Väestörekisterikeskus

Lausunto

07.09.2018 VRK/3920/2018

Asia: VM/276/00.01.00.01/2018

Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta

Yhteenveto

Kommentit yhteenvetoon:

-

Taustaa linjauksille

Kommentit taustaan:

Yleisiä kommentteja:

Linjaus lähtee liikkeelle teknisestä toteutusmallista niin, että pilvipalvelut on keskiössä. Yksittäinen ratkaisumalli ei sellaisenaan ole itseisarvo, tietojen käsittely tulisi suunnitella vaatimustenmukaisesti, turvallisesti ja tätä kautta saavuttaa laadun ohella kustannustehokkuutta. Tarkastelun tulisi käsitellä enemmän tietojen käsittelyvaatimuksia (tiedon sijainti) ja käsittelyyn liittyvää riskienhallintaa.

Pilvipalveluiden hankinnasta voisi olla erillinen opas, joka kertoo, mihin asioihin tulisi kiinnittää huomiota hankittaessa pilvipalveluita.

Linjaus keskittyy pilvipalveluihin, olisi hyvä huomioida linjauksen nimessä (esim ”tiedon sijainnista ja hallinnasta” asemesta ”pilvipalvelujen hyödyntämisestä”

Linjausten tavoitteet

Kommentit tavoitteisiin:

-

Pilvipalveluiden edut sekä toteutus- ja palvelumallit

Kommentit:

-

Pilviteknologian edut

Kommentit:

-

Palvelumallit

Kommentit:

-

Toteutusmallit

Kommentit:

-

Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Kommentit:

Ristiriita linjauksen 9 kanssa:

Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa

Tällaisen tiedon käsittelyyn käytettävän pilvipalvelun täytyy sijaita fyysisesti Suomen tai EU:n alueella ja sen täytyy olla Suomessa tai EU alueella sijaitsevan toimijan hallinnassa. Palvelun on täytettävä tiedon käsittelylle asetetut vaatimukset samalla tavalla kuin muiden toteutusmallien.

- - palvelun on oltava lisäksi viranomaisen hyväksymä.
- - sivun 10 linjauksessa rajataan käsittely Suomeen
- - sivun 10 linjauksessa edellytetään myös peruste sekä riskienhallintaa

Onko tästä linjauksesta mahdollisesti seurauksena, että rajoitetaan isojen toimijoiden palvelujen hyödyntämistä?

On pystyttävä mahdollistamaan tilanne, jossa hallintatoimenpiteitä voidaan tehdä EU/ETA-alueen ulkopuolelta, kuitenkin niin ettei itse tietoon ole pääsyä.

Tiedon käsittelyn vaatimukset

Kommentit:

-

Palveluiden ohjaus

Kommentit:

-

Haasteet

Kommentit:

-

1. Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta

Kommentit:

Hankinta ja muutos voi tarkoittaa eri asioita eri tilanteessa. Yleispätevät periaatteet jäävät niin yleiselle tasolle, että ne voisi luetella. Lisäksi pilvipalvelut eivät ole käsitteenä yksi kokonaisuus, vaan voi tarkoittaa eri asioita.

2. Tiedon sijaitessa Suomen rajojen ulkopuolella erityistä on kiinnitettävä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen

Kommentit:

Linjauksen tulisi koskea mitä tahansa kriittistä palvelua myös rajojen sisäpuolella.

3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset

Kommentit:

Hankittavan palvelun tulee lähtökohtaisesti aina olla hankkijalle hyödyllinen ja laadukas. Asiakas lähtökohtaisesti hankkii palvelua tai ratkaisua, eikä tiettyä ratkaisumallia. Mikäli ratkaisumalli tuottaa merkittävää hyötyä, tulisi se priorisoida. Tämä koskee myös pilvipalveluja.

4. Mikäli pilvipalvelut tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita

Kommentit:

-

5. Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti vähintään kerran vuodessa ja oleellisten sopimusehtojen muuttuessa.

Kommentit:

-

6 Viranomainen ylläpitää listaa hyväksytyistä palveluntarjoajista

Kommentit:

Mikä taho on tässä yhteydessä viranomainen?

Minkälainen on viranomaisen hyväksymisprosessi? Jos esim hankintayksikkö tekee itsenäisesti hankinnan, ja palveluntarjoajaksi valikoituu sellainen taho, joka ei vielä ole viranomaisen hyväksyntä, kuinka kauan viranomaisen hyväksymisprossissa menee? Vai valitaanko (kilpailutetaanko) palveluntuottaja hyväksyntälistalta? Tällöin tulee ottaa kilpailunäkökulmat huomioon.

Miten listalla olevia arvioidaan, eli että säännöllisesti voidaan varmistua, että toimittajat edelleen täyttävät vaatimukset? Mitä ”valvontakeinoja” nimetyllä viranomaisella on eli vaatimusten jatkuvaa täyttymistä seurataan?

Vaatimuslista pitäisi määrittää sellaiseksi, että on realistista saada listalle suuria kansainvälisiä toimijoita. Ei ole realistista odottaa, että nämä toimijat räätälöisivät palveluitaan Suomen mahdollisia erityistarpeita varten. Tukeudutaan esim. kansainvälisiin standardeihin.

7. Julkisen tiedon käsittelyä ei rajoiteta

Kommentit:

Linjauksen loppuun tulisi lisätä: Tässä tulee ottaa julkisen tiedon osalta sen saatavuuden ja eheyden merkitys osana tietoturvallisuuden toteutumista.

8. Henkilötietoa ja suojaustason IV tietoa voi käsitellä julkisessa pilvessä, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu

Kommentit:

Riittääkö tässä viraston oma arvio, kuka ”viranomainen” tässä tapauksessa on? Mitä tarkoitetaan, kts alla, todentamisella ja hyväksynnällä?

” asianmukaisesti toteutettu ja todennettu”

 - mikäli kyseessä viranomaisen hyväksymä palvelu, tarvitaanko lisäksi auditointi asiakasviraston toimesta?

” jatkuvuudesta on varmistuttu asianmukaisesti viranomaisen hyväksymällä tavalla”

 - tarkoittaako tämä ”hyväksyntä” auditointia, vai miten tämä vaatimus täytetään

”Henkilötietojen käsittelyn ja hallinnan osalta tulee lisäksi varmistua muista EU/ETA-alueen ulkopuolella vaadittavista edellytyksistä.”

Mitä tällä tarkoitetaan, ”vaadittavat edellytykset”?

Henkilötiedot on laaja ryhmä, linjauksissa tulisi huomioida paremmin eri tyyppiset henkilötiedot (esim. potilastiedot).

Kuten ei myöskään ole mahdollista ja järkevää rinnastaa suoraan henkilötietoja sekä ST IV-luokiteltuja tietoja keskenään, näillä on varsinkin tietosuoja-asetuksen näkökulmasta hyvin erilaisia vaatimuksia.

9. Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa

Kommentit:

-

Suosituksia toimenpiteiksi

Kommentit:

Eikä suuri osa jatkotoimenpiteitä hoituisi sillä, että Valtori tarjoaa koko valtionhallinnolle tarkoitetun viranomaisen hyväksymän pilvipalvelun.

Tuon ”baseline”-palvelun ”päälle” asiakasvirasto voi tehdä lisäarvioita.

Sopimusehtojen riittävä huomiointi: tähän täytyy olla osaamista ja neuvottelukykyä. Monet palveluntuottajat on siinä määrin isoja organisaatioita, etteivät välttämättä lähde neuvottelemaan näistä, tällöin ei saa hakea helppoa ratkaisua ja hyväksyä sopimusehtoja, jotka esim rikkovat tietosuoja-asetuksen periaatteita. Huomattavaa on, että palveluntarjoajilla voi olla ehtoja, jotka

tosiasiallisesti indikoivat sitä, etteivät vaatimukset palvelussa täyty (esim. rekisteröidyn oikeuksien toteuttaminen: saadaanko tosiasiallisesti palveluntarjoajalta ja tämän alihankkijoilta tieto siitä, mitä henkilön tietoa käsitellään ja missä).

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

-

Ristimäki Pekka
Väestörekisterikeskus