

Asia: VM/276/00.01.00.01/2018

Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta

Yhteenveto

Kommentit yhteenvetoon:

Pilvipalvelujen suurin arvo sekä tietotekniikasta vastaaville yksiköille että loppuasiakkaille on joustavuuden mahdollistaminen. IT-kentän muutostahdin kasvaessa pilvipalveluista koostuvan palveluportfolion hallinnointi tulee muodostumaan useille organisaatioille kriittiseksi menestystekijäksi. Koska pilvipalvelujen räätälöinnillä menetetään pilvipalvelujen kustannus- sekä muut edut, muutostarpeisiin vastataan konfiguroitavuuden rajojen tullessa vastaan pääosin vaihtamalla käytössä olevia palveluja. Tästä syystä pilvipalvelustrategiassa kannattaisi ohjata hankintayksiköt huomioimaan sen, että pilvipalveluja hankittaessa kannattaa varautua perinteisiä tietojärjestelmiä lyhyempiin elinkaariin.

Taustaa linjauksille

Kommentit taustaan:

-

Linjausten tavoitteet

Kommentit tavoitteisiin:

-

Pilvipalveluiden edut sekä toteutus- ja palvelumallit

Kommentit:

-

Pilviteknologian edut

Kommentit:

-

Palvelumallit

Kommentit:

-

Toteutusmallit

Kommentit:

-

Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Kommentit:

Pilvipalvelujen (erityisesti PaaS ja SaaS) kanssa on kiinnitettävä huomiota exit-ehdoin. Osa valmispalveluista ei mahdollista tietojen siirtämistä palvelusta ulos ja seuraavaan palveluun toimittaja- ja teknologiariippumattomalla tavalla. Useimmiten tämä ei ole merkittävä ongelma, mutta joidenkin tietoaisteistojen tapaksissa tämä voi heikentää tilaajan neuvotteluasetelmaa ja synnyttää voimakkaan toimittajalukon. Hyvä esimerkki kriittisestä tietoaisteistosta, jonka siirtyminen puhtaasti pilvipalveluun saattaisi aiheuttaa laajoja ongelmia, on käyttäjien identiteetin hallinta.

Tiedon käsittelyn vaatimukset

Kommentit:

-

Palveluiden ohjaus

Kommentit:

Eryyisesti SaaS- ja PaaS-tyyppiset ratkaisut mahdollistavat aktiviteettipohjaisen hinnoittelun. Ne kannattaa asettaa yleisesti tavoitteiksi, koska sopimuksien ja kustannusten skaalautuvuus helpottuu, SLA-tyyppisissä asioissa toimittaja ja tilaaja ovat ikään kuin samassa veneessä (esim. nurin olevassa palvelussa ei ole aktiviteettia!) ja palvelujen hankinta on mahdollista joustavammin erilaisten puitejärjestelyiden kautta. Tämä vaatii kuitenkin hankintayksiköiltä lisää osaamista, jonka rakentamiseksi suositellaan toimenpiteiden suunnittelua ja käynnistämistä.

Haasteet

Kommentit:

-

1. Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta

Kommentit:

-

2. Tiedon sijaitessa Suomen rajojen ulkopuolella erityistä on kiinnitettävä huomiota sopimukseen, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen

Kommentit:

Ulkomaiset toimittajat, joiden palveluilla on merkittävää mittakaavaetua, eivät tyypillisesti suostu asiakaskohtaisiin sopimuksiin ja ehtoihin, vaan ne on otettava vastaan as-is. Tämä rajaa voimakkaasti käytettävissä olevia toimittajia, erityisesti kun yleisistä pilvipalveluista on jo havaittu erilaisia puutteita.

3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset

Kommentit:

Ks. kommentti aktiviteettipohjaisesta hinnoittelusta. Se ratkaisee PaaS/SaaS tapauksissa useita tämän osa-alueen haasteita, joskin vaatii organisaatiolta hieman enemmän kypsyyttä.

4. Mikäli pilvipalvelut tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita

Kommentit:

-

5. Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti vähintään kerran vuodessa ja oleellisten sopimusehtojen muuttuessa.

Kommentit:

-

6 Viranomaisen ylläpitää listaa hyväksytyistä palveluntarjoajista

Kommentit:

Voisiko keskitetty julkisen hallinnon lista selkiyttää päätöksentekoa ja levittää tietoa hyväksytyistä ratkaisuksista viranomaisten välillä?

7. Julkisen tiedon käsittelyä ei rajoiteta

Kommentit:

-

8. Henkilötietoa ja suojaustason IV tietoa voi käsitellä julkisessa pilvessä, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu

Kommentit:

Ulkomaiset toimittajat, joiden palveluilla on merkittävää mittakaavaetua, eivät tyypillisesti suostu asiakaskohtaisiin sopimuksiin ja ehtoihin, vaan ne on otettava vastaan as-is. Asianmukainen todentaminen saattaa jäädä usein pilvipalvelun toimittajan aiemmin suorittamaksi itsearviointiksi tai 3. osapuolen tekemäksi arviointiksi, jossa on hyödynnetty esim. VAHTI- tai Katakri-kriteeristöistä eroavaa ohjeistusta. Tämän ongelmatiikan käsittely vaatii akuutisti lisäohjeistusta.

9. Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa

Kommentit:

Jos pilvipalveluille ei myönnetä tietoisesti hyväksyntää ja osa tiedoista siirtyy hallitsemattomasti pilvipalveluihin, tämä voi aiheuttaa laajamittaisen ongelmatilanteen. Riskiä pitäisi hallita painottamalla hyväksyntöjen perustumista voimassaolevan tietoturvallisuuden ohjeistuksen (VAHTI) mukaiseen arviointiprosessiin ja kriteeristöihin. Hyväksynnän tulee perustua viranomaisen suorittamaan kokonaisarvioon, joka perustuu riskien mallinnukseen sekä 3. osapuolen (yleensä lain tietoturvallisuuden arviointilaitoksista mukainen yritys) suorittamaan arviointiin.

Suosituksia toimenpiteiksi

Kommentit:

Suosittelimme selkiyttämään tietoturvallisuuden hyväksyntään pilvipalveluissa, huomioiden niiden huonon todennettavuuden, liittyvää ohjeistusta. Lisäksi suosittelimme huomioimaan linjauksissa aktiviteettipohjaisen hinnoittelun tarjoamat hyödyt sekä tarpeen varmistaa palvelujen helpon vaihdettavuuden.

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Esitetyt linjaukset ovat pääsääntöisesti hyvät ja kehittävät toimintaympäristöämme joustavampaan suuntaan. Joidenkin kohtien toimeenpanoon liittyvät haasteet kaipaavat kuitenkin ohjeistuksen ja linjausten jatkokehittämistä.

Lehtisalo Mikko
Oikeusrekisterikeskus - Tietojärjestelmäpalvelut