Lausunto

06.09.2021 V/26048/2021

Asia: VN/4400/2021

Arviomuistio julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista

Lausuntonne arviomuistiosta

1. Kommenttinne arviomuistiossa tehdystä nykytilan kuvauksesta

Nykytilan kuvaus antaa hyvän yleiskuvan julkisen hallinnon tietojärjestelmien automaattista päätöksentekoa koskevan lainsäädännön hajanaisuudesta ja puutteellisuudesta. Nykytilan kuvaukseen olisi kuitenkin hyvä lisätä käytännön esimerkkejä haasteista, joita julkisen hallinnon tietojärjestelmien päätöksenteossa tällä hetkellä on. Näin lainsäädännölliset muutostarpeet tulisivat paremmin ymmärretyiksi ja perustelluiksi.

2. Kommenttinne tietojärjestelmistä sääntelykohteena

Valvira ei kannata nykyisessä tilanteessa tietojärjestelmien säätelyn lisäämistä yleislainsäädäntötasoisena julkisen hallinnon tietojärjestelmiä koskien. Valvira pitää ajankohdallisesti perustellumpana seurata Euroopan komission antaman ehdotuksen asetuksen harmonisoiduista säännöistä tekoälylle etenemistä voimassa olevaksi. Valvira pitää yleisluontoisesti Euroopan komission ehdotusta asetukseksi merkittäviltä osin onnistuneena.

Valvira pitää kuitenkin hyvänä myös yksittäisten olemassa olevien kansallisten tietojärjestelmiä koskevien lakien päivittämistä ja tarkentamista. Tällaisia ovat erityisesti tiedonhallintalaki ja arviointilaitoslaki. Muutoin Valvira näkee, että julkisen hallinnon tietojärjestelmiä koskevien teknologiariippumattomien vaatimusten määrittely kaikille toimialoille soveltuvaksi ja lisäarvoa tuottavaksi on erittäin haastavaa. Kokemuksemme mukaan toimialakohtaisten erityislainsäädännön alaisten vaatimustenkin teknologiariippumaton määrittely vaatimustenmukaisuuden arvioinnin ja valvonnan näkökulmasta on haastavaa. Tästä syystä Valvira näkee paremmaksi edellyttää

mahdollisia tarvittavia säädöksiä erityislainsäädäntötasoisesti toimialoittain kuin yleislain-säädäntötasoisesti kaikkia toimijoita koskien.

Hallinnon tietojärjestelmien säätelyn lisäämisen sijasta Valvira kannattaa enemmän käytännön tietojärjestelmien suunnittelutyössä, hankinnoissa, käyttöönotoissa ja käyttöönoton jälkeisissä vaiheissa tukevien kansallisten suositusten edistämistä. Valvira näkee paremmaksi esimerkiksi omaehtoista arviointia tukevat suositukset ja työkalut kuin lakiperusteisen säätelyn lisäämisen. Julkisen hallinnon tieto-järjestelmien suunnittelua ja hankintaa määrittelee jo nyt voimakkaasti lainsäädäntö ja katsomme lisääntyvän lainsäädännön lisäävän kohtuuttomasti entisestään haastavaa suunnittelu- ja hankintatyötä sekä edellyttävän mittavia henkilöresursseja ja taloudellisia resursseja.

3. Millaisia yleisiä vaatimuksia tietojärjestelmien toiminnallisuuksille pitäisi lainsäädännöllä asettaa?

Valvira katsoo, että yleisluontoisia eri toimialoille soveltuvia toiminnallisia vaatimuksia ei voida asettaa vaan vaatimukset tulee asettaa tarvittaessa erityislainsäädännöllä, kuten on asetettu asiakastietolaissa sosiaali- ja terveydenhuollon tietojärjestelmille. On myös huomioitava, että toiminnalliset vaatimukset tietojärjestelmille muodostuvat pääasi-assa substanssilainsäädännön kautta.

4. Millaisia olennaisia teknisiä vaatimuksia hallintoasioita käsitteleville tietojärjestelmille pitäisi lainsäädännöllä säätää?

Valvira kannattaa sääntelyn sijasta vaatimuksia koskevia suosituksia.

Tarvetta hallintoasioita käsittelevien tietojärjestelmien teknisille vaatimuksille tulisi arvioida kriittisesti. Korkeintaan tulisi harkita tietoturvavaatimuksia, jotka perustuvat järjestelmien luokitteluun tai riskiperusteisuuteen. Lisäksi tulisi kriittisesti arvioida mahdollisia yleisluontoisia suorituskykyvaatimuksia erityisesti tulevaa käyttöä ja tietojärjestelmähankintoja tukemaan.

5. Millaisia vaatimuksia, kuten dokumentointivaatimuksia, tietojärjestelmien kehittämiselle pitäisi lainsäädännöllä säätää?

Valvira kannattaa sääntelyn sijasta dokumentointia koskevia suosituksia. Pois lukien erityislainsäädännössä mahdollisesti edellytettävät dokumentointivaatimukset ja vaatimustenmukaisuuden osoittaminen (esimerkiksi asiakastietolaki ja toisiolaki).

6. Miten lainsäädännöllä tulisi varmistua virkavastuun toteutumisesta ja kohdistumisesta, mitä tulee tietojärjestelmien kehittämiseen, käyttöönottoon ja käyttöön, sekä tietovarantojen käyttöön?

On suositeltavaa, että vastuukysymyksiä selkeytettäisiin tilanteissa, joissa hallinnollinen päätös tehdään kokonaan automatisoidusti (mm. eräajot ja automatisoidut käsittelyprosessit). Tällaisia prosesseja on jo käytössä esimerkiksi etuuskäsittelyssä, ja olisi toivottavaa, että vastuukysymysten selvittäminen ei jäisi vain organisaation sisäiseksi asiaksi. Kuitenkin automatisaatiosta saatavat hyödyt ovat niin suuret, että vastuukysymysten ratkaisemisessa tulisi huomioida se, että ratkaisu ei hidasta automatisaation hyödyntämistä julkishallinnossa. Valvira katsoo, että virkavastuun kohdentaminen lainsäädännöllä on erittäin haasteellista arviomuistiossa kuvatuista käytännön haasteista johtuen.

7. Mitä edellytyksiä tietovarannoille, niiden laadulle tai niiden käytölle tulisi lainsäädännössä asettaa, jotta niitä voidaan käyttää osin tai täysin automaattisessa päätöksenteossa?

Sääntelyn sijasta Valvira kannattaa suosituksia tiedonlaadulle: laatukriteereille ja niihin liittyville tarkastus-, seuranta- ja korjausmenettelyille. Valvira näkee, että Tiedon hyödyntäminen ja avaaminen -hankkeessa alustavasti laaditut tiedon laatukriteerit voisivat olla lähtökohta suosituksen muodostamiselle

8. Miten tietoturvallisuuden arviointia ja arviointijärjestelmää koskevaa lainsäädäntöä tulisi kehittää? Entä erityisesti viranomaisten tietojärjestelmien arvioinnin osalta?

Valvira pitää tärkeänä sitä, että tietoturvallisuuden arviointi on ulkopuolisten arvioitsijoiden tehtävä, mutta Valvira esittää, että tietoturvallisuuden arviointia tai muuta vaatimustenmukaisuuden arviointia ei pohjattaisi Suomessa liiketoimintaa tekevien arviointilaitosten suorittamiin arviointeihin vaan toiminta pohjautuisi viranomaisten omaan arviointiin ja lisäksi riippumattoman viranomaistoimijan suorittamiin arviointeihin virkavastuullisena toimijana. Valviran näkemyksen mukaan ulkoisten kaupallisten arviointilaitosten arvioinneissa on ollut puutteita ja ongelmia, joskin osa ongelmista on johtunut epäselvyyksistä käytetyissä tietoturvallisuuden vaatimuskriteeristöissä. Valviran näkemyksen mukaan liiketoimintaa tekevien arviointilaitosten kaupallinen kilpailu ei ole toteutunut asiakastietolain mukaisissa arvioinneissa, ja tällä hetkellä käytännössä vain yksi tietoturvallisuuden arviointilaitos toimii markkinoilla pääasiallisena toimijana.

Mikäli nykyiseen ulkoisten arviointilaitosten malliin ei kuitenkaan tehdä muutoksia, arviointilaitoslakia tulisi tarkentaa erityisesti siltä osin, mitä vaaditaan, jotta arviointilaitosten kyvykkyys arviointeihin voidaan varmistaa. Käytännössä ulkoisilla kaupallisilla arviointilaitoksilla on ollut mm. puutteita erityislainsäädännön hallinnassa ja sen alaisten vaatimusten hallinnassa sekä vaatimustenmukaisuustodistuksen myöntämisen edellytyksissä. Valvira katsoo, että esimerkiksi asiakastietolain mukaisissa tietoturva-arvioinneissa ei ole saavutettu nykyisillä menettelytavoilla lain tavoitteita eivätkä tietoturva-auditoinnit ole tuottaneet sitä lisäarvoa, joka niiden lähtökohtaisesti olisi pitänyt tuottaa. Jotta ulkoiset auditoinnit toisivat toivottua lisäarvoa, tulisi arvioin-tilaitoksia ja niiden yksittäisiä arvioitsijoita koskevia vaatimuksia tarkentaa merkittävästi nykyisestä.

9. Kommenttinne muistiossa todetuista sääntelytarpeista yleensä

Kuten edellä on todettu, Valvira esittää monin osin sääntelyn sijasta suosituksia. Niissä tulisi korostaa keinoja, joilla mahdolliset automaat-tisesta päätöksenteosta johtuneet virheet korjataan niiden kohteiden oikeudellisten vaikutusten näkökulmasta sekä teknisellä ja/tai tiedon tasolla virheen lähteestä riippuen (juurisyyn korjaus).

10. Muut yleiset kommentit arviomuistiosta

Valvira pitää tärkeänä, että NIS-direktiivin toimeenpaneminen johdettaisiin toimialakohtaisesti kansalliseen lainsäädäntöön. Tämä on jäänyt toteuttamatta sosiaali- ja terveydenhuollon toimialalla. Valvira katsoo, että sosiaalihuollon lisäämistä CER-direktiivin alaiseksi toimialaksi tulisi arvioida, mikäli sitä ei ole aiemmin tehty. Sosiaalihuoltoon kuuluu elintärkeitä kriittisiä toimintoja kuten kotipalvelut ja kotihoito, asumispalvelut ja laitoshoito sekä lastensuojelu ja vammaispalvelut.

Luvussa 5.5. Tietojärjestelmien käyttöönotto (s. 21-22) todetaan, että käyttöönoton edellytys on ”vaatimustenmukaisuuden arviointi joko arviointilaitoksen tekemänä tai eräissä tapauksissa

itsearviointina.” Tie-toturvallisuuden arviointilaitoksen tekemä tietoturvallisuuden arviointi kattaa yhden kolmesta asiakastietolaissa edellytetystä olennaisesta vaatimuksesta. Ennen käyttöönottoa A-luokan tietojärjestelmän val-mistajan tulee selvittää, että järjestelmä täyttää kaikki toiminnallisuut-ta koskevat vaatimukset, sen tulee läpäistä hyväksytysti Kansanelä-kelaitoksen yhteistestaus (todentaa yhteentoimivuuden), jonka jälkeen järjestelmän tulee läpäistä hyväksytysti tietoturvallisuuden arvi-ointi. Tämän jälkeen järjestelmä rekisteröidään Valviran ylläpitämään rekisteriin, ja Valvira tarkastaa vaaditut asiakirjat ennen rekisteröintiä. Käyttöönoton edellytys A-luokassa ei siten ole vain tietoturvallisuuden arviointi. Sama huomio koskee myös lukua 9.1.7. (s. 73), jossa kerro-taan, että luokkaan A kuuluvan tietojärjestelmän saa ottaa tuotantokäyttöön, kun tietoturvallisuuden arviointilaitos on antanut sitä koskevan vaatimustenmukaisuustodistuksen.

Luvussa 9.2.1. (s. 74) lukee seuraavasti: ”Asiakastietolain mukainen arviointilain mukaan suoritettava arviointi ulottuu osittain myös muihin tietojärjestelmien olennaisten vaatimusten toteutumisen arviointiin.” Asiakastietolain mukaisia olennaisia vaatimuksia on kolme: toiminnalliset vaatimukset, yhteentoimivuus sekä tietoturva. Tietoturvallisuu-den arviointilaitos ei arvioi yhteentoimivuutta, vaan sen tekee Kansaneläkelaitos järjestämässään yhteistestauksessa. Lisäksi Kansaneläkelaitoksen yhteistestauksessa, joka tehdään ajallisesti ennen tie-toturvallisuuden arviointia, voi ilmetä myös puutteita toiminnallisissa vaatimuksissa, jotka tulee korjata ennen siirtymistä tietoturvallisuuden arviointiin. Koska toiminnalliset vaatimukset tulevat tyypillisesti sub-stanssilainsäädännöstä, jonka kautta ne johdetaan toiminnallisiin vaa-timuksiin, tietoturvallisuuden arviointilaitoksen osaaminen ei oletetta-vasti riittäisi olennaisten toiminnallisten vaatimusten arvioimiseen.

Henriksson Markus
Valvira

Kujala Ritva
Valvira