkuvasti, mutta se myös aiheuttaa yrityksille huolenaihetta etenkin tietoturvaan ja tietosuojaan liittyvissä asioissa. Yritykset tallentavat arkaluonteisia henkilö – tai potilastietoja tietoliikenneyhteyksien välityksellä palvelimille, jotka saattavat sijaita fyysisesti hyvinkin kaukana. Palvelimet saattavat olla toisen yrityksen hallussa heidän konesalissaan, jolloin yksi ylimääräinen osapuoli tietorekisterin ylläpito ketjussa aiheuttaa luonnollisesti epäilyjä tietosuoja rikkomuksen mahdollisuudesta. Tarkoituksena on tutkia kenen vastuulla on tietojen koskemattomuuden säilyminen. Mitä jos tietosuojavuoto tapahtuu, kenen on vastuu ja mitkä ovat seuraamukset?

Kolmannessa kappaleessa käsittelen terveydenhuollon ohjelmistotoimitukseen liittyen tietoturvariskien vastuiden ja velvollisuuksien jakautumista ohjelmistovalmistajan, pilvipalveluasiakkaan sekä pilvipalveluntoimittajan kesken. Terveydenhuoltoalalla potilastietojen säilyttäminen asettaa tiettyjä ehtoja sovelluksen toiminnalle. Missä henkilö – ja potilastiedot tulee säilyttää? Yrityksen täytyy olla selvillä pilviympäristön sijainnista, koska ilman muutamaa poikkeusta Suomesta ei saa henkilötietoja siirtää EU/ETA maiden ulkopuolelle. Tässä kappaleessa tarkastelen normeista pakottavia, jotka ohjelmistovalmistajan ja pilvipalveluasiakkaan tulee tietää, sekä myös dispositiivisia normeja, joilla yritys voi turvata ennakolta mahdollisten tietoturva tai tietosuoja rikkomusten varalta.

Neljännessä kappaleessa tarkastelen riskienhallintaa. Yrityksen tai yhteisön toiminnalle saattaa ilmaantua erilaisia riskejä joko oman toiminnan tai ulkopuolisten toiminnan johdosta. Tämän vuoksi onkin tärkeää, että ennakolta pyrittäisiin kartoittamaan

mahdolliset riskitekijät ja –tilanteet, sekä luomaan toimintatavat joilla pyrittäisiin suojautumaan ennakolta liiketoimintaa uhkaavilta riskeiltä. Tietoturvaa uhkaavia tekijöitä on useita, ja kaikkiin mahdollisiin tilanteisiin on yrityksen tai yhteisön todella haastavaa suojautua ennakolta. Kuitenkin, yksi tärkeä tietoturvariskejä ennakolta suojaava tekijä on sopimuksellinen riskienhallinta, jossa tarvittavat sopimukset ennakolta kaikkien osapuolten kesken laatimalla, voidaan pyrkiä rajoittamaan tietoturvariskien mahdollisuutta. Kaikkien osapuolten ollessa tietoisia vastuista ja velvollisuuksista tietoturvaan liittyen, saattaa olla rajoittamassa väärinkäytösten mahdollisuutta.

Viidennessä kappaleessa käsittelen yleisimpiä sopimuksia IT-alalla painottuen pilvipalvelusopimukseen. IT-alalla käytetään paljon vakiosopimusehtoja, ja myös pilvipalveluympäristössä tämä on tyypillisin sopimustyyppi. Ohjelmistotoimittaja voi laatia yksin tai yhdessä asiakkaan kanssa käytettävän sopimuksen, mutta Suomessa on hyvin tyypillistä käyttää valmiita vakiosopimusehtoja. IT2015 sekä JIT2015 ovat käytetyimmät vakiosopimusehdot. Näitä ehtoja täydennetään laadittaessa sopimusta, erityisehdoilla tai sitten täysin yksilöllisillä sopimusehdoilla.

Viimeinen kappale on johtopäätökset, jossa pyrin pohtimaan pilvipalveluympäristön tietoturvariskien nykytilaa sekä tulevaisuutta. Tietotekniikan ja pilviympäristön nopea tekniikan kehittyminen aiheuttaa myös oikeudellisesti suuria haasteita ja viimeisessä kappaleessa pyrin myös tuomaan esiin myös tämän hetkisen lainsäädännön tilan sekä valottamaan mitä toimenpiteitä on tulossa, jotta ehkä hieman sekavaa ja ongelmallistakin toimintaympäristöä pystyttäisiin selkeyttämään.

2. TERVEYDENHUOLTOALAN OHJELMISTON TIETOTURVARISKIT PILVIPALVELUYMPÄRISTÖSSÄ

2.1. Pilvipalvelut

Pilvipalvelut tarkoittavat yleiskielessä internetistä hankittua tietoteknistä kapasiteettia, sovelluksia tai muita palvelusuoritteita. Se koostuu sekä uusista palveluista, että myös uudenlaisesta toimintatavasta. Yritys solmii sopimuksen pilvipalveluntoimittajan kanssa etukäteen määritetyistä palvelusuoritteista. Pilvipalveluissa voidaan halutessaan jopa luopua fyysisistä konesaleista ja näin vähentää yrityksen tarvetta sijoittaa tietoteknisiin laitteisiin pääomaa. [17]

Yritys voi valita ottaakseen pilvipalvelut käyttöön neljästä eri käyttöönottomallista sopivimman:

1. Public cloud

2. Private cloud

3. Hybrid cloud

4. Intercloud

Public cloud on internetyhteyden kautta käytettävä pilvipalvelukoneisto. Siinä palvelua tarjoava yritys vastaa pilvikoneistossa olevien laitteiden ylläpidosta ja kustannuksista. Asiakasyritys saa jaetusta pilviympäristöstä kapasiteettia ilman omaa dedikoitua laitteistoa tai kapasiteettia. Pilvipalveluntoimittaja järjestää tarvittavat osoite- ja nimipalveluresurssit. Asiakasyrityksen omasta verkosta kuljetaan pilvipalveluun useimmiten salatun VNP-tyyppisen yhteyden kautta. Asiakasyritys maksaa palvelusta, mutta ei mitään fyysisistä laitteista tai ohjelmistoista. [18] Taloudellisesti ajatellen etenkin pienen yrityksen kannalta on järkevää valita public cloud käyttöönottomalli. Sen käyttöönotto tuo lähes välittömästi organisaatiolle säästöä ja tehostaa IT-puolen toimintaa. Jaettu infrastruktuuri, lähes taattu toimintavarmuus ja tiedon säilytyksen turvallisuus ovat asiakasorganisaatiolle suuri etu.[19] Yritys ja pilvipalveluntoimittaja

[17] Heino 2010: 34.

[18] Heino 2010: 54 – 55.

[19] Krutz & Vines 2010: 45.

solmivat palveluista yleensä sopimuksen. Sopimukseen yleensä sisällytetään palvelukuvaukset, joista selviää mitä sovittuun palveluun sisältyy ja mitkä ovat asiakkaana olevan yrityksen ja mitkä pilvipalveluntoimittajan vastuut. Pilvipalveluntoimittaja sisällyttää useimmiten tarjoamaansa palvelutasoa koskevan sopimuksen (Service level agreement eli SLA). Mikäli SLA sopimusta ei ole, ei ole useimmiten olemassa mitään sopimuksellista lupausta palvelun toiminta-ajoista, palveluntoimittaja järjestämien huoltokatkojen maksimipituuksista tai vikatilanteessa korjauksiin vievän ajan maksimikestosta. [20] *Private cloud* on yrityksen oman LAN – lähiverkon tai muutoin järjestetyn luotettavan verkon kautta käytettävä pilvipalvelu. Tällöin ei erillistä tietoliikenneyhteyttä tarvita. Yritys organisoi ja omistaa itse pilvipalvelukoneiston kaikkine ylläpitoprosesseineen ja vastaa täten itse myös kustannuksista. Tämän mallin ajatellaan mahdollistavan tehokkaan it-resurssien käytön yrityksessä ja siten myös paremman hyötysuhteen yrityksen investoinnille. Sen ajatellaan tarjoavan parempaa palvelua käyttäjille esimerkiksi uusien palveluiden nopeamman käyttöönoton myötä. [21] Tässä mallissa yritys ei jaa infrastruktuuriaan minkään muun ulkopuolisen organisaation kanssa. Järjestelmään voivat kuulua kaikki yrityksen toimipisteet, liikekumppanit, jälleenmyyjät tai kaikki ne, joilla on jotain yhteistyötä yrityksen kanssa. [22] *Hybrid cloud* on private – ja public cloudin yhdistelmä. Asiakas yritys yhdistää oman private cloudin pilvipalveluntoimittajan tekniseen ympäristöön internetyhteyden kautta. Tämän käyttöönottomallin uskotaan lisäävän suosiotaan lähivuosina. [23] Hybrid Clouds voi olla tehokas yhdistelmä silloin, kun molemmat pilvityypit sijaitsevat samassa järjestelmässä. [24] *Intercloud* on kaikkien pilvien yhdistelmä. Tässä verkkomallissa yksittäinen pilvi voi tarpeen vaatiessa käyttää toisten pilvien resursseja hyväkseen. Tällöin voitaisiin puhua lähes rajattomasta kapasiteetista. [25]

Pilvipalvelut voidaan luokitella kolmella eri palvelumallilla teknisen toteutustavan perusteella. Nämä ovat sovellukset palveluna (SaaS), sovellusalusta palveluna (PaaS)

[20] Heino 2010: 34 – 36.

[21] Heino 2010: 55 – 56.

[22] Krutz & Vines 2010: 48.

[23] Heino 2010: 56.

[24] Krutz & Vines 2010: 49.

[25] Heino 2010: 56 – 57.

sekä infrastruktuuri palveluna (IaaS). Palvelun toteutustapa kertoo, minkälaisia funktioita pilvipalvelusta saadaan ja miten kyseessä olevaan koneistoon liitytään.

SaaS- tyyppisessä pilvipalvelussa yritys hankkii itse vaan pelkän sovelluksen. Tämä sovellus jaetaan tietoliikenneyhteyden välityksellä loppukäyttäjän selaimelle. Pilvipalveluntoimittaja huolehtii ja vastaa kaikesta muusta. Tämän tyyppisen pilvipalvelun hyötyjä on myös se, että pilvipalveluntoimittajalla on todennäköisesti kokemusta vaikeista sovellusten ylläpitoa koskevista suoritteista. [26]

PaaS- tyyppisessä pilvipalvelussa pilvipalveluntoimittajalla on virtuaalinen palvelinympäristö. Asiakkaalle lohkotaan palvelinympäristöstä palveluita hänen toivomustensa mukaan. Tämä sopii parhaiten asiakkaalle joka pystyy itse rakentamaan haluamansa sovellukset. Paas koneiston käyttö tuotantosovellusten käyttämiseen ei onnistu automaattisesti. [27]

IaaS-tyyppisessä pilvipalvelussa pilvipalveluntoimittajalla on internetissä yksi tai useampi virtuaalinen konesali. Näistä hän lohkoo asiakkaille etukäteen määriteltyjä sekä hinnoiteltuja osioita. Asiakas voi tähän hankkimaansa lohkoon perustaa tarvitsemansa käyttöjärjestelmän sekä asentaa sen päälle tarvitsemansa sovellukset. Tämän tyyppinen pilvipalvelu soveltuu asiakkaalle jolla on osaamista toiminnan aloittamiseksi sekä ylläpitämiseksi. [28] Perinteisesti yrityksen tietotekniikka infrastuktuurin kustannukset ovat olleet merkittäviä. Ostamalla vaadittavat laitteet yritys on kuluttanut jo merkittävän osan resursseistaan. Ostamalla palvelintilaa pilvipalveluntoimittajalta yrityksellä on käytössään aina vaadittava määrä kapasiteettia nykyaikaisimmalla tekniikalla. [29]

2.2. Ohjelmistotoimituksen riskit pilvipalveluissa

Kun asiakas hankkii ohjelmistotoimittajalta sovelluksen joka asennetaan pilvipalveluun, on hyvä kartoittaa mahdolliset riskitekijät. Salon [30] mukaan yleisimmät riskit pilvipalvelussa ovat;

[26] Heino 2010: 53.

[27] Heino 2010: 51.

[28] Heino 2010: 52 – 53.

[29] Krutz & Vines 2010: 42.

[30] Salo 2010: 71.

1.Tallennetut tiedot päätyvät yleiseen jakeluun.

2. Pilvipalvelun työntekijä tai joku muu ulkopuolinen pääsee käsiksi tietoihin, sovellukseen tai alustaan.

3. Pilvipalvelun työntekijä tai joku muu ulkopuolinen manipuloi tietoja, sovellusta tai alustan toimintaa.

4. Pilvipalvelu ei toimi odotetusti ja siitä riippuvainen liiketoimintaprosessi häiriintyy.

5. Pilvipalvelu ei toimi odotetusti ja siellä olevat tiedot, sovellus tai alusta ei ole käytössä.

6. Pilvipalveluntoimittajalle tulee vakava ongelma ja siellä olevat tiedot, sovellus tai alusta ei ole enää koskaan käytössä.

7. Pilvipalveluntoimittajalle tulee vakava ongelma jolloin pilvessä olevat tiedot, sovellus tai alusta häviää pysyvästi.

2.2.1. Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan yrityksen henkilöstöön liittyvien tietoturvariskien hallintaa. Se on erittäin tärkeä osa yrityksen tietoturvallisuuden hallintaa, koska henkilöstö on yrityksen turvallisuuden suurin riskitekijä. Yrityksen oma henkilöstö saattaa aiheuttaa toimillaan uhan tietojen eheyden, luottamuksellisuuden tai käytettävyyden kohdalla. Henkilöstöturvallisuus sisältää yrityksen henkilöstön sekä vierailijoiden toiminnan tarkkailun ja valvonnan. Suurin osa yrityksen henkilöstön aiheuttamista tietoturvavahingoista on tahattomia. Tahallisten vahinkojen osuus on kuitenkin yllättävän suuri, ja riski niille kasvaa yritysten siirtyessä pilviympäristöön tietojensa säilyttämisessä. [31]

Yrityksen henkilöstön aiheuttamien tietoturvariskien ehkäisemiseksi on henkilöstön koulutus sekä yrityksen yleinen ilmapiiri, kuinka tietoturvallisuuteen on yrityksessä panostettu, tärkeässä asemassa. Osa ihmisistä saattaa virhetilanteissa reagoida tilanteisiin epänormaalilla tavalla, jolloin hän pyrkii hätäisesti korjaamaan tekemänsä virheen. Tämä harkitsematon toiminta voi olla aiheuttamassa tietoturvallisuudelle enemmän haittaa, kuin hänen tekemänsä alkuperäinen virhe olisi aiheuttanut. Kouluttamalla yrityksen henkilöstöä ongelmatilanteiden varalle, voidaan vähentää

[31] Paavilainen 1998: 87 – 89.

huolimattomuudesta tai hätäisesti paniikissa tehtyjä virheitä, jotka voisivat vaarantaa yrityksen tietoturvallisuuden. [32]

Yrityksen henkilöstön vaihtuvuus on yksi merkittävimmistä riskitekijöistä yrityksen tietojen vuotamiselle. Mikäli avainhenkilö siirtyy kilpailijan palvelukseen, vuotaa aina jonkin verran yrityksen toiminnalle tärkeää tietoa hänen mukanaan. Usein tärkeiden avainhenkilöiden siirtymisen rajoittamiseksi työsopimukseen onkin sovittu kohdasta, jossa kielletään henkilön toimimisen samalla toimialalla seuraavien 3 – 5 vuoden aikana. Silloin kun työntekijä erotetaan tehtävistään, tietoturvariskin mahdollisuus on vieläkin suurempi. Tyytymätön tai jopa kostonhaluinen erotettu työntekijä saattaa ryhtyä toimiin, joilla hän aiheuttaa vaaraa yrityksen tietoturvallisuudelle. Sopimattomasta menettelystä elinkeinotoiminnassa (1061/1978) 4 §:ssä on säädetty liikesalaisuuksien suojasta. Lain mukaan henkilö joka elinkeinoharjoittajan palveluksessa ollessaan on saanut tiedon liikesalaisuudesta, ei saa sitä palvelusaikanaan käyttää siten, että siitä aiheutuu itselle etua tai pyrkiäkseen vahingoittamaan toista. Rikoslain 30 luvussa 4 - 6 §:ssä säädetään rangaistavaksi yritysvakoilu ja yrityssalaisuuden rikkominen sekä yrityssalaisuuden väärinkäyttö. [33]Yrityksen onkin tärkeää huolehtia välittömästi erotetun työntekijän kulkulupien takavarikoimisesta sekä käyttäjätunnusten lakkauttamisesta. Tietoturvallisuus riski on olemassa, mikäli yrityksessä ei enää työskentelevien tilapäisten tai erotettujen työntekijöiden käyttäjätunnukset jäävät järjestelmään roikkumaan mahdollistaen järjestelmään tunkeutumisen. [34]

Uutta työntekijää yritykseen palkatessaan, yrityksen on hyvä pyrkiä arvioimaan tulevan työntekijän luotettavuus, mikäli hän tulee työskentelemään arkaluonteisen yritykselle arvokkaan tiedon parissa. Yritys voi pyytää hakijan suostumuksella poliisilta turvallisuusselvityksen, jos hakijaa ollaan valitsemassa tehtävään jossa hänen toimenkuvaansa sisältyy esimerkiksi arkaluonteisten tietojen käsittelyä. Laissa ei ole erikseen määritelty tehtäviä, joissa toimivista henkilöistä turvallisuusselvitys voidaan tilata.[35] Poliisilta tilattava turvallisuusselvitys voidaan tehdä suppeana, perusmuotoisena tai laajana, riippuen siitä millaiseen tarkoitukseen henkilöä ollaan rekrytoimassa. Suppean turvallisuusselvityksen voi tehdä paikallisviranomainen, mutta

[32] Paavilainen 1998: 91 – 92.

[33] HE 48 / 2008.

[34] Paavilainen 1998: 92 – 93.

[35] Paavilainen 1998: 92.

perusmuotoinen ja laaja turvallisuusselvitys tulee tilata suojelupoliisilta. Suppeita ja perusmuotoisia selvityksiä voidaan tehdä yrityksille, mutta laajoja on mahdollista tehdä vain viranomaisten pyynnöstä. Suomessa on säädetty laki turvallisuusselvityksistä. Se on astunut voimaa 8.3.2002. Hallituksen esityksessä 57/2013 oli tavoitteena uudistaa lakia ja edistää etenkin yritys- sekä tietoturvallisuutta. Uudistuksen tavoitteena oli osoittaa, että suomalaiset yritykset ovat luotettavia sopimuskumppaneita kansainvälisessä yhteistyössä. Tämän pohjalta laadittiin turvallisuusselvityslaki 726/2014. Laissa kansainvälisistä tietoturvallisuusvelvoitteista 24.6.2004/588 säädetään, että henkilöturvallisuusselvitykset tehdään turvallisuusselvityksistä annetun lain mukaisesti. Kuitenkin selvitys voidaan toteuttaa suppeana myös silloin, kun katsotaan että se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi. [36]

Hallituksen esityksessä HE 53/2010 vp tuotiin esiin, että Suomelta puuttuu viranomainen joka arvioi tietoliikennejärjestelyjen ja tietojärjestelmien turvallisuutta. Tämän seikan nähtiin haittaavan Suomalaisten yritysten osallistumista mm. kansainvälisiin tarjouskilpailuihin. Hallituksen esityksessä ehdotettiin tehtävien uusjaosta siten, että viestintävirastolle uskottiin tietojärjestelmiin ja tietoliikenteeseen liittyvien asioiden valvonta ja vastaavana asiantuntijana toimiminen. [37]

EU:n tietosuoja-asetuksen myötä pilvipalveluasiakkaiden joiden toiminta täyttää tietyt kriteerit tulee jatkossa nimetä tietosuojavastaava. Mikäli on kyse julkisen organisaation toimijasta, tai organisaation ydintehtävänä on henkilötietojen käsittely, on organisaation julkistettava ja ilmoitettava tietosuojavastaavan yhteystiedot valvontaviranomaiselle. Yritykset tai organisaatiot voivat nimetä tietosuojavastaavan vaikka asetus ei sitä heiltä nimenomaisesti vaatisikaan. [38]

2.2.2. Fyysinen - ja laitteistoturvallisuus

Fyysinen – ja laitteistoturvallisuus ovat sisällöllisesti hyvin lähellä toisinaan. Fyysisellä turvallisuudella tarkoitetaan tilojen sekä siihen läheisesti kuuluvien elementtien turvallisuutta. Tilojen ja ympäristön suunnittelu, kulunvalvonta, tekninen valvonta,

[36] HE 57/2013 vp.

[37] HE 53/2010 vp.

[38] Oikeusministeriö selvityksiä ja ohjeita 4/2017.

vartiointi sekä erilaisten rakennukseen tai laitteistoon sisältyvien uhkien torjunta ja ennaltaehkäisy sisältyvät siihen. Se koostuu useista eri tekijöistä, joilla tietyn tilan ja laitteiston turvallisuutta ylläpidetään.[39]

Pyrittäessä mahdollisimman hyvään fyysiseen turvallisuuteen, on valvomaton liikkuminen palvelin tilassa estettävä mahdollisimman hyvin. Mitä arkaluonteisempaa tietoa palvelin tiloissa säilytetään, sitä paremmin kulunvalvonnasta on huolehdittava. Kulunvalvonnan on pystyttävä takaamaan, että henkilöt joilla on oikeus päästä kohteeseen voivat sinne mennä, mutta muuten kaikkien asiaankuulumattomien pääsy pystytään estämään. Henkilön tunnistamiseksi voidaan käyttää eri menetelmiä. Tunnistusmenetelmä riippuu tietenkin osin siitä, kuinka arkaluonteisesta tiedosta on kyse. Mitä salassa pidettävämpää aineisto on, sen korkeampi tulisi kulunvalvonnan tason olla. Yleisimpiä henkilön tunnistamistapoja ovat kuvalliset henkilökortit. Kulunvalvonnan tasoa voidaan helposti nostaa yhdistämällä kuvalliseen henkilökortin lisäksi esimerkiksi työntekijän henkilökohtainen tunnistaminen. Tämä voidaan toteuttaa esimerkiksi oven avautuminen tunnistustilaan henkilökohtaisella salasanalla. Biometriset tunnistustavat ovat vielä suhteellisen harvinaisia, mutta hyvin luotettavia. Tiedon digitointi on kuitenkin edelleen sen verran kallista, että biometrinen tunnistustapa ei ole vielä merkittävästi yleistynyt.[40]

Langattomissa verkoissa tiedonsiirto tapahtuu radioaaltojen avulla. Tällöin kytkeytyminen verkkoon sekä vakoilu on helpompaa kuin kaapeleita käyttävässä lähiverkossa. [41]Hajasäteily aiheutti ennen merkittävän tietoturvauhan. Asiantuntijan oli mahdollista siepata tietoliikenneverkossa tai näyttöpäätteellä olevaa informaatiota hajasäteilyn avulla. Nykyään laitteisto on kuitenkin jo niin kehittynyttä, että hajasäteilyä tulee alle 20 metriin laitteesta. Nykyään hajasäteilyä ei pidetä kovin merkittävänä tietoturvariskinä. Palvelintiloissa erilaisilla menetelmillä pystytään lisäksi estämään hajasäteilyn aiheuttaman tietoturvariskin syntyä. [42] Sähkömagneettinen voimakas pulssi, joka syntyy esimerkiksi salamaniskun osuessa kohdalle voi aiheuttaa paljon tuhoa tietoverkoille. Tietoverkot suojataan hyvin yleisesti nykyään ylijännitesuojalla, joka vaimentaa salamaniskusta aiheutunutta pulssia. Palvelintilassa laitteistot on asennettu

[39] Paavilainen 1998: 95 – 96.

[40] Paavilainen 1998: 97 – 100.

[41] Hakala & Vainio & Vuorinen 2006: 296.

[42] Paavilainen 1998: 101 – 104.

suojattuun tilaan estämään mahdollisia sähkömagneettisen pulssin aiheuttamia vahinkoja. [43]

Laitteistoturvallisuus sisältää fyysiset osakokonaisuudet sekä laitteistojen mukana olevat varusohjelmistot, kuten käyttöjärjestelmät. Se koostuu tietojenkäsittely- ja tietoliikennelaitteiden kokoonpanoon, kunnossapitoon ja laadunvarmistukseen liittyvistä turvallisuusnäkökohdista. Se millaisen tiedon käsittelyyn laitteisto on tarkoitettu, määrittää mitä tietoturvavaatimuksia laitteistolla on oltava. Paavilainen kirjassaan tietoturva mainitsee, että tiedon luottamuksellisuus edellyttää;

> *1. tiedot on luokiteltava niiden luottamuksellisuuden mukaisesti.*
>
> *2. On oltava säännöt, jolla annetaan oikeus tiedon käyttöön. Tämä oikeus voidaan myöntää pysyvästi tai harkinnanvaraisesti.*
>
> *3. On oltava menettelytapa, joka estää korkeamman turvaluokan tiedon viemisen alempaan turvaluokkaan.*
>
> *4. Korkeimpiin turvaluokkiin kuuluvien tietojen käyttö on aina kirjattava.*

Käytössä olevissa laitteissa tulee olla tunnistamisominaisuus, jolla pystytään tunnistamaan käyttäjät, ennen kuin he saavat käyttöön laitteen resursseja. Yleisin tunnistautumistapa on salasanat. Järjestelmän turvallisuuden kannalta salasanalla on suuri merkitys, ja tämän vuoksi sen määrittelyyn ja käyttöön tulisi kiinnittää huomiota. Salasanan tulisi mieluummin olla generoitu, kuin käyttäjän itsensä esimerkiksi lemmikkieläimensä mukaan nimeämä. [44] Jokaisella käyttäjällä tulee olla oma henkilökohtainen tunnus, jolla hän pystyy kirjautumaan laitteiston käyttäjäksi. Kirjautumisessa vaadittava tunnistautuminen voi toteututa salasanan lisäksi esimerkiksi älykortin tai biometrisen tunnistautumisen yhdistelmänä. [45]

2.2.3. Tietoliikenneturvallisuus

Tietoliikenneturvallisuus on merkittävä tekijä kun puhutaan ohjelmiston käytöstä pilvipalveluympäristössä. Se koostuu erilaisista toimenpiteistä, joilla on tarkoitus varmistaa televerkossa välitettyjen tietojen luottamuksellisuus, eheys sekä käytettävyys.

---

[43] Paavilainen 1998: 104 -105.

[44] Paavilainen 1998: 164 – 169.

[45] Hakala & Vainio & Vuorinen 2006: 124.

Tietoliikenneturvallisuudella ei tarkoiteta pelkästään ohjelmiston käyttöön liittyviä seikkoja vaan siihen sisältyvät myös verkkojen rakentamiseen ja suunnitteluun liittyvät asiat. Tietoliikenneturvallisuuden päämääränä on varmistaa, että viestien alkuperäisyys, koskemattomuus ja luottamuksellisuus pystytään varmistamaan sekä lähettäjä ja vastaanottaja pystytään todentamaan. Turvallisuuteen on vaikuttamassa käytettävät tiedonsiirtovälineet, tiedonsiirtoprotokollat, tietoverkkotopologiat, erilaiset tietoturvatuotteet, kuten turvasillat ja reitittimet sekä salausvälineet ja –algoritmit. [46]

Tietotekniikassa laitteistoa kehitetään ja uudistetaan hyvin nopeasti. Tietoliikenneturvallisuus onkin ongelmallinen osa tietoturvallisuutta. Pilvipalveluntoimittajan tulee pyrkiä pitämään tietoturva mahdollisimman korkealla tasolla, ja tämän vuoksi seurattava jatkuvasti alan kehitystä ja hankittava laitteistoja ja ohjelmistoja joilla pystytään suojautumaan mahdollisia uusia uhkia vastaan. [47] Tärkeää on myös huolehtia että infrastruktuurin kannalta on tehty kaikki viimeisimmät päivitykset. On väärin tuudittautua siihen uskoon, että vain joidenkin palvelimien päivittäminen olisi riittävä toimenpide. [48]

Tietoliikenneverkkojen tietoturvaongelmat voidaan luokitella usealla eri tavalla. Usein ongelmat luokitellaan kuitenkin sen mukaan, mistä mahdolliset uhat voivat tulla. Tällöin ne luokitellaan monesti sisäisiin ja ulkoisiin uhkiin. Sisäisten uhkien riski riippuu pitkälti siitä, miten yrityksessä on tietoturvallisuuteen panostettu. Mikäli lähes kaikki tietotekniikkaan liittyvä on ulkoistettu, suurin osa uhista on ulkoisia. Pilvipalvelu ympäristössä sisäisten riskien määrä on suhteellisen vähäinen. Yrityksen oma henkilökunta on yksi merkittävimmistä sisäisistä uhkatekijöistä. Yrityksen sisällä käyvät vierailijat ovat myöskin uhka, mikäli tietoturvasta on yrityksen sisällä huolehdittu huonosti. Laiteviat ovat yksi sisäisistä uhista. Pilviympäristössä laitevian osuus kohdentuu lähinnä tiedon käsittelyn ongelmiin. Kun ohjelmisto toimii pilviympäristössä ja tiedot ovat tallennetut virtuaalikonehuoneeseen, tiedon säilyminen ongelmatilanteissa ei niinkään ole yrityksen sisäinen uhkatekijä. Kapasiteetin riittävyys on myös yksi sisäisistä uhkatekijöistä. Terveydenhuoltoalan ohjelmiston kohdalla ongelmaton tietojen saanti sekä luotettava tallentaminen, ovat ensisijaisen tärkeitä. Mikäli tiedonsaannissa on ongelmia kapasiteetin riittämättömyyden johdosta se pahimmillaan voi vaarantaa potilasturvallisuuden. Pilviympäristössä yrityksen tehtävänä

[46] Paavilainen 1998: 108 – 109.

[47] Paavilainen 1998: 109.

[48] Thomas 2005:10

on huolehtia riittävistä tiedonsiirtonopeuksista päätelaitteissaan, jotta yritys pystyy hyödyntämään virtuaalikonehuoneesta hankkimansa serveritilan optimaalisesti. Kapasiteetin riittämättömyys näkyy pitkinä viiveinä tiedon välityksessä ja siten on aiheuttamassa ongelmia luotettavassa tiedonvälityksessä. [49] Kun kyseessä on hyvin tärkeät tietojärjestelmät niiden käytettävyys pyritään turvaamaan varayhteyksien avulla. Näiden varayhteyksien kapasiteetti on kuitenkin yleensä alhainen verrattuna. Mikäli pilveen ei syystä tai toisesta saada yhteyttä, ei pystytä siellä säilytettävää tietoakaan hyödyntämään. [50]

Tietoliikenneturvallisuuden ulkoisiin uhkiin voidaan laskea kaikki ne yrityksen ulkoiset tekijät jotka ovat vaarantamassa luotettavan tiedonsiirron sekä ongelmattoman käytön. Pilviympäristössä hakkerointi tai muu tietojärjestelmään kohdistuva tunkeutuminen on yksi ulkoisista uhista. Terveydenhuoltoalan ohjelmistossa säilytetään henkilötietoja sekä muita mahdollisesti arkaluonteisia tietoja, joiden hankkiminen joko uteliaisuudesta tai rikollisesti hyötymismielessä saattaa olla joidenkin intressien kohteena. [51]

Pilviympäristössä tietojen säilytys tapahtuu pilvipalveluntoimittajan virtuaalikonehuoneessa. Tällöin palveluntoimittajan oma henkilökunta saattaa aiheuttaa riskin pilvipalveluasiakkaan virtuaalipalvelimelle tallentamille tiedoille. Pilvipalvelun toimittajan henkilökunta saattaa pahimmillaan syyllistyä vakoiluun, jolloin ohjelmistoon tallennetut tiedot saattavat päätyä henkilöille, joiden käsiin niitä ei ole tarkoitettu. [52] Luonnollisesti pilvipalvelun toimittajan asiakkaat haluavat, että talletettu tieto on varmassa säilössä eikä siihen pääse ulkopuoliset, eivätkä toimittajan oma henkilökunta oikeudetta käsiksi. [53]

Yrityksen ulkoisista uhista yksi on myös tiedonsiirtoteiden katkaisu tai siirtohäiriöiden tuottaminen sekä käytettävyyden huonontaminen. Tällöin hakkerit suorittavat esimerkiksi syn-flood tyyppisen hyökkäyksen, jonka johdosta tiedonsiirto hidastuu, ja se on aiheuttamassa yritykselle ohjelmiston käytössä hankaluuksia. Tiedonvälitys hidastuu merkittävästi ja mikäli hakkerit uusivat hyökkäyksen lyhyin väliajoin, saattaa koko palvelin ajautua käyttökelvottomaksi. Toinen hakkereiden suorittamista verkkoon

[49] Paavilainen 1998: 136 – 138.

[50] Hakala & Vainio & Vuorinen 2006: 278 – 279.

[51] Paavilainen 1998: 139.

[52] Paavilainen 1998: 139.

[53] Salo 2013: 107.

kohdistuvista uhista on verkon aktiivilaitteisiin kohdistuva manipulointi. Tällöin hakkerit syöttävät reitittimille väärää reititystietoa ja pystyvät siten saamaan koko verkon toiminnan sekaisin. [54] Palvelunestohyökkäyksellä hakkerit voivat sulkea tai hidastaa verkon toimintaa.[55]

2.2.4. Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan kaikkien yrityksen käytössä olevien ohjelmistojen ja sovellusten tietoturvallisuusominaisuuksia. Ohjelmistoturvallisuus muodostuu ohjelmistojen ja tietokonearkkitehtuurin turvallisuudesta, sovellusten muodostamasta turvallisuudesta, tietokoneviruksista sekä ohjelmistojen sisältämistä salaporteista. [56] Terveydenhuoltosektorin ohjelmistojen käytettävyyden ongelmakohtia on, että eri ohjelmistovalmistajien sovellukset ovat voineet sisältää erilaisia tehtäväkuvauksia potilaan hoitoprosessin aikana. Tietojärjestelmiä ei ole toteutettu loogisena kokonaisuutena, jolloin tietoja on saattanut välittyä, myös sellaisille henkilöille, joilla ei siihen olisi tehtävänmukaista oikeutta. [57]

Varsinaisesti tietokonearkkitehtuuri kuuluu laitteistoturvallisuuteen. Kaikki muu siitä ylöspäin kuuluu ohjelmistoturvallisuuteen. Ohjelmistoturvallisuus on jaoteltu ohjelmistojen tunnistamisominaisuuksiin, eristämisominaisuuksiin, pääsynvalvonnan ominaisuuksiin, tarkkailu- ja paljastamistoimenpiteisiin sekä laadunvarmistamistekniikoihin. Ohjelmistojen tunnistamis- ja eristämisominaisuuksilla tarkoitetaan vastapuolen tunnistamista ohjelmiston käytön yhteydessä sekä käyttöoikeuksien hallintaa. Tarkkailu- ja paljastamistoimenpiteitä ovat lokitiedostojen pitäminen sekä mahdollisten virusten torjuminen. Laadunvarmistamisena pidetään ohjelmistojen eheyden varmistamista. [58]

Asianmukaisen tietoturvallisuuden saavuttaminen edellyttää, että tietojärjestelmän jokainen osa pyrkii mahdollisimman hyvään turvallisuustasoon. Mikäli jokin hierarkiataso ei pysty tarjoamaan vaadittavaa tietoturvapalvelua, voidaan seuraavalla

[54] Paavilainen 1998: 141 – 142.

[55] Thomas 2005: 297.

[56] Paavilainen 1998: 186.

[57] Kleemola & Tervo-Pellikka 1998: 89 – 93.

[58] Paavilainen 1998: 188 – 189.

rajapinnalla kompensoida tätä tason lisäominaisuudella. Jos esimerkiksi tietokonearkkitehtuuri ei kykene antamaan riittävää tietojen käsittelyyn liittyvää turvallisuutta, se voidaan kompensoida ohjelmallisesti käyttöjärjestelmässä. [59]

Aikaisemmin sovellukset suunniteltiin organisaatioiden sisäverkkokäyttöön. Tällöin palomuurilla oli merkittävä osa sovelluksen turvallisuudesta. Nykyään yhä enemmän sovelluksia käytetään pilviympäristössä julkisessa verkossa. Sovellusten suojaamisen tarve on muuttunut aikaisemmasta. Sovellukset itsessään täytyvät olla rakennettuina sellaisiksi, että ne pystyvät torjumaan jatkuvat verkkohyökkäykset. [60] Ohjelmistot voidaan jakaa perinteisesti käyttöjärjestelmiin ja sovelluksiin. Sovellukset rakennetaan kyseiseen käyttöjärjestelmään ja tietokonearkkitehtuuriin sitä varten luodulla kääntäjällä. Käyttöjärjestelmien tietoturvallisuusominaisuudet riippuvat pitkälti niiden käyttötarkoituksesta. Mikäli konetta on tarkoitus käyttää arkaluonteisten tietojen käsittelyyn, on myös käyttöjärjestelmän oltava suunniteltu tiettyjä tietoturvaominaisuuksia sisältäväksi. Useamman käyttäjän verkkopalvelimiin tarkoitetut käyttöjärjestelmät sisältävät tietoturvaominaisuuksia kuten käyttäjien tunnistus sekä tiedostojen ja oheislaitteiden käyttöoikeuksiin perustuvaa käyttö- ja turvallisuusominaisuuksien monitorointi. Ohjelmistoturvallisuuden yksi merkittävä tekijä on kääntäjä. Jos ohjelmiston on pystyttävä erittäin korkeaan tietoturvatasoon, on korkean tason kääntäjän käyttäminen huomattava riskitekijä. Myös erittäin alhaisen tason kääntäjällä on omat riskinsä, mutta niiden hallinta saattaa olla helpompaa. Ohjelmoinnissa on mahdollista käyttää valmiita kääntäjiä, jotka sisältävät suuren määrän luokkakirjastoja. Koska ohjelmoija ei voi varmuudella tietää miten luokat toimivat missäkin tilanteessa, voi se aiheuttaa ohjelmistossa merkittäviä tietoturvariskejä. Erittäin turvallisen ohjelmiston tekeminen vaatii, että ohjelmistokoodi on tehty täysin itse. Mikäli ohjelmistolta vaaditaan hyvin suurta tietoturvaominaisuutta, myös kääntäjän tulisi olla itse kyseistä ohjelmistoa varten tehty. [61]

Sovelluksen tietoturvavaatimuksia arvioitaessa tulee huomioida sovelluksen luottamuksellisuus, eheys, saatavuus ja jäljitettävyys.[62] Sovellusten tietoturvaongelmat liittyvät usein sovellusten laatuun. Ne voivat ilmetä sovellusten toimimattomuutena tai sovellus ei vastaa tilaajan vaatimuksia. Tärkein sovelluksen tietoturvaominaisuus on sen

[59] Paavilainen 1998: 188.

[60] Sovelluskehityksen tietoturvaohje VAHTI 1/2013: 11.

[61] Paavilainen 1998: 193 – 194.

[62] Sovelluskehityksen tietoturvaohje VAHTI 1/2013: 15.

saatavuus. Mikäli sovellusta ei voida käyttää, ei sen muistakaan turvaominaisuuksista ole hyötyä. Käytettävyys muodostuu käyttöliittymästä sekä sovelluksen toimintalogiikasta. Kun riittävän korkea käytettävyyden taso on saavutettu, on varmistuttava tietojen eheydestä. Kun sovelluksen toimintalogiikka ja tietovarastojen käyttöperiaate vastaavat toisiaan, myös eheys vaatimus täyttyy. Luottamuksellisuus rakentuu tietovarastojen käytöstä ja käyttöoikeuksista sekä niiden oikeanlaisesta yhdistämisestä. [63]

Tietokonevirukset ovat yksi ohjelmistoturvallisuuden riskeistä. Viruksen tyypistä riippuen ne saattavat aiheuttaa yrityksen sovellukselle ja toiminnalle erityyppisiä ongelmia. Erittäin tuhoisat virukset saattavat estää koko koneen ja sen sisältämien tietojen käytön. Virus voi esimerkiksi kopioida, poistaa ja vaihtaa tiedoston tai hakemiston nimeä. Se voi myös muuttaa dataa tai kerätä ja vaihtaa salasanoja. Melko vakavissa viruksissa mitään tärkeätä tietoa ei kokonaisuudessaan menetetä. Näissä tapauksissa pääasiallisin menetys on koneiden puhdistamiseen käytettävä työaika. Vähäisissä menetyksissä mitään tietoa ei menetetä, vaan haittana on yksittäisen henkilön työnteon estyminen tai viivästyminen. Tietokonevirukset ovat todellinen uhka nykypäivän yritystoiminnassa. Ei ole varmaankaan olemassa juurikaan organisaatioita, joissa ei olisi tavattu viruksia. Tämän vuoksi, jotta suuremmilta ongelmilta vältyttäisiin, niihin täytyy varautua tosissaan. Pilviympäristössä, kun yritykselle tärkeä tieto säilytetään virtuaalisessa konesalissa, pilvipalveluntoimittajan täytyy huolehtia tietojen säilymisestä muuttumattomana ja viruksilta suojassa. Kuitenkin, kun erilaisilla päätelaitteilla ollaan pilveen yhteydessä yrityksen toimipaikasta, täytyy heidän huolehtia myös omien päätelaitteidensa virusturvasta. Virusuhka on suurempi, kun ollaan yrityksen päätelaitteella yhteydessä yrityksen ulkopuoliseen verkkoon. [64]

Ohjelmistojen sisältämiä salaportteja pidetään hankalimpina tietoturvaongelmina. Salaportti on ohjelmiston osa, joka tekee jotain sellaista jota ei ole dokumentoitu eikä ohjelmistoon virallisesti suunniteltu. Salaportti on ohjelmistoon tehty tarkoituksella, vaikkakin se ei välttämättä aina ole tarkoitettu vahingontekoon. Tietoturvallisuuden kannalta tärkeissä ohjelmistoissa mahdollisten salaporttien olemassaolo on huomioitava. Kuitenkin, kun ajatellaan esimerkiksi terveydenhuollon tarpeisiin rakennettua sovellusta, niin ohjelmoija ei voi sovellukseen laittaa pahoja salaportteja, koska se olisi ohjelmistotalolle erittäin suuri riski ja julki tullessaan vaarantaisi koko ohjelmistotalon

[63] Paavilainen 1998: 198 – 201.

[64] Paavilainen 1998: 205 – 208.

liiketoiminnan. [65] Salaportin pystyy avaamaan henkilö joka tietää siihen luodun käyttäjätunnuksen sekä salasanan.[66]

2.2.5. Käyttöturvallisuus

Käyttöturvallisuuden katsotaan rakentuvan tietojärjestelmien turvallisista käyttöperiaatteista, käyttöympäristöstä, tietojenkäsittelytapahtumien valvonnasta sekä jatkuvuuden turvaamisesta. Usein käyttöturvallisuuteen kiinnitetään etenkin pienemmissä yrityksissä huomiota vasta sitten kun vahinko on jo tapahtunut. Pilviympäristössä, kun konesalipalvelu ostetaan pilvipalveluntoimittajalta, oletetaan käyttöturvallisuuden olemassa hyvin mietittynä. Pilvipalveluntoimittajan oletetaan huolehtineen, että hänen henkilökuntansa hallitsee tehtävät siten, että mikään tiedon säilytykseen pilviympäristössä liittyvistä tehtävistä ei ole vain yhden henkilön osaamisen takana. Tehtävien kahdentamiselta huolehditaan, että ongelmatilanteissa löytyy aina osaamista ongelmien ratkaisuun. [67] Tehtävien kahdentaminen on osa henkilöstöturvallisuutta, josta yleensä vastaa organisaation henkilöstöhallinto yhdessä tietohallinnon kanssa. [68]

Yksi tärkeä tietojenkäsittely tapahtumaan liittyvistä valvonta toimenpiteistä on toimintojen kohdennettavuus. Tämä muodostetaan lokitiedoista, joilla voidaan todentaa tietyn toimenpiteen suorittaneen henkilöllisyys. Kun kyse on henkilötiedoista ja mahdollisesti arkaluonteisista terveyteen liittyvistä tiedoista on tärkeää, että pystytään jäljittämään tietoja käsitelleet henkilöt. Lokitietoihin läheisesti liittyy myös käyttöoikeuksien hallinta. Periaatteisiin kuuluu, että henkilöille annetaan sellaiset käyttöoikeudet, jotka hän työtehtäviensä hoitamiseksi tarvitsee. Tärkeää on, että joku yrityksessä hallitsee myönnettyjä käyttöoikeuksia. Saattaa olla tietoturvalle riskialtista, mikäli henkilölle jää esimerkiksi suuremmat oikeudet, kuin mitä hän normaalisti työssään tarvitsisi. Tällöin mahdollisuus esimerkiksi arkaluonteisten tietojen leviämiselle kasvaa. [69]

---

[65] Paavilainen 1998: 210 – 212.

[66] Järvinen 2002: 284.

[67] Paavilainen 1998: 213 – 215.

[68] Hakala & Vaino & Vuorinen 2006: 11.

[69] Paavilainen 1998: 217 – 219.

Varmistukset ja varmuuskopiointi on tärkeä huomioitava jatkuvuuden turvaamiseksi. Varmistaviin toimenpiteisiin voidaan katsoa laitteiston kahdentaminen, tarvittavan varamateriaalin olemassaolo sekä henkilöstön kahdentaminen. Pilviympäristössä pilvipalveluntoimittajan tulisi huolehtia näistä asioista. Toki myös yrityksen sisällä toiminnan katkeamattomuuden turvaamiseksi on huolehdittava, jotta yrityksen käytössä olevat päätelaitteet ovat jatkuvasti käyttökelpoisia, sekä henkilöstö osaa sovelluksen käytön kaikissa tilanteissa. Tietojen varmuuskopiointi on pilvipalveluntoimittajan tehtäviin kuuluva. Hänen velvollisuutenaan on huolehtia, että on olemassa laitteisto, joka suorittaa säännöllisesti tietojen varmuuskopioinnin. Ongelmatilanteissa pilvipalveluntoimittajan tulee pystyä palauttamaan tarvittavat tiedot ja mahdollistamaan lähes katkeamattoman tietojen käsittelyn mahdollisuuden. Pilvipalveluntoimittajan tulee myös varmistua aika ajoin siitä, että varmuuskopiointi toimii ongelmitta. [70]

2.3. Hyvä tiedonhallintatapa

Laissa viranomaisen toiminnan julkisuudesta on asetettu vaatimus viranomaisen hyvän tiedonhallintatavan toteuttamisesta ja noudattamisesta. Lain 18.1 §:ssä on säädetty, että viranomaisen tulee huolehtia asiakirjojen ja tietojärjestelmien sekä niihin liittyvien tietojen tietoturvallisuudesta, sekä muista tietojen laatuun liittyvistä seikoista. Käsitteeseen on liitetty yleiset velvoitteet, jotka koskevat viranomaisten tietoaineistojen käyttöä. Näitä ovat mm. asiakirjan julkisuutta ja salassapitoa, henkilötietojen suojaa sekä tietoturvallisuutta koskevat seikat. [71]

Keskeinen tavoite hyvässä tiedonhallintatavassa on tiedon laadun säilyttäminen. Asiakirjojen ja tiedon saatavuus, käytettävyys, eheys ja suojaaminen ovat seikkoja, joihin tulee kiinnittää huomiota. Tiedon laadun säilyttämisestä tulisi huolehtia kolmella eri tasolla. Näitä tasoja ovat tiedot, asiakirjat sekä tietojärjestelmät. Asiakirjojen ja tiedon saatavuus sekä käytettävyys ovat toisiaan tukevia seikkoja. Jotta periaatteet toteutuisivat, olisi jokaisella oltava mahdollisuus saada tieto julkisesta asiakirjasta ja tietojärjestelmästä. Tiedon saatavuuden ja käytettävyyden periaatteen toteutuminen edellyttää, että tiedot sekä asiakirjat ovat asianmukaisesti luetteloitu sekä arkistoitu, ja tiedon saannin tekniset edellytykset ovat olemassa. Laissa viranomaisen toiminnan julkisuudesta 16 §:ssä on määritelty tavat, joilla viranomaisen tiedot ovat käytettävissä.

[70] Paavilainen 1998: 221 – 223.

[71] Voutilainen 2007: 60.

Asiakirjan ja tiedon käytettävyyden toteutumiseksi viranomaisen on järjestettävä asiakirja- ja tiedonhallintajärjestelmänsä mahdollisimman toimivaksi ja häiriöttömäksi. Tiedon eheydellä tarkoitetaan tiedon säilyttämistä muodossa, jossa se on tallennettu. Tällä pyritään turvaamaan asiakirjan ja tiedon oikeellisuus sekä aitous viranomaisen asiakirjoja ja tietoja käsiteltäessä. Tietojärjestelmien tasolla tiedon eheys tarkoittaa myös järjestelmien toiminnan varmistamista sekä mahdollisten häiriöiden välitöntä korjaamista. Viranomaisen pilvipalveluasiakkaana tulee myös varmistaa, että käytettävät tietojärjestelmät ovat toteutettu siten, että on suojauduttu tallennetun tiedon tahattomalta tai oikeudettomalta muuttamiselta. Tietojen suojaamisella tarkoitetaan viranomaisen toimia, joilla estetään ennakolta tietoon, asiakirjoihin ja tietojärjestelmiin kohdistuvat vahingot ja häiriöt. Tietojärjestelmät on suojattava siten, että vain tietoon oikeutetuilla on mahdollisuus saada tiedon asiakirjasta tai tiedosta. Toiminnot on toteutettava siten, että salassapitovelvoitteet ja henkilötietojen suoja toteutuu suhteessa sivullisiin. [72]

[72] Mäenpää 2009: 251 – 253.

3. TERVEYDENHUOLTOALAN OHJELMISTON TIETOTURVARISKIEN VASTUIDEN JA VELVOLLISUUKSIEN JAKAUTUMINEN PILVIYMPÄRISTÖSSÄ

3.1. Terveydenhuoltoalan erityispiirteitä

Terveydenhuoltoalalla rekistereihin kerättävän tiedon turvallinen käsittely sekä tiedonhallinta ovat keskeisessä asemassa. Asiakkaan hakeutuessa hoitoon terveydenhuoltoalan yritykseen tai –yksikköön, hänen täytyy pystyä luottamaan, että hänen luovuttamiaan henkilökohtaisia tietoja säilytetään ja käsitellään siten, että kukaan ulkopuolinen ei niihin pääse käsiksi. Terveydenhuoltosektorillakin on jo pitkään ollut käytössä sähköisiä asiankäsittelyjärjestelmiä sekä sähköistä tiedonsiirtoa. Yritysten ja yksiköiden verkostoituessa suuremmiksi palveluja tuottaviksi kokonaisuuksiksi, niin on tärkeää että hoidossa tarvittava tieto on kaikkien asiakkaan tai potilaan hoitoon liittyvien henkilöiden käytettävissä sähköisten järjestelmien avulla. [73]

Salassapitovelvollisuudella tarkoitetaan sekä asiakirjasalaisuuden säilyttämisvelvollisuutta että myös vaitiolovelvollisuutta. [74]Terveydenhuollon alueella asiakasrekisterien salassapito ei tarkoita suoranaisesti samaa kuin asiakkaan tietosuoja. Terveydenhuollossa asiakkaan tietosuojalla tarkoitetaan muutakin kuin salassapitovelvollisuuden noudattamista henkilökunnan käsitellessä häntä koskevia tietoja. Tämä seikka saattaa monesti käytännön hoitotilanteissa unohtua. Terveydenhuollon alueella tietosuojan tarkoituksena on asiakkaiden oikeuksien kunnioittaminen ja toteuttaminen, kaikissa hoidon vaiheissa hyvän tiedonkäsittelytavan luominen ja toteuttaminen sekä asiakkaiden ja rekisterinpitäjänä toimivan pilvipalveluasiakkaan oikeusturvan varmistaminen. Asiakkaan ollessa hoidossa terveydenhuoltopalveluita tarjoavassa yrityksessä tai yksikössä hänestä laaditut ja häntä koskevat asiakasrekisteriin tallennetut asiakirjat ja tiedot muodostavat arkaluonteisia tietoja sisältävän henkilörekisterin. Henkilötietolaki sekä julkisuuslaki ohjaavat yleislakeina terveydenhuollon asiakasrekistereihin laadittujen ja tallennettujen asiakastietojen käsittelyä, siltä osin kuin asiasta ei erityislainsäädännössä nimenomaisesti säädetä toisin. [75]

---

[73] Ylipartanen 2001: 18 - 19

[74] Pahlman 2010: 73.

[75] Ylipartanen 2001: 19 - 20

Terveydenhuollon sektorilla pilvipalveluasiakkaalla on henkilötietolain mukaan säädetty velvoite aktiivisesti informoida asiakasta rekisteritietojen käsittelyyn vaikuttavista keskeisistä asioista. Tämän tarkoituksena on lisätä informaatiota asiakkaiden keskuudessa siitä, että ovat tietoisempia asemastaan sekä oikeuksistaan. [76] Terveydenhuollon asiakasrekisterit sisältävät usein arkaluonteista aineistoa, ja tämän vuoksi asiakasrekisterinpitoon kohdistuu korostettu luottamuksellisuus, huolellisuusvelvoite sekä virheettömyysvaatimus. [77] Potilasrekisterin sisältämät potilastiedot tulisi olla kaikissa tarvittavissa yksiköissä käytettävissä ehjänä kokonaisuutena, jotta hoitopäätöksiä tehtäessä pystyttäisiin turvaamaan potilasturvallisuus. [78]

Yksityiselämän suoja määriteltiin perusoikeudeksi 1.8.1995 voimaan astuneessa perusoikeussäännöksiä koskeneessa hallitusmuodon uudistuksessa. Siinä määrättiin, että henkilötietojen suojasta on säädettävä tarkemmin lailla. Tämä perusoikeus sisältyy nyt 1.3.2001 voimaan astuneessa Suomen perustuslain 2. Luvussa. Suomen perustuslain 2:12 §:ssä mainitaan että,

> *”viranomaisten hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta”.*

Terveydenhuollon potilastiedot on kuitenkin säädetty salassa pidettäviksi julkisuuslaissa ja useissa terveydenhuollon erityislainsäännöksissä. Perustuslakivaliokunta on lausunnossaan (PeVL 14/1998 vp.) määritellyt henkilötietojen suojaa koskevan perusoikeussäännöksen kannalta tärkeiksi seikoiksi mm. tietojen sallitut käyttötarkoitukset, tietojen luovutettavuus, tietojen säilytysaika sekä rekisteröidyn oikeusturvan.[79] Perustuslain 8:1 §ssä mainitaan että, henkilötietojen suojasta säädetään tarkemmin lailla. Tämä henkilötietojen suojaa täydentävä yleislaki on henkilötietolaki (HetiL 523/1999).[80]

---

[76] Ylipartanen 2001: 17.

[77] Ylipartanen 2001: 22.

[78] Pahlman 2010: 142.

[79] Ylipartanen 2001: 37 – 39.

[80] Korhonen 2003: 92.

3.2. Ohjelmistovalmistajan vastuut ja velvollisuudet

Terveydenhuollon sovelluksen ohjelmistovalmistajan täytyy sovellusta suunnitellessaan ottaa huomioon normaalien rekisterienkeruuseen liittyvien seikkojen ohella tiukat tietoturvavaatimukset. Potilasasiakirjoihin sisältyy asioita henkilön terveydentilasta sekä mahdollisesti hyvinkin arkaluonteista salassa pidettävää tietoa. Näiden tietojen käsittely sovelluksessa edellyttää, että kaikki osapuolet voivat täysin luottaa siihen, että rakennettu sovellus on periaatteiltaan, teknisiltä ratkaisuiltaan sekä toteutukseltaan lainsäädännön mukainen. Sovelluksen tulee täyttää kaikki sille asetetut tietoturvavaatimukset. Käytettyjen tietojärjestelmien tulee lisäksi olla keskenään yhteensopivia. Suomessa Terveyden ja hyvinvoinnin laitos laatii ja vahvistaa tietojärjestelmän käytettävät kriteerit. Ohjelmistojen kriteerien täyttämisestä huolehtii tietojärjestelmien toimittajat sekä ohjelmistoja käyttävät organisaatiot ensisijaisesti laatujärjestelmän ja omavalvonnan keinoin. Mikäli ohjelmistovalmistajan sovellus liitetään Kansaneläkelaitoksen ylläpitämiin valtakunnallisiin tietojärjestelmäpalveluihin, tulee se hyväksyttää ulkopuolisen tahon toimesta. Toistaiseksi Kansaneläkelaitoksen valtakunnalliseen tietojärjestelmäpalveluihin on mahdollista tietojen tallentaminen vain terveydenhuollon organisaatioiden omien potilastietojärjestelmien kautta. Hallituksen esityksessä sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä lain muuttamisesta mainitaan, että jatkossa on mahdollista tietojen tallentaminen myös internet-selaimen kautta kun ohjelmistovalmistajat vain sellaisen sovelluksen toteuttavat.[81]

Tämän hallituksen esityksen HE 219/2013vp merkittävin muutos on, että myös muille kuin terveydenhuollon valtakunnalliseen tietojärjestelmään liitettäville tietojärjestelmille säädetään vaatimukset jotka tulee täyttää ennen niiden käyttöön ottoa. Samalla kaikilta terveydenhuollon tietojärjestelmiä käyttäviltä organisaatioilta edellytettäisiin käyttöön liittyvää omavalvontasuunnitelmaa, jonka tarkoitus on varmistaa potilastietojen tietoturva. Terveydenhuollon tietojärjestelmät luokitellaan kahteen luokkaan A ja B luokkaan. A- luokkaan kuuluvilta tietojärjestelmiltä edellytetään suuremmat tietoturvavaatimukset, koska ne toimivat valtakunnallisesti. Näin halutaan myös varmistaa yhteen toimivuus sekä ongelmatilanteissa tietoturva, sillä näiden järjestelmien kautta on mahdollista päästä lähes kaikkien suomalaisten terveystietoihin käsiksi. Luokkaan B kuuluvat järjestelmät ovat käytössä paikallisesti tai alueellisesti ja ne eivät ole liitännäisenä valtakunnallisiin tietojärjestelmäpalveluihin. Tällöin myös tietojen väärinkäyttöön liittyvät riskit ovat hieman pienemmät. Luokan B-

[81] HE 219/2013vp: 1.

tietojärjestelmiltä ei vaadita ulkopuolisen tahon auditointia, vaan riittää kun sovelluksen valmistaja laatii kirjallisen selvityksen olennaisten vaatimusten toteuttamisesta. Tietoturvaan liittyvät olennaiset vaatimukset perustuvat valtionhallinnon tietoturvallisuuden johtoryhmän hyväksymiin tietoturvaohjeistoihin. Tämän jälkeen ohjelmiston valmistajan tulee ilmoittaa sovelluksesta Valviralle ja järjestelmä voidaan ottaa tuotantokäyttöön. Valvira ylläpitää julkista rekisteriä, johon se merkitsee valmistajien ilmoittamat tietojärjestelmät. Rekisteristä sovelluksen hankkija pystyy tarkistamaan täyttääkö kyseinen sovellus lain asettamat vaatimukset. [82]

Valtionhallinnon tietoturvallisuuden johtoryhmä on sovelluskehityksen tietoturvaohjeissa 1/2013 määritellyt tietoturvallisuuden kannalta tärkeimmät seikat jotka tulee dokumentoida. Dokumentoitavia asiakirjoja ovat mm. tietoturvatason määrittely, sovelluksen tietoturvariskien kartoitus, tietoturvallisuuden vaatimusmäärittely tietoturva-arkkitehtuurin mukaisesti, noudatettavat standardit tai muut normit, tietoturvallisuuden testisuunnitelma ja –raportit, käyttöönottosuunnitelma, ylläpitosuunnitelma ja vastuut sekä jatkuvuus- ja toipumissuunnitelma. [83]

Laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä on 19 c §:ssä säädetty ohjelmistovalmistajan yleisistä velvollisuuksista. Pykälän mukaan valmistaja on aina itse vastuussa tietojärjestelmän suunnittelusta, valmistuksesta ja luokittelusta. Vaikka ohjelmistovalmistaja olisi hankkinut osan suunnittelutyöstä alihankintana, se ei vaikuta vastuuseen poistavasti. Ohjelmistovalmistajan tulee pystyä sovelluksen loppukäyttäjälle osoittamaan sovelluksen yhteen toimivuuden, tietoturvallisuuden sekä toiminnallisuuden kannalta tarpeelliset tiedot ja ohjeet. Samoin valmistajan tulee 19 d §:n mukaisesti pystyä osoittamaan, että tietojärjestelmä on vaatimusten mukainen sekä luokiteltu joko A tai B luokkaan kuuluvaksi. Luokkaan A kuuluvien tietojärjestelmien kohdalla ohjelmistovalmistajan tulee pystyä osoittamaan 19 e §:n mukaisesti, että sovellus on yhteen toimiva muiden valtakunnallisiin tietojärjestelmäpalveluihin liittyneiden tietojärjestelmien kanssa. Ohjelmistovalmistajan tulee aktiivisesti seurata tietojärjestelmän toimivuutta myös käyttöönoton jälkeen. Mikäli sovelluksen käytössä todetaan normaalista merkittäviä poikkeamia, valmistajan on välittömästi informoitava kaikkia järjestelmää käyttäviä palvelun antajia. Luokkaan A kuuluvien järjestelmien kohdalla asiasta on myös ilmoitettava tietoturvallisuuden arviointilaitokselle sekä sosiaali- ja terveysalan lupa- ja valvontavirastolle. Valmistajan

[82] HE 219/2013vp: 9 -10.

[83] Sovelluskehityksen tietoturvaohje VAHTI 1/2013: 24 – 25.

on säilytettävä vähintään viisi vuotta vaatimustenmukaisuutta osoittavat ja muut valvontaan liittyvät dokumentit. [84]

Todettaessa, että tietojärjestelmä ei vastaa käytössä oleviin tietojärjestelmiin kohdistuvia velvoitteita, on ohjelmistovalmistajan oma-aloitteisesti ryhdyttävä korjaaviin toimenpiteisiin. Valviralla on oikeus kieltää tietojärjestelmän käyttö, mikäli se epäilee sen vaarantavan asiakas- tai potilasturvallisuuden. Tämä kielto-oikeus koskee myös, mikäli epäillään tietosuojan vaarantuneen. Ohjelmiston käyttökielto perutaan kun tarvittavat toimenpiteet tilanteen korjaamiseksi on tehty. [85]

3.3. Pilvipalveluasiakkaan vastuut ja velvollisuudet

Terveydenhuoltoalan yritystä tai organisaatiota joka ottaa käyttöön ohjelmistovalmistajan sovelluksen ja kerää siihen tietoa asiakkaidensa tai potilaidensa terveydentilasta kutsutaan pilvipalveluasiakkaaksi. pilvipalveluasiakkaan vastuista ja velvollisuuksista on säädetty suomessa henkilötietolaissa. Henkilötietolain tarkoituksena on turvata yksityiselämän suojaa henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Yksilöllä on oikeus elää omaa elämäänsä sekä oikeus tietää ja päättää itseään koskevien tietojen käytöstä. Keskeistä onkin yksilön suostumus tietojen tallentamiseen ja säilyttämiseen rekisterissä. Henkilötietolaissa henkilötiedoilla tarkoitetaan kaikenlaista luonnollista henkilöä tai hänen ominaisuuksiaan sekä elinolosuhteitaan kuvaavia merkintöjä, joiden perusteella hänet voidaan tunnistaa. [86]

Lain 2:1 §:n mukaan rekisteröidyn henkilötietoja käsiteltäessä on noudatettava, mitä henkilötietolaissa on säädetty, jollei muualla laissa ole toisin säädetty. Henkilötietolaki onkin näin ollen henkilötietojen käsittelyn yleislaki. Lakia sovelletaan henkilötietojen automaattiseen käsittelyyn silloin kun henkilötiedot muodostavat henkilörekisterin tai sen osan. Hallituksen esitys (96/1998) painottaa, että aina kun yksilöitä kohdistavaa tietoaineistoa käsitellään automaattisen tietojenkäsittelyn avulla, kyseessä on lain tarkoittama henkilörekisteri. [87]

---

[84] HE 219/2013vp:23 – 28.

[85] HE 219/2013vp: 32.

[86] Vanto 2011: 18 – 19.

[87] Vanto 2011: 19.

Henkilötietolaissa on 3 §:n 3 kohdassa määritelty henkilörekisteriksi, käyttötarkoituksensa takia yhteenkuuluvista merkinnöistä muodostuvaksi tietojoukoksi, jotka sisältävät myös henkilötietoja. Rekisteri voi olla osin tai kokonaan muodostettu automaattisen tietojenkäsittelyn avulla. Oleellista ei ole mihin tai miten tiedot on tallennettu. Keskeistä hallituksen esityksen perusteella kuitenkin on, että samaan henkilörekisteriin katsotaan kuuluvaksi ne tiedot, joita käytetään samassa käyttöyhteydessä. Mikä tahansa järjestymätön tiedostojoukko ei kuitenkaan muodosta lain tarkoittamaa henkilörekisteriä. Tietosuojadirektiivissä painotetaan, että direktiivi soveltuu ainoastaan tietojärjestelmiin ja niiden tulee olla rakennettu siten, että rekisteröidyn yksityiskohtaiset tiedot ovat helposti tarvittaessa saatavissa. [88]

Uuden EU:n tietosuoja-asetuksen mukaan rekisteripitäjien ja henkilötietojen käsittelijöiden on huolehdittava jatkossa siitä, että yrityksessä tai organisaatiossa on nimetty tietosuojavastaava. Hänen tehtäviinsä kuuluu muun muassa seurata sitä että, henkilötietoja käsitellään lainmukaisesti sekä auttaa organisaatiota toteuttamaan lainsäädännön vaatimat velvoitteet. Tietosuojavastaava toimii myös yrityksen tai organisaation sekä valvontaviranomaisten välillä yhteyshenkilönä. [89]

3.4. Pilvipalveluntoimittajan vastuut ja velvollisuudet

Pilvipalveluntoimittajan vastuuta ohjaa pitkälti millä pilvipalveluntasolla liikutaan. Saas- tasolla palveluntoimittaja tarjoaa asiakkailleen valmiita paketteja, joita asiakkaan ei juurikaan ole mahdollista itsenäisesti laajentaa. Tällöin myös vastuu palvelun turvallisuudesta on yleisesti enimmäkseen palveluntoimittajalla. Paas- tasolla pilvipalveluntoimittaja tarjoaa asiakkaalle alustan, jonka päälle hänen asiakkaansa voi sovelluksen kehittää. Tämän johdosta alustan on oltava laajennettavampi kuin Saas-tasolla, jonka johdosta alustasta on karsittava Saas- tasolle valmiiksi integroituja turvallisuusominaisuuksia. Tällöin myös vastuu alustan ja sovelluksen tietoturvasta siirtyy enemmän asiakkaalle. Iaas-tasolla palvelun tulee olla mahdollisimman hyvin muokattavissa. Tällä tasolla Pilvipalveluntoimittaja vastaa yleensä ainoastaan laitteiston ylläpidosta ja käynnissä pitämisestä. Liikutaan millä pilvipalvelun palvelumallin tasolla tahansa, niin on tärkeää neuvotella palvelusopimuksen sisältö tarkkaan. Palvelusopimuksessa osapuolet voivat sopia mm. palvelun tasosta, palvelun

[88] Vanto 2011: 29.

[89] Oikeusministeriön selvityksiä ja ohjeita 4/2017.

turvallisuudesta, valvonnasta sekä osapuolten odotuksista ja vastuista pilvipalvelun suhteen. [90]

Pilvipalveluntoimittaja ei lähtökohtaisesti ole millään palvelumallin tasolla henkilötietojen käsittelijä. Mikäli henkilötietoja tallennetaan pysyvästi palveluntoimittajan palvelimelle tai mikäli pilvipalvelusopimukseen kuuluu tietojen prosessointia, niin tällöin palveluntoimittaja on kyseisten tietojen käsittelijä. Rekisterinpitäjä pilvipalveluntoimittaja ei kuitenkaan ole edes tässä tapauksessa, jolloin häntä ei koske rekisterinpitäjän vastuut, vaan ne säilyvät edelleen pilvipalveluasiakkaalla. Pilvipalveluntoimittajaa koskeva vastuu perustuu ainoastaan osapuolten väliseen sopimukseen. [91]

[90] Brunette & Mogull 2009: 54 – 55.

[91] Staffans 2013: 2 – 3.

4. TERVEYDENHUOLTOALAN OHJELMISTON TIETOTURVARISKIEN RISKIENHALLINTA

4.1 Riskien ja sitoumusten kartoitus

Yritykselle ja yhteisölle on tyypillistä luoda erilaisia tietokantoja, joita he käyttävät apuna organisoidessaan ja operoidessaan joka päivittäisissä toiminnoissaan. Nämä tietokannat sisältävät tietoja, jotka voivat olla hyvinkin kallisarvoisia sekä myös salaisia muille kuin organisaation toimintaan osallistuville. Kaikkeen yritystoimintaan liittyy riskejä, jotka aiheuttavat epävarmuutta ja mahdollisesti uhkaavat yrityksen tai yhteisön toimintaa tulevaisuudessa. Näiden mahdollisten riskien kanssa yritysten täytyy kuitenkin pystyä elämään ja toimimaan, niin että pelko tulevaisuudesta ei lamauta yrityksen tai yhteisön toimintaa. Riskiin liittyy aina epävarmuus. Kukaan ei pysty varmuudella ennustamaan tulevaisuutta, ja vaikka pystyisimmekin hyvin määrittelemään ja ennakoimaan yritykselle tai yhteisölle mahdollisesti epävarmuutta aiheuttavat tekijät, voi tapahtua jotain ennakoimatonta joka aiheuttaa joko suoraa rahallista haittaa tai epäsuoraa menetystä. [92]

Riski sana pohjautuu latinankieliseen termiin risco, joka tarkoittaa asiaa jonka olemassaolon uskomme tietävämme ja johon liittyy vahingon vaara. Kuitenkaan emme tiedä tarkasti missä kyseinen vaara voisi olla ja tämän vuoksi se aiheuttaa uhan siitä, että toteutuessaan voi myös aiheuttaa vahinkoa. [93] Sanan riski synonyymina Suomen kielessä ovat esimerkiksi sanat vahingonvaara ja vahingonuhka. Riski tarkoittaa aavistusta ja uhkaa siitä, että yritykselle mahdollisesti voisi tapahtua jotain ikävää. Riski on todennäköisyyksien arviointia. Yritykset välillä onnistuvat toimissaan ja välillä epäonnistuvat. Tätä onnistumisten ja epäonnistumisten välistä suhdetta voidaan ilmaista prosenttiluvulla. Mikäli yrityksen tietoturvapäivitys epäonnistuu kerran joka 20.päivityksessä, riski päivityksen epäonnistumiselle on 5 prosenttia. Riskin luonteeseen kuuluu, ettei kukaan voi tarkasti tietää, koska yritykselle sattuu jotain ei-toivottavaa. Yrityksen ja yhteisön täytyykin vain pyrkiä ennakolta varautumaan joillakin keinoin siihen, että jonain päivänä saattaa riski realisoitua ja yritykselle tapahtuu jotain ei-toivottavaa. Yrityksen tai yhteisön kannattaa arvioida riskit niiden laajuuden ja seurausvaikutusten suhteen tärkeysjärjestykseen. Riskeihin, joiden

[92] Suominen 2003: 7 – 9.

[93] Leppänen 2006: 29.

seurausvaikutukset ovat katastrofaaliset yritykselle, kannattaa ensisijaisesti suojautua mahdollisimman hyvin. Nämä riskit ovat sellaisia, että riskin realisoituessa koko yrityksen tai yhteisön toiminta on vaarassa kaatua.[94] Joihinkin riskeihin yrityksen tulee varautua jo lainsäädännönkin vuoksi. Tällaisia ovat esimerkiksi tietosuojariskit henkilörekisteri-tietokannan ollessa kyseessä. Suomen henkilötietolaki 523/1999 esimerkiksi velvoittaa pilvipalveluasiakkaan tekemään tarpeelliset tekniset ja organisatoriset toimenpiteet tietojen turvaamiseksi. Hänen tulee myös toimia laillisesti sekä noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa. [95]

Kun riskejä tarkastellaan, on huomioitava useita eri näkökohtia. Näitä ovat esimerkiksi riskien suuruus, hyväksyttävyys, kohdentuvuus sekä riskikokemuksen problematiikka. [96] Arvioitaessa riskien merkitystä yritykselle tai yhteisölle on tärkeää pyrkiä arvioimaan riskin suuruutta. Huomioon otettavia seikkoja ovat riskin realisoitumisen todennäköisyys sekä tästä seuraavan tappion suuruus. [97] Yrityksen tavoitteena riskienhallinnassa on, että yritys tai yhteisö pystyy säilyttämään tilanteen ennallaan. Mikäli riski realisoituu, yritykselle tai yhteisölle aiheutuvat menetykset voivat olla esimerkiksi rahallisia tai maineen ja luottamuksen menetyksiä. [98]

Mahdollisen tapahtuvan riskin suuruutta voidaan kuvata matemaattisesti riskin realisoitumisen todennäköisyyden sekä tästä seuraavan tappion välisellä suhdeluvulla. Jos esimerkiksi on 5 prosentin todennäköisyys, että aiheutuu yritykselle tai yhteisölle ei toivottava tilanne ja siitä aiheutuu 10 000 yksikön mahdollinen vahinko, on riskin suuruus 500 yksikön suuruinen. Mikäli tuotto-odotus on suurempi kuin 500 yksikköä, on kyseisen riskin ottaminen taloudellisesti perusteltua. Tämän tapaisten riskilaskelmien tekeminen on usein käytännössä vaikeaa, koska muuttujien arviointi eksaktisti on lähes mahdotonta. Vahingon todennäköisyyden mahdollisuus joudutaan arvioimaan summittaisesti kuten myös vahingosta aiheutuvan määrän suuruus. Erilaiset riskienhallintakeinotkaan eivät ole myöskään välttämättä vaikutukseltaan suoraviivaisia. Esimerkiksi vakuuttaminen on tehokas suojautumiskeino vahingosta aiheutuvien kustannusten peittämiseksi, mutta ei sekään aina täysin varma. Vakuutuksen suojaavaa

[94] Suominen 2003: 9 – 11.

[95] Pitkänen & Tiilikka & Warma 2013: 219 – 221.

[96] Kuusela & Ollikainen 2005: 15.

[97] Hemmo 2005: 10 – 11.

[98] Kuusela & Ollikainen 2005: 15 – 17.

tehoa saattaa heikentää esimerkiksi vakuutuksenottajan omasta laiminlyönnistä johtuvat seikat. [99]

Yrityksen tai yhteisön riskejä arvioitaessa on hyvä kiinnittää myös huomiota sidosryhmien asemaan. Yrityksen tai yhteisön sidosryhmiä voivat olla esimerkiksi omistajat, johto, työntekijät, tavarantoimittajat ja rahoittajat. Yrityksen ja sen sidosryhmien intressit saattavat olla samansuuntaisia tai niissä saattaa olla myös huomattavia eroja. Kun tarkastellaan riskejä yrityksen tai yhteisön itsensä kannalta, se ovat yleensä muita kuin oikeudellisia. Tällöin niiden kohdalla ei löydy myöskään käyttökelpoisia oikeudellisia suojautumiskeinoja. Tämäntyyppisiä riskejä voivat olla esimerkiksi tuotteiden tai palveluiden kilpailukyky markkinoilla, tuotekehittelyn onnistuminen, markkinoinnin menestyksellisyys, yrityksen julkinen kuva, rahoituksen riittävyys, johdon ja henkilökunnan asiantuntemus ja innovatiivisuus sekä erilaisten laitevaurioiden ja ohjelmistojen toimintahäiriöiden vaara. [100]

Sopimuksellinen riskienhallinta on osa yrityksen tai yhteisön yleistä kokonaisvaltaista riskienhallintaa. Keskitalo on esitellyt kirjassa ennakoiva sopiminen kuusi tekijää, joista muodostuu sopimuksellinen riskienhallinta. Näitä ovat;

1. *Sopimuksellisen riskienhallinnan tavoitteiden muodostuminen,*
2. *Riskien tunnistaminen,*
3. *Riskien arviointi,*
4. *Riskien sopimuksellinen käsittely,*
5. *Sopimuksellisen riskienhallinnan seuranta ja kehittäminen sekä*
6. *Liiketoiminnan ja riskienhallinnan strategioiden kehittäminen.* [101]

4.2 Riskien tyypit ja niiden luokittelu

Riskejä tyypiteltäessä ne voidaan jakaa esimerkiksi onnettomuuden luonteen mukaan (luonnollinen vastaan tekninen), riskin ilmenemisen mukaan (kausaalisuus, esimerkiksi arkaluontoisten tietojen kadottamisesta aiheutuvat vahingot) sekä seurausten luonteen

[99] Hemmo 2005: 11 - 12.

[100] Suominen 2003: 70 – 72.

[101] Pohjonen ym. 2002: 242.

mukaan (vammat vastaan vahingot). Toteutuessaan tämä ei toivottava tapahtuma alentaa kohteen arvoa joko osittaisesti tai sitten kokonaan. [102]

Liiketoiminnan riskeistä keskeisimpiä sopimuksellisen riskienhallinnan kannalta ovat taloudelliset-, poliittiset-, riippuvuus-, tuote- sekä keskeytysriskit. Taloudellisilla riskeillä tarkoitetaan esimerkiksi valuutta tai ostajan maksukyvyttömyysriskejä. Poliittisilla riskeillä tarkoitetaan esimerkiksi lainsäädännön muuttumisriskit. Riippuvuusriskeillä tarkoitetaan sitä kuinka riippuvainen yritys tai yhteisö on toisen yrityksen tai yhteisön toiminnasta. Keskeytysriski on riski siitä, että yrityksen tai yhteisön toiminta keskeytyy odottamattomasti. Tuoteriskillä tarkoitetaan riskiä tuotteiden tai palveluiden vastaavuudesta kysyntään. Tarkasteltaessa yksittäisiä transaktioita voidaan havaita, että ne useimmiten muodostuvat useista alitransaktioista. Esimerkiksi transaktio tietoturva koostuu useista siihen kohdentuvista alitransaktioista kuten esimerkiksi laite- ja ohjelmistovalmistajien kanssa tehdyt sopimukset, henkilökunnan kanssa tehdyt työsopimukset, asiakkaiden kanssa tehdyt tietojen säilytyssopimukset. [103] Tyypillisimmät tietoturvariskejä aiheuttavat tekijät ovat vastuiden ja riskien epäselvyys, lakien mukaisten käytäntöjen puute, ihmisten toiminnassa ennakoitavia tilanteiden tietoturvariskit, järjestelmien käytössä ennakoitavien tilanteiden tietoturvariskit sekä omaisuuden ja toiminnan suojaamisessa ennakoitavien tilanteiden tietoturvariskit. [104]

4.2.1 Vastuiden ja riskien epäselvyys

Epäselvä valvontavastuu saattaa aiheuttaa yrityksessä tai organisaatiossa välinpitämättömyyttä tietoriskien hallintaa kohtaan. Yrityksen tai organisaation henkilöstön toiminta saattaa olla tietoista välinpitämättömyyttä. He eivät koe tietoriskien hallintaa tärkeäksi, eivätkä myöskään usko mitään yllättävää tapahtuvan. Myös yksipuolinen tai puutteellinen tietoriskien analysointi saattaa antaa yrityksen tai organisaation johdolle väärän käsityksen riskien hallinnan tilasta ja näin ollen estää tai hidastaa ongelmien ratkaisua. Virheellisen käsityksen vuoksi yritys tai organisaatio

[102] Leppänen 2006: 31.

[103] Pohjonen ym. 2002: 247 – 248.

[104] Kyrölä 2001: 6.

saattaa painottaa vääriä kehitystarpeita, jos he ovat arvioineet riskit liian suppeasti tai eivät tunne järjestelmän käytön riskejä riittävän syvällisesti. [105]

Yrityksen tai yhteisön tulee kuitenkin tunnistaa mahdolliset riskitilanteet. Pyrittäessä tunnistamaan riskejä onkin katsottava tilannetta laajasti. Mikäli katsontakanta on liian suppea saattaa jäädä huomaamatta merkittäviä riskejä. Jotta vastuuriskien tunnistaminen on mahdollista, täytyykin tietää kaikki ne yrityksen tai yhteisön toiminnot, joista saattaa aiheutua oikeudellisia velvoitteita. [106]

Yrityksessä tai organisaatiossa saattaa myös syntyä vaarallisia työyhdistelmiä, joka tarkoittaa sitä, että yhden tai useamman henkilön kokoonpanolla on laajat oikeudet ylläpitää tai siirtää tärkeitä tietoja ilman kolmannen osapuolen hyväksyntää tai valvontaa. Nämä yhdistelmät syntyvät useimmiten huomaamatta ajan kuluessa. Tämä syntyminen saattaa tapahtua esimerkiksi organisaatiossa vastuullisessa tehtävässä olevan henkilön sairastuessa, hänen työtehtävänsä jaetaan väliaikaisesti jonkun toisen hoidattavaksi. Väliaikaisesti työtä tekevän työkenttä ja vastuu laajenee, jolloin hän tarvitsee myös useimmiten laajemmat oikeudet tietojen käyttöön ja käsittelyyn. [107]

Työntekijän jonka työtehtäviin kuuluu tärkeän ja yritykselle arvokkaan tiedon hallinnointi uskotaan jatkavan työtehtävissä loputtomiin. Tilannetta, jossa työntekijä ei pysty tai ei enää halua jatkaa yrityksen tai organisaation palveluksessa ei useimmiten uskota tapahtuvan. Tällöin ei myöskään varauduta ennakolta tilanteisiin, joissa vastuullisessa asemassa oleva työntekijä ei enää olekaan yrityksen tai organisaation palveluksessa. Tällaiseen tilanteeseen voitaisiin varautua ennakolta dokumentoimalla yritykselle arvokas tieto. Useimmiten tämä tärkeän tiedon dokumentaation puute on tiedostamatonta ja tahatonta. Jokaisella yksittäisellä työntekijällä on velvollisuus tunnistaa oman työtehtävänsä kannalta oleelliset tiedettävät seikat ja dokumentoida ne ymmärrettävästi sellaiseen muotoon, että niiden avulla toinen työntekijä pystyy tarvittaessa selviytymään työtehtävistä. Yrityksen tai organisaation keinoja tietovuodon estämiseksi työntekijöiden toimesta on allekirjoituttaa henkilöstöllä salassapito- ja vaitiolosopimukset. Kuitenkin on erittäin vaikeaa, jollei mahdotonta estää palveluksesta pois siirtyvää työntekijää hyödyntämästä osaamistaan jatkossa toisen työntekijän palveluksessa. On hyvä muistaa, että irtisanoutuvan henkilön haltuun ei jää

[105] Kyrölä 2001: 84 – 85.

[106] Aalto-Setälä ym. 2004: 399 – 401.

[107] Kyrölä 2001: 85 – 87.

lähtötilanteessa yrityksen asiakirjoja, avaimia, kulkukortteja tai käyttäjätunnuksia. [108] Tietoturvallisuuteen liittyviä asiakirjoja käsiteltäessä on syytä huolehtia, että luottamukselliset tiedot eivät paljastu asiattomalle tai luottamukselliseen suhteeseen sitoutumattomalle osapuolelle. Tiedot ja asiakirjat saakin luovuttaa vasta, kun osapuolet ovat allekirjoittaneet tarvittavat vaitiolo- ja salassapitosopimukset. Vastuullisessa asemassa oleva henkilö voi myös käyttää vastuuasemaansa väärin, esimerkiksi vaikuttamalla palvelujen tai hankintojen päätöksiin. Vakavimpina vastuuaseman väärinkäytön seurauksena saattaa olla esimerkiksi kavallus tai petos. [109]

4.2.2 Lakien mukaisten käytäntöjen puute

Yrityssalaisuus määritellään rikoslaissa (39/1889). Yrityssalaisuus ei ole tieto, joka on yleisesti tunnettu tai jota yritys ei halua pitää tai ei pidä salassa. Mikäli yrityksellä tai yhteisöllä on epäilys, että joku työntekijä on käyttänyt yrityssalaisuutta hyväkseen, yrityksellä on korotettu näyttövelvollisuus. Mikäli yritys aikoo menestyä mahdollisessa oikeudenkäynnissä, on sen ennalta huolehdittava yrityssalaisuuksien tosiallisesta suojaamisesta. [110] Yrityssalaisuuden termi sisältyy rikoslakiin. Muussa lainsäädännössä käytetään terminä liike- tai ammattisalaisuutta. [111]

Myös sisäpiiritiedot on osattava tunnistaa, sen eri olomuodot on huomioitava käsittelyohjeita tehtäessä ja suojauskeinoja toteutettaessa. Yrityksissä ja organisaatioissa tietoa muokkaavat ja käsittelevät useat eri henkilöt. Yrityksen tai organisaation sisäpiiriin kuuluvien tulee osata ennalta tunnistaa ne henkilöt, jotka saattavat olla kiinnostuneita sisäpiiritiedosta. [112]

Viestintäsalaisuuden loukkaus on yksi tavallisista tietoturvariskeistä. Yrityksen tai organisaation viestinnässä käytetään hyvinkin monipuolisia kuten avoimia ja suljettuja kirjeitä sekä ei-salattuja ja salattuja sähköpostiviestejä. Viestintäsalaisuuden loukkauksesta säädetään myös rikoslaissa. 3§:n mukaan,

---

[108] Kyrölä 2001: 88 – 89.

[109] Honkinen ym. 2016: 113 – 117.

[110] Kyrölä 2001: 90 – 91.

[111] Honkinen ym. 2016: 113.

[112] Kyrölä 2001: 92 – 93.

> ”*joka oikeudettomasti 1.) avaa toiselle osoitetun kirjeen tai muun suljetun viestin esimerkiksi murtamalla. 2.) salaa teknisen erikoislaitteen avulla kuuntelee taikka salaa teknisellä laitteella tallentaa toisen puhetta, joka ei ole hänen tietoonsa tarkoitettu, taikka hankkii tiedon televerkossa välitettävästä puhelusta tai viestistä, niin on tuomittava viestintäsalaisuuden loukkauksesta sakkoon taikka vankeuteen”.*

4 §:n mukaan, törkeä viestintäsalaisuuden loukkaus on*, ”*

> *mikäli tekijä käyttää hyväkseen asemaansa rikoksen tekemisessä, rikoksentekijä käyttää hyväkseen sitä varten suunnitelmaansa tietokoneohjelmaa, taikka rikoksen kohteena oleva viesti on sisällöltään, erityisen luottamuksellinen taikka loukkaa erityisesti yksityisyyden suojaa, näin ollen teko loukkaa huomattavasti yksityisyyden suojaa ja siten on kokonaisuutena arvostellen erityisen törkeä ja rikoksentekijä onkin tuomittava törkeästä viestintäsalaisuuden loukkauksesta vankeuteen enintään kolmeksi vuodeksi”.* [113]

Työntekijöiden tietosuoja tulee myös olla työpaikalla kunnossa. Kaikki tiedot, joista työntekijä voidaan henkilökohtaisesti tunnistaa, tulee olla suojattuna asiattomalta käytöltä sekä rajattuina vain näitä tietoja tarvitsevien käyttöön. Tietovarkaus voi tapahtua yrityksen sisällä olevan tai ulkopuolisen henkilön toimesta. Ulkoisia palveluntarjoajia valittaessa on tarpeen arvioida tietosuojan toteutumista. Jotta paras mahdollinen tietosuoja toteutuu, palveluntoimittajan kanssa tulee sopia toimintaohjeet sekä tekniset tiedon käsittelytavat ja menetelmät. [114] Käytettäessä etenkin uutta teknologiaa, kuten pilvipalveluja ja oletettaessa tietoturvariskin olevan kohtuullisen korkea on ennalta ennen henkilötietojen käsittelyn aloittamista toteutettava arviointi suunniteltujen käsittelytoimien vaikutuksesta henkilötietojen suojaan. Vaikutusten arviointi on tärkeää etenkin kun käsitellään henkilön salassa pidettäviä terveystietoja. [115]

4.2.3 Ihmisten toiminnassa ennakoitavat tilanteet

Yrityksissä ja organisaatioissa käsitellään suuri määrä tietoa. Näissä monesti rutiininomaisissa töissä tapahtuu aika ajoin joko tiedostamattomia tai tiedostettuja virheitä. Toimintavirheiden vuoksi sillä hetkellä toimintayksiköissä käsiteltävän tietojen sisältö tai arvo muuttuu toisenlaiseksi. Vaarana saattaa olla, että tieto näyttää hyvältä,

[113] Kyrölä 2001: 94.

[114] Kyrölä 2001: 96 – 97.

[115] Honkinen ym. 2016: 151.

mutta tarkempi arviointi osoittaa, että toimintavirheen vuoksi tiedon sisältö muuttuu toiseksi tai jopa käyttökelvottomaksi. Tietoa käsitellessään henkilö saattaa tarkoituksella tai vahingossa siirtää tai kopioida arkaluonteista tietoa tai paljastaa yritykselle, organisaatiolle tai kolmannelle osapuolelle liikesalaisuuksia sisältävää tietoa, josta aiheutuu asianomaisille merkittävää haittaa. Tällaisia virheitä saattaa olla esimerkiksi, että henkilö luovuttaa sopimuksen vastaisesti luottamuksellista tietoa ulkopuolisille ilman pyynnön esittävän henkilöllisyyden varmistamista tai työasemalta poistuttaessa jättää arkaluonteista tietoa sisältäviä ohjelmia tai dokumentteja auki näytölle. Perimmäisiä syitä virhetilanteiden syntyyn tällaisissa seikoissa on useimmiten kiire, osaamattomuus, tiedon puute tehtävästä, ohjeiden puute, välinpitämättömyys tai ohjeiden vastainen toiminta. Tämänkaltaiset toimintavirheet voivat aiheuttaa yritykselle tai organisaatiolle vahingonkorvausvaateen. [116]

Käsiteltäessä henkilötietoja sisältäviä ohjelmia, käyttäjille on luotu käyttöoikeudet ohjelmistojen käyttöön. Henkilöllä on velvollisuus huolehtia oman käyttäjätunnuksen ja salasanan asianmukaisesta käytöstä ja säilytyksestä. Hänen on myös huolehdittava tämän perusteella haltuunsa saamien tietojen huolellisesta käsittelystä. Henkilötietoja on käsiteltävä tietosuoja-asetuksen mukaan lainmukaisesti, asianmukaisesti sekä rekisteröidyn kannalta läpinäkyvästi. [117] Yrityksen tai organisaation tehtävänä on valvoa, että tiedonkäsittelyyn omaavia oikeuksia on vain niillä, jotka tarvitsevat työssään pääsyä kyseisin tietoihin. Vaarana on, että mikäli oikeuksia on liian monilla tai käyttöoikeuteen vaadittavat tunnukset joutuvat ulkopuolisten haltuun, niin yrityksen tai organisaation tietoja voidaan anastaa tai levittää ulkopuolisille. [118]

Yrityksessä tai organisaatiossa joillakin henkilöillä on oikeudet kaikkiin tiedostoihin ja tietovarastoihin. Nämä henkilöt saattavat olla vastuussa ohjelmistojen toimivuudesta tai luomassa esimerkiksi yhteenvetoraportteja luottamuksellisista tiedoista. Vastuuhenkilöiden toimintaa valvotaankin usein kirjaamalla erilaisia tietoja ohjelmiston käytöstä ja tietojen käsittelystä suojattuun valvontatiedostoon. [119] Pilvipalveluasiakas on

[116] Kyrölä 2001: 98 – 99.

[117] Honkinen ym. 2016: 142.

[118] Kyrölä 2001: 100 – 101.

[119] Kyrölä 2001: 102.

aina vastuussa henkilötietojen tai muiden arkaluontoisiksi laskettavien tietojen käsittelyn lainmukaisuudesta. [120]

Työntekijälle määrättyjen työtehtävien laiminlyönti saattaa olla myös aiheuttamassa tietoturvallisuusriskin. Laiminlyönti voi tapahtua, kun henkilö jättää tekemättä hänelle määrätyn tehtävän, ei noudata annettuja toimintaohjeita tai toimii vastoin niitä. Laiminlyöntejä ovat aiheuttamassa huolimattomuus, välinpitämättömyys tai asioiden unohtaminen. Syntyvät tietoturvarikkomukset ovatkin usein laiminlyönneistä aiheutuneita. [121] Yrityksen tai yhteisön avainhenkilöt sekä tietenkin myös työntekijät voivat toimillaan vaikuttaa tietoturvarikkomusten ehkäisemiseen. Avainhenkilöiden tietoturvallisuusrutiinit ovatkin tehokkaimpia keinoja estää tietojen väärinkäyttöä.[122]

Tietomurtoihin erikoistuneet rikolliset, etsivät keinoja saada haltuunsa yritysten tai organisaatioiden järjestelmien ja ohjelmistojen käyttäjätunnuksia ja salasanoja. Erityisen tärkeässä asemassa tietoturvallisuuden kannalta ovat ne käyttäjätunnukset, joilla pääsee muuttamaan järjestelemään asetuksia, luomaan uusia käyttäjätunnuksia tai hyväksymään raha- tai maksutapahtumia. Terveydenhuoltoalan yritysten ja organisaatioiden, joiden hallussa on potilas- ja henkilötietoja tulisi suhtautua erityisen huolellisesti käyttäjätunnusten ja salasanojen hallintaan. Henkilöiden ei tulisi säilyttää tunnuksia paperilla helposti saatavilla, vaan pyrkiä pitämään tunnukset vaan omassa muistissaan. [123]

Yhä useampi työntekijä tekee työtään osin etätyömahdollisuutta hyödyntäen. Ohjelmistojen sijainti pilvipalveluympäristössä luo tälle hyvät mahdollisuudet. Työntekijöiden tulee ymmärtää ja huomioida tietoturvaan liittyvät riskit, kun yritykselle tai yhteisölle arvokkaita tietoja käsitellään yrityksen sisäisen verkon ulkopuolella. Etätyökoneen tietojen varmistaminen ja luotettava säilyttäminen on aina koneen haltijan vastuulla. Tietokonevirukset ja erilaiset vakoiluohjelmat ovat myös asioita, joihin työntekijän tulee suhtautua riittävällä vakavuudella. Mikäli huolimattomuuttaan ei toimi yrityksen tai yhteisön antamien sääntöjen ja ohjeiden mukaisesti hän saattaa toimillaan vaarantaa tietoturvallisuuden ja aiheuttaa merkittävää haittaa ja ongelmia yritykselle tai

[120] Honkinen ym. 2016: 141.

[121] Kyrölä 2001: 102 – 103.

[122] Miettinen 1999: 171.

[123] Kyrölä 2001: 104.

yhteisölle. [124] Sähköisessä muodossa olevien tietojen säilytys on aina tapahduttava tietoturvallisissa laitteissa, jotka on varustettu asianmukaisin suojauksin. Vaikka tietojen säilytys on pilvipalveluympäristössä, on aina huolehdittava siitä, että käsittelyyn käytettävät laitteet ovat myös kriteerit täyttävät ja tietoihin pääsee käsiksi vain sellaiset henkilöt, joilla on siihen oikeus sekä asiallinen peruste. [125]

4.2.4 Järjestelmien käytössä ennakoitavat tilanteet

Ohjelmistoja hankittaessa yrityksen tai yhteisön tietotekniikasta vastaavan on selvitettävä millaisia mahdollisia puutteita tai aukkoja tietojen siirron luottamuksellisuudessa saattaisi olla olemassa sekä miten näihin ongelmiin voidaan ennakolta varautua. Ohjelmistot sekä yrityksille tai yhteisöille räätälöidyt sovellukset saattavat hyvinkin sisältää virheitä, joita joudutaan alkuvaiheessa korjaamaan. Tärkeää onkin ennakolta varautua mahdollisiin virheisiin ja niistä aiheutuviin ongelmiin, jotta vakavia henkilötietojen vuotoon johtavilta tilanteilta vältyttäisiin. [126]

Tietoliikenneverkoissa välitettävien tietojen eheys ja sisältö tulee aina suojata tarkoituksenmukaisesti. Mikäli yrityksen verkkoon pääsee asiattomia ohjelmia, niiden avulla saattaa ulkopuolinen saada ongittua arkaluonteista tietoa. Tämän vuoksi yrityksen tai yhteisön ohjelmistot täytyy olla hyvin suojattuina ulkopuolelta tulevilta haittaohjelmilta tai viruksilta. [127] Palomuurit ovat edelleen tärkeitä rakenteita suojaamaan yrityksen tai yhteisön verkkoa ulkopuolisten hyökkäyksiltä. [128]

4.2.5 Omaisuuden ja toiminnan suojaamisessa ennakoitavat tilanteet

Pilviympäristössä toimittaessa yrityksen tai yhteisön on kiinnitettävä erityistä huomiota siihen, että yritykselle tärkeät tiedot on suojattu sekä käytön aikana, että tiedon säilytyksessä. Hankalaksi asian tekee se, että usein tietojen säilytyspaikka saattaa olla

[124] Kyrölä 2001: 106 – 107.

[125] Honkinen ym. 2016: 145.

[126] Kyrölä 2001: 115 – 116.

[127] Kyrölä 2001: 119 . 120.

[128] Kuusela & Ollikainen 2005: 255 – 257.

kaukana tiedon käyttäjistä. Pahimmillaan yrityksen tai yhteisön johto ei edes tiedä missä tärkeitä tietoja sisältävä konesali sijaitsee. Sekä yrityksen tai yhteisön tiloissa, että myös konesalissa kaikki kulkeminen tulee olla valvottua ja asiaton kulkeminen tulee pystyä estämään. Jokaisen tiloissa liikkuneen henkilöllisyys tulee pystyä jälkikäteen tarkistamaan. Kiinteistön turvallisuusjärjestelyiden hankinnasta ja ylläpidosta kiinteistön omistajan sekä tiloissa toimivan yrityksen tai yhteisön tulee sopia keskenään. Useimmiten erilaisten turvallisuuteen liittyvien järjestelmien tai palveluiden hankkiminen on yrityksen tai yhteisön vastuulla. [129]

Pilvipalveluissa konesalin sijaitessa jopa toisessa maassa, kannattaa pilvipalvelusopimuksella varmistaa, että pilvipalveluntoimittaja vastaa konesalin kulunvalvontaan liittyvästä turvallisuudesta. Pilvipalveluasiakkaan on mahdotonta vaikuttaa konesalin turvallisuuteen muuten kuin sopimusoikeudellisin keinoin.

4.3 Riskianalyysit ja arviointi

Riskianalyysistä puhutaan silloin kun riskienhallintaprosessi etenee tietyssä suunnitellussa järjestyksessä. Analyysin tehtävänä on selvittää riskikohteet, riskien todennäköisyys, riskien vakavuus sekä riskeistä aiheutuvat seurausvaikutukset. Analyysin laajuus voidaan määritellä joko suppeasti tai laajasti. Riskianalyysia tehtäessä riskikohteet on käytävä systemaattisesti läpi noudattaen ennalta laadittua suunnitelmaa. Nykyaikainen riskianalyysi on monitieteinen kokonaisuus, jonka perustana käytetään muun muassa luotettavuusteoriaa, todennäköisyyslaskentaa sekä tilastotieteen eri menetelmiä. Riskianalyysien tekemiseen on nykypäivänä kehitetty useita eri tietoteknisiä sovelluksia, joita voidaan hyödyntää analyysiä tehtäessä. Yleisimpiä analyysimenetelmiä ovat tapahtumapuut sekä Hazop – analyysi. Viimeksi mainitun avulla pyritään tunnistamaan myös mahdollisia riskien syitä. Pk-yritysten riskienhallintaprojektissa on kehitetty myös haavoittuvuusanalyysi, jonka avulla voidaan tarkastella sekä muodostaa karkea kuva yrityksen toimintaan liittyvistä riskitekijöistä. Riski- ja haavoittuvuusanalyysien avulla yritykset ja yhteisöt pystyvät paikantamaan kaikkein riski alttiimmat kohdat prosesseissaan sekä sen perusteella suojaamaan paremmin nämä heikoimmat kohdat etukäteen. [130]

[129] Kyrölä 2001: 122 – 123.

[130] Suominen 2003: 35 – 40.

Riskianalyysin avulla voidaan pyrkiä varautumaan mahdollisilta yritystä tai yhteisöä kohtaavilta mahdollisilta riskeiltä. Ihmiset ovat nykypäivänä hyvin tietoisia kaikenlaisista mahdollisista riskeistä, mutta kuitenkaan niihin varautumiseen eivät kaikki ennalta luo suunnitelmaa. [131] Pyrittäessä toimivaan riskianalyysin on edellytyksenä se, että mahdolliset riskikohteet pystytään tunnistamaan. Käytännössä tämä tarkoittaa sitä, että yritys tai yhteisö erilaisten menetelmien avulla kykenee havaitsemaan itselleen alttiit erilaiset vaaratilanteet. Yrityksen tai yhteisön kannalta olisi erityisen tärkeää, että pystyttäisiin havaitsemaan myös mahdolliset piilevät riskitekijät, joiden olemassaolosta yritys tai yhteisö ei ehkä ole ollut edes tietoinen. Kun halutaan esimerkiksi analysoida mahdollisia henkilötietojen tietosuojaan liittyviä riskitekijöitä, on tärkeää ensin tarkastella, millaista vahinkoa säilytettävälle tietoaineistolle voi mahdollisen tietoturvavuodon johdosta tapahtua. Pyrittäessä kattavaan riskientunnistamistyöhön tarvitaan kunnollinen logiikka. Ilman tätä tunnistustyö on hyvin sattumanvaraista. Tärkeää on tarkastella muun muassa, missä ja miten tietoa säilytetään? Ketkä tietävät tietoaineksen säilytyspaikan ja ketkä pääsevät siihen laillisesti käsiksi. Kenellä on oikeus käsitellä tietoa ja keille on lupa tietoainesta pyydettäessä luovuttaa. Tarkasteltavia kysymyksiä on siis lukuisa määrä. [132]

Kun mahdolliset riskit on tunnistettu, seuraavana on tärkeää arvioida niiden laajuutta ja seurausvaikutuksia. Tämän vaiheen yhtenä tärkeänä tehtävänä on saada riskit keskinäiseen järjestykseen mahdollisten aiheutuvien riskivaikutusten perusteella. Ensinnäkin on arvioitava onko mahdollinen riski hyvin todennäköinen vaiko niin epätodennäköinen, että sitä ei todennäköisesti tapahdu koskaan. Myös tapahtuvan riskin aiheuttamien vahinkojen laajuutta on pyrittävä arvioimaan. Onko tapahtuva vahinko yrityksen tai yhteisön kannalta mitätön vahinko vai mahdollisesti katastrofaalinen vahinko tai jotain siltä väliltä. Kun riskit on luokiteltu järjestykseen todennäköisyyden sekä riskistä aiheutuvan vahingon laajuuden perusteella, on yrityksen tai yhteisön helpompi lähteä kohdentamaan riskienhallintaan ennakolta suuntaavia toimiaan. [133] Perinteisesti riskienhallintaa on jaettu riskien tunnistamiseen, analysointiin käsittelyyn sekä seurantaan. [134]

---

[131] Kuusela & Ollikainen 2005: 35 – 37.

[132] Suominen 2003: 40 – 43.

[133] Suominen 2003: 43 – 46.

[134] Haapio ym. 2005: 122.

Riskien analysoinnin lähtökohtana on löytää mahdollisimman kattavasti turvallisuutta uhkaavat tekijät ja arvioida niiden todennäköisyys sekä seurausten vakavuus. Tietoriskien analysoinnissa on mahdollista käyttää samoja riskien analysointimenetelmiä kuin muidenkin riskien kartoituksessa. Tietoriskien kohdalla on kuitenkin tärkeää huomioida, että ne ovat esimerkiksi abstrakteja jolloin niiden arvoa ja niitä uhkaavia riskejä on joskus vaikea määritellä. Erilaiset tekijä, kuten esimerkiksi monimutkaiset tietoverkot, tiedon eri säilytysmuodot sekä tietoturvallisuuden laaja-alaisuus asettavat haasteita riskien arvioinnille. [135]

4.4 Riskienhallinnan päätöksenteko

Corporate governance on käsite, jolle on vaikeaa keksiä suomenkielistä vastinetta sekä yksiselitteistä määritelmää. Yleisellä tasolla termin voidaan katsoa tarkoittavan sitä, että järjestelmällä on kaksi perustehtävää: yhtiön tai organisaation tehokkuus sekä tilivelvollisuus toiminnastaan. [136] OECD on määritellyt termin siten, että ”corporate governance on kokoelma suhteita yhtiön johdon, hallituksen ja osakkeenomistajien sekä muiden sidosryhmien välillä Se myös tarjoaa rakenteen, jonka avulla asetetaan yhtiön tavoitteet sekä määritellään keinot niiden saavuttamiseksi ja suorituksen valvomiseksi ”. [137] Suomessa termistä puhutaan yleisesti yrityksen hallinnointi- ja ohjausjärjestelmästä. Tämän järjestelmän avulla voidaan tarkastella miten yrityksen toimintaa johdetaan ja valvotaan. Sisäinen valvonta on oleellinen seikka corporate governancea. Riskienhallinta on osa sisäistä valvontaa. Yrityksen tai yhteisön johdon tehtäviin kuuluukin olla perillä siitä, että riskienhallinta on asianmukaisesti organisoitu. Yrityksissä ja organisaatioissa riskienhallintaan liittyvä ohjeistus ja siihen liittyvä dokumentaatio voidaan rakentaa kolmiportaisena. Jaottelu on rakennettu riskienhallintapolitiikkaan, riskienhallinnan periaatteisiin sekä toimintapolitiikkaan. Riskienhallintapolitiikka on yrityksen tai yhteisön hallituksen hyväksymä ja siinä on kuvattuna yleiset yritys- tai yhteisötason periaatteet ja tavoitteet, riskienhallintapolitiikan kattavuus sekä mitä riskillä yrityksessä tai yhteisössä tarkoitetaan. Eri osapuolten roolien ja tehtävien kuvaus sekä selvitys riskienhallinnan organisoinnista kuuluvat riskienhallintapolitiikkaan. Riskienhallinnan periaatteissa

[135] Suominen 2003: 83 – 84.

[136] Aalto-Setälä ym. 2004: 482 – 483.

[137] Kuusela & Ollikainen 2005: 123.

kuvataan ja dokumentoidaan tarkemmin riskienhallinnan strategiat sekä –prosessi, merkittävimmät riskialueet, yrityksen tai organisaation organisatoriset vastuut, riskienhallinnan mittausmenetelmät sekä yrityksen tai organisaation mittausmenetelmät riskienhallinnan tehokkaan toiminnan arvioimiseksi. Toimintapolitiikassa laaditaan eri osa-alueiden vastuuhenkilöille erillisiä ohjeita ja kuvauksia, jotta he saavat syvemmän taustainformaation oman vastuualueensa toiminnasta ja menetelmistä riskienhallinnassa. [138]

Yrityksissä ja yhteisöissä riskienhallinnan organisointi ja johtaminen on perinteisesti aiemmin sisällytetty, jonkin muun osa-alueen johtajan tehtäviin. Esimerkiksi rahoitusjohtaja tai turvallisuuspäällikkö ovat saattaneet kantaa päävastuun riskienhallinnasta. Tällöin oman toiminta-alueen erityistietämys on antanut painopisteen myös riskienhallinnan kohdalle ja riskienhallinnan kattavuus, ei ole ollut paras mahdollinen. Rahoitusjohtaja on esimerkiksi saattanut pitää riskienhallinnan painopisteen rahoitustoiminnoissa ja turvallisuuspäällikkö paloturvallisuudessa. Näin ollen riskienhallintaa ei ole aina nähty riittävän laaja-alaisesti. Suurissa yrityksissä tai yhteisöissä alkaakin olla nykypäivänä riskienhallintajohtaja, jonka ensisijaisena vastuuna on suunnitella ja organisoida yrityksen tai yhteisön riskienhallinta. Vastuu riskienhallinnasta tulee olla yrityksen tai yhteisön organisaatiossa riittävän korkealla, jotta valvontaa ja riskienhallinnan kehitystyötä voidaan tehokkaasti toteuttaa. Mikäli vastuuhenkilö ei ole organisaatiossa ylhäällä, on hänellä hankaluuksia tehokkaasti puuttua riskienhallinnan epäkohtiin, ja vahinkoa saattaa yritykselle tai yhteisölle muodostua, mikäli ongelmiin ei päästä puuttumaan riittävällä tehokkuudella. Riskienhallinnasta vastaava johtaja tai –päällikkö raportoi yleisimmin yrityksen tai yhteisön toimitusjohtajalle. [139]

Yrityksen tai yhteisön sidosryhmät vaativat organisaatiolta riskien hallintakykyä. Osakkaat tai sijoittajat, jotka sijoittavat esimerkiksi rahaansa yritykseen toivovat, että heidän sijoituksensa on pätevissä käsissä sekä suojattu kaikin mahdollisin keinoin riskeiltä, joihin pystytään ennakolta varautumaan. Myös asiakkaat tai yhteistyökumppanit edellyttävät, että yritys tai yhteisö on varautunut mahdollisten riskien varalta. Asiakkailla on oikeus vaatia, että hänen antamia tietojaan säilytetään huolellisesti. Myös yhteistyökumppanien kanssa tehtäviin yhteistyösopimuksiin, on nykypäivänä aiheellista liittää asiakkaiden tietojen käsittelyvaatimukset sekä kaikkien

[138] Kuusela & Ollikainen 2005: 126 – 129.

[139] Kuusela & Ollikainen 2005: 128 – 129.

sopimusosapuolten oikeudet ja velvollisuudet tietoriskien hallinnassa. Sijoittajat ovat erityisen kiinnostuneita sijoittamansa yrityksen arvosta. Arvo muodostuukin muun muassa tasearvosta sekä markkina-arvosta, johon on vaikuttamassa lukuisia seikkoja. Mikäli mahdolliset toteutuneet tietoturvaongelmat yrityksessä tulevat julki, on se itsessään aiheuttamassa kolhuja yrityksen imagoon ja tätä kautta yrityksen markkina-arvoon. Yritysten ja yhteisöjen tavoitteena tuleekin olla, että tieto joka ei ole julkista pysyy yrityksen ja yhteisön hallussa ja siihen pääsevät käsiksi vain tietoon oikeutetut ja kuitenkin samalla pystytään jakamaan ihmisille yhä enemmän kaikkien saataville tarkoitettua tietoa. Tietoriskien hallinta koostuu yrityksen johdon, operatiivisen johdon sekä yrityksen tai yhteisön kaikkien työntekijöiden noudattamista toimintamenetelmistä sekä tietojärjestelmien ja tietoliikenteen luotettavasta toiminnasta. Kaikilla tietoa käsittelevillä on vastuu huolellisesta tietojenkäsittelystä yrityksessä tai yhteisössä annettujen ohjeiden mukaan. [140]

4.5 Keskeiset keinot ja ennakoiva sopiminen

Riskien hallintaan yrityksessä tai yhteisössä on paljon erilaisia keinoja, ja riskienhallinta kokonaisuudessaan koostuukin useita erilaisia keinoja yhdistelemällä. Tiedon hallintaa osana yrityksen tai yhteisön riskienhallinnan kokonaisuutta ohjaa lukuisia erilaisia lakeja. Tiedonkäsittelyyn tavalla tai toisella liittyviä lakeja ovat muun muassa henkilötietolaki, työsopimuslaki, osakeyhtiölaki, arvopaperimarkkinalaki, laki sopimattomasta menettelystä liiketoiminnassa, teletoiminnan tietosuojalaki, tekijänoikeuslaki, patenttilaki, julkisuuslaki sekä toimialakohtaiset erityislait. [141] EU:n uuden tietosuoja-asetuksen olisi tarkoitus astua voimaan 25.5.2018. Nykyisin voimassa on henkilötietodirektiivi. Direktiivin ongelmana on ollut sen tulkinta eri maissa, joten uuden tietosuoja-asetuksen voimaantulon toivotaan tuovan tilanteeseen selkeyttä. [142]

Osakeyhtiölaki (21.7.2006/624) velvoittaa yritystä toimintojen organisointiin ja sitä kautta yhtiön omaisuuden hallintaan. Osakkailla on oikeus huolehtia yritykseensä sijoittaman sijoituksen arvosta ja yrityksen toimivan johdon onkin osoitettava huolellisuutta se pystyttävä osoittamaan sen miten yritys on järjestänyt tietojen ja tietojärjestelmien turvallinen käyttö. Osakeyhtiön mukaan yrityksen hallitus on ylin

[140] Kyrölä 2001: 52 – 54.

[141] Kyrölä 2001: 54 – 55.

[142] EU henkilötietodirektiivi (46/1995/Ey)

toimielin, jonka tehtäviin kuuluu huolehtia yrityksen sisäisestä ja ulkoisesta hallinnosta. Hallitus valvoo sekä myös ohjeistaa toimitusjohtajaa yrityksen johtamiseen liittyvissä asioissa. [143]

Arvopaperimarkkinalaki ohjaa yritystä erityisesti velvoittaen huomioimaan sisäpiiritiedon käytön yrityksen toiminnassa. Yrityksen on huomioitava, että kaikki organisaation jäsenet, jotka saavat mahdollisesti tietoonsa yrityksen toiminnasta oleellista julkaisematonta tietoa, ymmärtävät tiedon levittämisen vaikutuksen yrityksen arvoon. Yritysten tuleekin luoda käytännöt sisäpiiritiedon käsittelylle. Yrityksen sisäpiiriläisinä voidaan pitää kaikkia, jotka saavat tietoonsa julkisen kaupankäynnin kohteena olevasta yrityksestä tietoa, jolla saattaa olla vaikutusta yrityksen arvoon.[144]

Vaitiolo- ja salassapitovelvollisuudesta on merkitystä etenkin yrityksissä, joissa useat ihmiset pääsevät tekemisiin tietoihin, joilla on taloudellista tai ihmisten yksityiseen vaikutusta olevia tietoja. Työsopimuslain lojaalisuus- ja vaitiolovelvoitteet sekä kilpailukiellon merkitykset tulee olla selvillä kaikilla yrityksessä etenkin tiedon kanssa tekemisissä olevien ihmisten tulee tietää. Rikkomuksesta saattaa seurata vahingonkorvaus velvoite sekä työsopimuksen purkaminen. Työnantajalla onkin valvonta –sekä direktio oikeus.

4.6 Riskien huomioiminen sopimuksissa

Yrityksen tai yhteisön suunnitellessa riskienhallintaa, heidän kannattaa ottaa siinä huomioon ennakoiva näkökulma. Ennakoivan näkökulman omaksuminen edellyttää kuitenkin myös toimintamallien hahmottamista ennakoivalle sopimustoiminnalle. Kun kykenee hahmottamaan toimintamallit, se helpottaa myös ennakoivan sopimustoiminnan mahdollisuuksien hahmottamista liiketoiminnan johtamisen kannalta. Keskitalo on esitellyt kirjassa ”Ennakoiva sopiminen” kaksi yksinkertaistettua toimintamallia ennakoivan sopimustoiminnan integroimiseksi yrityksen liiketoimintaan. Toimintamallit ovat strateginen ja operatiivinen sopimuksellisen riskienhallinnan toimintamallit. Strateginen toimintamalli on koko yrityksen tai yhteisön

[143] Kyrölä 2001: 56 – 58.

[144] Kyrölä 2001: 58 – 59.

kokonaisvaltaiselle sopimustoiminnalle ja operatiivinen toimintamalli on yksittäisen transaktion suunnittelulle ja hallinnoinnille. [145]

Sopimuksellinen riskienhallinta on osa yrityksen juridista riskienhallintaa ja siten myös osa yrityksen yleistä laajaa riskienhallintaa. Tavoitteet eivät kuitenkaan rajoitu ainoastaan sopimustoiminnan juridisten riskien hallintaan, vaan hyvällä ja tehokkaalla sopimussuunnittelulla ja –hallinnoinnilla pyritään ennakoimaan ja estämään myös muita yrityksen tai yhteisön toiminnalle riskialttiita tapahtumia. Sopimuksellisesta riskienhallinnasta vastaavien tuleekin olla hyvin perillä koko yrityksen tai yhteisön toiminnasta ja sen hetkisistä mahdollisista uhkatekijöistä jotka voisivat olla vaikuttamassa yrityksen tai yhteisön toimintaan. Yrityksen tai yhteisön johdon näkökulma on yleensä johtaa siten, että pystyttäisiin huomioimaan liiketoiminnan mahdollisuudet. Riskienhallinnan johtamisen näkökulmana on taas huomioida liiketoiminnan riskit sekä turvata liiketoiminnan tulos. [146]

Suunniteltaessa yrityksen tai yhteisön sopimuksellista riskienhallintaa täytyy olla sisäistettynä liiketoimintamalli, liiketoiminnan strategia sekä riskienhallintastrategia. Ilman tätä osaamista sopimuksellinen riskienhallinta jää irralliseksi yksittäiseksi toiminnoksi. Lisäksi tulisi olla perillä myös yrityksen kilpailijoiden liiketoiminnasta sekä heidän strategioistaan. Luonnostaan on selvää, että yrityksellä tulee olla yleinen riskienhallinnan strategia. Yrityksen tai yhteisön sopimuksellinen riskienhallinnan strategian tulisi tarjota ratkaisun ainakin siihen mitkä ovat yrityksen tai yhteisön transaktioiden hallintamekanismit, millä sopimus instrumenteilla se toteutetaan sekä mitkä ovat sopimustoiminnassa ensisijaiset sopimuksiin sovellettavat oikeusnormistot. Tunnistettaessa riskejä on huomioitava, että sopimuksellinen riskienhallinta ei keskity ainoastaan sopimusriskien hallintaan vaan keskittyy sopimusoikeudellisin keinoin yrityksen tai yhteisön kaikkien liiketoiminnassa esiin tulevien riskien hallintaan. Sopimuksellinen operatiivinen riskienhallinta keskittyy yhden yksittäisen transaktioon liittyvien yksittäisten riskien hallintaan, arviointiin sekä sopimukselliseen käsittelyyn. Sopimuksellisessa riskienhallinnassa tulisi aina pyrkiä laajempaan kokonaisuuteen eli strategisen sopimuksellisen riskienhallinnan suuntaan. [147]

[145] Pohjonen ym. 2002: 241 – 242.

[146] Pohjonen ym. 2002: 244.

[147] Pohjonen ym. 2002:243.

5. PILVIPALVELUSOPIMUS TERVEYDENHUOLTOALAN OHJELMISTON TIETOTURVARISKIEN RAJAAJANA

5.1 Sopimus ja siihen liittyviä riskejä

Yritysten tai yhteisöjen välisiä sopimuksia luotaessa vallitsee merkittäviltä osin sopimusvapaus. Sopimuksellisen riskienhallinnan piiriin kuuluviin riskitekijöihin pystytään vaikuttamaan sopimussuunnittelulla. Liiketoiminnan ja transaktioiden riskien allokointi sopimuskumppaneiden kesken tapahtuu oikeusnormien avulla. Juridisten normien ohella transaktiota säätelee muutkin normit. Tällaisia ovat esimerkiksi moraaliset normit. Sopimuksellisessa riskienhallinnassa yrityksen tai yhteisön toimintaa ei voi kuitenkaan rakentaa ainoastaan näiden varaan. Nämä oikeusnormit sääntelevät sopimusta, mikäli sopimuskumppanit eivät ole niitä sopimuksessaan muuttaneet. Pelkästään oikeusnormien hahmottaminen oletusnormeina ei ole riittävää, koska tulkintaan vaikuttavat niiden ohella myös esimerkiksi vallitseva kauppatapa ja –käytäntö, vakiosopimusehdot ja standardit. [148] Sopimusprosessin eri vaiheisiin liittyy erilaisia riskitekijöitä. Vastuuriski on yksi merkittävimmistä riskeistä, joihin pyritään varautumaan huolellisella sopimussuunnittelulla. Tärkeää on, että pystytään mahdollisimman selkeästi määrittelemään sopimuksen perusteella, kuka on missäkin tilanteessa vastuussa riskien realisoituessa. Sitovuusriski tarkoittaa taasen sitä, että riskin realisoituessa sopimus jää sitomattomaksi. Tällaisia tilanteita saattavat olla esimerkiksi sellaiset tilanteen, joissa laadittu sopimus on kilpailuoikeudellisen lainsäädännön vastainen. Mikäli sopimusehdot on jostakin syystä muotoiltu epätäsmällisesti, saatetaan joutua ehtoja tulkittaessa tilanteeseen, jossa tulkinta on ristiriidassa osapuolen odotusten kanssa. Tällöin epätäsmällisten ehtojen vuoksi, eivät osapuolet pysty kaiken kattavasti tulkitsemaan ehtoja siten, että päädyttäisiin aukottamaan tulkintaan. Sopimuskumppanin luotettavuus on myös yksi ehdottaman tärkeistä tekijöistä. Laajasti katsoen sillä voidaan tarkoittaa sitä, että sopimuskumppanin tulee pystyä täyttämään kaikki häneltä sopimustilanteessa vaadittavat ominaisuudet ja valmiudet. Sopimuksiin liittyy myös tietynlaisena perusriskinä, odottamattoman kehityksen mahdollisuus. Tämä saattaa tarkoittaa esimerkiksi sitä, että sopimuskumppani jättää velvollisuutensa hoitamatta tai että odottamattomat ulkoiset tekijät vaikuttavat siihen jotta sopimus ei toteudu suunnitelman mukaisesti. [149]

[148] Pohjonen ym. 2002: 249 – 250.

[149] Aalto-Setälä ym. 2004: 13.

Sopimusneuvotteluissa päästyä valmisteluvaiheeseen, saattavat tapahtumat johtaa vastuuvaikutuksiin. Näin käy mahdollisesti silloin, mikäli toisen sopimusosapuolen väitetään menetelleen neuvotteluvaiheessa moitittavasti tai mikäli sopimuksen voimaantulosta syntyy erimielisyyttä. Korvausvaatimukset jotka pohjautuvat sopimuksentekotuottamukseen eivät ole vielä kovin yleisiä, mutta näyttäisivät olevan lisääntymässä. Syynä tähän on sopimusvalmistelujen kustannusten nousu. Tämän vuoksi olisikin tärkeää, että kun neuvotellaan taloudellisesti hyvin arvokkaista sopimuksista, sovittaisiin ennen neuvottelujen aloittamista sopimusneuvotteluista aiheutuneiden kustannusten jakamisesta. Useimmiten sopimusneuvotteluissa sopimusosapuolet vastaavat omista aiheutuneista kustannuksistaan. Ennen neuvotteluiden aloittamista olisi tärkeää vahvistaa tämä lähtökohta sekä sopia, että sopimuksen mahdollinen syntymättä jääminen ei muuta tätä tilannetta. Mikäli sopimusosapuolet kuitenkin haluavat lähteä jakamaan aiheutuneita kustannuksia, tulisi tästä tehdyssä sopimuksessa yksilöidä toimet sekä sovellettavat kustannusten jakoperusteet. Ennakolta kustannuskysymyksestä sopimisessa on se etu, että vallitseva oikeustila selkeytyy ja sopimusosapuolet tiedostavat kustannusten jakautumisen entistä selvemmin. [150]

Sopimusneuvotteluiden perusperiaatteita sekä kansallisesti että kansainvälisesti on neuvotteluvapaus sekä neuvotteluriski. Tämä tarkoittaa sitä, että mahdollisesta sopimuksesta neuvotteleminen ei sellaisenaan perusta velvollisuutta sopimuksen päättämiseen eikä aiheuta vastuuta sopimusosapuolelle neuvotteluista aiheutuneista kustannuksista. Mikäli sopimusosapuolet ovat ennen sopimusneuvotteluiden aloittamista solmineet sopimuksen aiheutuvien kustannusten jakamisesta, on se muuttamassa neuvotteluosapuolten välisten kustannusten jakautumista. Mikäli sopimusneuvotteluissa voidaan todistaa toisen neuvotteluosapuolen neuvottelukäyttäytymisen olleen moitittavaa, voi toinen osapuoli vaatia vahingonkorvausvaadetta. Sopimusten valmisteluun liittyvissä toimissa jotka koskevat vastuuriskien hallintaan, onkin oleellista kiinnittää huomiota neuvottelumenettelyn asianmukaisuuteen. Sopimusneuvottelut saattavat joskus kestää hyvinkin pitkään ja käytyjen neuvotteluiden pohjalta saattaa toinen osapuoli kokea, että sopimusneuvottelut tullaan saattamaan loppuun saakka. Aina on kuitenkin olemassa riski, ettei lopullista sopimusta tulla kirjoittamaan. Joskus saattaakin olla aiheellista muistuttaa sopimuskumppania tästä, mikäli hän on pitkälle edenneissä neuvotteluissa ryhtymässä toimenpiteisiin, joista on aiheutumassa jo merkittäviä kustannuksia. Hyvin toteutettu ja

[150] Aalto-Setelä ym. 2004: 14.

totuudenmukainen informaatio vallitsevasta tilanteesta on yleensä käyttökelpoinen tapa kaventaa neuvotteluvastuun riskiä. Maininta siitä, että neuvotteluosapuoli ei ole sitoutunut vielä mihinkään onkin hyvä sisällyttää neuvottelupöytäkirjaan. [151]

Yritykset tai yhteisöt saattavat käydä samaan aikaan sopimusneuvotteluita useiden mahdollisten sopimuskumppaneiden kanssa. Sopimusneuvotteluiden edetessä oikeustila saattaa kuitenkin muuttua osapuolten sopiessa, että neuvotteluiden jatkuessa ei ole sallittua neuvotella muiden sopimusehdokkaiden kanssa. Tällöin mikäli yritys tai yhteisö jatkaa neuvotteluita toisen sopimusehdokkaan kanssa se saattaa johtaa korvausvastuuseen. Sopimusneuvotteluissa harhaanjohtavien tietojen antaminen saattaa myöskin johtaa korvausvastuuseen. Mikäli neuvottelut eivät jatku sopimuksen allekirjoittamiseen saakka toisen osapuolen vilpillisen toiminnan vuoksi, se saattaa johtaa vilpillisen osapuolen velvollisuuteen korvata sopimusneuvotteluiden valmistelukulut vastapuolelle. [152] Mikäli toisen neuvotteluosapuolen perimmäisenä tarkoituksena ei ole ollut päättää neuvotteluja sopimuksen allekirjoittamiseen, tulee kyseeseen toisen neuvottelun osapuolen kulujen korvaaminen. Tällä korvauksella pyritään saattamaan toinen neuvotteluosapuoli sellaiseen asemaan, joka hänellä olisi ollut ilman neuvotteluiden käymistä. [153]

Sopimusoikeudellinen korvausvastuu on sopimusrikkomusperusteista. Laadittaessa sopimusta siihen tuleekin tarkasti pohtia kirjattavat seikat, jotta velvoitteet sekä oikeudet ovat täsmällisesti, yksiselitteisesti sekä riittävän kattavasti tuotu esiin. Näillä sopimukseen kirjatuilla tiedoilla on suuri merkitys sopimuksen perustamien vastuuriskien kannalta. Ristiriita tilanteissa velvoitteet määritelläänkin laaditun sopimuksen tulkinnan sekä täydentävän lainsäädännön perusteella. Asiantuntijapalveluissa huolellisuusvaatimus on asetettu yleisesti varsin ankaraksi. Kun esimerkiksi palveluntoimittaja vastaa henkilö- ja muita arkaluonteisia tietoja sisältävien suurien tietovarastojen säilytyksestä, huolellisuusvaatimus on erittäin korkea. Tällöin on luonnollista, että palveluntoimittajan täytyy kyetä riittävällä varmuudella huolehtimaan hänelle velvoitetuista tehtävistä. [154]

---

[151] Aalto-Setälä ym. 2004: 14-15.

[152] Aalto-Setälä ym.2004: 16.

[153] Saarnilehto 2005: 68 – 69.

[154] Aalto-Setälä ym. 2004: 17-18.

Nykypäivän liike-elämässä usein yhtä tuotetta tai palvelua on valmistamassa useita eri yrityksiä, joiden kanssa tilaajalla on liikesuhde. Tällöin myös sopimuksia suunniteltaessa on otettava huomioon mahdolliset valmistajan alihankkijat tai palveluntoimittajat. Pilvipalveluissa palvelua toteuttamassa saattaa olla useita eri palveluntoimittajia. Pilvessä ajettavia sovelluksia tarjoava yritys saattaa olla sopimussuhteessa oman asiakkaansa lisäksi pilvialustan tarjoavaan PaaS-palveluntoimittajaan. PaaS- palveluntoimittaja taas saattaa olla sopimussuhteessa pilvi-infrastruktuurin IaaS- palveluntoimittajaan. Lisäksi uutena tekijänä palveluntoimittajien verkossa saattaa olla mukana pilvipalvelun välittäjä, joka tarjoaa ja kokoaa lukuisista pilvipalveluista asiakkaalleen kokonaisratkaisun. Pilvipalvelun välittäjä saattaa tarjota asiakkaalle tarjottujen palveluiden päälle esimerkiksi omaa käyttöliittymää tai hän voi olla konsultti joka ainoastaan toimii välikätenä palveluntoimittajien ja asiakkaan välillä. [155]

5.2 Tyypillisimmät sopimustyypit IT-alalla

Suuret IT-alan toimeksiannot ovat yleensä projektimuotoisia. Sopimusosapuolten välille solmitaankin tällöin yleensä *projektisopimus*. Sen tavoitteena on varmistaa projektin tavoitteiden saavuttaminen. Useimmiten sopimuskumppaneina on työn tilaava asiakas sekä työn toteuttaja. Projektien tavoitteena on yleensä jonkin asian kehittäminen tai tietojärjestelmän toimittaminen. Terveydenhuoltosektorilla isoja projektiluontoisia hankkeita on ollut esimerkiksi KANTA- järjestelmän luominen. Ohjelmistosovellus voidaan toimittaa asiakkaalle tilaustyönä ja tällöin sopimusosapuolten velvoitteet määritellään projektisopimuksen kautta. [156]

Yrityksen tai yhteisön tilatessa uusi tietojärjestelmä tai uudistaessaan vanhaa sopimusosapuolten välille saatetaan solmia tyypillisesti hankintasopimus. Tietojärjestelmä koostuu tyypillisesti fyysisistä osista eli laitteista sekä käyttöjärjestelmistä ja erilaisista sovellusohjelmista. Hankintasopimuksiin sisältyy useimmiten myös järjestelmän käyttöönotto erilaisine asennuksineen, loppukäyttäjien koulutus sekä järjestelmän ylläpito. Hankintasopimuksessa on useimmiten sovellettavan lainsäädännön sekä sopimuksen sisällön suhteen hyvin erilaisia piirteitä. Hankintasopimus voitaisiinkin myös eriyttää selkeyden vuoksi useiksi erillisiksi

[155] Böhm ym. 2010:

[156] Takki 2002: 191 – 193.

sopimuksiksi, jolloin myytävästä tai leasing-vuokratusta laitteistosta, ohjelmistosta sekä ylläpitopalvelusta tehtäisiin omat erilliset sopimuksensa. Tämän sekatyyppisen sopimuksen sopimusosapuolina on yleensä tietojärjestelmän tilaaja sekä järjestelmän toimittava yritys. [157]

Tietojärjestelmien asiakkaalle luovutuksen jälkeen, käyttöönottoa seuraa ylläpitovaihe. Tänä aikana järjestelmään saatetaan tehdä korjauksia ja tarvittaessa muutoksia. Nämä sopimukset voidaan jakaa *huoltosopimuksiin*, *ylläpitosopimuksiin* sekä *tukisopimuksiin*. Huoltosopimuksilla tarkoitetaan järjestelmän laitteiston korjaamista sekä sekä tarvittavia muutoksia. Ylläpitosopimuksilla tarkoitetaan ohjelmistojen päivittämistä, ohjelmistovirheiden korjaamista sekä mahdollisten uusien ominaisuuksien lisäämistä. Tukisopimuksilla tarkoitetaan käyttäjien opastamista sekä etätukea. Sopimuksellisesti on tärkeää, että palvelujen sisältö on määritelty mahdollisimman tarkkaan. Kun määrittely on tehty huolellisesti, vältytään monilta ongelmatilanteilta. [158]

Konsultointisopimuksilla tarkoitetaan asiantuntemuksen tarjoamista kolmannelle osapuolelle korvausta vastaan. Konsultointi on usein erilaisten selvitysten tekemistä, joiden avulla asiakkaan toimintaa voidaan saada tehokkaammaksi. Konsultointi voidaan luokitella toimintavelvoitteeseen tai tulosvelvoitteeseen perustavaksi. Toimintavelvoitteisessa sopimuksen kohteena on itse tehty työ. Tulosvelvoitteisessa sopimuksen kohteena taasen on työn lopputulos.

Ohjelmistolisenssisopimus on yleisin sopimustyyppi tehtäessä ohjelmistosovelluksien kauppaa. Tämän tyyppinen sopimus mahdollistaa rajoitetun käyttöoikeuden ohjelmistoon, mutta tekijänoikeuksien haltija ei kuitenkaan luovu oikeuksistaan. Myös tämäntyyppinen sopimus on sekatyyppinen, eli sopimukseen saattaa kuulua monenlaisia muitakin ehtoja sovelluksen käytön lisäksi. [159]

Ohjelmistovuokraussopimus on jo askel kohti pilvipalvelusopimusta. Ohjelmistovuokraussopimuksella tarkoitetaan sitä, että asiakas ei osta itselleen ohjelmistolisenssiä. Sen sijaan hän saa vuokraussopimukselle avulla käyttöoikeuden käyttää ohjelmistoa, joka kuitenkin sijaitsee fyysisesti palveluntoimittajan palvelimella. Ohjelmistosovelluksen kehittäjä saattaa itse vuokrata sovellustaan eteenpäin, tai sitten palveluntoimittaja on ostanut lisenssin sovellukseen ohjelmiston kehittäjältä ja vuokraa

[157] Salonen 2000:

[158] Takki 2002: 236 – 237.

[159] Välimäki 2009: 152.

sovellusta nyt eteenpäin. Ohjelmiston kehittäjän ja palveluntoimittajan on täytynyt tällöin tehdä lisenssisopimus, jossa he ovat sopineet oikeudesta ohjelmiston edelleen jakeluun.[160]

5.3 Vakiintuneet sopimusmallit ja –käytännöt

Ohjelmistosovellusten sopimuksiin käytetään yleisesti erilaisia vakiintuneita sopimusmalleja ja –käytäntöjä. Tämä osin siitä syystä, että sopimusten teko vaatii runsaasti aikaa ja resursseja. Kun pystytään hyödyntämään olemassa olevia alan yleisiä käytäntöjä, sekä osapuolille jo mahdollisesti ennestään tuttuja sopimusehtoja, kaikki sopimusosapuolet ymmärtävät laaditut sopimukset paremmin ja mahdollisia ristiriitatilanteita pystytään ennalta ehkäisemään.

Terveydenhuoltoalan ohjelmistosovellusten kohdalla, kun käsitellään henkilötietoja ja muuta arkaluonteisia tietoja sisältävää aineistoa, niin on erityisen merkityksellistä, että kaikille sopimusosapuolille on selvää, mitä tehdyissä sopimuksissa sovitaan esimerkiksi tietosuojaan liittyvissä seikoissa. Pilvipalveluympäristössä toimiessa esimerkiksi tietojen säilyttäminen on tärkeä sovittava asia. Terveydentilaan ja henkilötietoihin kohdistuvassa tietoaineiston kohdalla, tietojen säilytykselle on olemassa lainpuolelta esimerkiksi säilytysmaata koskevia rajoitteita. On tärkeää, että myös tästä on olemassa sopimuksessa selkeät sopimuskohdat. Henkilötietolaissa pykälissä 22, 22a, 23, 36 ja 37 käsitellään tietojen siirtoa ulkomaille. [161]

5.3.1 Vakiosopimukset

Vakiosopimukset ovat hyvin yleisesti IT-alalla käytettyjä. Vakiosopimuksilla tarkoitetaan sitä, että sopimusta ei ole yksilöllisesti neuvoteltu sopimuskumppanin tai kumppanien kanssa. Hyvin yleistä on, että tehty sopimus koostuu vakioehdoista sekä osin sopimusosapuolten välillä neuvotelluista ehdoista. Tällaisen sekamuotoisen sopimuksen ollessa kyseessä on tärkeää, että sopimuksessa on mainittu erillisistä vakioehdoista, jotta ne tulisivat osaksi varsinaista sopimusta. Tällöin sopimusosapuolten on täytynyt olla mahdollisuus tutustua ennakolta sopimusehtoihin. Yritys voisi laatia

[160] Kulmala 2003: 8 – 11.

[161] Ylipartanen2004: s. 112.

käytettävät vakioehdot itse, mutta yleisesti yritysten- ja yhteisöjen välisissä sopimuksissa käytetään IT-alan yleisiä sopimusehtoja. Vakioehdoille on olemassa tietyntyyppisiä tunnusmerkkejä. 1. Ehdot laaditaan käytettäväksi niitä jatkossa useissa yksittäisissä sopimuksissa. 2. Ehdot laaditaan erityisesti myös myöhempiä tulevia sopimuksia silmälläpitäen. 3. Näitä laadittuja sopimusehtoja on tarkoitus käyttää monien eri sopimuskumppanien kanssa. [162]

Useimmiten vakiosopimusehdot ovat hyvin erilaajuisia ja erilaisia. Niitä ei muodosteta jotakin tiettyä sopimussuhdetta ajatellen, vaan yleisesti käytettäväksi useissa samantyyppisissä sopimussuhteissa. [163]Vakiosopimusehdot voi laatia sopijakumppani yksin tai yhdessä toisen sopimusosapuolen kanssa, mutta yleisempää on, että käytetään vakioehtoja jotka on laatinut jokin kaupanalan järjestö.[164] Suomessa ehkä tunnetuin IT-alalla käytettävä vakiosopimus on IT2015-sopimusehdot. Sen ovat laatineet yhdessä Keskuskauppakamari, Ohjelmistoyrittäjät ry, Suomen osto- ja logistiikkayhdistys LOGO ry, Teknologiateollisuus ry sekä Tietotekniikan liitto ry. IT2015 on korvannut aiemmin julkaistut IT2010 sekä IT2000-sopimusehdot. Uusimmassa IT 2015-sopimusehdoissa on aiempaa tarkemmin otettu huomioon myös pilvipalveluihin sekä tietoturvaan liittyvät seikat. [165] JIT2015 – ehdot ovat julkisen sektorin vakioehtokokoelma. Niiden käyttöä suositellaan kun kyseessä on julkishallinnon yksikkö. JIT2015-ehdot koostuvat myös yleisistä sopimusehdoista sekä erityisehdoista.

Sopimusasiakirjaan voidaan laittaa termi agreed documents. Tämä tarkoittaa sitä, että sopimuskumppanit tai näiden edunvalvontatahot ovat ne yhteisesti laatineet. IT-alan yleiset sopimusehdot eivät automaattisesti tule pelkän olemassaolonsa vuoksi sopimuksen velvoittavaksi sisällöksi. Tästä kuitenkin poikkeuksena on sellaiset normisopimukset, jotka lain perusteella muodostavat jonkin myöhemmin solmittavan sopimuksen minimiehdot. Yleisenä lähtökohtana onkin, että vakiosopimusehdot on saatettava voimaan selkeällä tahdonilmaisulla. Viittaus vakioehtoihin on yleensä riittävä, mikäli sopimuskumppaneilla on ollut mahdollisuus tutustua ehtoihin ennakolta. Mikäli sopimuskumppanit ovat jatkuvassa yhteistyössä keskenään, ei viittaamista vakioehtoihinkaan välttämättä pidetä tarpeellisena. Etenkin agreed documents

[162] Salonen 2000: 63 – 65.

[163] Wilhelmsson 2008: 36.

[164] Salonen 2000: 65.

[165] Erlund, Lindfors, Salminen & Turunen 2016: 31 – 34.

tyyppisissä vakioehdoissa sopimuskumppaneiden aikaisempi sopimuskäytäntö saattaa riittää liittämään laaditut ehdot osaksi sopimusta. [166]

Sille katsotaanko laaditut vakiosopimusehdot osaksi sopimusta, voidaan asettaa tiettyjä yleisiä kriteerejä. Ennen kaikkea merkitystä on tietenkin vakiosopimusehtojen sisällöllä jolle voidaan antaa merkitystä. [167] Samoin se, että ovatko sopimuskumppanit miten tasavertaisia keskenään. Mikäli sopimuskumppanit ovat hyvin paljon epätasapainossa oikeuksien ja velvollisuuksien suhteen, voidaan asettaa suurempia vaatimuksia selkeälle tahdonilmaisulle, jotta sopimusosapuolten todellinen tahto tulee selvästi esiin. Jos sopimusehdot ovat yksipuolisesti vaan toisen sopimuskumppanin laatimia, esitetään myös tässä tapauksessa selkeälle tahdonilmaisulle enemmän painoarvoa. Myös sille mikä on sopimuskumppanien tiedollinen ja taloudellinen tasa-arvo saattaa asettaa suurempia vaatimuksia ehtojen sitovuuden käyttöönottoon. Erityisesti se, mikäli ehdot ovat hyvin vaikeaselkoisia tai ehtojen kieli on sopimuskumppanille vieras. Myös sopimuskumppanien tahdonilmaisun laadulla on merkitystä. Mikäli sopimusasiakirjaan on painettu sopimusehdot, saattaa sopimuskumppani helposti kokea tilanteen sellaiseksi, että hänellä ei ole muuta mahdollisuutta kuin hyväksyä ehdot sellaisenaan. Yleisen kauppatavan perusteella vakioehdot eivät aina vaikuta sitovasti. Vaikutusta on sillä kenen toimesta vakioehdot on laadittu. Mikäli tilausvahvistukseen on liitetty vakioehdot, ja sopimuskumppani ei ole siinä yhteydessä niistä reklamoinut, vakioehdot tulevat sopimuskumppaneita sitoviksi. Mikäli sopimusaikana toinen osapuoli yksipuolisesti lähtee sopimusehtoja muuttamaan, se ei tee tehtyjä muutoksia sitoviksi. [168]

Aina vakioehdot eivät kuitenkaan tule sitoviksi. Kuitenkin, sitomattomuus on aina poikkeus ja ensisijaisesti kaikkia sopimukseen sisällytettyjä vakioehtoja on pidettävä sopimuskumppaneita sitovina. Sopimusta tehdessä saattaa kuitenkin käydä niin, että vakioehtoja ei käydä läpi yksityiskohtaisesti ja vakioehtojen ja sopimukseen yksilöityjen ehtojen välille saattaa syntyä ristiriita. Tässä tapauksessa ristiriita ratkaistaan yksilöityjen sopimusehtojen mukaisesti. Sopimusasiakirjaan kannattaakin kirjata lause jossa mainitaan, että ristiriita tilanteissa on yksilöityä sopimusehtoa noudatettava ennen vakiosopimusehtoa. Yllättävien ja erityisen ankarien vakioehtojen kohdalla, sitovuuden kriteeriksi on asetettu, että sopimusosapuolen tulee korostaa

[166] Salonen 2000: 66.

[167] Wilhelmsson 2006: 67.

[168] Salonen 2000: 67 – 68.

tällaisten ehtojen sitovuutta. Sopimusosapuolta tulee asiasta informoida ja useimmiten sopimusasiakirjassa tällaiset kohdat onkin alleviivattu, tummennettu tai muuten tuotu selvästi esiin. Oleellista sitovuuden kannalta on, että vastapuoli on havainnut ehdon olemassaolon ennen sopimukseen sitoutumista. Mikäli vakioehdot aiheuttavat epäselvyyden vuoksi tulkinnassa vaikeuksia on tehty periaate, että vakioehtoja tulkitaan ehtojen laatijan vahingoksi. Tällöin, mikäli jotakin ehto voidaan tulkita monella tavalla, se on ymmärrettävä siten, että se on sopimusosapuolelle edullisempi. Oikeustoimilain 36§:n mukaan sovittelusäännös koskee sekä yksilöllisiä, että vakiosopimusehtoja. [169]

5.3.2 Salassapitoehto

Tarkasteltaessa lainsäädäntöä sekä yritys- ja liikesalaisuuksien suojaa huomataan, että suoja ei ole täysin aukoton. Eri maiden välillä saattaa vielä olla suuria eroavaisuuksia suojan suhteen. [170] Sopimusosapuolien välillä on tyypillistä solmia erilaisia salassapitosopimuksia. Näiden sopimuksien tarkoituksena on turvata omia liikesalaisuuksia sekä saavutettuja kilpailuetuja. Yleensä suojattavia asioita ovat esimerkiksi erilaiset kaupalliset tiedot, kuten asiakastietokannat, hinnoittelu ja liiketoiminnan strategiat. Salassapitosopimus saattaa sisältyä johonkin muuhun sopimukseen liitteenä, tai sitten se voidaan tehdä omana itsenäisenä sopimuksenaan. Salassapitosopimuksen pääsisältö on, että toista tai kaikkia sopimusosapuolta kielletään sopimussakon uhalla käyttämästä tai jakamasta määrättyjä tietoja muuhun kuin ennalta sovittuun tarkoitukseen. [171] Kansallinen lainsäädäntö on osin jo itsessään suojaamassa liikesalaisuuksia. Laissa (1061/1978) sopimattomasta menettelystä elinkeinotoiminnassa, mainitaan 4§:ssä, että ”kukaan ei saa oikeudettomasti hankkia tai yrittää hankkia tietoa liikesalaisuuksista eikä käyttää tai ilmaista näin hankkimaansa tietoa”. Työsopimuslaissa (55/2001) taas on mainittu, että ”työntekijä ei saa työsuhteen kestäessä käyttää hyödykseen tai ilmaista muille työnantajan ammatti- tai liikesalaisuuksia. Jos työntekijä on saanut tiedon oikeudettomasti, kielto jatkuu myös työsuhteen päättymisen jälkeen”. Nämä lakikohdat eivät itsessään riitä kuitenkaan suojaamaan täysin, koska esimerkiksi työsopimuslaki suojaa lähinnä työsuhteen keston ajan, mutta ei ole niinkään suojaamassa siinä vaiheessa kun työntekijä vaihtaa

[169] Salonen 2000: 69 – 71.

[170] Honkinen ym. 2016: 120.

[171] Hemmo 2005: 325 – 327.

työnantajaa. Usein onkin tarpeellista suojata salassapidettäviä asioita myös yrityksen työntekijöille suunnatulla salassapitosopimuksella. [172]

Yksi salassapitoon liittyvistä merkittävimmistä seikoista on ketkä ovat tiedonsaantiin oikeutettuja henkilöitä. Nämä on tarpeellista selvästi täsmentää silloin, kun käsitellään arkaluonteista tai yritykselle hyvin kallisarvoista tietoa. Tiedonluovuttamisen oikeus esimerkiksi alihankkijoille tai muille kolmansille osapuolille saattaa aiheuttaa myös salassapitoon liittyvän riskin. Luotaessa salassapitosopimusta, onkin aiheellista luetteloida, millaisissa tilanteissa ja kenelle, on oikeus tietoa luovuttaa. Sopimuksen solmimisen jälkeen tulee usein tilanteita, joita ei ole sopimukselle tekovaiheessa osattu laittaa. Tällöin on aiheellista sopimuskumppaneilta varmentaa erikseen, onko tiedonluovuttaminen kyseiselle taholle tai henkilölle soveliasta. Tällöin sovittaessa tietojen siirrosta kolmannelle osapuolelle, onkin aiheellista solmia samansisältöinen salassapitosopimus myös hänen kanssaan. Henkilötietojen tietoturvaan liittyvä merkittävä seikka salassapitosopimusten kohdalla on maininta, että luovutettua aineistoa ei saa luvattomasti kopioida ja mikäli aineistoa jää kolmannen osapuolen haltuun sopimuksen päättyessä on se palautettava tai tuhottava sopimuksen mukaisesti. [173] Salassapitosopimus saattaa usein olla sisällöltään varsin lyhyt, mutta sisältää kuitenkin asioita, joiden määritteleminen kannattaa tehdä huolellisesti, jotta riittävä suoja saadaan aikaiseksi. [174]

5.3.3 Escrow-ehdot

Sanalla escrow – tarkoitetaan sitä, että ostettavan ohjelmiston lähdekoodin kopio siirtyy kolmannen osapuolen haltuun. Tätä osapuolta kutsutaan escrow – agentiksi ja hän vastaa ainoastaan lähdekoodin säilyttämisestä sekä sopimuksessa määritellyissä tilanteissa koodin luovuttamisesta ohjelmiston hankkijalle. Tämä escrow-ehto on sopimustekninen keino turvata pääsy ohjelmistoon jonka osapuoli on hankkinut tilanteissa, joissa esimerkiksi ohjelmiston valmistajan toiminta loppuu. Tällaisissa tilanteissa myös ohjelmiston kehitystyö päättyy ja pelkona on, että ohjelmiston elinkaari on hiipumassa. Mikäli tällainen tilanne tulee, niin ohjelmiston hankkijalla on mahdollisuus etsiä toinen ohjelmistotalo, joka alkaa heidän käytössään olevaa

[172] Hemmo 2005: 326-327.

[173] Hemmo 2005: 328 – 329.

[174] Honkinen ym. 2016: 122 – 123.

ohjelmistoa kehittämään ja ylläpitämään. Tämä ei tarkoita tekijänoikeuden siirtymistä vaan sillä varmistetaan, että ohjelmiston tekijän lopettaessa toimintansa, ohjelmiston kehittäminen ja ylläpitäminen on vielä ohjelmiston hankkijan näin halutessa mahdollista. [175]

Tämä ehto ei suoranaisesti ole aiheuttamassa tietosuojaan riskiä, koska kolmannelle osapuolelle luovutetaan ainoastaan ohjelmiston lähdekoodi. Päinvastoin se, että ohjelmiston kehittäminen sekä ylläpito on mahdollista ohjelmiston valmistajan mahdollisen toiminnan loppumisenkin jälkeen, on suojaamassa arvokasta tietoaineistoa mahdolliselta vahingolta.

5.3.4 Vahingonkorvaus ja vastuunrajoituslausekkeet

Sopimusoikeudellisesti vahingonkorvausvelvollisuus on tärkeä seuraamus. Sen tarkoituksena on hyvittää samoja intressejä kuin esimerkiksi sopimussakolla tai hinnanalennuksilla. Mikäli yrityksen tai yhteisön hankkimassa ohjelmistossa havaitaan virhe, josta aiheutuu vahinkoa ohjelmiston hankkineelle tai jollekin muulle taholle, on ohjelmiston valmistaja kauppalain 30 §:n mukaan korvausvelvollinen aiheutuneista vahingoista. Vahinko voi aiheutua suoraan esimerkiksi saamatta jääneestä voitosta tai kuluista tai se voi olla välillistä esimerkiksi tuotannon keskeytyminen tai omaisuuden vahingoittuminen. Ohjelmistossa havaitusta virheestä saattaakin näin ollen aiheutua laaja ja melko mittava korvausvastuu ohjelmiston valmistajalle. Sovittaessa vahingonkorvauksesta on se lähes aina vastuuta rajoittavaa. Tämä sen vuoksi, että laki ja sopimusoikeudelliset periaatteet ovat suojaamassa vahingon kärsinyttä osapuolta melko laajasti. [176]

Rajoitettaessa vahingonkorvausvelvollisuutta lähdetään yleensä siitä, että jotain tiettyjä vahinkolajeja ei korvata lainkaan. Kaikkein tyypillisin ja lukuisissa sopimuksissa käyttökelpoinen ehto on, että vastuun ulkopuolelle suljetaan välilliset vahingot. Myös tässä kohdassa on tärkeää tarkemmin eritellä mitä välillisillä vahingoilla kyseisessä sopimuksessa tarkoitetaan, koska puhutaan hyvin laajasta käsitteestä. Toisena tärkeänä ja paljon käytettynä rajoitusehtona on vastuun enimmäismäärän rajoittaminen. Usein

[175] Takki 2002: 222.

[176] Hemmo 2005: 239.

korvausvelvollisuuden enimmäisraja on määritelty sopimukseen. Riskienhallinnan kannalta vastuunrajoitusten ja sopimusehtojen huolellinen suunnittelu on tärkeää. [177]

5.4 Pilvipalvelusopimuksen erityispiirteitä

Kuluttajille tarjottavien palveluiden pilvipalvelusopimukset ovat yleensä varsin yksipuolisia. Palvelu ja sopimukset ovat kaikille kuluttajille samanlaiset. Näissä sopimuksissa ei ole neuvottelunvaraa, vaan mikäli kuluttaja haluaa kyseisen palvelun, on hänen hyväksyttävä kyseiset sopimusehdot. B2B-sopimuksissa, joissa sopimusosapuolina on palveluntoimittaja sekä pilvipalveluasiakkaana yritys tai organisaatio, ja pilvipalvelu ei ole mikään bulkkituote, voidaan sopimusehdoista neuvotella usein yksityiskohtaisesti.[178]

Ennen pilvipalvelun käyttöönottoa tulee koko prosessi suunnitella hyvin huolellisesti. Talletettaessa pilveen henkilötietoja sekä potilastietoja, on hyvin tarkasti sekä teknisellä, että sopimuksellisella suunnittelulla pyrittävä huolehtimaan siitä, että tietojen vuoto vääriin käsiin on lähes mahdotonta. Pilvipalvelusopimus on periaatteessa laaja erilaisten sopimusten yhdistelmä. Sopimuskokonaisuus voi sisältää esimerkiksi ohjelmistopalvelusopimuksen, ohjelmistopalvelun palvelukuvauksen ja hinnat, palvelutasokuvauksen, IT2015 ETP erityisehtoja tietoverkon välityksellä toimitettavista palveluista sekä IT2015 YSE yleiset sopimusehdot. [179] JIT 2015 ehtoja noudatetaan julkisensektorin hankintayksiköiden tekemisissä IT –tuotteiden ja –palveluiden hankinnassa. Myös nämä sopimusehdot sisältävät sekä yleiset- että erityisehdot tilanteeseen sopivan sopimuksen muodostamiseksi. [180]

5.4.1 Sopimuskokonaisuus ja sopimusasiakirjojen suhde toisiinsa

Sopimuksia solmitaan sekä asiakkaan ja palveluntoimittajan, asiakkaan ja välittäjän sekä välittäjän ja palveluntoimittajan välillä. Pilvipalveluntoimittajan ja -asiakkaan

[177] Hemmo 2005: 247 – 249.

[178] Lakius 2017, Digitaalisen liiketoiminnan lakiopas.

[179] Erlund, Lindfors, Salminen & Turunen: 2016: 373 – 374.

[180] Järvenoja ym. 2015: 21 – 23.

välinen sopimus on nimeltään ohjelmistopalvelusopimus. Tämän sopimuksen kohteena on pääsy suljettuun palveluun. Pilvipalvelusopimus on tyypiltään sekatyyppinen. Sen sopimisen kohteena voi olla palvelun käyttöoikeuden ohella esimerkiksi ylläpitopalvelujen tarjoaminen sekä käytön tuki. Palveluntoimittajalle kuuluu velvollisuuksiin huolehtia palvelinsalin laitteiston ja ohjelmiston toimimisesta, mahdollisten päivitysten asentamisesta ja toimintakuntoisuudesta huolehtiminen. Asiakkaan velvollisuuksiin kuuluu käyttää ohjelmistoa sellaisessa tarkoituksessa sekä menetelmällä kuin sopimuksessa on mainittu.

Palvelutasosopimuksella määritetään palveluntoimittajan takaama minimitaso. Mikäli käy niin, että palvelussa tapahtuu katkoja muista kuin niin sanotuista force-majore – syistä, niin palveluntoimittaja on yleensä korvausvastuussa asiakkaalleen. Tämä siitäkin syystä, vaikka syy olisi palveluntoimittajasta riippumaton. Asiakkaan ja välittäjän välisissä sopimuksissa ehdot saattavat vaihdella runsaasti, koska välittäjän rooli ei aina ole niin yksiselitteinen. Sopimuskumppanien väliset velvollisuudet vaihtelevat sen mukaan, onko välittäjä konsultti, kauppapaikka vai eri palveluiden yhdistelijä. Välittäjän ja palveluntoimittajan välinen sopimus on eniten muistuttamassa jälleenmyynti- tai jakelusopimusta. Tärkein tämän sopimuksen kohde on oikeus palvelun käyttöoikeuden välittämiseen. Kuitenkin on tärkeää myös määritellä millä teknisin laitteistovaatimuksin palvelun välitys pystytään toteuttamaan. Välittäjän ja palveluntoimittajan välisissä sopimuksissa tärkeään rooliin nousee myös heidän keskinäinen työnjakonsa esimerkiksi asiakkaalle esiin tulevien ongelmatilanteiden selvittämisessä. Mikäli tätä asiaa ei ole sovittu sopimusteknisesti, saattaa se myöhemmässä vaiheessa aiheuttaa tulkintavaikeuksia, koska periaatteessa se voisi kuulua kummalle tahansa. [181]

5.4.2 Oikeudet aineistoon

Pilvipalveluissa on tyypillistä, että sen käytön yhteydessä merkittävä osa asiakkaan tietokannoista ja muusta materiaalista on pilvipalvelun toimittajan hallussa. Tietokannat on tallennettu palvelun tuottajan konesaliin, jolloin ne ovat suurelta osin asiakkaan kontrollipiirin ulottumattomissa. Todellisuudessa, hyvin usein asiakas ei ole edes tietoinen missä päin sijaitsee palveluntuottajan konesali, johon tiedot on tallennettu. Pilvipalvelusopimusta luotaessa onkin tärkeää, että tilanteissa kuten esimerkiksi

[181] Kulmala 2003: 103 – 109.

sopimuksen päättyessä on tarkkaan määritelty kuinka konesalissa sijaitsevan tietoaineiston kanssa menetellään. Sopimusta luotaessa asiakkaan aineistoksi on hyvä määritellä kaikki asiakkaan lukuun pilvipalvelun toimittajalle luovutettu tai käyttöön asetettu tieto ja aineisto. Pilvipalvelusopimuksessa tämä on voitu määritellä esimerkiksi seuraavalla tavalla.

> *”Asiakkaan aineisto tarkoittaa asiakkaan ohjelmistopalveluun siirtämää tai muuten asiakkaan lukuun ohjelmistopalvelua varten toimittajalle luovutettua tai käyttöön asetettua tietoa tai aineistoa tai muuten sopijapuolten asiakkaan aineistoksi määrittelemää tietoa tai aineistoa”.* [182]

On tärkeää, että asiakkaan aineiston käsittely kirjataan sopimukseen, jottei oikeudet aineistoon siirry vahingossa toimittajalle vakioehtojen myötä. Julkishallinnon on myös oleellista huolehtia siitä, että sen aineistoa käsitellään vaan asiakkaan määrittelemään käyttötarkoitukseen. [183]

Sopimuksessa on myös aiheellista selvyyden vuoksi tarpeellista määritellä, mitä tarkoitetaan pilvipalveluntoimittajan aineistolla. Tällä on tarkoitus erotella asiakkaan ja pilvipalveluntoimittajan aineisto toisistaan, koska niihin kohdistuu erilaisia oikeuksia ja velvollisuuksia. Sopimuksessa pilvipalveluntoimittajan aineisto voidaan määritellä seuraavasti ehdossa ETP 2.3,

> *”toimittajan aineisto tarkoittaa toimittajan ohjelmistopalvelun käyttöä varten asiakkaalle luovuttamaa tai käyttöön asettamaa aineistoa sekä muuta sopijapuolten toimittajan aineistoksi määrittelemää tietoa tai aineistoa”.* [184]

Pilvipalvelussa voi muodostua myös yhdistettyä aineistoa kun asiakkaan aineistoa esitetään ohjelmistopalvelulla tuotettuna siten, että asiakkaan ja pilvipalveluntoimittajan aineistot yhdistyvät tuotoksessa. JIT 2015 erityisehdoissa tietoverkon välityksellä toimitettavista palveluista tämä on määritelty seuraavasti.

> *Tilaajalla ja tilaajan lukuun toimivalla kolmannella osapuolella on oikeus käyttää ja muokata toimittajan aineistoa ja yhdistettyä aineistoa sopimuksen voimassaoloajan tilaajan toimintaa varten. Tilaajalla ja*

[182] Erlund, Lindfors, Salminen & Turunen 2016: 375.

[183] Järvenoja ym. 2015: 253.

[184] Erlund, Lindfors, Salminen & Turunen 2016: 377 – 378.

> *tilaajan lukuun toimivalla kolmannella osapuolella sekä taholla, jolle tilaajan tehtävät mahdollisesti siirtyvät, on kuitenkin myös sopimuksen päättymisen jälkeen rajoittamaton oikeus käyttää ja muokata ohjelmistopalvelusta saatua yhdistettyä aineistoa mukaan lukien tilaajalle mahdollisesti luovutetut varmuuskopiot näistä aineistoista.* [185]

Aineistoa voi olla määritelmän mukaan kolmenlaista; 1. Toimittajan asiakkaalle nimenomaisesti luovuttamaa aineistoa, 2. toimittajan asiakkaan käyttöön asettamaa aineistoa sekä 3. Muuta sopijapuolten toimittajan aineistoksi määrittelemää tietoa tai aineistoa. [186]

Sopimuksessa voidaan sopimuskohdassa ETP 10.3 *"asiakkaan aineiston omistusoikeus ja immateriaalioikeudet kuuluvat asiakkaalle tai kolmannelle osapuolelle"* sopia, että toimittajalle ei synny oikeuksia asiakkaan aineistoon nähden pelkästään sen perusteella, että asiakas tallettaa tietoja pilvipalvelussa sijaitsevaan tietokantaan. Terveydenhuolto-alan ohjelmistosovelluksissa, joihin talletetaan henkilö- sekä potilastietoja täyttää aina luottamuksellisen aineiston määritelmän. Ohjelmistossa saattaa kuitenkin olla osia, jotka eivät täytä luottamuksellisuuden määritelmää. Tällöin siitä voidaan muotoilla oma sopimuslausekohta. Luottamuksellista tietoa saadaankin käyttää aina ainoastaan sopimuksen mukaiseen tarkoitukseen. Tämä voidaan pilvipalvelusopimuksessa muotoilla sopimukseen esimerkiksi lauseella ehdosta ETP 10.4

> *"toimittajalla on oikeus käyttää asiakkaan aineistoa vain sopimuksen mukaiseen tarkoitukseen".* [187]

5.4.3 Vastuu palvelun toimivuudesta

Pilvipalveluntoimittajan vastuulle kuuluu muun muassa palvelun toimivuudesta vastaaminen. Tämä tarkoittaa myös sitä, että välillä ohjelmiston toimivuuden takaamiseksi täytyy tehdä ohjelmistopäivityksiä, huoltoja ja korjauksia. Nämä toimenpiteet ovat välttämättömiä ohjelmiston ja pilvipalvelun toimivuuden kannalta. Tietoturvan kannalta on välttämätöntä, että pilvipalveluohjelmisto sekä koko palvelu on ajan tasalla virustorjunta ja muiden välttämättömien päivitysten osalta. Tämän vuoksi

[185] Järvenoja ym. 2015: 254.

[186] Erlund, Lindfors, Salminen & Turunen 2016: 375 – 378.

[187] Erlund, Lindfors, Salminen & Turunen 2016: 404 – 405.

säännölliset huolto- ja korjaustoimenpiteet sekä niiden mahdollistaminen myös sopimusteknisesti on välttämätöntä. Sopimuksessa on hyvä varautua niin sanottuun ohjelmistopalvelun huoltoikkunaan. Siinä ehtokohdassa pilvipalvelun toimittajalla on oikeus sopimukseen määritellysti keskeyttää pilvipalvelun tuottaminen ennalta sovituksi ajaksi. Terveydenhuoltoalan ohjelmistosovellusten kannalta niiden toimivuus on paikoin äärimmäisen tärkeää. Mikäli ohjelmisto on pois käytöstä väärään aikaan hyvin pitkiä aikoja se saattaa olla vaarantamassa pahimmillaan jopa potilasturvallisuuden. Sopimustekstiin voidaan huoltoikkuna määritellä seuraavasti ehdon ETP 11.1 mukaisesti,

> *”ellei ohjelmistopalvelun asennus-, muutos- tai huoltotoimenpiteistä ole keskeyttää ohjelmistopalvelun tuottaminen kohtuulliseksi ajaksi arkipäivisin kello 18.00 – 8.00, lauantaina, sunnuntaina tai yleisenä vapaapäivänä, jos se on tarpeen ohjelmistopalvelun asennus-, muutos- tai huoltotoimenpiteiden vuoksi eikä asennusta, muutosta tai huoltoa voida kohtuullisin kustannuksin toteuttaa ilman ohjelmistopalvelun tuottamisen keskeyttämistä. Jos toimittaja keskeyttää ohjelmistopalvelun tässä kohdassa mainitusta syystä, toimittajan on ilmoitettava ohjelmistopalvelun keskeyttämisestä ja keskeytyksen kestosta asiakkaalle hyvissä ajoin etukäteen, pyrittävä siihen, että keskeytyksestä aiheutuvat haitat jäävät mahdollisimman vähäisiksi sekä asiakkaan kirjallisesta vaatimuksesta hyvitettävä keskeytyksestä asiakkaalle aiheutunut palvelutason alitus sopimuksen mukaisesti”.* [188]

Myös julkisten sektorin palveluihin käytettävän JIT 2015 pilvipalvelusopimuksen perusteella käsitellään mahdollisia palvelun tuottamisessa aiheutuvia keskeytyksiä samalla tavalla. [189]Pilvipalvelun ohjelmiston keskeyttäminen saattaa tapahtua joskus myös pilvipalvelun toimittajasta johtumattomasta syystä. Tällöin sopimukseen voidaan määritellä tällaisessa tilanteessa, onko asiakkaalla oikeus palvelutason alituksesta johtuvaan hyvitykseen vai ei. Sopimusehtona, voidaan käyttää esimerkiksi tämän tyyppistä ETP 11.2 sopimuslauseketta,

> *”toimittajalla on oikeus keskeyttää ohjelmistopalvelun tuottaminen yleisen viestintäverkon asennus-, muutos- tai huoltotoimenpiteiden taikka ohjelmistopalveluun kohdistuvan vakavan tietoturvauhan vuoksi tai jos laki tai viranomaismääräys tätä edellyttää tai ylimääräisen esteen vuoksi. Jos toimittaja keskeyttää ohjelmistopalvelun tuottamisen tässä kohdassa mainitusta syystä, toimittaja ilmoittaa keskeytyksestä ja keskeytyksen*

[188] Erlund, Lindfors, Salminen & Turunen 2016: 409 – 412.

[189] Järvenoja ym. 2015: 404.

> *kestosta asiakkaalle hyvissä ajoin etukäteen tai, ellei tämä ole kohtuudella mahdollista, viipymättä sen jälkeen, kun toimittaja on saanut kyseisen tiedon kyseisestä seikasta".* [190]

Myös JIT 2015 erityisehdoissa on käsitelty ohjelmistopalvelun toiminnasta aiheutuvaa haittaa.

> "*Tilaajan on ilman aiheetonta viivästystä ohjelmistopalvelun käytön aloittamisen jälkeen tarkastettava ohjelmistopalvelun toimivuus ja reklamoitava toimimattomuudesta tai muusta toimituksessa havaitusta virheestä ja puutteesta. Jos tilaaja ei ole ilmoittanut virheistä seitsemän arkipäivän kuluessa ohjelmistopalvelun toimittamisen aloittamisesta, katsotaan ohjelmistopalvelu hyväksytyksi. Ohjelmistopalvelu katsotaan myös hyväksytyksi heti, kun se on sopijapuolten yhteisessä käyttöönottotestissä todettu toimivaksi. Sellaiset puutteellisuudet tai viat, jotka eivät olennaisesti haittaa ohjelmistopalvelun käyttämistä, eivät ole esteenä toimituksen hyväksymiselle, mutta toimittaja on velvollinen ilman aiheetonta viivytystä korjaamaan ne." [191]*

Varastoitaessa henkilö- ja potilastietoja suuriin tietokantoihin on sen toimivuuden varmistamiseksi tarkoin suunniteltava myös tietoaineiston varmuuskopiointi. Yleisten sopimusehtojen (YSE-ehdot) kumikin sopimusosapuoli vastaa omien tietojensa varmuuskopioinnista. Kuitenkin, kun kyseessä on pilvipalvelusopimus, on asiakkaalla ohjelmistopalvelun luonteesta johtuen lähes mahdotonta huolehtia itse aineiston varmuuskopioinnista. Näin ollen varmuuskopiointi vastuu onkin erillisten ehtojen mukaan määrätty ehdossa ETP 12.1 pilvipalveluntoimittajalle,

> *"ellei kirjallisesti ole toisin sovittu, toimittaja vastaa ohjelmistopalvelussa olevan asiakkaan aineiston varmuuskopioinnista, varmuuskopioiden toimivuuden tarkastamisesta ja siitä, että asiakkaan aineisto on palautettavissa varmuuskopioista. Toimittaja vastaa ohjelmistopalvelussa olevan asiakkaan aineiston varmuuskopioinnista siitä hetkestä lukien, kun asiakas ottaa ohjelmistopalvelun käyttöönsä." [192]*

Sopimuksellisesti on tärkeää myös määritellä varmuuskopioinnista vastaavan osapuolen lisäksi minimitaso varmuuskopioinnille. Ehtokohdassa voidaan määritellä kuinka usein

---

[190] Erlund, Lindfors, Salminen & Turunen 2016: 413 – 414.

[191] Järvenoja ym. 2015: 401.

[192] Erlund, Lindfors, Salminen & Turunen 2016: 416 – 417.

varmuuskopiointi toteutetaan, sekä kuinka varmuuskopiot tullaan säilyttämään. Ehtolauseke ETP 12.2 voidaan muotoilla esimerkiksi seuraavasti,

> *”jos toimittaja vastaa varmuuskopioinnista eikä muuta ole sovittu, toimittajan velvollisuutena on ottaa varmuuskopiot vähintään kerran työpäivän aikana tai toimittajan asiakkaalle etukäteen ilmoittamin aikavälein ja säilyttää varmuuskopioita tarkoitukseen soveltuvalla tavalla toimittajan asiakkaalle etukäteen ilmoittaman käytännön mukaisesti. Muilta osin asiakkaan aineiston varmuuskopioinnista vastaa asiakas. Tähän kohtaan perustuvat velvollisuudet voidaan täyttää myös muulla samaan lopputulokseen johtavalla teknisellä toimenpiteellä kuin varmuuskopioinnilla”.*

Varmuuskopioiden säilyttämisen osalta on yleisintä noudattaa alan yleisesti hyväksyttyjä standardeja. [193]

Edellisten ehtokohtien toimittajan varmuuskopiointivelvoite koskee vikatilanteita. Kuitenkin myös asiakas saattaa virheellisellä toiminnallaan aiheuttaa vahinkoa aineistolle esimerkiksi muuttamalla tai poistamalla sitä. Ehtokohdat eivät velvoita pilvipalvelun toimittajaa ylläpitämään historiapalvelua, josta voitaisiin palauttaa väärästä toiminnasta vahingoittuneet tiedot. Mikäli pilvipalvelun toimittajalla on kuitenkin varmuuskopioituna ja säilytettynä kyseiset tiedot, joista ne tarvittaessa voidaan palauttaa, on toimittajalla oikeus veloittaa tietojen palauttamisesta sovittujen veloitusperusteiden mukaisesti. Ehtolauseke ETP 12.3 kyseiseen tilanteeseen voidaan muotoilla seuraavasti.

> *”Jos ohjelmistopalvelussa oleva asiakkaan aineisto on tuhoutunut, kadonnut, muuttunut tai vahingoittunut asiakkaan käytettyä asiakkaan tunnistettaan taikka asiakas on muuten omalla toiminnallaan tuhonnut, kadonnut, muuttunut tai vahingoittanut ohjelmistopalvelussa olevaa asiakkaan aineistoa, tällaisten aineiston palauttamisesta toimittajalla on oikeus veloittaa sovittujen veloitusperusteiden mukaisesti”.* [194]

5.4.4 Asiakkaan ja toimittajan yleiset velvollisuudet

Pilvipalvelusopimuksessa, asiakkaan yleisiä velvollisuuksia on, muun muassa on olla huolellinen toimissaan. Sopimusehdossa ETP .1 on mainittu, että *”asiakas vastaa siitä,*

[193] Erlund, Lindfors, Salminen & Turunen 2016: 417 – 419.

[194] Erlund, Lindfors, Salminen & Turunen 2016: 419.

että asiakkaan vastuulla olevat tehtävät tehdään sopimuksen mukaisesti ja huolellisesti”. Asiakkaan kohdalla kuitenkin riittää, että hän toimii yleisellä huolellisuudella. Pilvipalvelun toimittajan kohdalla taas huolellisuuteen liitetään ammattitaito ja sen asettamat vaatimukset. Ehdossa ETP 4.2 vastuusta käyttöympäristöstä mainitaan, että

> *”asiakas vastaa ohjelmistopalvelun käyttämiseen tarvitsemiensa laitteiden, yhteyksien ja ohjelmistojen hankkimisesta ja toimintakunnosta. Asiakas vastaa ohjelmistopalvelun käyttämiseen liittyvistä tietoliikenne- ja muista vastaavista kustannuksistaan. Asiakas vastaa asiakkaan laitteiden, yhteyksien, ohjelmistojen ja tietojärjestelmien saattamisesta toimittajan toimittamien käyttöympäristövaatimusten mukaisiksi”.*

JIT 2015 pilvipalvelusopimuksessa on asiakkaan velvollisuuksiksi määritelty,

> *”1. Tilaaja vastaa siitä, että tilaajan vastuulla olevat tehtävät tehdään sopimuksen mukaisesti ja huolellisesti. 2. Tilaaja vastaa ohjelmistopalvelun soveltuvuudesta tilaajan käyttötarkoitukseen. 3. Tilaaja vastaa ohjelmistopalvelun käyttämiseen tarvitsemiensa laitteiden, tietoliikenneyhteyksien ja ohjelmistojen hankinnasta, toimintakunnosta ja suojauksista, mikäli ne eivät sopimuksen mukaan kuulu toimittajan vastuulle. Tilaaja vastaa käyttöympäristönsä saattamisesta palvelukuvauksessa esitettyjen määrittelyjen mukaiseksi.*
> *4. Tilaajan tulee opastaa palveluksessaan olevat tai lukuunsa toimivat ohjelmistopalvelun käyttäjät noudattamaan toimittajan antamia ohjeita käyttäessään ohjelmistopalvelua. Opastuksessa on kiinnitettävä erityistä huomiota ohjelmistopalvelun käytön tietoturvallisuuteen liittyviin kysymyksiin. 5. Ohjelmistopalveluihin liittyviä toimittajan yhteydenottoja varten tilaajan on ilmoitettava toimittajalle kirjallisesti yhteyshenkilönsä, tarpeelliset yhteystietonsa sekä näiden muutokset. “* [195]

Pilvipalvelun tuottamisessa palveluntoimittaja vastaa normaalisti palvelun toimittamisesta tietoverkon välityksellä. Asiakkaan vastuulle jää käyttöympäristön luominen sellaiseksi, että se pystyy tehokkaasti ja turvallisesti ottamaan pilvipalvelusta tulevan ohjelmistopalvelun vastaan sekä käsittelemään sieltä tulevaa ja tallennettavaa tietoa. Asiakkaan vastuulla on myös se, että hänellä on käytössään palvelun vaatima tietoliikenneyhteys ohjelmistopalvelun vastaanottoa varten. Mikäli siirrettävä tieto on sen laatuista, että se vaatii salatun tietoliikenneyhteyden ohjelmistopalveluun, on siitä ja sen kustannuksista sovittava erikseen. [196]

---

[195] Järvenoja ym. 2015: 399.

[196] Erlund, Lindfors, Salminen & Turunen 2016: 385 – 387.

Asiakkaan velvollisuutena on myös antaa riittävät tiedot pilvipalvelun toimittajalle toimitusta varten. Tämän ehtokohdan tarkoituksena on korostaa, että IT-projektissa on kysymys yhteistyöstä. Jotta, pilvipalvelun toimittaja pystyy suunnittelemaan parhaimman mahdollisen palvelun asiakkaalle, tulee hänellä olla riittävät vaadittavat tiedot esimerkiksi asiakkaan käyttöympäristöstä. Tämän vuoksi myös sopimusehtoihin on laitettu kohta asiakkaan velvollisuudesta antaa riittävät tiedot toimitusta varten. Ehtolauseke ETP 4.3 kuuluu, että

> *”asiakkaan on annettava toimittajalle riittävät ja oikeat tiedot toimitusta varten ja muutoinkin kohtuullisesti myötävaikutettava ohjelmistopalvelun toimittamiseen. Asiakas vastaa toimittajalle antamistaan tiesoista ja ohjeista sekä niiden päivittämisestä”.*

Ehdon viimeinen lause huomioi tilanteen, jossa asiakas jättää kertomatta esimerkiksi käyttöympäristössään tapahtuvista muutoksista. Kaikissa tilanteissa vastuu säilyy kuitenkin asiakkaalla. [197]

Pilvipalvelun toimittajan vastuulla on ennen kaikkea se, että pilvipalvelu on sovitun mukainen. Ehtolauseke ETP 3.1 kuuluu, että

> *”toimittaja vastaa siitä, että ohjelmistopalvelu vastaa sopimuksessa sovittua”.*

Tämä korostaa sitä, että sopijapuolten on tarkasti kuvailtava sopimuksessa palvelu, sen toiminta ja palvelutasot. Mikäli nämä jäävät suppeiksi tai epämääräisiksi, on se aiheuttamassa ristiriitatilanteissa tulkintaongelmia. Myös pilvipalvelun toimittajan tulee toimia huolellisesti, mutta myös lisäksi ammattitaitoisesti. Tietoturvaan liittyvissä seikoissa, huolellisuus on erityisen tärkeää. [198]Lauseke ehdossa ETP 3.2 kuuluu, että

> *”toimittaja vastaa siitä, että toimittajan vastuulla olevat tehtävät tehdään sopimuksen mukaisesti, huolellisesti sekä tehtävien edellyttämällä ammattitaidolla”.*

[197] Erlund, Lindfors, Salminen & Turunen 2016: 386 – 387.

[198] Järvenoja ym. 2015: 135 – 140.

On useimmiten äärimmäisen hankalaa osoittaa toimineensa huolellisuusvaatimusten mukaisesti. Tämän vuoksi onkin selkeämpää, että tämän lisäksi sopimukseen kirjataan selkeästi ja yksiselitteisesti sopimusvastuut sekä velvoitteet. [199]

Tietoturvan ja riskienhallinnan kannalta on tärkeää, että henkilökunta osaa käyttää laitteita sekä ohjelmistoa. Tämän vuoksi se, että käyttöohjeet sekä käyttöympäristövaatimukset ovat ajan tasalla, on oleellista riskienhallintaa. Tämäkin ehtolause on sisällytetty sopimukseen. Ehdon ETP 3.3 sisältö kuuluu,

> *”toimittaja vastaa siitä, että ohjelmistopalvelun käyttöohjeet sekä käyttöympäristövaatimukset ovat asiakkaan saatavilla. Toimittajan tulee antaa asiakkaalle ohjelmistopalvelun käyttöönottoon liittyvää muuta tukea ainoastaan, mikäli siitä on sovittu erikseen”.*

Vaadittavat käyttöohjeet voivat olla saatavissa internet-ympäristössä, joten niitä ei tarvitse välttämättä toimittaa paperisena asiakkaalle. Käyttöympäristövaatimukset toimittajan tulee myös saattaa asiakkaan tietoon. Kuitenkaan toimittajan vastuulla ei ole se, että käyttöympäristö on saatettu vaatimusten mukaiseksi. Mikäli käyttöönottoon tarvitaan tukea, se voidaan kirjata palvelutasosopimukseen, johon mahdollisimman yksiselitteisesti määritetään tukipalvelun toteutus ja saatavuus. [200]

Julkisten hankintojen kohdalla käytettävästä JIT 2015 vakiosopimusehdoissa on toimittajan vastuiksi määritelty seuraavat.

> *”1. Toimittaja vastaa siitä, että ohjelmistopalvelu vastaa sopimusta ja palvelukuvausta. 2. Toimittaja vastaa siitä, että toimittajan vastuulla olevat tehtävät tehdään sopimuksen mukaisesti, huolellisesti sekä tehtävien edellyttämällä ammattitaidolla. 3. Toimittaja toimittaa tilaajalle kirjallisesti ohjelmistopalvelun käyttöohjeet ja käyttöympäristövaatimukset.4. Ohjelmistopalveluihin liittyviä tilaajan yhteydenottoja varten toimittajan on ilmoitettava tilaajalle kirjallisesti yhteyshenkilönsä, muut yhteystietonsa sekä näiden muutokset.“* [201]

[199] Erlund, Lindfors, Salminen & Turunen 2016: 380 – 382.

[200] Erlund, Lindfors, Salminen & Turunen 2016: 383 – 384.

[201] Järvenoja ym. 2015: 399.

5.4.5 Ohjelmistopalvelun sisältö ja palvelukuvaus

Asiakkaalla on aina vastuu ohjelmistopalvelun soveltuvuudesta omaan tarkoitukseensa. Asiakkaan onkin aina tarkoin perehdyttävä ohjelmistopalvelun palvelukuvaukseen sekä palvelutasoihin. Asiakkaalla ei useimmiten ole tietämystä ja osaamista arvioida täysin pilvipalveluiden kaikkia ulottuvuuksia, sen vuoksi asiakkaan täytyykin olla sopimusneuvotteluiden aikana aktiivinen ja selvittää sekä kysellä pilvipalvelun toimittajalta, epäselväksi jääneitä kohtia. ETP 5.1 kohdassa ohjelmistopalvelun soveltumisesta käyttötarkoitukseen sanotaan, että

> *”asiakas vastaa siitä, että sopimuksen mukainen ohjelmistopalvelu soveltuu asiakkaan käyttötarkoitukseen ja että se täyttää asiakkaan palvelua koskevat vaatimukset. Ellei ohjelmistopalvelun sisältöä tai palvelutasoa ole määritelty sopimuksessa, noudatetaan toimittajan kulloinkin voimassa olevia ehtoja”.*

Mikäli näin on, että sopimuksessa ei ole määritelty ohjelmistopalvelun sisältöä ja palvelutasoa se jättää toimittajalle hyvin laajat valtuudet muuttaa halutessaan toimitettua ohjelmistopalvelun sisältöä sekä palvelutasoja. Tämä taas ei ole asiakkaan kannalta kaikkein optimaalisin tilanne, jos sisältö saattaa muuttua kesken sopimuskauden. [202]

Ohjelmistosovelluksen toimittajalla on pääsääntöisesti luotu omat palvelutasokuvauksensa tai –liitteensä. Näihin asiakkaan tulee hyvin tarkasti perehtyä sopimusneuvotteluiden yhteydessä. IT2015 –sopimusehto-kokoelmaan sisältyy myös malli palvelutasokuvauksesta, jota tarvittaessa toimittaja ja asiakas voivat käyttää muistilistana asioista, jotka minimissään tulisi sopimusta luotaessa sopia. Palvelutasokuvauksessa määritellään asiakkaalle muun muassa yleinen käytettävyysprosentti sekä pisimmän yhtäjaksoisen käyttökatkoksen hyväksyttävä pituus. Nämä seikat ovat tietoturvan ohella merkittäviä seikkoja ajateltaessa terveydenhuoltoalan ohjelmistosovelluksen käyttöä. Mikäli palvelu ei ole käyttäjän saatavilla suhteellisen varmasti se on aiheuttamassa jopa merkittävän riskin potilasturvallisuudelle. Ohjelmiston tuleekin olla käytettävyydellä mitattuna lähes 100 prosenttinen, jotta ongelmia ei potilasturvallisuuteen aiheudu. Ohjelmistopalvelun palvelutasokuvauksessa yleisimmin käytettävyyden mittaamispisteenä on yhteyspiste ja tällöin mittaajana on toimittaja. Terveydenhuoltoalan ohjelmistosovellusten kohdalla saattaa olla tarpeen mitata ohjelmistopalvelun käytettävyyttä omaan toimipisteeseensä

[202] Erlund, Lindfors, Salminen & Turunen 2016: 388.

saakka. Tällöin mittauksen useimmiten suorittaa riippumaton kolmas osapuoli ja tästä täytyy pilvipalvelusopimuksessa sopia erikseen. [203] Myös JIT 2015 vakiosopimusehtojen mukaan, sopijaosapuolet sopivat kirjallisesti palvelukuvauksen, joka sisältää mahdolliset seuraamukset mahdollisista palvelun käytön estävistä poikkeamista.[204]

ETP 5.2 toimittajan velvollisuus tiedottaa käytön estävistä seikoista sisältä lauseen

> *”Toimittajan on viipymättä ilmoitettava asiakkaalle tietoonsa tulleesta seikasta, joka saattaa estää ohjelmistopalvelun sopimuksenmukaisen käytön”.*

Sopimuskohta on merkittävä myös tietoturvallisuuden kannalta, koska mikäli ohjelmistopalvelun sopimuksenmukainen käyttö ei onnistu, saattaa vaarana olla myös tietoturvariski. Ohjelmistopalvelun toimittajalla on useimmiten ohjelmistopalvelun tuotantoympäristöön, jolloin myös kykenee näistä asiakasta paremmin informoimaan. Tällaisia mahdollisia ilmoitettavia seikkoja saattaa olla esimerkiksi laitteistopäivitysten ajankohdat sekä yleisen tietoliikenneverkon mahdolliset huolto- ja asennustyöt. Kohdassa ETP 5.3 sovitaan koulutuksesta ja käyttöönotosta. Siinä ehtolauseke kuuluu

> *”Ohjelmistopalvelu sisältää asiakkaan henkilöstön koulutukseen liittyviä tehtäviä vain siltä osin kuin niistä on kirjallisesti sovittu”.*

Monimutkaisten ohjelmistotoimitusten kohdalla toimittaja saattaa velvoittaa asiakaan pääkäyttäjää osallistumaan toimittajan järjestämään käyttökoulutukseen. Näin voidaan helpottaa palvelun käyttöönottoa, sekä myös vähentämään tietämättömyydestä ja osaamattomuudesta aiheutuvia riskejä. [205]

5.4.6 Yksityisyydensuoja ja tietoturvaloukkaukset

IT2015 yleisten sopimusehtojen kohdat 8.1 ja 8.2 määrittelevät tietoturvaa. Pilvipalvelusopimuksissa on kuitenkin tärkeää ottaa tietoturvaa koskevat seikat myös

[203] Erlund, Lindfors, Salminen & Turunen 2016: 389 – 390.

[204] Järvenoja ym. 2015: 400.

[205] Erlund, Lindfors, Salminen & Turunen 2016: 390 – 391.

erityisehdoissa, koska ne korostuvat merkitykseltään pilvipalveluympäristössä toimiessa. Erityisehdossa ETP 13.1 on tehty yleissääntö tietoverkon toiminnasta. Sen mukaan;

> *”kumpikin osapuoli vastaa oman tietojärjestelmänsä ja viestintäverkkonsa tietoturvasta. Kumpikaan osapuoli ei vastaa yleisen tietoverkon tietoturvasta tai siellä mahdollisesti ilmenevistä häiriöistä tai muista omien vaikutusmahdollisuuksiensa ulkopuolella olevista ohjelmistopalvelun käyttöä haittaavista tekijöistä tai niistä aiheutuvista vahingoista”.*

Tämä ehto tulee yleisimmin käyttöön silloin, kun tietoverkon käyttö estää pilvipalvelun käytön joko kokonaan tai osittain. Palvelun toimittaja vapautuu vastuusta osoittaessaan, että palvelupuute johtuu tietoverkon häiriöstä. Mikäli kuitenkin syynä on palveluntoimittajan oman konesalin palvelimen ongelmista, niin hän on kuitenkin vastuussa palvelunalentumisesta. [206]

Tietoturvaloukkauksissa molemmilla sopimuksen osapuolilla on oikeus reagoida tilanteeseen. Kuitenkin silloin, kun vasta epäillään mahdollista tietoturvaloukkausta, eivät sopimusosapuolet voi ryhtyä konkreettisiin toimenpiteisiin. [207] Ehtolausekkeen 13.2 mukaan

> *”sopijapuolella on oikeus ryhtyä tarvittaviin toimiin tietoturvaloukkausten torjumiseksi ja tietoturvaan kohdistuvien häiriöiden poistamiseksi. Tällaisia toimia ovat esimerkiksi viestien välittämisen ja vastaanottamisen estäminen tai tietoturvaa vaarantavien haittaohjelmien poistaminen viestistä. Sopijapuolen tulee mitoittaa toimenpiteet torjuttavan häiriön vakavuuden mukaan ja lopettaa ne heti, kun niiden toteuttamiselle ei ole perustetta”.* [208]

Myös julkisen sektorin JIT 2015 vakiosopimusehdot ovat samansuuntaiset käsiteltäessä tietoturvaloukkauksia tai niiden riskejä. Kaikki osapuolet ovat velvollisia toimillaan estämään mahdolliset tietoturvaan liittyvät riskit sekä myös toimillaan ehkäisemään

[206] Erlund, Lindfors, Salminen & Turunen 2016: 420 – 421.

[207] Järvenoja ym. 2015: 406.

[208] Erlund, Lindfors, Salminen & Turunen 2016: 421.

mahdolliset vahingot mahdollisimman pieniksi. [209] Yksi tärkeimmistä tietoturvaan liittyvistä erikoisehdoista on ehto ETP 13.3 henkilötietojen käsittelystä. Sen mukaan

> *”toimittajalla on oikeus käsitellä henkilötietoja vain sopimuksen ja asiakkaan antamien kirjallisten ohjeiden mukaisesti. Toimittaja noudattaa henkilötietoja käsitellessään lainsäädännön edellyttämää hyvää henkilötietojen käsittelytapaa ja tietojen suojaamista koskevia säännöksiä. Toimittaja toteuttaa tekniset ja organisatoriset toimet, joista on sovittu. Asiakas on henkilötietolain tarkoittama rekisterinpitäjä”.*

Ehto tuo selvästi esiin, mitkä ovat pilvipalvelun toimittajan oikeudet käsitellä tietoja. Yleisissä sopimusehdoissa on myös kohdassa 8.3 käsitelty henkilötietojen käsittelyyn koskevaa asiaa. Sen mukaisesti asiakas ja pilvipalvelun toimittaja voivat kirjallisesti sopia erikseen, mikäli asiakas luovuttaa henkilötietoja toimittajalle. Asiakkaalla on myös vastuu siitä onko sillä oikeutta tietojen luovuttamiseen. Toimittajalla ei ole kuitenkaan oikeutta siirtää henkilötietoja Euroopan talousalueen ulkopuolelle, eikä sallia pääsyä tietoihin Euroopan talousalueen ulkopuolelta. Pilvipalveluasiakas on henkilötietolain 32§:n mukainen rekisterinpitäjä. Ja hänen velvollisuutenaan on toteuttaa tarpeelliset tekniset sekä organisatoriset toimenpiteen henkilötietojen suojaamiseksi. [210] JIT 2015 vakiosopimusehtojen erityisehdoissa on maininta, että

> *”Sopijapuolet sopivat kirjallisesti, että siirtääkö tilaaja henkilötietoja toimittajalle. Tilaaja on pilvipalveluasiakkaana vastuussa näistä henkilötiedoista. Tilaaja vastaa siitä, että sillä on oikeus siirtää kyseiset tiedot toimittajalle sopimuksen mukaiseen käsittelyyn. Toimittaja noudattaa lainsäädännön edellyttämää hyvää henkilötietojen käsittelytapaa ja annettuja kirjallisia ohjeita. ”*[211]

Mikäli sopimusosapuolista toinen havaitsee mahdollisen tietoturvariskin tai -loukkauksen on hänellä velvollisuus ryhtyä toimiin ja ilmoittaa asiasta toiselle sopimusosapuolelle. Erityisehdon 14.1 mukaan

> *”sopijapuolella on velvollisuus ilmoittaa toiselle sopijapuolelle ilman aiheetonta viivytystä havaitsemistaan ohjelmistopalvelua tai sen käyttöä vaarantavista merkittävistä tietoturvariskeistä, tietoturvaloukkauksista tai niiden epäilyistä”.*

[209] Järvenoja ym. 2015: 405 – 406.

[210] Erlund, Lindfors, Salminen & Turunen 2016: 422 – 423.

[211] Järvenoja ym. 2015: 406.

Ehdossa ETP 14.2, jonka perusteella sovitaan sopijapuolten toimintavelvollisuudesta, sanotaan että

> *”sopijapuolten tulee osaltaan ryhtyä välittömästi toimenpiteisiin tietoturvaloukkauksen vaikutuksen poistamiseksi tai pienentämiseksi”.*

Sen perusteella se osapuolista, jolla on mahdollisuus poistaa tai pienentää tietoturvariskiä on velvollisuus toimia välittömästi. Usein tietoturvauhka tulee yleisestä tietoverkosta, jolloin toimintavelvollisuus on molemmilla sopijaosapuolilla. [212]

Mikäli tietoturvaloukkaus havaitaan toisen sopijaosapuolen vastuualueella, on myös toinen sopijaosapuoli velvollinen myötävaikuttamaan tietoturvaloukkauksen tutkintaan ja toimenpiteisiin. Ehdossa ETP 14.3 on mainittu, että

> *”sopijapuolella on velvollisuus myötävaikuttaa tietoturvaloukkausten tutkintaan”.*

Käytännössä tämä tarkoittaa esimerkiksi sitä, että asiakas epäilee pilvipalveluntoimittajan palvelimen levittävän virusta. Tällöin palveluntoimittaja on velvollinen tutkimaan väitteet, sekä ryhtymään mahdollisiin toimenpiteisiin. [213]

Pilvipalveluympäristössä on oleellista, että palvelua käyttävät pystytään jollakin perusteella tunnistamaan. Nämä vaadittavat tunnisteet voi luoda joko palveluntoimittaja tai asiakas itse. Yhä useammin tunnisteet luo asiakas itse. Tärkeää on kuitenkin se, että sopimukseen on kirjattuna, kuka tunnisteet luo. Sopimusehto voidaan kirjoittaa esimerkiksi ETP 9.1:n mukaisesti näin, että

> *”ellei kirjallisesti ole toisin sovittu, toimittaja luovuttaa sopimuksen mukaisesti asiakkaalle ohjelmistopalvelun käyttämiseksi tarvittavat tunnisteet”.*

JIT 2015 vakiosopimusehdoissa mainitaan, että toimittaja luovuttaa tunnukset asiakkaalle. Tilaaja vastaa tunnuksista ja niiden oikeasta käytöstä. [214] Luoduista käyttäjätunnuksista ja salasanoista vastaa aina asiakas. ETP 9.2 ehto kuuluu, että

---

[212] Erlund, Lindfors, Salminen & Turunen 2016: 424 – 425.

[213] Erlund, Lindfors, Salminen & Turunen 2016: 426.

[214] Järvenoja ym. 2015: 402.

> *”asiakas vastaa siitä, että sen käyttäjät säilyttävät tunnisteet huolellisesti ja eivätkä paljasta niitä kolmansille osapuolille. Asiakas on vastuussa tunnisteillaan tapahtuneesta ohjelmistopalvelun käytöstä”.* [215]

Mikäli asiakas luovuttaa tunnisteet jonkun kolmannen osapuolen haltuun ja tämä niitä väärinkäyttää on vastuu ensisijaisesti aina asiakkaalla. Mikäli tunnisteet joutuvat jonkun kolmannen osapuolen haltuun ilman asiakkaan suostumusta, on asiakas velvollinen siitä välittömästi ilmoittamaan. Mikäli tunnisteet luo ohjelmistotoimittaja, ilmoitus tulee tehdä sinne, mutta mikäli tunnisteet luo asiakkaan valtuuttama henkilö asiakkaan organisaatiossa on ilmoitus tehtävä hänelle, jolloin tunnisteet voidaan välittömästi sulkea. Ehtokohta on sopimukseen kirjoitettu ETP 9.3 mukaisesti olettaen, että tunnisteet luo ohjelmistotoimittaja. Ehto kuuluu, että

> *”asiakas sitoutuu viipymättä ilmoittamaan toimittajalle tunnisteen joutumisesta kolmannen osapuolen tietoon tai epäilemästään tunnisteen väärinkäytöstä. Asiakkaan vastuu tunnisteillaan tapahtuneesta ohjelmistopalvelun käytöstä lakkaa, kun toimittaja on vastaanottanut asiakkaan ilmoituksen tai toimittaja on muulla tavoin havainnut väärinkäytön”.*

Ohjelmistotoimittaja saattaa myös vaatia asiakasta vaihtamaan tunnisteen, epäilläkseen tai havaitessaan mahdollisen tietomurron tai muun väärinkäytöksen. Sopimusehtona se on kirjattu ETP 9.4 tietoturvauhka ja salasanan vaihtaminen. Ehto on kirjoitettu muotoon,

> *”asiakas on toimittajan kirjallisesta pyynnöstä velvollinen vaihtamaan ohjelmistopalvelun käyttämiseksi vaadittavan tunnisteen, jos se on tarpeen esimerkiksi ohjelmistopalveluun kohdistuvan vakavan tietoturvauhan vuoksi.”.*

Tästä tunnisteen vaihdosta saattaa aiheutua merkittäviä kustannuksia asiakkaalle, koska tunniste saattaa olla esimerkiksi SIM-kortti, älykortti tai muu vastaava fyysinen tunnistautumiskeino. Tällöin onkin sopimuksessa tarpeellista määrittää, kenen maksettavaksi tällaisessa tapauksessa tunnisteiden vaihto menee. [216]

---

[215] Erlund, lindfors, Salminen & Turunen 2016: 400 – 401.

[216] Erlund, Lindfors, Salminen & Turunen 2016: 400 – 404.

5.4.7 Sopimuksen irtisanominen

Pilvipalvelusopimus voi olla voimassa määräajan tai toistaiseksi voimassa oleva. ETP 15.1 kohdan mukaan

> *”määräajaksi sovittu ohjelmistopalvelua koskeva sopimus päättyy ilman irtisanomista määräajan kuluttua umpeen”.*

Sopimus ei siis vaadi irtisanomista vaan päättyy automaattisesti määräajan umpeuduttua. ETP 15.2 kohdassa irtisanomisajasta mainitaan, että

> *”ellei kirjallisesti ole toisin sovittu, toistaiseksi voimassa oleva sopimus voidaan kirjallisesti irtisanoa päättymään asiakaan puolelta 3 kuukauden ja toimittajan puolelta 6 kuukauden kuluttua irtisanomisesta. Irtisanomisaika lasketaan sen kalenterikuukauden viimeisestä päivästä, jonka aikana sopimus on irtisanottu”.*

Sopimusosapuolet voivat tietenkin sopia myös jonkinlaisista muista irtisanomisaikojen pituuksista. [217] [218]

Sopimuksen päättyessä tärkeä sovittava seikka on asiakkaalle arvokkaiden tietoaineistojen siirto asiakkaan ilmoittamaan paikkaan. Tietoturvan kannalta sekä tietenkin myös asiakkaan jatkotoiminnan kannalta on erityisen tärkeää, että aineisto saadaan siirrettyä turvallisesti sekä ongelmitta pois ohjelmistopalvelun toimittajan hallusta. ETP 16.1 kohdassa yleisestä myötävaikutusvelvollisuudesta mainitaan, että

> *”sopimuksen päättyessä toimittajalla on velvollisuus kohtuudella myötävaikuttaa toimittajan hallussa olevan asiakkaan aineiston siirtoon asiakkaan osoittamalle taholle. Ellei kirjallisesti ole toisin sovittu, myötävaikutusvelvollisuus päättyy, kun 3 kuukautta on kulunut sopimuksen päättymisestä. Toimittajan myötävaikutusvelvollisuuteen liittyvissä palveluissa noudatetaan sovittuja veloitusperusteita”.*

Ohjelmistopalveluntoimittajalla ei ole tämän perusteella velvollisuutta avustaa ohjelmistopalvelun siirrossa, vaan velvollisuus rajoittuu ainoastaan aineiston siirtoon. Terveydenhuoltoalan ohjelmistosovellusten kohdalla siirrettävä tietoaineisto saattaa olla

[217] Erlund, Lindfors, Salminen & Turunen 2016: 426 – 427.

[218] Järvenoja ym. 2015: 407.

huomattava, jolloin kolmen kuukauden myötävaikutusaika saattaa olla jopa lyhyt kaikelle vaadittavalle tekemiselle. Tällöin sopimuksen neuvotteluvaiheessa kannattaa sopia tämä sopimuskohta ajallisesti pidemmäksi tai muuten varmistaa aineiston turvallinen siirto kokonaisuudessaan. [219]

[219] Erlund, Lindfors, Salminen Turunen 2016: 428.

6. JOHTOPÄÄTÖKSET

Nykyinen lainsäädäntö on vaikeasti pilvipalveluihin sovellettavissa. Ongelmia aiheuttaa etenkin tietosuojaan, palvelun tietoturvaan sekä sopimusoikeudellisiin vastuisiin liittyvät kysymykset. Nämä seikat ovat hidastamassa pilvipalveluiden kasvua, koska etenkin yrityksiä sekä julkishallintoa askarruttaa, ovatko tiedot varmassa tallessa pilviympäristössä sekä kenen vastuulla on huolehtia turvallisesta pilviympäristöstä sekä palvelun katkeamattomasta käyttömahdollisuudesta. Euroopan komissio on tiedonannossaan "Pilvipalvelujen potentiaali käyttöön Euroopassa" pyrkinyt edistämään pilvipalveluiden nopeampaa käyttöön ottoa kaikilla sellaisilla aloilla, joilla tieto- ja viestintätekniikkakuluja voidaan leikata ja joilla pilvipalveluiden avulla voidaan tukea tuottavuutta, kasvua sekä työpaikkojen lisääntymistä. Komission esittämistä toimenpiteistä useat liittyvät käyttäjien käsitykseen siitä, että pilvipalveluiden käyttöön liittyy lisäriskejä. Ehdotetuilla toimenpiteillä pyritään puuttumaan tähän ongelmaan selventämällä sovellettavan oikeudellisen kehyksen tulkintoja, lisäämällä tietoa käyttäjien keskuudessa sekä kehittämällä oikeudellista kehystä edelleen. Puuttumalla pilvipalveluissa esiin tulleisiin erityishaasteisiin, se nopeuttaisi ja yhdenmukaistaisi teknologian käyttöönottoa yrityksissä, organisaatioissa sekä julkishallinnossa.

Komission esitöissä nousi esiin kolme keskeistä osa-aluetta, jotka kaipaavat toimenpiteiden muodossa jatkossa selvennystä. Näitä ovat digitaalisten sisämarkkinoiden hajanaisuus, sopimusongelmat sekä standardiviidakko. Digitaalisten sisämarkkinoiden hajanaisuus johtuu hyvin erilaisista kansallisista oikeudellisista puitteista sekä epätietoisuudesta sovellettavasta lainsäädännöstä. Pilvipalveluiden käyttäjiä huolestuttaa digitaalisen sisällön ja datan mahdollisuus sijaita lähes missä päin maailmaa tahansa. Tällöin keskeiseksi ongelmaksi muodostuu hankaluus hallinnoida palveluja ja käyttötapoja jotka ulottuvat mahdollisesti useille lainkäyttöalueille sekä useille lainosa-alueille kuten tietosuoja, sopimusoikeus ja kuluttajansuoja sekä rikosoikeus. Sopimusongelmat liittyvät käyttäjien huoleen datan saatavuudesta, siirrettävyydestä sekä datan omistajuudesta. Huolta aiheuttaa esimerkiksi epäselvyys siitä miten vastuu jakaantuu ongelmatilanteissa. Huolenaiheena on myös epäselvä "standardiviidakko", jossa erilaiset käytettävät standardit luovat epävarmuutta dataformaattien yhteentoimivuudesta. Epäselvää on myös mitä takeita on sille, että kaikissa standardeissa henkilötiedot asianmukaisesti suojataan ja pystytään estämään tietojen luvaton käyttö sekä suojautumaan mahdollisilta verkkohyökkäyksiltä. [220]

[220] Komission tiedonanto pilvipalveluiden potentiaalisesta käytöstä Euroopassa, KOM 2012, 529 lopullinen.

Euroopan Unionissa on laadittu uusi tietosuoja-asetus. Ehdotus hyväksyttiin lähes yksimielisesti Euroopan Parlamentissa Maaliskuussa 2014. Uusi EU:n tietosuoja-asetus tuli voimaan 24.5.2016. Suomessa asetus tulee voimaan kahden vuoden siirtymäajan jälkeen 25.5.2018. Aiemmin jokainen jäsenmaa toteutti henkilötietodirektiivin vaatimuksia omalla tavallaan kansallisessa lainsäädännössään. Uuden tietosuoja-asetuksen yhtenä tavoitteena on yhtenäistää tietosuojaa koskevaa lainsäädäntöä siten, että sitä tulkittaisiin jäsenmaissa samalla tavalla. Uusi tietosuoja-asetus myös ajantasaistaa tietosuojaa koskevaa sääntelyä, jotta lainsäädännöllä voidaan vastata teknologian kehitykseen sekä globalisaatioon liittyviin henkilötietojen suojaa koskeviin haasteisiin. Tietosuoja – asetus pyrkii lisäämään henkilötietojen käsittelyssä avoimuutta sekä tukemaan ihmisten oikeuksia valvoa henkilötietojensa käsittelyä. Uusi tietosuoja-asetus tulee selkeyttämään vastuita ja velvollisuuksia pilvipalveluympäristössä toimiessa. [221]

Suomessa Oikeusministeriö asetti työryhmän, jonka tavoitteena oli nykyaikaistaa henkilötietolaki liittyen EU:n tietosuoja-asetuksen jättämiin säännöksiä täsmentävään ja täydentävään liikkumavaraan. Nykyinen henkilötietolaki on ollut työryhmän työskentelyn pohjana, niiltä osin kuin se on ollut mahdollista sekä tarkoituksenmukaista. Tietosuoja-asetusta täydentävä kansallisen lainsäädännön valmistelu on vielä useissa EU:n jäsenvaltioissa kesken. Tämä saattaa vaikuttaa myöhemmässä vaiheessa siihen, että työryhmän ehdotusta joudutaan vielä arvioimaan yhdenmukaisuuden näkökulmasta.

Käytettäessä terveydenhuollon sovellusta pilvipalveluympäristöstä tulee huolehtia tietoturvaseikoista erityisen tarkkaan. Henkilö- ja potilastietoja säilytettäessä sekä siirrettäessä verkossa tulee varmistua, että tarvittavat suojaukset sekä tietoturvariskien ennaltaehkäisy on suoritettu hyvän tiedonhallintatavan mukaan sekä erityistä huolellisuutta noudattaen. Lainsäädännöllisesti eri osapuolten tulisi olla selvillä kenen vastuulla on tietojen turvallisesta käsittelystä vastaaminen, sekä myös pyrkiä estämään ja ilmoittamaan, mikäli tietoturvaan liittyviä ongelmia ilmenee vaikka se ei juuri kyseisen osapuolen vastuulle kuuluisikaan. Pilvipalvelusopimusten vakiosopimusmalleissa on otettu huomioon tämä seikka. Sekä IT-2015 että JIT 2015 erityisehdoissaan mainitsevat, että osapuolten on vaikutettava myönteisesti siihen, että pystytään tietoturvaa mahdollisesti uhkaavat tilanteet välttämään tai vahingot pitämään mahdollisimman pieninä. Vastuu henkilötietojen käsittelyn laillisuudesta on aina EU:n yleisen tietosuoja-asetuksen mukaan pilvipalveluasiakkaalla tai henkilötietojen

[221] Oikeusministeriö, mietintöjä ja lausuntoja 35 / 2017

käsittelijällä. Tietosuoja-asetuksen mukaan rikkomuksesta voidaan määrätä hallinnollinen sakko. Edelleenkin on oleellista myös rikoslakiin säätää eräistä henkilötietojen käsittelyyn liittyvistä rikoksen tunnusmerkistöistä. Näillä täydennettäisiin tietosuoja-asetuksen mukaisia hallinnollisia seuraamuksia.

Suurimmat pilvipalveluntoimittajat käyttävät pilvipalvelusopimuksissa yleisesti vakiosopimuksia, jolloin pienemmällä asiakkaalla saattaa olla vaikeuksia neuvotella joustavampia sopimusehtoja. Palvelutasosopimus SLA määrittää palveluntoimittajan asiakkaalle takaaman minimi palvelutason. Turvatakseen mahdollisimman hyvää tietoturvaa pilvipalvelusopimuksessa kannattaa pyrkiä vaikuttamaan sopimusehdoin oman tieto-omaisuuden säilytyspaikkaan. Terveydenhuollon potilas- ja asiakastietojen ollessa kyseessä, jo voimassaoleva lainsäädäntökin on asettamassa rajoituksia tiedon säilytyspaikan sijainnille. Suomalaisten henkilötietojen ollessa kyseessä tietojen säilytys tulisi tapahtua EU- maassa.

Pilvipalvelut tulevat nopeasti lisääntymään ja vaikuttamaan sekä yksittäisten ihmisten että yritysten tietotekniikan käyttöön. Verkkorikollisuus etsii myös uusia keinoja iskeä yksityisille ja yrityksille tärkeään tietoon, joka saattaa olla joissain tilanteissa jopa rahallisesti mitattuna arvokasta. Nykyinen lainsäädäntö kulkee vielä jäljessä nopeasti kehittyvän tekniikan muuttaessa tiedon käsittelyä ja säilyttämistä. Tämän vuoksi pilvipalveluja hankkivan ja käyttävän tulisi perehtyä teknisten seikkojen ohella myös tietosuoja sekä lainsäädännöllisiin seikkoihin. Lainsäädännön kehittyessä tilanteeseen tulee toivottavasti muutos.

Yrityksille ja eri organisaatioille pilvipalvelut luovat kuitenkin huikean mahdollisuuden tehostaa toimintaansa sekä jopa vähentää IT-sektorin kuluja. Yrityksille se, että kaikki tarvittava tieto on saatavilla lähes missä tahansa, luo mahdollisuuden kehittää liiketoimintaa entisestään. Pilvipalvelut ovat kehittyneet ja kehittyvät jatkossa entisestään. Tiedon tallennuspaikkana pilvi, on jo nykyisellään lähes varmempi ja turvallisempi säilytyspaikka kuin yrityksen tai organisaation omat tietokoneet. Palvelinsalissa huolehditaan tekniikan toimivuudesta sekä turvallisuustekijöistä keskimääräistä paremmin. Monella pienellä yrityksellä ei ole resursseja eikä osaamista huolehtia yritykselle tai organisaatiolle arvokkaan tietoaineksen turvallisesta säilyttämisestä. Juridisesti pilvipalveluympäristö on kuitenkin edelleen hieman pirstaleinen ja siten sopimusoikeudellisesti hieman hankala. Yritykselle tai organisaatiolle onnistuakseen riskienhallinnassa on kuitenkin ensiarvoisen tärkeää ymmärtää pilvipalveluympäristön toiminta sekä hahmottaa, siinä eri osapuolten vastuut ja velvollisuudet.

Pilvipalvelusopimus sekä lainsäädäntö suojaavat jo varsin hyvin henkilö- sekä terveystietoja. Tärkeää näiden tietojen kohdalla on olla tietoinen tietojen säilytyspaikasta. Lainsäädäntö on jo itsessään rajaamassa tätä, mutta asia on hyvä vielä sopia erityisin sopimuskohdin lopullista sopimusta solmittaessa. Lainsäädäntö kehittyy pilvipalveluiden kohdalla ja se parantaa yksittäisten ihmisten sekä yritysten ja organisaatioiden luottamusta pilvipalveluita kohtaan. Tietoturva on kuitenkin laaja asia, ja se, että pystytään takaamaan tietojen turvallinen säilytys ja käsittely koostuu se monesta eri asiasta. Jotta yritys tai organisaatio pystyy takaamaan mahdollisimman turvallisen tietojen käsittelyn, vaatii se kaikilta osapuolilta huolellista sekä suunnitelmallista toimintaa, jossa on otettu huomioon yrityksen tai organisaation mahdolliset tietoturvariskit. Yksinomaan lainsäädäntö tai sen pohjalta luotu pilvipalvelusopimus ei riitä takaamaan luotettavaa henkilö- ja terveystietojen säilytystä ja käsittelyä pilvipalveluympäristössä. Kuitenkin, sopimuksellisella tietoturvariskien hallinnalla pystytään selkeyttämään toimintaympäristöä, jonka myötä osapuolille on selvempää kenen vastuulla mikäkin asia on.

LÄHDELUETTELO

Kirjalliset lähteet:

Hakala, Mika & Vainio, Mika & Vuorinen, Olli (2006). *Tietoturvallisuuden käsikirja*. Jyväskylä: Dodenco Finland Oy. 422 s. ISBN 951-846-273-9.

Heino, Petteri (2010). *Pilvipalvelut – cloud computing*. Hämeenlinna: Talentum Media Oy ja Petteri Heino. 267 s. ISBN 978-952-14-1524-1.

Järvinen, Petteri (2002). *Tietoturva & yksityisyys*. Jyväskylä: Docendo Finland Oy. 456 s. ISBN 951-846-152-X

Kleemola, Maija & Tervo-Pellikka, Raija (1998). *Tietosuoja, vaatimukset verkottuvassa tietojärjestelmässä*. Espoo: Suomen ATK-Kustannus Oy. 203 s. ISBN 951-762-637-1.

Korhonen, Rauno (2003). *Perusrekisterit ja tietosuoja.* Helsinki: Edita Publishing Oy. 344 s. ISBN 951-37-3879-5.

Krutz, Ronald L & Vines, Russell Dean (2010) *Cloud security, A comprehensive guide to secure Cloud Computing*. United States of America: Wiley Publishing Inc. 358 s. ISBN 978-0-470-58987-8.

Mäenpää, Olli (2009). *Julkisuusperiaate*. Helsinki: WSOY Pro Oy ja Olli mäenpää. 402 s. ISBN 978-951-0-34293-0.

Paavilainen, Juhani (1998). *Tietoturva*. Jyväskylä: Suomen ATK-kustannus Oy. 228 s. ISBN 951-762-647-9.

Pahlman, Irma (2010). *Asiakastietojen käsittely, salassapito ja asiakkaan tiedonsaantioikeus sosiaali- ja terveydenhuollossa*. Helsinki: Edita Publishing Oy. 193 s. ISBN 978-951-37-5376-4.

Salo, Immo (2010). *Cloud computing, palvelut verkossa*. Porvoo: Bookwell Oy. 168 s. ISBN 978-951-0-36584-7.

Salo, Immo (2013). Big data, tiedon vallankumous. Jyväskylä: Docenco Oy. 147 s. ISBN 978-952-5912-71-5.

Thomas, Tom (2005) *Verkkojen tietoturva*. Helsinki: Edita Publishing Oy. 446 s. ISBN 951-826-780-4.

Vanto J, Jarno (2011). *Henkilötietolaki käytännössä*. Helsinki: WSOYpro Oy. 269 s. ISBN 978-951-0-36933-3.

Velte T, Anthony & Velte J, Toby & Elsenpeter, Robert (2010) *Cloud computing, A Practical Approach*. United States of America: The McGraw-Hill Companies. 334 s. ISBN 978-0-07-162694-1.

Voutilainen, Tomi (2007). *Hyvä sähköinen hallinto. 2. Painos*. Helsinki: Edita Publishing Oy. 325 s. ISBN 951-37-4570-8.

Ylipartanen, Arto (2001). *Tietosuoja terveydenhuollossa, potilaan asema ja oikeudet henkilötietojen käsittelyssä*. Helsinki: Tietosanoma Oy. 330 s. ISBN 951-885-190-5.

Sähköiset lähteet:

Brunette, G. & Mogull, R. (2009). *Security guidance for critical areas of focus in cloud computing V2.1*. USA: Cloud Security Alliance. Haettu 21.6.2014 osoitteesta https://cloudsecurityalliance.org/csaguide.pdf

Euroopan komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. (2012). *Pilvipalveluiden potentiaali käyttöön Euroopassa.* COM (2012) 529 final. Bryssel. Haettu 7.9.2014 osoitteesta http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:FI:PDF

Järvinen, Tomi (2012). *Pilvipalvelut lainsäädäntö ja sopimukset*. Aalto-yliopisto. Helsinki. Haettu 7.9.2014 osoitteesta https://wiki.aalto.fi/download/attachments/58941866/PILVIPALVELUT_LAINSAADANTO_POWERPOINT_31012012.pdf?version=1&modificationDate=1328079341000

Lakius Digitaalisen liiketoiminnan lakiopas. Juridinen opas verkkokaupan, pilvipalvelun tai mobiilisovellusliiketoiminnan käynnistämiseen. (2017) Haettu

12.2.2018 osoitteesta https://lakius.fi/wp-content/uploads/2017/04/Digitaalisen-liiketoiminnan-lakiopas.pdf

Luoma, Eetu & Rönkkö, Mikko (2014). *Software industry survey 2014*. Haettu 8.9.2014 osoitteesta http://www.softwareindustrysurvey.fi/SlidesFinland2014.pdf

Oikeusministeriö, tietosuojavaltuutetun toimisto (2017). *Miten valmistautua EU:n tietosuoja-asetukseen? Selvityksiä ja ohjeita 4/2017*. Helsinki: ISBN 978-952-259-558-4. Haettu 10.2.2018 osoitteesta http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Staffans Ida (2013). Muistio *Tietosuoja ja pilvipalvelut henkilötietolain näkökulmasta*. Kuntaliitto. Haettu 7.9.2014 osoitteesta http://www.kunnat.net/fi/asiantuntijapalvelut/laki/hallintojuridiikka/julkisuus_tietosuoja/tietosuoja-pilvipalvelut/Documents/Tietosuoja%20ja%20pilvipalvelut%20henkilötietolain%20näkökulmasta_Muistio.pdf

Valtionvarainministeriö (2013). *Sovelluskehityksen tietoturvaohje, VAHTI 1/2013.* Helsinki. Haettu 7.9.2014 osoitteesta http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20130207Sovell/VAHTI_1_Sovelluskehityksen_tietoturvaohje_NETTI.pdf.

Painettu artikkeli:

Välimäki, Mikko & Laine, Juha (2004) *Vastuunrajoituksista kolmannen osapuolen immateriaalioikeusväitteille ohjelmistotoimituksissa*. Defensor legis (5). s. 901 – 911.

Julkaisematon lähde:

Saarenpää, Asko (2014). Informaatio- ja tietotekniikkaoikeuden luennot Keväällä 2014. Vaasan Yliopisto. Oikeusinformatiikan oppimateriaali.

Hallituksen esitykset:

HE 125 / 2003

HE 48 / 2008

HE 53 / 2010 vp

HE 57 / 2013 vp

HE 219 / 2013