



Lausunto

04.09.2018

Asia: VM/276/00.01.00.01/2018

Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta

Yhteenveto

Kommentit yhteenvetoon:

Seuraavat kommentit linjauksiin:

2. Riippuen palveluntarjoajasta sopimukseen voi olla hankala vaikuttaa esim. Microsoft, Amazon, Google. Toki huomiota on kiinnitettävä jatkuvuuden turvaamiseen ja tiedon saatavuuteen. Hyvä peruslähtökohta sopimuksissa on EU:n mallilausekkeet, jotka muodostavat jo käytännössä yleisesti hyväksytyin markkinastandardin
4. Kohta on hyvä, mutta joustavuutta pitäisi jättää toimijalle itselleen.
5. Kerran vuodessa on liikaa. Parempi olisi, jos tarpeen mukaan arvioidaan EU:n tai kansallisten suositusten, oleellisten sopimusehtojen tai hankintayksiköiden tarpeiden muuttuessa.
6. Ei tulisi olla tässä ehdottomassa muodossa. Viranomaisen voisi korkeintaan ylläpitää suositusta. ICT-markkinan ja toimijoiden nopeasti muuttuvassa tilassa, miten varmistutaan, että viranomaistaho pystyy hyväksymään uudet toimijat riittävän nopeasti?

Taustaa linjauksille

Kommentit taustaan:

Pydetään tarkentamaan, mikä on linjauksen velvoittavuus.

Linjausten tavoitteet

Kommentit tavoitteisiin:

Tarkemmissa linjauksen tavoitteissa:

"Hallita palveluiden tuottamiseen liittyviä riskejä....." Kyseinen tavoite esitetään muutettavaksi esim muotoon: "tukea uusien teknologioiden turvallista käyttöönottoa." --> Myöhempi tavoite "Tukea pilvipalveluiden käyttöön liittyvää riskiarviointia" on hyvä ja kattaa riskit.

Pilvipalveluiden edut sekä toteutus- ja palvelumallit

Kommentit:

-

Pilviteknologian edut

Kommentit:

-

Palvelumallit

Kommentit:

-

Toteutusmallit

Kommentit:

-

Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Kommentit:

Kuvien 2 ja 3 osalta olisi tuotava esiin, että kuva on havainnollistava, ei koko totuus. Se, että palvelu on fyysisesti Suomessa, ei välttämättä pienennä palveluhyötyyn tai -takuuseen liittyviä riskejä. Sen arviointi on kompleksisempaa.

Tiedon käsittelyn vaatimukset

Kommentit:

Tietoturvan määritelmää voisi tarkentaa. Nyt määritelmän ensimmäinen lause "Tietoturva on yksi tietosuojaan toteuttamisen keino" voi aiheuttaa väärinymmärrystä ja voi johtaa käsitykseen, että tietoturva olisi ainoastaan tietosuojaan osa-alue. Yleisesti määritelmät tulisi pitää vakioituina siten, että ne ovat kaikissa vastaavissa dokumenteissa samanlaisia

Dokumentissa avataan melko pitkästi eri suojaustasoja ja mm turvallisuuluokamerkintöjä. Eivät ole tarpeen näin laajasti tässä dokumentissa, viittaus lainsäädäntöön riittää.

Suojaustasoja ja turvallisuusluokiteltavien tietojen osalta on määritelty, missä tieto voi niissä tapauksissa fyysisesti sijaita. Samanlaiset viittaukset myös henkilötietojen ja arkaluontoisten henkilötietojen osalta.

s. 9 ”Käsiteltäessä suojaustason III tai turvallisuusluokiteltavaa ST III Luottamuksellinen tai korkeampaa tietoa, tietoa saa käsitellä ainoastaan Suomessa ja omassa hallinnassa olevia palveluita hyödyntäen. Tästä on mahdollista poiketa, mikäli tälle löytyy selkeä peruste---”

virt.

s.17 ”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”

Suojaustasoa III koskevat periaatteet voisivat olla yhdessä kohtaa, tai eri kohdissa olevien mainintojen pitäisi olla yhdenmukaisemmat.

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 sopimukseen, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen

Kommentit:

Riippuen palveluntarjoajasta sopimukseen voi olla hankala vaikuttaa esim. Microsoft, Amazon, Google. Toki huomiota on kiinnitettävä jatkuvuuden turvaamiseen ja tiedon saatavuuteen. Hyvä peruslähtökohta sopimuksissa on EU:n mallilausekkeet, jotka muodostavat jo käytännössä yleisesti hyväksytyin markkinastandardin

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:

Toimijalle itselleen tulee jättää liikkumavaraa, eli ei nostaa pilvipalvelua muiden yläpuolelle. Lisäksi palveluhyöty ja -takuu pitäisi määritellä. Mitä nämä otsikot sisältävät ja onko niiden ulkopuolella kriteereitä joita normaalisti julkisessa hankinnassa otetaan huomioon tarjoajien vertailussa?

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

Kommentit:

Kerran vuodessa on liikaa. Parempi olisi, jos tarpeen mukaan arvioidaan EU:n tai kansallisten suositusten, oleellisten sopimusehtojen tai hankintayksiköiden tarpeiden muuttuessa.

6 Viranomaisen ylläpitää listaa hyväksytyistä palveluntarjoajista

Kommentit:

Ei tulisi olla tässä ehdottomassa muodossa. Viranomaisen voisi korkeintaan ylläpitää suositusta. ICT-markkinan ja toimijoiden nopeasti muuttuvassa tilassa, miten varmistetaan, että viranomaistaho pystyy hyväksymään uudet toimijat riittävän nopeasti?

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:

s. 17 ”Tällaisen tiedon käsittelyyn käytettävän pilvipalvelun täytyy sijaita fyysisesti Suomen tai EU:n alueella ja sen täytyy olla Suomessa tai EU alueella sijaitsevan toimijan hallinnassa.”

Vaikka palveluntuottajan palvelimet sijaitsisivat EU:ssa, palveluntuottaja saattaa kuitenkin käyttää erilaisia tiedon käsittelijöitä (esim. tekniseen tukeen), jotka eivät sijaitse EU:ssa. Miten näitä tilanteita tulkitaan? Tiedot saattavat näissä tilanteissa konkreettisesti siirtyä tai käsittelijällä on vain tekninen yhteys EU:ssa olevaan tietoon.

Suosituksia toimenpiteiksi

Kommentit:

-

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

-

Parviainen Matti
Espoon kaupunki