Rahoitusvakausvirasto

Lausunto

10.03.2023 RVV 57/07.00.00/2023-2

Asia: VN/3115/2023

Valtionhallinnon pilvipalvelulinjauksien päivittäminen

Valtionhallinnon pilvilinjaukset

1. Ensisijaisesti pilveen (Cloud 1st) strategia: Pilvipalvelu tai pilvipalveluteknologia tulee olla ensisijainen valinta, mikäli estäviä perusteita valintaan ei ole

-

2. Pilvi- ja ekosysteemiratkaisut tulee tuottaa lähtökohtaisesti EU/ETA –alueelta

-

3. Valtion yhteisten pilvi- ja ekosysteemiratkaisujen tulee olla ensisijainen valinta, mikäli estäviä perusteita valinnalle ei ole

-

4. Pilvialustapalveluihin liittyvät kilpailutukset ja hankinnat tulee tehdä ensisijaisesti valtionhallinnon yleisillä hankintasopimuksilla

-

5. Pilvipalveluiden hankintaa, käyttöönottoa ja hyödyntämistä tulee käsitellä kuin mitä tahansa muutakin palvelun hankintaa tai muutosta

-

6. Julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä

-

7. Salassa pidettävää turvallisuusluokittelematonta tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä

-

8. Henkilötietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä.

-

9. Turvallisuusluokan IV tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä

-

Pilvilinjauksien jatkovalmistelua tukevat kysymykset

1. Ovatko ehdotetut linjaukset rajoittavia? Ovatko ehdotut linjaukset mahdollistavia?

Rahoitusvakausviraston näkökulmasta selkeä linjaus siitä, että salassa pidettävän (linjaus 7.) ja erityisesti turvallisuusluokan IV (linjaus 9.) tiedon käsittely on tietyin ehdoin mahdollista julkisessa pilvipalvelussa, saattaisi mahdollistaa pilvipalveluiden nykyistä selkeästi laajemman käytön. Lisäksi tällainen linjaus saattaisi mahdollistaa merkittävät kustannussäästöt tulevaisuudessa, mikäli yhä suurempi osa viraston toimintaa tukevista yhteisistä IT-palveluista (esim. videoneuvottelupalvelut) siirtyy puhtaasti pilvipalveluiksi, koska tällöin viraston ei todennäköisesti tarvitsisi etsiä käyttöönsä korvaavia ratkaisuja.

Linjauksen 2 mukaan pilvi- ja ekosysteemiratkaisut tulee tuottaa lähtökohtaisesti EU/ETA –alueelta. Rahoitusvakausviraston näkökulmasta linjauksen rinnalla olisi kuitenkin keskeistä ottaa kantaa myös siihen, missä määrin linjauksesta poikkeamiseen liittyvä riskejä tulisi voida arvioida ja hallita keskitetysti yhteisissä palveluissa ja hankinnoissa (linjaukset 3. ja 4.). Ilman keskitettyjä riskienhallintakeinoja linjaus voi mahdollisesti rajoittaa nykyisten suurten, julkisten pilvipalvelutarjoajien palveluiden käyttöä merkittävästi ja nostaa käytettävissä olevien palveluiden hintaa erityisesti pienille virastoille, koska monien tällä hetkellä tarjolla olevien julkisten pilvipalveluiden osalta juuri EU/ETA-alueen ulkopuolelle tapahtuvat tiedonsiirrot aiheuttavat palveluiden käytön keskeisimmät riskit, ja erityisesti pienten virastojen mahdollisuudet tehdä kattavasti linjauksessa mainittu riskiarvio, ovat erittäin rajalliset. Resurssien käytön kannalta ei myöskään ole järkevää, että kukin viraston tekee arvionsa täysin itsenäisesti. Yhteisten palveluiden ja hankintojen osalta yksittäisten virastojen kyky määrittää hallintakeinoja on myös usein rajallinen.

Linjauksesta 9. jää epäselväksi, mitä seuraavalla tarkoitetaan: ”vain sellaista turvallisuusluokan IV tietoa, joka on luovutettavissa maihin, joilla on lainsäädännöllisiä vaikutusmahdollisuuksia kyseiseen pilvipalveluun”. Tätä olisi hyvä selventää.

2. Miten ehdotetut linjaukset vaikuttavat edelläkävijävirastojen pilvipalvelujen hyödyntämiseen? Miten ehdotetut linjaukset vaikuttavat pilvipalvelujen käytön hyödyntämistä suunnitteleville virastoille?

-

3. Miten tiedon ulkomaille sijoittamiseen liittyviä riskejä voidaan vähentää ja miten riskien vähentäminen voitaisiin ottaa huomioon linjauksissa?

RVV:n näkökulmasta kriittisen tiedon saatavuuteen vakavissa häiriötilanteissa ja poikkeusoloissa liittyviä riskejä voitaisiin vähentää esimerkiksi yhteisellä turvasatamapalvelulla. Tärkeintä tällaisten riskien vähentämisen kannalta olisikin erityisesti linjauksiin 3. (Valtion yhteisten pilvi- ja ekosysteemiratkaisujen tulee olla ensisijainen valinta, mikäli estäviä perusteita valinnalle ei ole) ja 4. (Pilvialustapalveluihin liittyvät kilpailutukset ja hankinnat tulee tehdä ensisijaisesti valtionhallinnon yleisillä hankintasopimuksilla) liittyvä ohjaus. Hankintasopimusten ja niiden myötä yhteisten palveluiden tulisi olla sellaisia, että niissä on otettu jo valmiiksi huomioon ulkomaille sijoittamiseen liittyvät riskit ja niiden hallintakeinot. Tällöin kunkin viraston ei tarvitse lähteä ratkomaan samoja ongelmia erikseen.

4. Mitä esteitä pilvipalvelujen hyödyntämisessä on tietosuojan ja henkilötiedonkäsittelyn osalta? Ja miten näitä esteitä voitaisiin käytännössä poistaa?

Tietosuojan näkökulmasta linjauksen 2 yhteydessä tulisi mainita myös maat, joiden osalta Euroopan komissio on katsonut, että henkilötietojen suojan taso on vastaava kuin yleisen tietosuoja-asetuksen tarjoama suoja. Maantieteellisen rajauksen lisäksi tietosuojan varmistamiseksi voitaisiin käyttää muun muassa sopimuslausekkeita, käytännesääntöjä ja toimivaltaisen tietosuojaviranomaisen vahvistamia kyseistä pilvipalveluiden tarjoajaa koskevia sitovia sääntöjä (BCR, Binding Corporate Rules) keinoina hallita tilanteita, joissa henkilötietoja siirretään Euroopan talousalueen ulkopuolelle. Esimerkki tällaisista keinoista on Belgian tietosuojaviranomaisen aloitteesta lähtenyt EU Cloud Code of Conduct, jonka nojalla (määräajaksi) hyväksytyt organisaatiot takaavat muun ohella, että niillä on asianmukaiset prosessit yleisen tietosuoja-asetuksen mukaisten velvoitteiden täyttämiseksi. Tällaisten käytännesääntöjen on tarkoitus helpottaa pilvipalvelutarjoajan valintaa, myös silloin, kun asiakkaana on viranomainen.

5. Mitkä ovat muut merkittävimmät esteet pilvipalvelujen laajemmalle hyödyntämiselle? Ja miten esteitä voitaisiin poistaa?

-

6. Mitä muita toimenpiteitä, ehdotettujen linjauksien lisäksi, voitaisiin käynnistää pilvipalvelujen hyödyntämisen edistämiseksi?

-

Rahoitusvakausvirasto - Kari Hietaniemi, tietohallinto- ja huoltovarmuusasiantuntija