



Valtiovarainministeriö

Viite:

Valtiovarainministeriön lausuntopyyntö 13.2.2023, VN/3115/2023

Asia:

Valtionhallinnon pilvipalvelulinjauksien päivittäminen

Lausunto laadittu lausuntopalvelu.fi –palvelun kysymysten mukaisesti

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

Ei lausuttavaa.

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

Linjaus on tärkeä, erityisesti kun palvelussa on tarkoitus käsitellä henkilötietoja sisältävää viranomaisen aineistoa. Olennaisen tärkeää on, että valtionhallinnon viranomaiset eivät joudu ilman valtionhallinnon yhteisiä ratkaisuja ja niitä edeltänyttä riittävän perusteellista oikeudellista arviointia tilanteisiin, joissa ne joutuisivat pilvi- ja ekosysteemiratkaisun johdosta asiallisesti luovuttamaan henkilötietoja EU/ETA-alueen ulkopuolelle ja siten soveltamaan sitä koskevia Euroopan unionin yleisen tietosuoja-asetuksen (EU) 2016/679 säännöksiä asetuksen 44 – 46 artikloissa. On huomattava, että rekisterinpitäjällä on lakisääteinen velvollisuus noudattaa näitä ja Suomessa virastojen ja laitosten johdolla ja henkilöstöllä on laajasti virkavastuu myös kyseisten säännösten noudattamisesta. Euroopan tietosuojaneuvoston suositusten ja ohjeiden huomioon ottaminen asian jatkovalmistelussa on erittäin tärkeää.

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

Valtion yhteisten ratkaisujen käyttö on kannatettavaa. Tämä kuitenkin edellyttää, että yhteisten ratkaisujen hankinnassa ja kehityksessä ei ole tehty sellaisia ratkaisuja jotka pakottavat viranomaisia hyväksymään laajoja poikkeamia tiedon säilymisestä EU/ETA-alueella tai hyväksymään muuten tiedonkäsittelyn tietoturvaa ja tietosuojaa koskevia poikkeamia.

Olen laillisuusvalvonnassani käsitellyt tilannetta, jossa viranomaisen valitsema alustapohjainen viestintäratkaisu johtaa henkilötietojen siirtämiseen unionin ulkopuolelle sekä asiallisesti saattaa rajoittaa myös kansalaisen tiedollista itsemääräämisoikeutta (ks. [valtioneuvoston oikeuskanslerin päätös OKV/949/10/2021, 7.2.2023, YouTube –palvelun käyttäminen viranomaisviestinnässä](#)). Päätöksessäni korostin, että suunnitellessaan viestintää ja toteuttaessaan sitä, viranomaisen on otettava huomioon tiedon saatavuus ja saavutettavuus, hallintolain (434/2003) sisältämä palveluperiaate, tiedollinen itsemääräämisoikeus sekä lain julkisen hallinnon tiedonhallinnasta (906/2019) eli tiedonhallintalaista ja EU:n yleisestä tietosuojasetuksesta johtuvat velvoitteet. Totesin, että näiden vaatimusten huomioimista voisi edesauttaa se, että viranomaisilla olisi käytettävissään keskitetty videoportaali tai muu vastaava yhteinen ratkaisu tiedon jakeluun. Päätöksessäni todettu valtionhallinnon yhteisen ratkaisun selvittämisen oikeudellinen perusteltavuus on laajennettavissa yleisesti koskemaan pilvipalveluita edellyttäen kuitenkin, että ne on asianmukaisesti hankittu ja täyttävät tietosuojasta, julkisuudesta, tiedonhallinnasta, hyvästä hallinnosta sekä tiedollisesta itsemääräämisoikeudesta johtuvat vaatimukset.

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

Ei lausuttavaa.

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

Ei lausuttavaa.

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

Ei lausuttavaa itse periaatteesta. Aito toteuttaminen kuitenkin edellyttää, kohtien 2., 3. ja 4. periaatteet huomioon ottaen, että yhteiset ratkaisut ja yleiset hankintasopimukset on toteutettu niin, että tiedonhallintayksiköjä ja virastoja ei pakoteta hyväksymään yhteistä ratkaisua tai yleistä hankintasopimusta tehdessä jo tehtyjä poikkeamia tietosuoja- ja tietoturva-vaatimuksiin. Totean lisäksi, että pilvipalveluiden hankintaa ja käyttöönottoa tulee edeltää riittävän laaja-alainen ja huolellinen oikeudellinen arviointi ja riskiarviointi. Kaikkiin teknologisiin ratkaisuihin ja vaihtoehtoihin liittyy eritasoisia tietojärjestelmäriskejä. Tiedonhallintalain 13 §:n 1 momentin perusteella viranomaisten tiedonhallintayksiköiden olisi arvioitava tietoaineistoihin ja tietojärjestelmiin liittyviä riskejä säännöllisesti niiden koko elinkaaren ajan. Riskiarvioinnissa olisi tunnistettava olennaiset riskit, jotka voisivat vaikuttaa tietoaineistojen luottamuksellisuuden, eheyden ja saatavuuden vaarantumiseen taikka tietojärjestelmien käyttöön ja vikasietoisuuteen. Säännös muodostaa sen esitöiden mukaan kokonaisuuden, johon kuuluu riskien arviointi, tietoturvaluustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvaluustoimenpiteiden toteuttaminen (HE 284/2018 vp, s. 92). Korostan, että riskien arvioinnin tulee tiedonhallintalain perusteella olla jatkuvaa toimintaa. Totean lisäksi, että viranomaisviestinnän suunnittelussa ja toteutuksessa tulee ottaa huomioon EU:n yleisen tietosuoja-asetuksen 25, 32 ja 35 artiklasta johtuvat velvoitteet.

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

Ei lausuttavaa itse periaatteesta, sama lisäys kuin kohdan 6. vastauksessa.

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

Ei lausuttavaa itse periaatteesta, sama lisäys kuin kohdan 6. vastauksessa.

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

Ei lausuttavaa itse periaatteesta, sama lisäys kuin kohdan 6. vastauksessa.

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

Ei lausuttavaa.

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

Ei lausuttavaa.

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

Parhaiten esimerkiksi tietosuojavaatimuksia vastaava tapa vähentää riskejä on huolehtia siitä, että tietoa ei sijoiteta EU/ETA –alueen ulkopuolelle.

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

Tietosuoja ja henkilötietojen käsittely ei itsessään aseta esteitä pilvipalvelujen hyödyntämiselle. Esteitä syntyy, jos pilvipalvelu on toteutettu tavalla joka ei täytä henkilötiedon käsittelylle asetettuja vaatimuksia.

Pilvipalvelujen hankinnassa ja kehittämisessä on syytä tarkoin seurata esimerkiksi Euroopan tietosuojaneuvoston suosituksia ja mahdollisia Tietosuojavaltuutetun ohjeita ja suosituksia. Pilvipalvelujen esteet voi poistaa toteuttamalla pilvipalvelut tavalla joka täyttää tiedonkäsittelylle säädetyt vaatimukset.

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

Ei lausuttavaa.

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

Ei lausuttavaa.

Tämä asiakirja on allekirjoitettu sähköisesti.

Oikeuskansleri

Tuomas Pöysti

Vanhempi oikeuskanslerinsihteeri

Pekka Liesivuori