Helsingin kaupunki, Kaupunginkanslia

Lausunto

05.09.2018

Asia: VM/276/00.01.00.01/2018

Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta

Yhteenveto

Kommentit yhteenvetoon:

-

Taustaa linjauksille

Kommentit taustaan:

-

Linjausten tavoitteet

Kommentit tavoitteisiin:

Esityksen yleissävy antaa vaikutelman siitä, että patistetaan pilvipalveluiden/kapasiteetin käyttöön ja että on-premise olisi aina paras. Tämä kuva muodostui useammallakin asiantuntijalla tekstiä lukiessa. Olisi ehkä syytä miettiä esityksen painopisteitä ja muotoilua tältä kannalta.

Pilvipalveluiden edut sekä toteutus- ja palvelumallit

Kommentit:

-

Pilviteknologian edut

Kommentit:

-

Palvelumallit

Kommentit:

-

Toteutusmallit

Kommentit:

Sisältö painottuu siten liikaa yleisluontoiseen kuvaukseen mitä eri palveluntuotantotavat ovat (ihan perustietoa) ja liian vähän siihen, millaisissa tilanteissa saatavuusvaatimukset edellyttävät kotimaista pilveä tai dedikoitua ratkaisua. Saatavuuden osalta on vain maininta, että pilvipalvelut (EU-pilvi, globaali) eivät sovellut tärkeille palveluille. Tätä pitäisi huomattavasti avata lisää. Pilvipalveluita pitäisi katsoa toteutustavoittain. Nyt kaikkia pilvipalveluita käsitellään yhdessä. On kuitenkin aivan eri asia toteuttaa palvelu tilaajan vaatimuksien mukaisesti pilvialustalle kuin ostaa SaaS:ina palvelu, jonka tietoturvallisuuden tasosta on päättänyt palvelun omistaja.

Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Kommentit:

-

Tiedon käsittelyn vaatimukset

Kommentit:

Turvaluokitellun aineiston käsittely pilvessä on myös liian ohuesti. Tässä viitataan yleisluontoisesti vain että STIV:tä voisi käsitellä pilvessä jos salaamisesta jne. on huolehdittu ja STIII viranomaisvaatimuksen mukaan. Kuitenkin salaamisesta ei pilvipalvelussa ole merkitystä, jos sivulliset pääsevät tietoihin esimerkiksi ylläpidon yhteydessä käsiksi. Tässä tulisi tarkemmin avata, että salaamisella pitää estää pääsy jo STIV-tason tietoihin niin, että sivullisella ei ole mahdollista päästä tietosisältöihin esimerkiksi ylläpidon yhteydessä. Tämä on erityisen tärkeää pilvipalvelussa, jossa käsittelyoikeuksia ei todellisuudessa pystytä valvomaan.

Erittäin tervetullut on maininta, jossa todetaan, että poikkeusoloissa tarvittavat järjestelmät on sijoitettava Suomeen.

Palveluiden ohjaus

Kommentit:

-

Haasteet

Kommentit:

Haasteissa puhutaan tiedon sijainnista ja hallinnasta. Pitäisikö puhua myös tiedon käsittelystä?

Haasteissa mainitaan myös yksipuoliset sopimusehdot. Pitäisikö sen lisäksi nostaa esiin myös sopimusehtojen neuvottelujen haasteet eli niistä ei kaikkien osalta käytännössä voi edes neuvotella?

Pilvipalveluiden osalta yksi mielenkiintoinen kysymys on palvelun auditointioikeudesta eli kuka voi auditoida ja miten, millä tavoin auditointitietoja asiakkaat voivat ja saavat käyttöönsä erityisesti jos on esim. SLA-ongelmia tai muita epäilyjä palvelun luotettavuudesta.

Toinen tyypillinen pilvipalvelun piirre on tarjota tukipalvelua 24/7 mallilla, siten että tukiorganisaatio on maantieteellisesti hajautettu (saatavuuden parantamisen ja kustannustehokkuuden vuoksi).

Maantieteellinen hajautus saattaa tarkoittaa tietojen käsittelyä Suomen rajojen ulkopuolella tai EU/ETA alueen ulkopuolella, vaikka itse ko. pavelu sijaitseekin esim EU/ETA-alueella.

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

Kommentit:

Perusteluissa voisi korostaa enemmän sitä, että vastuut siirtyvät näissä hankinnoissa, erityisesti SaaS-pohjaisissa palvelutasojen ja palvelulaadun hallintaan omasta teknisestä osaamisesta (esim. tietokanta). Asioita on huomioitava enemmän siis sopimuksellisesti kuin ennen. Kysymys on siis myös ostajan osaamisen ja kyvykkyyksien muutostarpeesta.

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

Kommentit:

”Palvelun hankkijan on varmistettava tiedon saatavuus erilaisissa tilanteissa sekä myös palveluntarjoajaa vaihdettaessa.” Tämä kyllä koskee kaikkia pilvipalvelutarjoajia. Jossain ehkä olisi syytä mainita se, että vaikka palveluntarjoaja olisikin Suomalainen, se ei automaattisesti tarkoita sitä että palvelu sijaitsee Suomessa. Alihankintaketjut voivat olla pitkiä myös pilvipalveluissa.

3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset

Kommentit:

-

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

Kommentit:

Palveluhyöty sekä palvelutakuu on termeinä syytä määritellä jossain tai sitten viitata lähteeseen jossa ne ovat määritelty. Kumpikaan ei ole vakiintunut ja sisällöllisesti yksikäsitteinen termi, ja ilman määrittelyä linjausten ymmärtäminen jää tulkinnanvaraiseksi.

Palveluhyötyyn nimittäin liittyy hyvin monenlaisia asioita eri toimijoiden kannalta. Esim. käyttäjän kannalta pilvipalvelun mahdollistaa, kun autentikointi on hoidettu oikein, palvelun käytön hyvinkin liikkuvasti ja eri verkoista paljon helpommin kuin omaan konesallin ja oman verkon ”sisään” paketoitu palvelu.

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

Kommentit:

Kuten minkä muunkin palvelun. Siinä mielessä linjaus on "itsestäänselvyys" ja voi johtaa harhaan siitä, että ettieikö niitä "itsekin tuotetettujen" palveluiden hyötyjä pitäisi arvioida säännöllisesti.

6 Viranomainen ylläpitää listaa hyväksytyistä palveluntarjoajista

Kommentit:

Kuka on mainittu viranomainen (ajateltu)?

Ovatko myös listalle pääsyn valintaperusteet avoimia eli listan hyödyntäjä myös tietää millä perusteilla se on listalle päässyt? Hyödynnetäänkö työssä globaaleja sertifikaatteja ja niiden sisältöjä vai ollaanko tekemässä jotain kansallista kriteeristöä, mihin globaalit toimijat eivät lähtökohtaisesti lähde mukaan ja näin rajoitetaan vaihtoehtoja mahdollisesti merkittävästikin?

”Listalla olo ei ole ennakkovaatimus hankintoihin osallistumiselle, mutta ennen kuin palvelu voidaan ottaa käyttöön, sen on täytettävä määritellyt vaatimukset.”

Mitä mainitussa lauseessa tarkoitetaan määritellyillä vaatimuksilla? Listalle pääsyn edellytykset vai palvelua hankkivan tahon asettamat vaatimukset ja , missä ne määritellään?

Olisiko linjauksessa tai erikseen täsmennettävä seuraavia seikkoja ja huomioita. Palveluntarjoaja saattaa saatavuuden varmistamiseksi erityisesti poikkeustilanteissa kahdentaa/monentaa palvelun maantieteellisesti, muuttaa dynaamisesti palveluin sijaintipistettä. Joissakin tilanteissa pilvipalvelun oheispalvelu – esimerkkinä varmistuspalvelut – tai osa palvelusta saattavat sijaita maatieteellisesti toisaalla kuin mitä ”pääpalvelu”.

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:

-

9. Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa

Kommentit:

-

Suosituksia toimenpiteiksi

Kommentit:

-

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

-

Miskala Kari
Helsingin kaupunki, Kaupunginkanslia

Andersin Ari
Helsingin kaupunki, Kaupunginkanslia - Tietohallinto