SOTE-TIETOJÄRJESTELMÄT PILVIPALVELUINA

Soveltamisohje

AKUSTI

Alueiden ja kuntien sosiaali- ja terveydenhuollon tietohallinto-yhteistyöfoorumi

Kirjoittajat: Akusti-foorumi

ISBN 978-952-293-835-0 (pdf)

Kuntaliitto
Toinen linja 14, 00530 Helsinki
PL 200, 00101 Helsinki
Puhelin 09 7711
www.kuntaliitto.fi

Sisällysluettelo

1 Tausta

1.1 Johdanto

Sosiaali- ja terveydenhuollon palveluilla ja tietojärjestelmillä on kriittinen rooli yhteiskunnan tukiverkossa. Toisaalta sote-sektorilla on kasvava tarve palvelutuotannon tehostamiseen ja tietojärjestelmille on ladattu tässä kehityksessä isoja odotuksia. Tavoitteiden saavuttaminen vaatii pysymistä teknologisessa kehityksessä muiden toimialojen mukana. Tässä kehityksessä pilvipalveluiden rooli on merkittävä.

Sote-sektoria tehostavia ICT-ratkaisuja on hyvin erityyppisiä. Niistä kasvava osa on kansainvälisille markkinoille ja kansainvälisten vaatimusten mukaisesti toteutettuja valmisohjelmistoja tai SaaS-palveluita. Ohjelmistokehityksen ja palvelujen tuottamisen tehokkuudesta johtuen, ratkaisut ovat usein pilvipohjaisia. Pilvipalveluilla onkin merkittävä ja kasvava rooli palvelutuotannon tehostamisessa.

Pilvisiirtymän tuomien muutosten, mahdollisuuksien ja riskien arviointi on haastavaa muutoksen ja tarpeiden moniulotteisuuden vuoksi. Erityisesti sote-sektorille sovitettua ohjeistusta pilvipalveluiden käytöstä ei ole ollut tarjolla.

Samaan aikaan koko EU:n tasolla luottamuksellisen tiedon käsittelyn sääntely on kehittymässä, sekä yleisen tietosuoja-asetuksen GDPR pohjautuvan Schrems II -päätöksen (ks. 4.2) vaikutusten, että yleensäkin *EU:n pilvisuvereniteettiin* (ks. 5.3.1) liittyvien kysymysten vuoksi. Ei ole siis ihme, jos pilvipalveluihin liittyvät asiat eivät ole selkeitä yksittäiselle sote-toimijalle Suomessa, kun ne eivät ole olleet yksiselitteisiä kansallisesti tai EU-tasolla viime vuosina. Sote-toimijoiden keskuudessa onkin ollut epätietoisuutta siitä, millaisen pilvipalveluiden hyödyntämisen nykyinen sääntely todellisuudessa mahdollistaa. Tulkinnat ovat vaihdelleet eri toimijoiden ja viranomaisten välillä ja harkinnan jälkeen eri organisaatiot ovatkin päätyneet hyvinkin erilaisiin linjauksiin.

1.2 Soveltamisohjeen tarkoitus

Soveltamisohjeen yksinkysymykset ovat, miten pilvisiirtymä vaikuttaa sote-kenttään, miten sosiaali- ja terveydenhuollon asiakastietoa käsittelevien palveluiden toteuttaminen pilvessä eroaa perinteisemmistä toteutusmalleista ja miten nämä asiat on huomioitava?

Pyrkimys on keskittyä sote-tietojärjestelmien pilvisiirtymän ajankohtaisiin erityiskysymyksiin, hyviin käytäntöihin sekä haasteisiin organisaation pilvisiirtymän alkuvaiheissa.

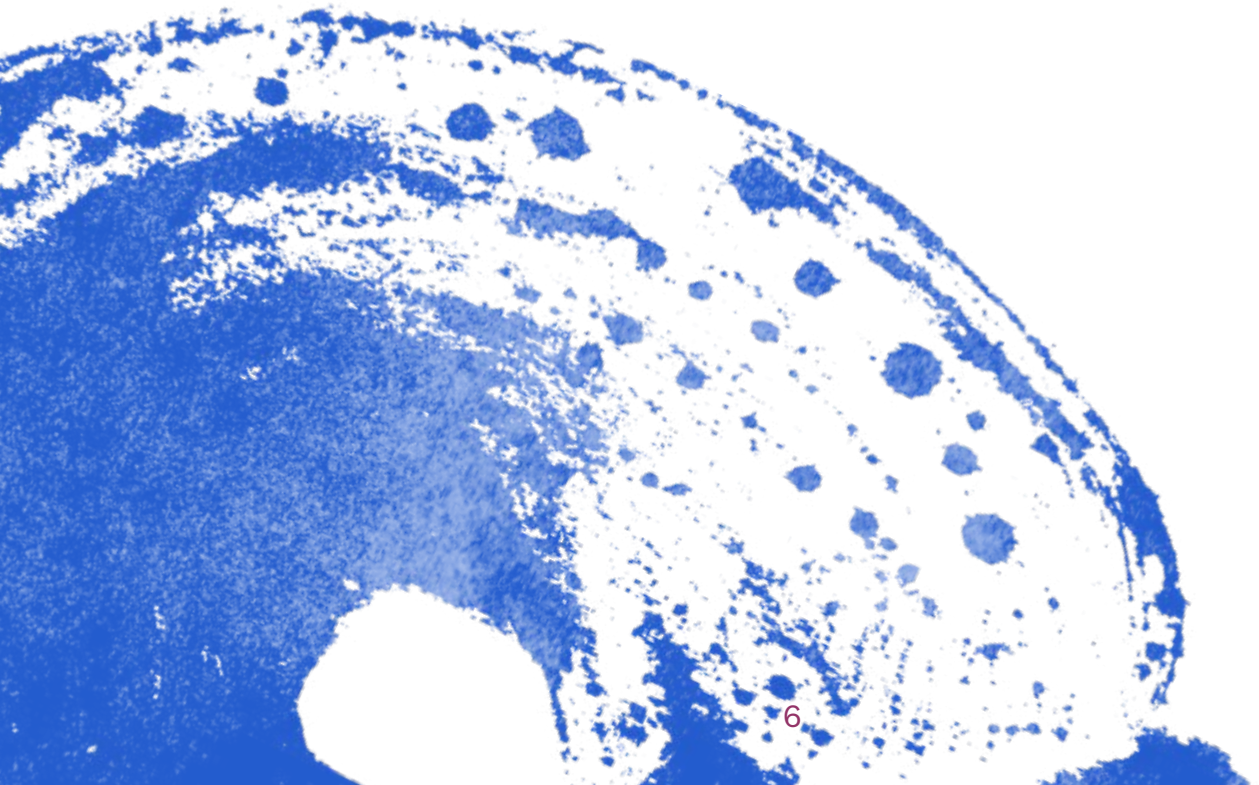
Soveltamisohje on suunnattu organisaatioiden pilvilinjauksista päättäville, tiedonhallinnan ja -käsittelyn asiantuntijoille, pilvipalveluiden ja teknologian hankinnasta vastaaville sekä organisaatioiden sidosryhmien, kuten ratkaisujen ja pilvipalvelualustojen toimittajien, kanssa tehtävän yhteistyön tueksi. Ohjeen avulla saa läpileikkauksen pilvipalveluiden käyttöön liittyvistä kysymyksistä sote-näkökulmasta.

Ohje ei pyri eikä pysty antamaan kaikkiin kysymyksiin kyllä/ei ratkaisua johtuen organisaatioiden ja ratkaisujen erilaisista ympäristötekijöistä, kuten tavoitteista, tarpeista, nykypalveluista, teknologiavalinnoista, sijainnista, osaamisen tasosta sekä kumppaneista. Pilvipalvelut ovat osa organisaation kokonaisratkaisua ja ei ole olemassa ”yhdenkoon” ratkaisua pilvipalveluidenkaan osalta. Soveltamisohje ei pyri olemaan kaikenkattava ohjeistus pilviteknologioista, tietoturvasta tai varautumisesta

erityisesti, näistä aiheista löytyy syvempää tietoa muista lähteistä. Näistäkin aiheista oppaasta saa vähintään hyvän yleiskuvan.

Soveltamisohje perustuu kirjalliseen lähdemateriaaliin, haastatteluihin ja laajaan pyöreänpöydänkeskusteluun. Lisäksi asiantuntijoilla on ollut mahdollisuus käydä läpi ohjeen luonnosta ja antaa siitä palautetta. Mukana on ollut merkittävä määrä sote-kenttää, ministeriöiden ja muiden viranomaistahojen, sekä teknologiantoimittajien edustajia. Suuret kiitokset kaikille teille korvaamattomasta yhteistyöstä ja ratkaisuhakuisuudesta soveltamisohjetta synnytettäessä!

Kiireisimpien lukijoiden kannattaa aloittaa lukeminen kappaleesta ”7 Yhteenveto”.



2 Nykytilanne, mahdollisuudet ja kehityssuunta

2.1 ICT on siirtymässä palveluna ostettavaksi

Yleinen trendi myös sote-sektorilla on jo pitkän aikaa ollut se, että merkittävä osa ICT-ratkaisuista siirtyvät palveluna ostettavaksi. Nämä palvelut tuotetaan yhä useammin jonkin muotoisesta pilvestä oman organisaation ja lähikonesalin ulkopuolelta. Uusilla teknologioilla toteutettavia ICT-palveluja saa enää rajoitetusti oman organisaation tai lähikonesalien alustoille.

Teknologiainvestoinnit kohdistuvat pilveen. Kansainvälisesti merkittävien toimijoiden kehityspanokset ovat keskittyneet jo yli kymmenen vuotta pilvialustoihin. Suomen sote-toimialan kehittymisen kannalta on olennaista hyödyntää näitä investointeja. Tämä saavutetaan näiden kehityspanostusten kanssa ”myötäkarvaan” tapahtuvalla kehityksellä. Tietohallintojohtajien viestin mukaan lähikonesaliin asennettavissa olevat ratkaisut vähenevät vuosi vuodelta, ja ne ovat usein jo jääneet vuosia kehityksessä jälkeen verrattuna vastaaviin pilvipalveluihin. Tutkimusten ja valtionvarainministeriön (VM):n arvioiden[1] mukaan Suomen julkishallinto ei ole pilven hyödyntämisen kärkimaita, vaan enemmänkin pilvisiirtymän alussa.

ICT:n kansainvälistymisen johdosta myös Suomessa tarjolla olevat sosiaali- ja terveydenhuollon ratkaisut ovat entistä enemmän suunniteltu kansainvälisten markkinoiden vaatimusten mukaan. Suomalaisia erityisvaatimuksia ei näissä ole kovin pitkälle mahdollista huomioida. EU-tasoisten vaatimusten, kuten GDPR:n ja lääkinnällisten laitteiden asetuksen (MDR), osalta tietoisuus on kansainvälisesti nykyään hyvällä tasolla. Kansalliset linjaukset ja laintulkinnat tuleekin olla hyvin linjassa EU:n yhteisen sääntelyn kanssa, jotta Suomen sote-järjestelmä saa moderneja ratkaisuja käyttöön.

ICT-arkkitehtuurin yleinen hajautuminen näkyy palveluiden siirtymisenä organisaatio seinien ulkopuolelle, sopimusosapuolien, integraatioiden, mobiililaitteiden, kotiin vietävien palveluiden sekä erilaisten sensoreiden lisääntymisenä. Perinteisesti isot tietojärjestelmätoimittajat ovat hallinneet ICT:tä, mutta viime vuosina on kehittynyt runsaasti pistemäisiä ratkaisuja eri erikoisaloille. Pilvipalvelut ovat merkittävä osa tätä pitkään jatkunutta trendiä.

Pilvipalveluiden käytön rajoittaminen aiheuttaa vaihtoehtokustannuksia. Yhä useammin uudet ratkaisut tuodaan tarjolle ainoastaan SaaS ratkaisuna pilvestä ja usein Suomen ulkopuolelta tuotettuina. Tähän ohjaavat pilviteknologioiden ja SaaS mallin edut ohjelmistojen tuottajille ja toimittajille. Pilvipalveluiden kategorinen linjaaminen pois ratkaisupaletista kansallisesti tai organisaatiokohtaisesti muodostaisi esteen uusien innovaatioiden käyttöönotolle. Vaihtoehtoiskustannus näkyy ICT-kustannusten kasvamisena sekä muita toimialoja hitaampana tehokkuuden kehittymisenä, mikä näkyy lopulta sosiaali- ja terveydenhuollon palveluiden laadussa ja vaikuttavuudessa. Tämän vuoksi on syytä suositella, että kategorisesti tällaisia sovellusaluetta koskevia rajauksia ei tehtäisi.

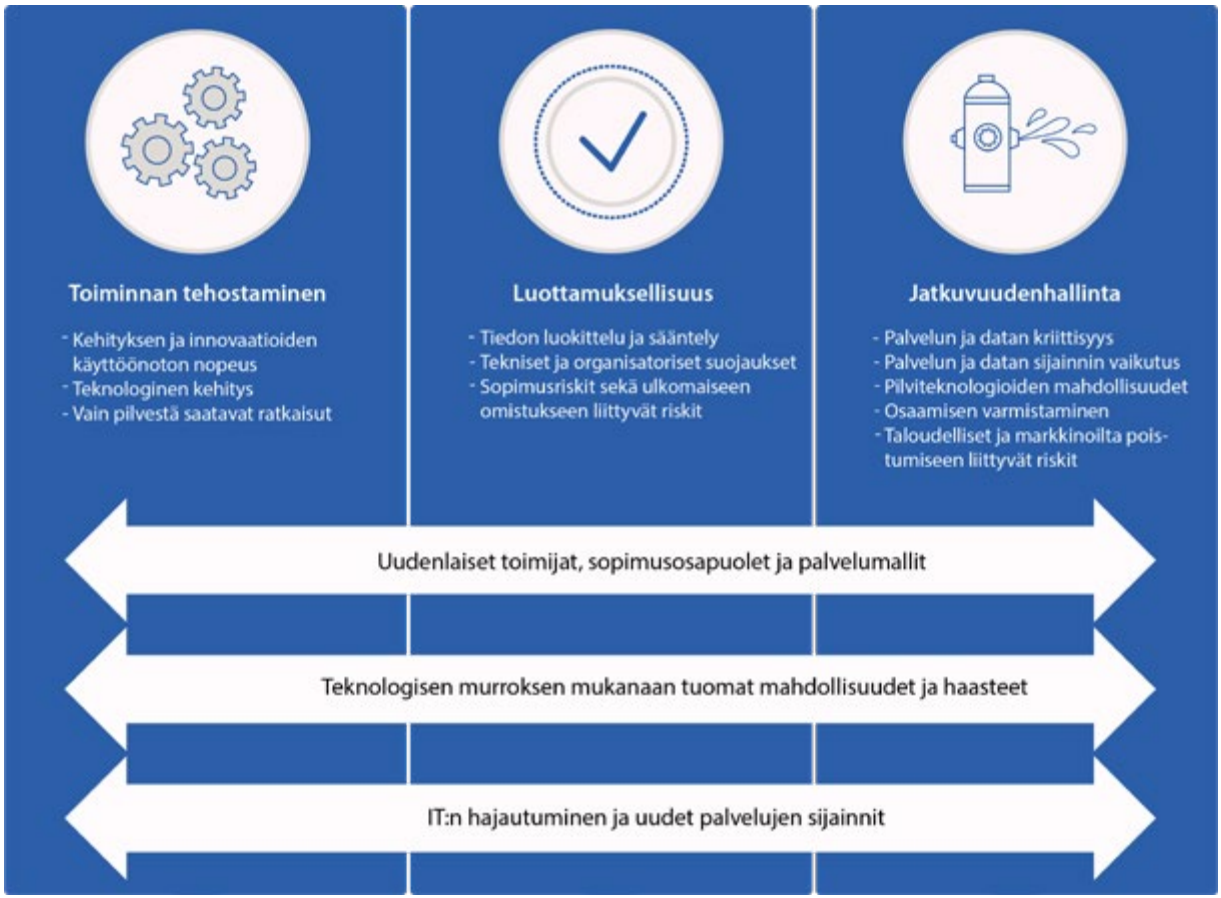
2.2 Pilvisiirtymä vaatii uutta osaamista

Sosiaali- ja terveydenhuollon pilvisiirtymässä ratkaisevaksi nousee tasapainoilu kolmen ylätason vaatimuksen ja niihin liittyvien riskien kanssa pilvipalveluissa:

1) ratkaisulla haettava **toiminnan tehostaminen**,
2) sote-toimialan erityispiirteisiin kuuluva **luottamuksellisuuden varmistus**,
3) sekä **jatkuvuudenhallinnan** erityistarpeiden huomiointi.

Näiden vaatimusten optimointi pilvipalvelua käyttöönotettaessa on haastavaa useiden yhtäaikaisten muutosten vuoksi:

1) mukaan tulevat uudenlaiset toimijat, sopimusosapuolet ja palvelumallit
2) teknologisen murroksen mukanaan tuomat mahdollisuudet ja haasteet
3) ICT:n hajautuminen ja uudet palvelujen sijainnit (= konesalit).



Kuva 1. Sotepalveluiden pilvisiirtymän keskeiset näkökulmat.

Muutosten hallinta vaatii monipuolista osaamista. Riskien arviointi ja vaatimuksenmukaisuuden todentaminen vaatii yhdistettyä osaamista teknologian-, sopimusten- ja jatkuvuudenhallinnasta. Pilvilinjauksen tekemiseen, sopimustenhallintaan, riskienarviointiin, palvelutuotantoon ja kokonaisarkkitehtuurityöhön on syytä kasvattaa pilviosaamista. Osaamisen kasvattaminen vaatii aikaa sekä panostuksia. Siksi on syytä huomata, että pilvistrategia ja siinä tehdyt valinnat vaikuttavat merkittävästi myös organisaation ja sen yhteistyökumppaneiden tulevaisuuden osaamisvaatimuksiin. Kaikkien asiaan törmäävien on syytä opetella pilven perusteet (ks. ”3.2 Ohjeita pilvistrategian työstöön”).

Palveluna ostettavat SaaS-ratkaisut poistavat tilaajalta suurelta osin perinteisen näkyvyyden sovellusten ”konepellin alle” teknisiin ratkaisuihin. Sen vuoksi niiden vaatimuksenmukaisuuden todentaminen perustuu valtaosin sopimuksiin, järjestelmäkuvauksiin, sertifiointeihin, riskiarviointeihin, tietoturvallisuuden arviointeihin sekä lopulta luottamuksella toimittajaan. Organisaatiot kokevat vaatimuksenmukaisuuden todentamisen sopimusten ja ratkaisunkuvausten perusteella usein haastavaksi. Paikoin tulkinnanvarainen ja ristiriitainen kansallinen sääntely on lisännyt vaikeuskerrointa. Tällaista osaamista ja yhdenmukaisia linjauksia tulee systemaattisesti kehittää, että SaaS-ratkaisujen etuja voidaan hyödyntää Suomen sote-kentällä.

2.3 Yleisesti käytettyjä sote-pilviratkaisuja

Alla olevat esimerkit Suomessa käytössä olevista sote-pilviratkaisuista antavat kuvaa, kuinka laajasti ja millaisia pilvipalveluita sote-sektorilla hyödynnetään. Luettelon ei ole kattava erityisesti kymmenien/satojen erikoisalakohtaisten järjestelmien osalta. Tässä kuvattuja esimerkkejä hyödynnetään myös myöhemmin tämän soveltamisohjeen jatkuvuuden skenaarioanalyysin- ja kriittisyysluokittelun esimerkeissä. Huomioi, että selvyyden vuoksi EU/ETA-alueelta tuotettavaksi kuvatut palvelut voivat kuitenkin sisältää esim. tukipalveluita, joita tuotetaan EU/ETA-alueen ulkopuolelta esim. valmistajan kotimaasta ja näin GDPR mukaista tietojen siirtämistä EU/ETA-alueen ulkopuolelle voi tapahtua.

SaaS palveluna tuotettavat **sähköposti, kalenteri ja tiimityön ratkaisut** ovat hyvin yleisesti käytössä, yleisimpänä Office 365, jota tuotetaan suurelta osin Microsoftin konesalista Suomesta. Myös **intranet** sekä **tiedostojen hallinta** ovat kasvavissa määrin osa pilvestä ostettavaa, hyperskaalautuvissa pilvialustoilla EU/ETA-alueelta tuotettavaa, SaaS kokonaisuutta. Microsoftin Teams on monille tuttu esimerkki SaaS palveluna tuotettava sovelluksesta, joka kehittyy jatkuvasti. Sen lähikonesaliin asennettava *Skype for Business* -vaihtoehto on käytännössä jäänyt viitisen vuotta jälkeen pilviversioista, eikä sitä enää kehitetä.

Pilvi data-alustat, mukaan lukien **tietoallas** (data lake) on lähes poikkeuksetta toteutettu EU/ETA-alueella sijaitseviin hyperskaalautuville pilvialustoille, vaikka myös yksittäisiä lähikonesaliin toteutettuja ratkaisuja on toteutettu. Hyperskaalautuvat pilvialustat ovat teknologian puolesta optimaalisia suurien data määrien käsittelyyn. Tietoaltaisiin viedään, niiden tarkoituksen mukaisesti, hyvin laajasti myös asiakastietoa sekä muuta henkilötietoa. Toisiokäyttöä tukevat **tutkijantyötilat** rakentuvat yleensä tietoaltaan yhteyteen samoja lähdejärjestelmän data integraatioita hyödyntäen. Samoin tietojohtamisen **tietovarastoja** (Enterprise Data Warehouse, EDW) rakennetaan tietoaltaan yhteyteen hyperskaalautuviin pilvipalveluina, ja tähän on ohjannut myös kansallinen *Virta*-referenssiarkkitehtuuri. Modernien tietovarastointiratkaisujen rakentaminen lähikonesaliin on poikkeuksellisen kallista ja haastavaa sovellusarkkitehtuurin sekä saatavilla olevien osaamisen vuoksi. Tietojohtamisen **raportointi ja analytiikka** (Business Intelligence, BI) ratkaisut ovat myös usein pilvipalveluna EU/ETA-alueelta. BI-työkalut, kuten Power BI, ovat jatkuvasti integroi-

tuneet tiiviimmäksi osaksi pilvipohjaisia toimistotyökaluja ja muita valmissovelluksia.

Erilaiset **laaturekisterit** ovat käytännössä pilvipalveluita luoteensakin puolesta. Samoin kansalliset rekisterit, kuten tartuntatautirekisteri on organisaatioiden näkökulmasta suomalainen pilvipalvelu.

Kanta-palvelut nousivat tätä soveltamisohjetta varten tehdyissä haastatteluissa esiin keskeisenä kansallisena pilvipalveluna. Palvelut tuotetaan Kelan toimesta heidän keskitetystä konesalistansa Suomessa. Jatkuvuuden kannalta Kanta-palveluiden rooli on jatkuvasti kasvanut operatiivisen käytön lisääntyessä. Haastatteluissa nostettiin riskinä esiin, että Kanta-palvelusta muotoutuu joltain osin operatiivinen pilvipalvelu, jota ilman APTJ-järjestelmä ei enää toimisi itsenäisesti potilaan kriittisessä hoidossa. Tällöin koko Suomen terveydenhuolto olisi riippuvainen yhdestä kotimaisesta pilvipalvelusta ja yhteyksistä sinne. Tämä muuttaisi kaikkien organisaatioiden jatkuvuudenhallinnan suunnittelun perusteita. Toisaalta nähtiin hyvänä, että toisissa riskiskenaarioissa Kanta toimii varajärjestelmänä yksittäisen APTJ-järjestelmän katkon aikana. Ks. riskiskenaarioanalyysien esimerkit kappaleessa ”6.3.7 Esimerkki skenaario 4: Kansalliset palvelut pois käytöstä”.

Hyvinvointialueen tasoista operatiivista tuotannonohjausta ja tilannekuvia suunnitellaan toteutettavan pilvipalveluna EU/ETA-alueelta. Varsinaiset yksiköiden operatiiviset tilannekuvat (esim. potilaslistat, osastokartta) tietohallintopäättäjät näkevät edelleen osana kriittistä APTJ:tä, joita ilman yksiköiden toiminta puuroutuisi melko nopeasti.

Organisaation toiminnanohjaus (ERP) – logistiikka-, taloushallinto- ja HR-järjestelmiä käytetään vaihtelevasti sekä Suomessa että muualla EU/ETA-alueella sijaitsevista pilvipalveluista. Näiden ratkaisujen uusimmat versiot ja sekä ominaisuudet kehitetään ainoastaan pilviratkaisuihin, lähikonesalin ratkaisujen jäädessä vuosi vuodelta jälkeen kehityksestä.

Kansallisiin todistuksiin ja lausuntoihin käytettävä **lomakepalvelut** ovat EU/ETA-alueelta tai Suomesta toteutettuja SaaS-ratkaisuja Kanta-liitynnällä.

Erilaisia **erikoisalakohtaisia järjestelmiä**, ts. suppeamman ammattilaisjoukon käytössä olevia ratkaisuja, tuotetaan pilvipalveluina Suomesta, EU/ETA-alueelta sekä mm. Yhdysvalloista. Tämä on iso heterogeeninen joukko SaaS-sovelluksia. Joissain tapauksissa vain osa järjestelmästä on pilvessä ja ydinosa lähikonesalissa.

Leikkaus- ja anestesiajärjestelmien ei-kriittisiä osia, kuten analysointi ja optimointialgoritmeja tuotetaan pilvipalveluista. Vastaavasti myös muita kliinistä tietoa koostavia, rakenteistavia ja operatiivista toimintaa optimoivia algoritmeja tuotetaan pilvestä.

Kansalaisille suunnatut palvelut ovat luontevia toteuttaa EU/ETA-alueelta tuotettuna pilvipalveluna, koska ne on voitava saavuttaa eri päätelaitteilla Internetistä. Usein asiakasdatasta säilytetään kuitenkin edelleen APTJ-järjestelmässä, josta palvelut sitä hyödyntävät ohjelmointirajapintojen (*API, Application Programming Interface*) kautta. Toisin sanoen kansalaisille suunnatut palvelut ovat pilvipalveluita, mutta data on siellä mistä APTJ-järjestelmäkin on tuotettu (eli lähikonesalissa tai pilvessä). Julkisen verkon palveluita ei siis tällöin tuoteta organisaation omasta ympäristöstä ja organisaation sisäisen tietoliikenneyhteyden yli, jolloin mm. DDoS (Distributed Denial-of-Service) -hyökkäyksiltä puolustautuminen on helpompaa. Kansalaisen palvelut tukeutuvat Suomi.fi-tunnistukseen, joka tuotetaan nykyisin EU/ETA-alueen pilvialustalta.

Kotiin toimitettavien palveluiden palvelualustat ovat usein pilviratkaisuja ja keräävät mm. sensoridataa ja hälytyksiä kotihoidosta. Toteutuksissa käytetään EU/

ETA-alueella sijaitsevaa hyperskaalautuvaa pilveä sekä kotimaisia pilvialustoja. Palvelualustojen kautta hallitaan myös kotihoidon hälytyksiä.

Hyvinvointilaitealustat, jotka koostavat asiakkaiden tuottamaa sensoridataa erilaisilta hyvinvointilaitteilta, sijaitsevat tyypillisesti EU/ETA-alueella, josta tieto siirretään organisaatioiden data-alustoilla hyödynnettäviksi.

Terveysportti on esimerkki Suomesta tuotetusta pilvipalvelusta, joka on keskeinen lääkäreiden (ja muiden kliinikoiden) paljon käyttämä tietolähde. **Laboratorion tutkimusohjekirja** voi myös olla joltain osin pilvipalvelu. Samoin **kliinisen päätöksentuen** ratkaisut tuotetaan organisaatioille usein Suomesta pilvipalveluna. Lääkärintyötä tehostava **puheentunnistus** voidaan tuottaa pilvipalveluista EU/ETA-alueelta tai Suomesta. Puheentunnistukseen ja muihin vastaavissa oppiviin algoritmeihin perustuvissa ratkaisuissa pilvestä tuotetun SaaS-palvelun merkittävä etu on opetusaineiston suuri määrä ja laadukkuus – ratkaisu kehittyy nopeasti.

Asiakastiedon hakukone ja aluekatseluratkaisut ovat työtä tehostavia APTJ:n operatiivisia tukijärjestelmiä. Näitä on toteutettu sekä EU/ETA-alueella sijaitsevista pilvipalveluista ja suomalaisista konesaleista.

Organisaatioiden **www-sivut** ovat yleensä pilvipalvelussa Suomesta tai muualla EU/ETA-alueella. Niitä myös käytetään EU/ETA-alueen ulkopuolelta. Hyperskaalautuva pilvipalvelu tuo toimintavarmuutta mm. purskeisen kuorman, palvelun vikasietoisuuden ja saatavuuden hallintaan. Nykyään yleisten palveluestohyökkäysten torjuminen on helpohkoa ja kustannustehokasta hyperskaalautuvilla pilvialustoilla, mutta pahimmillaan erittäin haastavaa lähikonesalissa. Jopa maailmanlaajuisen hajautuksen mahdollisuus kustannustehokkaasti tuo luotettavuutta eri tilanteisiin ja käyttötarpeisiin. Henkilökunnan **koulutus- ja perehdytysalustat** ovat myös usein pilvipalveluita.

Taloautomaatiojärjestelmiin (sähköinen kulunhallinta, hissit, jätekuilut, putkiposti, lääkekaapit, sisätilapaikannus, etävalvonta, lämmitys, ilmastointi, vesi) voi kuulua osia, kuten etämonitorointi ja -hallinta, jotka on tuotettu valmistajan pilvipalvelusta Suomesta tai EU/ETA-alueelta. Yleistymässä ovat ratkaisut, joissa kiinteistöön tuodaan vain paikallisen automaation mahdollistavat ohjausyksiköt ja koko ohjelmallinen hallinta tapahtuu pilvipalvelusta. Tällöin erityishuomiota kiinnitettävä siihen, miten hyvin ratkaisulla täytetään jatkuvuuden vaatimukset.

Julkisen terveydenhuollon päivystysvelvollisten organisaatioiden operatiivisen toiminnan kannalta kriittisistä järjestelmistä on toteutettu pääsääntöisesti Suomessa sijaitsevissa konesaleista (hosted-onprem, private cloud, onprem). Näitä järjestelmiä ovat ensisijaisesti ydintoiminnan (päivystys, leikkaustoiminta, tehohoito, synnytysosastot, ensihoito) keskeiset järjestelmät. Arkkitehtuurin ja hallittavuuden vuoksi tämä APTJ-kokonaisuus on yleensä erittäin laaja järjestelmäkokonaisuus (ks. ”6 Pilvi ja jatkuvuudenhallinta”). Huomioitavaa on, että jo nykyisin ”lähikonesali” voi olla jopa satojen kilometrien päässä esim. perusterveydenhuollon yksiköistä sekä maantieteellisesti laajalla alueella usean keskussairaalan mallilla toimivilla sairaanhoitopiireillä (kuten HUS).

Kansainvälisesti huomioitavaa on, että yleisiä APTJ-järjestelmiä (mm. Cerner, Epic) on jo käytössä sekä A) täysin hyperskaalautuvasta pilvestä toteutettuna järjestelmänä, että B) ratkaisuina, jossa primäärisesti lähikonesalissa olevan järjestelmän hyperskaalautuvassa pilvessä olevaa kopiota hyödynnetään varajärjestelmänä esim. lähikonesalin ongelmatilanteissa (high availability / disaster recovery)[2]. Cernerin ja hyperskaalautuvaa pilveä tarjoavan Oraclen yhdistyminen osaltaan vauhdittanee toiminnanohjausjärjestelmistä (ERP) tuttua kehityspolkua, missä näiden kehityspanostukset kohdistuvat ensisijaisesti järjestelmien pilviversioihin.

Erityisesti ensihoitopalveluissa käytettään turvallisuusverkon (**TUVE**) palveluita **Virve**, kenttäjohtamisen järjestelmä **Kejo** sekä hätäkeskustietojärjestelmä **Erica**. Nämä ovat turvallisuudesta vastaavien viranomaisten yhteiskäytössä ja niillä turvataan sujuva viranomaisyhteistyö ja tiedonvaihto kaikissa tilanteissa. Käyttäminen on lakivelvoitteista, ks. 4.2 Lainsäädäntö.

2.4 Tyypillisiä pilven hyötyjä

Mittakaavaetu (suuruuden ekonomia, economies of scale) tuo kustannussäästöjä mahdollistamalla investointien jakamisen suurelle asiakasjoukolle sekä erikoisosaajien tehokkaan hyödyntämisen. Mittakaavaetu mahdollistaa myös panostamisen automatisointiin, mikä laskee yksikkökustannuksia edelleen. Erikoisosaamisen tehokas käyttö sekä korkea automaatioaste mahdollistaa korkean laadun mm. vähentämällä inhimillisen virheen mahdollisuutta. Näin voidaan parantaa myös tietosuojaa ja -turvaa, kun teknologian keinoin nämä rakennetaan oletusarvoiseksi osaksi ratkaisua ja sen hallintaa. Energiatehokkuus syntyy myös mittakaavaeduista.

Skaalautumiskyky mahdollistaa kapasiteetin (palvelinten, tallennustila) nopean lisäämisen ja vähentämisen tarpeen muuttuessa ilman investointitarpeita. Lisäpalvelimien (= kapasiteetti) käyttöönotto voidaan automatisoida tapahtumaan tarpeen mukaan esim. vuorokaudenajan tai ruuhkahuippujen mukaan ja maksaa vain todellisesta käytöstä. Organisaation kiinteät ICT-kustannukset pienenevät ja teknisten alustapalveluiden laatu paranee, koska kyetään hyödyntämään *mittakaavaetua*. Käytännössä skaalautumiskyvyllä on suoraa vaikutusta sote-palveluiden saatavuuteen ja potilasturvallisuuteen erityisesti ruuhkahuippujen kohdalla.

Aina ajan tasalla olevat alustat ja sovellukset; PaaS- ja SaaS-ratkaisut pilvessä ovat yleensä aina päivitettynä viimeisimmillä tietoturva- ja ominaisuuspäivityksillä automaattisesti. Jatkuvat inkrementaaliset päivitykset vähentävät suurien migraatio- ja käyttöönottoprojektien tarvetta sekä tätä kautta näihin liittyviä operatiivisen toiminnan riskejä ja kankeutta. Tämä on yksi isoimmista pilvipalveluiden konkreettisista hyödyistä. Kymmenien tai satojen eri versioissa olevien eri lähikonesaleissa olevien asennusten tukeminen on toimittajille (ja asiakkaille) kallista verrattuna yhteen tai muutamaan keskitetysti ylläpidettävään aina ajantasaisen versioon ratkaisusta. **Useiden kymmenien hyvin iäkkäidenkin versioiden ylläpito samasta järjestelmästä on haaste myös kotimaisissa sote-tietojärjestelmissä ja vaikuttaa radikaalisti kehitysnopeuteen ja laatuun.** Tämän takia useat sote-järjestelmätoimittajat ja käyttäjäorganisaatiot, Suomessa sekä ulkomailla, näkevät tarpeen kehittää sote-ratkaisuja SaaS-palvelumallilla ja pilvestä tuotettaviksi. Usein tapahtuvien päivitysten vuoksi korostuu stabiilien rajapintojen (API) käyttäminen integraatioissa.

Nopeammat käyttöönotot ja ketterä toiminnan kehittäminen. Myös sote-organisaatioissa on konkreettisesti havaittu pilvipalveluiden käytön merkittävästi parantaneen kykyä ottaa käyttöön uusia ratkaisuja ja näiden mahdollistamia innovatiivisia palvelumalleja. SaaS ratkaisut mahdollistavat uusien ratkaisujen pilotoinnin ja käytön pienessä mittakaavassa vaivattomasti ennen laajempaa käyttöönottoa. Tällä on merkittävä vaikutus koko organisaation muutosnopeuteen sekä kokeilualttiuteen (ketteryys, muovautuvuus). Pilvipalveluiden tuoman ketteryyden hyödyt ovat konkretisoituneet myös COVID-19 pandemian aikana mm. data alustoilla tiedon jalostamisen sekä kokonaan uusien sovellusten toteuttamisen nopeutena. Toisaalta epidemian aikana on perinteisten tuotanto- ja palvelumallien kankeus konkretisoitunut uusien kiireellisten tarpeiden toteuttamisen haastavuutena, silloin kun ne ovat vaatineet pienenkin teknisen muutoksen APTJ:iin. Lähikonesaleista tuotettujen, eri toimittajien eri versioissa olevien, asiakaskohtaisten asennusten päivitykset ovat työläitä, virheherkkiä ja vievät paljon kalenteriaikaa. Virheiden todentaminen ja korjaus on vastaavasti myös usein hidasta.

Parempi tietoturva. Pilvipalvelun tuottajilla on tuottamaansa palveluun liittyen parempi kyvykkyys ja resurssit toteuttaa tietoturvaa, kuin palvelun käyttäjällä. Tietoturva on pilvipalveluntarjoajien kymmenienmiljardien eurojen liiketoiminnan kannalta täysin kriittistä ja heidän panostuksensa tietoturvaan ovat massiivisia, käytännössä siis mm. maineriskin vuoksi. Pilvialustoilla on mm. valmiita automatisoituja työkaluja tietoturvan varmistamiseen sekä riskien arvioimiseen alan parhaiden käytäntöjen mukaisesti. Palvelun käyttäjän näkökulmasta palvelun tietoturvaan liittyvä osaamistarve pienenee, mutta osaamisprofiili muuttuu laajemmaksi; aiemman lähikonesaliratkaisujen *lisäksi* täytyy hallita myös pilvikokonaisuus, nopeasti kehittyvineen uusine tekniikkoineen, osana tietoturvaa. Myös pilvipalvelun tietoturvan voi osaamattomuuttaan tai väärästä paikasta säästämällä yksittäinen työntekijä toteuttaa katastrofaalisen huonosti (ks. ”5.2.1 Hyvien tietoturvakäytäntöjen toteuttaminen pilvipalveluissa”), aivan kuten lähikonesalissakin toimittaessa. Pilvialustojen hyvien tietoturvakäytäntöjen automatisointia sekä rajattuja roolipohjaisia käyttöoikeuksia onkin ehdottomasti hyödynnettävä.

2.5 Pikaopas pilvipalveluihin

Pilviä ja pilvipalveluita on monenlaisia ja markkinointitermistöön on helppo eksyä. Geneerisesti *pilvestä* puhumisen sijasta on tärkeä tiedostaa ainakin pilven eri palvelu- ja toteutusmallit. Alla on tiiviisti kuvattu yleisimmät palvelumallit ja toteutusmallit sekä joitain keskeisiä termejä. Pilvipalveluiden tietoliikenneyhteyksiä käsitellään kohdassa ”5.2.2 Tiedonsiirron luottamuksellisuuden turvaaminen”.

Tämän osan voi huoletta ohittaa, jos nämä asiat ovat jo ennestään tuttuja.

2.5.1 Palvelumallit

Pilvipalvelumallien rinnalla on hyvä muistaa **perinteiset palvelumallit**, joita ovat:

1) **Oma konesali** (onprem) jolloin palvelu tuotetaan itse käyttäjäorganisaation omasta *lähikonesalista*, tyypillisesti toimijan omassa kiinteistössä sijaitseva palvelintilasta. Palvelintilaa syötetään mahdollisesti kiinteistön omalla varavoimalla ja se kytkeytyy fyysisesti kiinteistön paikallisverkkoon. Paikallisen toiminnan jatkuvuuden turvaamisen näkökulmasta ratkaisussa on paljon positiivista. Merkittävä riski sisältyy siihen, että ympäristön ylläpidon osaaminen ja resurssit voidaan turvata. *Konesaliin liittyvä oma osaamistarve* on suurin sekä joustavuus ja reagointimahdollisuudet pienimmät.

2) **Isännöity konesali** (hosted onprem); Palvelu tuotetaan organisaation *lähikonesalista*, mutta sen ylläpidosta vastaa ulkoinen palvelun tuottaja pääosin etäyhteyksiä hyödyntäen. Fyysisen ylläpidon jatkuvuuden varmistaminen voi olla erityisen haastavaa, sillä ulkopuolisten toimijoiden 24x7 pääsyä huoltotoimia suorittamaan ei usein haluta sallia kuin saatettuna. Käyttäjäorganisaation oma *konesaleihin liittyvä* osaamistarve on vähäisempi. Sopimusten rooli ja kumppanin valinnan tärkeys sekä näiden hallintaan liittyvän osaamisen tarve korostuvat. Hankaluutena on, ettei sopimuksessa pystytä kaikkia osapuolien vastuiden rajoilla olevia hallinnan yksityiskohtia yleensä määrittelemään tarkasti etukäteen, jolloin näitä tulkitaan haasteiden ilmetessä. Teknisesti skaalautuminen on rajattua ja kehitykseen yleensä yhä hidasta reagoida pilvipalveluihin verrattuna. Julkisilla sote-toimijoilla *isännöity konesali* on yleinen palvelumalli. Perinteisissä palvelumalleissa palvelinkapasiteettia täytyy yleensä aina mitoittaa (hankkia) korkeimman kuormitushuipun mukaisesti.

Pilvipalvialustojen palvelumallit luokitellaan yleisesti seuraaviin pääkategorioihin: **IaaS** (Infrastructure as a Service) on yksinkertaistettuna palvelinten ja muun teknisen infrastruktuurin ostamista pilvialustalta lähikonesalin sijasta. **PaaS** (Platform as a Service) on käyttövalmiiden alustaratkaisujen kuten tietokanta- ja sovellusalustojen ostamista pilvipalveluna. Tällöin perinteistä palvelinten ylläpitovastuuta siirtyy merkittävästi itseltä pilvialustan tuottajalle, sovelluksen ylläpidon ollessa yhä tilaajaorganisaation vastuulla. **SaaS** (Software as a Service) -mallissa koko ratkaisu ostetaan palveluna ja pilvipalveluntarjoaja vastaa ratkaisun tuottamisesta ja ylläpidosta. Palvelun käyttäjältä poistuu palvelun tuottamiseen ja ylläpitämiseen liittyvä osaamistarve. **BPaaS** (Business Process as a Service) mallissa koko liiketoimintaprosessi, kuten palkanlaskentatoiminta sisältäen sitä tukevat järjestelmät ostetaan (pilvessä tuotettuna) palveluna. Myös toiminnan kannalta kriittisiä prosesseja järjestelmineen voidaan ostaa palveluna, esim. diagnostiikkapalvelut.

Osa palveluista ei istu näihin mainittuihin kategorioihin; pilvipalvelut ovat kehittyneet ja kasvaneet ulos perinteisistä peruskategorioista (IaaS / PaaS / Saas). Muitakin ”aaS”-termejä markkinointikoneistot keksivät tasaiseen tahtiin. Nämä usein hyvinkin mielikuvitukselliset termit korostavat ICT:n yleistä muutosta palveluna ostettaviksi. Organisaatioiden ja yritysten pilvilinjauksissa trendinä on pyrkiä hyödyntämään korkeimman mahdollisen jalostusasteen palveluita (esim. SaaS), milloin tämä vain tämä on mahdollista ja järkevää. Näin organisaatio voi itse keskittyä tehokkaammin ydintoimintansa kehittämiseen.

2.5.2 Pilven tuotantomalleja

Julkinen pilvi (public cloud) tarkoittaa pilvipalvelua, joka on *julkisesti tarjolla kenen tahansa hankittavaksi*. Palvelut ovat tyypillisesti erittäin pitkälle tuotteistettuja ja kustannustehokkaita. Palvelun käyttäjän neuvotteluasema tarjoajaan nähden on pieni. Sopimukset ovat usein EU/ETA alueelle pitkälti standardoituja, joltain osin neuvoteltavissa riittävän isoilla asiakkailla. Julkiset pilvet ovat yleensä hyperskaalautuvia pilvipalveluita. Julkisen pilven tietoturva voi olla yksityistä pilveä paremmalla tasolla *mittakaavaetujen* vuoksi. Julkinen pilvi -termi ei tarkoita, että siellä toteutetut palvelut ovat oletuksena jotenkin julkisempia kuin muilla tuotantomalleilla toteutetut palvelut. Yleensä myös mielletään, että julkipilvipalvelut ovat aina julkisessa Internetissä, mutta näin asia ei ole.

Yksityinen pilvi (private cloud), tarkoittaa palvelua, joka tuotetaan vain palvelua käyttävälle organisaatiolle. Käyttäjän neuvotteluasema vaihtelee, mutta on parhaimmillaan suuri. Palveluhyöty ja -takuu, sekä käyttösopimukset ovatkin tyypillisesti neuvoteltavissa. Vakioinnin taso on toisaalta pienempi kuin julkisessa pilvessä, mikä voi näkyä kustannuksissa. Yksityisessä pilvessä palveluntarjonta on myös huomattavan rajattua verrattuna julkiseen pilveen.

Hybridi pilvi (hybrid cloud) tarkoittaa kokonaisuutta, jossa yhdistetään oma lähikonesali sekä pilvialusta yhdeksi palvelukokonaisuudeksi, usein niin että myös lähikonesalin hallintaa tehdään pilvialustan työkaluilla. Tällöin voidaan esimerkiksi

a) käyttää omaa konesalia pilvipalvelualustalla toimivan järjestelmän jatkuvuuden varmistavana ympäristönä (DR, Disaster Recovery) tilanteessa, jossa ulkoiset yhteydet ovat katkenneet. Lähikonesalista käytettävä varajärjestelmä on usein rajoitettu palvelutasoltaan ja ominaisuuksiltaan.
b) käyttää pilvipalvelualustaa tukemaan vaiheittaista pilvisiirtymää integroimalla osa lähikonesalin järjestelmistä ylläpidollisesti yhtenäiseksi, pilvipalvelualustan kautta ylläpidettäväksi, kokonaisuudeksi. Näin toimitaan esim. silloin kun ei haluta tai voida siirtää joitain palveluita kokonaan pilvialustalle.
c) käyttää pilvipalvelualustaa oman konesalin ”jatkee-

na” mm. tilanteessa, jossa tarvitaan joustavasti lisää kapasiteettia tai luotettavuutta kahdentamalla palveluita pilvikonesalin ja lähikonesalin välillä.

Teknisesti hybridiratkaisuja, joilla pilvipalvelualustojen kyvykkyyksiä voidaan ottaa käyttöön esim. sote-organisaation lähikonesalissa, on hyvin erilaisia. Tässä muutamia esimerkkejä antamaan kuvaa tarjonnan monipuolisuudesta: 1) *AWS Outpost*, joka perustuu AWS:n toimittamaan laitteistoon ja ohjelmistoon, tavallaan AWS konesalin osa tuodaan lähikonesaliin. Tämä on vastaava laitteisto ja ohjelmisto, jota he käyttävät myös omassa pilvipalvelussaan ja Suomen *AWS Local Zone* tiettäväsi perustuukin Outpost-teknologiaan jonka ”isäntä” on Ruotsissa oleva täydenpalvelun AWS konesali (”*region*”). 2) Oracle *Cloud@Customer* avulla on mahdollista tuoda Oraclen pilven palvelut asiakkaan omaan tai kumppanin konesaliin. 3) *Azure Stack* avulla voidaan tuoda Azuren pilvipalvelun ohjelmistolla lähikonesaliin valikoiduilla laitteistoalustoilla. 4) *Azure Arc* taas mahdollistaa asiakkaan lähikonesalin omien palvelinten sekä konttialustojen, sekä niiden ohjelmistojen ylläpidon osana Azure pilvityökaluja. 5) *Google Cloud Anthos* on hieman vastaava, perustuen konttiteknologiaan. Se voidaan asentaa asiakkaan omille palvelimille. Nämä ratkaisut voivat vaatia toimiakseen lähes jatkuvan yhteyden pilveen. Ylläpito vaatii usein paljon erikoistumista omalta tai kumppaniorganisaatiolta. Usein ylläpito tapahtuu myös osittain pilvipalvelutarjoajan toimesta. Ratkaisut sisältävät usein vain osan pilvipalveluiden kyvykkyyksistä. Nämä ratkaisut onkin hyvä nähdä pilvipalvelualustojen mahdollisuuksia täydentäviä, ei korvaavina teknologioina.

Monipilvi (multi cloud) on toisenlainen hybridimuotoinen lähestyminen, joka mahdollistaa tietojen hajasijoittamisen usean eri yrityksen tarjoamien pilvialustojen välillä. Tämä voi olla hyödyllistä jatkuvuuden- sekä toimittajariskien hallinnan kannalta, mutta toisaalta lisää hallinnan monimutkaisuutta ja organisaation osaamistarvetta merkittävästi. Erityisesti yksittäisen pilvipalvelun hajauttaminen usealle pilvialustalle voi tarpeettomasti lisätä ratkaisun monimutkaisuutta vaikeuttaen mm. ongelmien selvittelyä ja näin syöden nopeasti hajautuksen tuomia hyötyjä. Pilvitaipaleen alussa ja pienemmissä organisaatioissa kannattaa harkita oman pilviosaamisen kehittämisen kohdentamista valitulle pilvipalvelualustalle. Kun pilvitaipaleella ollaan ottamassa askelta pitemmälle esim. uuden kokonaisen pilvistrategian teeman (ks. 3.1 Pilvistrategian teemat) mukaan tulon myötä, on syytä pysähtyä miettimään useammalle pilvipalvelualustalle hajauttamisen hyötyjä. Monipilveä käytetään myös korkeaa käytettävyyden ratkaisuna, jossa pilvessä olevasta järjestelmästä on hätävarana passiivinen kopio ja/tai datan varmuuskopiot toisen toimittajan pilvessä ongelmatilanteiden varalta.

Hyperskaalautuvat pilvipalvelut termillä halutaan korostaa merkittävää eroa muun tyyppisiin pilvipalveluihin. Nämä suuryritysten pilvipalvelut ovat Suomesta ja muualta EU/ETA-alueelta tarjottavia massiivisia ja usein julkisia pilvialustoja. Hyperskaalautuvia pilvipalveluita tarjoavat mm. Amazon AWS, Microsoft Azure, Google Cloud Platform (GCP) sekä Oracle Cloud Infrastructure (OCI). Yrityksistä useimmat ovat tuomassa tai ovat jo

tuoneet palveluitaan tarjolle myös Suomessa sijaitsevista konesaleista (ks. ”7 Käsitteistöä”). Täysin eurooppalaista tai suomalaista kilpailukykyistä hyperskaalautuvaa palvelua ei käytännössä ole, isoin eurooppalainen toimija on ranskalaislähtöinen *OVHcloud*. Hyperskaalautuvuuden ansiosta palvelut pystyvät tukemaan purskeista (hetkellisesti korkeaa) sekä valtavan suurta kapasiteettitarvetta kustannustehokkaasti. Asiakkaan henkilöstö voi ottaa ylläpitotyökalujen avulla itsepalveluna käyttöön käytännössä rajoittamattoman määrän uusia palvelimia (laskentakapasiteettia), levytilaa (levykapasiteettia) sekä erilaisia PaaS/SaaS palveluita. Palveluiden kapasiteetti voidaan myös asettaa skaalautumaan automaattisesti kuormituksen kasvaessa / pienentyessä (dynamic scaling, auto scaling). Kapasiteetin muutoksia voidaan myös ajastaa esim. minimoida jotkin kapasiteetit yön ajaksi.

Reunalaskenta (edge computing) on nouseva teema ja tarkoittaa tavallisesti pilvessä toteutettavan ratkaisun tai alustan tuomista osittain lähemmäksi käyttäjää, joko lähikonesaliin tai päätelaitteille. Näin saatetaan haluta tehdä esim. tiukkojen tietototurva-, jatkuvuus- tai latenssivaatimusten vuoksi. Tätä on yleensä tuettava sovellusten arkkitehtuurissa, johon vaikuttaminen valmistuotetta hankittaessa on rajattua. Reunalaskenta näyttää yleistyvän ja yhdessä 5G-verkkojen kanssa tuo uusia ratkaisuskenaarioita myös sote-kentän tarpeisiin.

2.5.3 Muita tärkeitä termejä

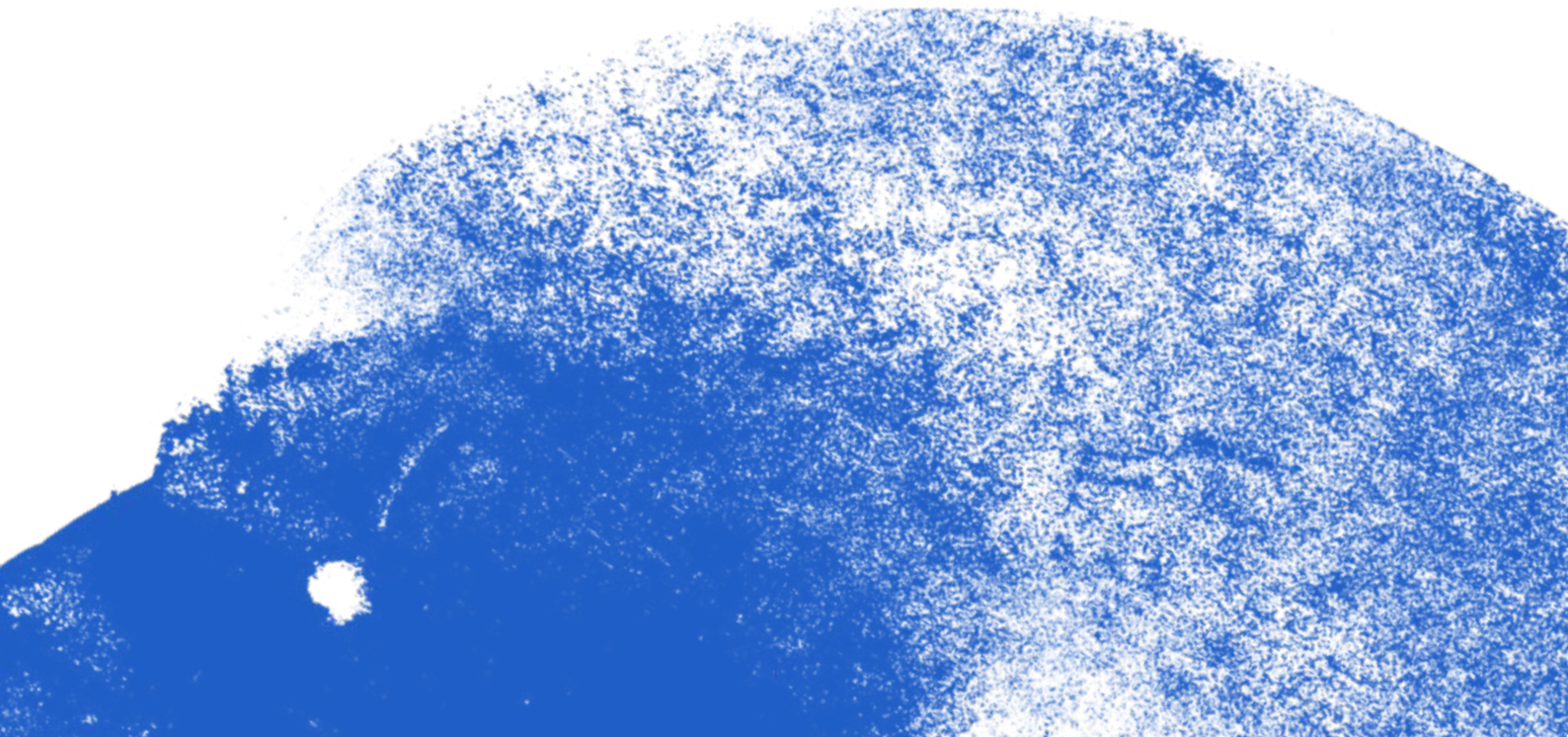
Pilvinatiivi (cloud native); Kun sovellus suunnitellaan alusta asti tehokkaasti hyödyntäen pilvipalvelualustan kyvykkyyksiä ja palveluita, sanotaan sen olevan pilvinatiivi. Kyvykkyyksiä ovat pilvialustalla tarjolla olevat erilaiset **serverless** (”palvelimeton”) -teknologiat, valvonta- ja automaatiotyökalut, pilvitietokannat, viestinvälitys- ja integraatioratkaisut, jne. Tavoitteena on tehostaa sovelluskehitystä hyödyntämällä pilven kyvykkyyksiä ja palveluita maksimaalisesti. Näiden avulla sama ominaisuus saadaan toteutettua parhaillaan muutamilla kymmenillä koodirivillä yhdessä päivässä, kun ns. ”pitkästä tavarasta” toteuttamalla työhön kuluisi esim. tuhatkertainen työmäärä. Pilvinatiivi tuotekehitys muuttaa myös organisaatiota ketterämmäksi; uusiin tarpeisiin reagointi on nopeampaa, kun aikaa ei mene niin paljon yleistarpeiden ratkaisuun.

Pilvinatiivi termiä käytetään joskus kuvaamaan myös ratkaisuja, jotka on alusta asti suunniteltu toimimaan useiden eri valmistajien pilvissä mm. konttialustoja (containers) ja standardeja teknologioita hyödyntäen. Tällöin voitaisiin puhua myös tältä osin **pilvi agnostisesta** ratkaisusta. Pelkkä konttiteknologian käyttö ei kuitenkaan varmista ratkaisun siirrettävyyttä alustojen välillä.

Cloud lock-in (vrt. vendor lock-in eli toimittajalukko) syntyy, kun pilvinatiivi sovellus toimii vain tietyllä pilvialustalla, tai organisaation prosessit integroituvat tiukasti käyttämään tietyn pilvialustan hallinta-, automatisointi- ja valvontatyökaluja. Tällöin sovelluksia ei ole joko teknisistä tai kaupallisista syistä käytännössä mahdollista siirtää toiselle pilvialustalle tai tuoda lähikonesaliin ilman merkittävää uudelleentoteutusta. Yleensä taustalla on harkitut tekniset ja kaupalliset valinnat hyödyntää ratkaisussa pilvipalveluiden *korkean jalostusasteen valmiskomponentteja (ks. pilvinatiivi)*. Cloud lock-in ei siis sinällään ole hyvä tai huono asia, mutta täytyy olla tiedostettu valinta palveluita ostettaessa ja asia on syytä käsitellä ratkaisunkuvauksissa. Tiettyyn hyperskaalautuvaan pilvialustaan panostaminen ja ”lukittautuminen” on usein strateginen valinta, jolla pyritään tukemaan ja ohjaamaan toimittajia käyttämään samoja pilviteknologioita. Näin voidaan luoda kehitysekosysteemiä organisaation omalle alustalle ja täten vähentää riippuvuutta yhdestä sovellustoimittajasta. Tällöin syntyy riippuvuutta tiettyyn pilvitoimittajaan. Riippuvuutta voidaan vähentää käyttämällä mahdollisuuksien mukaan standardeja teknologioita, kuten tavanomaisia lähikonesalissakin käytettäviä virtuaalikoneita, konttialustoja, tietokantoja, jne. Tällöin tosin yleensä menetetään paljon pilvipalvelualus-

tan mahdollisuuksista (ks. *pilvinatiivi*), eikä tätä lähestymistä siis ole syytä käyttää kategorisena lähestymisenä pilvipalveluihin. Aivan kuin muidenkin palveluiden elinkaaren suunnittelussa, on pilvipalveluidenkin osalta aika ajoin hyvä huomioida, että mitä pilvipalvelualustasta luopuminen tarkoittaisi (ns. exit plan). Erityisesti data lähtöisissä ratkaisuissa voi olla merkitystä, että yleensä tiedon siirtäminen pilvipalvelualustalle (”ingress”) ei maksa erikseen, mutta pilvestä poispäin (”egress”) tapahtuva tietoliikenne maksaa. Tämä voi aiheuttaa merkittäviä kustannuksia, jos vuosien varrella pilvipalvelualustalle on kertynyt massiivisia tietomääriä (petatavu kokoluokassa) ja nämä kaikki halutaan jostain syystä siirtää kerralla muualle.

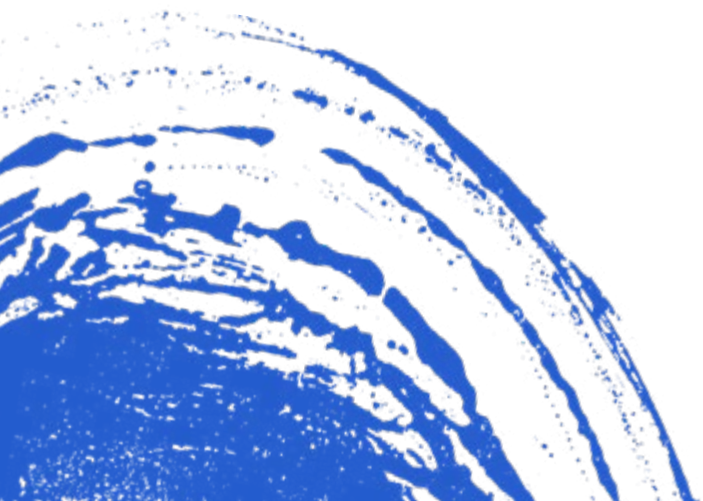
Infrastruktuurin määrittely koodilla (Infrastructure as a Code, IaC tai IaC-automaatio) tarkoittaa kapasiteetin (palvelimet, tallennustila) sekä tietoverkkojen (kuten IP-osoitteet, virtuaaliverkot, palomuurit) määrittämistä ohjelmakoodilla. Ohjelmakoodi on käytännössä tietynmallinen tekstitiedosto, jossa kerrotaan mitä palveluita pilvialustalle luodaan ja miten ne linkittyvät toisiinsa. Sovellusta asennettaessa tai muokattaessa koodi suoritetaan pilvialustalla osana asennuspakettia. Infrasta on siis tullut osa varsinaista ohjelmistoratkaisua ja sen määrittelystä osa ohjelmistokehitystä. Uudelle kehittäjäsukupolvelle palvelin onkin käytännössä rivi koodissa, ja fyysistä palvelinta he eivät ole nähneet. IaC-automaatio vähentää inhimillisen virheen mahdollisuutta konfiguroinnissa. Sovellusympäristöjä voidaan luoda lyhytaikaiseen tarpeeseen esim. testausta varten. Pilvialustoilla tulee aina hyödyntää mahdollisimman pitkälle IaC-automaatiota alusta alkaen. Kannattaa myös harkita, pilvipalvelualustojen omien tehokkaiden automatisointityökalujen lisäksi, myös useilla eri pilvialustoilla toimivia IaC-ratkaisujen käyttöä (esim. Terraform), jolloin samaa osaamista voidaan hyödyntää eri pilvipalvelualustoilla.



3 Pilvistrategia

Pilvipalvelut ovat megatrendi, joka tulee vain kiihtymään. Pilvipalveluiden yleistyminen on kokonaisvaltainen muutos sote-ICT:lle, mikä vaikuttaa myös ihmisten työskentelytapoihin. Pilvipalveluiden näkökulma onkin huomioitava organisaation ICT-strategiassa. Pilvistrategiassa kuvataan tärkeimmät linjaukset pilvipalveluiden hyödyntämisestä. Se on osa organisaation ICT-strategiaa ja kokonaisarkkitehtuurityötä, tuoden siihen pilvipalveluiden erityisnäkökulman. *Pilvistrategian* sijasta usein puhutaan myös *pilvilinjauksista*, käytännössä kyse on samasta tarpeesta.

Pitkän ajan kuluessa opitut tavat eivät muutu eikä uusi osaaminen rakennu hetkessä. Muutosta täytyy lähestyä määrätietoisesti ja hyväksyä että sen läpivientiin kuluu sote-sektorilla todennäköisesti mieluummin vuosia kuin kuukausia. Pilvitaipaleen edetessä pilviteknologioiden erikoisosaamisen tarve kasvaa. Nämä osaajat ovat kysyttyjä Suomessa ja maailmalla, mikä tuo lisähaasteetta. Organisaation onkin tärkeä miettiä pilvistrategiassaan mitä avainosaamista ja kyvykkyyksiä kasvatetaan itselleen ja mitä ulkoistetaan. Myös yhteistyö erityisosaamisen osalta esim. muiden hyvinvointialueiden kanssa on järkevää.



3.1 Pilvistrategian teemat

Pilvistrategia on työn selkeyttämiseksi hyvä jakaa tarvealueittain esim. seuraaviin osastrategioihin eli teemoihin:

1) Pilvivalmissovellukset
2) Pilvikonesalipalvelut
3) Data-alusta pilvessä

Muita teemoja voi tarpeen mukaan olla esim. ”Pilvisovelluskehitys”. Nämä pilvipalveluiden osa-alueet ovat erilaisia luonteeltaan ja kunkin teeman työstäminen vaatii erilaista osaamista. Kullekin teemalle koostetaan nykytila sekä tavoitetila mm. tavoitteiden, teknologiastrategian, tietoturvan, kumppaneiden ja oman osaamisen kehittämisen osalta. Teemoja voi soveltaa ja linjausten ei tarvitse olla yksityiskohtaisia. Oleellista on, että hyväksytty ja kommunikoitava pilvistrategiaa on olemassa, sitä on yhdessä työstetty ja siihen voidaan tukeutua sisäisesti ja kumppaneille kommunikoitaessa sekä tiekarttoja ja toimenpidesuunnitelmia tehdessä.

3.1.1 Pilvivalmissovellukset-teema

Teemassa käsittää linjauksia sovelluksille, jotka hankitaan SaaS pilvipalveluina. Lähes kaikilla sote-organisaatioilla on lähikonesalin ulkopuolella jo kymmeniä ratkaisuja eri pilvialustoilla ja sijainneissa. Tämä teema onkin enimmäkseen pilvinäkökulma organisaation sovellusportfolion hallintaan. Teeman isoin linjaus voi olla esimerkiksi, että kaikissa valmisohjelmistoissa suositaan aina kun mahdollista pilvestä ostettavia SaaS ratkaisuja.

Teemassa kuvataan minimivaatimukset (kriteerit) jotka pilvipalveluiden on erityisesti toteutettava. Lähtökohtana käytetään tässä dokumentissa mainittuja kansallisia

kriteeristöjä, joita sovelletaan organisaation tarpeisiin. Erona lähikonesalin palveluihin, merkittävä osa vaatimuksenmukaisuuden varmistamisesta SaaS palveluissa tapahtuu sopimuksellisesti sekä ratkaisusta ja toimittajasta tehdyn riskiarvioiden avulla. Ratkaisukuvaus ja tietoturvakuvaus kuvaavat mm. luottamuksellisuuden toteutumista. Hallintamalli kuvaa ylläpitokäytännöt, käyttöoikeuksien hallinnan, datan käsittelyn käytännöt sekä elinkaarenhallinnan palvelun käyttöä päätettäessä.

Ratkaisujen riskiarvioinnissa listataan pilvipalveluiden osalta erityishuomioitavat asiat, kattaen koko palveluiden elinkaaren hankinnasta aina palvelun lopettamiseen. Suositeltavaa on integroida nämä kontrollit samaan kokonaisuuteen muun tyyppisten palveluiden ja ratkaisujen riskiarviointikriteeristön kanssa. Ei siis ole suositeltavaa luoda pilvipalveluille omia erillisiä prosesseja.

Teknisesti SaaS-valmissovellukset usein toimivat tietyllä pilvipalvelualustalla, jonka toimittaja on valinnut osana tuotekehitystään. Käytännössä organisaatiolla tulee siis olemaan valmissovelluksia useilla eri pilvialustoilla, eikä organisaatiolla yleensä ole teknistä pääsyä valmissovelluksen käyttämälle hyperskaalautuvalle pilvialustalle.

3.1.2 Pilvikonesalipalvelut-teema

Pilvikonesalipalvelut korvaavat sekä täydennetään lähikonesalin palveluita tai toimivat lähikonesalin palveluiden jatkeena (hyperskaalautuvassa) pilvessä. Strategiassa kuvataan tarvelähtöisesti millä perusteilla palveluita (palvelimia ja dataa) pilveen siirretään, sekä toisaalta millä periaatteilla jätetään lähikonesaliin. Tyypillisiä valintaperusteita ovat kustannusten optimointi, infrastruktuurin modernisoinnin tarve (valmiita alustoja hyödyntäen), parempi ylläpidettävyys, vikasietoisuus kasvattaminen, joustavampi skaalautuvuus sekä nopeampi kehittäminen. Priorisointi pohjautuu organisaation tarpeisiin ja nykyisiin sopimuksiin. Jatkuvuudenhallinta on tärkeä mielessä pidettävä asia. Teeman mukaisia pilvipalveluita ostetaan usein IaaS-palveluina, esim. virtuaalikoneina. Näihin ”pilviperuspalveluihin” eri hyperskaalautuvan pilven tarjoajilla on kaikilla hyvä tarjoama.

Osana teeman käytännönläheistä työstöä voidaan haarukoida ne järjestelmät, joille tehdään nosta-ja-siirrä (lift-and-shift) muutto pilvialustalle esimerkiksi nopeiden voittojen saamiseksi. Myös pilvialustan PaaS palveluiden käyttöä mm. tietokanta-alustojen sekä sovelluspalvelinten osalta on hyvä pohtia. Teeman linjauksien yhteydessä mietitään myös pilvihajautuksen (monipilvi lähestyminen) hyötyjä ja haittoja; halutaanko palveluita ostaa myös joltain toiselta toimittajalta kuin esim. pilvi data-alusta, vai onko keskittäminen organisaation valinta? Päätöksiä tehdään tarvelähtöisesti pilvipolun edetessä.

3.1.3 Pilvi data-alusta-teema

Moderni data-alusta tyypillisesti koostuu tietoaltaasta (data lake), data integraatioista, tietovarastoista (EDW, DW, data mart), raportoinnista (BI), tutkimuksen (tutkijan työtilat) sekä koneoppimisen (ML/AI, jne.) ratkaisuista. Data-alustoilla hyödynnetään hyvin laajasti ja monipuolisesti pilvipalvelualustojen kehittyneitä kyvykkyyksiä. Vaikka data-alusta tuotetaan lähes poikkeuksetta nykyisin hyperskaalautuvasta pilvestä, voi organisaation pilvistrategia päätyä pitämään data-alustan ydin lähikonesalissa.

Data-alusta ovat olleet organisaatioissa yleinen isomman kokoluokan ensikosketus pilvialustalle toteutettaviin räätälöityihin ratkaisuihin ja pilvikehitykseen. Samalle pilvialustalle, samojen dataintegraatioiden varaan usein päädytään kehittämään myös operatiivisia sovelluksia samoja data integraatioita hyödyntäen, jolloin linkitys muiden strategian teemojen kanssa on huomioitava tai mahdollisesti eroteltava kokonaisuus omaksi Pilvisovelluskehitys-teemaksi. Tässä yhteydessä *DevOps*-toimintatapojen ja työkalujen käyttöönotto on yleensä iso muutos perin-

teiseen toimintaan verrattuna.

Data-alustan rakentaminen ja ylläpito on monimutkainen kokonaisuus ja iso investointi. Alueilla onkin päädytty myös yhteistyöhön alustan tai sen osien suunnittelussa ja toteutuksessa myös sairaanhoitopiirien (hyvinvointialueiden, yms.) välillä. Teemassa teknologiastrategia, organisaation oman osaamisen kehittäminen sekä kumppanistrategia ovat keskiössä.

3.2 Ohjeita pilvistrategian työstöön

Strategiatyön apuna voi hyödyntää tämän soveltamisohjeen lisäksi mm. Valtionvarainministeriön ohjeita ja linjauksia pilvipalveluista, jotka ovat tiiviitä paketteja pilvipalveluiden hyödyntämisestä. Tuottavuutta pilvipalveluilla[3] (2020) sekä laajempi Pilvipalveluiden soveltamisohje[4] (2020) jatkavat vuonna 2019 julkaistun Julkisen hallinnon pilvipalvelulinjaukset[5] (2019) -ohjeen perustalta. Pilvipalveluiden Soveltamisohjeen liitteestä löytyy mallipohja strategiadokumentille. Pilvipalvelualustojen tarjoajien kokemusta kannattaa hyödyntää.

Hyperskaalautuvien alustojen laajemman käyttöönoton yhteydessä kannattaa hyödyntää hyviä käytäntöjä, joita on kuvattuna toimittajien vapaasti saatavilla olevissa materiaaleissa, esim. Azuren[6], Googlen[7], Oraclen[8] sekä AWS:n[9] *Cloud Adoption Framework* -materiaalit. Strategian luominen ja jalkauttaminen vaatii osaamista laajasti organisaatiossa. Pilviosaamisen kasvattamisessa on syytä hyödyntää pilvipalveluntarjoajien laadukkaita ja ilmaisia koulutusmateriaaleja, esim. Azuren[10], Googlen[11], AWS:n[12] sekä Oraclen[13] ”Fundamentals/Basics”-tason itseopiskelu materiaalit. Tällaiset perustason koulutukset sopivat kaikille pilviasioista kiinnostuneille itseopiskeluun, ei siis ainoastaan ICT-väelle. Oman organisaation sekä kumppanien osaamisen todentamisessa suositellaan käytettävän sertifiointeja, ne viestivät kumppanin sitoutumisesta ko. pilvialustaan liittyvän osaamisen kehittämiseen.

4 Sote-pilvipalveluiden sääntely

Sote-pilvipalveluille sääntelyn asettamat vaatimukset eivät eroa muualla tavoin toteutettujen sote ICT-järjestelmien ylätason vaatimuksista.

Lainsäädännössä ei oteta erityisesti kantaan puoleen tai toiseen pilvipalveluiden hyödyntämiseen asiakastietojen käsittelyssä. Pilvipalveluiden käytön sääntely perustuu samoihin lakeihin ja asetuksiin, kuin muissakin konesaleissa ja palvelumalleilla tapahtuvan asiakas- ja henkilötiedon käsittely. Keskeiset asiat kaikissa palvelu- ja tuotantomalleissa ovat luottamuksellisuuden sekä jatkuvuuden varmistaminen.

Kuitenkin erilaisista palvelu- ja toteutusmalleista johtuen vaatimusten toteutumiseen pilvipalveluita käytettäessä tulee kiinnittää erityishuomioita. Mahdollisten uusien toimijoiden mukaantulo on huomioitava, verkkoratkaisun laajentuminen tehtävä turvallisesti, luottamuksellisuuden, jatkuvuuden sekä toipumisen eri näkökulmat huomioitava myös palvelun ja datan sijainnin näkökulmasta. Näistä on tarkemmin kappaleissa *”5 Luottamuksellisuuden varmistaminen pilvessä”* sekä *”6 Pilvi ja jatkuvuudenhallinta”*.

4.1 Asiakastietojen käsittely EU/ETA-alueella

Sosiaali- ja terveydenhuollon asiakastiedot ovat henkilötietoja. GDPR:n mukaisesti eurooppalaisten henkilötietojen käsittely ja säilyttämisen tulee tapahtua joko EU/ETA-alueella tai mikäli nämä tapahtuvat EU/ETA-alueen ulkopuolella, on kyseessä henkilötietojen siirto EU/ETA-alueen ulkopuolelle, ja tietosuojan ja tietoturvan riittävästä tasosta varmistuttava. **Sote-ratkaisuissa on aina suositeltavaa käyttää EU/ETA-alueella tuotettua pilveä, mikäli vain mahdollista.** Tällöin sopimusriskien hallinta on aina helpompaa (ks. 5.3 Pilvipalvelun sopimusriskien hallinta). Henkilötietojen siirto EU/ETA:n ulkopuolelle tarkoittaa myös tilanteita, joissa konesalit, joissa tiedot säilytetään, sijaitsevat EU/ETA-alueella, mutta niissä olevia henkilötietoja käsitellään alueen ulkopuolelta esim. etäyhteydellä.

Asiakastiedot eivät ole kansallisesti turvallisuusluokiteltua asiakirjoja, joita koskisi erityislainsäädäntöä mm. maantieteellistä käsittelystä Suomessa, ks. ”Tiedonhallintalaki” alempaa. Asiakastiedot ovat kuitenkin *terveydenhuollon ja sosiaalihuollon salassa pidettäviä tietoja*. Tietojen luottamuksellinen käsittely täytyy varmistaa myös pilvipalveluita käytettäessä, aivan kuin mitä muuta tahansa tekniikkaa käytettäessä.

4.2 Lainsäädäntö

Asiakastietolaki[14] (784/2021, Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä) sääntelee asiakastiedon käsittelyä ja **THL:n määräykset**[15] tarkentavat näitä.

- **5/2021: Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista**. Asiakastietojen käsittelyä pilvipalveluissa todetaan, että EU/ETA-tasoinen tietojen liikkuvuusperiaate mahdollistaa sen, että asiakastietoja voidaan käsitellä samantasoisilla suojatoimenpiteillä Suomessa ja EU/ETA-maissa (määräyksen liite 1, kappale 6.4). Jatkuvuussuunnittelua tehtäessä on huomioitava myös ”A3 Kriittiset”-luokitelluille järjestelmille asetetut erityiset varautumisen vaatimukset seuraavasti: *”Luokan A3 kriittisissä järjestelmissä järjestel-*

män jatkuva toimivuus tai viiveetön palauttaminen toimivaksi on oltava mahdollista nopeasti sellaisen poikkeavan tilanteen vallitessa, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle." (liite 3g, vaatimus AKYM16). Määräystä ei sovelleta tietojärjestelmiin, joiden käyttötarkoituksena ovat pelkästään Findatan antaman määräyksen 1/2020 mukaiset käyttökohteet (ks. alta).

- **4/2021 Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista.** Määräyksessä kuvataan periaatteet järjestelmien luokitteluun B, A1, A2, A3 sekä "A3 kriittiset" -luokkiin sekä korkean tai normaalin riskin järjestelmiin. Määräykset mm. laajentavat minimivaatimuksia järjestelmille, riskiarviointi sekä arviointilaitoksen tekemän tieturvallisuuden arvioinnin vaateita. Määräyksen liitteenä on tukimateriaalina riskiarviointityökalu tietojärjestelmille. Määräyksen kappaleessa 5 määritellään päivystyksen ja ensihoidon toteuttamisessa käytettäviä järjestelmiä koskemaan erityisiä varautumisen vaatimuksia: *"Kriittisiä luokan A3 järjestelmiä ovat ne luokan A3 tietojärjestelmät, joita käytetään erikoissairaanhoidossa tai kuntien tai hyvinvointialueiden sairaaloissa tai julkisen perusterveydenhuollon avosairaanhoidossa päivystysvastuun toteuttamisessa ja ensihoidossa taudinmääritykseen, sairauksien tutkimukseen ja hoitoon ja näihin liittyvien asiakastietojen hallintaan. Kriittisten järjestelmien joukkoa on mahdollista laajentaa myöhemmin."*
- **3/2021 "Tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset"**. Määräyksessä kuvataan palveluantajalta edellyttämän tietoturvasuunnitelman vaatimukset, sisältäen mm. kuinka palvelunantaja osaltaan varmistaa tietojärjestelmien vaatimustenmukaisuuden näiltä osin.

Toisiolaki[16] (552/2019, Laki sosiaali- ja terveystietojen toissijaisesta käytöstä) ja sitä tarkentavat Sosiaali- ja terveysalan tietolupaviranomaisen, eli **Findatan määräyksissä** säätelevät ja rajoittavat sote datan toisiokäyttöä. Findatan määräystä 1/2020 "Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista" on ollut haastavaa tulkita hyperskaalautuvien palveluiden hyödyntämisen osalta ja määräystä ollaankin uudistamassa. Luonnosten mukaan siinä tullaan paremmin ottamaan pilvialustat huomioon mm. paikan päällä konesaleissa tehtävistä tilojen turvallisuuden arvioinnin sekä viranomaisten tekemien henkilöstöturvallisuuden arvioinnin vaatimuksien väljentämisen myötä.

GDPR eli EU:n yleinen tietosuoja-asetuksen[17] (2016/679) sekä **Tietosuojalain**[18] (1050/2018), jolla säädetään GDPR:n mukaisesta kansallisesta liikkumavarasta, keskeisenä tavoitteena on taata henkilötietojen vapaa liikkuvuus Euroopan talousalueella. Henkilötietoja saa siirtää EU/ETA-alueen maihin samoin perustein kuin Suomen sisällä. Tietosuoja-asetus edellyttää, että tietojen käsittelyn tulee aina olla sallittu peruste[19] ja rekisterinpitäjän ja henkilötietojen käsittelijöiden (esim. pilvipalveluntarjoaja) välillä pitää olla sopimus henkilötietojen käsittelystä, **DPA** (Data Processing Agreement). Rekisterinpitäjän on myös arvioitava henkilötietojen käsittelyyn liittyviä riskejä aina ryhtyessään käsittelemään henkilötietoja[20], esim. uutta järjestelmäkokonaisuutta käyttöönotettaessa. Yksi työkalu riskien arviointiin on tietosuojan vaikutuksenarviointi[21] (**DPIA**, Data Protection Impact Assessment). DPIA tekeminen ei ole pakollista kaikissa tapauksissa, kun henkilötietoja käsitellään, mutta sitä voi aina hyödyntää edellä mainitun pakollisen riskien arvioinnin apuna. VAHTI hyvät käytännöt -tukimateriaaleissa on ohjeistusta DPIA:n tekemiseen (ks. alempaa).

Myös kun henkilötietojen säilytys tai käsittelyä tapahtuu osittainkin EU/ETA-alueen ulkopuolella, on tietosuojan ja tietoturvan riittävästä tasosta varmistuttava. Tällöin **edellytetään siirtoperustetta**, muiden edellä mainittujen vaatimusten noudattamisen lisäksi.[22] **Schrems II** -päätöksen[23] myötä poistui EU ja USA:n väliltä erityinen *Privacy Shield* menettely henkilötietojen siirrosta. Päätöksellä USA:n erityisasema siis päättyi (vastaavasti

Schrems I päätös poisti aiemman Safe Harbor menettelyn). Jatkossa aina kun EU:ssa olevaa henkilötietoa käsitellään EU/*ETA-maiden ulkopuolelta*, täytyy palveluntoimittajalla olla käytännössä siirtoperusteena olla käytössä uudet EU:n vakiolausekkeet (**SCC**, Standard Contractual Clauses)[24]. Lisäksi on pohdittava tapauskohtaisten lisäsuojamekanismien tarve. Tästä on tehtävä erillinen tiedonsiirtoja koskeva tapaus- ja maakohtainen riskiarviointi eli **TIA** (Transfer Impact Assessment)[25], eli arvioida mm. onko sopimuskumppanin mahdollista noudattaa vakiolausekkeita esim. kohdemaan lainsäädännön vuoksi. Tiedonsiirron riskiarvion tekeminen on rekisterinpitäjän velvollisuus. Varsinainen TIA-arvio ei siis ole osa toimittajan kanssa tehtävää sopimusta, mutta voi arvioinnin lopputuloksilla vaikuttaa tarvittaviin sopimusehtoihin sekä ratkaisun teknisiin ja organisaationaalisiin suojatoimiin.

Tietosuoja-asetuksen mukaisesti henkilötietojen käsittely EU/ETA-alueen sisällä ei siis eroa niiden käsittelystä Suomessa, mutta siirrettäessä tietoja EU/ETA-alueen *ulkopuolelle* vaaditaan lisävarmistuksia. GDPR myötä henkilötietojen käsittely EU/ETA-alueella on yksinkertaisempaa ja näin asetus ohjaa käsittelemään ja säilyttämään henkilötiedot lähtökohtaisesti EU/ETA alueella. Onkin vahvasti suositeltavaa mahdollisuuksien mukaan rajaamaan henkilötietojen tallennus ja käsittely tapahtumaan EU/ETA-alueella. Tällöin mahdollisiin tuleviinkin kansainvälisiin sopimusmuutoksiin on myös helpompi mukautua. Nämä vaatimukset ovat pilvipalveluita tarjoavilla kansainvälisillä suuryrityksillä yleensä tiedossa ja he tarjoavat omalta osaltaan tukea arviointien tekemiseen mm. DPA-sopimuspohjien, SCC-lausekkeiden sekä DPIA tekemistä tukevien sertifiointien ja muiden materiaalien muodossa.

Terveydenhuoltolaki (1326/2010[26]) sekä **sosiaalihuoltolaki** (1301/2014); jatkuvuudenhallintaan liittyen laeissa määriteltyjä vastuita ja velvollisuuksia valmiussuunnitelmien tekemisestä on yhdenmukaistettu 03/2021 voimaantulleella lakimuutoksella[27], jonka mukaan alueellista valmiussuunnittelua ohjaavat yliopistosairaalat. Valmiussuunnitelmien pohjana on kansalliseen ja alueelliset riskiarvioinnit, joihin eri hallinnon tasoilla tehtävät valmiussuunnitelmat perustuvat. Näihin riskiarvioihin myös tässä soveltamisohjeessa esimerkkeinä kuvatut jatkuvuuden riskiskenaariot pilvipalveluiden näkökulmasta pohjautuvat (ks. 6.3 Pilvipalvelut huomioiva riskiskenaarioanalyysi).

Potilaslaki[28] (1992/785, Laki potilaan asemasta ja oikeuksista) sääntelee mm. potilasasiakastietojen salassapitoa (13 §). Siellä todetaan, että potilasasiakirjoihin sisältyvät tiedot ovat salassapidettäviä. Lähtökohtaisesti niihin sisältyviä tietoja ei saa antaa sivullisten tietoon. Sivullisia ovat käytännössä kaikki hoitoon tai siihen liittyviin tehtäviin osallistumattomat henkilöt.

Julkisuuslaki[29] (621/1999, Laki viranomaisten toiminnan julkisuudesta) sisältää periaatteita asiakirjojen salassapidolle ja luovuttamiselle sekä tiedonsaantiin omista henkilötiedoista. Laki ei määrittele miten tietoa luokitellaan ja miten sitä käsitellään erilaisissa ympäristöissä ja/tai palveluissa.

Tiedonhallintalaki[30] (906/2019, Laki julkisen hallinnon tiedonhallinnasta) ja sitä tarkentavat asetukset[31] on laaja kokonaisuus. Se velvoittaa mm. kuvaamaan tiedonhallintamalliin tietojärjestelmät, tietovarannot ja mm. niiden riippuvuuksista muihin toimijoihin, esim. väestörekisteriin. Nämä kuvaukset ovat hyödyllisiä myös pilvipalveluiden jatkuvuuden analysoinnissa. Laki myös edellyttää muutosvaikutusten arviointia. Pilviratkaisuissa muutokset tapahtuvat yleensä nopealla sykkeellä ja siksi on suositeltavaa suunnitella palvelutuottajan kanssa, miten mahdollinen muutosvaikutusten arviointi toteutetaan. Tiedonhallintalaissa säädetään muun muassa tietoturvallisuustoimenpiteiden vähimmäistasosta, mutta jätetään tiedonhallintayksiköille riskiperusteista harkintavaltaa toimenpiteiden toteuttamiseksi. Tiedonhallintalaissa (18

§) määritellään myös turvallisuusluokiteltavat asiakirjat, joihin asiakastiedot eivät kuulu.

MDR[32] (2017/745, EU:n Lääkintälaiteasetus) sekä täydentävän kansallinen Lääkintälaitelaki[33] (laki lääkinnällisistä laitteista, 719/2021) mukaisesti lääkinnälliset laitteeksi luokitellut ohjelmistot tulee ilmoittaa Lääkealan turvallisuus- ja kehittämiskeskus Fimean rekisteriin[34]. MDR vaatimukset eivät ota kantaa pilviteknologioiden käyttöön ja MDR lääkintälaitteeksi luokiteltuja ohjelmistoja voidaan siis tuottaa myös pilvipalveluista. Huom: Vaikka asiakastietoa käsittelevä tietojärjestelmää ei olisi luokiteltu MDR mukaiseksi lääkintälaitteeksi, koskee sitä kuitenkin edellä mainitut THL:n määräyksien (Asiakastietolain) vaatimukset mm. tietoturvallisuuden arvioinnista, jotka ovat osittain vastaavia kuin MDR:n vaatimukset.

Arviointilaki[35] (1406/2011, Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista), tuleva Julkri -kriteeristö tulee tarkemmin ohjeistamaan tähän lakiin liittyvää tietoturvallisuuden arviointia.

Päivystysasetus[36] (583/2017, Valtioneuvoston asetus kiireellisen hoidon perusteista ja päivystyksen erikoisalakohtaisista edellytyksistä) määrittelee päivystyksen vaatimuksista, toimintaedellytyksistä ja laajuudesta, myös ns. laajan ympärivuorokautisen päivystyksen osalta. Asetuksen mukaan päivystystoiminnan suunnittelussa on otettava huomioon normaaliolojen häiriötilanteet ja päivystyksen ruuhkatilanteet sekä terveydenhuoltolain 38 §:ssä tarkoitettu alueellinen valmiussuunnitelma.

Ensihoitoasetus[37] (585/2017, Sosiaali- ja terveysministeriön asetus ensihoitopalvelusta) määrittelee mm. ensihoidon tavoittamisaikoja, käytännössä siis ensihoidon ”SLA-vaatimuksia”, jotka aiheuttavat vaatimuksia myös ensihoidon toteuttamisessa käytettäville järjestelmille.

Laki julkisen hallinnon turvallisuusverkkotoiminnasta[38] (2015/10) velvoittaa mm. ensihoitopalveluissa käyttämään turvallisuusverkkoa (**TUVE**) ja sen palveluita. Se on valtion omistuksessa ja hallinnassa oleva korkean varautumisen ja turvallisuuden vaatimukset täyttävä hallinnon turvallisuusverkko, jota tuottaa Suomen Erillisverkot Oy. Sote-toimijoilla onkin käytössä TUVE:ssa toimivia kansalliset korkean varautumisen viestintä- ja tietojärjestelmiä ja näihin liittyviä vastuita. Näitä järjestelmiä ovat viranomaisverkko **Virve**, kenttäjohtamisen järjestelmä **Kejo** sekä hätäkeskustietojärjestelmä **Erica**. Järjestelmiä käytetään erityisesti ensihoidossa, mutta myös sairaalan sisällä osana operatiivista toimintaa. Nämä ovat turvallisuudesta vastaavien viranomaisten yhteiskäytössä ja niillä turvataan sujuva viranomaisyhteistyö ja tiedonvaihto kaikissa tilanteissa.[39]

Valmiuslaki[40] (1552/2011) määrittelee mm. velvollisuuden etukäteisvalmisteluin varmistaa tehtävien mahdollisimman hyvä hoitaminen myös poikkeusoloissa.

4.3 Ohjeet, suositukset ja standardit

Nämä ohjeistukset eivät ole sitovia, vaan nimensä mukaisesti tarkoitettu organisaatioiden tekemän palveluiden arvioinnin ja kehittämisen tueksi. Standardien noudattaminen tuo selkänojaa palvelun laatua ja vaatimustenmukaisuutta arvioidessa.

1. **VM:n ohjeistukset ja linjaukset pilvipalveluiden käytöstä** suosittelevat pilvipalveluiden käyttämistä ensisijaisesti, mikäli ei ole erityistä syytä käyttää perinteisempiä muotoja palvelujen tuottamiseen. Turvallisuusluokittelematon tieto (mitä asiakastieto on) on mahdollista viedä pilveen, kunhan sen turvallisuudesta huolehditaan. **Tuottavuutta pilvipalveluilla**[41] (2020) sekä laajempi **Pilvipalveluiden soveltamisohje**[42] (2020). Ne jatkavat **Julkisen hallinnon pilvipalvelulinjaukset**[43] (2019) ohjeeseen tiivistetyn pilvipalvelulinjausten perustalta.

2. **(valmistelussa) Julkri** (Tiedonhallintalautakunta): Julkisen hallinnon digitaalisen turvallisuuden arviointikriteeristö on valmistelussa oleva, arviolta keväällä 2022 valmistuva kriteeristö. Tarkoituksena on tuottaa Pitukria ja Katakria laajempi ohjeistus mm. turvallisuusluokittelemattoman tiedon osalta, jota mm. sote-asiakastiedot siis ovat. Ohjeistus tuo kriteeristöä myös jatkuvuuden ja varautumisen näkökulmista osittain vanhentuneet VAHTI-ohjeistukset huomioiden. Julkri kriteeristössä ei ennakkotietojen mukaan tulla *erityisesti* huomioimaan sote-palveluiden käyttötapauksia, jolloin tällä ohjeella on jatkossakin rooli sote-sektorille sovitettuna soveltamisohjeena.
3. **Pitukri**[44]; Pilvipalveluiden turvallisuuden arviointikriteeristö on Kyberturvallisuuskeskuksen julkaisema ohjeistus. Pitukri ei ole suoraan velvoittava vaan ohjeluonteinen kriteeristö ja sitä kautta tuo tukea turvallisuus ja luottamuksellisuus asioiden huomioimiseen sekä arvioimiseen pilvipalveluiden osalta. Pitukri on toteutettu valtaosin turvalisuusluokiteltujen asiakirjojen näkökulmasta, jota sote-asiakastieto ei ole, eikä se ole siis kaikilta osin relevatti sote-tiedolle. Ohje on turvallisuusluokittelemattoman tiedon fyysisen sijainnin osalta ohjeistuksena tiukempi kuin THL:n määräykset ja VMn linjaukset. Sote erityispiirteitä ja -tarpeita ei ole erikseen käsitelty. Hyperskaalautuvan pilven toimittajat, esim. AWS[45], ovat arvioittaneet palvelujansa Pitukrin mukaisesti. Ks. myös Findata määräykset.
4. Katakri[46]; kansallisen turvallisuuden kriteeristö (2020) painottuu kansallisesti ja kansainvälisesti turvallisuusluokiteltujen asiakirjojen käsittelyyn ja hyvin paljon fyysiseen turvallisuuteen. Sote erityispiirteitä ja -tarpeita ei ole käsitelty. Jotkin hyperskaalautuvan pilven toimittajat ovat arvioittaneet palvelujansa Katakrin mukaisesti.
5. **VAHTI** (Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, DVV) julkaisee ”VAHTI hyvät käytännöt -tukimateriaaleja”[47] tietoturvaan ja tietosuojaan liittyen, mm. aiemmin mainittu tietosuojan vaikutuksen arvioinnin (DPIA) tukimateriaalit. Aiemmat ”VAHTI-ohjeet”[48] ovat jo osittain vanhentuneita, mutta edelleen huomion arvoisia ohjeita varautumisen sekä jatkuvuudenhallintaan liittyen, erityisesti lähikonesalissa. Julkri-työssä on tiedostettu tarve näiden ohjeiden päivittämiseen.
6. **Tiedonhallintalakiin liittyvät suositukset**.[49] ”Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalvelussa”[50] käsittelee pilvipalveluiden riskienhallintaa kattavasti ja täydentää aiempaa ”Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä”[51] *pilvinäkökulmasta. Valmisteilla on myös ”Suositus salassa pidettävän tiedon käsittelystä pilvipalveluissa*”. Nämä käsittelevät salassapidettäviä ja turvallisuusluokiteltuja *asiakirjoja*, eivätkä siis kata suoraan soten erityislainsäädännön mukaista salassa pidettävää asiakastietoa.
7. **ISO standardeista 27000, 27017, 27018, 27701 ja 9001.** määrittelevät tietoturvallista tietojenkäsittelyä myös pilvipalveluiden osalta. Standardit ovat hyödyksi varmistettaessa pilvitarjoajan palvelun laatua ja vaatimuksenmukaisuutta. Useilla toimittajilla ei kuitenkaan ole ISO tietoturvasertifiointia, niinpä näiden vaatiminen voi hankittaessa toimia tarkoituksettoman rajaavana. Lisätietoja yleisimpien kansainvälisten pilvipalveluiden standardinmukaisuudesta löytyy toimittajien Compliance-dokumentaatioista (Oracle[52], GCS[53], AWS[54] ja Azure[55])
8. **Tietosuoja-asetuksen 40 artiklan mukaiset käytännesäännöt**[56] (CoC, Code of Conduct); näiden noudattamista voidaan käyttää ns. pehmeän sääntelyn mukaisena osoituksena[57] GDPR:n noudattamisesta. Käytännesäännöt hyväksyvät Euroopan tietosuojaneuvosto[58] (European Data Protection Board, EDPB). Hyväksyttyjä käytännesääntöjä ovat EU Cloud Code of Conduct (SCOPE Europe)[59] sekä CISPE[60] (Cloud Infrastructure Services Providers in Europe). Pilvipalvelun tarjoajat, jotka ilmoittavat, että heidän palvelunsa noudattavat hyväksyttyjä käytännesääntöjä, voivat antaa asiakkailleen paremmat takeet siitä, että

palvelun suorittama käsittely on GDPR:n mukaista. Huomioitavaa on, että käytännesäännöt eivät välttämättä kata niihin sitoutuneiden pilvipalveluntarjoajien kaikkia palveluita, mikä voi rajoittaa niiden hyödyllisyyttä.

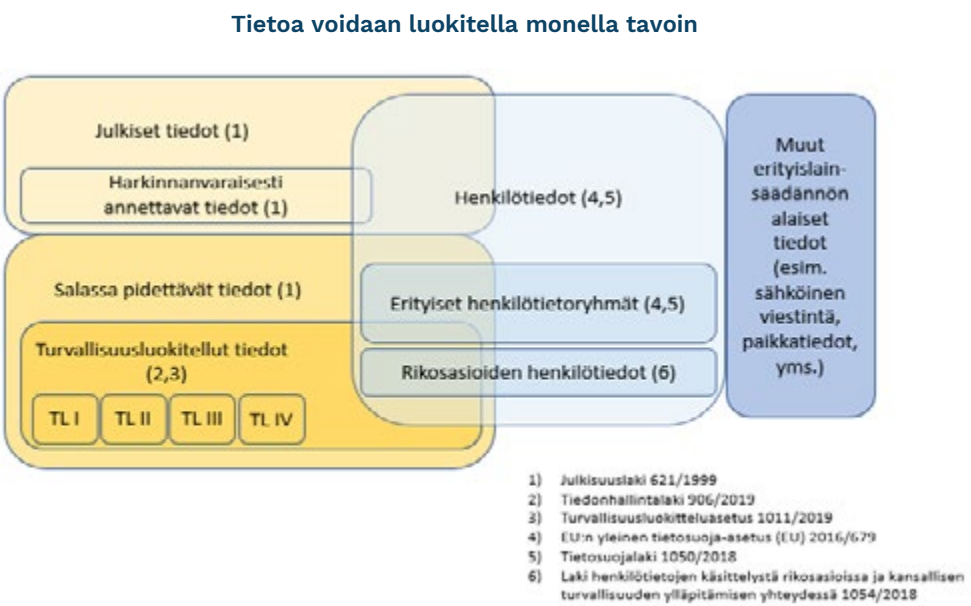
4.4 Sote-tiedon julkisuusluokat

Käsiteltävien tietojen luokittelun tunteminen on välttämätöntä, jotta niitä koskevaa sääntelyä voidaan tulkita. Pilvipalvelun tietosuoja- ja tietoturvakäytännöt täytyy suunnitella luottamuksellisimman siellä säilytettävän tiedon mukaisesti. Useimmissa pilvipalveluissa käsitellään asiakastietoa ja **pilvipalveluissa käsiteltävistä tietojoukoista kiinnostavin onkin sosiaali- ja terveydenhuollon asiakastiedot.** On myös kuitenkin pilviratkaisuja, joissa käsitellään kyllä *henkilötietoa*, mutta ei kuitenkaan *sote-asiakastietoa (esim. laskutusjärjestelmä, HR-järjestelmä sekä teknisten lokien hallinta on todennäköisesti tällaisia)*.

4.4.1 Julkiset, salassa pidettävät ja turvallisuusluokiteltavat tiedot

Julkista tietoa on kaikki tieto, joiden käsittelyyn ei liity erityissääntelyä salassapidosta tai luottamuksellisuudesta. Iso osa potilasohjeista, neuvonnasta ja yleisestä tiedottamisesta on julkista tietoa. Myös osa henkilötiedoista on julkista tietoa. Julkinen tieto ei tarkoita, että tieto on aina kaikkien nähtävillä, esim. osa julkisesta tiedosta on harkinnanvaraisesti annettavia tietoja. Tuttu esimerkki julkisista henkilötiedoista ja niiden näkyville saattamisesta on vuosittain julkaistavat henkilöiden tulotiedot.

Turvallisuusluokitellut tiedot; Turvallisuusluokiteltavan asiakirjan käsittelyä säädetään tiedonhallintalaissa sekä valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa. Turvallisuusluokkia on neljä. Pääosin vain valtionhallinnon viranomaiset voivat turvallisuusluokitella tietoja. Kansallinen turvallisuusviranomainen[61] (National Security Authority, NSA) ohjeis-



Kuva 2. Tietojen luokittelun eri näkökulmia. Lähde: DVV ”Suositus salassa pidettävän tiedon käsittelystä” (luonnos)

taa kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyssä. Sote-organisaatioillakin erityistehtävissä on käytössään turvallisuusluokiteltua tietoaineistoja esim. varautumisvelvoitteisiin liittyen. Niiden käsittely pilvipalveluissa täytyy suunnitella omana kokonaisuutena ks. ”Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalvelussa”[62]. Sote-*asiakastieto* ei siis ole turvallisuusluokiteltua tietoa. Luokitteluun liittyy myös ns. *kasaumavaikutus*, joka voi nostaa tiedon turvallisuusluokittelua, kun tiedon määrä tai yhdistettävien tietolähteiden määrä kasvaa.

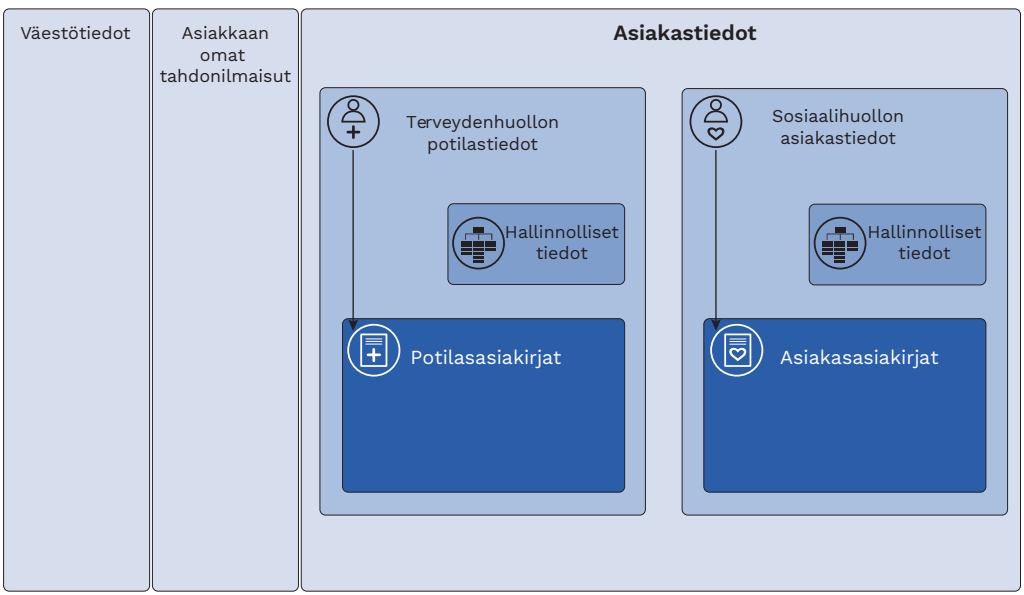
Sote-asiakastieto on suurelta osin asiakastietolain mukaisia **erityisiä henkilötietoryhmiin** kuuluvaa ja **sosiaali- ja terveydenhuollon salassa pidettävää asiakastietoa** ja sitä koskee aivan erityistä sääntelyä. Erityiset henkilötietoryhmät ovat rotu, poliittinen mielipide, uskonnollinen vakaumus, ammattiliiton jäsenyys, *terveyttä koskevat tiedot*, geneettinen- tai biometrinentieto. Näiden käsittelyyn liittyy erityisiä sääntelyä käsittelyn perusteisiin liittyen, mutta ei kuitenkaan erityistä sääntelyä tietojen käsittelyyn pilvipalveluissa.

4.4.2 Henkilötiedot

Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa mm. nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella. Henkilötiedon käsittelyä sääntelee erityisesti tietosuoja-asetus (GDPR) ja sitä täydentävä tietosuojalaki. Esimerkkejä sotessa käsiteltävistä henkilötiedoista ovat:

- väestötiedot (nimi, osoite, jne.)
- terveyden- ja sosiaalihuollon asiakastiedot
- asiakkaan omat tahdonilmaisut
- henkilökunnan henkilötiedot (henkilöstöhallinto, HR).

Salassa pidettävät henkilötiedot. Asiakastiedot ovat terveyden ja sosiaalihuollon salassa pidettäviä henkilötietoja. Niiden salassapidosta on säädetty laissa potilaan asemasta ja oikeuksista. Työntekijöiden tiedot ovat pääsääntöisesti luottamuksellista henkilötietoa (GDPR).



Kuva 3. Sosiaali- ja terveydenhuollon henkilötiedon luokittelua.

4.4.3 Asiakastiedot

Asiakastieto pitää sisällään terveydenhuollon potilastiedot sekä sosiaalihuollon asiakastiedot. Asiakastieto on luottamuksellista ja sitä säätelee Asiakastietolaki.

Terveydenhuollon potilastiedot ovat asiakastietoa ja pitävät sisällään **potilasasiakirjat**, kuten potilaskertomus, lääkitys ja laboratoriotulokset sekä **hallinnolliset potilastiedot** tiedot kuten ajanvaraukset ja lähetteet. Lisäksi luokittelussa huomioitavaa on **erityissuojatut potilasasiakirjat** (perinnöllisyys ja psykiatria), jotka ovat potilasasiakirjojen erityistapauksia ja joiden *käsittelyyn* liittyy erityisiä rajauksia. Nämä rajaukset tulee toteuttaa samalla tavalla pilvessä tai lähikonesalista tuotetuissa sovelluksissa, niinpä tällä on vain vähän merkitystä tämän ohjeistuksen avainkysymysten kannalta.

Sosiaalihuollon asiakastiedot pitävät sisällään **sosiaalihuollon asiakirjat**, kuten päätökset ja hakemukset sekä **sosiaalihuollon hallinnolliset tiedot** kuten ajanvaraukset.

Asiakkaan omat tahdonilmaisut ovat henkilötietoja, mutta eivät ole asiakastietoja. Ne pitävät sisällään hoitotahdon, erilaiset informoinnit sekä tiedon luovutuskiellot.

4.4.4 Erityisesti huomioitavia tietoluokkia

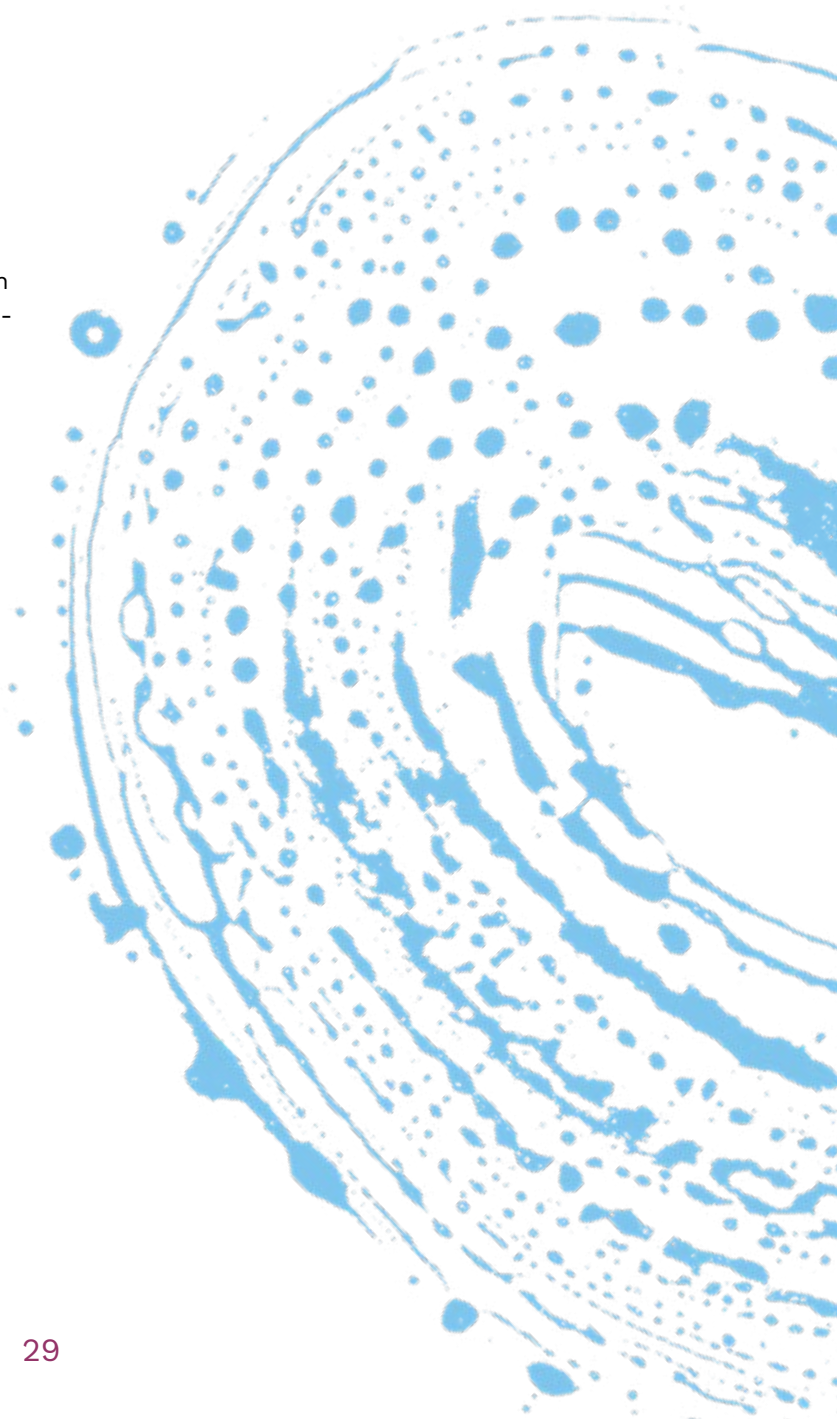
Pseudonymisoitu henkilötieto; pilvipalveluissa käsitellään ja säilytetään laajasti pseudonymisoitua ja anonymisoitua tietoa, esim. tietojohtamisessa sekä tutkimustoiminnassa. Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja. Tällaiset lisätiedot täytyy säilyttää huolellisesti erillään henkilötiedoista. Vaikka tiedot olisivat pseudonymisoitu, niiden avulla yksilö voidaan edelleen erottaa joukosta ja usein myös yhdistää eri tietoaineistoissa. Kun samalla avaimella pseudonymisoidaan iso määrä asiakas- ja henkilötietoa, riski asiakkaan ei toivottuun yksilöitymiseen vuoksi kasvaa. Pseudonymisoidut henkilötiedot ovat yhä henkilötietoja, ja niiden käsittelyssä on sovellettava tähän liittyviä säännöksiä. Vastaavasti pseudonymisoitu *asiakastieto* on edelleen *asiakastietoa*. Lisätietoa Tietosuoja.fi -sivustolta.[63] Pseudonymisoinnin systemaattinen toteuttaminen järjestelmään on tehokas tapa toteuttaa tietosuoja-asetuksen mukaista *sisäänrakennettua tietosuojaa* (”Data Protection by Design”), jossa yksityisyyden- ja tietosuojan periaatteita sovelletaan järjestelmässä suunnittelun alusta lähtien.

Anonymisoitu tieto ei ole henkilötietoa ja niihin ei sovelleta siis henkilötiedon tietosuojasäännöksiä. Henkilötiedon anonymisoinnissa tieto on käsitelty niin, että henkilöä ei voi enää tunnistaa niistä. Anonymisoitua dataa on esim. tilastoitaessa ja tietojohtamisessa käytettävä summatieto tai tilastolliseen muotoon muutettu tieto. Muuttaminen on peruuttamatonta. Huomioitavaa on, että edes summatietoina esitettävien terveystietojen aito anonymisointi ei ole yleensä suoraviivaista mm. harvinaisten sairauksien ja hoitojen vuoksi. Anonymisoidunkin asiakastiedon julkisessa levittämisessä kehotetaankin varovaisuuteen.

Asiakkaan hyvinvointitiedot ovat potilaan itsensä joko manuaalisesti tai hyvinvointilaitteiden avulla tuottavia tietoja. Esimerkkeinä on paino, aktiivisuus, verenpaine, pulssi, unen laatu silloin kun ne ovat asiakkaan itsensä tuottamia. Nämä eivät lähtökohtaisesti ole asiakastietoja, vaan henkilötietoja, joiden omistaja on kansalainen itse. Jos asiakkaan tuottamista hyvinvointitiedoista viedään esimerkiksi kooste APTJ järjestelmän potilaskertomukseen, niin tuo kooste on terveydenhuollon asiakastietoa.

Asiakastiedon käyttölokit sisältävät asiakkaan yksilöivää tietoa asiakastietojen käsittelystä (esim. kuka ja missä yksikössä on potilaan tietoja käsitellyt) ja näin ollen tiedot ovat salassa pidettävää henkilötietoa ja niiden kokoamiseen liittyy myös erityistä sääntelyä. Myös pilvi-

palveluissa käyttöloki tulee syntyä lain vaatimalla tavalla ja yleensä päätyä säilytettäväksi keskitettyyn lokienkäsittelyjärjestelmään analysointia ja mahdollista asiakkaille raportointia varten. **Järjestelmän tekniset lokit** ja käyttöstatistiikat eivät sisällä (ei tule sisältää) asiakastietoa, eikä näin olleen niiden käsittelyyn pilvipalveluissa liity sote-järjestelmien osalta poikkeuksellisesti huomioon otettavia asioita. Lokit kuitenkin usein sisältävät ammattilaisen ja/tai kansalaisen yksilöivää henkilötietoa (IP-osoite) ja näin olleen tavanomaiset GDPR-vaatimukset on huomioitava. **Synteettinen testidata** on täysin keksittyä dataa eikä näin ollen ole henkilötietoa, asiakastietoa tai muutoin luokiteltua. Usein synteettistä dataa generoidaan automaattisesti ja sen pohjana ei voi käyttää todellista dataa. Jos pohjana käytetään todellista dataa, synteettisen datan sijasta lopputuloksena voi ollakin anonymisoitua tietoa.



5 Luottamuksellisuuden varmistaminen pilvessä

Pilvipalveluiden mahdollistama teknologinen hyppäys nähdään joskus uhkana luottamuksellisuuden ja jatkuvuuden varmistamisen kannalta. Tätä se voi ollakin huonosti suunniteltuna ja osaamattomissa käsissä. Käytännössä pilviteknologiat ovat kuitenkin tuoneet täysin uusia mahdollisuuksia molempiin. Osaavasti toteutettuna pilviratkaisujen tietoturva on paremmalla tasolla kuin perinteisillä malleilla toteutetun ratkaisun.

Luottamuksellisuuden varmistaminen vaatii perinteisillä malleilla tuotetuista palveluista poikkeavaa lähestymistä ja osaamista. Esimerkkinä konesalin fyysisen turvallisuuden varmistaminen kansainvälisten pilvipalveluiden konesalissa vierailemalla on käytännössä mahdotonta, eikä tällaista vaatimusta omiin sopimusehtoihin tule siis sisällyttää. Samassa valtavassa konesalissa on tuhansien asiakkaiden tietoja, eikä heitä kaikkia päästetä konesaleihin. Varmuus konesalin fyysisestä turvallisuudesta taataankin kansainvälisen standardien ja ulkopuolisten arviointilaitosten sertifioinnin avulla. Sopimusten rooli korostuu entisestään ratkaisujen ja palveluiden vaatimustenmukaisuutta arvioitaessa.

Kuten aiemmin todettu (ks. 4.4 Sote-tiedon julkisuusluokat), hyvin suuri osa pilvessäkin toteutetuista sote-tietojärjestelmistä sisältää sosiaali- ja terveydenhuollon salassa pidettäväksi luokiteltua asiakastietoa. Sotepilven luottamuksellisuuden varmistamiseen on kaksi merkittävää tarkastelukulmaa: 1) Tekniset ja organisatoriset suojaukset ja 2) Pilvipalvelun sopimusriskien sekä ulkomaiseen omistukseen ja vaikutusvaltaan liittyvien riskien hallinta.

5.1 Fyysinen sijainti luottamuksellisuuden kannalta

Edellä on GDPR sääntelyn yhteydessä kuvattu periaatteet tiedon käsittelyyn ja tallentamiseen pilvessä, joiden mukaan suositeltavaa on siis säilyttää ja käsitellä tietoja aina EU/ETA-alueella, jos vain mahdollista. Huomioitavaa on myös, että ratkaisujen alihankintaketjut saattavat olla hyvinkin pitkiä. Ratkaisujen arvioinnin yhteydessä tuleekin tarkastella koko alihankintaketjun vaatimusten mukaisuus myös datan ja palvelun sijainnin osalta. Varsinaisen ydinratkaisun lisäksi on huomioitava myös toimittajan käyttämien alihankkijoiden (aliprosessoijien) osalta tietojen käsittely EU/ETA-alueella. Tällaisia aliprosessoijia voivat olla myös ratkaisussa hyödynnettävät SaaS- tai PaaS-palvelut.

Esimerkkeinä palveluista, jotka saattavat yllättää ratkaisun toimittajankin globaaliudellaan:

1. Mobiili notifikaatioiden ja tekstiviestienvälitys loppukäyttäjälle.
2. Ylläpito-, monitorointi- ja käyttöstatistiikka palvelut.
3. Tukipalvelutyökalut ja teknisen tuen etäyhteydet kolmansista maista.
4. Luontaiseksi globaaliksi rakennetut pilvitietokannat sekä välimuistiratkaisut. Arkkitehtuurinsa takia nämä eivät ole konfiguroitavissa pelkästään EU/ETA-alueella toimiviksi.
5. Sellaisten aliprosessoijien palvelut, joilla ei ole vielä merkittävästi EU/ETA-alueen asiakkuuksia eikä kehittynyt ymmärrystä EU-sääntelystä.

Mikäli aliprosessoija käsittelee tai tallettaa tietoja EU/ETA-alueen ulkopuolella, on vaihtoehtoina a) varmistaa ettei näihin palveluihin välitetä henkilötietoa (esim. anonyymi SMS-viesti), b) tehdä aiemmin kuvatut GDPR mukaiset sopimukset ja riskiarviot datan siirrosta kolmansiin maihin tai c) löytää korvaava palvelu.

5.2 Tekniset ja organisatoriset suojaukset

Tekniikkaan, ylläpitoon ja hallintaan liittyvät suojaukset varmistavat tiedon luottamuksellisuuden, eheyden ja saatavuuden. Tarve ja riskit ovat samoja, kuin mm. ulkoistetun konesalissa (hosted-onprem) toteutetuissa ratkaisuissa, kuitenkin pilvipalveluiden erityispiirteet huomioiden.

Myös pilvessäkin suojautumisen on pohjauduttava *syvään puolustukseen*, jolloin yksittäinen haavoittuvuus tai konfiguraatiovirhe ei johda katastrofaalisiin seurauksiin. Menetelmiin kuuluvat mm. tiedon salaaminen, käyttöoikeuksien hallinta, verkon palomuurit, haittaohjelmien havainnointi ja järjestelmien päivittäminen. Merkittävä osa tietoturvallisia pilvipalveluita on myös hyvät hallinnointikäytännöt ja roolipohjaisten käyttöoikeuksien rajaava käyttö ylläpidolle. Oletuksena ”kaikki on kiellettyä”, on hyvä lähtökohta.

Pilvialustoissa tietoturva on yhteispeliä organisaation, alihankkijoiden ja alustalla operoivien toimittajien välillä. Tämä vaatii selkeät yhteiset toiminta- ja hallintamallit. Myös ylläpidon ja kehityksen osalta on tärkeää tunnistaa alihankintaketjuihin liittyvät riskit, esim. kuinka isoja vaikutuksia voi yksittäisen alihankkijan yksittäisen henkilön tekemällä yksittäisellä konfiguraatiovirheellä olla? Organisaatiolla itsellä on tärkeä olla omistajuus ja teknistä osaamista strategiassa valituista hyperskaalautuvista pilvialustoista tai vaihtoehtoisesti strateginen kumppani, joka ottaa vastuun kokonaisuuden hallinnasta.

Tässä kappaleessa kuvataan karkealla tasolla esimerkkejä teknisiä- ja organisaationaalisen suojauksen menetelmiä. Tarkemmin parhaista käytännöistä on mm. toimittajien dokumentaatiossa sekä edellä mainitussa Pitukrissa.

5.2.1 Hyvien tietoturvakäytäntöjen toteuttaminen pilvipalveluissa

Jotta nämä sovitut käytänteet myös toteutuvat, tulee ne mahdollisuuksien mukaan toteuttaa pakottavasti (”enforce”) pilvialustojen mahdollistamilla työkaluilla mm. monivaiheisen tunnistautumisen (MFA, Multifactor Authentication), roolipohjaisten käyttöoikeuksien (RBAC = Role Based Access Control), menettelytapojen (policy), resurssilukkojen (locks) sekä nimeämiskäytäntöjen avulla. Vahvan tunnistautumisen käyttö on keskeinen suojausmekanismi pilvipalveluiden tietoturvassa; käyttäjän identiteetti on pilvipalveluissa käytännössä avain kaikkeen tietoon. Käyttöoikeuksissa on syytä noudattaa pienimmän oikeuksien periaatetta ja vain tarvittavaksi määräajaksi tarpeen mukaan korotettavia käyttöoikeuksia. Menettelytavalla voidaan rajata, että tietty alihankkija ei voi luoda internetiin julkaistavia palveluita tai mitään palveluita muulle kuin tiettyyn konesaliin EU/ETA-alueella. Tällaisten rajausten ja menettelytapojen luomisen tärkeyttä ei voida liikaa korostaa.

Pilvessä olevat palvelut tulee myös koventaa mm. poistamalla tarpeettomat palvelut ja portit käytöstä. Pilvipalveluiden tarjoamia tietoturvan hyvien käytäntöjen automaattisia kontrolleja, monitorointia sekä uhkien havainnointia on syytä tehokkaasti hyödyntää. Samoin haittaohjelmilta suojautuminen, haavoittuvuuksien hallinta, tietojen varmistaminen, jne. täytyy tehdä myös pilvipalveluissa.

Data on säilytettävä (”data at rest”) aina kun mahdollista salattuna, mikä nykyisin pilvialustoilla onkin käytännössä lähtökohta. Salausavaimia ja varmenteita on syytä har-

kita hallittavan itse (”bring your own keys”). Varmenteiden hallinta itsenäisesti vaatii hyviä käytäntöjä, selkeitä vastuita ja erityistä huolellisuutta, koska esim. vanhentunut varmenne pysäyttää koko järjestelmän toiminnan ja hukatut varmenteet voivat tehdä datasta lopullisesti lukukelvotonta. Varmenteiden hallintaan liittyvät unohdukset ja virheet ovat edelleen yleisiä palvelutuotannon ongelmien aiheuttajia. Varmenteiden hallinnasta on kontrolleja myös THL:n määräyksissä.

Tiedonkäsittelyyn pilvipalveluissa tarjotaan myös ns. Confidential Computing -ratkaisuja (”salattu tietojenkäsittely”), joissa tietoa käsitellään suojattuna myös palvelimen muistissa tarjoten lisä tietoturvaa. Tällaisten ratkaisut ovat kuitenkin yleensä matalan tason palvelinvirtualisointia (~IaaS), eikä sitä ole tarjolla siis esim. SaaS palveluissa, jos tätä tarvetta ei ole alusta asti huomioitu sovellusarkkitehtuurissa. Confidential computing -kapasiteetti on myös kalliimpaa, johtuen tarvittavista erikoislaitteistoista.

Tietosuojan toteutukseen ja arkaluonteisen tiedon turvaamiseen pilvipalvelut tuovat myös uusia automaattisia välineitä, kuten *tietojen menetyksen estäminen* (DLP, Data Loss Prevention). Välineiden avulla tietoa ja dokumenttia voidaan luokitella arkaluonteisuuden perusteella, tunnistaa poikkeamia tiedon käytössä ja tarvittaessa estää arkaluonteisen tiedon siirrot. Ratkaisut ovat integroitumassa osaksi mm. toimistotyökaluja, data-alustoja ja raportointivälineitä.

5.2.2 Tiedonsiirron luottamuksellisuuden turvaaminen

Pilvipalveluita käytettäessä henkilötiedot on jo GDPR vaatimustenkin mukaisesti siirrettävä salattuna (”data in motion”). Selaimella käytettävän sovellusten osalta tämä toteutetaan minimissään TLS (Transport Layer Security) salauksella, samalla mitä verkkopankitkin hyödyntävät.

Myös eri pilvipalveluiden välillä (pilven sisällä) tietoliikenteen on kuljettava salattuna, näin suojaudutaan pilven runkoverkossa tapahtuvan liikenteen kuuntelun riskiltä (syvä puolustus). Myös pilvipalvelun sisällä palvelut erotellaan segmentteihin ja segmenttien välilläkin vain välttämätön liikennöinti sallitaan (”default-deny”). Pilvipalveluiden sisällä kommunikoitaessa on oltava myös tarkkana, että liikennettä ei erehdyksessä reitity Internetin kautta.

Käytettäessä pilvipalvelualustoja on syytä varmistaa, että yhteys on suojattu riittävällä tasolla. Suojauksessa tulisi mobiilikäytön ja pilvipalveluiden lisääntyessä keskittyä pelkän verkkoliikenteen suojaamisen sijaan palveluiden käyttäjän identiteetin suojaamiseen. Mikäli organisaatiolla on laajempaa käyttöä tiettyyn hyperskaalautuvaan pilvipalveluun, on pilvipalveluun syytä luoda suojattu VPN-yhteys lähiverkon ja pilvikonesalin välille (VPN = Virtual Private Network). Kun pilvipalveluiden käyttö kasvaa, suositellaan muodostamaan dedikoitu tietoliikenneyhteys (esim. *AWS Direct Connect*[64], *Azure Express Route*[65], *Oracle FastConnect*[66] *sekä GCP Interconnect*[67]) pilvistrategian mukaisiin hyperskaalautuviin alustoihin ja myös ohjaamaan liikenne pilvialustoille kulkemaan tämän yhteyden kautta. Dedikoidussa yhteydessä on sovittu tiedonsiirtokaista sekä palvelutaso (SLA, Service Level Agreement). Nämä yhteydet kannattaa toteuttaa esim. hyvinvointialueen laajuisesti kustannusten optimoimiseksi. On aina tiedostettava ja dokumentoitava, että siirtyykö ratkaisussa data Internetin yli vai kulkeeko se suojatun dataputken kautta pilvipalveluun. Tämä ei ole aina selvää ratkaisuntoimittajalle tai sovelluskehittäjällekään.

Kun toteutetaan lähiverkosta yhteys pilvipalveluun, laajenee organisaation verkkoinfrastruktuuri pilvipalvelun virtuaaliverkkoon. Tämä vastaa tavallaan verkkoyhteyksien rakentamista kumppaniorganisaation verkkoon ja vaatii siis erityistä huomiota. Huonosti rakennetun yhteyden kautta hyökkääjä voi päästä sisäverkon haavoittuvuuksien kautta käsiksi pilvipalveluihin tai toisinpäin.

Usein myös pilvipalveluiden IP-osoitteet liitetään organisaation DNS:ään (Domain Name System), jolloin niille saadaan kotoinen osoite tyyliin ”palvelu.soteorganisaatio.fi”.

Dedikoidun tietoliikenneyhteyden muodostamista hyperskaalautuvaan pilvipalveluun voi ajatella vastaavan kiinteän verkkoyhteyden muodostamista organisaation eri toimipaikkojen välille; nyt toinen ”toimipaikka” sijaitseekin hyperskaalautuvassa pilvessä esim. Keski-Euroopassa. Käytännössä Suomessa olevan organisaation liikenne kulkee lähiverkosta operaattorilta ostettua verkkoyhteyttä myöten Pääkaupunkiseudulle, jossa sijaitsevan hyperskaalautuvan pilvialustan yhteyspiteen kautta liikenne ohjautuu optimoitua kaistaa pitkin suoraan pilvikonesaliin Keski-Euroopassa. Liikenne ei kulje missään vaiheessa Internetissä ja yhteydelle saadaan sovittu palvelutasosopimus (SLA), jota Internetissä kulkevalla liikenteellä ei ole. Mitä lähempänä pilvialustan Etelä-Suomessa sijaitsevaa yhteyspistettä ja/tai pilvikonesalia organisaatio teknisesti sijaitsee, sitä vähemmän koko yhteydessä on Suomessa sopimusosapuolia ja alihankkijoita. Suomesta on Keski-Eurooppaan useita maantieteellisiä tietoliikennereittejä (ainakin neljä) ja samalta toimijalta ostettu yhteys reitittyy tarpeen mukaan eri reittejä. Kukin reitti on myös itsessään rakennettu vikasietoiseksi. Tarvittaessa data voidaan myös pakottaa reitittymään vain haluttujen maiden kautta. Dedikoidun kaistan osalta varmistetaan toteutuskohtaisesti, että tieto kulkee halutulla tavalla suojattuna.

Pilvitaipaleen edetessä kannattaa myös varmistaa, että mahdollisesti Keski-Euroopassa pilvessä vierekkäin olevien palveluiden keskinäinen liikenne ei kierrä turhaan Suomen kautta. Myös eri valmistajien hyperskaalautuvien pilvialustojen liikenne voidaan reitittää suoraan niiden välille, kierrättämättä liikennettä turhaan Suomen kautta. Tällä on positiivinen vaikutus suorituskykyyn, luotettavuuteen sekä kustannuksiin.

5.3 Pilvipalvelun sopimusriskien hallinta

Kansallisten linjauksen mukaan sote datan tallennus ja käsittely EU/ETA-alueella sijaitsevissa kansainvälisten teknologiayritysten tarjoamissa pilvipalveluissa on mahdollista samoilla ehdoilla, kuin Suomessa sijaitsevissa palveluissa. Sopimukselliset, tekniset sekä organisatoriset varmistukset tulee täyttää. GDPR:ää ja siihen liittyvän Schrems II -päätöksen mukaisia tarkennuksia noudattamalla henkilötietoa voidaan käsitellä myös EU/ETA-alueen ulkopuolella. Kuitenkin organisaatioiden on sopimusriskien minimoimiseksi syytä rajoittaa tallennus ja käsittely EU/ETA-alueelle aina kun mahdollista tai rajoittaa kolmannessa maassa tapahtuva käsittely välttämättömään minimiin. Katso tarkemmin kappaleesta ”4.2 Lainsäädäntö”. Huomioi suojauksissa myös tarpeen mukaan tilanteet, joissa asiakkaat käyttävät palvelua EU/ETA-alueen ulkopuolelta esim. lomamatkoillaan.

Hyperskaalautuvat pilvialustat ovat yhdysvaltalaisia yrityksiä, sopimukset tosin yleensä tehdään eurooppalaisen tytäryhtiön kanssa. Käytännössä täysin eurooppalaisia vaihtoehtoja ei yleensä ole, johtuen näiden yhtiöiden teknisestä etumatkasta. Sopimusten osalta yksittäisen toimijan neuvotteluvara kansainvälisiin suuryhtiöihin on yleensä pieni, mikä vaikeuttaa sopimusriskien hallintaa. Kansainväliset suuryrityksillä on yleensä vakioituneet EU-tasoiset sopimuskäytännöt, jotka yhdessä edellä kuvattujen organisaation tekemien riskiarviointien ja suojausten kanssa (ks. 4.2 Lainsäädäntö) yleensä mahdollistavat tiedon käsittelyn ja tallentamisen pilvipalveluissa.

Joissain sopimusehdoissa on edelleen olla varattuna mahdollisuus yksipuolisesti muuttaa sopimusehtoja. Tällaisen hyväksymistä tulee ehdottomasti välttää ja/tai rajata ne niin, ettei hankalasti hallittavaa riskiä luottamukselliselle tiedon käsittelylle muodostu. Esim. Microsoftin mukaan heidän uudet palvelusopimuksensa sitovat heidän toimintaansa, mutta asiakas voi sopi-

muskauden ajan aina vedota sopimushetkellä voimassa olleeseen sopimukseen tai sen DPA-liitteeseen. Vastaavia menettelyjä on muidenkin erikseen sovittavissa ”enterprise”-sopimuksissa. Alaviitteen linkissä esimerkkilistaus AWS-sopimuksen muutoksista vuosien varrella[68].

Sopimusriskien vaikutuksia voidaan joiltain osin hallita myös arkkitehtuurivalinnoilla, sekä miettimällä muutoinkin onko sovellukset siirrettävissä millä aikataululla ja kustannuksilla toiseen konesaliin tai toiselle pilvialustalle jäännösriskien realisoituessa (”cloud exit plan”).

5.3.1 Ulkomaiseen omistukseen ja vaikutusvaltaan liittyvät riskit

Ulkomaiseen omistukseen ja vaikutusvaltaan liittyvät riskit viittaavat ulkomaalaisomisuksessa olevien pilvipalveluiden paikallisen maan lainsäädännöstä, jotka voivat velvoittaa myös pilvipalveluntarjoajan toimimaan joissain tapauksissa yhteystyössä kyseisen maan viranomaisen kanssa ja mahdollistaen näin vieraan valtion pääsemiseminen käsiksi luottamukselliseen tietoon. Näitä riskejä kutsutaan lyhenteellä FOCI (*Foreign Ownership, Control, or Influence*). Lainsäädäntöjohdannainen tietojen luovuttaminen ja tutkimisoikeus on useissa maissa rajattu koskevaksi poliisia sekä tiedusteluviranomaisia. Yhdysvalloissa asiaan liittyy ns. CLOUD Act -laki, jonka tavoitteena on ollut helpottaa poliisin ja muiden viranomaisten toimintaa kansainvälisissä tutkinnoissa. Yleensä pilvialustojen tarjoajat pyrkivät ensisijaisesti kääntämään viranomaisten tietopyynnöt tiedot omistavalle asiakkaalle, haastamaan ne, sekä vaativat sen maan oikeuden päätöksiä missä palvelun sopimukset on tehty (esim. Suomi, Irlanti, EU). He myös pyrkivät kommunikoimaan avoimesti näistä pyynnöistä ja niiden määristä, ks. esim. Microsoftin sivusto aiheesta alaviitteessä[69]. Vain osa viranomaisten pyynnöistä hyväksytään ja valtaosassa hyväksytyistä pyynnöistä välitetään metatietoa kuluttajien palvelun käytöstä, ei varsinaista sisältö dataa (vrt. esim. puheluiden lokitiedot). Huomioitavaa on, että vastaavia riskejä voidaan nähdä myös perinteisempiin lähikonesalin teknologioihin, tietoverkkoihin, jne. liittyen.

Perimiltään kyse on *data suvereniteetista* (data/cloud/digital sovereighty) Suomen osalta aihe on osa koko EU:n pilvisuvereniteettia. Ei ole olemassa eurooppalaista kilpailukykyistä hyperskaalautuvan palvelun tarjoajaa. Tähän liittyy mm. Gaia-X -hanke[70] sekä Saksan ja Ranskan investoinnit *luottamukselliseen pilveen* yhdessä kansainvälisten hyperskaalautuvien pilvialustojen teknologiatoimittajien ja paikallisten yritysten kanssa[71]. Vastaavantyyppistä ratkaisua on jo toteutettu Saksassa aiempinakin vuosina, silloin haasteeksi osoittautui kohonneet kustannukset sekä palveluiden jääminen jälkeen muista toimittajan pilvipalveluista ylläpidon hankaluuden vuoksi. Pilvi- ja datasuvereniteetti on nouseva teema myös muissa maissa ympäri maailman. Pilvisuvereniteetin kansainvälisistä lainsäädännöllisistä ja poliittisista juurisyistä johtuen, yksittäisen organisaation vaikutusvalta sekä riskien täydellinen arviointikyky näihin liittyen on rajallista. Helposti ajaudutaan miettimään teknologiasia riskejä, joita ei yhtä syväluotaavasti perinteisimmissä teknologioissa toteutetuissa ratkaisuissa käydä läpi (esim. kansainvälisen yhtiön Suomessa ylläpitämä hosted-onprem konesali). Usein riskejä voidaan hallita pilvipalveluntarjoajan valinnalla (ei esim. suositella kiinalaista pilveä), hyvillä sopimuskäytännöillä ja sekä laadukkailla teknisillä sekä ylläpidollisilla suojauksilla.

Erityisesti ns. Schrems II -ratkaisuun liittyen on toisinaan katsottu riskiksi, että USA:han sijoittuneet pilvipalveluita tarjoavat teknologiayhtiöt voivat USA:n lakien perusteella olla velvoitettuja luovuttamaan GDPR:n vastaisesti niiden eurooppalaisten tytäryhtiöiden hallussa olevia henkilötietoja USA:n viranomaisille. Täysin samoin perustein olisi perusteltua epäillä myös kaikkia muitakin yhtiöitä, joilla on *toimintaan* USA:ssa, velvollisuudesta luovuttaa henkilötietoja USA:n viranomaisille. Lainsäädäntö on tältä osin teknologianeutraalia, eivätkä pilvipalveluita tarjoavat yritykset poikkea muista yrityksistä. Lainsäädän-

nön näkökulmasta edellä todettu riski kuuluu EU:n toimivallan piiriin ja siitä on huolehdittu GDPR:n normein ja mekanismein. GDPR:n 1 artiklan 3 kohdan mukaan ”Henkilötietojen vapaata liikkuvuutta unionin sisällä ei saa rajoittaa eikä kieltää syistä, jotka liittyvät luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä”. Kansallisella lainsäädännöllä voidaan siten ainoastaan täydentää GDPR:ssä todettua sääntelyä GDPR:n nimenomaisesti sallimissa rajoissa. EU/ETA-alueella toimiva alueella voimassa olevaa oikeutta noudattavan yrityksen palveluiden käytölle ei siten voida asettaa luonnollisten henkilöiden henkilötietojen suojeluun liittyviä esteitä.

5.3.2 Erityisiä lisäsopimuksia tuki- ja ylläpitotoimiin

Schrems II päätöksen vauhdittamana erityisesti suuryritykset tarjoavat myös erityisiä lisäsopimuksia/palveluita tietojen luottamukselliseen käsittelyyn EU-alueella. Näiden palveluiden käyttö on kuvattava ja sovittava asiakaskohtaisesti.

Pilvipalvelut tuotetaan ja ylläpidetään siitä maasta (ja maanosasta), jossa palvelun konesalit sijaitsevat. Hallinta- ja valvontatehtävät eivät usein vaadi yksittäisen asiakkaan ympäristöjen kanssa suoraan tekemisissä oloa, vaan hallintatoimenpiteitä suoritetaan vakioituina tukitoimina ylläpitäjän kannalta ”anonyymeille” resursseille. Normaalitilanteessa tuki (valvonta, ongelmien selvittely) toimii kustannusten optimoimiseksi ns. *follow-the-sun* periaatteen mukaisesti, yksinkertaistettuna aina sieltä päin maailmaa missä on kulloinkin päivä. **Useilla pilvipalveluntarjoajilla on mahdollista (nyt tai vuoden 2022 aikana) rajata tukitoimenpiteet tapahtumaan EU/ETA-alueella olevan henkilöstön toimesta.** Tuen rajaaminen tapahtumaan ainoastaan EU/ETA-alueelta todennäköisesti nostaa kustannuksia ja kaikkien palveluiden osalta rajaaminen ei ole lainkaan mahdollista. Samoin tämä saattaa vaikeuttaa harvinaisten haastavien ongelmien selvitystä, koska esim. USA:ssa tai Intiassa olevaa tietyn teknologian erityisosaajia ei voida ihan niin tehokkaasti hyödyntää kriittisessä ongelmanselvityksessä. Ongelmien selvitysten osalta on huomioitavaa, että myös useiden Suomessa yleisesti käytössä olevien konesalien taustajärjestelmien ja sote-tietojärjestelmien kehityksestä merkittävä osa tapahtuu EU:n ulkopuolella ja haastavien ongelmien selvittelyissä onkin jo pitkään hyödynnetty EU-ulkopuolella olevien tiimien työpanosta GDPR:n vaatimukset huomioiden. Tukitoimenpiteiden rajaamista EU/ETA-alueelle kannattaa harkita sitten kun sen toiminnasta on enemmän käytännön kokemuksia.

Lupamenettely ylläpitotoimenpiteille. Sopimuksen perusteella pilvialustan tuottajan on aina etukäteen pyydettävä lupa tiettyjen ylläpitotoimenpiteiden suorittamiseen asiakkaan pilviympäristössä, kuten Azure *Customer Lockbox*, AWS *Access Approval, GCP Access Approval sekä* Oracle European Union Restricted Access (EURA). Huomioitavaa on, että palveluiden käyttäminen voi vaatia organisaatiolta 24/7 resurssointia ylläpitotoimenpiteiden hyväksymisprosessiin. Isoilla pilvipalveluntarjoajilla on muutenkin hyvät ylläpitokäytännöt, eikä ylläpitohenkilökunta saa pääsyä yksittäisen asiakkaan ympäristöön missään tilanteessa ilman vastuuhenkilön/-henkilöiden hyväksyntää. Lupamenettelyä kannattaa harkita, mikäli organisaatiolla on aidosti riittävä kypsyys vastata 24/7 hyväksymispyyntöihin.

6 Pilvi ja jatkuvuudenhallinta

Yhteiskunnan varautumisen tavoitteena on turvata elintärkeät toiminnot. Sosiaali- ja terveydenhuollon **jatkuvuudenhallinnalla ja varautumisella** varmistetaan sote-palveluiden mahdollisimman häiriötön hoitaminen, sekä mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet normaaliolojen häiriötilanteissa ja poikkeusoloissa. Sosiaali- ja terveydenhuollon varautumista häiriötilanteisiin ja poikkeusoloihin johtaa, valvoo ja yhteensovittaa sosiaali- ja terveysministeriö[72] ja siellä valmiusasioista vastaa valmiusyksikkö[73].

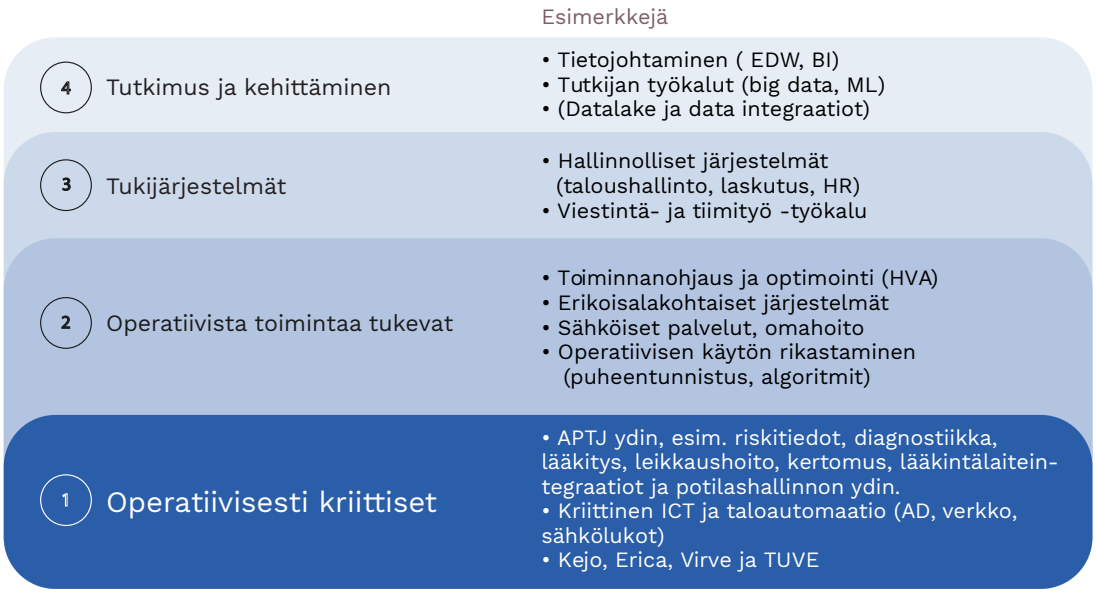
Sote-tietojärjestelmät ovat tietointensiivisiä, ja järjestelmien kriittisyys jatkuvuuden kannalta konkretisoituukin tiedon saatavuuteen häiriötilanteissa. Käytännössä kliinikon on saatava tarvitsemansa potilastiedot hoitopäätöksiä varten. Sote-tietojen tai järjestelmien kriittisyyden luokitteluun ei ole kattavaa kansallista ohjeistusta. Kriittisten järjestelmien ja tietojen määritteleminen onkin lopulta organisaatioiden omalla vastuulla. Tässä kuvataan perussääntöjä ja työkaluja tämän työn tueksi kansalliseen sääntelyyn perustuen.

THL määräyksissä asetetut jatkuvuuden erityisvaatimukset kriittisille järjestelmille täytyy ottaa huomioon pilven käytössä ensihoitoa ja päivystystä tukevien järjestelmien osalta (ks. 4.2 Lainsäädäntö). Jatkuvuudenhallinnassa tärkeää on tunnistaa riskit ja häiriötilanteet mitä vasten varaudutaan, tätä esitellään skenaarioanalyysissä. Siinä huomataan, että pilvialustat voivat tuoda kustannustehokkaita uusia mahdollisuuksia korkean käytettävyyden varmistamiseen myös kriittisimmissä palveluissa.

6.1 Järjestelmäluokittelu jatkuvuudenhallinnan kannalta

Tämän soveltamisohjeen tuottamisen yhteydessä luotiin jatkuvuudenhallinnan suunnittelun tueksi sote-tietojärjestelmien luokittelu neljään luokkaan toiminnallisen kriittisyyden mukaan:

1. **Operatiivisesti kriittisiin järjestelmiin** kuuluvat ne järjestelmät, jotka ovat organisaation kriittisten toimintojen kannalta välttämättömiä. Näitä ovat: APTJ:n ydin (riskitiedot, diagnostiikka, lääkitys, leikkaushoito, kertomus, lääkintälaiteintegraatiot ja potilashallinnon ydin), kriittinen ICT (AD, lähiverkon palvelut), taloautomaatio (mm. sähköinen kulunhallinta, putkiposti, sisätilapaikannus, LVIS-ohjaus) sekä erityisesti ensihoitopalveluissa käytettävät TUVE, Virve, Kejo sekä Erica.
2. **Operatiivista toimintaa tukevat ja täydentävät järjestelmät pitävät** sisällään laajan joukon erikoisalakohtaisia järjestelmiä, sähköisiä palveluita, HVA tasoista toiminnanohjausta sekä erilaisia operatiivisen käyttöä rikastavia palveluita. Nämä ovat organisaation ydinprosesseihin käytettäviä järjestelmiä, joita ilman kuitenkin pärjätään (vaikkakin nilkuttaen) varautumistilanteessa pitemmänkin aikaa. Mikäli esim. tilannekuvat tai kliinisen tiedon hakukoneet tms. ovat riippuvaisia tietoaltaasta, on myös tietoallas niiltä osin tässä luokassa.
3. **Tukijärjestelmät** sisältävät mm. hallinnollisia järjestelmiä (taloushallinto, laskutus, HR) sekä esim. viestinnän ja tiimityön järjestelmiä. Potilasturvallisuus ei välittömästi vaarannu.
4. **Tutkimus- ja kehittämistoiminnan järjestelmät** sisäl-



Kuva 4. Sote-järjestelmien luokittelu jatkuvuuden näkökulmasta.

tävät mm. tietojohtamisen järjestelmät ja tutkijoiden työkalut, sekä myös näiden tarvitsemat tietoaltaan data integraatiot. Näitä ilman pärjätään varautumistilanteissa pitempäänkin.

6.2 Operatiivisesti kriittisten järjestelmien määrittely

Organisaation kriittisten toimintojen määrittely on lähtökohta määritellessä kriittisiä järjestelmiä. Hyvinvointialueilla henkeä ylläpitävät ja -pelastavat toiminnot katsotaan yleensä kriittiseksi. Näitä toimintoja ovat sairaaloiden ns. kuuman puolen toiminnot (päivystys, leikkaustoiminta, tehohoito, synnytysosastot) sekä ensihoito. Näissä toiminnoissa välttämättömiä kriittisiä järjestelmiä ovat ainakin lääkintälaitteet, APTJ-järjestelmien ydin (kertomus, lääkitys, diagnoosit, riskitiedot, ydin potilashallinto, jne.), tärkeimmät diagnostiset palvelut sekä lääkehuollonjärjestelmät. Koska APTJ-järjestelmät ovat pääsääntöisesti isohkoja jakamattomia kokonaisuuksia, niin APTJ-järjestelmän ”ydin” on todellisuudessa melko laaja kokonaisuus pitäen sisällään myös ei-ihan-niin-kriittisiä osajärjestelmiä.

Lisäksi on huomioitava Ensihoitoasetuksen sekä ”Laki julkisen hallinnon turvallisuusverkkotoiminnasta” asettamat vaatimukset (ks. 4.2 Lainsäädäntö) ja näin ollen TUVE-, Virve-, Kejo- sekä Erica-järjestelmien rooli kokonaisuudessa erityisesti ensihoidon osalta.

6.2.1 Kriittisten järjestelmien erityiset varautumisen vaatimukset

THL:n määräys 4/2021[74] määrittelee kriittiseksi luokiteltuja järjestelmiä koskemaan ”erityisiä varautumisen vaatimuksia”. Määräys velvoittaa varmistamaan näiden järjestelmien jatkuva toimivuus potilasturvallisuuden vaarantumatta myös tilanteissa, joissa verkkoyhteydet on rajattu Suomen maantieteellisten rajojen sisäpuolelle. Kriittisiksi järjestelmiksi (*”A3 kriittiset”*) luokitellaan ne

tietojärjestelmät, joita käytetään julkisen terveydenhuollon päivystysvastuun ja ensihoidon toteuttamiseen. Järjestelmien joukkoa on mahdollista myöhemmin laajentaa.

Määräykseen on myös kirjattu mahdollisuus toteuttaa ratkaisu niin, että palvelut ovat palautettavissa toimintaan nopeasti varautumistilanteissa, tämä tuo joustavuutta teknisiin varautumisen ratkaisuihin mahdollistamalla mm. lähikonesaliin kahdennetun järjestelmäkopion käyttämisen pilvessä toteutetun järjestelmän poikkeustilanteessa käyttöönotettavana varajärjestelmänä (hybridi pilvi). Nykyisin käytössä olevilla APTJ-järjestelmillä tällaisen toteuttaminen voi kuitenkin olla mm. integraatioista johtuen haastavaa.

6.2.2 Jatkuvan toiminnan varmistaminen paikallisissa häiriöissä

Kriittisten järjestelmien jatkuvalle toiminnoille on erilaisia riskejä, kuten tietoliikenne-, sähkönsyöttö- tai muut alueelliset ongelmat. Jatkuvan päivystyksen sairaaloiden on pystyttävä toimimaan myös pitkittyneen alueellisen sähkökatkon aikana itsenäisenä kokonaisuutena (ks. Päivystysasetus, kohdasta 4.2 Lainsäädäntö).

Jatkuvan toiminnan vaatimusten täyttämiseksi eri riskiskenaarioissa on kriittiset järjestelmät, tai niiden itsenäisesti toimiva kopio on, syytä pitää fyysisesti ja sopimuksellisesti riittävän lähellä päivystys- ja ensihoidon yksikköitä myös jatkossa.

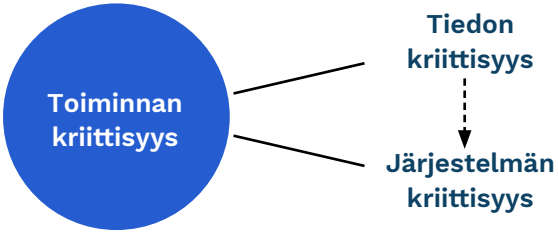
Sopimuksellisesti lähellä pitäminen tarkoittaa palvelun tuotannon kannalta merkittävien kumppanien ja kriittisten aliprosessoijien minimointia sekä sopimuksellisten vastuiden selkeyttä, jolloin kriittisten ongelmien selvittäminen on suoraviivaisempia. **Järjestelmien fyysinen läheisyys** minimoi mm. tietoliikenneongelmien todennäköisyyttä eri riskiskenaarioissa, myös latenssi ja sen vaihtelut pienenevät. Fyysistä läheisyyttä ei siis määrittele niinkään kilometrit, vaan tietoliikenneratkaisun infrastruktuuri ja sen luotettavuus eri tilanteissa. Laajasti käytetyissä APTJ-järjestelmissä on tosin edelleen myös osajärjestelmien vanhasta kaksitasoarkkitehtuurista johtuvia tiukkoja latenssivaatimuksia (tietoliikenteen viive), joiden saavuttaminen satojen kilometrien päästä on haastavaa reitillä olevien reitittimen sekä ihan fyysisen välimatkan aiheuttavan viiveen vuoksi.

Yksityinen terveydenhuolto voi jo nykyään, perusteellisen riskianalyysin jälkeen niin todettuaan, toteuttaa lähes kaikki järjestelmänsä pitkänkin etäisyyden päästä kaikkiin toimipisteisiinsä. Ratkaisu voi olla pilvialustalla joko Suomessa tai EU/ETA-alueella. Tämä on käytännössä mahdollista, koska heillä on vaihtoehtona äärimmäisessä kriisitilanteissa ohjata potilaat päivystysvastuulliseen sairaalaan ja ensihoitoon. Harvinaisimmissa varautumisen riskiskenaarioissa he siis voivat todennäköisesti tukeutua julkiseen terveydenhuoltoon. Samoin sellaisilla perusterveydenhuollon organisaatioilla, joilla ei ole päivystysvastuuta tai sairaaloita ja on edelleen oma APTJ, tämä voi olla mahdollista.

Haja-asutusseutujen perusterveydenhuollon yksikköihin ICT-palvelut toteutetaan jo nykyisin kymmenien tai jopa satojen kilometrien päästä sijaitsevasta keskitetystä konesalista. Tulevaisuudessa on hyvin mahdollista, että hyvinvointialueiden terveyden- ja sosiaalihuollon järjestelmät keskitetään entisestään lähelle jatkuvan päivystyksen yksiköitä (lähellä sairaalaa) tai vielä etäämmältä tuotettuihin pilvipalveluihin. Tämä todennäköisesti kuitenkin parantaa heidän ICT-palvelunsa luotettavuutta konesalien suuruuden ekonomian tuomien korkean käytettävyyden ratkaisujen vuoksi, vaikka verkkoyhteyksien osalta jatkuvuudenhallin riskit toisaalta lisääntyvät.

6.2.3 Kriittisten tietojen suhde järjestelmien kriittisyyteen

Kriittiset primääriset järjestelmät: Tietyn tietojoukon kriittisyys jatkuvuuden kannalta tekee sitä tuottavan ja



Kuva 5. Toiminnan, tiedon ja järjestelmän kriittisyyksien suhde.

primäärisesti (ensisijaisesti) käsittelevästä järjestelmästä kriittisen. Esimerkkinä lääkitystiedot ovat tietojoukkona saatavuudeltaan kriittinen ja niinpä APTJ:n Lääkitys-sovellus on myös jatkuvuuden kannalta kriittinen.

Kriittiset tukijärjestelmät: Toisaalta järjestelmä voi olla jatkuvuuden kannalta kriittinen, vaikka siinä ei käsiteltäisi lainkaan sote-tietoa. Esimerkki tällaisesta järjestelmästä ovat taloautomaatio tai työasemalle kirjautumiseen tarvittava AD (Active Directory). Kriittinen toiminta estyy, mikäli henkilökunta tai potilaat eivät pääse sisään ja kirjautumaan työasemille tai rakennuksen sisälämpötila menee pakkaselle. Taloautomaation osalta on mahdollista, että niiden etähallintayhteys ohittaa 5G-modeemin kautta organisaation palomuurit ja muut mahdolliset suojaukset ottaessa yhteyttä suoraan valmistajan pilvipalveluihin Internettiin. Näistäkin järjestelmissä on siis tärkeää jatkuvuudenvarmistamiseksi selvittää missä valmistajan pilvipalvelimet sijaitsevat, miten sinne kommunikoidaan ja miten palvelu on suojattu. IoT (Internet of Things, esineiden internet) ja 5G yleistyessä erilaiset verkkoon liitetyt laitteet tulevat lisääntymään ja asia onkin huomioitava esim. pilvistrategiassa.

Kriittisen järjestelmän riippuvuus ei-kriittisistä järjestelmistä: Kriittiset järjestelmät voivat olla myös riippuvaisia vähemmän kriittisistä osajärjestelmistä. Esimerkiksi usein APTJ on käytännössä jakamaton kokonaisuus ja niinpä, kun yksi APTJ-osajärjestelmä on palveluiden tuottamisen kannalta kriittinen, niin käytännössä koko jakamatonta APTJ-järjestelmää on kohdeltava jatkuvuuden kannalta kriittisenä. Vastaavasti kriittisen järjestelmän toiminnalle välttämättömistä integraatioista voi joissain tapauksissa muodostua jatkuvuudelle kriittisiä.

Kriittistä tietoa käsittelevät, mutta ei kriittiset järjestelmät: Kriittiseksi luokiteltua tietoa hyödynnetään primäärisen järjestelmän lisäksi tavallisesti myös useissa muissa järjestelmissä (sekä ensisijaisessa että toisiokäytössä), mutta tämä ei suoraan tee näistä järjestelmistä jatkuvuuden kannalta kriittisiä. Esimerkkinä laboratoriovastaukset ovat tietona kriittistä lähes kaikessa kliinisessä toiminnassa. Tämä ei kuitenkaan suoraan tee kaikista laboratoriovastauksia hyödyntäviä järjestelmiä (kuten omahoitopalvelut, diabetesseurannat, tilastot, laskutus, tutkijantyötilat, biopankki, raportointi, jne.) toiminnan kannalta kriittisiä.

Sosiaalihuollon järjestelmien kriittisyyden luokittelu koetaan usein haastavaksi; esim. sosiaalihuollon päivystyksen toiminnan, kotihoidon palveluiden tai tukien maksatuksen häiriintymisellä voi olla nopeastikin kriittisiä vaikutuksia asiakkaiden elämään. Järjestelmien saatavuuden kriittisyyttä sosiaalihuollon osalta eri riskiskenaarioissa onkin syytä analysoida huolella erikseen.

6.3 Pilvipalvelut huomioiva riskiskenaarioanalyysi

ICT-palvelut hajautuvat, mikä hankaloittaa kokonaisuuden hallintaa myös jatkuvuusanalyysien teossa. Viimeisten vuosien aikana kyberturvallisuuden reaaliaikainen tilannekuvan hallinta ja ylläpito, sekä kansallisesta että organisaatioiden näkökulmasta on korostunut. Toisissa riskiskenaarioissa pilvipalvelut voivat olla turvaverkko, ja toisessa skenaariossa uhka jatkuvuudelle. Häiriötilanteessa on varmistettava, että kriittisten operatiivisten palveluiden osalta on sovittu yhteinen toimintamalli

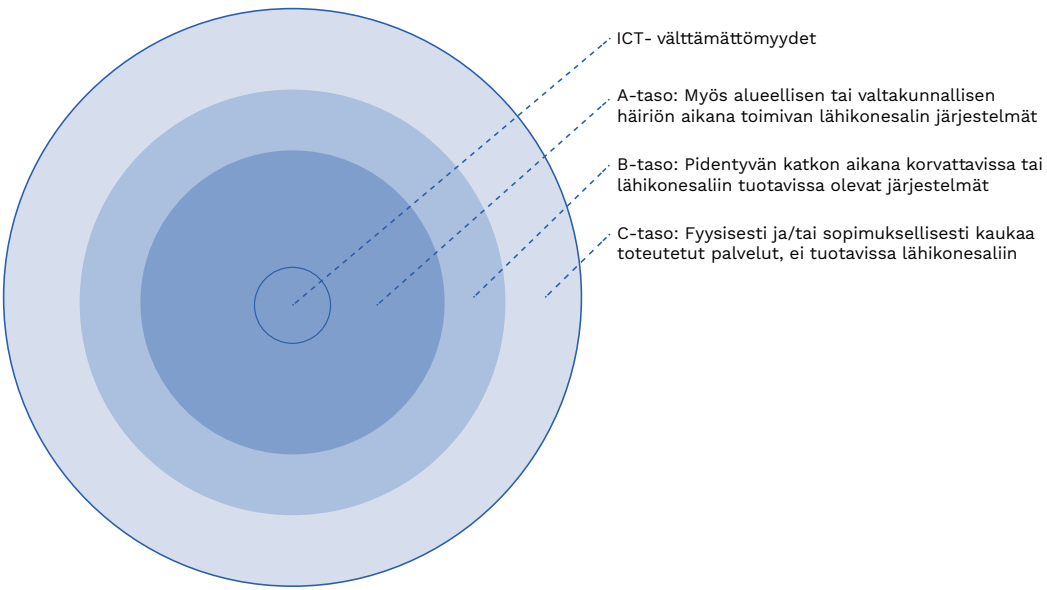
poikkeamahallintaan. Pilvipalveluiden osalta on varmistettava, että havainnointi- ja reagointikyvykkyys säilyvät joko itsellä tai sopimusteitse toimittajan toimesta. Tämä voi vaikuttaa vahvasti pilven toteutustapaan ja kustannuksiin.

Pilvipalveluiden vaikutusta toimintaan on hyödyllistä tarkastella **jatkuvuuden riskiskenaarioiden** avulla. Kommunikoinnin tueksi riskiskenaarion vaikutus erityisesti pilvipalveluiden osalta visualisoidaan kokonaisuutena organisaation sidosryhmien (johto, kliinikot, ICT, tukipalvelut) sekä muiden sidosryhmien (kansalliset toimijat, ratkaisuntoimittajat, infratoimittajat, pelastuslaitos, puolustusvoimat) nopeasti sisäistettävässä tiiviissä muodossa. Yksinkertaistetusta kokonaiskuvasta on mahdollista keskustella kiireistenkin henkilöiden kanssa, saada tärkeitä huomioita tarkentaviin skenaarioihin sekä tehdä toimenpide suunnitelmilla. Kuvauksen ei ole siis tarkoitus olla täydellinen kuvaus kaikkine riippuvuuksineen ja järjestelmineen, vaan toimia keskeisten skenaarioiden analyysin työkaluna. Riskianalyysiä on hyvä käyttää keskustelutyökaluna myös teknologiantoimittajien kanssa, ratkaisuvaihtoehtoja kartoittaessa.

6.3.1 Sipulimallin eri tuotantosegmentit

A-taso: Myös alueellisen tai valtakunnallisen häiriön aikana toimivat järjestelmät. Näitä ovat operatiivisesti kriittiset järjestelmät mahdollistavat toiminnan itsenäisenä kokonaisuutena kokonaan ilman ulkopuolista verkkoyhteyttä tai virransyöttöä. Yleensä tämä on HA (High Availability, korkea käytettävyys) -toteutus lähellä keskeistä päivystysyksikköä. Kriittiset palvelut pystytään hoitamaan potilasturvallisuuden vaarantumatta, kuitenkin toiminnan tehokkuus kärsii varautumistilanteessa. **A-tason ytimessä** on ICT välttämättömyydet.

B-taso: Pidentyvän katkon aikana korvattavissa tai lähikonesaliin tuotavissa olevat järjestelmät. Sisältää muissa kuin lähikonesalissa tuotettavat järjestelmät, jotka kriisitilanteessa voidaan tuoda lähikonesaliin tai korvata riittävän nopeasti ”ICT-eristyksen” aikana.



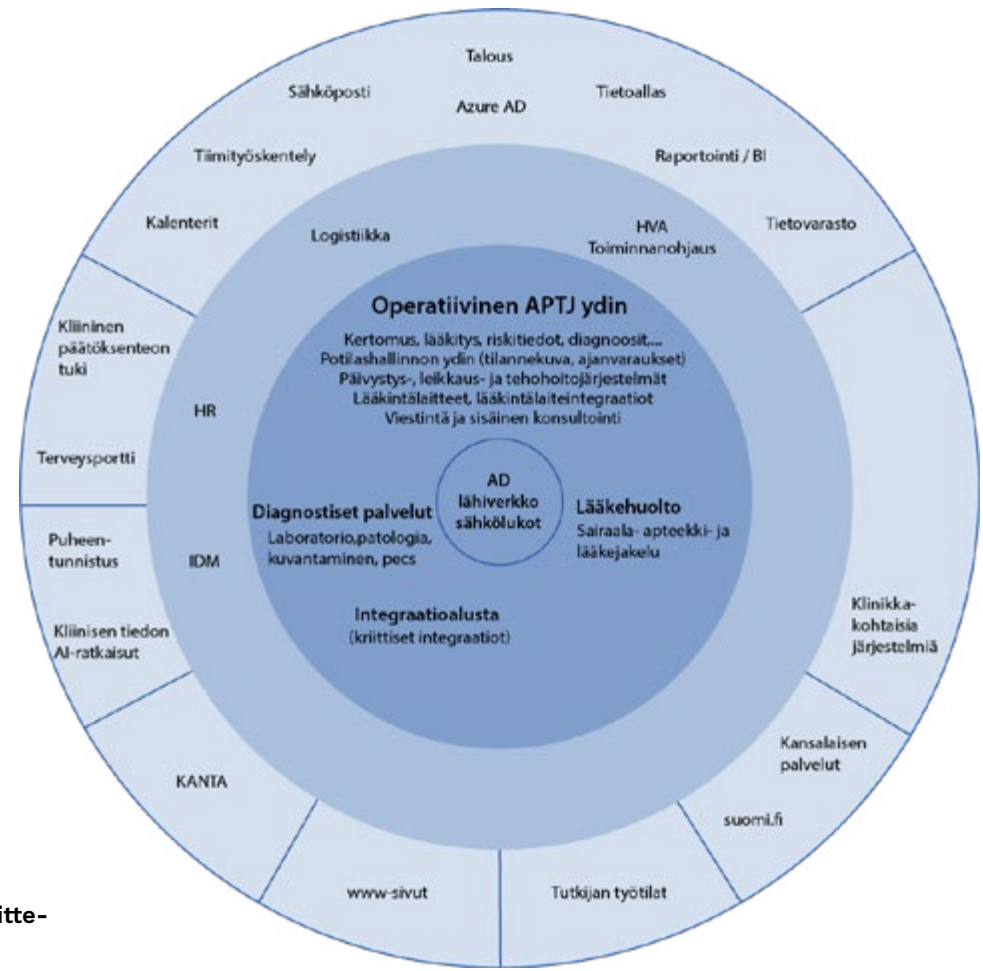
Kuva 6. Eri tuotantosegmentit jatkuvuusanalyysissä.

C-taso: Fyysisesti ja/tai sopimuksellisesti kaukaa toteutetut ratkaisut, ei tuotavissa lähikonesaliin. Sisältää esim. pilvipalvelut, joiden tuominen lähikonesaliin häiriötilanteessa ei ole järkevää tai mahdollista. Näitä ilman on pärjättävä varautumistilanteessa.

6.3.2 Palveluiden sijoittelu sipulimalliin

Keskeiset järjestelmäkokonaisuudet sijoitetaan näille tuotantosegmenteille todellisuutta vastaavasti. Segmenttejä voidaan jakaa erityyppisten ja eri paikoissa sijaitsevien konesalien mukaan alisegmentteihin. Alla olevassa kuvassa on esimerkki sote-järjestelmien jaottelusta eri tuotantosegmenteille. Huomaa, että tämä on esimerkkisijoittelu, ei varsinainen suositus.

Huomaa: Näissä esimerkeissä ei ole otettu kantaa erityisesti ensihoidossa käytettäviin korkean varautumisen ja turvallisuuden palveluiden (TUVE, Virve, Kejo ja Erica) saatavuudelle eri skenaariossa, niiden turvallisuusluokitellun luonteen vuoksi. Ne on kuitenkin syytä huomioida organisaatiokohtaisia riskiarvioita tehtäessä.



Kuva 7. Esimerkki järjestelmien sijoittelusta eri tuotantosegmenteille.

6.3.3 Jatkuvuuden riskiskenaarioiden analysointi

Seuraavilla sivuilla on muutamia esimerkkiskenaariota havainnollistamaan mikä on eri riskiskenaarioiden vaikutus keskeisiin sote-järjestelmiin ja sitä kautta palveluiden saatavuuteen erityisesti pilvipalveluiden näkökulmasta.

Riskiskenaarioiden pohjana käytetään Terveydenhuoltolain sekä Sosiaalihuoltolain määritysten mukaisesti kansallista tai paikallista riskiarviota[75] *(ks. 4.2 Lainsäädäntö-kappaleesta Terveydenhuoltolaki-kohta)*. Tässä kuvatut esimerkkiskenaariot on siis hyvä täydentää päivitetyillä kansallisten ja paikallisten riskiarvioiden mukaisilla skenaarioilla ja niiden variaatioilla.

Nämä kansallisen riskinarvion sisältämät häiriötilanteet on jaettu yhteiskunnan vakauteen, teknologiaan ja logistiikkaan sekä terveysturvallisuuteen liittyviin uhkiin ja laajoihin onnettomuustilanteisiin. Skenaarioita voidaan tarkentaa paikallisesti. Kansallisten ja paikallisten riskiarvioihin pohjautuvien skenaarioiden käyttö mahdollistaa eri alueiden, viranomaisten ja organisaatioiden analyysien ja suunnitelmien yhteensopivuuden, vaikkakin väljänkin. Esimerkkinä tästä esim. Suomi.fi tunnistautumisen riippuvuus kansalaisen palveluihin.

Skenaariossa on häiriön kestolla iso merkitys. Potilaan riskitiedot, diagnoosit ja lääkitys ovat selkeästi kriittisiä heti häiriön ensi hetkillä. Hallinnollisen tiedon ja toimintaa optimoivien järjestelmien merkitys korostuu häiriötilanteen pitkittyessä. Jopa ilman koko APTJ-järjestelmää pärjätään nilkuttaen ainakin useita tunteja toimintaa rajoittamalla. Katkon pitkittyessä tilanne käy kuitenkin nopeasti haastavaksi. Pitemmän päälle jo yksittäisen toimintaa optimoivan järjestelmän puuttuminen voi johtaa puuroutumiseen ja palvelutason laskuun.

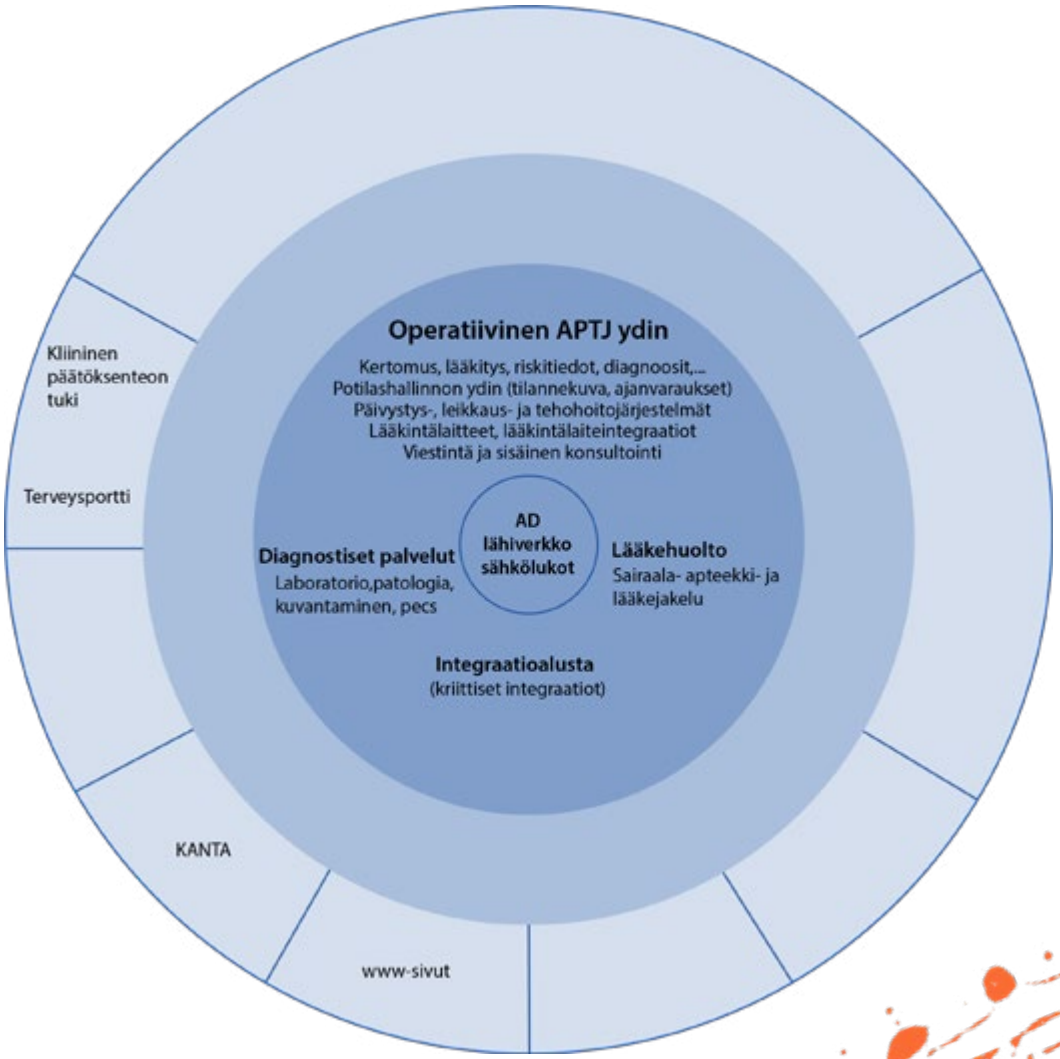
Samoin on arvioitava osaamisen saatavuus eri skenaarioissa, pääseekö ylläpito palvelimiin käsiksi? Yleensä osaamisen varmistaminen on sitä helpompaa, mitä laajemmin käytetystä teknologiasta on kyse. Näihin on helpompi löytää osaajia häiriötilanteissa myös tulevaisuudessa.

6.3.4 Esimerkki skenaario 1: Verkkoyhteydet Suomeen ovat poikki

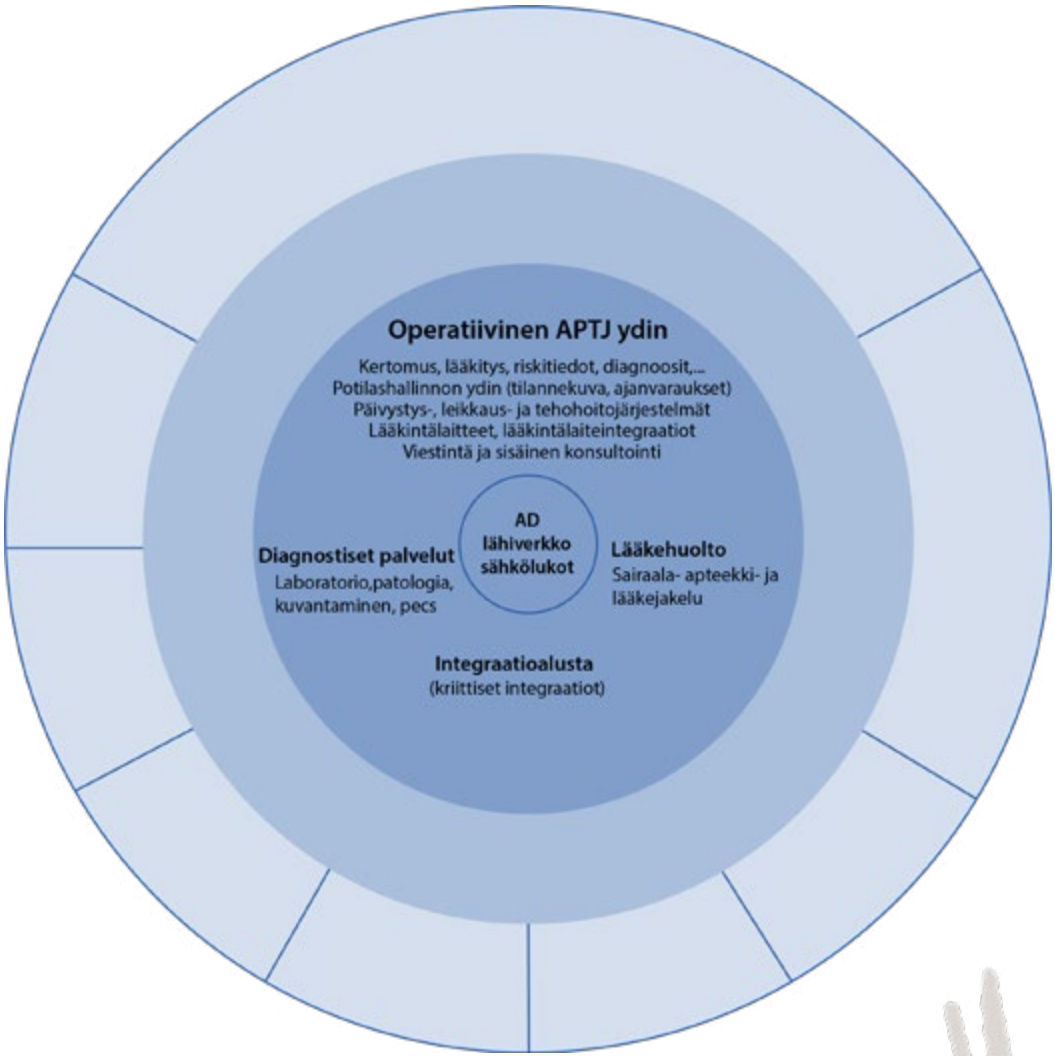
Verkkoyhteydet Suomesta muualle Eurooppaan ovat katkenneet esim. terrori-iskun, kyberhyökkäyksen, teknisen häiriön tai vastaavan vuoksi. Skenaario on ilmeisen harvinainen, mutta otettava huomioon jo edellä mainittujen THL:n Määräysten asettamien vaatimusten vuoksi. Internetin-yhteydet ovat yleensä haavoittuvampia, kuin yksityiset verkkoyhteydet (dedikoitu yhteys).

Variaatiot / työpöytä testaa

1. Voidaanko pitkittyneen katkon aikana tietoliikenne keskeisiin reitittää väliaikaisesti eri reittiä tai esim. satelliittiyhteyden kautta?
2. Onko kriittisimmistä tiedoista ja/tai koko järjestelmästä mahdollista säilyttää kopiota Suomessa? Onko tapaa hyödyntää näitä tietoja? Voisiko palvelu olla pilvipalvelussa Suomessa?
3. Voidaanko jotain toimintoja hoitaa siirtämällä henkilökuntaa ulkomaille käyttämään pilvessä olevia palveluita?
4. Onko palvelutuotanto riippuvainen muiden organisaatioiden tuottamista palveluista, jotka tukeutuvat esim. ulkomailta tuotettuihin pilvipalveluihin?
5. Huomioi myös TUVE, Virve Kejo ja Erica.



Kuva 8. Riskiskenaario: Verkkoyhteydet Suomeen ovat poikki.



Kuva 9. Esimerkki skenaario 2: Sairaalan tietoliikenne on kokonaan poikki

6.3.5 Esimerkki skenaario 2: Sairaalan tietoliikenne on kokonaan poikki

Sairaalan tietoliikenneyhteydet ulkomaailmaan ovat teknisen häiriö, kyberhyökkäyksen, terrori-iskun tai alueellinen sähkökatko vuoksi poikki. Teknisessä häiriössä esim. pääyhteys katkeaa samaan aikaan kun varayhteyttä huolletaan.

Variaatiot / työpöytä testaa

1. Miten pärjätään ilman Kanta-yhteyttä? Tiedottamisen hoitaminen?
2. Onko mobiiliverkko käytettävissä? Voidaanko sitä kautta ohjata ammattilaiset kännykällä pilvessä olevan intran, tiedotussivun sekä muiden pilvipalveluiden käyttöön? Voidaanko tietoliikenne keskeisiin pilvipalveluihin reitittää väliaikaisesti mobiiliverkon kautta?
3. Osa diagnostisista palveluista ei käytettävissä, koska ostotoimintana HL7 liittymän varassa? Mitkä integraatiot eivät toimi, vaikutus toimintaan?
4. IDM, saadaanko keikkatyöntekijöille tunnuksia järjestelmään?
5. Variaatiossa vain osa verkkoyhteyksistä, esim. Internetin kautta tuotettavat SaaS-palvelut eivät toimi, mutta dedikoitu yhteydet pilvipalvelualustoihin toimivat.
6. Huomioi myös TUVE, Virve Kejo ja Erica.

6.3.6 Esimerkki skenaario 3: Lähikonesali ei käytettävissä

Lähikonesalin laitteissa, ohjelmistoissa, virransyötössä tai verkkoyhteyksissä on tekninen vika tai on tapahtunut kyberhyökkäys, terrori-isku tai muu katastrofaalinen paikallinen ongelma. Myös pitkäkestoiset APTJ käyttökatkot johtavat jo lähelle tätä skenaariota, tosin yleensä ennakoidusti ja rauhallisimpaan mahdolliseen aikaan. Havaitaan että pilvipalvelut tuovat hajautuminen myötä hyödyllistä vikasietoisuutta ja mahdollisuuksia jatkaa toimintaa, vaikkakin rajoitetusti.

Variaatiot / työpöytä testaa

1. Onko ylläpidon tiedot ja dokumentit saatavilla?
2. Poistuuko verkon palveluita kuten DNS (Domain Name System) ja DHCP (Dynamic Host Configuration Protocol) käytöstä? Onko nämä saatavissa työasemille myös pilvestä?
3. Onko syytä varautua pilvipalveluiden käyttöön kännykkäliittymien avulla?
4. Voiko lähikonesalin järjestelmien vikasietoisuutta lisätä pilvikopiolla?
5. Onko sähköinen kulunhallinta tai sen ylläpito riippuvainen lähiverkosta?
6. Onko kansalaisen palvelut riippuvaisia lähikonesalin tiedoista?
7. Tukeutuuko pilvipalveluiden potilasvalinta lähikonesalin järjestelmiin?
8. Onko variaatioita, joissa osa lähikonesalin palveluista on käytössä?
9. Onko AD pois käytössä? Tämä voi estää kirjautumisen myös pilvipalveluihin, riippuen AD ja AAD integroivassa ”Hybrid identity”[76] ratkaisusta?
10. Missä määrin esim. Kanta-palvelu voi toimia varmistavana ratkaisuna tässä tilanteessa, mitä se mahdollistaa? Mihin kirjataan tiedot?
11. Huomioi myös TUVE, Virve Kejo ja Erica.

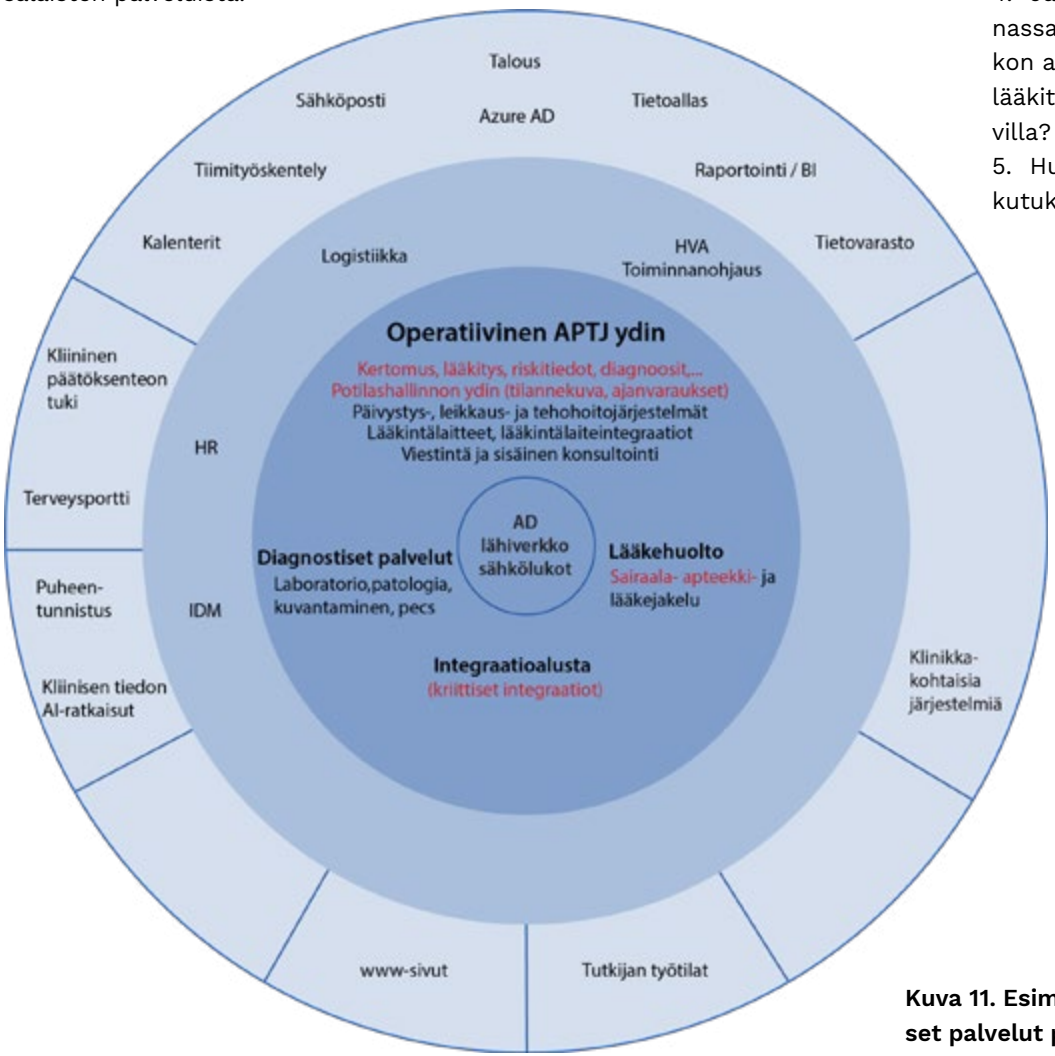
Kuva 10. Esimerkki skenaario 3: Lähikonesali ei käytettävissä

6.3.7 Esimerkki skenaario 4: Kansalliset palvelut pois käytöstä

Kansalliset palvelut kuten Kelan Kanta-palveluissa sekä Suomi.fi on käyttökatko esim. kyberhyökkäyksen, virransyötön ongelmien tai teknisten häiriöiden vuoksi. Tämä aiheuttaa *kaikkiin Suomen APTJ järjestelmiin* hitautta ja joihinkin käyttökatkoja, riippuen sovellusarkkitehtuurista. Suomi.fi palvelun käyttökatko vaikuttaa valtaosaan kansalaisten palveluista.

Variaatioita / työpöytä testaa

1. Tunnistaako APTJ-järjestelmät Kantan ongelmatilanteet mukautuen tilanteeseen, vai hidasteleeko APTJ? Tukeeko Kanta palvelut tätä tuottamalla tilatietoa palveluidensa tilasta API:n kautta?
2. Tahdonilmaisut (luovutusluvat, luovutuskiellot ja hoitotahto) eivät ole käytettävissä
3. Riskitiedot eivät päivity Kannan kautta muilta palveluantajilta.
4. Jatkossa avolääkitys vain Kannassa? Voiko käydä niin että katkon aikana potilaiden ajantasaista lääkitystä ei ole kliinikoiden saatavilla?
5. Huomioi myös mahdolliset vaikutukset Kejoon.



Kuva 11. Esimerkki skenaario 4: Kansalliset palvelut pois käytöstä.

7 Yhteenveto

Pilvisiirtymä etenee julkishallinnossa EU:ssa sekä Suomessa kiihtyvällä vauhdilla ja SaaS-palvelumalli jatkaa yleistymistään. Hyperskaalautuvat pilvipalvelujen skaalaedut ja SaaS-palvelumalli mahdollistavat hyötyjä, joita ei voida saavuttaa pienemmissä mittakaavoissa perinteisimmillä tuotantomalleilla. Suomen sote-sektorin ei ole varaa jättäytyä / joutua jäämään näiden megatrendien ulkopuolelle.

Sopimuksellisten haasteiden juurisyynä on palveluiden kansainvälistyminen, eurooppalaisen hyperskaalautuvan pilviteknologian kehittymättömyys ja kansainvälisen lainsäädännön edelleen kehittyvät EU-tason tulkinnat. Pilvialustojen toimittajat ovat sitoutuneet toimimaan EU:n lakien mukaisesti, aivan kuten perinteisempiinkin tuotantomalleihin tekniikkaa ja palveluita toimittavat kansainväliset yritykset. Haastetta tuo, että he toimivat myös kotimaansa lakien mukaisesti, jotka voivat nyt tai tulevaisuudessa olla ristiriidassa EU:n lakien kanssa.

Kivijalka pilvelle

(ks. ”2 Nykytilanne, mahdollisuudet ja kehityssuunta” ja ”3 Pilvistrategia”)

1. Luokaa organisaatiolle pilvistrategia (pilvilinjaukset) tukeutuen myös kansallisiin pilvilinjauksiin (VM), yhteisesti hyväksytyt linjausten tuovat selkänojaa. Päivittäkää linjauksia matkan edetessä.
2. Kehittäkää omaa ja organisaation pilviosaamista pitkäjänteisesti. Tunnistakaa kokeneen pilvikumppanin tarve. Pilvisiirtymä on suuri muutos, joka vaatii aidosti uudenlaista osaamista. Rakentakaa osaamista myös ratkaisujen riskianalyysien ja hankintojen tekoon.
3. Rakentakaa alusta alkaen kattava hallintamalli pilvipalvelualustoille, hyödyntäen alustojen valmiita parhaita käytäntöjä.

Sääntely: Sote-tiedon julkisuusluokat

(ks. ”4.4 Sote-tiedon julkisuusluokat”)

4. Sote-tiedot ovat isolta osin asiakastietoa, joka on *salassa pidettäviä sosiaali- ja terveydenhuollon henkilötietoja*. Tämän lisäksi käsitellään paljon myös muuta henkilötietoa. Sote-asiakastiedot eivät ole *turvallisuusluokiteltavia asiakirjoja*. Organisaatioilla on yleensä myös rajatusti turvallisuusluokiteltavia asiakirjoja käytössä mm. varautumiseen liittyen, joiden käsittely on huomioitava erikseen.
5. Pilvipalveluissa dataa suositellaan säilyttämään pääosin pseudonymisoituna, tämä on tapa toteuttaa GDPR mukaista *sisäänrakennettua tietosuojaa* teknisenä suojamekanismina. Pseudonymisoitu asiakastieto on kuitenkin yhä asiakastietoa.

Sääntely: Pilvipalveluiden käytön mahdollisuus

(*ks. ”4 Sote-pilvipalveluiden sääntely”*).

6. VM:n linjaukset suosittelevat pilvipalveluiden käyttöä julkishallinnossa aina ensisijaisesti, kun ne ovat paras ratkaisu tarpeeseen.
7. Sääntelyssä ei lähtökohtaisesti erotella pilvipalveluita ja perinteisempiä palvelu- ja tuotantomalleja. Samat perusvaatimukset koskevat pilvessä, ulkoistetuissa konesalissa sekä omassa konesalissa tuotettuja järjestelmiä.
8. Sääntelyssä ei oteta erityisesti kantaan puoleen-tai-toiseen pilvipalveluiden hyödyntämiseen salassa pidettävän sosiaali- ja terveydenhuollon asiakastietojen käsittelyssä. Pilvipalveluiden käytölle ei siis ole kategorista estettä.
9. Sääntelyssä korostuu ratkaisun riskipohjainen arviointi.
10. Jatkuvuuden varmistamiselle asetetaan erityisiä kansallisia vaatimuksia julkisen terveydenhuollon ensihoidon ja päivystyksen toteuttamiseen tarvittavien järjestelmien osalta (ns. ”A3 kriittiset”). Näiden järjes-

telmien osalta on varmistettava ”jatkuva toimivuus tai viiveetön palauttaminen toimivaksi mahdollisimman nopeasti” myös silloin, kun verkkoyhteydet ovat rajoittuneet ainoastaan Suomen rajojen sisäpuolelle. Tämä on otettava huomioon pilvipalveluiden käytössä ja/tai ratkaisun toteutuksessa. ks. ”4.2 Lainsäädäntö” kohdasta THL:n määräykset.

Sääntely: Tiedon ja palvelun sijainti

(*ks. ”4 Sote-pilvipalveluiden sääntely”*).

11. Sääntely ei eroa sen suhteen talletetaanko ja käsitelläänkö tietoa Suomessa vai muualla EU/ETA-alueella. EU/ETA alueella henkilötietojen vapaa liikkuvuus on taattu GDPR:n avulla.
12. Henkilötietojen käsittely ja tallentaminen on mahdollista myös EU/ETA-alueen ulkopuolella, kun GDPR:n vaatimukset huomioidaan (ks. ”Sopimukset ja riskiarviot” alta).
13. Myös tulevaisuuden kansainvälisen lainsäädännön riskien hallittavuuden vuoksi suositellaan rajaamaan käsittely EU/ETA-alueelle aina kun mahdollista.

Luottamuksellisuuden varmistaminen pilvessä

(ks. ”4.2 Lainsäädäntö” ja ”5 Luottamuksellisuuden varmistaminen pilvessä”)

14. Vaatimustenmukaisuuden todentaminen on erilaista pilvipalveluissa, kuin perinteisimmissä palvelu- ja tuotantomalleissa. Sopimusten, tietoturvakuvausten, ratkaisukuvausten, riskiarvioiden ja hallintamallin rooli korostuu pilvipalveluita hankittaessa.
15. Pilvipalvelun toimittajan yksipuolisilta sopimusmuutoksilta tai niiden vaikutuksilta tulee mahdollisuuksien mukaan suojautua, aivan kuten muissakin sopimuksissa. Osa suojautumista on myös arvioida pilvestä poistumisen tai pilvipalvelun vaihtamisen kustannuksia tekemällä ”exit plan”.
16. Myös pilvipohjaisille ratkaisuille tarvitaan tavanomaiset sote-järjestelmän luokittelun mukaiset kuvaukset ja sertifioinnit (tiedonhallintalaki, asiakastietolaki, MDR).
17. GDPR vaatimusten huomioiminen pilvipalveluissa tiivistettynä:
    - Aina henkilötietoja käsiteltäessä (EU/ETA-alueen sisälläkin) täytyy:
      i Olla **henkilötietojen käsittelyperuste**
      ii **Tehdä DBA** (Data Processing Agreement) -sopimus henkilötietojen käsittelystä rekisterinpitäjän ja käsittelijän/käsittelijöiden välille
      iii **Arvioida henkilötiedon käsittelyyn liittyviä riskejä.** Mahdollinen käytettävissä oleva työkalu riskien arviointiin on tietosuojan vaikutuksenarviointi (DPIA, Data Protection Impact Assessment). DPIA käyttäminen ei ole kuitenkaan kaikissa tilanteissa pakollista, vaikka riskien arviointi onkin pakollista.
    - Lisäksi kun tietoja siirretään (käsitellään) EU/ETA-alueen ulkopuolelle, esim. USA:ssa, on lisäksi oltava **siirtoperuste***, käytännössä yleensä:*
      iv Käytettävä **EU:n vakiolausekkeita** (SCC, Standard Contractual Clauses)
      v Pohdittava **tapauskohtaisten lisäsuojamekanismien tarve** tekemällä tapaus- ja maakohtainen **TIA-riskiarvio** (Transfer Impact Assessment).
      vi Mahdollisesti **TIA-riskiarvion** pohjalta toteuttaa **lisäsuojamekanismeja** tarkentamalla sopimusehtoja sekä ratkaisun teknisiä- ja organisaationaalisia suojatoimia.
18. Teknisten ja organisatoristen (lisä)suojamekanismien huomioiminen
    - Ratkaisukohtaisesti määriteltäviä käsiteltävän tiedon, käytettävien pilvipalveluiden ja riskiarvion perusteella.
    - Ks. 5.2 ”Tekniset ja organisatoriset suojaukset” (sis. myös tiedonsiirron suojaamisesta).

Pilvi ja jatkuvuudenhallinta

(ks. ”6 Pilvi ja jatkuvuudenhallinta” ja ”5 Sote-pilvipalveluiden sääntely”)

19. Soveltamisohjeessa on esitetty järjestelmien luokittelu neljälle eri kriittisyysluokkaan jatkuvuuden kriittisyyden analysoinnin tueksi. Käytännössä integraatiot

ja riippuvuudet voivat tehdä ei-kriittisestä osajärjestelmästä kriittisen teknisten riippuvuuksien vuoksi. Ks. ”6.1 Järjestelmäluokittelu jatkuvuudenhallinnan kannalta”

20. Pilvipalveluiden yleistyessä ja ICT:n hajautuessa korostuu jatkuvuudenhallinnassa kokonaisuuden skenaariopohjainen riskianalyysi pohjautuen kansallisiin ja alueellisiin riskiarvioihin. Hyödynnä soveltamisohjeessa esiteltyä sipulimallia pilvipalvelut huomioivaan riskiskenaarioiden analyysiin ja kommunikointiin sidosryhmille. Havaitaan että pilvipalvelut tuovat usein parempaa kriisinsietokykyä kokonaisarkkitehtuuriin, mutta myös hallittavia riskejä, riippuen riskiskenaariosta. ks. ”6.3 Pilvipalvelut huomioiva riskiskenaarioanalyysi”
21. Huomioikaa myös taloautomaation ja muut IoT-pilviratkaisut osana jatkuvuudenhallinnan riskianalyysiä.

8 Käsitteistöä

AD ja AAD	Active Directory (AD) on Microsoftin tuottama palvelu, jolla hallitaan mm. käyttäjiä ja käyttöoikeuksia. Käytännössä käytössä lähes poikkeuksetta kaikissa sote-organisaatioissa Suomessa. Azure Active Directory (AAD) on Microsoftin Azuressa AD:n vastine, joka on (lähes) kaikkien heidän pilvipalveluiden taustalla. AAD yleensä liitetään organisaation sisäverkossa olevaan AD:hen, kun Microsoftin pilvipalveluita otetaan käyttöön (esim. Office 365 käyttöönoton yhteydessä). AAD lisensointi on huomioitava pilvisiirtymässä.
API (Application Programming Interface)	Sovelluksen tarjoama ohjelmallisesti kutsuttava rajapinta, jota toiset sovellukset voivat käyttää suorittaakseen eri tehtäviä tai saadakseen haluamaansa dataa.
APTJ (asiakas- ja potilastietojärjestelmä)	Sosiaali- ja terveydenhuollon asiakastietojen käsittelyn ydintietojärjestelmäkokonaisuus.
AWS (Amazon Web Services)	Amazonin hyperskaalautuva pilvialusta. Markkinajohtaja maailmanlaajuisesti. Lähimmät konesalit Ruotsissa ja Keski-Euroopassa. Kevyempi Local Zone -konesali tulossa Suomeen 2022 (Outpost-tekniikkaan perustuva, riippuvuus täysveriseen konesaliin esim. Ruotsissa). Suora verkkoliikenteen yhteyspiste konesaleihin Helsingistä. (tilanne Q1/2022)
Azure	Microsoftin toimittama yleisesti käytetty hyperskaalautuva pilvialusta. Laajasti käytössä suomessa sote-sektorilla. Lähimmät konesalit Norjassa ja Ruotsissa sekä Keski-Euroopassa. Office 365 osalta myös Suomessa. Oma suora yhteyspiste konesaleihin Helsingistä tulossa, tällä hetkellä kumppanin kautta. (tilanne Q1/2022)
DDoS (Distributed Denial of Service)	Palvelunestohyökkäys (DoS) on verkkohyökkäys, jossa pyritetään estämään verkkopalvelun tarkoitettu käyttö lähettämällä verkkopalveluun niin paljon liikennettä, että tämä ei kykene palvelemaan asiakkaitaan. Hajautetussa palvelunesto hyökkäyksessä (DDoS) hyödynnetään usein kaapatuista tietokoneista muodostettuja bottiverkkoja, jolloin hyökkäys on hankalammin torjuttava.
Dedikoitu yhteys	Dedikoitu yhteys tarkoittaa operaattorin tietylle asiakas organisaatiolle varattua kiinteää tietoliikennekaistaa, johon muiden asiakkaiden käyttö ei vaikuta. Yksittäiseen tiedonsiirron nopeuteen vaikuttaa tällöin kyseisen asiakasorganisaation sen hetkinen oma käyttö, ei muiden asiakkaiden vaikeasti ennustettava käyttö. Vastakohta on tavanomainen Internetin tietoliikenne, jossa kaikkien muiden internetin käyttö voi vaikuttaa tiedonsiirron nopeuteen.
DevOps	

Disaster recovery, DR	Käytännöt, työkalut ja menetelmät, joiden avulla mahdollistetaan palveluiden toipuminen odottamattomasta tuotannon / palvelut pysäyttäneestä ongelmasta. DR:n yhteydessä yleensä, vikaantunutta järjestelmää tai sen osaa ei saada nopeasti käyttökuntoon, vaan on turvauduttava esim. tietojen palauttamiseen, uudelleenasennuksiin ja/tai siirryttävä käyttämään varalla olevaa järjestelmäasennusta. Disaster recoveryä kutsutaan suomeksi usein toipumissuunnitelmaksi, DR-termiä käytetään kuitenkin suunnittelun lisäksi kuvaamaan myös varsinaista toipumistoimintaa. Ks. myös korkea käytettävyys (High availability, HA).
DLP, Data Loss Prevention	Teknologioita arkaluonteisten tietojen menetyksen estämiseen. Niiden avulla voidaan luokitella tietoa ja tietolähteitä niiden luottamuksellisuuden mukaan. Tunnistaminen on usein osittain automaattista kyeten esim. tunnistamaan henkilöiden yksilöiviä tietoja materiaaleista. Luokittelujen perusteella organisaatio voi rajata tiedon käyttöoikeuksia ja julkaisumahdollisuuksia sen arkaluonteisuuden mukaan. DLP on tapa toteuttaa *sisäänrakennettu ja oletusarvoista tietosuojaa*.
Skaalautuminen, dynaaminen ja automaattinen skaalautuminen (Dynamic scaling, auto scaling)	Skaalautuminen on ratkaisun kyky sopeutua järjestelmän tai sen osan käyttömääriin. Skaalautumista toteutetaan lisäämällä ja poistamalla palvelusta resursseja. Ylöspäin skaalautumisessa lisätään resursseja, alaspäin skaalautumisessa vähennetään resursseja. *Vertikaalisessa skaalautumisessa* lisätään olemassa oleviin palvelimien resursseja (CPU, muisti), *horisontaalisessa skaalautumisessa* lisätään infrastruktuuriin uusia palvelimia auttamaan kuormituksenkäsittelyssä. Dynaaminen skaalautumien tarkoittaa kuormitukseen mukautuvaa skaalautumista, ts. resursseja lisätään ja poistetaan palvelutarpeen mukaan. Tämä voi tapahtua ajastetusti, esim. niin että kuormahuipun kohdalla työaikana resursseja on enemmän ja öisin hyvin vähän. Automaattinen skaalautuminen voi tapahtua myös esim. prosessorikuormituksen kohoamisen (ja laskemisen) perusteella, myös ennakoimattomissa tilanteissa esim. nopeasti eskaloituvassa kriisitilanteessa tms.
Suuruuden ekonomia (economies of scale)	Palvelun tuottamisen yksikkökustannukset pienenevät, kun samaa palvelua tuotetaan suurissa määrin jopa tuhansille tai miljoonille asiakkaille. Hyöty kertyy investointien jakamisen, automatisoinnin tehokkuuden ja erikoistumisen kautta.
Reunalaskenta (Edge computing)	Reunalaskenta. Ks. Pilven tuotantomalli -kappale.
Egress	Pilvestä poispäin kulkeva tietoliikenne. Tästä menee pilvipalvelualustoilla yleensä erillinen maksu siirrettävän datan määrän mukaisesti. Kustannus voi isoilla tietomäärillä nousta merkittäväksi.
Follow-the-sun	Palveluiden ylläpitoon ja tukeen kehitetty järjestely, jossa eri puolella maapalloa toimivat tiimit tekevät yhteistyötä esim. peräkkäisenä kolmivuorotyönä siten, että jokainen tiimi työskentelee omaan päiväaikaansa. Palvelun tuottaminen seuraa aurinkoa maapallon ympäri. Tällä saavutetaan mm. kustannustehokkuutta.
GCP, Google Cloud Platform	Googlen hyperskaalautuva pilvialusta. Lähin konesali Haminassa. Suora yhteyspiste Haminan konesaliin saatavilla Suomen sisältä. Suora yhteyspiste muihin konesaleihin Helsingistä. https://cloud.google.com/about/locations (tilanne Q1/2022)

HVA	Hyvinvointialue
Hybrid cloud	Ks. Pilven tuotantomalleja
Hyperskaalautuminen	Ks. Pilven tuotantomalleja
IaaS, PaaS, Saas	Pilvipalvelumalleja, ks. Palvelumallit -kappale.
Ingress	Pilveen sisäänpäin menevä tietoliikenne. Usein sisäänpäin kulkevasta liikenteestä ei mene pilvipalvelualustoilla erillistä maksua.
Kapasiteetti	Kapasiteettia tarkoittaa yksinkertaistettuna palvelimen prosessoritehoa (laskentakapasiteetti), tiedon tallennustilaa (tallennuskapasiteetti) tai tiedonsiirtokapasiteettia. On myös muita kapasiteettityyppejä, kuten sanomanvälityskapasiteetti. Käytännössä siis yleensä fyysisen palvelimen, kovalevyn tai tietoliikenneyhteyden korvaaja virtualisoidussa nykymaailmassa. Kapasiteettia voidaan pilvipalveluissa ostaa yleensä tarpeen mukaan tuntihinnalla, vähän kuten sähköä sähköyhtiötä.
Kasaumavaikutus	Kasautumisvaikutuksessa on kyse ilmiöstä, jossa suuri määrä tietoa voi muodostaa yksittäisiä tietoja merkittävämmän asiakokonaisuuden. Tällöin suojaamistarpeet voivat erota yksittäisten tietoalkioiden luokittelusta ja suojaamistarpeista. Määrä ei ole ainoa tekijä, vaan joskus esimerkiksi kahden eri tietolähteen yhdistäminen voi johtaa merkittävän kasaumavaikutuksen syntymiseen. Kasautumisvaikutuksen arviointiin ei tunneta yleistä, kaikkiin tilanteisiin sellaisenaan sopivaa laskentatapaa, mikä hankaloitta kasaumavaikutuksen riskiarviointia. Terveydenhuollon datoissa kasaumavaikutuksen rinnalla on tiedostettava kliinisen asiakastiedon anonymisoinnin ja pseudonymisoinnin haastavuus mm. hyvin yleisten harvinaisten sairauksien kohdalla.
Konesali, palvelinkeskus, datakeskus (data center)	Konesali (datakeskus, palvelinkeskus, data center) sijainti, rakennus tai huone, joka on omistettu suuria määriä dataa käsitteleville tietokoneille ja niiden oheislaitteille. Pieniä palvelinkeskuksia tavataan kutsua myös serverihuoneiksi (server room). Samassa konesalissa on nykyisin jopa satojatuhansia palvelimia konesaleihin erikoistuneiden toimijoiden tiloissa. Pilvipalvelukin sijaitsee käytännössä jollain paikkakunnalla olevassa konesalissa, pilven yhteyksissä konesalien sijainneista käytetään nimeä ”region”.
Region	Pilvipalveluiden sijainnit joista pilvipalveluita ostetaan. Yleensä kuhunkin regioonaan kuuluu kaksi tai useampi eri sijainnissa oleva konesali, ns. Availability Zone tuomaan vikasietoisuutta kokonaisen konesalin tasoisen häiriön varalta. Pilvipalvelualustoilla voidaan myös varautua kokonaisen regioonan häiriöön, hajauttamalla palveluita useammalle regioonalle maailmanlaajuisesti. Ks. esim. AWS Regions[77], Azure Regions[78], GCP locations[79] ja Oracle Cloud[80].
Kontti, konttiteknologiat, kontitus	Konttiteknologialla viitataan tavaralogistiikkaa aikanaan mullistaneeseen ajatuksen tavaroiden liikuttamisesta standardoiduinta yksikköinä eli kontteina soveltamisesta ICT ratkaisuihin. Konttiratkaisussa sovellus on paketoitu teollisuusstandardiksi kontiksi (Docker tai Kubernetes container), joka voidaan ajaa eri valmistajien alustoilla esim. eri pilvessä tai omassa lähikonesalissa. Kyseessä on tietynlainen sovelluksen virtualisointiratkaisu. Konttien hyödyntämisellä voidaan osittain vähentää riippuvuutta tietystä valmistajasta ja pilvipalvelusta.

Korkea käytettävyys, korkea saatavuus (high availability, HA)	Suunnittelu käytäntö, joka pyrkii varmistamaan, että järjestelmä on aina käytettävissä. HA suunnittelulla pyritään minimoimaan suunnittelemattomien katkojen määrä ja kesto. Menetelminä on mm. yksittäisen yhden pisteen virheet infrastruktuurissa; yksittäisen pisteen virheet jotka aiheuttavat palvelun saatavuuden menettämisen. Ratkaisuna on yleensä eri järjestelmän ja infrastruktuurin osien kahdentaminen, jolloin toisen komponentin vikaantuessa toiminta jatkuu toisen komponentin varassa. Saatavuutta mitataan ja määritellään SLA:ssa (Service Level Agreement) prosentteina ajasta, esim. 99,9% tarkoittaa n. 9 tunnin katkoa vuodessa ja 99,999% (”viiden ysin”) HA-tason järjestelmässä saa olla vain n. 5 minuutin katko koko vuoden aikana.
latenssi	Tietoliikenteen viive, joka aiheutuu pitkillä välimatkoilla valonnopeuden rajallisuudesta sekä verkkolaitteiden (kuten reitittimet) aiheuttamasta viiveestä.
Lift-and-shift (nosta-ja-siirrä)	Lähikonesalin palvelinten ja niiden tarjoamien palveluiden siirtämistä sellaisenaan toiseen konesaliin, yleensä hyperskaalautuvaan pilvipalvelun IaaS alustalle ilman järjestelmämuutoksia. Siirto toteutetaan usein samoja virtualisointiratkaisuja hyödyntämällä pilvessä, kuin lähikonesalissakin.
lähikonesali	Lähikonesali on sote-organisaation itseylläpitämä (onprem) tai ulkoistettu (hosted-onprem) konesali(t), yleensä lähellä sote-organisaation keskeisintä toimipistettä, kuten päivystysvastuullista sairaalaa.
OCI, Oracle Cloud Infrastructure	Oraclen hyperskaalautuva pilvialusta. Myös Oraclen sovellus- ja teknologiapilvi-palvelut ovat laajasti Suomessa SOTE-sektorilla käytössä. Lähimmät konesalit ovat Ruotsissa ja muissa EU/ETA-maissa. Kyky myös toimittaa vastaavia pilvipalveluja Suomesta asiakkaan määrittelemästä konesalista, jota jo hyödynnetään Suomessa SOTE-sektorilla. (tilanne Q1/2022)
onprem, hosted-onprem	Perinteisiä järjestelmien palvelumalleja, ks. Palvelumallit -kappale.
Pay as you go	Pilvipalveluissa yleinen malli, jossa kustannuksia kertyy sen mukaan, paljonko palveluita käytetään. Esim. kustannuksia kertyy sitä enemmän mitä enemmän palvelimia (laskentakapasiteettia) on käytössä pilvessä.
Pilvimigraatio	Perinteisillä tuotantomalleilla tuotettujen järjestelmien ja palveluiden siirtäminen pilveen. Pilvimigraatioon on eri tyyppisiä vaihtoehtoja, mm. lift-and-shift siirto, järjestelmän ja datojen migraatio järjestelmän uuteen pilviversioon (vrt. versiopäivitys), järjestelmän uudelleentoteutus kokonaan tai osittain, sekä järjestelmän vaihtaminen kokonaan uuteen järjestelmään.
Sisäänrakennettu ja oletusarvoinen tietosuoja (Data Protection by Design and Default)	GDPR:n mukainen henkilötietojen käsittelyperiaate[81] ja velvollisuus[82]. Teknisiä ja organisatorisia toimenpiteitä käsittelytoimintojen suunnittelun alkuvaiheessa, jotta yksityisyys- ja tietosuojaperiaatteita suojellaan alusta saakka. Organisaatioiden on oletusarvoisesti varmistettava, että henkilötiedot käsitellään korkea yksityisyyden-suoja varmistaen. Esimerkiksi vain välttämättömiä tietoja olisi kerättävä ja käsiteltävä, lyhyt säilytysaika, rajoitetut käyttöoikeudet, automaattinen poistaminen.

Skaalautuminen, dynaaminen skaalautuminen	Pilvipalveluissa skaalautumisen avulla voidaan joko automaattisesti tai manuaalisesti lisätä (ja vähentää) kapasiteettia (palvelimia) tarpeen mukaan sovelluksen kuormituksen muuttuessa. Dynaaminen skaalautuminen tarkoittaa skaalautumista automaattisesti esim. palvelun kuormituksen mukaan.
SSO, Single-Sign-On	SSO on ratkaisu, jonka ansiosta käyttäjän ei tarvitse kirjautua kymmeniin eri ohjelmiin erikseen, sen sijaan kerran tehty kirjautuminen välitetään toisille sovelluksille erilaisilla teknisillä ratkaisuilla.
Tietoallas (datalake)	Tietoallas on tapa ja teknologia kerätä eri järjestelmien (tietokantojen, tiedostojen) tiedot keskitettyyn paikkaan lähdejärjestelmän tarjoamassa muodossa. Tietoaltaassa eri lähteistä tulevat tiedot voidaan jatkojalostaa sekä yhdistää keskenään mm. tietojohtamisen, tutkimuksen sekä analytiikan tarpeisiin. Tietoallas toteutetaan usein hyperskaalautuvaan pilvipalveluihin ja muodostaa data-alustan ytimen.
Tietoturvallinen käyttöympäristö	Findatan toisiolain määräysten mukainen tekninen ympäristö, jossa esim. tutkijat käsittelevät heidän käyttöönsä toimitettua dataa tietoturvallisesti.
TLS, Transport Layer Security	TSL on salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne. Aiempi versio on tunnettu nimellä Secure Sockets Layer (SSL). Se on nykyisin yksi tavallisimpia tapoja suojata tietoliikennettä. Tavallisin TLS:n käyttötapa on suojata verkkosivujen siirtoa HTTPS-protokollalla, mitä mm. verkkopankit yleisesti käyttävät.
Toimialariippumaton järjestelmä	Järjestelmät, joita voidaan käyttää eri toimialoilla. Järjestelmät eivät siis ole esim. sote-spesifisiä tietojärjestelmiä. Nämä ovat usein valmisohjelmistoja. Esim. taloushallinnon, logistiikan, henkilöstöhallinnon, hallinnon, sähköposti- ja toimistosovellukset sekä tietohallinto.
VPN	Virtual Private Network on tietoturvallinen verkkoyhteys, jossa kaikki tietoliikenne liikkuu salattuna. Kyseessä on virtuaalinen verkkoyhteys, tarkoittaen että muodostaa yleensä julkisen internetin läpi virtuaalisen turvallisen ”tietoliikenneputken” jonka sisällä kulkevaa tietoa muut eivät näe.

Loppuviitteet

1 Tuottavuutta pilvipalveluilla: Ohje julkisen hallinnon pilvipalvelujen hyödyntämiseen, kappale 3 http://urn.fi/URN:ISBN:978-952-367-327-4
2 https://customers.microsoft.com/en-us/story/772376-ottawahospital-healthprovider-azure-canada
3 http://urn.fi/URN:ISBN:978-952-367-327-4
4 http://urn.fi/URN:ISBN:978-952-367-503-2
5 http://urn.fi/URN:ISBN:978-952-251-982-5
6 https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/
7 https://cloud.google.com/adoption-framework
8 https://www.oracle.com/cloud/cloud-adoption-framework/
9 https://aws.amazon.com/professional-services/CAF/
10 https://docs.microsoft.com/fi-fi/learn/certifications/azure-fundamentals/
11 https://www.cloudskillsboost.google/course_templates/60
12 https://aws.amazon.com/getting-started/fundamentals-overview/
13 https://education.oracle.com/learning-explorer
14 https://www.finlex.fi/fi/laki/ajantasa/2021/20210784
15 https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset
16 https://www.finlex.fi/fi/laki/ajantasa/2019/20190552
17 https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32016R0679
18 https://www.finlex.fi/fi/laki/ajantasa/2018/20181050
19 https://tietosuoja.fi/kasittelyperusteet
20 https://tietosuoja.fi/arvioi-riskit
21 https://tietosuoja.fi/vaikutustenarviointi
22 https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle
23 https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fi.pdf
24 https://tietosuoja.fi/komission-hyvaksymat-vakiolausekkeet
25 https://tietosuoja.fi/tiedonsiirtovalineita-taydentavat-suojatoimet
26 https://www.finlex.fi/fi/laki/ajantasa/2010/20101326
27 https://valtioneuvosto.fi/-/1271139/lakimuutosten-myota-sosiaali-ja-terveydenhuollon-varautuminen-hairio-ja-uhkatilanteisiin-paranee
28 https://www.finlex.fi/fi/laki/ajantasa/1992/19920785
29 https://www.finlex.fi/fi/laki/ajantasa/1999/19990621
30 https://www.finlex.fi/fi/laki/ajantasa/2019/20190906
31 https://vm.fi/tiedonhallintalaki
32 https://www.fimea.fi/laakinnalliset_laitteet/
33 https://www.finlex.fi/fi/laki/ajantasa/2021/20210719
34 https://www.fimea.fi/laakinnalliset_laitteet
35 https://www.finlex.fi/fi/laki/ajantasa/2011/20111406
36 https://www.finlex.fi/fi/laki/ajantasa/2017/20170583
37 https://www.finlex.fi/fi/laki/alkup/2017/20170585
38 https://www.finlex.fi/fi/laki/ajantasa/2015/20150010
39 https://stm.fi/documents/1271139/1334666/Korkean+varautumisen+viestint%C3%A4-ja+tietoj%C3%A4rjestelmien+hallinnan+ja+k%C3%A4yt%C3%B6n+toimintamalli+ohje.pdf
40 https://www.finlex.fi/fi/laki/ajantasa/2011/20111552
41 http://urn.fi/URN:ISBN:978-952-367-327-4
42 http://urn.fi/URN:ISBN:978-952-367-503-2
43 http://urn.fi/URN:ISBN:978-952-251-982-5
44 https://julkaisut.valtioneuvosto.fi/handle/10024/162453
45 https://aws.amazon.com/blogs/security/aws-publishes-pitukri-isae3000-type-ii-attestation-report-for-finnish-customers/
46 https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille
47 https://dvv.fi/vahti
48 https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet
49 https://vm.fi/suositukset
50 http://urn.fi/URN:ISBN:978-952-367-906-1
51 http://urn.fi/URN:ISBN:978-952-367-500-1
52 https://www.oracle.com/corporate/cloud-compliance/
53 https://cloud.google.com/security/compliance
54 https://aws.amazon.com/compliance/
55 https://docs.microsoft.com/en-us/azure/compliance/
56 https://iprinfo.fi/uutiset/euroopan-tietosuojaneuvosto-hyvaksyi-ensimmaiset-ylikansalliset-kaytannesaannot/
57 https://tietosuoja.fi/osoitusvelvollisuus
58 https://edpb.europa.eu/edpb_fi
59 https://eucoc.cloud/
60 https://www.codeofconduct.cloud/
61 https://um.fi/kansallinen-turvallisuusviranomainen
62 http://urn.fi/URN:ISBN:978-952-367-906-1
63 https://tietosuoja.fi/pseudonymisointi-anonymisointi
64 https://aws.amazon.com/directconnect/
65 https://azure.microsoft.com/services/expressroute/
66 https://www.oracle.com/cloud/networking/fastconnect/
67 https://cloud.google.com/network-connectivity/docs/interconnect
68 https://aws.amazon.com/agreement/recent-changes/
69 https://aka.ms/MSLERR

70 https://www.data-infrastructure.eu/
71 https://fortune.com/2021/09/08/germany-sovereign-cloud-google-t-systems/
72 https://stm.fi/valmiusasiat
73 https://stm.fi/tuto
74 ”Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista” (kappale 5) https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset
75 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161332/5_2019_Kansallinen%20riskiarvio.pdf
76 https://docs.microsoft.com/fi-fi/azure/active-directory/hybrid/choose-ad-authn
77 https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
78 https://infrastructuremap.microsoft.com/
79 https://cloud.google.com/about/locations
80 https://www.oracle.com/cloud/data-regions/
81 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_fi
82 https://tietosuoja.fi/henkilotietojen-kasittelijan-velvollisuudet

AKUSTI on sosiaali- ja terveydenhuollon tietohallintoyhteistyöfoorumi. Verkosto tukee sosiaali- ja terveyspalveluiden uudistamista ja tähän liittyvää tietohallintoyhteistyötä.
www.kuntaliitto.fi/akusti

KUNTALIITTO | Kommunförbundet

ISBN 978-952-293-835-0 (pdf)

Helsinki 2022

AKUSTI

Alueiden ja kuntien sosiaali- ja terveydenhuollon tietohallinto-yhteistyöfoorumi