Ulkoministeriö

Lausunto

05.09.2018

Asia: VM/276/00.01.00.01/2018

Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta

Yhteenveto

Kommentit yhteenvetoon:

Pilvipalvelut ovat yksi tietoteknologian kehitykseen vaikuttavista megatrendeistä ja on hyvä asia, että niiden hyödyntämiseen otetaan kantaa. Tällaisenaan kannaotot jäävät kuitenkin linjausten osalta hyvin yleisiksi eikä sinänsä ole riittävällä tasolla ohjaamaan viranomaisten toimintaa. Arvioitaessa hyöty-, turvallisuus-, takuu- jne. näkökohtia olisi määritettävä prosessi ja asiantuntijatoimijat tämän arvioinnin tueksi vastaavalla tavalla kuin mitä noudatetaan esimerkiksi kansainvälisten luokiteltujen tietoaineistojen käsittelykriteereissä. Tämä edellyttäisi käytetyn käsitteen "viranomainen" jonkinasteista määrittelyä rooleineen ja toimivaltuuksineen. Pilvipalvelujen määrittelyssä olisi myös tarkasteltava reunaehtoja yksityisen, hybridi- tai julkisen pilven käyttömahdollisuuksien näkökulmasta huomioiden kotimaisuus/ulkomaisuus -näkökohdat. Arkkitehtuuritarkastelu onkin kokonaisuuden suhteen syytä suorittaa pikaisesti odottamatta tiedonhallintalainsäädännön etenemistä.

Taustaa linjauksille

Kommentit taustaan:

Selkeämpi jako olisi tiedon käsittely-ympäristön sijainti joko kotimaassa tai ulkomailla. Välttämättä sijainti EU- tai ETA-alueella (versus muu maailma) ei tuo merkittävää lisäarvoa kansallisen turvaluokitellun aineiston käsittelyn suhteen, koska tieto joka tapauksessa sijaitsee toisen kansallisvaltion alueella.

Linjausten tavoitteet

Kommentit tavoitteisiin:

Tällaisenaan linjaukset eivät yksityiskohtaisuutensa osalta tue määritettyjä tavoitteita esim. riskienhallinnan, kustannusten ja hyötyjen arvioinnin sekä hankintaprosessin osalta. Ei ole nähtävissä, miten ne valmistavat ICT-henkilöstöä pilvipalvelujen hyödyntämiseen.

Pilvipalveluiden edut sekä toteutus- ja palvelumallit

Kommentit:

SaaS julkisessa pilvessä tuo toki maksimaalisen hyödyn, mutta turvanäkökulmasta myös maksimaaliset uhkatekijät.

Pilviteknologian edut

Kommentit:

-

Palvelumallit

Kommentit:

On huomioitava, että tiedon omistajan vastuut tiedon hallinnalle säilyvät riippumatta siitä, missä ja miten tietoa hallitaan esim. pilvipalvelualustalla. Teknisestä osaamisesta tarve siirtyy hallinnalliseen ja koordinaatio-osaamiseen kun siirrytään itse tekemisestä muiden tekemiseen. Vanhat lainalaisuudet eivät poistu; pilvipalvelujen taustalla ovat edelleen tietokoneet ja kyseessä on ainoastaan se, että joku toinen taho tekee järjestelmien operointia jossain muualla ja tekijöiden roolitukset ovat erilaiset verrattuna perinteiseen konesali- tai kapasiteettipalveluun.

Toteutusmallit

Kommentit:

Oma konesali ei ole pilvipalvelu, mutta oma konesalikapasiteetti voidaan järjestää pilvikonseptin mukaiseksi palveluksi.

Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Kommentit:

Big Data -ajattelussa tietomassa tarpeeksi suureksi muodostuessaan saattaa turvallisuusvaateidensa osalta muodostaa kokonaisuuden, jota ei ole syytä käsitellä julkisen tiedon tapaan. On täsmennettävä mitä tarkoitetaan tiedon käsittelyllä; yleensä siihen kuuluu myös mahdollisuus tiedon muokkaamiseen.

Tiedon käsittelyn vaatimukset

Kommentit:

Ulkoasiainhallinto kyseenalaistaa vahvasti linjauksissa esitetyn periaatteen, että suojaustason neljä (ST IV) voitaisiin käsitellä ulkomaisessa pilvipalvelussa. Mikäli näin menetellään, on tarkemmin määriteltävä mitä muita suojausmetodiikkoja (esim. kryptaus) käytetään tiedon suojaamiseksi. Edelleen haasteeksi jää, että tiedot saatavuutta ei voida taata STIV-tietojen sijaitessa muualla kuin kotimaassa.

Palveluiden ohjaus

Kommentit:

Luottamus on tässäkin mallissa hyvä asia, mutta kontrolli tiedon hallintaan on joka tapauksessa parempi ja siten säilytettävä ja todennettava, jotta edellä viitattu tiedon omistajan vastuu tiedon elinkaaren hallinnasta on varmennettavissa.

Haasteet

Kommentit:

Edellä kommentoidun lisäksi on syytä korostaa, että yhdelläkään kansallisella viranomaisella ei ole tosiasiallista mahdollisuutta selvittää suurten kansainvälisten pilvipalvelutoimittajien osalta, mihin palvelujen turvallisuus käytännössä pohjautuu. Tässä mielessä riskiarvion teko jää merkittävän puutteelliseksi.

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

Kommentit:

On huomioitava edellä mainittujen varaumien lisäksi, mikä on ns. exit-strategia, mikäli palvelusta joudutaan syystä tai toisesta luopumaan.

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

Kommentit:

Suomalaisen viranomaisen mahdollisuudet vaikuttaa suurten palvelutuottajien sopimusehtojen sisältöön on erittäin rajallinen. Kustannusetuhan palveluissa perustuu siihen, että kaikille asiakkaille tuotetaan samaa palvelua.

3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset

Kommentit:

-

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

Kommentit:

Pilvi ensin -ajattelu on toki kustannushyötyjä tavoittelevalle vaihtoehto. Toki vastaavan lauseen voi pilvi-sana poistamalla kirjata kaikkien hallinnon hankkimien ICT-palvelujen tavoitteeksi.

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

Kommentit:

Vastaavan kirjauksen voi tehdä kaikkien hallinnon hankkimien palvelujen osalta.

6 Viranomainen ylläpitää listaa hyväksytyistä palveluntarjoajista

Kommentit:

Käsite viranomainen tulee määritellä. Vastaavasti tulee määrittää millä toimivaltuuksilla ko. viranomainen toimii. Mikäli viranomaisella tarkoitetaan jokaista tietojen omistajatahoa, tulee tukintojen kirjosta laaja ja tämä aiheuttaa haasteita viranomaisten keskinäiselle tietojen vaihdolle.

7. Julkisen tiedon käsittelyä ei rajoiteta

Kommentit:

Vapaa käsittelyoikeus tarkoittaa käsitteenä myös oikeutta muokkaamiseen. Tällöin tiedon eheys ja oieellisuus ei ole hallittua.

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

Kommentit:

On huomioitava, että tiedon tulee on suojattuna sekä siirron (käsittely) että tallennuksen aikana mikäli periaatetta noudatetaan. Henkilötieto voi toisaalta olla joko luokiteltua tai julkista. Salaaminen tulee toteuttaa toimivaltaisen viranomaisen hyväksymällä menetelmällä ml. avainten hallinta. Voiko tiedon omistava viranomainen kieltää tiedon käsittelyn pilvipalvelussa, mikäli se oman riskiarvion perusteella ei ole mahdollista (tiedon yhteiskäyttötapaus)?

9. Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa

Kommentit:

EU muodostuu kansallisvaltioista. Ero Unionin ja muun maailman osalta ei siten ole merkittävä käsittelyn osalta. Kyseisten asioiden arvioinnissa tulee noudattaa vastaavia periaatteita ja arviointi/auditointikäytäntöjä kuin kansainvälisen turvaluokitellun tiedon käsittelykonseptissa.

Suosituksia toimenpiteiksi

Kommentit:

Jatkotyöksi esitetyt toimenpiteet ovat kannatettavia, sillä nykytasollaan linjauksia ei voida ottaa käyttöön ennen merkittäviä täsmennystoimia. Tiedonhallintalain kehitys ja vaikutukset tulee arvioida ennen linjausten käyttöönottoa.

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Esitetyt linjaukset eivät varsinaisesti vastaa kysymyksiin joiden johdosta työryhmä oli alun perin perustettu. Toimenpiteiden täsmällisempi linjaaminen vaikuttaa siirtyneen esitetyiksi jatkotoimenpiteiksi.

Uusikartano Ari
Ulkoministeriö