Valtion tieto- ja viestintätekniikkakeskus Valtori

Lausunto

07.09.2018 Dnro 110/00.04/2018

Asia: VM/276/00.01.00.01/2018

Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta

Yhteenveto

Kommentit yhteenvetoon:

Linjaus 8. ”Henkilötietoa ja suojaustason IV tietoa voi käsitellä julkisessa pilvessä, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu.” on kannatettava ja erittäin keskeinen Valtorin palvelutuotannon kannalta. Linjaukseen syytä kirjoittaa ne periaatteet, joiden mukaan tietoturvan ja -suojan voidaan todeta olevan asianmukaisesti toteutettu ja todennettu.

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:

Kohdassa 5.1.2 on seuraava kappale: ”Mikäli kyseessä on laaja-alainen, esimerkiksi koko julkiseen hallintoon tai valtionhallintoon tarkoitettu yhteinen palvelu, palvelun omistajan tulee ennen palvelun toteuttamista varmistaa sen asiakkailta palvelun tuottamiseen liittyvät edellytykset koskien salassa pidettävien tietojen ja toiminnan jatkuvuudelta edellytettäviä vaatimuksia.”

Valtori toimii linjauksessa esitettynä palvelun omistajana, joka tuottaa valtionhallintoon asiakkailleen laaja-alaisia yhteisiä palveluja ja siten sen tulee linjauksen mukaan varmistaa asiakkailtaan mitä edellytyksiä palvelun tuottamiseen liittyy koskien asiakkaan salassa pidettäviä tietoja ja toiminnan jatkuvuutta. Valtori tunnistaa tämän velvoitteen ja noudattaa sitä toiminnassaan. Haasteena on, että asiakkaiden näkemys ei ole yhtenevä, vaan eri asiakkailla on erilaisia vaatimuksia ja tulkintoja asiasta. Valtori pyrkii, tukeutumalla olemassa oleviin säädöksiin ja linjauksiin, integroimaan erilaiset asiakasnäkemykset/-tarpeet tuottamiinsa palveluihin. Keskeinen asiakkaita askarruttava asia erilaisten pilvipalveluiden käytön mahdollistamiseksi (tiedon sijainti huomioiden) kulminoituu kysymykseen, millä edellytyksillä/kriteereillä ns. ’pilvipalvelut’ ovat todennettavissa olevan soveltuvia luokitellun tiedon käsittely- ja tallennusympäristöiksi ja kenen toimesta todentaminen tulee tehdä. Näihin kysymyksiin linjauksessa tulisi ottaa selkeästi kantaa.

Tiedon käsittelyn vaatimukset

Kommentit:

-

Palveluiden ohjaus

Kommentit:

-

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 sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen

Kommentit:

-

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:

-

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

Kommentit:

-

6 Viranomainen ylläpitää listaa hyväksytyistä palveluntarjoajista

Kommentit:

-

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:

Tarkennettava, mitä tarkoittaa ”Suomessa tai EU alueella sijaitsevan toimijan hallinnassa”. Tällä ilmeisesti tarkoitetaan palvelun hallintaa tuottavien henkilöiden fyysistä sijaintia. Tämän tulisi koskea kaikkia palvelun hallintaa tuottavan organisaation ja sen alihankkijoiden henkilöstöä, joilla on pääsy järjestelmään. Voiko ko. organisaation EU:n ulkopuolella sijaitsevasta toimipisteestä tuottaa hallintapalveluja, ja jos voi niin minkälaisia? Onko esim. etätyön tekeminen EU-alueen ulkopuolelta mahdollista? Lisäksi on syytä huomioida haasteet muiden kuin Suomessa pysyvästi asuvien henkilöiden henkilöturvaselvitysten haasteet, ts. käytännössä muiden selvittäminen on joko erittäin hankalaa tai mahdotonta.

Suosituksia toimenpiteiksi

Kommentit:

-

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Valtori näkee erittäin tärkeänä julkisen hallinnon yhteisten linjausten muodostamisen pilvipalvelujen suunnitteluun, hankintaan ja käyttöön. Yhteisten linjausten puute erityisesti tietoturvavaatimusten osalta on jo nyt muodostunut haasteeksi Valtorin tuotteistettujen palvelujen kehittämisessä ja levittämisessä virastoasiakkaiden käyttöön.

Tietoturvan vaatimukset ja todentamiseen liittyvät seikat on päivitettävä käsi kädessä tämän linjauksen kanssa, jotta vältytään turhalta keskustelulta siitä, miten ja millaisilla vaatimuksilla asianmukainen tietoturvallisuus voidaan hyväksyttäväksi todentaa. Vai onko tarkoitus, että yksittäisen organisaation tapauskohtainen riskiarviointi riittää? Hyväksyttävien vaatimusten asianmukaiselle toteutukselle ja todentamismenetelmille on oltava sellaisia, että ne huomioivat julkisella pilvipalvelumallilla toteutettavat ratkaisut ja niiden erityispiirteet, eivätkä vaadi todennusmenetelmiä, jotka pilvipalvelutoimittajan on mahdotonta hyväksyä jaettavassa kapasiteetissa toteutettavaksi (esimerkiksi verkkoliikenteen tutkiminen pilvi-infrastruktuurin sisällä, jossa voi liikkua tuhansien eri organisaatioiden dataa). Asianmukaisen tieturvallisuuden toteuttaminen pilvipalvelussa on myös kirjoitettava selväsanaisesti auki, jotta eri organisaatiot voivat

lähtökohtaisesti arvioida pilvipalvelun käyttöä ja turvallisuutta yhteismitallisesti. Liian yksityiskohtaisia teknisiä vaatimuksia kannattaa välttää, koska teknologiat päivittyvät nopeampaa tahtia, kuin ohjeita ennätetään päivittää. Siirtymävaiheen ajaksi (ennen kuin uudet tietoturvallisuusvaatimukset on saatu hyväksyttyä) on tähän linjaukseen syytä kirjoittaa ne periaatteet, joilla pilvipalveluita voidaan hyväksyttäväksi käyttää myös salassapidettävän STIV -aineiston tallentamiseen.

Taskinen Pirkko
Valtion tieto- ja viestintätekniikkakeskus Valtori - Valtion tieto- ja viestintätekniikkakeskus Valtori