CSC - Tieteen tietotekniikan keskus Oy

Lausunto

10.03.2023

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

Pilvipalveluiden käyttöönotto on usein taloudellisempaa ja joustavampaa kuin asiakasorganisaation itse tuottamien alustojen ja palveluiden käyttöönotto, mutta myös pilvipalvelun riittävästä turvallisuudesta tulee varmistua käyttötarkoitus ja riskienhallinnan tarve huomioiden. Pelkkä tieto tietoturvasertifioinnin olemassaolosta ei vielä takaa palvelun turvallisuutta, vaan esim. sertifioinnin asianmukainen kattavuus on syytä myös varmistaa.

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

Riskiperusteiseen päätöksentekoon tulee olla tarkempaa ohjeistusta, jotta vastuu ei lankea yksittäisille tiedonhallintayksiköille/virastoille vaan linjausta sovelletaan samalla tavalla. On esimerkiksi tärkeää linjata, minkä palveluiden tai tiedon täytyy olla saavutettavissa, vaikka kansainväliset tietoliikenneyhteydet muualle Eurooppaan olisivat poikki. Lisäksi tarvitaan ohjeet siitä, mitä riskiarvioinnissa on huomioitava ja miten eri riskejä painotetaan. Samoin tulee linjata ne periaatteet, joilla käsitellään palveluiden toimitusketjuja tai vaikutusmahdollisuuksia, joihin viitataan linjauksen kohdassa 9.

Riskienhallinnan tueksi olisi myös hyödyllistä ja tehokasta tehdä yhteisiä riskiarviointeja eri käyttötarkoitusten ja turvallisuusvaatimusten lähtökohdista.

Linjausten yhteyteen päivitettävien soveltamisohjeiden ja toimenpidekorttien valmistelussa tulee kuulla laajasti sidosryhmiä, jotta linjauksiin liittyvät menettelytavat esim. riskienhallinnan, teknisten ratkaisujen ja tuloksellisuuden kannalta saadaan riittävän konkreettisiksi.

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

Yhteentoimivuus on tärkeä tavoite, mutta on aina huomioitava käyttötarkoitus ja sen mukainen mahdollisimman tarkoituksenmukainen ratkaisu. Olemassa olevia ratkaisuja kannattaa hyödyntää. Esimerkiksi tieteellisen laskennan alueella on kansallisia ja eurooppalaisia yhteisiä ratkaisuja, joita

kannattaa hyödyntää erillisten pilviratkaisujen sijaan. Tämän linjauksen ja 1. linjauksen välistä suhdetta tuleekin näiltä osin selventää.

Estävät perusteet tai niiden periaatteet tulee määritellä mahdollisesti erillisessä ohjeistuksessa, eikä niiden arvioinnin kannata olla yksittäisen organisaation/henkilön vastuulla. Lisäksi on huomioitava esim. huoltovarmuus ja turvallisuusnäkökohdat.

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

Tässä tulee huomioida koko Euroopan laajuiset korkeakoulutuksen ja tutkimuksen pilvihankinnat (GÉANT IaaS+ / OCRE), joiden käyttö on siellä tarkoituksenmukaista. Lisäksi valtionhallinnossa ja valtion sidosyksiköissä tuotetaan kansallisia pilviratkaisuja mm. tutkimukselle ja koulutukselle, joiden käyttö tulee jatkossakin olla mahdollista näihin tarkoituksiin. Linjauksen tavoitteessa tuleekin tarkentaa, mihin valtionhallinnon yksiköihin määrittely rajoittuu.

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

Hankinnassa ja muutoshallinnossa tulee olla yhteiset valtakunnalliset toimintamallit ja vähimmäisvaatimukset.

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

Riskiperusteiseen päätöksentekoon on tärkeää saada tarkempaa ohjeistusta, jotta linjausta sovelletaan yhdenmukaisesti. Esimerkiksi henkilötietojen käsittelystä säädetään yleisessä tietosuoja-asetuksessa. Osa henkilötiedoista on julkisia tietoja (esim. autojen rekisterit), mutta silti niitä on käsiteltävä henkilötietoina. Se, onko jokin tieto määritelty julkiseksi tiedoksi, ei näin ollen sovellu kategorisesti kriteeriksi käsittelyn määrittelyyn.

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

Riskiperusteiseen päätöksentekoon on tärkeä olla tarkempaa ohjeistusta, jotta linjausta sovelletaan samalla tavalla. Salassa pidettävän tiedon siirtämisestä pilveen on oltava yhtenäiset kansalliset linjaukset/ohjeistus vaatimustenmukaisuuden ja tietoturvan vähimmäisvaatimuksiin.

Riskiarviointi on vaativaa ja päätöksen vastuuttaminen yksittäiselle tiedonhallintayksikölle/virastolle luo mahdollisuuden eriäville käytännöille ja päätöksille. Nyt kommentoitavana olevat linjaukset vaativat tuekseen ohjeet siitä, mitä riskiarvioinnissa on huomioitava ja miten riskejä painotetaan.

Pidämmekin tärkeänä, että jatkovalmistelussa olevien linjausten yhteyteen päivitettävien soveltamisohjeiden ja toimenpidekorttien valmistelussa kuullaan laajasti sidosryhmiä, jotta linjauksiin liittyvät menettelytavat esim. riskienhallinnan, teknisten ratkaisujen ja tuloksellisuuden kannalta saadaan riittävän konkreettisiksi.

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

Riskiperusteiseen päätöksentekoon on tärkeä olla tarkempaa ohjeistusta, jotta linjausta sovelletaan samalla tavalla. Olisi myös täsmennettävä, koskeeko linjaus myös erityisiä henkilötietoryhmiä.

Tällä hetkellä tiedonsiirtojen mahdollisuus Yhdysvaltoihin on epäselvä. Yhdysvaltojen tietosuojan riittävyyspäätöksen käsittely EU:ssa on kesken. Mm. Euroopan tietosuojaneuvosto (EDPB) on esittänyt varauksia päätösluonnokseen suhteen. https://tietosuoja.fi/-/euroopan-tietosuojaneuvosto-antoi-lausuntonsa-yhdysvaltojen-tietosuojan-riittavyyspaatoksen-luonnoksesta

Euroopan tietosuojaneuvosto julkaisi tammikuussa selvityksen eurooppalaisten tietosuojaviranomaisten yhteistyöhankkeena suorittamasta pilvipalveluiden käytöstä julkishallinnossa. Kansallisissa linjauksissa tulee ottaa huomioon EU-tasolla tehtävät linjaukset, suositukset ja soveltamisohjeet. https://edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-use-cloud-based-services-public_en

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

Riskiperusteiseen päätöksentekoon tarvitaan tarkempaa ohjeistusta, jotta linjausta sovelletaan yhdenmukaisesti. Erityisen tärkeää on tarkentaa, miten tunnistetaan turvallisuusluokiteltu tieto, jota voi siirtää muihin maihin linjauksessa kuvatulla tavalla. Samoin tulee avata, mihin maihin tässä linjauksen kohdassa viitataan.

Pilvilinjauksien jatkovalmistelua tukevat kysymykset

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

Linjaukset eivät ole riittävän konkreettisia, jotta ne olisivat mahdollistavia. Kaikista keskeisimmät pilvien hyödyntämiseen liittyvät kysymykset on jätetty linjauksessa viraston tai tiedonhallintayksikön ratkottavaksi. Laaja, virasto- tai tiedonhallintayksikkökohtainen riskiperusteinen päätöksenteko voi johtaa hankalaan sovellettavuuteen ja toisistaan eroaviin käytäntöihin. Tarkempien linjausten puute aiheuttaa myös päällekkäistä työtä. Tarkempi ohjeistus esimerkiksi riskiarvioinnista ja hyväksyttävästä jäännösriskistä sekä erityisistä perusteista on tarpeen.

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

Tarkemmat linjaukset poistaisivat pilvipalvelujen käytön esteitä ja epäselvyyttä.

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

Tärkeää on tunnistaa valtionhallinnon palvelut ja tieto, joiden täytyy olla saavutettavissa myös kansainvälisten, Suomen muuhun Eurooppaan liittävien tietoliikenneyhteyksien katketessa. Riskejä voi pienentää myös tiedon varmistamiseen liittyvillä ratkaisuilla. Yhteiset, riskipohjaiset linjaukset poistaisivat mahdollisuutta erilaisille tulkinnoille. Pilvipalvelujen hyödyntäminen ei poista organisaation oman tietoturvaosaamisen tarvetta. Myös selkeämmät maakohtaiset ohjeistukset vähentäisivät riskejä.

Riskejä voidaan vähentää vaatimalla palveluntuottajalta ennalta määriteltyjä teknisiä ja organisatorisia suojatoimia. On huomioitava myös tilaajaosaaminen sekä se, ettei pilvipalvelujen käyttö voi tarkoittaa tietoturvaosaamisen ulkoistamista.

Tulee myös kiinnittää huomiota datan palauttamiseen ja siirrettävyyteen, mikäli pilviratkaisua vaihdetaan.

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

Suurimmat esteet liittyvät tietosuoja-asetuksen ja lainsäädännön soveltamiseen ja käytännön tulkintaan. Sekä EU- että kansalliselle tasolle tarvitaan yhteistä linjanvetoa, jolla vältetään keskenään erilaiset tulkinnat.

Arviointia ja päätöksiä näiden palveluiden käytöstä kannattaa tehdä kansallisesti ja/tai EU-tasolla yksittäisten organisaatioiden sijaan. Tämä auttaisi välttämään mahdollisten eriävien tulkintojen ja soveltamisen aiheuttamia ongelmia virastojen ja tiedonhallintayksiköiden välillä, ja varmistaisi myös mm. kansalaisten yhdenvertaisuutta tietosuoja-asioissa.

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

Pilvipalveluiden, kuten kaikkien digitaalisten infrastruktuurien, keskiössä on data. Lainsäädännölliset esteet datan liikkuvuudelle tulee kartoittaa ja purkaa, jotta palveluita voidaan täysmääräisesti hyödyntää.

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

Linjauksille tarvitaan ajantasaiset konkreettiset soveltamisohjeet, jotta niitä sovelletaan yhdenmukaisesti. Lisäksi on tärkeää tarkastella pilvipalveluita osana laajempaa digitaalisten infrastruktuurien kokonaisuutta, joka ei rajoitu vain yhdenlaiseen käyttötarkoitukseen tai yksittäiseen teknologiaan. Pilvipalvelut tulee nähdä osana yhteiskunnan prosessien ja rakenteiden kehittämistä myös laajemmin kuin pelkkänä teknologisena asiana, jolloin korostuu niiden käyttötarkoitus ja sen mukaiset käyttöperiaatteet.

Espoossa 10.3.2023

Kimmo Koski, toimitusjohtaja
Irina Kupiainen, johtaja, yhteiskuntasuhteet