



Asia: VM/276/00.01.00.01/2018

## **Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta**

### Yhteenveto

#### **Kommentit yhteenvetoon:**

-

### Taustaa linjauksille

#### **Kommentit taustaan:**

-

### 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:**

-

Tiedon käsittelyn vaatimukset

**Kommentit:**

-

Palveluiden ohjaus

**Kommentit:**

-

Haasteet

**Kommentit:**

-

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

**Kommentit:**

-

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

**Kommentit:**

-

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:**

-

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

**Kommentit:**

-

6 Viranomaisen ylläpitää listaa hyväksytyistä palveluntarjoajista

**Kommentit:**

-

7. Julkisen tiedon käsittelyä ei rajoiteta

**Kommentit:**

-

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

**Kommentit:**

-

9. Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa

**Kommentit:**

-

Suosituksia toimenpiteiksi

**Kommentit:**

-

Lausunnonantajan lausunto

**Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään**

Sisäministeriö pitää tärkeänä yhteisten julkisen hallinnon linjauksien laatimista tiedon sijainnista ja hallinnasta. Lausuttava asiakirja on kuitenkin keskeneräinen,

ydintavoitteiltaan ja linjauksiltaan tarkennettava ja yhtenäistettävä sekä kokonaisuudessaan selkiytettävä vastamaan linjausten tavoitteita.

## Yhteenveto

Yhteenvedon alussa linjauksien pääasiana mainitaan määrittää miten tietoa voidaan sijoittaa ja hallita maantieteellisesti. Tämä ei kuitenkaan välity itse linjauksista eikä dokumentista. Linjauksissa ainoa kohta maantieteelliseen sijaintiin liittyen on kohta 2, jossa mainitaan vain tiedon sijaitessa Suomen rajojen ulkopuolella tarpeen kiinnittää erityistä huomiota sopimukseen, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen. Tämän pitäisi olla lähtökohta tiedon sijainnista huolimatta. Muuten linjauksissa, linjausten tavoitteissa tai linjausten näkökulmissa ei maantieteellistä sijaintia mainita mitenkään. Kappaleessa 3. Linjausten tavoitteet mainitaan linjausten keskittyvän kahteen kokonaisuuteen; pilvipalveluiden hyötyihin ja haasteisiin. Lukijan kannalta dokumentti, sen tarkoitus ja sisältö jää epäloogiseksi ja sekavaksi.

Pilvipalveluiden ominaisina etuina mainitaan olevan mm. kustannustehokkuus. Tähän ei kuitenkaan ole esitetty yhtään viitettä tai perustelua. Sen sijaan mm. Gartner on esittänyt (Can you save money migrating to cloud IaaS? 2016), että siirtyminen pilvipalveluihin voi olla jopa 20 % kalliimpaa kuin olemassa oleva toiminta. Jyväskylän yliopiston tietojenkäsittelytieteiden laitoksella tehdyssä tutkielmassa (Asiakkuudenhallintajärjestelmien ja niiden pilviratkaisujen hinnoittelun vertailu 2013) esitetään kyselytutkimuksesta saatujen vastausten mukaan pilvipalveluna toimivan asiakkuudenhallintajärjestelmän kustannusten keskiarvon olleen korkeampi kuin paikallisesti asennettavan asiakkuudenhallintajärjestelmän kustannusten vastaava luku. Tilastokeskuksen 2014 tekemän Tietotekniikan käyttö yrityksissä kyselyssä pilvipalveluja käyttäviltä yrityksiltä kysyttiin onko pilvipalveluissa jotain tekijöitä jotka rajoittavat niiden käyttöä. Kolmannes näistä yrityksistä piti tietoturvariskejä rajoittavana tekijänä, samoin kolmannes piti korkeita kustannuksia rajoittavana tekijänä. Vaikka nämä tutkimukset ja kyselyt ovatkin jo vanhoja antavat ne viitteitä siihen, että pilvipalvelut eivät itseisarvoisesti ole kustannustehokkaampia kuin muut

ratkaisut, vaan kustannustehokkuus tulisi aina arvioida tapauskohtaisesti kyseisen palvelutarpeen mukaan sovitettuna.

Dokumentista välittyy helposti harhaan johtava kuva pilvipalveluiden kustannustehokkuudesta ilman perusteltua tutkimusta. Dokumentissa painotetaan erityisesti pilvipalveluita, vaikka pääpaino pitäisi olla kokonaisvaltaisella arvioinnilla palvelutarpeesta ja siihen parhaiten (tiedon sijainnin ja hallinnan kannalta) sopivimmasta ratkaisusta. Linjauksista kohta 1 tai 4 olisi sopivampaa olla muodossa: ICT-palveluita hankittaessa tulisi palvelu- ja toteutusmalleista valita tietoturva ja varautuminen huomioiden kustannustehokkain ratkaisu, joka täyttää palvelutarpeen.

Taustaa linjauksille

Ei lausuttavaa.

Linjausten tavoitteet

Linjausten tavoite tukea valtion, maakuntien ja kuntien päätöksentekoa niiden suunnitellessa ja hankkiessa uusia ICT-palveluita on erittäin kannatettava. Tämä tavoite ei kuitenkaan välity itse linjauksista. Myös lueteltujen tarkempien linjausten tavoitteiden suhde linjauksiin on epäselvä. Linjausten näkökulmat ovat hyviä, mutta jäävät irtonaiseksi. Lisäksi linjausten tavoitteista puuttuu olennaisesti kappaleessa 4.1 pilvipalveluteknologian edut ja 4.2 Palvelumallit eri kohdissa perusteena käytetty osaamistarpeen väheneminen tai kokonaan poistaminen. Jos osaamistarpeen poistaminen tai merkittävä vähentäminen on selkeä perusteltu tavoite, tulisi se myös mainita tavoitteissa ja nostaa omana linjauksenaan näkyviin.

Viimeinen kohta linjausten koskemisesta pääasiassa Suomen ulkopuolelta hankittavia palveluita, mutta samaan aikaan esitetään niitä sovellettavan myös Suomesta hankittaviin palveluihin on epälooginen huomioiden dokumentin sisältö sekä varsinkin tätä seuraava lause "Kaikissa hankittavissa palveluissa tarvitsee arvioida toimintaan

(minkä ja kenen toimintaan?) liittyvät riskit sekä toteuttaa muut palvelulta edellytettävä vaatimuksenmukaisuus.". Tämän pitäisi olla itsestäänselvyys minkä tahansa palvelun hankintaan eikä vain tiedon sijainnin ja hallinnan kannalta Suomen ulkopuolelta hankittavista palveluista.

Pilvipalveluiden edut sekä toteutus- ja palvelumallit

Esitettäessä pilvipalvelujen etuja ja malleja tulisi määrittää millaisia pilvipalveluja tarkoitetaan; nyt lausunnolla olevassa dokumentissa todetaan, että pilvipalveluilla tarkoitetaan asiayhteydestä riippuen eri asioista ja tämän jälkeen on esitetty mitä tyyppillisesti tarkoitetaan. Jos linjaukset keskittyvät pilvipalveluiden hyötyihin ja haasteisiin tulisi määrittää mitä pilvipalveluilla tässä yhteydessä tarkoitetaan, jotta niiden etuja voi arvioida.

Samassa yhteydessä todetaan, että maksimaalinen hyöty on saavutettavissa julkisessa pilvessä tuotetusta SaaS tyyppisestä palvelusta ilman perusteluja väitteen tueksi tai viitteitä mitä täällä tarkoitetaan. Maksimaalinen hyöty on tässä aika abstrakti käsite.

Pilvipalveluteknologian edut

Osaamistarpeen vähentäminen tai kokonaan poistaminen palvelun käyttäjältä on nostettu esille useassa eri kohdassa, jolloin se pitäisi nostaa selkeästi esille linjauksiin ja/tai niiden tavoitteisiin; palvelun tuottamiseen ja ylläpitämiseen, tietoturvaan, palvelujen käyttöönottoon, konesaleihin ja infrastruktuurin liittyvän osaamisen poistaminen palvelujen käyttäjäorganisaatioilta ja käyttäjiltä.

Tietoturvallisuudesta todetaan pilvipalveluiden tuottajalla olevan parempi kyvykkyys ja resurssit toteuttaa tietoturvallisuutta, mutta samalla pilvipalveluiden haasteena mainitaan olevan tietoturvan toteutuminen tiedon sijainnista ja hallinnasta riippuen. Tähän lisättyä pilvipalvelun käyttäjän näkökulmasta etuna on todettu palvelun tietoturvaan liittyvän osaamistarpeen pieneneminen, jolloin kokonaisuuden osalta lukijalle ei välity mitä tietoturvallisuuden osalta linjauksilla halutaan. Selkeämpää olisi välttää käyttämästä tietoturvaa yläkäsitteenä eri kohdissa ja mieluummin linjata mitä eri tietoturvan osa-alueita kulloinkin tarkoitetaan.

Palvelumallit

Ei lausuttavaa

Toteutusmallit

Toteutusmalleja on tuotu hyvin esille sekä niiden jatkuvaa kehittymistä. Viimeinen kohta on kuitenkin merkityksellisin ja se voitaisiin nostaa suoraan linjaukseksi: "Minkä tahansa ICT-palvelun toteutusmallissa on otettava huomioon tietoturvaan, varautumiseen ja palvelun kriittisyyteen liittyvät tekijät ja tehtävä riskiarvio palvelun toteuttamisesta eri malleissa kustannusvaikutuksineen."

Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Tekstissä esitetään liian suoria yleistyksiä vain yhden kriteerin perusteella esimerkiksi julkiseksi luokiteltavan tiedon osalta mainitaan sitä voitavan lähtökohtaisesti käsitellä vapaasti sijainnista ja hallinnasta riippumatta. Tiedon käsittelyä ja hallintaa arvioitaessa tulisi lähtökohtaisesti ottaa huomioon kaikki palveluun vaikuttavat tekijät tiedon suojaamisen ja varautumisen kannalta.

Tiedon käsittelyn vaatimukset

Tietoturvan tarkoituksena on mainittuna olevan mm. järjestelmien tarkoituksenmukaisen käytettävyyden varmistaminen sekä rekisteröidyn oikeuksien toteutuminen. Näiden esittäminen tietoturvan tarkoitukseksi kaipaasi lisäperusteluja. Termien osalta olisi selkeintä ja yhdenmukaisinta käyttää kaikissa kohdissa yhtä ja samaa kotimaista kieltä. Autentikointi on tekstissäkin mainittu olevan todennus. Tietojen luokittelu kohdassa on erinomaisesti tuotu esille (vaikkakin epäselvästi ilmaistuna) organisaation tarve arvioida palvelun kriittisyys ja tärkeys yhteiskunnan, organisaation ja sen mahdollisten asiakkaiden näkökulmasta ja tämän perusteella varmistaa palvelun ja oman toimintansa jatkuvuus esimerkiksi valmius-, varautumis- ja toipumissuunnitelmin. Tämän voisi kokonaisuuteen nostaa selkeämmin esille vaikka

linjaustasolle yleisesti arvioitavaksi eri vaihtoehtoja vertailtaessa.

#### Palveluiden ohjaus

Neuvotteluasemaan liittyvä riskikappale vaikuttaa keskeneräisesti kirjoitetulta ja kaipaisi selventämistä.

#### Haasteet

Pilvipalveluiden haasteena on tässä kohdassa esitetty tietoturvan toteutuminen tiedon sijainnista ja hallinnasta riippuen, mutta esimerkiksi yhteenvedossa ja pilvipalveluteknologioiden edut kappaleessa mainitaan päinvastoin tietoturvallisuus pilvipalveluille ominaiseksi eduksi ja palvelun käyttäjän näkökulmasta pieneneväksi osaamistarpeeksi.

Seuraava virke kaipaisi selventämistä, koska sen perusteella tietoturvan tasoon liittyvät riskit ovat suuremmat Suomessa kuin muualla eivätkä maantieteelliset sijainnit vastaa täysin dokumentissa mainittuja: "Tiedon ja palveluiden sijaitessa EU:n tai ETA:n alueella, tai sen ulkopuolella, riski tietoturvan tasosta laskee erityisesti koskien kyseistä palveluntarjoajaa ja maata koskevan lainsäädännön johdosta sekä tietoliikenteen osalta esimerkiksi tiedon saatavuuden osalta." Huomioitavaa on, että Suomessa on erittäin hyvä tietoliikenneinfrastruktuuri joka luo hyvän perustan tietoturvalle palveluille ja tiedonhallinnalle. Lisäksi tietoliikenteen valvonta ja havainnointikyky ovat korkealla tasolla verrattuna yleisesti muihin EU maihin.

#### Linjaukset julkisen hallinnon tiedon sijainnista ja hallinnasta

1. Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta. Pilvipalvelu on vain yksi mahdollinen palvelumalli ja samat huomiot tietosuojaan, tietoturvaan, varautumiseen, riskienhallintaan, markkinakartoitukseen ja neuvotteluasemaan pitäisi tehdä hankinnan valmisteluvaiheessa riippumatta palvelumallista. Linjauksen tekstiosuudesta välittyy helposti mielikuva, että näihin kohtiin ei tarvitse kiinnittää erityistä huomiota muissa palvelumalleissa.



2. Tiedon sijaitessa Suomen rajojen ulkopuolella erityisesti on kiinnitettävä huomiota sopimukseen, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen. Vastaavasti kuin ensimmäisessä kohdassa palvelun hankkijalla tulisi olla suunnitelma palvelutason säilyttämisestä tarvittavalla tasolla myös häiriötilanteissa riippumatta tiedon maantieteellisestä sijainnista. Viimeinen kappale kaipaisi selventämistä ja tarkentamista varsinkin yhteiskäyttötapausten osalta.
3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset. Termit ja teksti tulisi selkiyttää sekä muuttaa linjaus muotoon minkä tahansa palvelun tulee täyttää...
4. Mikäli pilvipalvelut tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita. Pilvipalvelu on vain yksi vaihtoehto ja perusteita sen ensisijaisuudelle muihin vaihtoehtoihin ei ole tuotu esille. Linjaus tulisi poistaa tai muuttaa muotoon: ICT-palveluita hankittaessa tulisi palvelu- ja toteutusmalleista valita tietoturva ja varautuminen huomioiden kustannustehokkain ratkaisu, joka täyttää palvelutarpeen.
5. Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti vähintään kerran vuodessa ja oleellisten sopimusehtojen muuttuessa. Palvelun hankkijalta edellytetään jatkuvaa seuranta sopimusehtojen tilanteesta, mikä osaltaan on huomioitava resursoinnin, osaamistarpeen ja kustannusten osalta.
6. Viranomaisen ylläpitää listaa hyväksytyistä palveluntarjoajista. Viranomaista ei ole määritelty, palveluntarjoajien arviointi on jatkuvaa työtä ja näidenkin osalta käytännöt muuttuvat jatkuvasti, joten tämän linjauksen toteuttaminen käytännössä tulisi ensin varmistaa.
7. Julkisen tiedon käsittelyä ei rajoiteta. Itsestään selvä yleistys, jossa tulee huomioida kuten kaiken tiedon osalta kriittisyys ja muu tärkeys, varautuminen. Esitetään poistettavaksi tämä linjaus.
8. Henkilötietoa ja suojaustason IV tietoa voi käsitellä julkisessa pilvessä, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu. Tämä on enemmänkin tavoite kuin linjaus. Tietoturva ja -suoja sekä varautumisvaatimukset

kultakin suojauksen ja varautumisen tasolta määrittävät ensisijaisesti missä tietoa voi käsitellä. Palvelumallit, jotka täyttävät nämä vaatimukset tulisi ottaa huomioon arvioitaessa parhaiten sopivaa palvelumallia. Lisäksi viimeinen kohta EU/ETA-alueen ulkopuolella muista kuin henkilötiedon käsittelyn ja hallinnan osalta vaadittavista edellytyksistä pitäisi tarkentaa muotoon, josta käy ilmi keneltä vaaditaan ja kuka vaatii.

9. Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa. Viranomaista ei ole määritelty. Tekstissä mainittu: "Palvelun on täytettävä tiedon käsittelylle asetetut vaatimukset samalla tavalla kuin muiden toteutusmallien". Tämä on pääsanoma palveluvaatimuksille ja sen voisi nostaa suoraan linjaukseksi: Valittavan palvelumallin on täytettävä tiedon käsittelylle asetetut vaatimukset riippumatta toteutusmallista.

Tietohallintojohtajan sijaisena,  
johtava asiantuntija  
Minna Bloigu

Johtava asiantuntija Ismo Parviainen

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Sisäministeriö 07.09.2018 klo 08:05. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Parviainen Ismo  
Sisäministeriö