TURUN YLIOPISTO
Kauppakorkeakoulu

Yleisen tietosuoja-asetuksen noudattaminen pilvipalveluissa

Tietojärjestelmätieteen kandidaatintutkielma

Laatija:
Inkeri Nirvi

Ohjaaja:
FT Kai Kimppa

9.12.2024
Turku

Kanditutkielma

Oppiaine: Tietojärjestelmätiede
Tekijä: Inkeri Nirvi
Otsikko: Yleisen tietosuoja-asetuksen noudattaminen pilvipalveluissa
Ohjaaja: FT Kai Kimppa
Sivumäärä: 34 sivua
Päivämäärä: 9.12.2024

Tämä tutkielma analysoi Euroopan unionin yleisen tietosuoja-asetuksen (engl. General Data Protection Regulation, GDPR) vaikutuksia asiakasdatan hallintaan organisaatioissa, erityisesti asiakasdatan ulkoistamisen yhteydessä pilvipalveluihin. Yleinen tietosuoja-asetus on mullistanut henkilötietojen käsittelyä koskevat käytännöt, asettaen organisaatioille velvoitteita sekä sisäisten tietojärjestelmien kehittämisessä että ulkoisten ratkaisujen, kuten pilvipohjaisten tietovarastojen ja asiakkuudenhallintajärjestelmien hyödyntämisessä. Pilvipalvelut tarjoavat organisaatioille kustannustehokkaita ja skaalautuvia ratkaisuja, mutta niiden käyttö tuo mukanaan haasteita tietosuojan ja kyberturvallisuuden näkökulmasta, mikä puolestaan luo ongelmia yleisen tietosuoja-asetuksen noudattamiseen.

Tutkielmassa tarkastellaan erityisesti pilvipalveluiden ja yleisen tietosuoja-asetuksen vaatimusten välisiä ristiriitoja, sisältäen asiakasdatan käsittelyn haasteita ja tietoturvaongelmia. Lisäksi organisaation oman tietojärjestelmän kehittämistä vertaillaan pilvipalveluiden käyttöön tietoturvan ja resurssien hallinnan näkökulmasta. Tutkimus hyödyntää yleisen tietosuoja-asetuksen artikloja ja teknologisen riskienhallinnan viitekehyksiä, kuten NIST-standardia (engl. National Institute of Standards and Technology), arvioidakseen pilvipalveluiden tietoturvakäytäntöjen tehokkuutta. Tutkielmassa hyödynnetyt tutkimukset osoittavat, että organisaatioiden on tasapainoteltava kustannustehokkuuden, tietosuoja-asetuksen noudattamisen ja tietoturvariskien hallinnan välillä. Oikeaa ratkaisua järjestelmävalintaan ei ole, minkä myötä organisaation on itse päätettävä omat prioriteetit, harkiten hyötyjen ja haittojen painoarvoa.

Avainsanat: GDPR, pilvipalvelu, tietovarasto, CRM, NIST

SISÄLLYS

KUVIOT

TAULUKOT

1 Johdanto

Euroopan unioni hyväksyi vuonna 2016 yleisen tietosuoja-asetuksen (engl. General Data Protection Regulation, GDPR) (EU) 2016/679, joka muutti merkittävästi organisaatioiden tapaa käsitellä henkilötietoja. Asetus kohdistui erityisesti tietojärjestelmiin, joita käytetään asiakasdatan käsittelyssä. Organisaatioiden on noudatettava uutta asetusta, jos toimintaa halutaan jatkaa Euroopan unionin jäsenmaiden markkinoilla. Yleinen tietosuoja-asetus sisältää 99 artiklaa, jotka käsittelevät yksilöiden henkilötietojen suojaa sekä organisaatioille asetettuja määräyksiä, joita noudattaa. (Yleinen tietosuoja-asetus, 2016.)

Tietosuoja-asetuksen myötä organisaatioiden sidosryhmien toimintatapoja uudistettiin vastaamaan asetuksen velvoitteita, mikä oli monille organisaatioille haastava prosessi. Asetus vaikutti myös kansainvälisiin organisaatioihin, jotka toimivat EU:n alueella. Monet organisaatiot integroivat tietosuoja-asetuksen osaksi strategiaansa, tehostaen sen avulla toimintaansa. (Farhad, 2024). Tietosuoja-asetuksen myötä kuluttajien kiinnostus tietosuojaa kohtaan kasvoi (Presthus & Sørum, 2021), ja tietosuojaa alettiin hyödyntää myös markkinointitarkoituksissa lupaamalla kuluttajille parempaa yksityisyyden suojaa (Garber, 2018).

Tietojärjestelmät kokivat suurimman muutoksen, kun henkilötietojen käsittelyn laillisuus oli integroitava osaksi järjestelmiä. Tämä muutos näkyi organisaatioiden sisällä esimerkiksi nykyisin vaadittuna lokitietojen tallentamisena sekä läpinäkyvänä henkilötietojen keräämisenä ja käsittelynä (Yleinen tietosuoja-asetus, 2016). Tietojärjestelmäarkkitehtuurin muutos ja tietosuojaprosessien lisääminen olivat monimutkaisia ja kalliita investointeja. Muutokset olivat kuitenkin välttämättömiä tietosuojan toteuttamisen kannalta, sillä näiden prosessien avulla voidaan osoittaa asianmukainen henkilötietojen käsittely, jota yleinen tietosuoja-asetus edellyttää. (Farhad, 2024.)

Teknologian kehittyessä organisaatiot kohtaavat haasteita pyrkiessään integroimaan uusia teknologisia trendejä tietojärjestelmiinsä tehokkuuden parantamiseksi. Yleinen tietosuoja-asetus asetti uusia puitteita erityisesti tietojärjestelmäkehitykselle, mikä tuo mukanaan sekä rajoitteita että velvollisuuksia. (Ayala-Rivera ym., 2024.) Haasteiden ja suurien investointivaatimusten myötä organisaatiot suosivat asiakasdataprosessien ulkoistamista pilvipalveluihin. Ulkoistaminen mahdollistaa hallinnollisen taakan vähentymisen ja kustannustehokkuuden. Ongelmana pilvipalveluissa on ristiriidat yleiseen tietosuoja-asetukseen, kun pilvipalveluissa voi yhä havaita tietoturvaongelmia. Vastuun määrittely asiakasdatan hallinnassa voi olla epäselvä, kun datan käsittely jaetaan pilvipalveluiden ja sitä hyödyntävän organisaation kesken.

Tässä tutkielmassa selvitetään, miten Euroopan unionin asettama yleinen tietosuoja-asetus vaikuttaa organisaatioiden ulkoistamaan asiakasdataan pilvipalveluissa, erityisesti keskittyen pilvipohjaisiin tietovarastoihin ja asiakkuudenhallintajärjestelmiin. Lisäksi tutkielmassa tarkastellaan NIST-viitekehystä tietojärjestelmien teknologiseen riskienhallintaan, mikä tukee yleistä tietosuoja-asetusta. Tutkielman tutkimuskysymyksinä ovat:

1. Mitkä ovat yleisen tietosuoja-asetuksen vaikutukset asiakasdatan käsittelyyn organisaatioissa?
2. Mitkä ovat yleisen tietosuoja-asetuksen vaikutukset pilvipalveluiden hyödyntämisessä?

Tutkielmassa keskitytään yleisen tietosuoja-asetuksen noudattamiseen organisaatioiden sisällä ja asiakasdataa käsittelevissä pilvipalveluissa. Tietosuoja-asetuksen noudattaminen pilvipalveluissa, kuten tiedon varastoinnissa ja asiakkuudenhallintajärjestelmissä, voi olla laillisesti haastavaa. Pilvipalvelut kohtaavat jatkuvasti kyberhyökkäyksiä, mikä vaarantaa asiakasorganisaation asiakasdatan. Kyberturvallisuuden kannalta monet pilvipalvelutarjoajat hyödyntävät teknisiä viitekehyksiä, kuten NIST-viitekehystä, suojaamaan järjestelmiä riskeiltä. Asiakasdatan prosessoinnissa pilvipalveluissa on yhä epäkohtia ja yleisen tietosuoja-asetuksen tuomat edellytykset eivät aina täyty. Tutkielma keskittyy organisaatioiden ja pilvipalveluiden tietoturvahaasteisiin yleisen tietosuoja-asetuksen näkökulmasta.

2 Yleinen tietosuoja-asetus organisaation asiakasdatan hallinnassa

Huhtikuussa 2016 Euroopan unioni antoi yleisen tietosuoja-asetuksen (EU) 2016/679, jonka tarkoituksena on suojella ja turvata EU:n kansalaisten oikeuksia ja vapauksia henkilötietojen käsittelyssä asettamalla velvoitteita organisaatioille ja yrityksille (Yleinen tietosuoja-asetus, 2016). Asetus antaa yksilöille oikeuksia hallita omia henkilötietojaan sekä yhtenäistää EU:n jäsenmaiden tietosuojakäytäntöjä. Asetus tuli voimaan toukokuussa 2018 ja muutti merkittävästi organisaatioiden käytäntöjä, erityisesti henkilötietoja käsittelevien tietojärjestelmien osalta.

Ennen yleistä tietosuoja-asetusta oli voimassa vuoden 1995 tietosuojadirektiivi (EU-direktiivi 95/46/EY, 1995). Tietosuojadirektiivi oli ensimmäinen askel kohti vuoden 2016 yleistä tietosuoja-asetusta ja se muodosti nykyisen henkilötietosuojan perustan. Direktiivin tavoitteena oli asettaa säännöt henkilötietojen keräämiselle ja käsittelylle sekä velvoittaa jäsenvaltiot perustamaan valvontaviranomaisen direktiivin toteuttamista varten. Tietosuojadirektiivin mukaan kaiken henkilötietojen keräämisen ja käsittelyn tuli olla oikeudenmukaista, laillista ja täsmällistä. Esimerkiksi jo tämän direktiivin aikana henkilöistä ei saanut kerätä erityisiä henkilötietoryhmiä, kuten uskonnollisia näkemyksiä tai terveystietoja, elleivät ne olleet välttämättömiä keräämis- ja käsittelytarkoituksiin – sama periaate näkyy myös nykyisessä tietosuoja-asetuksessa. Lisäksi henkilötietojen siirto EU:n ulkopuolelle sallittiin ainoastaan, jos kyseisen maan tietosuojataso oli riittävä. (EU-Direktiivi 95/46/EY, 1995.)

2000-luvulla teknologinen kehitys nopeutui huomattavasti, ja Euroopan unionin tietosuojaneuvostossa havaittiin, että vuoden 1995 tietosuojadirektiivin säännöt eivät enää vastanneet teknologian kehityksen tuomiin haasteisiin. Tammikuussa 2012 Euroopan komissio ehdotti tietosuojasääntöjen uudistamista, jotta henkilötietojen suojaa voitaisiin vahvistaa. Kaksi kuukautta komission ehdotuksen jälkeen Euroopan tietosuojavaltuutettu antoi lausunnon uudistusehdotuksesta, ja sen pohjalta aloitettiin valmistelut Euroopan tietosuojatyöryhmässä saman vuoden aikana. Maaliskuussa 2014 Euroopan parlamentti hyväksyi lopulta uuden yleisen tietosuoja-asetuksen (EU) 2016/679. (Euroopan tietosuojavaltuutettu, 2018.)

Yleinen tietosuoja-asetus tuli voimaan 25. toukokuuta 2018, kumoten sitä edeltävän tietosuojadirektiivin 95/46/EY. Uusi asetus asetti tiukat velvoitteet organisaatioille ja yrityksille, jotka käsittelevät Euroopan unionin jäsenvaltioiden kansalaisten henkilötietoja tietojärjestelmissään. (Yleinen tietosuoja-asetus, 2016.) Yleisen tietosuoja-asetuksen myötä erityisesti kansainvälisten

yritysten, jotka käsittelevät henkilötietoja, oli varmistettava, että niiden tietojärjestelmät noudattavat asetusta, mikäli ne halusivat säilyttää toiminnan EU-markkinoilla.

Tietosuojalainsäädännön konkreettisena tavoitteena on parantaa henkilötietojen suojaa ja vahvistaa yksilöiden tietosuojaoikeuksia. Sen tulee myös vastata digitalisaation ja globalisaation tuomiin uusiin tietosuojakysymyksiin. Henkilötiedoilla tarkoitetaan kaikkia tietoja, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, kuten nimi, ikä ja kotikaupunki. Yksilön näkökulmasta uusia oikeuksia ovat esimerkiksi oikeus pyytää omia henkilötietoja organisaatioilta, saada tietoa henkilötietojen käsittelyn tarkoituksesta ja pyytää omien tietojen poistamista organisaation tietojärjestelmistä. (Tietosuojavaltuutetun toimisto, 2024.) Organisaatioiden velvollisuutena on vastata näihin yksilöiden uusiin oikeuksiin, mikä vaati sisäisiä muutoksia niin teknologisessa kehityksessä kuin myös hallinnollisella tasolla (Ayala-Rivera ym., 2024).

Asetuksen seurauksena organisaatioiden toimintaedellytykset toteutetaan erilaisissa toimintamalleissa ja prosesseissa. Yleisimmät keinot ovat vaatimustenmukaisuuden hallinta, jota hoitavat organisaatioiden nimeämät tietosuojayksiköt tai -toimijat. Tietosuojavastaavien tehtävänä on valvoa, että tietosuoja-asetusta noudatetaan kaikissa prosesseissa, joissa käsitellään henkilötietoja. Tämä vaatii järjestelmällistä tiedonhallintaa ja kattavaa dokumentointia, jotta asetuksen noudattamista voidaan seurata ja tarvittaessa puuttua mahdollisiin puutteisiin. Tietosuojavastaavat suorittavat myös tietosuoja-arviointeja ja riskienhallintaa erityisesti henkilötietoja käsitteleville tietojärjestelmille, jotka voivat aiheuttaa riskejä asiakkaille tai muille sidosryhmille. (Tietosuojavaltuutetun toimisto, 2024.) Monet organisaatiot ovat integroineet tietosuojavastaavat osaksi liiketoimintaprosessejaan, ja yleinen tietosuoja-asetus on tullut osaksi organisaation periaatteita (Garber, 2018).

Yleisen tietosuoja-asetuksen tavoitteena on yhtenäistää Euroopan unionin jäsenmaiden tietosuojakäytäntöjä, mikä vähentää hallinnollista taakkaa. Organisaatioiden tietosuojasäännöt uudistettiin kerralla ja EU:n sisällä toimivien organisaatioiden tietosuojakäytännöt yhtenäistyivät. Yhtenäistämisen myötä henkilötietojen jakaminen organisaatioiden välillä helpottui, kun pystyttiin luottamaan toiselle organisaatiolle luovutetun henkilötiedon laillinen käsittely tietosuoja-asetuksen mukaisesti. Tämä helpottaa tilanteita, joissa asiakkaiden tietojen jakaminen on olennaista. Henkilötietojen vapaa liikkuvuus mahdollistaa myös organisaatioiden laajentumisen yhteismarkkinoilla. (Protection of Personal Data, EUR-Lex, 2016.) Yleinen tietosuoja-asetus tuo kuitenkin rajoitteita kansainvälisille organisaatioille, jotka haluavat toimia EU:n jäsenmaissa.

Asetuksen mukaan Euroopan unionin ulkopuolisten organisaatioiden on mukautettava käytäntönsä asetuksen vaatimuksiin, mikä on johtanut tietosuoja-asetuksen kansainväliseen implementointiin. Tietosuojakäytännöistä on tullut globaali ilmiö. Esimerkiksi Yhdysvalloissa Kalifornian osavaltiossa otettiin käyttöön yleisen tietosuoja-asetuksen inspiroima Kalifornian kuluttajayksityisyysasetus (engl. California Consumer Privacy Act), josta on tullut uusi normi yhdysvaltalaisissa organisaatioissa. (Farhad, 2024.)

Yleisen tietosuoja-asetuksen organisaatiovelvoitteiden myötä merkittävimmät muutokset kohdistuivat tietojärjestelmiin. Suurin osa henkilötiedoista käsitellään organisaatioissa automaattisesti tietojärjestelmien kautta, kuten asiakastietoihin sisältyvät nimi, ikä ja kotiosoite. Näiden henkilötietojen säilyttämisen, hyödyntämisen ja keräämisen prosesseja oli uudistettava vastaamaan tietosuoja-asetuksen vaatimuksia. (Farhad, 2024.) Asetuksen mukaan henkilötietojen käsittelyn tulee olla lainmukaista, läpinäkyvää ja tarkoituksenmukaista. Tietoja saa kerätä vain tiettyä ja nimenomaista käyttötarkoitusta varten, ainoastaan siinä määrin kuin on tarpeellista kyseiseen tarkoitukseen. Organisaatioiden on myös kyettävä korjaamaan tai poistamaan asiakkaiden tietoja heidän sitä pyytäessään. (Tietosuojavaltuutetun toimisto, 2024.) Tietojärjestelmien näkökulmasta tämä edellyttää teknologisia muutoksia tietojärjestelmien toiminnassa ja arkkitehtuurissa, jotta ne noudattaisivat tietosuoja-asetuksen vaatimuksia. Järjestelmävastaavien on hallittava kerättävien tietojen rajaamista ja käyttöä. Rajaamisen ja käytön lisäksi on järjestelmiin lisättävä lokitustoiminto, joka mahdollistaa henkilötietojen lainmukaisen käsittelyn seurannan. (Labadie & Legner, 2023.) Nämä tietojärjestelmien muutokset aiheuttivat merkittäviä kustannuksia, mutta samalla ne lisäsivät kuluttajien luottamusta organisaatioihin (Farhad, 2024).

Tietojärjestelmämuutokset edellyttävät organisaatioilta merkittäviä resursseja, kuten riittävää henkilöstömäärää, aikaa ja rahoitusta. Organisaatioiden sisäinen tietojärjestelmäkehitys vaatii erityistä huomiota silloin, kun käsitellään henkilötietoja sisältävää asiakasdataa. Teknologiset muutokset vaikuttavat kaikkiin järjestelmiin, joissa asiakasdataa kerätään, säilytetään, hallinnoidaan tai analysoidaan. Useimmissa organisaation toiminnoissa käsitellään jollain tavoin asiakasdataa, joko suorassa hallinnassa tai osana muuta toimintaa. Yleisen tietosuoja-asetuksen velvoitteiden täyttäminen on tuonut haasteita organisaatioille, joilla ei ole riittäviä resursseja tietojärjestelmien uudistamiseen. Tietosuoja-asetuksen laaja-alaiset vaatimukset vaikuttavat koko organisaation toimintaan, mikä tekee tietojärjestelmämuutoksista erityisen haastavia. (Seo ym., 2018.)

Tietojärjestelmäkehityksen kustannukset voidaan jakaa yleisesti suunnittelu-, henkilöstö-, teknologia- ja ylläpitokustannuksiin. Näiden näkyvien kustannusten lisäksi järjestelmäkehityksessä

on usein myös piilokustannuksia, kuten henkilöstön koulutus, dokumentoinnin ylläpito sekä käyttöönoton viivästysten aiheuttamat kulut. Tietojärjestelmien kehitykset ja organisaation sisäiset järjestelmämuutokset ovat usein mittavia investointeja, mikä takia ennen järjestelmäkehityksen aloittamista organisaation tulee määrittää selkeästi projektin tavoitteet, käytettävissä olevat resurssit sekä arvioida hallinnollinen vastuu. (Love & Irani, 2003.) Tietosuoja-asetuksen edellytysten mukainen kehitys voi joissakin tapauksissa olla kustannustehokas: pienet järjestelmäpäivitykset, kuten organisaation itse tuotetun lokitustoiminnon lisääminen olemassa oleviin järjestelmiin eivät yleensä aiheuta merkittäviä kuluja. Mikäli tietosuoja-asetuksen vaatimukset edellyttävät laajamittaisia muutoksia organisaation tietojärjestelmissä, voi kustannukset kasvaa merkittävästi, mikä voi luoda haasteita erityisesti pienille ja keskisuurille organisaatioille. (Istvan ym., 2020.)

Resurssirajoitteet pakottavat organisaatiot etsimään uusia tapoja hallita asiakasdataa lainmukaisesti, mikä usein johtaa tietojenkäsittelyprosessien ja järjestelmäkehityksen ulkoistamiseen kolmansille osapuolille. Asiakasdataa käsittelevien järjestelmien ulkoistaminen voi parantaa kustannustehokkuutta ja tietoturvan tasoa, sillä ammattitaitoiset palveluntarjoajat vastaavat asiakasdatan turvallisesta säilyttämisestä, käsittelystä ja analysoinnista. Ulkoistaminen voi myös edistää tietosuoja-asetuksen mukaista noudattamista, kun ulkopuolinen palveluntarjoaja ottaa hallinnollisen vastuun asiakasdatan käsittelystä ja valvoo tietosuojan noudattamista. (Jakobi ym., 2020.)

3 Pilvipalveluiden hyödyntäminen asiakasdatan käsittelyssä

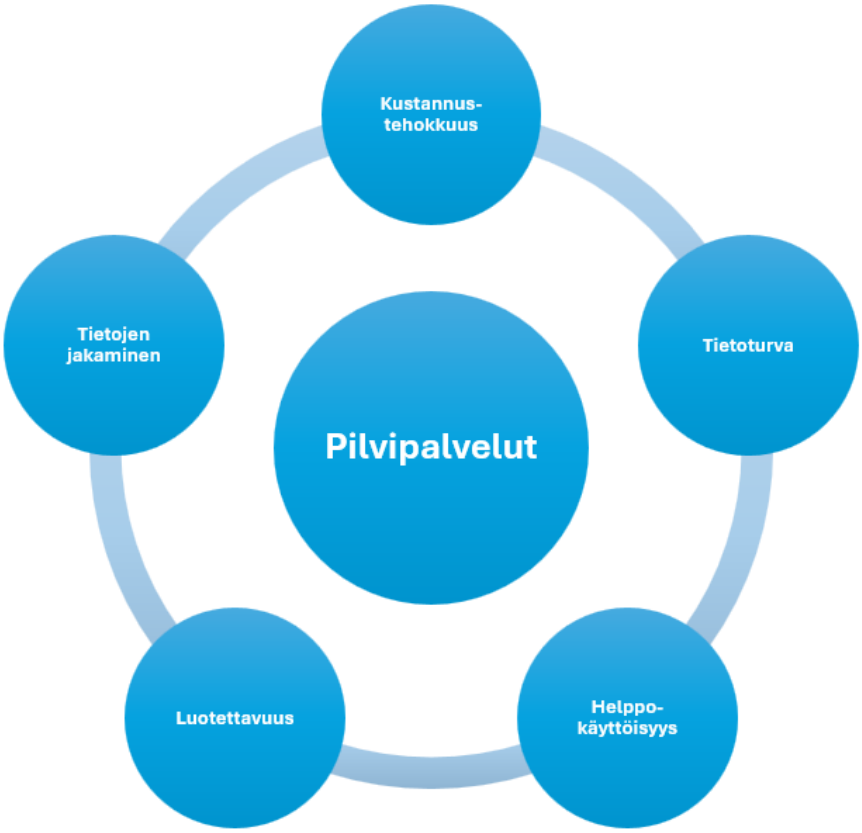
3.1 Pilvipalvelut

Monien tutkimusten (ks. esim. Caruccio ym., 2020; Garber, 2018; Jakobi ym., 2020) mukaan yleisen tietosuoja-asetuksen velvoitteiden täytäntöönpano tuo organisaation laajuisia muutoksia tietojärjestelmien hallintaan ja kehitykseen. Velvoitteiden toteuttaminen vaatii kaikkien sidosryhmien, kuten tiedonhallinnan asiantuntijoiden, tietosuoja-asiantuntijoiden ja insinöörien, yhteistyötä. Ongelmaksi on havaittu joidenkin sidosryhmien tiedon puute yleisen tietosuoja-asetuksen vaatimuksista, mikä on heijastunut negatiivisesti tietojärjestelmien lailliseen kehitykseen (Ayala-Rivera ym., 2024). Toisaalta Farhad (2024) nostaa esiin tietosuoja-asetuksen tarjoamat mahdollisuudet organisaatioille. Hänen tutkimuksensa mukaan asetus voi tuoda tietojärjestelmiin yhdenmukaisuutta ja samalla muodostaa kilpailuedun, joka vetää puoleensa kuluttajia lisääntyneen luottamuksen ansiosta.

Tietosuoja-asetuksen mukaisen kehityksen merkittävin haaste organisaatioille on asetuksen noudattamisen aiheuttamat kustannukset. Tietojärjestelmien uudelleenmuotoilu ja kehittäminen yleisen tietosuoja-asetuksen vaatimusten mukaiseksi edustaa suurta investointia, joka on erityisen haastava pienille ja keskisuurille yrityksille. Suurissa organisaatioissakin tietojärjestelmäkehitykseen liittyvät kustannukset muodostavat pitkällä aikavälillä epävarman investoinnin nopeasti kehittyvässä teknologiaympäristössä. (Fayard ym., 2012.)

2000-luvulla pilvipalveluiden suosio kasvoi merkittävästi, sillä ne tarjoavat organisaatioille kustannustehokkaan vaihtoehdon asiakasdatan prosessointiin ja tallentamiseen. Pilvipalvelut mahdollistivat suurten datamäärien ulkoistamisen kolmannelle osapuolelle samalla, kun organisaatio säilytti osittaisen hallintaoikeuden omaan dataansa. Pilvipalveluiden etuja ovat kustannustehokkuuden lisäksi myös käytön helppous, luotettavuus, tiedon jakamisen mahdollisuudet ja tietoturvaominaisuudet. Pilvipalvelut voidaan rinnastaa sähköverkkoon, jossa resurssit, kuten laitteistot, ohjelmistot ja data, yhdistetään ja jaetaan loppukäyttäjille internetin välityksellä. Tämä resurssien jakelumalli mahdollistaa niiden tehokkaan hyödyntämisen ilman, että käyttäjien tarvitsee tietää digitaalisten tietojensa tarkkaa fyysistä sijaintia. Pilvipalveluiden viitekehys perustuu korkealaatuisten, vuokrattujen IT-resurssien tarjoamiseen, mikä vähentää organisaation tarvetta rakentaa tietojärjestelmäinfrastruktuuria alusta alkaen. (Gupta ym., 2013.) Pilvipalveluiden käyttöön perustuva laskutusmalli tuottaa merkittäviä säästöjä verrattuna omien tietojärjestelmien ylläpitoon ja kehitykseen. Pilvipalveluiden kustannukset nousevat sen käytön

mukaan, esimerkiksi asiakasdatan varastointitilan kasvaessa ja tiedonsiirron mukaan. (Google Cloud Storage, 2024.) Pilvipalveluiden merkittävimmät edut organisaatioille on koottu alle kuvaan 1, jossa voidaan nähdä edellä mainittuja hyötyjä. Erityisesti kustannustehokkuus ja helppokäyttöisyys ovat suuria etuja, mutta pilvipalvelut tarjoavat myös tietoturvaa, tehokasta tietojen jakamista ja luotettavuutta asiakasorganisaatioille.



Kuva 1 Pilvipalveluiden hyödyt organisaatioille. (Perustuu Ahmadi, 2023; Gupta ym., 2013; Wang ym., 2011.)

Pilvipalvelut jaetaan yleisesti kolmeen pääpalvelutyyppiin: Software as a Service (SaaS), Platform as a Service (PaaS) ja Infrastructure as a Service (IaaS). Asiakasdatan käsittelyn ja hallinnan näkökulmasta SaaS, PaaS ja IaaS tarjoavat organisaatioille helppokäyttöiset ja skaalautuvat ratkaisut asiakasdatan käsittelyyn ja säilytykseen. Näiden pilvipalveluiden välillä on merkittäviä eroja erityisesti siinä, kuinka ne tukevat asiakasdatan hallintaa. SaaS-pilvipalvelu tarjoaa käyttövalmiita ohjelmistoja internetin välityksellä, mikä mahdollistaa asiakasdatan hallinnan ilman merkittävää teknistä osaamista. PaaS-pilvipalvelu puolestaan tarjoaa kehitysalustan ja ympäristön asiakasdatan tallentamiselle ja sovelluskehitykselle. IaaS-pilvipalvelu tarjoaa organisaatioille virtuaalisia laitteistoja palveluna, mikä antaa yrityksille laajan kontrollin asiakasdatan käsittelyyn liittyvästä infrastruktuurista. Näille pilvipalvelutyypeille yhteistä ovat joustavat hinnoittelumallit,

riittävä kapasiteetti suurten tietomäärien käsittelyyn sekä nopea käyttöönotto, mikä tekee niistä kustannustehokkaita ratkaisuja eri kokoisten organisaatioiden tarpeisiin. (Gupta ym., 2013.)

Organisaatioiden hyödyntäessä SaaS-pilvipalveluita asiakasdataa käsitellään, analysoidaan ja tallennetaan valmiiksi tuotetuissa ohjelmistoissa ja sovelluksissa, jotka ovat pilvipalveluntarjoajan ylläpitämiä. SaaS-palvelut vapauttavat käyttäjät teknisen ylläpidon vastuusta, mikä tekee niistä kustannustehokkaan ja hallinnointia helpottavan ratkaisun asiakasdatan hallintaan. (Ahmadi, 2023.) Tunnettu SaaS-palveluntarjoaja on yhdysvaltalainen Salesforce, joka tarjoaa monipuolisia asiakasdatan käsittelyratkaisuja, kuten analytiikka- ja markkinointiautomaatiopalveluita (Salesforce, 2024).

PaaS-pilvipalvelut puolestaan tarjoavat organisaatioille kehitysalustan sovellusten rakentamiseen ja datan hallintaan ilman, että fyysisiä infrastruktuuriratkaisuja tai ohjelmistojen asennusta tarvitaan. PaaS-palvelut sisältävät työkaluja data-analytiikkaan ja tietokantojen hallintaan, mikä tehostaa asiakasdatan prosessointia ja hallintaa. Toisin kuin SaaS-palveluissa, PaaS mahdollistaa käyttäjille laajemmat hallintaoikeudet datan käsittelyyn. (Ahmadi, 2023.) Microsoftin Azure-pilvipalvelu on suosittu PaaS-alusta, joka tarjoaa laajat mahdollisuudet sovelluskehitykseen ja asiakasdatan hallintaan organisaation erityistarpeisiin (Microsoft, 2024).

IaaS-pilvipalvelut tarjoavat organisaatiolle mahdollisuuden hallinnoida asiakasdataa käyttämällä virtuaalisia palvelimia, tallennustilaa ja verkkoresursseja. Tässä palvelumallissa organisaatiolla on vastuu asiakasdatan hallinnasta ja ylläpidosta pilvi-infrastruktuurissa. IaaS-palvelut mahdollistavat tietojärjestelmäinfrastruktuurin räätälöinnin organisaation tarpeisiin ilman fyysisten laitteistojen hankintaa. (Ahmadi, 2023.) Esimerkiksi Google Cloud Platform on laajasti käytetty IaaS-pilvipalvelu, joka mahdollistaa asiakasdatan tallennuksen ja analysoinnin tehokkaasti organisaation omilla ehdoilla (Google Cloud Platform, 2024).

Organisaatiot hyödyntävät usein useita pilvipalveluita eri tarkoituksiin, mutta asiakasdatan käsittelyyn valitaan useimmiten yksi keskeinen tallennus- ja analysointipalvelu tiedon eheyden varmistamiseksi. Hallinnollisesta näkökulmasta asiakasdatan keskitetty säilyttäminen yhdessä pilvipalvelussa lisää tietoturvaa, sillä pääsy- ja hallinnointioikeudet voidaan rajata ja hallita tarkoituksenmukaisesti. Toisaalta puutteellinen osaaminen pilvipalveluiden käytössä voi lisätä tietoturvariskejä, erityisesti jos asiakasdata hajautetaan useisiin eri palveluihin. Tällöin kasvaa virheellisen käsittelyn, säilytyksen ja analysoinnin riski, mikä voi heikentää asiakasdatan luotettavuutta ja turvallisuutta. (Wang ym., 2011.)

3.2 Yleisen tietosuoja-asetuksen mukainen tietoturva pilvipalveluissa

Tietoturvallisuus on keskeinen ja jatkuvasti ajankohtainen teema tietotekniikan alalla. Sen merkitys korostuu erityisesti silloin, kun organisaatiot hyödyntävät kolmansien osapuolten palveluja ja siirtävät suuria määriä dataa oman infrastruktuurinsa ulkopuolelle. Euroopan unionin yleisen tietosuoja-asetuksen voimaantulo on lisännyt yksityisyyden suojan ja tietoturvallisuuden merkitystä sekä kuluttajien että organisaatioiden näkökulmasta. (Badii ym., 2020.) Pilvipalveluiden tietoturvaa tutkitaan ja kehitetään jatkuvasti, sillä palveluntarjoajat pyrkivät tarjoamaan mahdollisimman turvallisia ratkaisuja, jotka houkuttelevat asiakkaita ja mahdollistavat luotettavat toimintaprosessit. (Farhad, 2024.)

Tietoturva on yksi merkittävimmistä tekijöistä, joita organisaatiot huomioivat valitessaan pilvipalveluita. Tämä johtuu datan siirtämisestä ulkopuolisille palveluntarjoajille, mikä sisältää potentiaalisia riskejä, kuten tietovuotoja ja virheellistä käsittelyä. Tietoturva ja tietosuojaan liittyvät kysymykset ovat olennainen osa pilviarkkitehtuurin suunnittelua niin laitteistojen kuin ohjelmistojenkin osalta. Palveluntarjoajien kyky vastata näihin haasteisiin on ratkaiseva, jotta organisaatiot voivat luottaa ulkoistettuihin ratkaisuihin ilman, että tietojen eheys tai yksityisyys vaarantuvat. (Wang ym., 2011.)

Pilvipalveluiden hyödyntämisen on osoitettu parantavan organisatorisella tasolla tietoturvaa merkittävästi erityisesti asiakasdatan hallinnan osalta. Asiakasdatan ulkoistaminen pilvipalveluihin varmistaa datan saatavuuden ja vähentää organisaation riippuvuutta omista teknisistä laitteistoistaan ja tietojärjestelmistään. Pilvipalvelut tarjoavat suojaa erityisesti riskitilanteissa, kuten kyberhyökkäysten tai luonnonkatastrofien sattuessa, kun asiakasdata ei ole riippuvainen organisaation fyysisestä laitteistosta. Myös pilvipalveluihin sisältyvä automaattinen varmuuskopiointi mahdollistaa datan palauttamisen häiriötilanteissa, mikä vähentää merkittävästi datan katoamiseen liittyviä riskejä. (Yang ym., 2020.) Näiden ominaisuuksien avulla organisaatiot voivat tehokkaammin täyttää yleisen tietosuoja-asetuksen vaatimukset.

Pilvipalveluntarjoajat vastaavat palveluiden ylläpidosta, kehityksestä ja jatkuvasta toimivuudesta, mikä vähentää organisatorista taakkaa. Näillä palveluntarjoajilla on käytössään erikoistuneita tietoturva-asiantuntijoita sekä teknistä osaamista, mikä mahdollistaa korkeatasoisen tietoturvan ylläpitämisen ja tietosuoja-asetuksen vaatimusten täyttämisen. (Yang ym., 2020.) Pilvipalvelutarjoajien asiantuntijat huolehtivat järjestelmien tietoturvan päivittämisestä ja kehittämisestä, minkä ansiosta asiakasdata pysyy suojattuna kehittyviltä kyberuhilta.

Pilvipalveluntarjoajien avulla on mahdollista vähentää asiakasorganisaatioiden hallinnollista vastuuta tietoturvan ylläpidossa. Pilvipalvelut, kuten Microsoft Azure ja Salesforce, ilmoittavat noudattavansa yleisen tietosuoja-asetuksen vaatimuksia (Microsoft, 2024; Salesforce, 2024). Sertifikaatteja hankitaan usein osoittamaan asiakasorganisaatioille palveluiden korkeaa tietoturva- ja tietosuojatasoa, mikä helpottaa tietosuoja-asetusten noudattamisen varmistamista. Pilvipalveluiden käytössä palvelutarjoajan ja asiakasorganisaation välillä voidaan laatia palvelutasosopimuksia, joissa määritellään tietoturvaan liittyvät sitoumukset, kuten datan eheys, palautusprosessit ja käyttöoikeudet (Mirobi & Arockiam, 2015). Lisäksi yleisen tietosuoja-asetuksen mukaiset auditoinnit voidaan toteuttaa säännöllisesti yhteistyössä pilvipalveluntarjoajan ja asiakasorganisaation kanssa, mikä edistää tietosuojavaatimusten täyttämistä. Tällöin vastuuta voidaan myös siirtää asiakasorganisaatiolta pilvipalvelutarjoajalle, mikä helpottaa asiakasorganisaation hallinnollista työtä. (Nicolaou ym., 2012.)

Tekniseltä osalta pilvipalvelut tarjoavat merkittäviä tietoturvaominaisuuksia. Pilvipalvelut mahdollistavat asiakasdatan salauksen, joka usein toteutetaan vahvana salauksena. Vahva salaus toteutetaan esimerkiksi AES-256-salausalgoritmilla (Advanced Encryption Standard, 256 bittiä), jolla voidaan varmistaa suuren datamäärän tehokas salaus asiakasdatan siirrossa ja tallennuksessa. (Biryukov & Khovratovich, 2009.) Asiakasdatan salaus noudattaa yleisen tietosuoja-asetuksen määritystä tietojen anonymisoinnista ja pseudonymisoinnista, mikä tarkoittaa tiedon prosessointia siten, että henkilö ei ole tunnistettavissa tietojen perusteella (Yleinen tietosuoja-asetus, 2016).

Pilvipalveluissa hyödynnetään usein monivaiheista tunnistautumista, jossa henkilöllisyys varmennetaan kahden tai useamman tunnistautumistavan avulla (Kyberturvallisuuskeskus, 2024). Tällä menettelyllä pyritään varmistamaan, että asiakasdatan käsittelyoikeudet rajataan ainoastaan valtuutetuille henkilöille, mikä on yleisen tietosuoja-asetuksen vaatimusten mukaista (Yleinen tietosuoja-asetus, 2016). Monivaiheisen tunnistautumisen avulla voidaan estää asiattomien pääsy asiakasdataan ja hallita pääsyoikeuksia järjestelmällisemmin. Näin ollen tietoturvaa vahvistetaan, mikä edesauttaa organisaatioita täyttämään tietosuoja-asetuksen velvoitteet koskien henkilötietojen suojaa ja hallintaa. (Kyberturvallisuuskeskus, 2024.)

Lokitietojen kerääminen on keskeinen osa tietoturvakäytäntöjä, sillä se mahdollistaa tapahtumien ja niiden aiheuttajien seurannan ja analysoinnin (Kyberturvallisuuskeskus, 2023). Lokitiedot ovat välttämättömiä, jotta voidaan varmistaa asiakasdatan laillinen käyttö pilvipalveluissa. Erityisesti tietosuojaloukkaustilanteissa lokitiedoilla voidaan selvittää virhetilanteet, kuten asiakasdatan vahingollinen tai tahallinen väärinkäyttö. Pilvipalveluiden tarjoamat valmiit lokitustoimintaratkaisut

vähentävät asiakasorganisaation hallinnollista taakkaa ja helpottavat tietosuoja-asetuksen noudattamista. (Khan & Ullah, 2017.) Lokitiedot ovat myös osana järjestelmän auditointia, minkä avulla auditointi voidaan toteuttaa tehokkaasti (Kyberturvallisuuskeskus, 2023).

Pilvipalvelut lupaavat vahvaa tietoturvaa käyttäjille, mutta yleisen tietosuoja-asetuksen näkökulmasta asiakasdatan täysi ulkoistaminen tuo myös epävarmuutta. Wang ym., (2011) tutkimuksen mukaan tietokantojen ja sovellusohjelmistojen ulkoistaminen pilvipalveluiden tietokeskuksiin tuo laaja-alaisia tietoturvaongelmia, kun tietojen ja palveluiden hallinta ei ole täysin luotettavaa.

Pilvipalvelut voivat luoda ongelmia organisaatioille, jotka ovat velvoitettuja noudattamaan yleistä tietosuoja-asetusta. Suuret pilvipalveluiden tuottajat käyttävät usein globaaleja datakeskuksia, jotka eivät toimi suoraan Euroopan unionin alueella. Pilvipalveluiden virtuaalipalvelimet voivat olla sijoitettuna esimerkiksi Intiassa tai Yhdysvalloissa, mikä tarkoittaa asiakasdatan tiedonsiirtoa EU:n ulkopuolelle. (AlSudiari, 2012.) Pilvipalvelutarjoajien toimiessa EU:n ulkopuolella, yleisen tietosuoja-asetuksen noudattaminen ei ole yhtä tarkasti valvottua, tai mahdollisesti noudatetaan toisen maan tietosuojakäytäntöjä, jotka eivät vastaa sisällöltään EU:n tietosuoja-asetusta. (Bell ym., 2024.) Organisaation hyödyntäessä pilvipalveluita asiakasdatan laillinen siirto ja tallentaminen voi olla vaikea määrittää ja seurata, mikä puolestaan rikkoo yleisen tietosuoja-asetuksen artikloita 44–50.

Yleisen tietosuoja-asetuksen mukaan organisaation tulee vastata asiakasdatan tiedonhallinnasta. Pilvipalveluiden käyttö voi johtaa asiakasdatan hallinnan menettämiseen ja käsittelyprosessien epävarmuuteen, mikä vaikeuttaa tietosuoja-asetuksen edellytyksien toteutumista. Ongelmana tiedonhallinnassa voidaan myös nähdä vastuunjaon epäselvyys organisaation ja pilvipalvelutarjoajan välillä. Asetuksen mukaiseen tiedonhallintaan kuuluu asiakasdatan käyttöoikeuksien hallinta, mikä pilvipalveluissa ei aina toteudu. Pilvipalveluissa ulkopuoliset tahot voivat päästä käsiksi tietoihin, mikäli pilvipalvelun suojatoimet ovat heikot. (Wang ym., 2011.) Yleisen tietosuoja-asetuksen artikloiden 5, 25 ja 32 mukaan pääsy henkilötietoihin tulee olla tarkasti rajattu ja oikeudet määräytyvät nimetyn tarkoituksen mukaan (Yleinen tietosuoja-asetus, 2016).

Asiakasdatan siirto pilvipalveluihin luo tietoturva-aukkoja tietojensalausvaatimuksiin, kuten pseudonymisointiin ja anonymisointiin. Yleisen tietosuoja-asetuksen (2016) artikloiden 6, 25 ja 32 ja Tietosuojavaltuutetun toimiston (2024) mukaan pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja. Anonymisointi puolestaan tarkoittaa henkilötietojen käsittelyä siten, että henkilöä ei enää voida

tunnistaa niistä. Ongelmana pilvipalveluissa nähdään kaiken asiakasdatan säilyttäminen samassa pilvipalvelussa, jolloin pseudonymisointi ja anonymisointi ei välttämättä täyty (Badii ym., 2020). Henkilötietovuotojen ilmetessä pilvipalveluiden tuomat riskit ovat vahingollisia asiakkaille ja organisaatiolle, samalla rikkoen yleistä tietosuoja-asetusta.

Yleisen tietosuoja-asetuksen artikloiden 17 ja 19 mukaan asiakkaalla on oikeus pyytää omien tietojen poistamista ja tarjota mahdollisuus tietojen unohtamiseen. Organisaation vastuulla on hallita asiakasdataa siten, että kyetään vastaamaan asiakkaan pyyntöä tiedonhallinnasta. (Yleinen tietosuoja-asetus, 2016.) Pilvipalveluissa ristiriitana on tietojen poiston varmuus, sillä asiakkaan tiedot voivat olla hajautettuna pilvipalveluissa ja organisaation käyttöoikeudet tiedonhallintaan voivat olla rajalliset. Tietosuoja-asetuksen asettamaa edellytystä henkilötietojen poistoon asiakasdatasta voi olla haastavaa pilvipalveluissa ja tietojen poistoa voi olla vaikea varmistaa. Tiedonhallinnan rajatut oikeudet hajautetussa pilviympäristössä voi johtaa asiakasdatan osittaiseen poistoon. Asiakkaasta jää yhä tietoja pilvipalveluun, mikä rikkoo yleistä tietosuoja-asetusta ja asiakkaan oikeuksia. (Bell ym., 2024.)

Yleisen tietosuoja-asetuksen artiklat 24, 32 ja 35 velvoittavat organisaatioita asiakasdatan laillisen ja asianmukaisen käsittelyn myös pilvipalveluissa. Tätä velvoitetta pystytään toteuttamaan tietosuoja-auditointien avulla, jossa selvitetään organisaation sisällä tapahtuvien prosessien lainmukaisuus ja ajantasaisuus (Bell ym., 2024). Auditoinnissa organisaation on varmistettava pilvipalvelutarjoajien riskinhallintatoimien riittävyys ja kyky osoittaa asiakasdatan käsittelyn oikeellisuus. Ongelmaksi voi ilmetä auditoinnin toteuttamisen vaikeus, jos asiakasdata on hajautettu useampaan pilvipalvelualustaan ja -varastoon. Hajautetussa pilviympäristössä auditointi on monimutkaisempi prosessi, kun kaikista asiakasdataa käsittelevistä pilvipalveluista vaaditaan omat auditoinnit. Monen pilvipalvelun auditoinnissa virheiden riski kasvaa ja auditointitulokset voivat olla heikompia. (Chou, 2015.)

Pilvipalveluiden käytön suurin riski organisaatiolle on tietomurrot, jossa ulkopuolinen taho pääsee käsiksi organisaation keräämään asiakasdataan (Nordlayer, 2024). Ongelmana pilvipalveluiden käytössä on organisaation riippuvuus pilvipalvelutarjoajan kykyyn havaita tietomurto (Badii ym., 2020). Jos tietomurtoa ei havaita, tai se havaitaan liian myöhään, on asiakasorganisaatio rikkonut yleistä tietosuoja-asetusta ja on velvollinen sen seurauksista. Tietomurroissa asiakasdatan leviäminen on tuhollista asiakasorganisaation maineelle samalla loukaten asiakkaiden oikeuksia.

Yhteenvetona asiakasdatan siirron, tiedonhallinnan ja poistamisen ulkoistaminen pilvipalveluille muodostaa monimutkaisen kokonaisuuden tietosuojan ja tietoturvariskien osalta. Yleisen tietosuoja-

asetuksen vaatimusten noudattaminen ei aina toteudu, kun pilvipalvelut toimivat hajautetusti globaalilla tasolla. Tietoturvallisuutta ei voida suoraan rinnastaa yleiseen tietosuoja-asetukseen, mikä aiheuttaa oikeudellisia riskejä pilvipalveluita hyödyntäville asiakasorganisaatioille (Chauhan & Shiaeles, 2023). Suuret pilvipalvelutarjoajat, kuten Microsoft ja Salesforce, tunnetaan kuitenkin luotettavuudestaan ja tietosuoja-asetuksen noudattamisesta. Asiakasdatan ulkoistaminen tällaisille toimijoille voi vähentää tietoturvariskejä ja parantaa yleisen tietosuoja-asetuksen toteutumista. Vastuu tietosuoja-asetuksen noudattamisesta säilyy kuitenkin asiakasorganisaatiolla, joka vastaa laillisten velvoitteiden täyttämisestä (Yleinen tietosuoja-asetus, 2016). Edellä mainitut hyödyt ja haitat on koottu alla olevaan taulukkoon 1. Taulukossa esitetään, kuinka pilvipalveluiden hyödyt voivat olla ristiriidassa yleisen tietosuoja-asetuksen edellytysten kanssa.

Taulukko 1 Yhteenveto pilvipalveluiden hyödyistä ja haitoista yleisen tietosuoja-asetuksen näkökulmasta.

Hyödyt	Haitat
Pilvipalvelut vähentävät asiakasorganisaatioiden hallinnollista taakkaa tietoturvan ylläpidossa.	Tietosuoja-asetuksen noudattaminen voi vaikeutua, jos pilvipalveluiden toiminta ei täytä tietosuoja-asetusten vaatimuksia.
Palveluntarjoajien erikoistuneet tietoturva-asiantuntijat ylläpitävät ja kehittävät tietoturvaa jatkuvasti.	Asiakasdata voi sijaita globaalisti hajautetuissa datakeskuksissa, mikä aiheuttaa epävarmuutta tiedon laillisessa siirrossa ja tallennuksessa.
Vahvat salausmenetelmät, kuten AES-256, suojaavat asiakasdataa siirrossa ja tallennuksessa.	Asiakasdata voi olla alttiina tietoturvariskeille, jos palveluntarjoajan toimenpiteet eivät riitä esimerkiksi tietomurtojen ehkäisyyn.
Monivaiheinen tunnistautuminen parantaa pääsyoikeuksien hallintaa ja tietoturvaa.	Asiakasorganisaatio voi menettää hallinnan asiakasdatan käsittelyyn ja käyttöoikeuksiin, mikä voi vaikeuttaa tietosuoja-asetuksen noudattamista.
Automaattiset varmuuskopiot ja tietojen palautusprosessit vähentävät datan katoamiseen liittyviä riskejä.	Pilvipalveluiden käyttö voi johtaa henkilötietojen poistamisen epävarmuuteen, mikä rikkoo tietosuoja-asetuksen vaatimuksia.
Valmiit lokitustoimintoratkaisut tehostavat tietoturva-auditointeja ja helpottavat tietosuoja-asetusten noudattamista.	Lokitustoiminnon tietoturvariskit pilvipalveluissa luo uuden riskityypin asiakasorganisaatiolle.
Pilvipalvelut tarjoavat suojaa kyberhyökkäysten ja luonnonkatastrofien varalta datan sijainnin riippumattomuuden avulla.	Tietomurtojen havaitsemisen ja hallinnan riippuvuus pilvipalveluntarjoajasta voi johtaa tietosuoja-asetusten rikkomiseen ja seurauksiin.

3.3 Asiakasdatan varastointi pilvipalveluissa

Yksi keskeisistä tavoista ulkoistaa asiakasdataa pilvipalveluihin on sen varastointi pilvipohjaisten tietovarastojen (engl. data warehousing) avulla. Pilvipalveluntarjoajien tietovarastot ovat erityisen tehokkaita suurten datamäärien käsittelyssä ja tallentamisessa. Näitä tietovarastoja hyödynnetään tallennuksen ohella myös datan analysointiin ja raporttien laatimiseen organisaatioissa, mikä tekee niistä ihanteellisen ratkaisun laajamittaiseen tiedonhallintaan, erityisesti asiakasdatan hallinnan

näkökulmasta. Pilvitietovarastojen avulla organisaatiot voivat yhdistää dataa useista lähteistä keskitetylle alustalle, mikä parantaa tiedon hallittavuutta ja saavutettavuutta. (Rehman ym., 2018.) Tietovarastot usein toteutetaan IaaS-pilvipalveluna, jossa asiakasorganisaation data on tallennettuna virtuaalisella palvelimella (Ahmadi, 2023). Asiakasorganisaatio vastaa datan hallinnasta, mutta ylläpito on pilvipalvelutarjoajan vastuulla.

Tietovarastojen täyttämiseen käytetään yleensä ETL-prosessia (engl. Extract, Transform, Load), joka on dataintegraation keskeinen vaihe. Tässä prosessissa dataa kerätään useista lähteistä, muunnetaan organisaation tarpeisiin sopivaan muotoon ja lopulta ladataan pilvipohjaiseen tietovarastoon. ETL-prosessi mahdollistaa datan yhtenäistämisen ja hyödyntämisen eri liiketoimintatarpeissa. Pilvitietovarastot tarjoavat perustan liiketoimintatiedon hallinnalle (engl. Business Intelligence, BI), jossa kerätty ja prosessoitu data muunnetaan strategista ja operatiivista päätöksentekoa tukevaksi tiedoksi. (Rehman ym., 2018.)

Pilvipalvelutarjoajien tietovarastot tarjoavat merkittäviä tietoturvaetuja asiakasorganisaatioille. Nämä tietoturvaominaisuudet ovat usein linjassa yleisen tietosuoja-asetuksen vaatimusten kanssa, erityisesti asiakasdatan tarkoituksenmukaisessa käsittelyssä. Tietovarastojen avulla pääsyoikeuksia voidaan rajata tarkasti, mikä mahdollistaa pääsyn määrittämisen asiakasdatan käsittelijän työtehtävien mukaisesti. (Ahmadi, 2023.) Esimerkiksi asiakasorganisaation markkinointiosastolle voidaan määritellä pääsyoikeudet, jotka rajoittuvat kuluttajakäyttäytymistä koskevan asiakasdatan tarkasteluun, kun taas talousosastolle voidaan myöntää pääsy ainoastaan taloustietoihin perustuvaan asiakasdataan.

Pääsyoikeuksien hallinta ehkäisee virheellistä asiakasdatan käsittelyä ja tukee yleisen tietosuoja-asetuksen tehokasta noudattamista. Pääsyoikeuksien hallintaa voidaan edelleen vahvistaa monivaiheisella tunnistautumisella, joka varmistaa, että vain valtuutetut henkilöt pääsevät käsittelemään asiakasdataa. Tämä lisää asiakasdatan turvallisuutta ja vähentää tietovuotojen riskiä, edistäen samalla organisaation tietosuoja- ja turvallisuustavoitteiden toteutumista. (Jung ym., 2013.) Monet pilvitietovarastot, kuten Google ja Microsoft, tarjoavat myös yleisen tietosuoja-asetuksen edellyttämän lokitustoiminnon tietovarastoissa, jolloin pääsyoikeuksia kyetään seuraamaan, varmistaen laillisen tiedonkäsittelyn (Google Cloud Storage, 2024; Microsoft Azure, 2024).

Pilvitietovarastoissa asiakasorganisaation data suojataan useilla edistyneillä teknologisilla menetelmillä, joista keskeisin on datan salaus. Salaus estää tietojen päätymisen luvattomiin käsiin mahdollisten tietovuotojen tai tietomurtojen yhteydessä. (Sun ym., 2014.) Tämä lähestymistapa on linjassa yleisen tietosuoja-asetuksen (2016) artikloiden 6, 25 ja 32 kanssa, erityisesti henkilötietojen

pseudonymisoinnin ja anonymisoinnin osalta. Datan salaus mahdollistaa siis vahvemman tietosuojan ja helpottaa organisaatioita noudattamaan yleistä tietosuoja-asetusta pilvitietovarastoissa.

Pilvitietovarastojen turvallisuutta vahvistaa lisäksi niiden infrastruktuurin suunnittelu ja hallinta, joista vastaavat järjestelmien tietoturvaan erikoistuneet asiantuntijat. Tämä vähentää merkittävästi teknologisia riskejä, kuten järjestelmien haavoittuvuuksia tai inhimillisistä virheistä johtuvia tietoturvaloukkauksia. Pilvitietovarastot hyödyntävät kehittyneitä suojausmekanismeja, kuten useita palomuureja, tunkeutumisen havaitsemisjärjestelmiä ja monivaiheista tunnistautumista, jotka takaavat tietojen suojan sekä organisaation sisäisiltä että ulkoisilta uhilta. (Ahmadi, 2023.)

Tietoturvan lisäksi pilvitietovarastot tarjoavat varmuuskopiointiin ja tietojen palauttamiseen liittyviä ratkaisuja. Ratkaisut parantavat organisaation resilienssiä mahdollisten häiriötilanteiden, kuten tietojen menetysten varalta. Näiden ominaisuuksien ansiosta asiakasorganisaatiot voivat varmistaa datan saatavuuden ja eheyden myös odottamattomissa tilanteissa. Pilvipohjaiset tietovarastot ovat siten keskeinen osa nykyaikaista tietoturvastrategiaa, yhdistäen kehittyneet suojausteknologiat, luotettavuuden ja skaalautuvuuden. (Kahn ym., 2022.)

Pilvitietovarastoinnissa voidaan kuitenkin havaita merkittäviä tietoturvauhkia, jotka rikkovat lähes poikkeuksetta aina yleistä tietosuoja-asetusta. Kun asiakasorganisaatio ulkoistaa datan varastoinnin pilvipalveluihin, se tulee riippuvaiseksi pilvipalveluntarjoajan tietoturvasta ja toiminnan luotettavuudesta (Mishra ym., 2023). Kyberrikokset ovat lisääntyneet viime vuosikymmeninä ja monet niistä ovat kohdistuneet erityisesti pilvipalveluihin, mukaan lukien niiden tietovarastoihin. Esimerkiksi vuonna 2019 Microsoftin pilvitietokantoihin kohdistui kyberhyökkäys, jonka seurauksena yli 250 miljoonan henkilön tiedot vuotivat. Microsoft on tunnettu ja luotettu pilvipalvelutarjoaja, jonka tietoturvamaine on vahva, mutta riittävilläkään resursseilla täydellistä tietoturvaa ei voida taata. (Morgan, 2024.)

Pilvitietovarastojen tietoturvahaasteena on erityisesti pilviympäristön monimutkaisuus, joka vaikeuttaa tehokkaiden turvallisuus- ja yksityisyystoimenpiteiden toteuttamista. Pilvi-infrastruktuuri, jossa yhdistyvät erilaiset palvelumallit ja dynaamisesti skaalautuvat resurssit, luo haasteita tietoturvan hallinnalle. Monimutkaisuuden lisäksi pilvipohjainen tietovarastointi on integroitu järjestelmä, joka voi tuoda haasteita, kun se yhdistetään organisaation aikaisempiin järjestelmiin. Erilaiset teknologiat ja tietoturvakehykset voivat vaikeuttaa yhtenäisten turvallisuusprotokollien toteuttamista. Tämä asettaa merkittäviä haasteita asiakasorganisaatioille,

sillä ne eivät voi suoraan vaikuttaa pilvitietovarastojen tekniseen toteutukseen ja turvallisuustoimenpiteisiin. (Ahmadi, 2023.)

Asiakasorganisaation riippuvuus pilvitietovarastoista on erityisen ongelmallista yleisen tietosuoja-asetuksen näkökulmasta, sillä organisaatio joutuu luottamaan sokeasti pilvipalveluntarjoajan tietoturvatoimiin. Usein tämä luottamus perustuu vain pilvipalveluntarjoajan sitoumuksiin tietosuoja-asetuksen noudattamisesta. Sevillan (2023) tutkimuksen mukaan jopa kolmasosa yhdysvaltalaisista yrityksistä on salannut kyberhyökkäyksiä ja tietomurtoja välttääkseen asiakkaille maksettavat korvaukset. Tämä luo merkittäviä ongelmia tietosuoja-asetuksen noudattamisen kannalta pilvipalveluja hyödyntäville asiakasorganisaatioille, sillä ne ovat lain mukaan vastuussa pilvipalveluissa säilytettävästä asiakasdatasta. Jos asiakasorganisaatioilta salataan tietoa tietomurroista, asiakkaille ei voida asianmukaisesti tiedottaa tietovuodoista. Tietosuoja-asetus velvoittaa organisaatioita ilmoittamaan aina tietomurroista ja -vuodoista, mikä tekee tiedon salaamisesta erityisen ongelmallisen organisaatioille ja asiakkaille (Yleinen tietosuoja-asetus, 2016).

Yhteenvetona voidaan todeta, että pilvitietovarastot tarjoavat tehokkaan ratkaisun asiakasdatan tallentamiseen ja analysointiin, mutta ne tuovat myös tietoturvahaasteita. Keinoja, kuten datan salaus, pääsyoikeuksien hallinta ja monivaiheinen tunnistautuminen, käytetään turvallisuuden parantamiseen ja siten yleisen tietosuoja-asetuksen noudattamiseen. Kuitenkin pilvipalveluntarjoajan tietoturvasta riippuvuus luo riskejä, sillä organisaatiot eivät voi suoraan vaikuttaa tietovarastojen turvallisuuteen. Jos pilvipalveluntarjoaja ei noudata yleistä tietosuoja-asetusta, kuten salaa tietomurrot, asiakasorganisaatio ei voi tiedottaa asiakkaitaan tietovuodoista, mikä rikkoo tietosuoja-asetuksen edellytyksiä.

3.4 Pilvipohjaiset asiakkuudenhallintajärjestelmät

Asiakkuudenhallintajärjestelmiä (engl. customer relationship management systems, CRM-järjestelmät) hyödynnetään organisaatioissa asiakasdatan hallintaan ja käsittelyyn. Näiden järjestelmien avulla asiakasdataa voidaan käyttää erilaisiin toimintoihin, kuten myynnin seurantaan, markkinoinnin automatisointiin ja asiakaspalautteiden hallintaan. (Rababah, 2011.) Pilvipohjaiset CRM-järjestelmät toteutetaan tyypillisesti SaaS-palveluina, joissa asiakasdatan hallinta tapahtuu valmiiksi tuotetun ohjelmiston tai sovelluksen kautta (Chen ym., 2018).

SaaS-pohjaiset CRM-järjestelmät eroavat perinteisistä asiakkuudenhallintajärjestelmistä siten, että ne eivät vaadi organisaatiolta merkittäviä investointeja laitteistoihin, ohjelmistoihin tai työvoimaan

järjestelmien ylläpitämiseksi. Tämä tekee niistä houkuttelevia erityyppisille yrityksille. Pilvi-CRM-järjestelmät mahdollistavat asiakkuudenhallinnan työkalujen käytön verkkoselaimella missä tahansa, mikä lisää liiketoimintaprosessien joustavuutta ja tuottavuutta internetin välityksellä. Tämän myötä organisaatioiden työntekijöiden liikkuvuutta ja tehokkuutta voidaan parantaa merkittävästi. (Chen ym., 2018.) Yleisen tietosuoja-asetuksen näkökulmasta pilvipohjaiset CRM-järjestelmät tarjoavat etuja tietosuojan ylläpidossa, hyödyttäen asiakasorganisaatioita valmiiden tietoturvaratkaisujen ja teknisen ylläpidon ansiosta.

Pilvipohjaiset CRM-järjestelmät tarjoavat asiakasorganisaatioille tehokkaita keinoja pääsyoikeuksien hallintaan, mikä mahdollistaa asiakasdatan käsittelyn rajoittamisen vain siihen oikeutetuille työntekijöille asiakasorganisaatiossa. Roolipohjainen pääsynhallinta mahdollistaa pääsyoikeuksien määrittämisen käyttäjien työtehtävien mukaisesti, mikä vähentää merkittävästi asiakasdatan virheellisen käsittelyn riskiä. Lisäksi roolipohjaisen pääsynhallinnan reaaliaikaiset ominaisuudet mahdollistavat pääsyoikeuksien joustavan ja nopean muokkaamisen organisaation tarpeiden mukaan. (Prince & Lovesum, 2020.) SaaS-pohjaiset CRM-järjestelmät tukevat pääsyoikeuksien hallintaa tarjoamalla mahdollisuuden integroida järjestelmään asiakasorganisaation omia toiminnanvalvontajärjestelmiä, mikä tehostaa pääsyoikeuksien valvontaa (Amin, 2023). Näiden ominaisuuksien ansiosta CRM-järjestelmät tukevat yleisen tietosuoja-asetuksen noudattamista, mikä yksinkertaistaa organisaatioiden tiedonhallintaprosesseja ja edistää tietoturvan ylläpitoa.

Tiedonsiirron salaus pilvipohjaisissa CRM-järjestelmissä on keskeinen etu tietoturvan ja yleisen tietosuoja-asetuksen näkökulmasta. Tiedonsiirron salaus ei rajoitu pelkästään asiakasdatan varastointiin, vaan kattaa myös tiedonsiirtoprosessit, mikä vahvistaa asiakasdatan turvallisuutta. (Sanodia, 2019.) Pookandyn (2020) tutkimuksen mukaan pilvipalveluiden CRM-järjestelmiin on integroitu End-to-End-salausmekanismeja (lyh. E2EE), jotka varmistavat asiakasdatan salauksen sen alkuperäisestä lähteestä määränpäähänsä saakka. E2EE estää luvattomien osapuolien, mukaan lukien pilvipalveluntarjoajan, pääsyn asiakasdataan tiedonsiirron aikana. Tämä salausmekanismi varmistaa asiakasdatan eheyden ja oikeellisuuden ja noudattaa tietosuoja-asetuksen vaatimuksia, kuten tietojen anonymisointia ja pseudonymisointia.

Pääsynhallinta ja tiedonsiirron salaus pilvi-CRM-järjestelmissä sisältyy CIA-malliin, joka perustuu kolmeen keskeiseen tietoturvaperiaatteeseen: luottamuksellisuus, eheys ja saatavuus (engl. Confidentiality, integrity, availability). Tietoturvaperiaatteet muodostavat niin sanotun CIA-mallin. Pilvipalveluntarjoajat pyrkivät noudattamaan näitä periaatteita CRM-järjestelmissään.

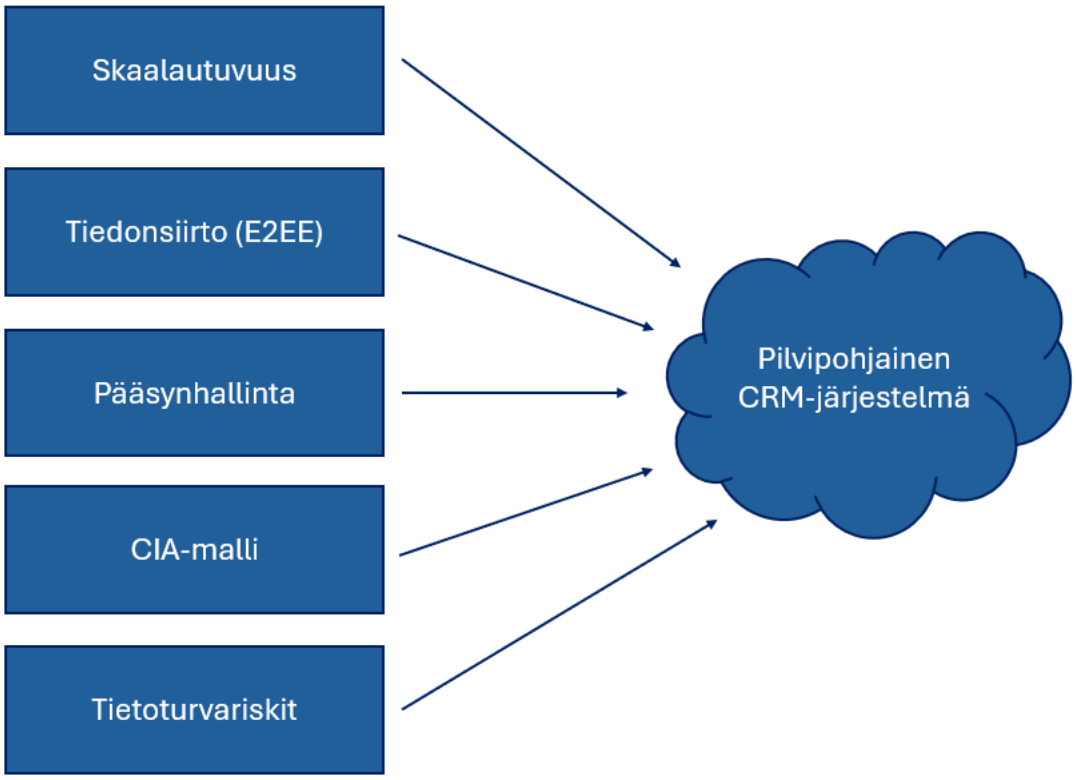
Luottamuksellisuus varmistaa, että tieto on vain lähettäjän ja vastaanottajan käytettävissä, estäen kolmansien osapuolien pääsyn tietoihin. Tiedon eheys takaa, että tiedot pysyvät muuttumattomina, eivätkä ne ole alttiina menetyksille tai vahingoittumiselle. Saatavuus puolestaan takaa, että valtuutetut käyttäjät voivat käyttää tietoja tarvittaessa. Näitä periaatteita tukevat kehittyneet salausalgoritmit ja monivaiheiset tietoturvaprotokollat. CIA-mallin perusperiaatteet vastaavat yleisen tietosuoja-asetuksen vaatimuksia, erityisesti tiedon suojaamisen ja käyttöoikeuksien hallinnan osalta. (Shaqrah, 2016.)

Pilvipohjaisilla CRM-järjestelmillä on hyvä tietoturva, mutta ne altistuvat myös vakaville tietoturvariskeille, jotka rikkovat yleisen tietosuoja-asetuksen edellytyksiä. Näillä järjestelmillä esiintyy samoja kyberhyökkäyksiä ja tietovuotojen uhkia kuin pilvipohjaisilla tietovarastoilla. CRM-järjestelmissä käsiteltävä asiakasdata ja asiakasorganisaatioiden tiedot ovat arvokasta tietoa, mikä tekee niistä houkuttelevia hyökkäyskohteita. Yleisimmät riskit pilvipohjaisissa CRM-järjestelmissä liittyvät palvelunestohyökkäyksiin, joissa hyökkääjät voivat ylikuormittaa palvelimen kapasiteetin, mikä johtaa järjestelmän toimintakyvyn menetykseen. (Amin, 2023.) Palvelunestohyökkäyksillä voi olla merkittäviä seurauksia niin taloudellisesti kuin oikeudellisesti, ja asiakasdatan päätyminen luvattomille henkilöille rikkoo yleisen tietosuoja-asetuksen edellytyksiä.

Pilvipohjaisissa CRM-järjestelmissä tietoturvahaasteena on myös asiakasdatan pitkäaikainen säilyttäminen, mikä voi johtaa sen unohtumiseen järjestelmissä. Pilvipohjaiset CRM-järjestelmät keräävät jatkuvasti suuria määriä asiakasdataa niiden skaalautuvuusedun vuoksi, mutta asiakasdatan pitkäaikainen säilytys tuo mukanaan merkittäviä tietoturvariskejä. Datan määrän kasvaessa myös riskien hallinta vaikeutuu ja niiden seuraukset voivat olla huomattavasti vakavampia. (Shaqrah, 2016.) Yleisen tietosuoja-asetuksen noudattaminen voi muodostua haastavaksi, jos asiakasorganisaatiot eivät pysty poistamaan asiakasdataa asiakkaan toiveiden mukaisesti CRM-järjestelmistä. Erityisesti, jos asiakasdata on hajautettu useisiin CRM-järjestelmiin, sen hallinta voi käydä lähes mahdottomaksi, mikä voi loukata yksilöiden oikeuksia (Souri ym., 2017).

Yhteenvetona voidaan todeta, että pilvipohjaiset CRM-järjestelmät tarjoavat organisaatioille tehokkaita tapoja hallita asiakasdataa ilman suuria investointeja laitteistoon ja ohjelmistoihin. Ne tukevat tietosuoja-asetuksen noudattamista kehittyneillä tietoturvaratkaisuilla, kuten roolipohjaisella pääsynhallinnalla ja tiedonsiirron salauksella. Kuitenkin pilvipohjaisilla CRM-järjestelmillä on myös tietoturvariskejä, kuten palvelunestohyökkäykset ja asiakasdatan pitkäaikainen säilyttäminen, mikä voi vaikeuttaa tietojen hallintaa ja aiheuttaa tietosuojaongelmia. CRM-järjestelmän ulkoistaminen pilvipalveluille voidaan nähdä resurssien ja osaamisen puolesta järkevämpänä

ratkaisuna. Alla olevassa kuvassa 2 on tiivistetysti edellä mainitut CRM-järjestelmien päähyödyt ja haitta tietoturvan näkökulmasta.



Kuva 2 Pilvipohjaisen CRM-järjestelmän tietoturva. (Perustuu Amin, 2023; Biryukov & Khovratovich, 2009; Chen ym., 2018; Pookandy, 2020; Shaqrah, 2016.)

3.5 NIST-viitekehys

Yleinen tietosuoja-asetus toimii laillisena viitekehyksenä asiakasdatan käsittelyssä. Pilvipalvelutarjoajat, kuten Microsoft, Salesforce ja Google kehittävät palveluitaan tietosuoja-asetuksen mukaisesti, mutta sen lisäksi pilvipalveluissa voidaan noudattaa muita viitekehyksiä, jotka kohdistuvat järjestelmien tekniseen puoleen. Tekniset viitekehykset usein kohdistuvat kyberturvallisuuteen, jolla varmistetaan tietosuojatoimenpiteet pilvipalveluissa (Cambronero ym., 2024). Laajasti käytetty kyberturvallisuuden viitekehys on Yhdysvalloista peräisin oleva NIST (engl. National Institute of Standards and Technology), joka sisältää ohjeistuksia kyberturvallisuuden, tietosuojan ja riskienhallinnan osa-alueilta. NIST-viitekehys tarjoaa organisaatioille käytännön ohjeita ja työkaluja teknologisen turvallisuudenhallinnan tueksi. (Shen, 2014.) Viitekehys on Euroopan unionin yleistä tietosuoja-asetusta vanhempi, mutta se tukee vahvasti tietosuoja-asetuksen edellytyksiä teknologisella tasolla.

NIST-viitekehys tukee yleisen tietosuoja-asetuksen edellytyksiä omilla periaatteillaan, jotka tarjoavat rakenteen järjestelmien kyberuhkien torjunnalle. Viitekehys perustuu viiteen keskeiseen periaatteeseen: tunnista, suojaa, havaitse, reagoi ja palauta. Nämä periaatteet on suunnattu erityisesti kyberuhkien hallintaan, mikä on erityisen tärkeää pilvipalveluissa, joissa asiakasdatan suojaaminen on keskeistä. (Shen, 2014.) NIST-viitekehyksen pääperiaatteet tarjoavat vankan pohjan pilvipalveluiden kyberturvallisuudelle ja niiden noudattaminen tukee tehokkaasti yleisen tietosuoja-asetuksen vaatimusten täyttämistä, erityisesti asiakasdatan suojaamisessa ja käsittelyssä.

Viitekehyksen ensimmäinen pääperiaate ”tunnista” keskittyy organisaation vastuuseen arvioida ja ymmärtää kyberturvallisuusriskejä omissa järjestelmissään. Arvion perusteella voidaan kehittää suojausperiaatteita mahdollisiin kyberuhkiin. Suojaa-periaate keskittyy suojatoimien toteuttamiseen, kuten tietojen salaamiseen ja käyttöoikeuksien hallintaan. Suojaa-periaate vastaa sisällöltään vahvasti yleisen tietosuoja-asetuksen periaatteita asiakasdatan anonymisoinnista, pseudonymisoinnista ja henkilötietojen tarkoituksellisesta käsittelystä. Havaitse-periaate koskee järjestelmävalvontaa ja siinä ilmeneviä kyberuhkien havaitsemista, mikä mahdollistaa nopean reagoinnin uhkiin. Reagoi-periaate käsittelee niitä toimia, jotka toteutetaan uhkien tapahtuessa, jotta seuraukset ovat mahdollisimman minimaaliset. Palauta-periaatteessa organisaatio keskittyy palauttamaan liiketoimintansa normaaliksi kyberhyökkäyksen tapahduttua. (Liu ym., 2011.)

NIST-viitekehys on tehokas tapa pilvipalveluiden turvallisuuden parantamiseksi, sillä se mahdollistaa tietosuoja-asetuksen vaatimusten täyttämisen teknisestä näkökulmasta. Viitekehys tuo mukanaan merkittäviä etuja pääperiaatteidensa lisäksi, kuten joustavuutta ja selkeyttä. Se on mukautettavissa eri kokoisiin järjestelmiin ja pilvipalveluiden eri muotoihin, kuten SaaS-, IaaS- ja PaaS-palveluihin (Liu ym., 2011). NIST-viitekehys on selkeä, mikä helpottaa riskien kartoittamista ja mahdollistaa tehokkaiden suojaustoimenpiteiden kehittämisen kyberuhkia vastaan. Riskilähtöinen lähestymistapa varmistaa, että asiakasdatan suojaaminen pilvipalveluissa on entistä tehokkaampaa ja organisaatiot pystyvät reagoimaan asianmukaisesti riskitilanteissa.

NIST-viitekehys tukee yleistä tietosuoja-asetusta myös monilla muilla tavoilla asiakasdatan turvaamisessa. Vertaillessa yleisen tietosuoja-asetuksen artikloita ja NIST-viitekehystä taulukossa 2, niissä voidaan havaita monia samanlaisuuksia:

Taulukko 2 Yleisen tietosuoja-asetuksen ja NIST-viitekehyksen yhtenäisyydet. (Perustuu Liu ym., 2011; Souri ym., 2017; Sun ym., 2014; Yleinen tietosuoja-asetus, 2016.)

Yleisen tietosuoja-asetuksen artikla	Vastaavat NIST-viitekehyksen tietoturvaominaisuudet pilvipalveluissa
Artikla 5: Henkilötietojen käsittelyn periaatteet	NIST-viitekehys auttaa pilvipalveluiden tarjoajia varmistamaan, että pilvipalveluissa käsitellään henkilötietoja lainmukaisesti, säilyttämällä tietojen eheyden ja luottamuksellisuuden koko niiden elinkaaren ajan.
Artikla 6: Laillinen käsittelyperuste	NIST-viitekehys tukee pilvipalveluiden tietosuojakäytäntöjen kehittämistä ja dokumentointia, varmistaen, että pilvipalvelut noudattavat laillisia käsittelyperusteita ja -käytäntöjä.
Artikla 32: Tietoturva	NIST-viitekehys tarjoaa pilvipalveluille ohjeita kyberturvallisuuden toteuttamisesta, kuten tiedonsalauksen, pääsynhallinnan ja autentikoinnin käyttämisestä pilvipalveluiden tietoturvan ja asiakasdatan suojan varmistamiseksi.
Artikla 24: Vastuullisuus ja tietosuojan varmistaminen	Pilvipalveluiden tarjoajat voivat käyttää NIST-viitekehystä määrittääkseen vastuuroolit ja valvontamekanismit pilvipalvelujen tietosuojan ja tietoturvan varmistamiseksi, mukaan lukien jatkuva valvonta ja auditointi.
Artikla 33: Tietoturvaloukkauksista ilmoittaminen	NIST-viitekehys tukee pilvipalveluita kehittämään prosesseja ja käytäntöjä tietoturvaloukkauksista ilmoittamiseksi, mukaan lukien häiriöiden ja kyberhyökkäysten havaitseminen ja reagointi tehokkaasti pilvipalveluympäristössä.
Artikla 35: Vaikutusten arviointi	NIST-viitekehys tukee pilvipalveluita suorittamaan riskinarviointeja ja vaikutusten arviointeja, jotka keskittyvät erityisesti pilvipalveluissa tapahtuvien tietoturvauhkien ja riskien tunnistamiseen ja hallintaan.
Artikla 44: Henkilötietojen siirrot kolmansiin maihin	NIST-viitekehys voi tukea pilvipalveluiden tarjoajia hallitsemaan kansainvälisten tietosuojaa koskevien sääntöjen ja siirron turvallisuustoimenpiteiden, kuten tiedonsalauksen ja pääsynhallinnan, noudattamisen pilvipalveluiden rajat ylittävissä siirroissa.

Yleisen tietosuoja-asetuksen noudattaminen voi tehostua merkittävästi hyödyntämällä pilvipalveluissa lisäturvallisuutta tarjoavia viitekehyksiä. Esimerkiksi NIST-viitekehys tukee teknisen turvallisuuden ylläpitoa järjestelmissä tarjoamalla selkeitä ohjeita ja käytäntöjä kyberriskien hallintaan. NIST-viitekehyksen kaltaiset lisäsuojatoimenpiteet vahvistavat organisaation osaamista tietoturvallisuudessa, mikä puolestaan tukee yleisen tietosuoja-asetuksen edellytysten täyttämistä erityisesti asiakasdatan suojauksen ja käsittelyn osalta.

4 Yhteenveto ja johtopäätökset

Pilvipalveluiden hyödyntäminen tarjoaa merkittäviä etuja asiakasdatan käsittelyssä, erityisesti yleisen tietosuoja-asetuksen noudattamisen näkökulmasta. Näitä palveluita voidaan pitää turvallisena ratkaisuna, sillä ne yhdistävät kustannustehokkuuden korkeatasoiseen tietoturvaan. Pilvipalveluntarjoajien vahva järjestelmäinfrastruktuuri ja riittävät resurssit mahdollistavat tietoturvan jatkuvan ylläpidon ja kehittämisen, mikä tukee asiakasorganisaatioiden kykyä täyttää yleisen tietosuoja-asetuksen vaatimukset.

Erityisesti asiakasdatan salaus, pääsyoikeuksien hallinta ja lokitustoiminnot ovat yleisen tietosuoja-asetuksen kannalta merkittäviä pilvipalveluiden ominaisuuksia. Näiden keinojen avulla palveluntarjoajat takaavat tiedon eheyden ja suojaavat sitä luvattomalta käytöltä. Lisäksi pilvipalvelut vähentävät asiakasorganisaatioiden hallinnollista taakkaa ja parantavat toimintaprosessien tehokkuutta, mikä mahdollistaa resurssien kohdentamisen asiakasorganisaation ydintoimintoihin.

Pilvipalvelut tarjoavat organisaatioille myös skaalautuvan ja edullisen tavan säilöä, analysoida ja hyödyntää asiakasdataa. Pilvipalveluiden kyky vastata kehittyviin kyberuhkiin ja tietosuojavaatimuksiin tekee niistä houkuttelevan vaihtoehdon asiakasdatan hallintaan. Erityisesti pilvipalvelutarjoajien hyödyntäessä muita tietoturvaviitekehyksiä, kuten NIST-viitekehystä, pilvipalveluiden järjestelmäturvallisuuden voidaan katsoa olevan hyvä vaihtoehto. NIST-viitekehys tukee yleistä tietosuoja-asetusta teknologisesta näkökulmasta, keskittyen kyberuhkiin ja niistä palautumiseen. Se tarjoaa käytännön ohjeita ja työkaluja tietoturvan ylläpitoon järjestelmissä, mikä luo vahvan perustan myös yleisen tietosuoja-asetuksen noudattamiseen. NIST-viitekehyksen hyödyntäminen pilvipalveluissa lisää tietoturvan tasoa, jolloin myös asiakasdata pysyy vahvemmin turvattuna kyberuhkilta. Kokonaisuutena arvioiden pilvipalveluiden hyödyntäminen edistää tietoturvaa ja tietosuoja-asetuksen tavoitteiden toteutumista.

Pilvipalveluiden tarjoamasta korkeasta tietoturvatasosta huolimatta kyberturvallisuusuhat ovat jatkuva huolenaihe. Suurten palveluntarjoajien, kuten Googlen, Microsoft Azuren ja Salesforcen laaja käyttö ja keskeinen rooli tekevät niistä houkuttelevia kohteita kyberhyökkäyksille. Vaikka pilvipalveluissa hyödynnetään kehittyneitä riskinhallintajärjestelmiä ja lisäviitekehyksiä, kuten NIST-viitekehystä, tietomurtoja ei voida kuitenkaan aina täysin estää. Tietomurtojen lisäksi asiakasdatan hajauttaminen eri palveluihin voi aiheuttaa haasteita erityisesti yleisen tietosuoja-asetuksen edellytysten täyttämisessä.

Inhimilliset virheet, kuten asiakasdatan unohtaminen tai virheellinen käsittely pilvipalveluissa, ovat merkittäviä ongelmia, jotka ovat myös tietosuoja-asetuksen vastaista. Riskienhallinta edellyttää tarkkaa prosessien suunnittelua ja jatkuvaa seurantaa. Suuri riski asiakasorganisaatioille pilvipalveluita käytettäessä on niiden riippuvuus palveluntarjoajista. Kyberhyökkäysten ilmetessä, kuten tietomurroissa tai palvelunestohyökkäyksissä, asiakasorganisaatiolla on rajalliset mahdollisuudet vaikuttaa tilanteeseen. Riippuvuus pilvipalvelutarjoajaan lisää epävarmuutta asiakasdatan hallinnassa.

Lisäksi pimitetyt tietomurrot pilvipalveluissa voivat johtaa merkittäviin oikeudellisiin seuraamuksiin asiakasorganisaatioille. Yleisen tietosuoja-asetuksen mukaisesti tietoturvaloukkauksista on ilmoitettava viipymättä. Palveluntarjoajan laiminlyödessä tätä velvoitetta, voi seurauksena olla valtavat oikeudelliset ongelmat asiakasorganisaatiolla. Pilvipalveluiden käyttöön liittyvien riskien tunnistaminen ja hallinta on kriittinen osa organisaatioiden tietosuoja- ja tietoturvastrategiaa.

Organisaation päätös oman tietojärjestelmän rakentamisen ja pilvipalvelun käytön välillä on hyvä arvioida organisaation tarpeiden ja resurssien mukaisesti. Oman järjestelmän kehittäminen on kallis ja aikaa vievä prosessi, mutta se tarjoaa täyden hallinnan asiakasdatan käsittelyyn. Yleisen tietosuoja-asetuksen noudattaminen varmistetaan helpommin, kun järjestelmä on organisaation omassa hallinnassa. Pilvipalveluiden käyttöä pidetään kustannustehokkaana ja hallinnollista taakkaa vähentävänä ratkaisuna, mutta se luo riippuvuuden palveluntarjoajan toimintaan ja tietoturvaan. Pilvipalveluita käyttäessä asiakasorganisaation on luotettava sokeasti siihen, että yleistä tietosuoja-asetusta noudatetaan. Pilvipalvelut voivat olla parempi ratkaisu pienemmille yrityksille resurssien kannalta. Suurissa organisaatioissa se helpottaa suuren asiakasdatan käsittelyä. Molemmat ratkaisut asiakasdatan käsittelyyn ovat toimivia, mutta lopullisen päätöksen tulee perustua organisaation omiin tarpeisiin.

Lähteet

Ahmadi, S. (2023). Security and privacy challenges in cloud-based data warehousing: A comprehensive review. *International Journal of Computer Science Trends and Technology (IJCST), 11*(6). https://ssrn.com/abstract=4683262

AlSudiari, M. A. T. (2012). Cloud Computing And Privacy Regulations: An Exploratory Study On Issues And Implications. *Advanced Computing: An International Journal*, *3*(2), 159–169. https://doi.org/10.5121/acij.2012.3216

Amin, I. (2023, lokakuuta 10). Noudettu 17.11.2024. Most Common CRM Security Concerns and Solutions. Microsoft Dynamics and NetSuite Partner & Dynamics CRM Consultants in San Diego. https://www.alphabold.com/most-common-crm-security-concerns-and-solutions/

Ayala-Rivera, V., Portillo-Dominguez, A. O., & Pasquale, L. (2024). GDPR compliance via software evolution: Weaving security controls in software design. *Journal of Systems and Software*, *216*, 112144. https://doi.org/10.1016/j.jss.2024.112144

Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart city IoT platform respecting GDPR privacy and security aspects. *IEEE Access*, *8*, 23601–23623. https://doi.org/10.1109/ACCESS.2020.2968741

Bell, C., Broklyn, P., & Egon, A. (2024). Cloud Security and Data Privacy (SSRN Scholarly Paper No. 4904978). *Social Science Research Network*. https://doi.org/10.2139/ssrn.4904978

Biryukov, A., & Khovratovich, D. (2009). Related-Key Cryptanalysis of the Full AES-192 and AES-256. *Teoksessa M. Matsui (Toim.), Advances in Cryptology – ASIACRYPT 2009* (ss. 1–18). Springer. https://doi.org/10.1007/978-3-642-10366-7_1

Cambronero, M. E., Martínez, M. A., Llana, L., Rodríguez, R. J., & Russo, A. (2024). Towards a GDPR-compliant cloud architecture with data privacy controlled through sticky policies. *PeerJ Computer Science*, *10*, e1898. https://doi.org/10.7717/peerj-cs.1898

Caruccio, L., Desiato, D., Polese, G., & Tortora, G. (2020). GDPR Compliant Information Confidentiality Preservation in Big Data Processing. *IEEE Access*, *8*, 205034–205050. https://doi.org/10.1109/ACCESS.2020.3036916

Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network, 3(3)*, 422-450. https://doi.org/10.3390/network3030018

Chen, Y.-S., Wu, C., Chu, H.-H., Lin, C.-K., & Chuang, H.-M. (2018). Analysis of performance measures in cloud-based ubiquitous SaaS CRM project systems. *The Journal of Supercomputing*, *74(3)*, 1132–1156. https://doi.org/10.1007/s11227-017-1978-x

Chou, D. C. (2015). Cloud computing risk and audit issues. *Computer Standards & Interfaces, 42*, 137–142. https://doi.org/10.1016/j.csi.2015.06.005

EU-direktiivi 95/46/EY. (1995). https://eur-lex.europa.eu/eli/dir/1995/46/oj

Euroopan tietosuojavaltuutettu. (2018). Yleisen tietosuoja-asetuksen historia. https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Farhad, M. A. (2024). Consumer data protection laws and their impact on business models in the tech industry. *Telecommunications Policy, 48(9), 102836.* https://doi.org/10.1016/j.telpol.2024.102836

Fayard, D., Lee, L. S., Leitch, R. A., & Kettinger, W. J. (2012). Effect of internal cost management, information systems integration, and absorptive capacity on inter-organizational cost management in supply chains. *Accounting, Organizations and Society, 37(3),* 168–187. https://doi.org/10.1016/j.aos.2012.02.001

Garber, J. (2018). GDPR – compliance nightmare or business opportunity? *Computer Fraud & Security, 2018*(6), 14–15. https://doi.org/10.1016/S1361-3723(18)30055-1

Google Cloud Platform. (2024). Noudettu 14.11.2024. Google Cloud. https://cloud.google.com/gcp

Google Cloud Storage. (2024). Noudettu 19.11.2024. Google Cloud. https://cloud.google.com/storage/pricing

Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management, 33(5),* 861–874. Scopus. https://doi.org/10.1016/j.ijinfomgt.2013.07.001

István, Z., Ponnapalli, S., & Chidambaram, V. (2020). Towards software-defined data protection: GDPR compliance at the storage layer is within reach. arXiv preprint arXiv:2008.04936. https://doi.org/10.48550/arXiv.2008.04936

Jakobi, T., von Grafenstein, M., Legner, C., Labadie, C., Mertens, P., Öksüz, A., & Stevens, G. (2020). The Role of IS in the Conflicting Interests Regarding GDPR. *Business & Information Systems Engineering, 62(3),* 261–272. https://doi.org/10.1007/s12599-020-00633-4

Jung, T., Li, X.-Y., Wan, Z., & Wan, M. (2013). Privacy preserving cloud data access with multi-authorities. *2013 Proceedings IEEE INFOCOM,* 2625–2633. https://doi.org/10.1109/INFCOM.2013.6567070

Kahn, M. G., Mui, J. Y., Ames, M. J., Yamsani, A. K., Pozdeyev, N., Rafaels, N., & Brooks, I. M. (2022). Migrating a research data warehouse to a public cloud: Challenges and

opportunities. *Journal of the American Medical Informatics Association, 29(4),* 592–600. https://doi.org/10.1093/jamia/ocab278

Khan, M. N., & Ullah, S. (2017). A log aggregation forensic analysis framework for cloud computing environments. Computer Fraud & Security, 2017(7), 11–16. https://doi.org/10.1016/S1361-3723(17)30060-X

Kyberturvallisuuskeskus. (2023). Noudettu 15.11.2024. Näin keräät ja käytät lokitietoja. Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

Kyberturvallisuuskeskus. (2024). Noudettu 15.11.2024. Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology, 38(1),* 16-44. https://doi.org/10.1177/02683962221141456

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST Cloud Computing Reference Architecture. https://doi.org/10.6028/NIST.SP.500-292

Love, P. E. D., & Irani, Z. (2003). A project management quality cost information system for the construction industry. *Information & Management, 40(7),* 649–661. https://doi.org/10.1016/S0378-7206(02)00094-0

Microsoft. Microsoft Azure. Noudettu 14.11.2024. https://learn.microsoft.com/en-us/azure/

Mirobi, G. J., & Arockiam, L. (2015). Service Level Agreement in cloud computing: An overview. 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 753–758. https://doi.org/10.1109/ICCICCT.2015.7475380

Mishra, A., Jabar, T. S., Alzoubi, Y. I., & Mishra, K. N. (2023). Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework. Concurrency and Computation: Practice and Experience, 35(26), e7831. https://doi.org/10.1002/cpe.7831

Morgan, N. (2024). Noudettu 16.11.2024. Cloud cyber attacks: The latest cloud computing security issues. https://www.triskelelabs.com/blog/cloud-cyber-attacks-the-latest-cloud-computing-security-issues

Nicolaou, C. A., Nicolaou, A. I., & Nicolaou, G. D. (2012). Auditing in the Cloud: Challenges and Opportunities. The CPA Journal, 82(1), 66–70.

Nordlayer. (2024). Cloud Security Threats, Risks & Vulnerabilities. Noudettu 13.11.2024. Https://Nordlayer.Com. https://nordlayer.com/learn/cloud-security/risks-and-threats/

Pookandy, J. (2020). End-to-end encryption and data integrity verification in cloud CRM as a framework for securing customer communications and transactional data. *International Journal of Computer Science and Engineering Research and Development*, 10(1), 19-32. https://ijcserd.com/index.php/home/issue/view/IJCSERD_10_01_2020

Presthus, W., & Sørum, H. (2021). A THREE-YEAR STUDY OF THE GDPR AND THE CONSUMER. https://www.iadisportal.org/digital-library/a-three-year-study-of-the-gdpr-and-the-consumer

Prince, P. B., & Lovesum, S. P. J. (2020). Privacy Enforced Access Control Model for Secured Data Handling in Cloud-Based Pervasive Health Care System. *SN Computer Science, 1(5),* 239. https://doi.org/10.1007/s42979-020-00246-4

Protection of personal data | EUR-Lex. Noudettu 25.9.2024. https://eur-lex.europa.eu/EN/legal-content/summary/protection-of-personal-data.html

Rababah, K. (2011). Customer Relationship Management (CRM) Processesfrom Theory to Practice: The Pre-implementation Plan ofCRM System. *International Journal of E-Education, e-Business, e-Management and e-Learning.* https://doi.org/10.7763/IJEEEE.2011.V1.4

Rehman, K. U. U., Ahmad, U., & Mahmood, S. (2018). A Comparative Analysis of Traditional and Cloud Data Warehouse. VAWKUM Transactions on Computer Sciences, 15(1), 34. https://doi.org/10.21015/vtcs.v15i1.487

Salesforce.com. Salesforce. Noudettu 14.11.2024. https://www.salesforce.com/eu/

Sanodia, G. (2019). CRM AND CYBERSECURITY: PROTECTING CUSTOMER DATA IN A DIGITAL WORLD, ENSURING COMPLIANCE AND DATA PRIVACY. https://www.researchgate.net/publication/383943917_CRM_AND_CYBERSECURITY_PROTECTING_CUSTOMER_DATA_IN_A_DIGITAL_WORLD_ENSURING_COMPLIANCE_AND_DATA_PRIVACY

Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2018). An Analysis of Economic Impact on IoT Industry under GDPR. *Mobile Information Systems, 2018*(1), 6792028. https://doi.org/10.1155/2018/6792028

Sevilla, G. (2023). Noudettu 16.11.2024. Study: One-third of US companies cover up cyber breaches and ransomware. *EMARKETER*. https://www.emarketer.com/content/study-one-third-of-us-companies-cover-up-cyber-breaches-ransomware

Shaqrah, A. (2016). Cloud CRM: State-of-the-Art and Security Challenges. *International Journal of Advanced Computer Science and Applications*, *7*(4). https://doi.org/10.14569/IJACSA.2016.070405

Shen, L. (2014). The Nist Cybersecurity Framework: Overview and Potential Impacts. *Scitech Lawyer*, *10*(4), 16–19. https://www.proquest.com/trade-journals/nist-cybersecurity-framework-overview-potential/docview/1639830271/se-2.

Souri, A., Asghari, P., & Rezaei, R. (2017). Software as a service based CRM providers in the cloud computing: Challenges and technical issues. *Journal of Service Science Research*, *9*(2), 219–237. https://doi.org/10.1007/s12927-017-0011-5

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*, *10*(7), 190903. https://doi.org/10.1155/2014/190903

Tietosuojavaltuutetun toimisto. Rekisteröidyn oikeudet. Tietosuojavaltuutetun toimisto. Noudettu 26.9.2024. https://tietosuoja.fi/rekisteroidyn-oikeudet

Tietosuojavaltuutetun toimisto. *Yritystä koskevat sitovat säännöt*. Tietosuojavaltuutetun toimisto. Noudettu 2.10.2024. https://tietosuoja.fi/yritysta-koskevat-sitovat-saannot

Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011). Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, *22*(5), 847–859. Scopus. https://doi.org/10.1109/TPDS.2010.183

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access*, *8*, 131723–131740. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3009876

Yleinen tietosuoja-asetus (GDPR). (2016). Your Europe. Noudettu 25.9.2024. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm