4.9.2018 TUVEDno-2018-379

Valtori TUVE-yksikön lausunto asiakirjaan ’Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta’

TUVE – yksikkö sai lausuntopyynnön *’Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta*’ – dokumenttiin.

Esitämme lausuntomme kokonaisuuksina eri teemoihin liittyen.

1 Julkishallinnon palveluiden digitalisaatio ja ICT -palveluhankinnat

Julkishallinnon digitalisaation edistyminen edellyttää koko ajan uusien teknologiapalveluiden arviointia ja käyttöönottoa. Teknologiapalvelut ovat kuitenkin vain väline viranomaisen tehtävän täyttämiseksi ja tieto on oleellinen resurssi sekä julkishallinnon sisäisessä toiminnassa että palveluita tuotettaessa.

Julkishallinnossa tuotettavalla ja käsiteltävällä tiedolla on aina tiedon omistajalle ja käyttäjälle jonkinlainen arvo ja merkitys. Julkishallinnollisen tiedon arvo voi olla vaikeasti määriteltävissä, se voi olla joko rahallinen tai julkishallinnollisen tehtävän käyttöarvoon perustuva. Julkishallinnossa käsiteltävän tiedon luottamuksellisuuden, saatavuuden, eheyden ja jatkuvuuden toteutusmallit tulee sovittaa tiedon arvoon ja käyttötarpeeseen perustuen. Lähtökohtaisesti ICT -palveluhankinnat tulisi toteuttaa siten että viranomaisen toiminta on turvattu kaikissa normaaliolojen poikkeustilanteissa ja soveltuvin osin poikkeusoloissa myös digitalisaation yleistyessä.

Ei liene tarpeen erotella ICT-palveluiden tuotantomalleja (on-premise, hosted, cloud, edge computing, jne.) linjattaessa tiedon sijaintiin ja hallintaan liittyviä asioita, samat vaatimukset ovat sovellettavissa ICT -palveluiden tuotantomallista riippumatta.

ICT – palveluhankintoja toteutettaessa tulee arvioida palvelutuotantomallin soveltuvuus toiminnallisista ja taloudellisista lähtökohdista ja valita aina soveltuvin vaihtoehto.

Valtion tieto- ja viestintätekniikkakeskus
TUVE-yksikkö
PL 56, 96301 Rovaniemi
Puhelin +358 295 480 151, Faksi +358 295 411 700 | valtori.fi

2 Osaaminen, sovelluskehitys ja palvelumuotoilu

Siirtyminen joustavien ICT – teknologiapalveluiden käyttöön tulee haastamaan ohjelmistohankkeiden osaamisen ja käytettävät sovelluskehityksen ja palvelumuotoilun menetelmät.

2.1 Osaamistarve ja -profiili

Hyödynnettäessä uusia teknologiapalveluita ostajan hankinta- ja teknologiaosaamisen tarve ja merkitys eivät vähene, vaan tarvittava osaamisprofiili muuttuu.

Tarvittava osaamisprofiili uusien teknologiapalveluiden hyödyntämisessä painottuu hieman eri tavalla eri teknologiapalveluita käytettäessä. Pilvipalveluiden hankinta sekä teknologiapalvelun konfiguraatio itsepalveluna vaatii erilaista osaamista verrattuna oman palvelutuotannon mahdollistamiseen.

Teknologiapalveluiden hyödyntämiseen ja tuottamiseen liittyvää *osaamistarvetta* arvioitaessa, kääntöpuolella on tarpeen täyttyessä myös *kyky tuottaa palvelua itsenäisesti* joka joissakin tapauksissa saattaa olla merkityksellinen tuotantomallia arvioitaessa.

2.2 Sovelluskehitys yhteiskäyttöisillä palvelualustoilla

Joustavien ICT – palveluiden käyttöönoton vaikutus sovelluskehityksen menetelmiin tulee ottaa huomioon.

Pilvipalvelupohjainen sovellusalusta päivittyy hyvin tiheään tahtiin. Valtionhallinnon sovelluksilla on tyypillisesti pitkä elinkaari ja kokemukseemme perustuen niiden päivitystiheys on ollut todella pitkä. Asiakkaat ajavat hyvin vanhoilla sovellusversioilla omia substanssisovelluksiaan.

Pilvipalveluita käyttöönotettaessa pitää huomioida ketterän kehittämisen tavat ylläpitää omia sovelluksia koska alusta voi muuttua hyvin nopealla aikataululla (esim. SharePoint tai Exchange pilvipalveluversioiden päivitykset tapahtuvat aikataululla johon asiakkaalla ei ole vaikutusvaltaa, uusin versio on käytössä dynaamisesti per heti). Esimerkkinä SharePoint komponentteihin perustuva järjestelmä. Jos järjestelmä sijoitetaan pilvipalveluun, sovellustoimittajan tulee varmistaa tietojärjestelmän yhteensopivuus sovellusalustapalvelun kanssa hyvin nopealla aikataululla.

Joustavien ICT – palveluiden hyödyntämisessä tulee huomioida myös tietojen yhteiskäyttö ja siirrettävyys eri palvelualustojen välillä, jotta vältytään liialliselta riippuvuudelta ICT – palveluntarjoajasta. Sovelluskehityksessä tulee varmistaa että tieto ei jää palveluntarjoajan palveluun siten että sen migraatio tiedon elinkaaren aikana on liian hankalaa toteuttaa tiedon omistajan resurssein.

Siirtyminen joustavien ICT – palveluiden (PaaS, SaaS) käyttöön tulee haastamaan julkishallinnon tietojärjestelmähankkeiden toteutusmallit ja siirtyminen ketterän kehityksen menetelmiin on edellytyksenä pilvipalveluiden täysimääräiselle hyödyntämiselle.

3 Sopimukset, budjetointi, kustannukset

Kustannustietoisuuden merkitys ICT – palveluhankinnoissa tulee digitalisaation edistymisen myötä vielä kasvamaan. Uusien teknologiapalveluiden lisääminen keinovalikoimaan mahdollistaa julkishallinnon digitalisaation joustavasti ja kustannustehokkaasti sekä organisaation sisäisessä toiminnassa että palvelutoiminnassa.

Pilvipalveluiden käytöllä on vaikutusta budjetinhallintaan.

Pilvipalvelut ovat pitkälti subscription tyyppisiä, eli käyttöoikeus on niin kauan kun käytöstä maksetaan. Valtionhallinnon taloushallinnon perusteissa on pitkälti lähdetty ajatuksesta jossa ns. perpetual (pysyviä) käyttöoikeuksia suositaan. Ts. jos budjettissa oleva rahoitus pitää siirtää muualle (esim. poikkeustilanne) tietojärjestelmän käyttöoikeus lakkaa per heti. Tämä on tietysti ohjeistuksessa huomioitava jatkuvana kustannuksena. Palvelua hankittaessa lienee tarpeen suunnitella palvelun päättymiseen tai palveluntarjoajan vaihtamiseen liittyvät menettelyt tiedon siirrettävyydestä.

Lisäksi budjetoinnin kannalta haasteeksi saattaa muodostua käyttöasteen mukaan skaalautuvien palveluiden kustannusten hallinta, jota riskiä toki voidaan kompensoida hyvällä teknologiaosaamisella ja sopimushallinnalla.

ICT – palveluhankinnoissa sopimusten ymmärtäminen ja niiden ehtoihin vaikuttaminen tulee olemaan merkittävässä roolissa jatkossakin, erityisesti mikäli niissä tulee huomioitavaksi luokiteltujen tietojen käsittely.

4 Tietoturva ja tietosuoja

ICT – palveluhankinnoissa tulee jatkossakin kiinnittää huomiota tietoturvan ja tietosuojan toteutumiseen tiedon suojaamiseksi. Pilvipalveluita hyödynnettäessä, erityisesti IAAS/PAAS tuotantomalleilla, tietoturvan peruskomponenttien toteuttaminen jää palvelun omistajan vastuulle ja vaaditaan erittäin vaativaa osaamista jo palvelun tai järjestelmän hankintavaiheessa.

ICT – palveluntarjoajaa arvioitaessa tulee huomioida tarjoajan kyvykkyys tuottaa palvelu riittävän tietoturvallisesti sekä GDPR vaatimukset täyttävällä tavalla. Luokitellun tiedon osalta dokumenttiluonnoksessa mainitaan kohdissa 6.8 ja 6.9, että edellytyksenä on tietoturva- ja tietosuoja-asioiden asianmukainen toteutus. Jatko-ohjeistuksessa tulisi kuvata selkeästi ne vaatimukset, mihin viitataan.

ICT – palveluita sijoitettaessa ulkopuolelle sekä identiteetin- että pääsynhallinnan toeutusmallit tulee myös huomioida. Single-sign on –tyyppinen autentikaatio mahdollistaa palveluiden sujuvan loppukäyttäjäkokemuksen, mutta vaatii sekä palveluntarjoajan että käyttäjän luotettavan tunnistamisen. Identiteetin- ja pääsynhallinnan toteutusmallit tulevat huomioitavaksi ohjelmistohankkeissa, jotta voidaan varmistaa sujuva käyttökokemus.

Julkiseksi luokitellun tiedon sijoittaminen ulkoiselle ICT – palvelualustalle on mahdollista ja jopa suotavaa tiedon saatavuuden varmistamiseksi suurelle yleisölle joustavasti. Julkisen tiedon osalta tulee huomioitavaksi tietoturvaperiaatteista saatavuuden lisäksi myös tiedon *eheys*. Ei ole yhdentekevää miten ja kenen hallintaan julkinen tieto asetetaan. (Ks. kappale 6.)

Palvelun tietoturvallisuuden ja – suojan toteutuminen koko ICT-palveluketjun osalta tulee huomioida, samalla tavalla kuin jatkuvuus huomioidaan ”päästä päähän”. Samalla myös palveluntarjoajan alihankintaketjun riskit saattavat kohdistua pilvipalveluympäristöön.

Pilvipalveluiden käyttö lisää verkkokapasiteetin käyttötarvetta merkittävästi.

Jos ulkoisen ICT – palvelualustan suorakäyttö ilman reititystä sisäverkon kautta sallitaan laajamittaisesti, Havaro tyyppisten havainnointipalveluiden käyttö estyy koska valtaosa liikenteestä ohittaa keskitetyt seurantajärjestelmät. Vastavuoroisesti jos tietoliikenne kierrätetään ulkoista ICT – palvelualustaa käytettäessä aina Havaro tyyppisten palveluiden kautta, seurantajärjestelmien kapasiteetti pitää kasvattaa merkittävästi.

Dokumenttiluonnoksen kohdassa 5.3 mainitaan, että tiedon kriittisyydestä riippuen voi tulla vaatimukseksi sijoittaa tieto ja sen hallinta Suomeen. Jatko-ohjeistuksessa tulisi kuvata ne kriteeristöt ja luokittelut, mihin viitataan.

5 Varautuminen ja jatkuvuus

Linjattaessa julkishallinnollisen tiedon sijaintia ja hallintaa tulee tiedon suojaustason lisäksi arvioida myös tiedon saatavuuden ja jatkuvuuden vaikutus sen omistaja- tai käyttäjäorganisaation toimintaan sekä sisäisessä- että palvelutoiminnassa. Varautumisen ja jatkuvuuden vaatimukset ICT – palveluhankinnoissa tulee arvioida tiedon merkitykseen ja tarkoitukseen perustuen.

Jatkuvuutta arvioitaessa tulee huomioida ICT – palvelualustan tavoitettavuus tiedon käyttäjille koko ICT – palveluketjun häiriötilanteissa (paikalliset-, kansalliset-, kansainväliset- ja kyseisen palveluntuottajan ja sen sijainnin häiriöt).

Jatkuvuuden arvioinnissa tulee arvioida palvelun jatkuvuuden lisäksi tiedon jatkuvuus pidemmällä aikavälillä, mikäli tieto on sellaista että se pitää säilyttää. ICT – palveluhankinnassa tulee huomioida tiedon siirrettävyys palveluntarjoajaa vaihdettaessa, millä menetelmin ja kustannuksin julkishallinnon tieto on poimittavissa ICT – palveluntarjoajan palvelualustalta toiselle palveluntarjoajalle tai tarvittaessa omaan ICT-ympäristöön.

Tiedon jatkuvuuden ja saatavuuden hallinnan merkitys realisoituu ulkoisen palvelutuottajan häiriötilanteessa kun yhteys palveluntarjoajaan menetetään jostain syystä ja sopimusmenettely ei tarjoa menetelmiä riskin kompensoimiseksi.

6 Riskienhallinta

Tiedon merkitys organisaation sisäiselle- ja palvelutoiminnalle tulee tiedostaa jo ICT-palveluhankintaa tehtäessä. Tietosuojatasojen ja tietoteknisen varautumisen tasojen lisäksi tulee huomioitavaksi organisaation ja tiedon jatkuvuuden hallinta.

Riskienhallinnan tueksi julkishallinnon organisaatioille tulee luoda menetelmät riskien hahmottamiseksi ja luokittelemiseksi. Riskejähän ovat esim. tiedon menetys väliaikaisesti tai pysyvästi, tiedon vuotaminen, tiedon hallitsematon muuttuminen, palvelualustan kustannusten hallitsematon kasvu, jne.

Riskien kompensaatiomenetelmiä voi olla mm. sopimuksen takuu ja sanktiomenettelyt, lainsäädäntöön sitoutuminen, palveluiden hajauttaminen, tiedon sijoittamisen rajoittaminen, jne.

Häiriötilanteisiin ja kyberuhkiin liittyvien riskien lisäksi julkishallinnon varautumisessa tulee huomioida myös hybridivaikuttamisen keinot ja niiden aiheuttamat riskit joko suoraan tai välillisesti. Hybridivaikuttamisen menetelmät voivat olla epäsuoraa vaikuttamista kohdeorganisaatioon pidemmällä aikavälillä, esim. organisaation palveluntarjoajien tai kumppanien kautta. Esim. ICT- palveluntarjoajayrityksen ostaminen kybervaikuttamisen mahdollistamiseksi, ICT – palveluntarjoajan ajaminen konkurssiin, jne.

Asiakirjaluonnoksen kohdassa 5.3 tulkinnanvarainen lause:
”Kun tieto tai palvelut sijaitsevat EU:n tai ETA:n alueella, tai sen ulkopuolella, riski tietoturvan tasosta laskee erityisesti koskien kyseistä palveluntarjoajaa ja maata koskevan lainsäädännön johdosta sekä tietoliikenteen osalta esimerkiksi tiedon saatavuuden osalta.” Tuota lausetta voisi tehdä selkeämmäksi.

Riskienhallintaa ICT – palveluhankinnoissa tulee toteuttaa hankinnan aikana mutta koko ajan myös palveluaikana. Tilanne sopimusehtojen, lainsäädännön, palveluntarjoajan omistajuuden suhteen voi muuttua myös sopimusjakson aikana.

7 Lainsäädäntö ja toimivalta

ICT – palveluita hankittaessa palveluntarjoajan soveltama oikeuskäytäntö tulee tiedostaa kun arvioidaan mitä tietoa palveluun ollaan sijoittamassa.

Oikeuskäytäntö sisältää pakkokeinoja joissa tietojärjestelmiä tai siihen liittyvää dataa takavarikoidaan viranomaisten toiminnan tutkimisessa. Samojen pakkokeinojen soveltaminen tulee varmistaa tiedon sijoittuessa ulkomaille jolloin virkarikostutkinnassa ja muussa vastaavassa tilanteessa tiedonsaanti varmistetaan.

Palveluntarjoajan sitoutuminen kansalliseen ja EU lainsäädäntöön hankinnan hetkellä ja myös palvelutuotannon aikana tulee huomioida ja arvioida sen vaikutukset palvelutuotantoon ja siihen aiheutuviin riskeihin.

8 Vaatimustenmukaisuus

Luokiteltujen tietojen käsittelystä on annettu vaatimuksia ja jaettujen palvelualustojen käytössä näiden vaatimusten toteutuminen voi olla hyvin hankalaa tai mahdotonta todentaa mikäli ostajan neuvotteluasema on heikko palveluntarjoajaan nähden. Voi olla että palveluntarjoaja ei mahdollista kansallisen arviointilaitoksen tarkastustoimintaa omissa tuotantotiloissaan, jolloin vaatimustenmukaisuuden arviointia ei voi suorittaa.

Haasteena on varmistua palveluntarjoajan tuotannossa käytettävien palveluiden elinkaarenhallinnan toteutusmalleista. Jaetussa kapasiteetissa on hyvin vaikeaa varmistua laitteiston massamuistien käsittelystä nykyvaatimusten mukaan, esim. ylikirjoitusohje, varmistusten käsittely, jne.

Lisäksi haasteeksi voi muodostua palveluntuottajan koko alihankintaketjun vaatimustenmukaisuuden varmistaminen. Samaan palveluympäristöön voi liittyä useita alihankkijoita, joiden toiminta ja riskit saattavat kohdistua kyseiseen palveluympäristöön.

Asiakirjaluonnoksessa mainitaan luokitellun tiedon sijoittamiseen liittyen ”viranomaisen hyväksymästä ratkaisu”. Tarkoittaako viranomainen tässä tapauksessa yleisen käytännön mukaan kyseiselle suojaustasolle hyväksyttyä arviointilaitosta?

Miten varmistetaan että palvelun päättymisen jälkeen viranomaistiedot eivät jää palveluntarjoajalle (luokittelusta riippumatta).

9 Tuotantomallit, vaihtoehtoiset ratkaisut ja ympäristöystävällisyys

9.1 Tuotantomallien arviointia

Pilvipalvelutuotantomalli on arvioitu joustavaksi, mutta joustavuus voidaan käsittää monella tavalla. Pilvipalvelu ei ole joustava esim. ostajan neuvotteluasemaan nähden tai teknologisilta ominaisuuksiltaan. Toisaalta pilvipalvelu voi olla varsin joustava käyttöönottomenettelyiltään ja kapasiteetiltaan.

Pilvipalvelumallin valinta vaikuttaa vahvasti palvelun tietoturvallisuuteen, uhat kasvavat jos ostetaan pelkästään infrastruktuuri palveluna. Tässä mallissa tietoturvakorjausten ja uhilta suojautuminen on asiakkaan vastuulla. Pilvipalveluita käytettäessä pitäisi suosia palvelualustoja joissa käytetään palveluntarjoajan tarjoamia sovellustason komponentteja jolloin ylläpito on toimittajan vastuulla. Tällöin kuitenkin käänteisesti syntyy vaatimus nopeasta sovelluskehityksestä

Verkkoratkaisuissa pitää huomioida pilvipalveluiden mahdollisuudet tuottaa ratkaisu dedikoitujen omien tietoliikenneyhteyksien kautta, jolloin tietoliikennettä ei reititetä julkisen verkon kautta.

9.2 Vaihtoehtoiset ratkaisut

Pilvipalveluteknologioita (esim. Azure stack) voi hyödyntää myös ”on premise” tuotantomallilla, jolloin tiedon sijoittamiseen ja hallintaan liittyviä riskejä on helpompi hallita, mutta pilvipalvelualustan teknologisia etuja joustavuuden suhteen voidaan saavuttaa.

9.3 Ympäristöystävällisyys

ICT – hankintoja toteutettaessa ympäristöystävällisyys tulee arvioida palveluntarjoajaa valittaessa. Tuotantomallina pilvipalvelut mahdollistavat teknologiakomponenttien korkean käyttöasteen, mutta se on vain yksi osa arvioitaessa energiatehokkuutta tai palveluntarjoajan ympäristötietoisuutta. Mittakaavaetu ei tuo automaattisesti energiatehokkuutta. Mittakaavaetu tuo hankittujen resurssien hyvää käyttöastetta joka on osa energiatehokkuutta, mutta ei takaa vaikkapa kasvihuonepäästöjen vähentämistä, lämmön talteenottoa tms. energiatehokkuutta.

10 Yhteenveto ja suositukset

Linjaus julkishallinnollisten organisaatioiden tietojen sijoittamisesta ja hallinnasta on viranomaistoiminnalle erittäin merkityksellinen ohjaus, jonka tulee mahdollistaa julkishallinnon toiminnan ja palveluiden digitalisaatio riskienhallinta huomioiden. Julkishallinnon digitalisaatio tulee toteuttaa siten että se ei vaaranna viranomaistoiminnan jatkuvuutta normaaliolojen poikkeustilanteissa, poikkeusoloissa tai poikkeusolojen normalisoituessa.

Linjauksella tulee varmistaa että julkishallinnollisen tiedon sijoitusta arvioitaessa digitalisaatioon kohdistuvat kyber- ja hybridiuhkat tulevat asiallisesti huomioiduksi palveluita toteutettaessa.

Tuemme dokumenttiluonnoksen kappaleessa 6 esitettyjä linjausesityksiä, joissa on hyvin tuotu esille samoja teemoja mitä itse käsittelimme lausunnossamme.

TUVE – yksikön suositukset:

- julkishallinnollisten organisaatioiden tulee arvioida tiedon sijoittamiseen ja hallintaan liittyvät ratkaisut tuotantomallista riippumatta (sekä pilvipalveluissa että perinteisemmillä tuotantomalleilla)
- riskiperusteinen lähestymistapa ICT – palvelutuotantomalleja arvioitaessa tulee perustua tiedon luokitteluun ja tarkoitukseen (suojaus, saatavuus, jatkuvuus)
- oleellisten riskien tunnistamiseen ja arviointiin ICT – palveluhankinnoissa tulee laatia tarkennettu ohjeistus
- riskiarviointi tulee tehdä tietoturva- ja kyberuhkien lisäksi myös hybridivaikuttamisen uhat huomioiden (esim. sijoituspaikan lainsäädännöllinen, poliittinen ja taloudellinen tilanne)

Linjausesityksessänne mainituilla jatkotoimenpiteillä tulee tarkentaa dokumenttiluonnoksessanne esitettyjä vaatimuksia ja tukea julkishallinnollisten

organisaatioiden ICT – palveluihin liittyvien riskien arvioinnin osaamista ja menetelmiä palveluita hankittaessa.

Lisätietoja:

Pääarkkitehti, TUVE -palvelut Petri Alariesto

Palvelujohtaja, TUVE -palvelut Hannu Naumanen

Rovaniemellä 4.9.2018

Valtori TUVE -yksikkö