Vihreä kasvu
Leena Nyman

6.3.2023

Valtionhallinnon pilvipalvelulinjauksien päivittäminen
Kirjoita tähän

Elinkeinoelämän keskusliitto EK kiittää mahdollisuudesta lausua koskien lausuntoa "Valtionhallinnon pilvipalvelulinjauksien päivittäminen" (VN/3115/2023).

EK kannattaa pääosin valtionhallinnon esittämiä pilvilinjauksia. Alla kuitenkin muutama huomiomme koskien pilvipalvelulinjausten päivittämistä.

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

   Kannatettava esitys.

   Kysymys on eritoten kustannustehokkaasta julkisten palveluiden järjestämisestä. Joustavan käytön ja kapasiteetin hankinnan lisäksi ratkaisua perustelee pilvipalveluissa laajasti saatavilla olevat yleiset käyttöympäristöpalvelut sekä laajasti tietotekniikka-alan palveluntarjoajien kehitysympäristöt.

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

   EU/ETA alueen pilvi- ja ekosysteemiratkaisut ovat kannatettavia.

   Perusratkaisulla kyetään hallitsemaan laajasti ns. lainsäädönriskeihin laskettavia uhkavektoreita aina datan sijaintipaikan oikeudenkäyttöpiiriin kuuluvista viranomaisten tietojen luottamuksellisuutta vaarantavista toimivaltuuksista henkilötietojen siirtoihin ja prosessointiin liittyviin haasteisiin.

   Valtionvarainministeriön tulisi kiinnittää erityistä huomiota linjauksen ohjeisiin koskien poikkeamien hyväksymistä. On tunnettua, että tiedonhallintayksiköt, tarkemmin sanottuna vastuuvirkamiehet ovat

välttäneet kaikenlaisia poikkeamien hyväksymisiä perustuen jokseenkin määrittymättömään epävarmuuteen virkavastuun rajoista ja poikkeamien muodostamista jäännösriskeistä.

Lisäksi linjauksessa tulisi huomioida tarkasti yleisen tietosuoja-asetukseen (GDPR) liittyvän Euroopan tietosuojaneuvoston linjaukset julkishallinnon pilvipalveluiden käytöstä (2022 Coordinated Enforcement Action, Use of cloud-based services by the public sector Adopted on 17 January 2023). Asian suhteen on syytä korostaa, että ko. asiakirjan tarkoitus on edistää pilvipalvelujen hyödyntämistä jäsenvaltioiden julkishallinnossa.

Tähän liittyen Valtiovarainministeriön tulisi varmistua, että Suomella on kaikkien viranomaisten käyttöön soveltuva sopimukseen liitettävä pilvipalvelun tarjoajaa koskeva toimintaohjemalli. Lisäksi Valtionvarainministeriön tulisi varmistua, että Suomessa on koko julkishallinnolle tarjolla ainakin keskeisistä pilvipalveluntarjoajien datakeskusten tai -prosessointipaikkojen sijaintiin perustuvista kyseistä valtiota koskeva kattava arviointi kolmannen valtion lainsäädännön sovellettavuudesta viranomaisten tietoihin. Optimaalisin tilanne olisi, että Valtionvarainministeriö, tai sen ohjauksesta muu keskeinen virasto sopisi esim. koko valtionhallinnon puolesta keskeisten pilvipalveluntarjoajien kanssa käytänteistä, joiden perusteella kolmansien maiden toimivallan käyttö estetään Union alueella prosessoitavien tietojen osalta. Linjauksen suhteen tulisi varmistua, että aiheeseen liittyvässä, Valtionvarainministeriön ja DigiFinlandin Cirrus-hankkeessa näkökulma on huomioitu riittävällä tasolla.

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

Kannatettava esitys.

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

Julkisten hankintojen tietoturvallisuusvaatimuksissa ongelmana on ajoittain se, ettei hankintaorganisaatio ole räätälöinyt vaatimuksia hankintakohteen kannalta, vaan käyttää osin tai kokonaan räätälöimätöntä ”vaatimuskirjastoa”. Tämä johtaa tehottomiin, tarpeeseen nähden liian kalliisiin ratkaisuihin ja karsii myös tarjoajia. Pilviratkaisujen turvallisuus ei ole sellaista, että se joko on tai sitä ei ole. Pilviratkaisuihin tyypillisesti pätee se, että pilven palveluntarjoaja vastaa pilven turvallisuudesta, mutta pilveen tietoja sijoittava vastaa pilvessä olevien tietojensa turvallisuudesta. Turvallisuuden varmistaminen vaatii näin päätöksiä ja ratkaisuja myös palveluiden

käyttäjiltä. On tärkeää, että hankintakohteen turvallisuusvaatimukset arvioidaan ja yksilöidään tarkkaan tarjouspyynnössä. Tähän liittyy olennaisesti myös hankintaosaamisesta huolehtiminen; tarjouspyyntö on valmisteltava huolella ja vaatimusten asettamisessa on käytettävä riittävää asiantuntemusta.

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

Kannatettava esitys.

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

On olennaista kiinnittää huomiota, että kohdissa 6-9 todetut käyttötapaukset eivät ole tietoturvallisuuden tasovaatimuksiltaan samantasoisia, vaikka linjaus onkin muotoiltu kaikissa samoin. Julkisen tiedon turvallisuusvaatimukset eivät ole, eivätkä saa olla yhtä korkeita verrattuna henkilötietojen tai turvallisuusluokan IV-luokan tietojen turvallisuusvaatimuksiin. Se toki ei ole ollut linjausluonnoksessa todetun tarkoituskaan, mutta käytännössä toisinaan näin on hankintatapauksissa tapahtunut. Ks. kohdassa 4 todettu.

Vaikka onkin selvää, että turvallisuusvaatimusten ei tarvitse, tai tule olla samantasoisia, korkea perustaso tulee varmistaa kaikissa tilanteissa tietojen saatavuuden ja eheyden varmistamiseksi.

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

On olennaista kiinnittää huomiota, että kohdissa 6-9 todetut käyttötapaukset eivät ole tietoturvallisuuden tasovaatimuksiltaan samantasoisia, vaikka linjaus onkin muotoiltu kaikissa samoin. Julkisen tiedon turvallisuusvaatimukset eivät ole, eivätkä saa olla yhtä korkeita verrattuna henkilötietojen tai turvallisuusluokan IV-luokan tietojen turvallisuusvaatimuksiin. Se toki ei ole ollut linjausluonnoksessa todetun tarkoituskaan, mutta käytännössä toisinaan näin on hankintatapauksissa tapahtunut. Ks. kohdassa 4 todettu.

Vaikka onkin selvää, että turvallisuusvaatimusten ei tarvitse, tai tule olla samantasoisia, korkea perustaso tulee varmistaa kaikissa tilanteissa tietojen saatavuuden ja eheyden varmistamiseksi.

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

On olennaista kiinnittää huomiota, että kohdissa 6-9 todetut käyttötapaukset eivät ole tietoturvallisuuden tasovaatimuksiltaan samantasoisia, vaikka linjaus onkin muotoiltu kaikissa samoin. Julkisen tiedon turvallisuusvaatimukset eivät ole, eivätkä saa olla yhtä korkeita verrattuna henkilötietojen tai turvallisuusluokan IV-luokan tietojen turvallisuusvaatimuksiin. Se toki ei ole ollut linjausluonnoksessa todetun tarkoituskaan, mutta käytännössä toisinaan näin on hankintatapauksissa tapahtunut. Ks. kohdassa 4 todettu.

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**

On olennaista kiinnittää huomiota, että kohdissa 6-9 todetut käyttötapaukset eivät ole tietoturvallisuuden tasovaatimuksiltaan samantasoisia, vaikka linjaus onkin muotoiltu kaikissa samoin. Julkisen tiedon turvallisuusvaatimukset eivät ole, eivätkä saa olla yhtä korkeita verrattuna henkilötietojen tai turvallisuusluokan IV-luokan tietojen turvallisuusvaatimuksiin. Se toki ei ole ollut linjausluonnoksessa todetun tarkoituskaan, mutta käytännössä toisinaan näin on hankintatapauksissa tapahtunut. Ks. kohdassa 4 todettu.

Lisäksi laadukkaiden pilvipalveluiden sekä vastuullisten palveluntarjoajien kyvyt tarjota tietoturvallisuuden perusratkaisuiltaan erittäin korkeatasoisia palveluita on tunnettu tosiasia. Tämän lisäksi tiedonhallintayksiköiden, tai laajemmin valtion yhteisten pilvi- ja ekosysteemiratkaisujen suunnittelun ja toteuttamisen yhteydessä tulisi kiinnittää erityistä huomiota asianmukaisen salaus- ja avaintenhallintaratkaisujen käyttöönotosta niin, että palveluntarjoajalla ei ole edes teknisesti mahdollisuutta purkaa salausta tai muutoin saada tietoonsa salassa pidettävää tietoa salaamattomassa muodossa.

Pilvilinjauksien jatkovalmistelua tukevat kysymykset

Vihreä kasvu
Leena Nyman

6.3.2023

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

   Pilvipalvelun määritelmällä on merkitystä - luetaanko pilvipalveluiksi vain IaaS-kerros vai myös PaaS ja SaaS kerrokset? (Infrastructure / Platform / Software as a Service). Jos kaikki kerrokset luetaan pilvipalveluiksi, EU/ETA-alueen rajaus voi osoittautua hyvinkin rajoittavaksi linjaukseksi. Esimerkiksi PaaS-kerroksen erilaisia ohjelmistokomponentteja käytetään tänä päivänä laajalti ohjelmistokehityksessä ja kaikki eivät toimi EU/ETA-alueen sisällä. SaaS sovellusten kirjo on tänä päivänä jo valtavan laaja ja EU/ETA-rajaus olisi myös hyvin rajoittava.

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?

   Riskejä voidaan hallita seuraavasti:
   - Tietosuojaa koskevan vaikutustenarvioinnin (DPIA) ja riskiarvioinnin kautta tunnistetaan ja hallitaan riskejä.
   - Riskiä liittyen tiedonsiirtoon kolmansiin maihin hallitaan jäännösriskinä.
   - Tukipyyntöjen osalta tapauskohtainen hyväksyntä tiedon siirrolle EU/ETA- alueen ulkopuolelle. Omien salausavaimien käyttö ja tehokas, nykyaikainen salausavainten hallinta.
   - Henkilöstön tietosuojakoulutus.

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

   Merkittävin este on kahtalainen: ensinnäkin yleinen suhtautuminen siihen, että henkilötietoja ei voitaisi käsitellä pilviteknologiaratkaisuissa, sekä toisaalta se, että henkilötietoa koskevaa määritelmää laajennetaan tarpeettomasti ja osittain väärin koskemaan lähes kaikkia tietoa, vaikka suoraa yhteyttä henkilön tunnistamiseen ei ole. Tätä seikkaa pahentaa lisäksi se, että tosiasiallisesti yleisen tietosuoja-asetuksen henkilötietoja koskevien periaatteiden kuten minimoinnin, anonymisoinnin muiden suhteellinen vajaa käyttö.

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

   Kohdassa 1 mainittu pilvipalvelun määrittely ja IaaS/PaaS/SaaS kerrosten rajaus olisi tärkeää tehdä selkeästi.

   Termiä huoltovarmuus käytetään toisinaan hämärtävästi perusteluna pilvipalveluiden kieltämiselle. Venäjän hyökkäyssota Ukrainassa on osoittanut vain kotimaisten konesalien haavoittuvuuden perinteisen kineettisen sodankäynnin keinoin (esim. ohjusiskut ja sabotaasi). Kriittisten datojen ja sovellusten hajautus myös ulkomaisiin konesaleihin on uudella tavalla perusteltua.

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

- Osapuolten välillä tulee olla selkeästi tiedossa ja ymmärrettynä, miten tietosuojan toteuttamisen roolit, vastuut ja velvoitteet muodostavat kokonaisuuden.
- Osapuolten välillä tulee olla GDPR:n vaatimukset täyttävät toimintamallit (sopimukset, käytänteet, sertifioinnit)
- Kunkin käsittelijän tulee kyetä etukäteen osoittamaan sekä tietosuojavaatimusten täyttyminen että palvelun tietoturvallisuuden taso siten, että rekisterinpitäjä voi arvioida niiden riittävyyden.
- Käsittelijä – alikäsittelijä ketjujen tulee olla läpinäkyviä
- Sopimusmuutokset ketjussa tulee toteuttaa siten, että käsittelijät eivät voi heikentää tietosuojan tai tietoturvallisuuden tasoa yksipuolisesti.
- Yleinen API-/rajapintalähtöisyys julkisen sektorin ohjelmistohankkeissa olisi tärkeä myös pilvipalveluiden hyödyntämisen edistämiseksi.

Kunnioittavasti

Elinkeinoelämän keskusliitto EK

Ulla Heinonen
Johtaja