Verohallinto

Lausunto

07.09.2018

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:

-

Pilvipalveluiden edut sekä toteutus- ja palvelumallit

Kommentit:

-

Pilviteknologian edut

Kommentit:

-

Palvelumallit

Kommentit:

-

Toteutusmallit

Kommentit:

-

Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Kommentit:

-

Tiedon käsittelyn vaatimukset

Kommentit:

Tietojen luokittelua koskevassa kappaleessa on ristiriita periaatteen 9 kanssa "Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa" - Tällaisen tiedon käsittelyyn käytettävän pilvipalvelun täytyy sijaita fyysisesti Suomen tai EU:n alueella ja sen täytyy olla Suomessa tai EU alueella sijaitsevan toimijan hallinnassa. Palvelun on täytettävä tiedon käsittelylle asetetut vaatimukset samalla tavalla kuin muiden toteutusmallien.

Kappaleessa, joka alkaa sanoilla "Kuten kaikissa palveluhankinnoissa ..." on aika lavea lause, joka vaatisi mielestämme tuekseen konkretiaa. Henkilötietojen suojan näkökulmasta tulee myös ottaa huomioon yleisen tietosuoja-asetuksen ((EU) 2016/679) 35 artiklan vaikutusten arviointi, jonka mukaisesti artiklassa tarkoitetuissa tilanteissa pitää arvioida käsittelyn riskit henkilötietojen suojalle. Lisäksi tulee arvioida tietojen käsittelyä kansallisen turvallisuuden näkökulmasta. Silloin, kun kansallinen tieto on Suomen lainsäädännön soveltamisalueen ulkopuolella on aina mahdollista että se joutuu sellaisen tahon haltuun joka voi käyttää tietoa Suomen vahingoksi jollain tavalla. Näin ollen tulee arvioida onko jotkut tiedot sellaisia, suojaustasosta riippumatta, että pitää käsitellä vain Suomessa.

Kappaleessa, joka alkaa sanoilla "Mikäli kyseessä on laaja-alainen, esimerkiksi koko julkiseen hallintoon ..." on esitetty haastava vaatimus, joka on monille organisaatioille mahdoton toteuttaa. Avoimeksi jää myös mitä tarkoitetaan asiakkaalla esim. laajaan viranomais- ja kansalaiskäyttöön tarkoitetuissa palveluissa? (esim. Vero, VTJ, Trafi, MML yms). Tässä tulee arvioida palvelun tuottamisen edellytykset suhteessa siihen tietoon jota asiakkaat käsittelevät. Lisäksi jatkuvuuden osalta tulee huomioida riskin kertautuminen käyttäjäorganisaatioiden määrällä.

Kohdassa esitetty luokittelu on myös seuraavilta osin vanhentunut jo nyt ja vaatisi tämän suosituksen päivitystä varsin pian

- ST IV tai ST IV Käyttö rajoitettu
- ST III tai ST III Luottamuksellinen
- ST II tai ST II Salainen

- ST I tai ST I Erittäin salainen

Palveluiden ohjaus

Kommentit:

-

Haasteet

Kommentit:

Kappaleessa on mainittu seuraavaa: " 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. "

Onko todella niin, että riski pienenee, jos palvelu sijaitsee EU/ETA-alueella tai sen ulkopuolella?

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:

Ko. linjauksessa käytetään termiä viranomainen täsmentämättä mitä sillä tarkoitetaan. Tässä yhteydessä olisi hyvä tarkentaa viranomaisen määritelmää esim. tarkoitetaanko laajaa viranomaiskäsitettä, joka on säädetty viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 4 §:ssä.

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:

Ko. linjauksessa samoin kuin linjauksessa 6 käytetään termiä viranomainen täsmentämättä mitä sillä tarkoitetaan. Tässä yhteydessä olisi hyvä tarkentaa viranomaisen määritelmää esim. tarkoitetaanko laajaa viranomaiskäsitettä, joka on säädetty viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 4 §:ssä.

Suosituksia toimenpiteiksi

Kommentit:

Linjauksissa tiedon sijainnista ja hallinnasta pitäisi mielestämme painottaa tiedon myös omistajuuden ja vastuun määrittämistä. Palvelusopimuksiin olisi syytä kirjata selkeästi vastuut esim.

- kuka vastaa tiedon oikeellisuudesta ja eheydestä
- kuka määrittää tiedon käsittelysäännöt
- kuka huolehtii tiedon elinkaaren hallinnasta, arkistoinnista ja hävittämisestä

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

-

Laakso Mikko
Verohallinto

Hämäläinen Tuula
Verohallinto