Pohjois-Karjalan hyvinvointialue

Pilvipalvelujen yleiset periaatteet Siun sotessa

Sisällysluettelo

1 Johdanto

Pilvipalveluiden käyttö on kasvanut merkittävästi viime vuosina, ja niiden merkitys julkishallinnossa on korostunut entisestään. Suomessa julkisen sektorin organisaatioiden on tärkeää laatia selkeät pilvipalvelulinjaukset, jotta voidaan varmistaa palveluiden tehokas, turvallinen ja lainmukainen käyttö. Pilvipalvelut tarjoavat mahdollisuuden parantaa palveluiden saatavuutta, joustavuutta ja kustannustehokkuutta. Sosiaali- ja terveydenhuollon alalla paineet digitalisaation edistämiseksi ja kustannustehokkuuden lisäämiseksi ovat merkittäviä. Pilvipalveluista on tulossa yhä tärkeämpiä, ja monissa tapauksissa niistä voi tulla ainoa mahdollinen palvelumalli, erityisesti uusien teknologioiden, kuten tekoälyn, myötä.

Pilvipalveluihin liittyy kuitenkin myös merkittäviä uhkia, kuten tietoturvariskit, tietosuojaloukkaukset ja palvelunestohyökkäykset. Nämä uhat eivät kuitenkaan poikkea muilla teknologiaratkaisuilla toteutettujen palveluiden riskeistä. Globaali toimintamalli ja uudenlainen teknologia korostavat tietosuojariskien arvioinnin merkitystä. Näiden uhkien hallinta edellyttää huolellista suunnittelua ja selkeitä linjauksia. Pilvipalvelulinjaukset auttavat varmistamaan, että tietosuoja ja tietoturva ovat asianmukaisesti huomioituja, ja ne tarjoavat selkeät ohjeet palveluiden hankintaan ja käyttöön. Lisäksi linjaukset tukevat organisaatioiden digitaalista muutosta ja parantavat yhteistyötä eri toimijoiden välillä. Näin voidaan vastata paremmin kansalaisten tarpeisiin ja parantaa julkisten palveluiden laatua ja saavutettavuutta.

1.1 STRATEGISET TAVOITTEET PILVIPALVELUIDEN HYÖDYNTÄMISEN OSALTA POHJOIS-KARJALAN HYVINVOINTIALUEELLA

Pohjois-Karjalan hyvinvointialueen strategioissa ei suoraan puhuta pilvipalveluiden käytöstä mutta monien tavoitteiden toteutumista voidaan edesauttaa pilvipalveluiden käytöllä. Muun muassa hyvinvointialueen palvelustrategiassa digitaaliset palvelut esitetään keskeisenä osana palvelujen tarjoamista. Tavoitteena on, että palvelujen saatavuus, saavutettavuus ja oikea-aikaisuus paranevat ja monikanavainen palveluverkko vastaa alueen asukkaiden palvelutarvetta.[1] Pilvipalvelut tarjoavat infrastruktuurin, skaalautuvuuden ja joustavuuden, joita tarvitaan monenlaisten digitaalisten palvelujen tukemiseen. Strategiassa on tunnistettu, että huomattava osa Pohjois-Karjalan hyvinvointialueen väestöstä asuu maaseudulla. Maantieteelliset kulkuesteet ja julkisen liikenteen heikko tarjonta vaikuttavat paljon asukkaiden mahdollisuuksiin hakeutua palveluihin.[2] Pilvipalvelut tarjoavat keinon olla yhteydessä potilaisiin ja asiakkaisiin pitkienkin matkojen päästä. Pilvipalveluihin pääsee käsiksi mistä tahansa internet-yhteydellä, mikä mahdollistaa syrjäisillä alueilla asuvien ihmisten tavoittamisen. Henkilöstöpulaan vastaamisessa ja kustannustehokkuuden lisäämisessä pilvipalveluilla voi olla merkittävä

[1] Pohjois-Karjalan hyvinvointialueen palvelustrategia 2024–2038
[2] Pohjois-Karjalan hyvinvointialueen palvelustrategia 2024–2038

vaikutus kokonaisuuden kannalta. Pilvipalvelut voivat auttaa lieventämään henkilöstöpulaa automatisoimalla tehtäviä, parantamalla viestintää, mahdollistamalla etätyön ja tukemalla resurssien tehokasta kohdentamista. Tämä voi vapauttaa henkilöstöä keskittymään suoraan hoitoon, mikä voi parantaa henkilöstön pysyvyyttä. Edellä mainitut asiat vaikuttavat myös hyvinvointialueen kustannustehokkuuteen. Tehokkuutta voidaan parantaa myös tehostamalla prosesseja, vähentämällä fyysisten infrastruktuurien tarvetta ja mahdollistamalla paremman tiedonhallinnan ja -analyysin tietoon perustuvan päätöksenteon tueksi. Pohjois-Karjalan hyvinvointialueen strategiaan sisältyy myös suunnitelmia laajentaa hyvinvointiteknologian käyttöä erilaisilla aloilla, kuten kotihoidossa ja etäpalveluissa.[3] Myös näissä käyttökohteissa pilvipalveluilla voi olla iso merkitys, sillä pilvipalveluiden avulla voidaan tarjota erilaisia ratkaisuja monenlaisiin haasteisiin aina päätöksenteosta toiminnanohjaukseen asti.

Kaiken kaikkiaan pilvipalvelut ovat tehokas työkalu Pohjois-Karjalan hyvinvointialueelle parantaa palvelujen tehokkuutta, saavutettavuutta ja kustannustehokkuutta palveluiden ollessa käyttäjäystävällisiä ja tarpeeseen sopivia. Nämä kaikki ovat keskeisiä elementtejä hyvinvointialueen strategiassa.

1.2 KANSALLISET LINJAUKSET JA SOVELTAMISOHJEET PILVIPALVELUIDEN KÄYTÖLLE

Kansallisesti on laadittu linjauksia ja toimenpide-ehdotuksia pilvipalveluiden käytölle. Muun muassa Valtiovarainministeriön asiakirja "Valtionhallinnon pilvipalvelulinjaukset" tarjoaa ohjeet pilvipalveluiden käytöstä julkisella sektorilla. Ohjeiden tavoitteena on tukea päätöksentekoa hallituksessa, hyvinvointialueilla ja kunnissa pilvipalveluiden käyttöön liittyen. Asiakirjassa pilvipalveluja pidetään ratkaisevan tärkeinä julkisen hallinnon digitalisaation edistämisessä ja tuottavuuden parantamisessa.[4]

Ohjeet rakentuvat yhdeksän keskeisen periaatteen ympärille:

1. Pilvipalveluiden tai -teknologian tulisi olla ensisijainen valinta, ellei valinnalle ole pakottavia perusteita
2. Pilvi- ja ekosysteemiratkaisujen tulisi lähtökohtaisesti olla peräisin EU/ETA-alueelta.
3. Etusijalle tulisi asettaa valtion yhteiset pilvi- ja ekosysteemiratkaisut, kun ne ovat sopivia.
4. Pilvialustapalveluihin liittyvät kilpailutukset ja hankinnat tulisi tehdä ensisijaisesti valtionhallinnon yhteisillä hankintasopimuksilla.
5. Pilvipalveluiden hankinnan, käyttöönoton ja hyödyntämisen tulisi noudattaa samoja menettelyjä kuin minkä tahansa muun tietojärjestelmän kohdalla.

[3] Pohjois-Karjalan hyvinvointialueen palvelustrategia 2024–2038
[4] Valtionhallinnon pilvipalvelulinjaukset 2024

6. Julkista tietoa voidaan käsitellä julkisessa pilvipalvelussa, jos tietoturva, tietosuoja ja jatkuvuudenhallinta on toteutettu, varmistettu ja otettu käyttöön tietojenkäsittelystä vastaavan yksikön tai viraston johdon riskiperusteisella päätöksellä.
7. Salassa pidettävää tietoa voidaan käsitellä julkisessa pilvipalvelussa samoin edellytyksin kuin julkista tietoa edellyttäen riskiperusteista päätöksentekoa ja tietoturvan, tietosuojan ja jatkuvuudenhallinnan vaatimustenmukaisuutta.
8. Henkilötietojen käsittely julkisissa pilvipalveluissa on sallittua, jos tietoturvan, tietosuojan ja jatkuvuudenhallinnan vaatimukset täyttyvät, ne on varmistettu ja otettu käyttöön tietojenkäsittelystä vastaavan yksikön tai viraston johdon riskiperusteisella päätöksellä.
9. Turvallisuusluokan IV tietoja voidaan käsitellä julkisessa pilvipalvelussa samoin edellytyksin kuin edellä mainituissa luokissa, mukaan lukien tiukka tietoturva, tietosuoja ja jatkuvuudenhallinta sekä tietojenkäsittelystä vastaavan yksikön tai viraston johdon riskiperusteinen päätös.

Valtiovarainministeriön asiakirja ei kuitenkaan käsittele erikseen sosiaali- ja terveydenhuollon tietojen käsittelyä pilvipalveluissa. AKUSTI:n laatima soveltamisopas "SOTE-tietojärjestelmät pilvipalveluna" on kattava opas suomalaisille sosiaali- ja terveydenhuollon organisaatioille, jotka harkitsevat pilvipalveluiden käyttöönottoa. Soveltamisoppaan mukaan sosiaali- ja terveydenhuollon asiakastieto ei ole turvaluokiteltavaa tietoa vaan voi rinnastua henkilötietoihin tai julkisiin ja salassa pidettäviin tietoihin käyttötapauksen mukaan. Kuitenkin pelkkä tiedon luokiteltavuus ei ole ainoa kriteeri tietojen hallinnointiin pilvipalveluissa vaan myös palveluiden kriittisyydellä ja arkkitehtuurin joustavuudella on merkitystä pohdittaessa sote-tietojen säilyttämistä pilvipalveluissa. Soveltamisoppaassa tarkastellaan arkaluonteisten potilastietojen hallintaan tarkoitettujen pilvipohjaisten järjestelmien käyttöön liittyviä mahdollisuuksia, haasteita ja sääntelyyn liittyviä kysymyksiä.[5] Tätä näkökulmaa ei käsitellä Valtiovarainministeriön asiakirjalla.

2 Pilvipolitiikan tarkoitus

Tämän dokumentin tarkoituksena on kuvata Pohjois-Karjalan hyvinvointialueen perustason linjaukset, miten pilvipalveluita käytetään kaikkialla organisaatiossa ja minkälaisia prosesseja ja toimenpiteitä niiden käyttöönotto ja ylläpito Pohjois-Karjalassa vaatii. Linjauksia on hyödynnettävä aina pilvipalveluita käyttöönotettaessa. Linjauksia sovelletaan alueella moninaisissa ympäristöissä ja tilanteissa, joten tilannekohtaisten yksityiskohtaisen toimintaohjeiden dokumentointia ei nähty tarpeelliseksi. Tämä tarkoittaa muun muassa sitä, että vastuita tai vastuullisia toimijoita ei nimetty linjausten yhteydessä. Pilvipolitiikan tueksi on laadittava erillinen

[5] AKUSTI:n SOTE-tietojärjestelmät pilvipalveluina

toimeenpanosuunnitelma, josta käy ilmi, miten politiikan linjauksiin päästään. Linjausten tarkoituksena on ohjata organisaation toimintaa yhtenäiseen suuntaan, auttaa kehittämään yhtenäisiä toimintatapoja ja selkiyttää päätöksentekoa pilvipalveluihin liittyvissä asioissa. Dokumentissa käsitellään aiheita, jotka ovat yhteisinä nimittäjinä kaikenlaisissa käyttötapauksissa ja jotka vaikuttavat lopullinen ratkaisun toteutukseen. Aiheet eivät koske pelkästään teknisiä tai fyysisiä tekijöitä vaan kaikenlaisia prosesseja arvioinnista ja päätöksenteosta hallintaan, seurantaan ja käytöstä poistamiseen saakka.

Dokumentti on laadittu joulukuussa 2024 ja sen omistaa Pohjois-Karjalan hyvinvointialue.

3 Perusperiaatteet

Pilvipalveluiden käytölle julkisessa organisaatiossa ei ole kategorisia esteitä riippumatta siitä, minkälaista tietoa pilvipalvelussa käsitellään. Pilvipalveluiden kirjo on niin laaja, että hyvin arkaluonteisellekin tiedolle on löydettävissä ratkaisuja, jotka soveltuvat näiden tietojen käsittelyyn pilvessä. Olennaisinta on riskiskenaarioita analysoimalla, luottamuksellisuuden varmistamisella ja organisaation kokonaisarkkitehtuuria hyödyntämällä laatia linjaukset, jotka istuvat pilvipalveluita hyödyntävän organisaation toimintaan.

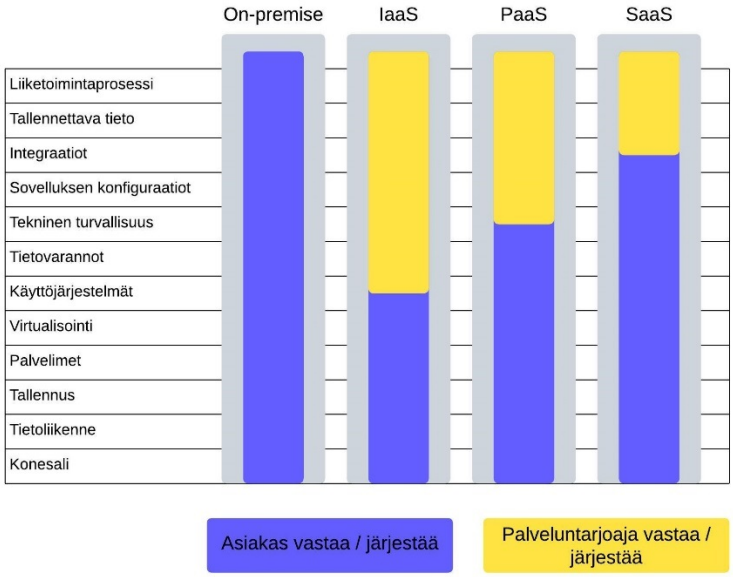
3.1 PALVELUIDEN TARKASTELU TEKNISESTÄ VASTUUNJAKONÄKÖKULMASTA

Erilaisten pilvipalveluiden tarjontamallien (IaaS, PaaS ja SaaS) käsittely erikseen on tietoturvan näkökulmasta perusteltua, koska jokaisella mallilla on omat erityispiirteensä ja riskinsä, jotka vaikuttavat tietoturvavaatimuksiin ja -käytäntöihin. Tämä auttaa organisaatioita suojaamaan tietojaan tehokkaasti ja varmistamaan, että pilvipalveluiden käyttö on turvallista ja lainmukaista.

IaaS tarjoaa perusinfrastruktuurin, kuten virtuaaliset palvelimet ja tallennustilan. Mallissa on tärkeää varmistaa, että infrastruktuuri on suojattu asianmukaisesti, ja että käyttäjä hallitsee pääsynhallintaa ja tietojen salausta.

PaaS tarjoaa alustan sovellusten kehittämiseen ja käyttöönottoon. Mallissa on tärkeää varmistaa, että sovellukset on kehitetty turvallisesti ja että ne noudattavat tietoturvakäytäntöjä.

SaaS tarjoaa valmiita ohjelmistoja, joita käyttäjät voivat käyttää suoraan internetin kautta. Mallissa on tärkeää varmistaa, että palveluntarjoaja täyttää tietoturvavaatimukset ja että käyttäjä hallitsee pääsynhallintaa ja tietojen salausta.



Kuva 1: Kohdealueiden tyypillinen vastuunjako asiakkaan ja palveluntarjoajan kesken. Kuva laadittu Cirrus-hankkeen materiaaleissa olevasta kuvasta. Alkuperäisestä kuvasta poistettu BPaaS ratkaisukokonaisuuden arviointi.

3.2 PALVELUIDEN TARKASTELU TIEDON LUOKITTELUN NÄKÖKULMASTA

Pilvipalveluiden käytön kannalta on tärkeää pohtia myös palvelussa käsiteltävän tiedon luonnetta. Kaikki tieto ei ole samanarvoista, vaan tiedolla on erilainen painoarvo riippuen siitä, mitä ja minkälaista tieto on. Sosiaali- ja terveydenhuollon asiakastiedoilla ja varsinkin varautumiseen liittyvällä tiedolla on hyvin erilainen painoarvo verrattuna organisaation osoitetietoihin. Tiedon luonteen eroavaisuuksien takia tietoa voidaan luokitella merkityksensä perusteella. Täten eri turvaluokilla ja julkisuusluokilla on merkittävä rooli pilvipalveluiden käytön rajaamisessa. Henkilötiedot ja sosiaali- ja terveydenhuollon salassa pidettävät asiakastiedot ovat erityisen arkaluonteisia ja niiden käsittelyssä on noudatettava tiukkoja tietosuoja- ja tietoturvavaatimuksia.

Julkiset tiedot ovat kaikkien saatavilla, ja kuka tahansa voi pyytää niistä tietoa. Näiden tietojen käsittelyä pilvessä on rajattu kaikkein vähiten ja käytännössä tietoja on mahdollista käsitellä missä tahansa aluerajoista riippumatta.

Henkilötiedot sisältävät tietoja, jotka voivat tunnistaa yksilön, kuten nimi, osoite, henkilötunnus ja terveystiedot. Näiden tietojen käsittelyssä on noudatettava EU:n yleistä tietosuoja-asetusta (GDPR), joka asettaa tiukat vaatimukset tietojen suojaamiselle ja käsittelylle. Henkilötietojen siirto ja käsittely pilvipalveluissa edellyttää, että palveluntarjoaja täyttää GDPR:n vaatimukset, kuten tietojen salauksen, pääsynhallinnan ja säännöllisen auditoinnin.

Sosiaali- ja terveydenhuollon salassa pidettävät asiakas- ja potilastiedot sisältävät arkaluonteisia tietoja, kuten potilastiedot, hoitosuunnitelmat ja diagnoosit. Asiakas- ja potilastiedot ovat pysyvästi salassa pidettäviä ja niiden

käsittelyssä on noudatettava erityisiä tietoturvavaatimuksia. Tietojen käsittelyssä on käytettävä vahvaa salausta, tiukkaa pääsynhallintaa ja varmistettava, että tiedot säilyvät luottamuksellisina ja eheinä.

Turvaluokitellut tiedot ovat tietoja, joiden paljastuminen voisi aiheuttaa vakavaa haittaa kansalliselle turvallisuudelle, julkiselle järjestykselle tai organisaation toiminnalle. Näiden tietojen käsittelyssä on noudatettava erityisen tiukkoja tietoturvavaatimuksia, kuten vahvaa salausta, pääsynhallintaa ja säännöllistä auditointia. Turvaluokiteltujen tietojen käsittely pilvipalveluissa edellyttää, että palveluntarjoaja täyttää korkeimmat tietoturvastandardit ja että tietojen käsittely on tarkasti valvottua. Pohjois-Karjalan hyvinvointialueen pilvipolitiikan näkökulmasta turvaluokat II, III ja IV ovat merkityksellisiä. Eri luokille on määritelty erilaisia käytännön rajauksia kansallisesti.

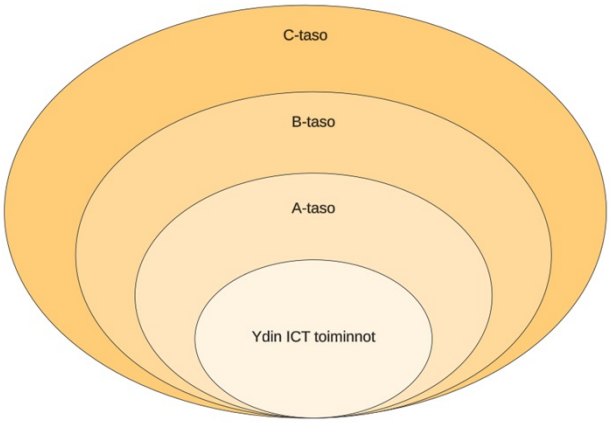
Näin ollen turvaluokitukset ja julkisuusluokat ovat keskeisiä tekijöitä, jotka ohjaavat pilvipalveluiden valintaa ja käyttöä.

3.3 SIPULIMALLI OHJAA RISKIENARVIOINTIA JA PÄÄTÖKSENTEKOA

Sipulimalli on hyvä riskienhallintatyökalu kuvaamaan eri toimintojen riskitasoja. Huomioiden edellisten kappaleiden eri näkökulmat pilvipalveluiden vastuunjaosta ja palveluihin tallennettavasta tiedosta, myös Pohjois-Karjalan hyvinvointialueen toimintoja pitää pystyä katsomaan erilaisten riskitasojen kautta. Verkkosivujen ylläpito eroaa merkittävästi hyvinvointialueen lääkehuollosta riskien näkökulmasta, joten pilvipalveluiden käyttöönoton kannalta on ensisijaisen tärkeää tunnistaa pilvipalvelua käyttävän toiminnon riskitaso. Riskitasoa määrittelee muun muassa toiminnon vaikutukset muihin henkilöihin ja tieto, jota toiminnossa käsitellään tai tuotetaan. Näiden perusteella määräytyy myös se, minkä tason vastuunjako on hyväksyttävää.

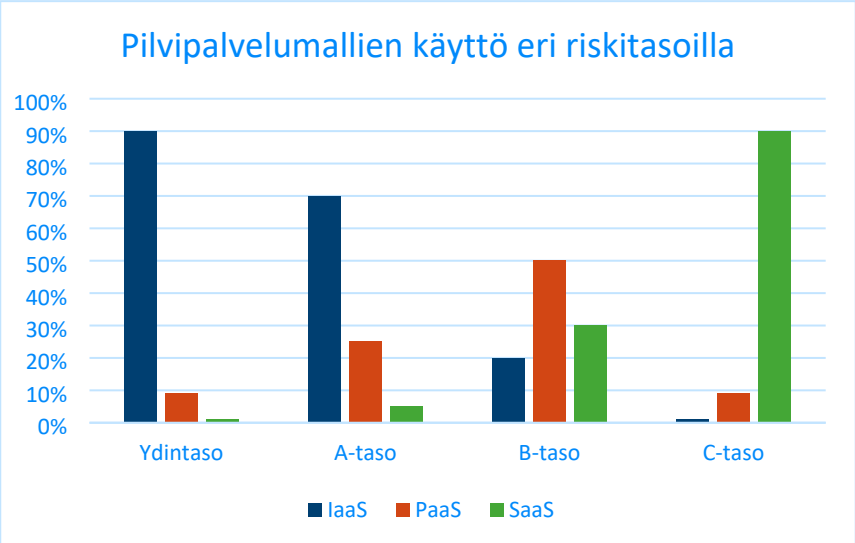
Sipulimallia voidaan käyttää riskiarvioinnin lisäksi vastuun jakamisen välineenä. Sisemmän tason ratkaisuiden ylläpidosta ja seurannasta ovat pääasiassa vastuussa johtotason henkilöt, ja käyttöön liittyy hyvin tarkkoja prosesseja ja kattavia riskienhallinta-analyyseja ja -toimenpiteitä. Ulomman tason ratkaisuja voidaan taas ottaa käyttöön huomattavasti kevyemmillä prosesseilla. Ulommalla tasolla ratkaisujen päävastuu olisi käyttöönottavalla tiimillä tai organisaation osalla muun muassa tietosuojavastaavan tuella. Käytännössä ulkokehällä tiedostetaan, että pilvipalveluiden käyttöön liittyy sellaista tietojen käsittelyä palveluntarjoajan taholta, josta ei olla täysin tietoisia, mutta riskit huomioiden ollaan valmiit hyväksymään. Kunhan tietyt ehdot esimerkiksi tiedon fyysisen sijainnin ja henkilötietojen käsittelyn osalta täyttyvät, voidaan palveluita ottaa matalalla kynnyksellä käyttöön. Joustavuutta ja matalan kynnyksen käyttöönottoja mahdollistava toimintamalli tukee Pohjois-Karjalan hyvinvointialueen strategisia tavoitteita kuten henkilöstön riittävyyden, työhyvinvoinnin ja sitoutumisen varmistaminen sekä toiminnan sujuvuuden, laadun ja vaikuttavuuden parantaminen.

Seuraavalla sivulla (kuva 2) on esimerkinomainen kuva, miltä sipulimalli näyttää. Tasoja voi lopullisessa mallissa olla enemmän tai vähemmän, mutta periaatetasolla organisaation toimintoja sijoitetaan eri kerroksiin riskiarvion perusteella.



Kuva 2: Esimerkki sipulimallista ja riskiperusteisesta toimintojen jaottelusta.

Riskiluokituksen, vastuun jakamisen ja eri palveluratkaisujen luonteen takia IaaS, PaaS ja SaaS ratkaisujen käyttö ei jakaudu tasaisesti eri tasojen välille. IaaS ja PaaS ratkaisut ovat selvästi yleisempiä korkean riskitason toiminnoissa, kun taas käytännöllisyyden vuoksi SaaS ratkaisujen käyttö korostuu matalan riskitason toiminnoissa. On jopa suotavaa, että SaaS ratkaisuja ei käytetä korkean riskitason toiminnoissa. Alla esimerkinomainen taulukko ratkaisumallien jakautumisesta eri riskitasojen välille. Taulukon tarkoituksena ei ole toimia virallisena tavoitteena vaan havainnollistaa mahdollista lopputulemaa edellä mainitut seikat huomioiden.



Linjaus 1:

Pohjois-Karjalan hyvinvointialueen toiminnot on jaoteltava sipulimallin mukaisesti eri riskitasoille, jotta pilvipalveluiden käyttöönotto voidaan toteuttaa tehokkaasti riskiarviopohjaisesti. Sipulimallia käytetään myös vastuunjakovälineenä, jolloin pilvipalveluiden tietoturvaan ja -suojaan liittyvien asioiden seurantaa voidaan hajauttaa organisaatiossa riskiperusteisesti.

3.4 KYTKENTÄ KOKONAISARKKITEHTUURITYÖHÖN

Kansallisten linjausten sallivuudesta huolimatta Pohjois-Karjalan hyvinvointialueen näkökulmasta yhtä avoimet linjaukset eivät välttämättä ole järkeviä. Pilvipalveluiden riskianalyysit ja valvonta sekä palveluiden ylläpitoon liittyvät prosessit voivat olla työläitä ja jopa ylivoimaisia organisaation resursseihin nähden, jos pilvipalveluiden käytön osalta ei laadita rajoitteita. Pahimmassa tapauksessa hyvät pilvipalveluratkaisut jäävät ottamatta käyttöön raskaiden arviointiprosessien takia, olemassa olevien ratkaisujen tietoturvapuutteita ei havaita ja ratkaisut eivät täytä lakien vaatimuksia. Tämän takia käyttöönotettava pilvipalvelu on aina kytkettävä osaksi Pohjois-Karjalan hyvinvointialueen kokonaisarkkitehtuuria. Osana kokonaisarkkitehtuurityötä voidaan rajata ratkaisujoukkoja muun muassa tietoturvan ja kokonaishallittavuuden perusteella. Tietoturvan ja kokonaishallittavuuden näkökulmien lisäksi kokonaisarkkitehtuurin auttaa ottamaan pilvipalveluita käyttöön Pohjois-Karjalan hyvinvointialueen strategisten linjausten mukaisesti, huomioida yhteentoimivuus- ja integraatioasiat muihin järjestelmiin ja ohjeistaa kustannusten hallintaan ja optimointiin liittyviä asioita.

Käyttöönottoon tähtäävässä projektissa on mietittävä seuraavia asioita liittyen pilvipalvelun käyttöön:

- Kuka tai ketkä käyttävät pilvipalvelua?
- Mihin ratkaisua käytetään?
- Mitä ja minkä turvaluokan tai julkisuusluokan tietoa tallennetaan?
- Missä maassa tietoa fyysisesti säilytetään?
- Kuka pääsee käsiksi palvelussa käsiteltävään tietoon ja minkälaisia käyttöoikeuksia vaaditaan?
- Miten pilvipalvelun käyttöä seurataan?
- Onko organisaation ulkopuolisilla toimijoilla mahdollisuus päästä käsiksi palvelussa oleviin tietoihin?
- Miten väärinkäytöksiin reagoidaan?
- Miten toimitaan, kun palvelun toimintaympäristössä tapahtuu muutoksia, joilla on vaikutuksia riskiarvioihin?
- Minkälaisia sopimuksia palveluntarjoajan kanssa laaditaan?
- Miten tiedon palvelun ja tiedon koko elinkaari huomioidaan? Miten palvelun hallittu poisto on toteutettavissa?

Näitä tietoja käytetään hyödyksi osana kokonaisarkkitehtuurityötä selvitettäessä, miten ehdotettu palvelu sopii

Linjaus 2:

Kokonaisarkkitehtuurityö ohjaa ja palvelee pilvipalveluiden käyttöönottoa Pohjois-Karjalan hyvinvointialueella. Pilvipalvelut on aina kytkettävä osaksi organisaation järjestelmäkenttää ja huomioitava mahdolliset integraatiot ja tietovirrat järjestelmien välillä. Käyttöönoton aikana pilvipalvelun käyttöönotosta on (omistajan tai pääkäyttäjän) kirjattava asianmukaiset tiedot Pohjois-Karjalan hyvinvointialueen dokumentointiympäristöön.

osaksi Pohjois-Karjalan hyvinvointialueen tietojärjestelmäkenttää ja minkälaisia muutoksia sen käyttöönotto voi aiheuttaa muihin tietojärjestelmiin tai prosesseihin. Käyttöönoton yhteydessä listatut tiedot dokumentoidaan organisaation määrittelemään ympäristöön.

3.5 MUUTOSVAIKUTUSTEN ARVIOINTI

Muutosvaikutusten arviointi on keskeinen työkalu Pohjois-Karjalan hyvinvointialueen harkitessa pilvipalveluiden hankintaa ja käyttöä sekä kehittäessä kokonaisarkkitehtuuriaan. Arvioimalla pilvipalveluiden käyttöönoton vaikutuksia tunnistetaan ja hallitaan mahdolliset riskit, kuten tietoturvaan, tietosuojaan ja palvelun jatkuvuuteen liittyvät haasteet. Muutosvaikutusten arviointi varmistaa, että uudet pilvipalvelut ovat yhteensopivia olemassa olevien järjestelmien ja prosessien kanssa. Yhteensopivuuden varmistaminen mahdollistaa saumattoman tiedonhallinnan ja tietovirrat.[6]

Arvioimalla muutosten taloudellisia vaikutuksia varmistetaan, että pilvipalveluiden hankinta ja käyttö ovat kustannustehokkaita ja tuovat odotettuja hyötyjä organisaatiolle. Pilvipalveluiden käyttöönotto tuo mukanaan erityisiä tietoturva- ja tietosuojavaatimuksia, jotka tunnistetaan ja varmistetaan muutosvaikutusten arvioinnin avulla.[7] Valtioneuvoston julkaisuarkistosta löytyy muistio ja arviointitaulukko, jota käytetään muutosvaikutusten arviointiin.[8] Muistio ja arviointitaulukko dokumentoidaan organisaation määrittelemään dokumentointiympäristöön.

Muutosvaikutusten arviointi tukee kokonaisarkkitehtuurin kehittämistä varmistamalla, että kaikki muutokset ovat linjassa organisaation strategisten tavoitteiden ja arkkitehtuuriperiaatteiden kanssa. Tämä prosessi on olennainen osa suunnittelua ja päätöksentekoa, joka auttaa organisaatioita tekemään tietoon perustuvia päätöksiä ja varmistamaan, että muutokset toteutetaan hallitusti ja tehokkaasti.

Linjaus 3:

Muutosvaikutusten arviointi tukee Pohjois-Karjalan hyvinvointialueen kokonaisarkkitehtuurityötä ja täten on ensisijaisen tärkeä työkalu pilvipalveluiden hankintaa, käyttöönottoa ja käyttöä arvioitaessa. Arvioinnin työkaluina käytetään Tiedonhallintalautakunnan tarjoamaa muistiota ja arviointitaulukkoa. Muistio ja arviointitaulukko dokumentoidaan Pohjois-Karjalan hyvinvointialueen määrittelemään dokumentointiympäristöön.

[6] Suositus tiedonhallinnan muutosvaikutusten arvioinnista
[7] Suositus tiedonhallinnan muutosvaikutusten arvioinnista
[8] Suositus tiedonhallinnan muutosvaikutusten arvioinnista -dokumentin liitteet (muistio ja arviointitaulukko)

4 Tarkempia linjauksia aihealueittain

4.1 PÄÄSY POHJOIS-KARJALAN HYVINVOINTIALUEEN PERUSPALVELUIHIN

Pohjois-Karjalan hyvinvointialueen työntekijöiden perusoikeuksien takaamiseksi jokaisella työntekijällä on oltava pääsy organisaation peruspalveluihin. Nämä palvelut voivat olla muitakin kuin pilvipalveluina tuotettuja. Näitä peruspalveluita ovat muun muassa Intra, Teams, sähköposti, henkilökohtainen OneDrive ja henkilöstöhallinnon järjestelmät. Näiden palveluiden kautta muun muassa mahdollistetaan työntekijöiden lakisääteiset oikeudet, informoidaan organisaatiossa tapahtuvista asioista sekä mahdollistetaan työskentely turvallisesti ja asianmukaisesti.

Linjaus 4:

Jokaisella Pohjois-Karjalan hyvinvointialueen työntekijälle on taattava mahdollisuus päästä mahdollisimman vaivattomasti lukemaan ja käsittelemään organisaation yleisissä pilvipalveluissa olevia tietoja. Näiden palveluiden kautta muun muassa mahdollistetaan työntekijöiden lakisääteiset oikeudet, informoidaan organisaatiossa tapahtuvista asioista sekä mahdollistetaan työskentely turvallisesti ja asianmukaisesti.

4.2 PILVIPALVELUIDEN KÄYTTÖ PELASTUSTOIMESSA

Pelastustoimessa käytössä oleva Erillisverkon tarjoama turvallisuusverkko vaikeuttaa merkittävästi pilvipalveluiden käyttöä toimialalla. Käytännössä ei ole pilvipalveluratkaisua, jota voitaisiin käyttää huomioiden alaa ohjaavien lakien vaatimukset. Vaikka suurin osa pelastustoimessa käsiteltävästä tiedosta on joko julkista tai salassa pidettävää, pieni osa käsiteltävästä arkaluonteisesta tiedosta ohjaa kaikkien pilvipalveluiden käyttöä. Pelastustoimessa on pääasiassa tukeuduttava niihin pilvipalveluihin, joita Erillisverkko tarjoaa.

Pelastustoimen työntekijöille on kuitenkin mahdollistettava pääsy organisaation yleisiin peruspalveluihin. Tästä on linjattu kappaleessa Pääsy Pohjois-Karjalan hyvinvointialueen peruspalveluihin.

Linjaus 5:

Pelastustoimessa käytetään Erillisverkon tarjoamia palveluita ja näin ollen pilvipalveluiden käyttö rajataan vain Pohjois-Karjalan hyvinvointialueen peruspalveluihin sikäli, kun Erillisverkko ei pysty muita pilvipalveluita tarjoamaan.

4.3 TIETOSUOJAN VAIKUTUSTENARVIOINTI

Tietosuojan vaikutustenarviointi eli DPIA (Data Protection Impact Assessment) on tietosuoja-asetuksen (GDPR) mukainen prosessi, jossa arvioidaan, miten suunniteltu henkilötietojen käsittely voi vaikuttaa ihmisten yksityisyyteen ja mitä riskejä siihen liittyy. Sen tavoitteena on varmistaa, että henkilötietoja käsitellään turvallisesti ja lainmukaisesti.

Vaikutustenarviointi on tehtävä, jos henkilötietojen käsittelyyn liittyy suuri riski rekisteröityjen oikeuksille ja vapauksille. Esimerkkejä tällaisista tilanteista ovat:

1. **Suuri määrä tietoja tai arkaluontoisia tietoja:** Käsitellään laajasti erityisiä henkilötietoryhmiä (esim. terveyttä, uskontoa, poliittisia mielipiteitä koskevia tietoja).

2. **Systemaattinen seurantaa tai profilointi:** Käytetään teknologioita, kuten kasvojentunnistusta, käyttäytymisen analysointia tai laajamittaista paikannusseurantaa.

3. **Automaattiset päätökset:** Kun henkilötietoihin perustuvat päätökset tehdään ilman ihmisen osallistumista.

4. **Uudet teknologiat:** Otetaan käyttöön uusia teknologioita, joiden vaikutuksia yksityisyyteen ei vielä täysin ymmärretä.

Lisäksi kansallisessa lainsäädännössä voidaan erikseen vaatia vaikutustenarvioinnin tekemistä. [9] [10]

Vaikutustenarviointi ei kuitenkaan ole tarpeen, jos:[11]

1. **Käsittely on yksinkertaista ja riskitöntä:** Käsitellään ainoastaan tavanomaisia henkilötietoja ilman laajaa tai arkaluontoista käsittelyä.

2. **Käsittely on identtistä jo arvioidun toiminnan kanssa:** Jos vastaava käsittely on jo arvioitu aiemmassa arvioinnissa eikä uutta riskiä ole syntynyt.

3. **Käsittely on lain mukaan pakollista:** Jos henkilötietojen käsittelyyn liittyvä vaikutusarviointi on jo tehty osana lakisääteistä prosessia.

---

[9] https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista
[10] https://tietosuoja.fi/vaikutustenarviointi
[11] https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#when-is-a-dpia-not-required

4. **Käsittely kuuluu poikkeusluetteloon:** Kansallinen tietosuojaviranomainen voi määritellä tiettyjä tilanteita, joissa DPIA ei ole tarpeen.

DPIA on tärkeä työkalu kaikille organisaatioille, jotka käsittelevät henkilötietoa. Pohjois-Karjalan hyvinvointialueella DPIA on lähtökohtaisesti aina läsnä pilvipalveluita hankittaessa mutta toiminnon riskitaso ja toisaalta pilvipalvelun käyttöön liittyvät lähtötiedot (mainittu kappaleessa ”Kytkentä kokonaisarkkitehtuurityöhön”) huomioiden arvioidaan, onko DPIA tarpeen tehdä vai ei.

Linjaus 6:

Tietosuojan vaikutustenarviointi tulee tehdä erityisesti silloin, kun pilvipalvelua käytetään korkean riskitason toiminnoissa. Myös matalamman riskitason toiminnoissa arviointi on tehtävä, jos osana palvelua käytetään uutta teknologiaa, käsiteltävän tiedon määrä on suuri tai toiminnon riskitaso sitä muuten edellyttää. SOTE-toiminnoissa on pohdittava, onko käsittely lain mukaan pakollista.

4.4 IAAS JA PAAS RATKAISUJEN VÄHIMMÄISVAATIMUKSET

IaaS ja PaaS ratkaisujen käyttö edellyttää, että palveluntarjoaja on sitoutunut käsittelemään henkilötietoja GDPR:n mukaisesti ja tietojen käsittely on mahdollista rajata pelkästään EU/ETA-alueelle. Lisäksi tiedon sensitiivisyydestä tai turvaluokasta riippuen, kansalliset kriteeristöt täyttävät pilviratkaisut toimivat hyvinä kriteereinä luotettavuuden määrittelemiseksi. Muun muassa PiTuKrin, JulKrin tai Katakrin mukaisesti toteutetut palvelut takaavat, että tietoja voi käsitellä tietoturvallisesti korkeankin riskin käyttötapauksissa. Kansallisten kriteeristöjen lisäksi muun muassa ISO 27000, 27017, 27018 ja 27701 standardit tarjoavat hyvän perustan sensitiivisen tiedon käsittelyyn. ISO 9001 on riittävä, jos käsiteltävät tiedot ovat julkisia mutta ei riitä käsiteltäessä sensitiivistä tietoa. Se, minkä turvatason pilvipalvelua on missäkin tilanteessa käytettävä, määräytyy toiminnon riskien vaikuttavuusluokan ja toiminnon sipulimallin mukaisen riskitason perusteella.

Tietoturvataso ei ole ainoa kriteeri, jota on pohdittava IaaS tai PaaS ratkaisua hankittaessa. Muun muassa varautumisen näkökulmasta suojattavat tiedot, suuri määrä salassa pidettävää tai/ja henkilötietoja ja turvaluokan II, II ja IV tietoja on säilytettävä Suomessa ja palveluntarjoajan tulee olla kansallinen viranomainen, julkinen toimija tai yritys. Lisäksi toiminnon luonne rajaa vaihtoehtoja. Sosiaali- ja terveydenhuollossa käytössä oleville A3-luokan tietojärjestelmille on asetettu THL:n toimesta erityisiä varautumiseen liittyviä vaatimuksia. Näissä vaatimuksissa on todettu, että järjestelmissä jatkuva toimivuus tai viiveetön palauttaminen toimivaksi on oltava mahdollista nopeasti.[12] A3-luokan järjestelmien kohdalla puhutaan korkean riskiluokan järjestelmistä, jolloin

[12] THL Määräys 05/2024, liite 3g, vaatimus AKYM16

nämä kuuluvat Pohjois-Karjalan hyvinvointialueella ydin ICT-toimintoihin. Näin ollen kyseisissä järjestelmissä hallinnoitavat tiedot vertautuvat tietoon, jota on säilytettävä Suomessa ja palveluntarjoajan tulee olla kansallinen viranomainen, julkinen toimija tai yritys.

Liitteenä on taulukko, jossa kuvataan tietoluokat ja niitä vastaavat käsittelyehdot.

Linjaus 7:

Käytetään ratkaisuja, joille on myönnetty kansainvälisiä laatustandardeja (ISO ISO 27000, 27017, 27018, 27701 ja 9001). Sopiva taso määrittyy riskiarvioinnin avulla. Myös kansallisesti merkittävien kriteeristöjen (PiTuKri, Katakri, JulKri) mukaisesti toteutetut ratkaisut ovat käyttökelpoisia.

Riskiarvioinnin avulla arvioidaan myös tiedon fyysisen sijainnin merkitystä. Suomi on ainoa mahdollinen tiedon fyysinen sijainti, kun on kyse turvallisuusluokan II, III ja IV sekä varautumiseen liittyvästä tiedosta. Myös terveydenhuollon A3-luokan järjestelmien tieto on sijaittava Suomessa.

4.5 PÄÄSYOIKEUKSIEN HALLINTA

Pääsyoikeuksien hallinnassa annetaan käyttäjille ja palveluille minimioikeudet, jotka tietojärjestelmä tarvitsee toimiakseen odotetusti. Tästä puhutaan vähimpien oikeuksien periaatteena (principle of least privileges). Käyttöoikeuksia hallinnoidaan Pohjois-Karjalan omassa IAM-palvelussa. Pohjois-Karjalan hyvinvointialueella pääsynhallintaa toteutetaan Meidän IT- ja talous Oy:n tuottamalla Laituri-ratkaisulla. Pääjärjestelmien osalta IAM-palvelussa on hallinnoitava pääsyoikeuksien lisäksi käyttöoikeuksia.

Pilvipalveluun pääsyssä pitää lähtökohtaisesti aina käyttää yhden kirjautumisen periaatetta (SSO eli Single sign-on). Käyttäjien on pystyttävä kirjautumaan organisaation IAM-palvelun avulla kaikkiin pilvipalveluratkaisuihin. Jos pilvipalvelun käytössä ei voida hyödyntää yhden kirjautumisen periaatetta, palvelun käyttö on rajattava vain julkisen tiedon käsittelyyn.

Asukkaille tarkoitetuissa palveluissa tunnistautumisen on tapahduttava Suomi.fi vahvalla tunnistautumisella tai GDPR:n mukaisesti tietoja käsittelevän palveluntarjoajan yhden kirjautumisen menetelmän (SSO) mahdollistavalla palvelulla. Tällaisia ovat muun muassa Googlen ja Microsoftin tarjoamat Sign-in -ratkaisut.

Linjaus 8:

Pilvipalveluiden käyttöoikeuksia hallinnoidaan Pohjois-Karjalan omassa IAM-palvelussa. Käyttäjät, sekä ammattilaiset että kansalaiset, tulee ensisijaisesti tunnistaa vahvasti tai käyttämällä Pohjois-Karjalan hyvinvointialueen kirjautumistunnuksia (SSO).

4.6 SISÄLTÖTIETOJEN SIIRROT

Pohjois-Karjalan hyvinvointialueen linjaus on, että henkilötietoa ei saa käsitellä EU/ETA-alueen ulkopuolella. Muiden tietojen kohdalla on tehtävä riskiperusteista pohdintaa tietojen fyysisen sijainnin rajauksista. Liitteenä oleva taulukko (Tietotyypit ja niitä vastaavat palveluehdot) linjaa tarkemmin tietotyypeittäin muun muassa missä tietoa voi käsitellä. Linjaus koskee kaikkia pilvipalveluiden tarjoamismuotoja: IaaS, PaaS ja SaaS.

Linjauksen perusteluna on Pohjois-Karjalan hyvinvointialueen vähäiset resurssit toteuttaa kattavia riskianalyyseja. Erityisesti henkilötietojen siirtämiseen EU/ETA alueen ulkopuolelle liittyvä riskienarviointiprosessi TIA (Transfer Impact Assessment) on tarpeettoman raskas saavutettuihin hyötyihin verrattuna. Linjauksesta huolimatta aina pilvipalvelua käyttöönotettaessa on varmistuttava, että palveluntarjoaja tarjoaa palvelua käyttävälle osapuolelle mahdollisuuden valita henkilötietojen säilytyspaikan ja varmistaa, että tiedot säilytetään valitulla alueella.

Pilvipalvelua voidaan käyttää pilvilaskentakapasiteettina, jolloin kerätylle tiedolle voidaan suorittaa paljon suoritustehoa vaativia toimenpiteitä kuten esimerkiksi tekoälyn analysointeja. Tiedon fyysinen sijainti voi tällaisissa tapauksissa olla Suomessa omalla konesalilla. Vaikka tiedon ensisijainen sijainti ei ole pilvipalvelussa, käsitetään laskentatoimien tekeminen tässä tapauksessa tiedon varsinaiseen käsittelyyn. Näin ollen pilvilaskennan kohdalla on noudatettava samoja riskiarviointimenetelmiä kuin muissakin dokumentissa mainituissa tilanteissa.

Linjaus 9:

Pohjois-Karjalan hyvinvointialueella käsiteltävää henkilötietoa on käsiteltävä ainoastaan EU/ETA-alueella. Muiden tietojen kohdalla fyysisen sijainti määräytyy riskiperusteisen arvioinnin sekä dokumentin liitteenä olevan taulukon pohjalta.

4.7 PALVELUDATAN KÄSITTELY JA SUOJAAMINEN

Palveludataan liittyvät asiat ovat olennainen osa määritettäessä pilvipalveluratkaisun sopivuutta tietyn riskiluokan toiminnolle. Palveludatalla tarkoitetaan tietoja, jotka liittyvät pilvipalvelun toimintaan ja käyttöön. Tämä data voi sisältää erilaisia teknisiä ja operatiivisia tietoja, jotka auttavat palveluntarjoajaa ja käyttäjää ymmärtämään, hallitsemaan ja optimoimaan pilvipalvelun käyttöä. Palveludata voi sisältää esimerkiksi käyttö- ja istuntodataa, suorituskykymittareita, laskutustietoja, lokitietoja, konfiguraatioita sekä virhe- ja diagnostiikkadataa. Palveludataa kerätään erityisesti julkipilviratkaisuissa, koska sen avulla palveluntarjoaja pystyy optimoimaan palvelun käyttöä, parantamaan suorituskykyä ja varmistamaan tietoturvan. Toisaalta on hyvä huomata, että muun muassa ja

diagnostiikkatiedot voivat linkittyä IP- ja laitetietoihin ja laskutus- ja tilien hallintaan vaadittavat tiedot palvelusta vastaaviin henkilöihin.[13]

Riskiarviointi määrittelee, mitä tietoa voidaan missäkin pilvipalvelutyypissä käsitellä. Liitteenä oleva taulukko antaa ohjeita päätöksentekoon mutta jokainen käyttöönotettava pilvipalvelu on arvioitava erikseen päätöstä tehdessä. On hyvä ymmärtää, että SaaS-ratkaisut pääosin pyörivät julkipilvessä. Linjauksena on, että matalan riskitason toiminnoissa tämä on hyväksyttävää, jotta mahdollistetaan arkea helpottavien ratkaisujen käyttöönotto sujuvasti ja vaivattomasti. Korkean riskitason toiminnoissa pyritään välttämään julkipilviratkaisuja estääkseen edellisessä mainittujen tunnistetietojen valumisen palveluntarjoajille.

Linjaus 10:

Riskiarviointi määrittelee, mitä tietoa voidaan missäkin pilvipalvelutyypissä käsitellä. Matalan riskitason toiminnoissa voidaan ottaa käyttöön pilvipalveluita, joissa palveludataa käytetään aktiivisesti palveluiden parantamiseen. Korkean riskitason toiminnoissa käytetään joko yhteisö- tai yksityispilviratkaisuja.

4.8 PILVIPALVELUN SAATAVUUDEN VARMISTAMINEN

Pilvipalvelun saatavuuden taso riippuu siitä, minkä riskitason toiminnasta on kyse. Matalan riskitason toiminnoissa riittää isoimpien pilvipalvelutoimittajien tarjoamat käytettävyystaso IaaS -ratkaisut. Korkean riskitason toiminnoissa on taattava saatavuus myös tilanteissa, joissa yhteydet Suomen ulkopuolelle ovat katkenneet. SaaS ratkaisuissa voi olla omat palvelutasosopimukset ja nämä on määriteltävä erikseen riskitason ja toiminnon merkityksellisyyden perusteella.

Linjaus 11:

IaaS ratkaisuissa voidaan luottaa isoimpien pilvipalvelutoimittajien (muun muassa Microsoft, Amazon, Google) saatavuus- ja käytettävyystasoon. Korkean riskitason toiminnoissa on pohdittava myös tiedon fyysistä sijaintia sekä palveluntarjoajan kotimaata. SaaS ratkaisuissa on pohdittava riittävää palvelutasoa ja fyysistä sijaintia toimintokohtaisesti. Apuna käytetään liitteenä olevaa taulukkoa.

[13] Cirrus-hankkeen tekninen yhteenveto

4.9 PILVIPALVELUN TURVALLISUUDEN SEURANTA

Pilvipalveluiden turvallisuuden jatkuva seuranta on tärkeä osa jatkuvaa riskienhallintaa. Käytössä olevien palveluiden käyttöehtoihin saattaa tulla muutoksia ajan saatossa ja näihin muutoksiin on pystyttävä reagoimaan tarvittaessa. Erityisesti tämä koskee SaaS ratkaisuja, joissa esimerkiksi tiedon fyysiseen sijaintiin saattaa tulla muutoksia mutta myös muiden julkipilveen rakennettujen ratkaisujen osalta on oltava tietoinen käyttöehdoissa tapahtuvissa muutoksissa.

Linjaus 12:

Pilvipalveluiden turvallisuutta on seurattava jatkuvasti. Korkea riskitason toiminnoissa seurannan tulee olla jatkuvaa ja muutoksiin on vastattava välittömästi. Matalamman riskitason palveluissa riittää vuosittainen perustietojen tarkastus.

4.10 HENKILÖSTÖN OSAAMISEN VARMISTAMINEN

Tietoturvan näkökulmasta henkilöstön tietotaito ja osaaminen pilvipalveluiden teemoihin liittyen on tärkeä osa asianmukaisen tietoturvan mahdollistamiseksi. Henkilöstön osaamisen varmistamisen tarkoituksena on lisätä henkilöstön ymmärrystä pilvipalveluiden tietoturva- ja tietosuojariskeistä, varmistaa, että henkilöstö tuntee Pohjois-Karjalan hyvinvointialueen tietoturva- ja tietosuojakäytännöt ja edistää turvallisia työskentelytapoja pilvipalveluiden käytössä.

Jokaisen pilvipalvelun pääasiallisen käyttäjän tietotaidosta ja osaamisesta on varmistuttava ja käyttäjille on tarjottava opiskelu- ja oppimisratkaisuja pilvipalvelun käyttöön liittyvissä asioissa. Käyttäjän on muun muassa ymmärrettävä mihin palvelua käytetään, mitä tietoa palveluun kerätään ja mitä tietoa palveluun ei saa viedä. Roolipohjaisilla käyttäjäoikeuksilla pidetään huoli, että käyttäjillä on mahdollisuus päästä käsiksi niihin tietoihin ja toiminnallisuuksiin, jotka ovat käyttäjän tehtävien perusteella tarpeellisia. Käyttäjäoikeuksista linjataan tarkemmin kappaleessa Pääsyoikeuksien hallinta.

Jokaiselle Pohjois-Karjalan hyvinvointialueen työntekijälle on tarjottava tietoa eri luokiteltujen tietojen käsittelystä Pohjois-Karjalan hyvinvointialueen laatimien ohjeistusten mukaisesti. Myös perehdytysohjelmaan on sisällytettävä materiaalia, jonka avulla mahdollistetaan uusien työntekijöiden tietotaidon ja osaamisen kehittyminen.

Tietoturvaan ja pilvipalveluiden käyttöön liittyvää osaamista on seurattava säännöllisin väliajoin.

Linjaus 13:

Jokaisen pilvipalvelun pääasiallisen käyttäjän tietotaidosta ja osaamisesta on varmistuttava ja käyttäjille on tarjottava opiskelu- ja oppimisratkaisuja käyttöön liittyvissä asioissa. Jokaiselle työntekijälle on tarjottava koulutusta eri luokiteltujen tietojen käsittelystä Pohjois-Karjalan hyvinvointialueen laatimien ohjeistusten mukaisesti. Tietoturvaan ja pilvipalveluiden käyttöön liittyvää osaamista on seurattava säännöllisin väliajoin.

4.11 PALVELUN KÄYTÖSTÄ POISTAMINEN

Tiedon elinkaariajattelun mukaisesti pilvipalvelun käytöstä poistamiseen on varauduttava jo hankinnan aikana. Hankinnan suunnittelussa ja sopimusten laadinnassa on otettava huomioon järjestelmässä käsiteltävän tiedon säilytysaika järjestelmän käytön päättymisen jälkeen tehtävät toimenpiteet. Järjestelmän käytön päätyttyä tiedot tulee joko siirtää toiseen järjestelmään, Pohjois-Karjalan hyvinvointialueen omaan sähköiseen säilytysjärjestelmään tai Kanta-arkistoon. Pilvipalvelujen tarjoamat omat arkistoratkaisut soveltuvat vain harvoin tiedon pitkäaikaissäilyttämiseen. Kun tietojen säilyminen on varmistettu, tulee järjestelmätoimittajan pystyä tuhoamaan tiedot.

Tiedon säilytysajat perustuvat voimassa olevaan lakiin ja hyvinvointialueen linjauksiin, joissa on huomioitu muun muassa oikeusvaikutukset ja vahingonkorvausoikeudelliset vanhenemisajat. Säilytysajat on kuvattu tiedonohjaussuunnitelmassa sekä hyvinvointialueen toimintaohjeissa.

Linjaus 14:

Tiedon elinkaari on otettava huomioon jo hankinnan aikana. Tietojärjestelmiä hankittaessa on huomioitava, miten tietojärjestelmään kerätyt tiedot saadaan siirrettyä toiseen järjestelmään, arkistoitua asianmukaisesti tai poistettua kokonaan.

5 Vaikuttava lainsäädäntö

Alla on lista keskeisistä laeista, jotka tulee huomioida pilvipalveluiden käyttöönotossa Pohjois-Karjalan hyvinvointialueella:

- Perustuslaki (731/1999)
- Työsopimuslaki (55/2001)
- Henkilötietojen käsittely ja tietosuoja
    - Yleinen tietosuoja-asetus (2016/679) (GDPR)
    - Tietosuojalaki (1050/2018)

- Julkista hallintoa säätelevä lainsäädäntö:
    - Hallintolaki (434/2003)
    - Laki julkisen hallinnon tiedonhallinnasta (906/2019)
    - Laki digitaalisten palvelujen tarjoamisesta (306/2019)
    - Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015)
    - Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)
    - Laki viranomaisten toiminnan julkisuudesta (621/1999)
    - Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)
    - Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
    - Laki sähköisen viestinnän palveluista (917/2014)
    - Arkistolaki (831/1994)
- Sosiaali- ja terveydenhuollon lainsäädäntö:
    - Sosiaali- ja terveydenhuollon järjestämislaki (612/2021):
    - Sosiaalihuoltolaki (1301/2014):
    - Terveydenhuoltolaki (1326/2010):
    - Laki potilaan asemasta ja oikeuksista (785/1992):
    - Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023)
    - Päivystysasetus (583/2017)
    - Ensihoitoasetus (585/2017)
- Lääkinnällisten laitteiden lainsäädäntö:
    - Asetus lääkinnällisistä laitteista (2017/745)
    - Laki lääkinnällisistä laitteista (719/2021)
- Sote-tiedon toissijaista käyttöä säätelevä lainsäädäntö:
    - Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)
    - Eurooppalainen terveysdata-avaruus (*European Health Data Space* EHDS, tulossa 2026)

Pilvipalveluiden turvallinen ja lainmukainen käyttö Pohjois-Karjalan hyvinvointialueella on aina perustuttava voimassa olevaan lainsäädäntöön.

6 Sanasto

Pilvipalvelu

Pilvipalvelut ovat internetin kautta tarjottavia palveluita, jotka mahdollistavat tietojen tallentamisen, käsittelyn ja hallinnan ilman, että käyttäjän tarvitsee ylläpitää omaa fyysistä infrastruktuuria, kuten palvelimia tai tietovarastoja. Pilvipalvelut tarjoavat monenlaisia resursseja, kuten laskentatehoa, tallennustilaa, tietokantoja, verkkoresursseja, ohjelmistoja ja analytiikkaa.

Infrastructure as a service (IaaS)

Tarjoaa perusinfrastruktuurin, kuten virtuaaliset palvelimet, tallennustilan ja verkkoresurssit. Käyttävä organisaatio voi hallita ja konfiguroida näitä resursseja tarpeidensa mukaan.

Esimerkkejä: Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine.

Platform as a service (PaaS)

Tarjoaa alustan sovellusten kehittämiseen, testaamiseen ja käyttöönottoon. Palvelu sisältää kehitystyökalut, tietokannat ja käyttöjärjestelmät**.**

Esimerkkejä: Heroku, Google App Engine, Microsoft Azure PaaS.

Software as a service (SaaS)

Tarjoaa valmiita ohjelmistoja, joita käyttävä organisaatio tai organisaation osa voivat käyttää suoraan internetin kautta. Ei vaadi asennusta tai ylläpitoa käyttäjän puolelta.

Esimerkkejä: Google Workspace, Microsoft Office 365, Salesforce.

On-premises -ratkaisu

On-premises -ratkaisuissa organisaatio omistaa ja hallinnoi itse infrastruktuurin, mikä vaatii suuria alkuinvestointeja ja jatkuvaa ylläpitoa, mutta tarjoaa täyden kontrollin.

IAM-palvelu (identity and access management)

Keskitetty palvelu, jossa asiakas voi hallita käyttöoikeuksia.[14]

Yksityinen pilvi (Private Cloud)

Pilvipalvelu, joka on omistettu yksinomaan yhdelle organisaatiolle. Se voi sijaita joko organisaation omissa tiloissa tai kolmannen osapuolen datakeskuksessa. Yksityinen pilvi tarjoaa korkean tason hallinnan ja tietoturvan, koska resursseja ei jaeta muiden organisaatioiden kanssa. Tämä tekee siitä erityisen sopivan organisaatioille, joilla on tiukat tietoturva- ja sääntelyvaatimukset.[15]

---

[14] Cirrus-hankkeen tekninen yhteenveto
[15] https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-private-cloud

Yhteisöpilvi (Community Cloud)

Pilvipalvelu, jota jakavat useat organisaatiot, joilla on yhteiset tavoitteet, vaatimukset tai intressit, kuten tietoturva- ja sääntelyvaatimukset. Yhteisöpilvi voi sijaita joko yhden osallistuvan organisaation tiloissa tai kolmannen osapuolen datakeskuksessa. Tämä malli mahdollistaa resurssien jakamisen ja kustannusten alentamisen samalla, kun se tarjoaa korkean tason tietoturvaa ja hallintaa.[16]

Julkipilvi (Public Cloud)

Pilvipalvelu, jota tarjoaa kolmas osapuoli ja joka on kaikkien halukkaiden organisaatioiden käytettävissä. Julkipilvipalvelut, kuten Amazon Web Services (AWS), Microsoft Azure ja Google Cloud, tarjoavat laajan valikoiman palveluita ja resursseja, jotka ovat helposti skaalattavissa. Julkipilvi on kustannustehokas ja joustava, mutta tietoturva ja hallinta ovat jaettuja palveluntarjoajan kanssa.

7 Tekoälypolitiikan hyväksyminen ja ylläpito

Tämän dokumentin on hyväksynyt Aluehallitus ja sen seurannasta ja ylläpitämisestä vastaa ICT- ja digipalvelut.

Päiväys:

Allekirjoitus:

[16] https://www.gartner.com/en/information-technology/glossary/community-cloud

8 Liitteet

Liite. Tietotyypit ja niitä vastaavat palveluehdot. Pohjautuu PiTuKri:ssa olevaan taulukkoon mutta lisätty SOTE asiakastiedon tietotyyppi.

Tietotyyppi	Pilvipalvelutyyppi	Fyysinen sijainti	Palveluntarjoaja	Lisätietoja
Julkinen	Ei rajoitteita	Ei rajoitteita	Ei rajoitteita	Soveltuvien suojausten arvioinnissa painotus riittävän eheyden ja saatavuuden varmistamisessa.
Salassa pidettävä	Ei rajoitteita	Ei rajoitteita	Ei rajoitteita	Mikäli ei sisällä henkilötietoja. Mikäli sisältää, vertaa riviin “Henkilötieto” alla.
Henkilötieto	Ei rajoitteita	EU/ETA	Ei rajoitteita	Palvelukokonaisuuden tulee täyttää henkilötietojen suojaamiseen liittyvä erityislainsäädäntö. Henkilötietojen käsittely edellyttää tietojen luonteen perusteella tehtävää riskiarviointia, mistä voi seurata rajoitteita myös tietojen fyysisen sijainnin, tietojen hallinnoinnin ja palveluntarjoajan valintaan. Henkilötietojen käsittelystä on sovittava tietosuoja-asetuksen (28art.) mukaisesti rekisterinpitäjän ja henkilötietojen käsittelijän välillä.
Varautumisen näkökulmasta suojattavat tiedot	Ei rajoitteita	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon kohdistuu tarve olla käytettävissä myös poikkeavissa olosuhteissa (varautuminen). Tiedon hallinnoinnin oltava mahdollista tilanteessa, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle.

Turvallisuusluokka IV	Ei rajoitteita	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut.
Suuri määrä salassa pidettävää tai/ja henkilötietoa (TL IV -kasauma)	Ei rajoitteita	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut.
Suuri määrä salassa pidettävää tietoa tai/ja TL IV -tietoa tai/ja henkilö- tietoa (TL III -kasauma)	Yksityinen/ yhteisö	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut.
TL III ja TL II	Yksityinen/ yhteisö	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut.
SOTE asiakastieto	Yksityinen/ yhteisö / julkinen	Suomi/EU/ETA	Ei rajoitteita ellei kyseessä ole korkean riskiluokan toiminto. Tällöin kansallinen viranomainen/ julkinen toimija/ yritys	SOTE tietoa ja sen käyttöä ohjaa omat lait eikä tietoa voi suoraan verrata edellä mainittuihin tietotyyppeihin. Pilvipalvelutyyppiä ja fyysistä sijaintia määrittää enemmän toiminnon riskitaso kuin itse tieto.