Sara Saari

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:

-

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:

-

Suosituksia toimenpiteiksi

Kommentit:

-

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

On todella arvokasta ja tärkeää, että VM on laatimassa linjausta julkisen hallinnon tiedon sijainnista ja hallinnasta.

Linjauksessa on käsitelty aihetta monipuolisesti. Keskeiset käsitteet on kuvailtu hyvin.

Muutamissa kohdin teksti on ylimalkaista.

Mitä ovat tarvittavat sopimukset rekisterinpitäjän ja henkilötietojen käsittelijän välillä (sivu 9/19)?

Mitkä ovat toimenpiteet, joilla käyttäjä- ja pääsynhallintaan kiinnitetään erityistä huomiota (sivu 10/19)?

Mikä on riittävä tietosuojan taso (sivu 14/19)?

Koska linjaus on vielä luonnos, teksti ei ole kielenhuollon näkökulmasta viimeisteltyä. Tämä korjautunee myöhemmässä versiossa.

Lopussa olevat suositukset toimenpiteiksi ovat tarpeellisia, koska useissa kohdin linjausta on tarve tarkempaan ohjeistukseen. Toimenpidesuosituksissa tarve tarkempaan ohjeistukseen todetaan, ja ohjeistus toivottavasti tullaan toteuttamaan joko VAHTI-ohjeistuksena tai muulla tavoin.

Kommentoin linjausta ainoastaan henkilötietojen tietosuojan näkökulmasta.

Yhden tulkinnan mukaan tietosuoja ja tietoturva ovat kaksi eri ympyrää, jotka leikkaavat toisensa osittain. Toisen tulkinnan mukaan tietoturva on iso ympyrä, jonka sisällä on pienempi tietosuojaympyrä kokonaisuudessaan.

Tulkitsen tietosuojan ja tietoturvan ensimmäisen tulkinnan mukaan toisensa leikkaaviksi ympyröiksi. Tulkintani mukaan tietosuoja ja tietoturva ovat toisiinsa linkittyneitä, mutta ne eivät ole toistensa synonyymejä. Niillä on yhteisen alueen lisäksi myös toisesta riippumaton itsenäinen alueensa. Sen vuoksi näkisin tarpeellisena eritellä kautta koko linjauksen huolella sen, milloin linjaus kohdistuu tietoturvaan, milloin tietosuojaan ja milloin näiden yhteiseen leikkauspintaan.

Esimerkiksi sivulla 13 (Palveluiden ohjaus) palvelutakuuseen liittyvinä riskeinä luetellaan kapasiteetti, saatavuus, jatkuvuus ja tietoturva. Katsotaanko tietoturvan sisältävän tietosuojan?

Koska henkilötiedot ovat pilvipalveluissa aivan toisenlaisessa ympäristössä kuin käyttäjäorganisaation hallinnoimassa omassa konesalissa, ehdotan, että henkilötietojen tietosuojan huomioimiselle pilvipalveluissa laaditaan ohje, esimerkiksi VAHTI-ohje.

Pilvipalveluissa olevilla henkilötiedoilla tarkoitan tässä julkisen hallinnon pilvipalveluun tallentamia henkilörekistereitä ja muita kuin rekisterimuodossa olevia henkilötietoja sisältäviä tiedostoja.

Ohjeessa tulisi käsitellä muun muassa seuraavat henkilötietojen tietosuojaan vaikuttavat seikat:

Pilvipalveluiden työntekijöiden pääsy katselemaan henkilötietoja: tuleeko pilvipalveluiden työntekijät tunnistaa yksilöllisesti ja tuleeko heidän käyttäjätietojaan (loki) seurata käyttäjäorganisaation toimesta?

Tuleeko pilvipalveluiden työntekijöiden vaihtuessa uusien työntekijöiden hyväksymisestä sopia palvelun tarjoajan kanssa tehdyssä sopimuksessa?

Tuleeko pilvipalveluiden työntekijöistä tehdä turvallisuusselvitys?

Ohjeessa tulisi pyrkiä vähintään samaan ja mieluiten vielä tarkempaan yksityiskohtaisuuteen kuin valtionhallinnon tietoturvallisuuden johtoryhmän laatimassa lokiohjeessa (VAHTI 3/2009).

Sara Saari