[Valtiovarainministeriö]
[Tommi Kangasaho]

Lausunto on valmisteltu lausuntopalvelu.fi:ssä

Viite: Lausuntopyyntönne [10.3.2023 VN/3115/2023]

Valtionhallinnon pilvipalvelulinjauksien päivittäminen

Ehdotukset valtion pilvipalvelulinjauksiksi

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

Tavoitteet: Uudet tuotteistetut tietoturvallisemmat palvelut ja kyvykkyydet helposti saatavilla sekä käyttöönotettavissa. Palvelut mahdollistavat joustavan käytön ja kapasiteetin hankinnan.

- On-Premise-palveluille on edelleen tarvetta mm. sensitiivisen aineiston käsittelyyn ja tallennukseen. Pilvipalveluihin liittyy myös haasteellisia tietosuojan vaatimuksia erityisesti kv. tiedonsiirtojen osalta. Lähtökohtaisesti pilvipalveluilla saadaan aikaan skaalautuvuutta ja kustannushyötyä niissä tapauksissa, joissa aineisto ei ole salassa pidettävää ja tietosuojahaasteet saadaan ratkaistua.

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

Tavoitteet: Varmistetaan palveluiden toteutus, hallinnointi/hallinta ja tiedonkäsittely on aina, mikäli mahdollista, EU/ETA –alueen lainsäädännön piirissä ja poikkeamat hyväksytään tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä.

- Erityisesti tärkeä huomioida henkilötietojen osalta, että palvelua tuotetaan EU/ETA-alueelta.

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

Tavoitteet: Valtion yhteisten ratkaisujen laajempi hyödyntäminen ja yhteentoimivuuden varmistaminen.

- Strateginen päätös kunhan huomioidaan kohta 1.

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

Tavoitteet: Valtori ja Hansel tarjoavat pilvialustapalveluiden ajan tasalla olevat hankintasopimukset sekä siihen liittyvät tukipalvelut virastoille. Virasto vastaa palveluiden valinnasta oman strategiansa ja tavoitteidensa mukaisesti.

- Tavoite on kannatettava.
- Valtorin ja Hanselin asiakkaiden tulisi voida luottaa siihen, että hankittavat palvelut ovat jatkossakin lainmukaisia (esim. kv-tiedonsiirrot ovat tällä hetkellä asiakkaan omalla vastuulla).

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

   Tavoitteet: Varmistetaan asianmukainen ja huolellinen hankinta sekä muutoshallinta valtion sekä virastojen prosessien mukaisesti.
   - Pilvipalveluiden hankintaan liittyy paljon erilaisia, kansainvälisiä sopimusehtoja, joiden kanssa tulee olla erityisen huolellinen kilpailutuksia ja hankintoja tehdessä. Hankintaosaamiseen tulee kiinnittää huomiota myös jatkossa.

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

   Tavoitteet: Mahdollistaa julkisen tiedon käyttö ja hyödyntäminen pilvipalveluissa. Tiedon luokittelun kautta on varmistettu, että toteutettava palvelu sisältää vain julkista tietoa.
   - Tulisi olla selkeät kriteerit, jotka palvelun tulee täyttää riittävällä selkeydellä, jotta tiedonhallintayksikkö tai virasto voi tehdä riskiperusteisen päätöksen.

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**

   Tavoitteet: Mahdollistaa salassa pidettävän ei luokitellun tiedon käyttö ja hyödyntäminen pilvipalveluissa. Tiedon luokittelun kautta on varmistettu, että toteutettava palvelu sisältää vain turvallisuusluokittelematonta salassa pidettävää tietoa.
   - Tulisi olla selkeät kriteerit, jotka palvelun tulee täyttää riittävällä selkeydellä, jotta tiedonhallintayksikkö tai virasto voi tehdä riskiperusteisen päätöksen.
   - Yhteiset linjaukset esimerkiksi siitä, mitä tietoja voidaan esim. kansalaisten henkilötiedoista käsitellä pilvipalveluissa.
   - Riskiperusteiseen päätökseen olisi hyvä saada käytännön ohjeistus ja kriteerit.

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

   Tavoitteet: Mahdollistaa henkilötiedon käyttö ja hyödyntäminen pilvipalveluissa. Tietoluokittelun kautta on varmistettu, että kun toteutettava palvelu sisältää henkilötietoa on sen vaatimat toimenpiteet tehty siirrettäessä henkilötietoa ETA-alueen ulkopuolelle ja tiedonsiirtoa koskevat erityiset tietosuojavaatimukset täyttyvät.
   - Lähtökohtaisesti kyseinen palveluntuottaja tulisi olla EU/ETA-alueen toimija ja kolmannen osapuolen auditoima. Palveluntarjoajalla olisi oltava esittää sertifikaatti tai auditointiraportti (esim. PiTukRi) ja toimijat tulisi olla ns. hyväksyttyjä toimijoita (esim. kuten Traficom pitää listaa salaustuotteista, jotka on arvioitu tietylle turvatasolle).
   - Tulisi olla selkeät kriteerit, jotka palvelun tulee täyttää riittävällä selkeydellä, jotta tiedonhallintayksikkö tai virasto voi tehdä riskiperusteisen päätöksen.

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**

   Tavoitteet: Mahdollistaa tietoturvaturvallisuusluokitellun tiedon käyttö sekä hyödyntäminen pilvipalveluissa. Riskien arvioinnissa on otettu huomioon koko palvelun tuottamisessa käytetty toimitusketju. Tiedon luokittelun kautta on varmistettu, että tuotettava palvelu sisältää vain sellaista turvallisuusluokan IV tietoa, joka on luovutettavissa maihin, joilla on lainsäädännöllisiä vaikutusmahdollisuuksia kyseiseen pilvipalveluun. Mikäli tiedot eivät ole luovutettavissa palveluun määräysvallassa oleviin muihin valtioihin, on se toteutettava kansallisiin pilvipalveluihin edellyttäen, että ne on vaatimustenmukaisesti toteutettu.
   - Lähtökohtaisesti kyseinen palveluntuottaja tulisi olla EU/ETA-alueen toimija ja kolmannen osapuolen auditoima. Palveluntarjoajalla olisi oltava esittää sertifikaatti tai auditointiraportti (esim. PiTukRi) ja toimijat tulisi olla ns. hyväksyttyjä toimijoita (esim. kuten Traficom pitää listaa salaustuotteista, jotka on arvioitu tietylle turvatasolle).
   - Tulisi olla selkeät kriteerit, jotka palvelun tulee täyttää riittävällä selkeydellä, jotta tiedonhallintayksikkö tai virasto voi tehdä riskiperusteisen päätöksen.

Pilvilinjausten jatkovalmistelua tukevat kysymykset

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

   - Linjaukset ovat mahdollistavia.

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

   - Mahdollistaa laajemman käytön, mikäli kriteerit palvelun valinnalle on selkeät.
   - Linjaukset jättävät paljon vastuuta ja työtä virastoille erityisesti tietosuojalainsäädännön vaatimusten osalta.

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

   - Lait ja asetukset tulisi ohjata toimintaa ja tukea päätöksenteossa. EU-tasoinen hyväksyntä tietyille palveluille.

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

   - EU-tasoinen ja riippumaton hyväksyntä palveluille.

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

- Ilman selkeitä kriteereitä tai auditoituja palveluita luottamus palveluntuottajaan on aina suurin kysymys. Lähtökohtaisesti tunnustetaan pilvipalveluita tuottavien toimijoiden tietoturvallisuus, mutta edelleen salassa pidettävän tiedon siirtäminen pois omasta kontrollista (ts. pilveen) on iso periaatteellinen ja luottamukseen perustuva kysymys.
- Eurooppalaisten pilvipalveluiden tarjoajien puute markkinoilla on ehkä suurin este.
- Schrems II -ratkaisun mukaisesti ratkaisematon haaste on edelleen erityisesti julkisiin pilvipalveluihin liittyvät henkilötietojen tiedonsiirrot EU/ETA-alueen ulkopuolelle. EU:n ja Yhdysvaltojen välinen tekeillä oleva uusi tiedonsiirtojärjestely on oikeusvarmuudeltaan heikko, siihen liittyy uusi vuosia kestävä oikeusprosessi sekä riskejä, joita tarkoin lakia noudattavan viranomaisen voi olla mahdotonta hyväksyä toiminnassaan. Sen sijaan kestävä ratkaisu olisi siirtyminen aidosti EU/ETA-alueella toimiviin pilvipalveluihin, kunnes EU-kansalaiset saavat yhtäläiset tietosuojaoikeudet Yhdysvaltojen kansalaisten kanssa. Joka tapauksessa olisi toivottavaa, että Valtionhallinto antaisi selkeät linjaukset, kuinka viranomaiset voivat käyttää pilvipalveluita ilman tiedonsiirtoihin liittyviä laillisuushuolia. Riskinottoa tämän suhteen ei tulisi säilyttää yksittäisten virastojen vastuulle.

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

- Tuotteistetut ja auditoidut pilviratkaisut, joita voisi ostaa kuin hyllytavaraa

Pääjohtaja Markku Tervahauta

Osastonjohtaja Mia Nykopp

SIGNATURES **ALLEKIRJOITUKSET** **UNDERSKRIFTER** **SIGNATURER** **UNDERSKRIFTER**

This documents contains 4 pages before this page
Tämä asiakirja sisältää 4 sivua ennen tätä sivua
Detta dokument innehåller 4 sidor före denna sida
Dokumentet inneholder 4 sider før denne siden
Dette dokument indeholder 4 sider før denne side

Mia Johanna Nykopp
1477f1b0-35ba-441e-b833-2e01547f93a6 - 2023-03-10 16:52:33 UTC +02:00
BankID / MobileID - e4fb413a-bb1f-4d1a-bbaf-32422954ed3c - FI

Markku Petteri Tervahauta
968a1265-b9ce-4d22-9a68-fa4c51d1b2ba - 2023-03-21 13:05:55 UTC +02:00
BankID / MobileID - fc666600-f380-4b47-93b3-a294f1863228 - FI

authority to sign	asemavaltuutus	ställningsfullmakt	autoritet til å signere	myndighed til at underskrive
representative	nimenkirjoitusoikeus	firmateckningsrätt	representant	repræsentant
custodial	huoltaja/edunvalvoja	förvaltare	foresatte/verge	frihedsberøvende