

Asia: VN/15936/2023

Luonnos hallituksen esitykseksi valtion yhteisten tieto- ja viestintätekniisten palvelujen järjestämisestä annetun lain ja valtion virkamieslain 7 §:n muuttamisesta

Lausunnonantajan lausunto

1. Yleisiä huomioita esityksestä

Maanmittauslaitos kiittää mahdollisuudesta lausua Valtiovarainministeriön lausuntopyyntöön luonnoksesta hallituksen esitykseksi valtion yhteisten tieto- ja viestintätekniisten palvelujen järjestämisestä annetun lain ja valtion virkamieslain 7 §:n muuttamisesta. Maanmittauslaitos lausuu asiassa seuraavaa.

Maanmittauslaitoksella ei ole kommentoitavaa.

2. Yhteiset palvelut

- **Kommentit 2 §:n muuttamisesta**

Maanmittauslaitoksen näkemyksen mukaan palvelun tuottamiseen liittyvä tietoturvallisuuden huomioiminen lainsäädännöllisestä näkökulmasta on hyvä asia. Poikkeamien tarkastelussa on tarve hyödyntää lokitietoja tapahtuman todentamiseen toimialasidonnaisten tietojärjestelmien ja perustietotekniikan Tori-palveluiden audit trail -ketjujen kautta. Tori-palveluiden ja toimialasidonnaisten tietojärjestelmien lokien yhteensovittaminen ja saatavuus tulee mahdollistaa siten, että lokeja voidaan hyödyntää viiveettä selvitystyössä.

Asiakas voi nykyisin tuottaa itse tai hankkia joltakin muulta palveluntarjoajalta kuin palvelukeskukselta tietoturva-, valvonta- ja lokienhallintapalveluita. Jos asiakkaalle tulee jatkossa velvoite käyttää vain palvelukeskuksen tarjoamia tietoturva-, valvonta- ja lokienhallintapalveluita, tulee kuvata menettelyt ja siirtymäajat palveluiden käyttöönotolle. Palvelukeskuksen palveluiden käytön velvoittavuus ei saa johtaa siihen, että lokitietoja ei voida yhteensovittaa tai niitä ei voida

kerätä. Siltä osin kuin asiakas joutuu toimialasidonnaisessa toiminnassa toteuttamaan itse palveluita, pitää olla mahdollista ratkaista käytön velvoittavuus asiakkaalle toiminta- ja kustannustehokkaasti. Palvelukeskuksen palvelut tulisi voida nykyistä paremmin integroida osaksi toimialasidonnaisia palveluita, jolloin alusta olisi aidosti toimialariippumaton.

3. Yhteisten palvelujen rekisterinpitäjät

- **Kommentit uuden 2 a §:n lisäämisestä**

Maanmittauslaitos kannattaa muutoksia ehdotetuista valtion yhteisten tieto- ja viestintäteknisten palvelujen tiedonhallinnan ohjauksista ja yhteisten palvelujen rekisterinpitäjä- ja tiedonhallintavastuista. Niiden toivotaan tuovan asiakkaiden ja palvelukeskuksen osalta yhtenäisyyttä.

Ehdotuksessa rekisterinpitäjä olisi se organisaatio, joka lakisääteisten tehtäviensä hoitamisen yhteydessä käsittelee henkilötietoja valtion yhteisissä tieto- ja viestintäteknisissä palveluissa. Palvelukeskuksen tulee palveluiden käyttöönottopäätösprosessin yhteydessä määrittää, onko rekisterinpitovastuu asiakkaalla vai palvelukeskuksella. Maanmittauslaitoksen mielestä asiakkaiden (Asiakasneuvottelukunta ANK, Tori-kokonaisturvallisuuden yhteistyöryhmä TORI KT) tulisi ottaa kantaa asiaan ennen prosessin loppuun saattamista. Esityksestä jää epäselväksi, miten tullaan määrittelemään rekisterinpitäjä, jos on olemassa sellaisia tapauksia, joissa kumpikin osapuoli hoitaa lakisääteisiä tehtäviä tai kumpikaan osapuoli ei hoida lakisääteisiä tehtäviä.

Rekisterinpidon osalta tulee varmistaa, että eri asiakkaiden kohdalla päädytään samanlaisiin ratkaisuihin. Palvelukeskuksen rekisterinpitäjäyys ei saa estää asiakasta saamasta tarvitsemiaan tietoja esim. lokitietoja loppuasiakkaan pyytäessä omia tietojaan tai tietoturvapoikkeaman selvittelyn yhteydessä. Maanmittauslaitoksen kokemuksen perusteella asiakkaalla ei ole nykyään mahdollisuutta vaikuttaa rekisterinpitäjän vastuisiin (tietojen suojaamiseen riittävän teknisin ja organisatorisin keinoin) yhteisissä palveluissa, vaikka asiakas toimiikin rekisterinpitäjänä. Rekisterinpitäjäyydestä tulisi linjata niin, että se määritellään aina ja molemmat osapuolet ovat asiasta tietoisia.

Maanmittauslaitos esittää, että ehdotetun 2a §:n osalta pyrittäisiin välttämään yhteisrekisterinpitäjäyyttä. Yhteisrekisterinpitäjäyyden kannalta asiakkaan rekisterinpitäjäyys koskisi asiakkaan lakisääteisten tehtävien hoitamiseksi kerättyjä henkilötietoja. Palvelukeskuksen erillinen rekisterinpitäjäyys sen sijaan koskisi kaikkia teknisen toiminnan varmistamiseksi käsiteltäviä henkilötietoja erikseen. Kumpikin osapuoli määrittäisi tarkoitukset ja keinot itsenäisesti. Tarkoituksen voinee katsoa olevan kummallakin erilainen. Toiminnan tulisi olla mahdollisimman yhtenäistä kaikilla valtionhallinnon asiakkailla. Asia tulee kirjata täsmällisesti asiakkaan ja palvelukeskuksen väliseen sopimukseen tai sen liitteisiin (missä palveluissa ja mitkä tiedot).

Yhteiskäyttöisten järjestelmien osalta keskeinen komponentti henkilötietojen hallinnassa on käyttäjähallinta eli AD, jonka yhteisrekisterinpitäisyys tulee olemaan vaikeaa nykyisten yhteensovitushaasteiden takia.

4. Yhteisten palvelujen käyttöönoton ja liittämisen hyväksyminen

- **Kommentit uuden 7 §:n lisäämisestä**

Maanmittauslaitoksen näkemyksen mukaan tässä kohdassa mainitun 2 §:n osalta tarvitaan tarkennusta, miten vaatimukset tulee toteuttaa. Ehdotuksesta jää epäselväksi täytyykö asiakkaan toimialasidonnaisten palveluiden osalta käyttää palvelukeskuksen monitorointi- ja lokipalveluita vai saako ne hoitaa asiakkaan omilla ratkaisuilla. Jää myös epäselväksi riittääkö selvitys lainmukaisten vaatimusten täyttymisestä vai vaaditaanko niiden osalta myös palvelukeskuksen hyväksyntä ratkaisun käyttöönottamiselle.

Ehdotettu nykytilaa selkeämpi vaatimustenmukaisuuden osoittamisvelvollisuudesta säättäminen lisäävät yhtenäisyyttä ja turvallisuutta, vaikka aiheuttavatkin asiakkaiden käyttöönottoprosesseihin muutoksia ja täsmennyksiä, jos näiden ratkaisujen osalta edellytetään jatkossa palvelukeskuksen hyväksyntää. Vaatimuksenmukaisuuden todentamiseen liittyvä dokumentaatio tai muu vaadittava selvitys tulisi määritellä niin, että se vaatisi mahdollisimman vähän normaalista tietojärjestelmien dokumentaatiosta erillistä ja siten ylimääräistä työtä aiheuttavaa selvitysmateriaalia.

Perusteluissa on arvioitu, että vaatimuksenmukaisuuden todentaminen ei synnyttäisi merkittävää työpanosta. Maanmittauslaitoksen kaltainen toimija, joka on tuottanut merkittävän osan tietojärjestelmäkannastaan itse, voi joutua tekemään merkittäviä toimenpiteitä vaatimustenmukaisuuden osoittamiseksi. Toimenpiteiden yhteydessä saatetaan joutua uudistamaan merkittävästi myös koko tietojärjestelmäarkkitehtuuria. Työpanos voi näin ollen olla huomattava. Esityksestä jää epäselväksi, miten palvelu varmistetaan, jos sitä ei saada tuottaa nykyisessä ympäristössä.

Maanmittauslaitos esittää, että laissa voisi mainita valtiovarainministeriön edellyttämät Tori-vähimmäisvaatimukset palveluun liittämiseen hyväksymiselle, jotka sitovat sekä palvelukeskusta että asiakasta. Liittymisessä tulee huomioida myös korjaussuunnitelma, jos asiakkaan palvelut eivät ole liittämisen hetkellä vaaditulla turvallisuustasolla. Esityksestä jää epäselväksi, mitä tapahtuu, jos asiakas ei perustelluista syistä yllä Tori-vähimmäisvaatimusten tasolle ja palvelukeskus kieltäytyy hyväksymästä palvelun liittämistä. Hankkiiko tällöin asiakas kyseisen palvelun itse muualta kuin palvelukeskukselta? Maanmittauslaitoksen kokemuksen mukaan esimerkiksi EU:n jäsenvaltioiltaan vaatimat ja näille toteuttamat palvelut ovat tietoturvaltaan heikkoja. Esityksestä ei myöskään selviä, onko palvelukeskuksella velvollisuus tarjota Tori-vähimmäisvaatimukset ylittävää palvelutasoa, jos asiakas sitä tarvitsee.

Maanmittauslaitoksen näkemyksen mukaan palvelukeskuksen vastuulla olevan nykyisen toimialasidonnaisen palvelutuotannon osalta voitaisiin

joustaa asiakkaan vähimmäisvaatimusten osoittamisvelvoitteesta ja ulottaa vaatimus vain uusiin käyttöönotettaviin palveluihin. Säännöskohtaisissa perusteluissa (torilaki 7§, 1. mom) on tärkeä maininta siitä, että "Ehdotettava sääntelytapa mahdollistaisi palvelun käyttöönoton hyväksymisen määräaikaisena riskiarvioon perustuen, vaikka kaikki vaatimukset eivät täytyisikään kaikilta osin.", koska tämä lisää käyttöönottojen joustavuutta. Joustoa ja kustannussäästöä saataisiin siitä, käytetäänkö resursseja vaatimustenmukaisuuden korjaustoimenpiteisiin vai järjestelmien uusimiseen elinkaaren täytyessä.

Yhteiset palvelut voivat parhaimmillaan tuottaa suuria kustannussäästöjä ja synenergiaetuja huomioiden kuitenkin palveluvaatimusten yhdenmukaisuus ja säästämisvelvoitteet.

Maanmittauslaitoksen mielestä on huolehdittava, että asiakkaalla on mahdollisuus saada perusteltuja lisäpalveluita tai muuten varmistettava, että yhteiset palvelut eivät heikennä asiakkaan kykyä tuottaa omaa palveluaan. Yleensä tällaisissa on kyse toimialasidonnaisesta palvelutarpeesta. Toimialasidonnaisia palveluita ei saa alkaa kutsua toimialariippumattomiksi taloudellisten seikkojen perusteella.

5. Valtion yhteisiä perustietotekniikka- ja tietojärjestelmäpalveluja tuottavan palvelukeskuksen toimitusjohtaja

- **Kommentit uuden 8 §:n 2 momentin lisäämisestä**

Maanmittauslaitoksella ei ole kommentoitavaa.

6. Valtion yhteisiä perustietotekniikka- ja tietojärjestelmäpalveluja tuottavan palvelukeskuksen henkilöstö

- **Kommentit 9 §:n muuttamisesta**

Maanmittauslaitoksen näkemyksen mukaan ehdotus tuo joustoa palvelussuhteen laatuun ja selkiyttää julkisen vallan käyttöön liittyvää virkavastuuta. Perusteluissa viitataan, että Maanmittauslaitoksessa jo toimitaan ehdotetulla tavalla, mikä on Maanmittauslaitoksessa koettu hyväksi toimintatavaksi.

7. Valtion yhteisiä perustietotekniikka- ja tietojärjestelmäpalveluja tuottavan palvelukeskuksen asiakkaat

- **Kommentit uuden 10 §:n 2 momentin lisäämisestä**

Maanmittauslaitoksen näkemyksen mukaan lain täydennysesitys vahvistaa jo olemassa olevaa yleistä toimintatapaa asiakkaan ja palvelukeskuksen välillä. Epäkohtana mainittakoon, että valtion liikelaitokset, eivät välttämättä pääse palvelukeskuksen asiakkaiksi, vaikka sitä haluaisivat.

Toinen epäkohta on, että Maanmittauslaitoksen kokemuksen perusteella nykyisten palvelukeskuksen asiakkaiden sopimusten kilpailutukset on aloitettu liian myöhään, jolloin on jouduttu sopimuksettomaan tilaan. Näistä tilanteista ei saa tulla asiakkaalle lisää vastuuta vaan yleisen periaatteen tulee olla, että kilpailutukset tehdään ajallaan. Asiakkaalle ei saa myöskään syntyä uusia velvoitteita tai työtä siksi, että palveluntuottaja ei kykene sopimustilanteen vuoksi hoitamaan tehtäviään. Asiakkaalla ei ole välttämättä osaamista eikä resursseja hoitaa palvelukeskukselle kuuluvia tehtäviä. Huomiona, että turvallisuuteen liittyvä yleinen huolellisuus- ja turvallisuusvelvoite on olemassa jo muun lainsäädännön kautta.

8. Integraatiopalvelujen tuottaja ja sen tehtävät

- **Kommentit uusien 13 § ja 14 §:n lisäämisestä**

Lainsäädännön toimeenpanoon tarkoitetut räätälöidyt tietojärjestelmät ovat kokonaisarkkitehtuurin mallin mukaisesti integroitu keskenään sekä virastokohtaisesti että laajemmin mm. perusrekisteriviranomaisten osalta toiminnoittain. Integraatioiden kehitys ja niihin liittyvä ylläpito liittyvät toimialasidonnaisiin ratkaisuihin. Lainsäädännössä näitä tehtäviä ei voi osoittaa toimialariippumattomiksi palveluiksi. Palvelukeskus ei ole kykenevä tarjoamaan integraatiopalveluita asiakkaan toimialasidonnaisten palveluiden välillä, tai ainakaan asiakasta ei pidä pakottaa käyttämään tällaisia palveluita.

Integraatioyhteydet valtion yhteisiin tietojärjestelmiin on tarkoituksen mukaista järjestää palvelukeskuksen tarjoaman yhteisen ratkaisun ns. hubin avulla (tällä hetkellä VIA-palveluväylä). Sitä käytetään tiedonsiirtoon viraston omien ja valtion yhteisten järjestelmien sekä eri virastojen välillä (esimerkiksi Maanmittauslaitos ja Ulosottovirasto). Esityksestä jää epäselväksi, mikä on suomi.fi-palveluväylän ja siihen liittyvän KAPA-lakiin kirjoitetun velvoittavuuden suhde kuvattuihin integraatioihin.

VIA-palveluväylä on jo toimiva ratkaisu valtiohallinnon yhteisten palveluiden palveluväylänä. Palveluväylät ja integraatiot ovat tyypillisesti B-to-B -ratkaisuja, joiden tekninen toteuttaminen vaatii datamäärien ja prosessointikapasiteetin huomioimisen palveluiden sijoittelussa ja kustannuksissa. Liika sääntely vaikeuttaa palvelun tuottamista tai kustannustehokkuutta.

9. Varautuminen ja palvelutuotannon häiriötilanteet

- **Kommentit uusien 15 §:n 3 ja 4 momentin lisäämisestä**

Toimialasidonnaiset palvelut ovat tärkeä osa yhteiskunnan toimivuutta kriisitilanteessa. Maanmittauslaitoksen näkemyksen mukaan esitys mahdollistaisi yhteisten palveluiden priorisoinnin korkeammalle kuin todella kriittisen toimialasidonnaisen palvelun toimivuuden.

Palveluiden toimivuus tulee varmistaa kaikissa tilanteissa siten, että lähtökohtaisesti miehitys riittää turvaamaan varautumisen ja palvelutuotannon häiriötilanteet. Tämä toteutuu varmimmin, kun myös poikkeustilanteissa noudatetaan mahdollisuuksien mukaan normaalipalveluiden käytäntöjä, mikä on huomioitava esimerkiksi henkilövarauksissa. Tori-palvelut ovat keskeisiä, jotta asiakkaat kykenevät tuottamaan heitä koskevat varautumisvelvoitteet myös toimialasidonnaisten palveluiden osalta.

Esityksen tavoite palvelujen varmistamisesta on hyvä, mutta liian kevyt kuulemisvelvoitteen sivuutus kiireeseen vedoten lisää riskiä hallintatoimien aiheuttamista palvelukatkoista muille toimijoille. Tiedonhallintalaki velvoittaa virastoja huolehtimaan mm. sopimuksellisesti siitä, että heidän varautumisensa mukainen palvelutaso on turvattu. Maanmittauslaitoksen näkemyksen mukaan erityisen poikkeaman säätäminen lailla ei ole tarkoituksenmukaista.

Säädösehdotuksen viimeisen momentin tekstissä ”muussa”-sanalla pitänee olla ”muuta”: Palvelujen tuottajien alihankkijoiden on noudatettava palvelujen tuotannon ja käytön ensisijaisuus-, kiireellisyys- ja muussa tärkeysjärjittelyä suorittaessaan tämän lain mukaisia tehtäviä.

10. Esityksen vaikutukset organisaatiosi toimintaan

Asiakkaalta vaaditaan toimenpiteitä veloitteesta siirtyä käyttämään palvelukeskuksen tarjoamia tietoturva-, valvonta- ja lokienhallintapalveluita, jotka asiakas on hankkinut aikaisemmin itse. Esityksen velvoite vaatimuksen mukaisuuden osoittamisesta tulee vaatimaan Maanmittauslaitokselta huomattavasti resursseja, mikäli palvelukeskus vaatii kaikista toimialasidonnaisista järjestelmistä kattavaa dokumentointia ja ohjeistusta.

Palvelukeskuksen huomioiminen asiakkaan toimialasidonnaisten palveluiden käyttöönottoprosessissa aiheuttaa muutoksia niin käyttöönottoprosessiin kuin dokumentaatioonkin.

Maanmittauslaitoksen näkemyksen mukaan 15 §:n 3 ja 4 momentin lisääminen mahdollistaisi yhteisten palveluiden priorisoinnin korkeammalle kuin todella kriittisen toimialasidonnaisen palvelun toimivuuden.

11. Muut kommentit

Maanmittauslaitoksella todetaan, että valtion virkamieslain 7 §:n muuttaminen, jossa säädetään, että virkaan voidaan nimittää vain Suomen kansalainen, on linjassa Liikenne- ja viestintäviraston vastaavan säätelyn kanssa. Kansalaisuusvaatimus rajoittuu niihin virkoihin, joihin kuuluu tieto- ja kyberturvallisuuteen olennaisesti vaikuttavia tehtäviä. Maanmittauslaitoksessa vastaavia Suomen kansalaisuuden vaativia virkoja ovat valtion virkamieslain 7 §:n 1 momentin kohdassa 11 mainitut Maanmittauslaitoksen paikkatietokeskuksen ylijohtajan virka ja tuotantotoimintayksikön ylijohtajan virka.

Mikkonen Soile

Maanmittauslaitos - Pääjohtaja Pasi Patrikainen ja ylijohaja Petri Korpinen