tulli.fi

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:

- Tulisiko linjausten ottaa kantaa myös (esim. ulkomaiseen) lainsäädäntöön, joka voi mahdollistaa tiedon käsittelyn ulkopuolisten tahojen toimesta? Tähän voi vaikuttaa esimerkiksi pilvipalvelun tarjoajan päätoimiston sijainti. Ts. pilvipalveluita arvioitaessa tulisi maantieteellisen sijainnin lisäksi arvioida myös toimittajaa velvoittava lainsäädäntö.

Linjausten tavoitteet

Kommentit tavoitteisiin:

- Linjausten tulisi perustua pilvipalvelujen käyttöön liittyvään yleiseen riskiarvioon

- Huomioitava , että Maakuntien ja kuntien osalta valmiudet tiedon suojaamiseen tai suojaamisperusteiden arvioimiseen eivät ole samalla tasolla valtionhallinnon toimijoilla. Kunnalliset toimijat eivät ole olleet esim. velvollisia noudattamaan tietoturva-asetusta.

- Pilvipalveluita ovat yleisimmin erilaiset SaaS-palvelut, jotka tarjoavat valmiin sovellustoiminnallisuuden jaetusta palvelusta.

- Mitä seuraava tavoite käytännössä tarkoittaa näiden linjausten puitteissa: "Mahdollistaa ICT-palveluiden kysynnän ja tarjonnan kohtaaminen parantamalla esimerkiksi saatavaa asiakashyötyä ja kustannustehokkuutta"?

Pilvipalveluiden edut sekä toteutus- ja palvelumallit

Kommentit:

- Maksimaalinen hyöty riippuu organisaation omista tarpeista. SaaS-malli paremminkin minimoi organisaation tarvitsemat omat ICT-resurssit (mikäli organisaation tarvitsema toiminnallisuus on saatavilla valmiina SaaS-palveluna).

Pilviteknologian edut

Kommentit:

- Eduissa voisi mahdollisesti olla mukana myös jatkuvuuden turvaaminen, pilvipalvelu ei ole välttämättä niin sidoksissa tiettyyn yhteen fyysiseen alustaan, jolloin esim. yhden konesalin tuhoutuminen ei estä koko palvelun käyttöä

- Palvelun käyttäjän osaamistarpeet riippuvat käytettävästä pilvipalvelumallista. Esimerkiksi IaaS-mallissa palvelun käyttäjällä on edelleen suuria vastuita sen tuottamisen ja ylläpitämisen osalta (mutta ei niinkään SaaS-mallissa).

- Esimerkiksi SaaS-mallilla tuotettu palvelu ei tyypillisesti ole erityisen joustava, sillä samaa vakioitua toiminnallisuutta tarjotaan kaikille käyttäjille.

Palvelumallit

Kommentit:

- Oma konesali tai isännöity konesali eivät oikeastaan liene pilvipalveluita (tai niiden toteutusmalleja)

- "Isännöidyn konesalin" sijasta terminä voisi käyttää "konesali- tai käyttöpalveluita".

- mainitaan että PaaS- ja SaaS-ratkaisuissa ”käyttäjäorganisaatiolta poistuu infrastruktuurin/palvelun tuottamiseen liittyvä osaamistarve”. -> käyttäjäorganisaatiossa vaaditaan aina IT-infran sekä palvelunhallinnan osaamista, koska muuten on mahdotonta ostaa näitä palveluita oikein palveluntarjoajilta.

- SaaS-mallissa tarvitaan kuitenkin tyypillisesti käyttäjien tunnistamiseen ja käyttövaltuushallintaan liittyvää osaamista (esimerkiksi identiteetin federointi)

Toteutusmallit

Kommentit:

- Oma konesali ei oikeastaan liene pilvipalvelun toteutusmalli

- Vaikka toteutusmallit kehittyvät koko ajan voisi kansallisen pilven ohella käsitellä ”EU-pilveä ja ”Globaalia pilveä”. Nämä pilvimuodot tulevat esille lainsäädännön kautta niiden tietoturvaan ja tietosuojaan tuomien vaatimusten/eroavuuksien vuoksi.

Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Kommentit:

- Maantieteellisen sijainnin muuttuessa riskit tai riskienhallinnan merkitys eivät välttämättä kasva vaan uhat vain muuttuvat (esimerkiksi oman konesalin jatkuvuusriski ja tietomurron riski voivat olla korkeampia kuin julkisen pilven mutta julkisessa pilvessä riski tietojen joutumiselle vieraan lainsäädännön piiriin on suurempi)

- Henkilötietojen suhteen huomioitavaa on myös se, että tiedot tulee siirtää ETA-alueen ulkopuolelle lainmukaista siirtomekanismia käyttäen (tämä on käyttäjäorganisaation vastuulla).

Tiedon käsittelyn vaatimukset

Kommentit:

- ST-IV turvallisuusluokiteltuja tietoja ei ole käsitelty/huomioitu tarkemmin asiakirjassa, eli ei siis eroa onko luokiteltu vai turvallisuusluokiteltu? Tämä on nyt tuotu esille vain haasteena luvussa 5.3.

- KV-turvaluokiteltujen tietojen käsittelystä voisi myös todeta linjauksia

- Estävätkö linjaukset siis STIV-tason tietojen käsittelyn ETA-alueen ulkopuolisissa maissa (esim. Komission turvalliseksi katsomissa maissa tai Privacy Shieldin piirissä olevissa yrityksissä ulkopuolisissa maissa)?

- Mitä käytännössä tarkoittaa "..omassa hallinnassa olevia palveluita hyödyntäen"? Harva viranomainen/virasto tuottaa enää itsenäisesti omia palveluitaan.

- Tietosuoja-kappale on hyvin kevyt eikä pääosin sisällä suoraan tietosuojaan liittyviä asioita (enemmän tietoturvaa).

Palveluiden ohjaus

Kommentit:

- Kuvan 3. merkitys jää tähän liittyvien käsitteiden suhteet jäävät hieman epäselviksi

- Neuvotteluasemaan liittyvät riskit jäävät epäselviksi. Hyvä neuvotteluasema ei väistämättä takaa hyvää palveluun liittyvien riskien hallintaa tai toisin päin.

Haasteet

Kommentit:

-

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

Kommentit:

- Varsinkin nyt jos ohjeistusta ollaan muuttamassa, pilvipalveluja ja niiden hankintaa tulee käsitellä erityisen huolellisesti.

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:

- Pilvipalvelun tulee täyttää aina asetetut turvallisuus/jatkuvuus ja varautumisvaatimukset. Palveluhyöty ja – takuuvaatimukset eivät täyty ilman turvallisuusvaatimuksia.

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

Kommentit:

- Tulisiko olla muodossa: ”eikä muita palvelun vaatimuksiin liittyvä esteitä ole”…

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

Kommentit:

-

6 Viranomainen ylläpitää listaa hyväksytyistä palveluntarjoajista

Kommentit:

- Tällaisen kattavan listan ylläpitäminen lienee mahdotonta kun scopessa myös erilaiset SaaS-palvelut, mutta tuossa oli mainittukin ettei listalle kuuluminen ole sinänsä välttämätöntä palvelun hankinnalle. Tässä kiinnostaisi kuka viranomainen listaa ylläpitää, vai jokainen viranomainen omaansa?

7. Julkisen tiedon käsittelyä ei rajoiteta

Kommentit:

- Tiedon luokittelu ei kuitenkaan saa rajoittaa tarvetta suojata myös julkista tietoa korkeammin vaatimuksin jos siihen on tarvetta. Tiedon luottamuksellisuus ja eheys eivät saa vaarantua vaikka kyseessä olisi ns. julkinen tieto.

- Julkisen tiedon osalta tiedon saatavuus tulee usein varmistaa (jos on kriittinen tieto) - on siis tarve ehkäpä rajoittaa myös tämän käsittelyä

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

Kommentit:

- Todentaminen voi olla pilvipalvelujen osalta haasteellista. Jos viranomaisten kansallisesti tuotettujen ST- IV palvelujen tulee täyttää tietoturva-asetuksen minimitaso niin kuinka tämä taso todennetaan tasapuolisesti pilvipalvelujen osalta? Tulisi ainakin selkeästi kirjata vain EU-pilven käyttöä koskevaksi.

9. Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa

Kommentit:

-

Suosituksia toimenpiteiksi

Kommentit:

-

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

-

Heikkinen Pyry
tulli.fi