Terveyden ja hyvinvoinnin laitos THL

Lausunto

06.09.2021 THL/3794/4.00.02/2021

Asia: VN/4400/2021

Arviomuistio julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista

Lausuntonne arviomuistiosta

1. Kommenttinne arviomuistiossa tehdystä nykytilan kuvauksesta

Arviomuistiossa on kuvattu onnistuneesti nykytilaan johtaneita syitä ja nykyisen lainsäädännön sirpaleisuutta. Toiminnan haasteet on hyvin tunnistettu.

2. Kommenttinne tietojärjestelmistä sääntelykohteena

Kasvava tietojärjestelmien sääntely voi nostaa tietojärjestelmien kehitys- ja ylläpitokustannuksia.

Kasvava tietojärjestelmien sääntely voi vaikeuttaa valmisohjelmistojen käyttöä. Valmisohjelmistoja tuottavat kasvavassa määrin suuret kansainväliset toimijat jotka eivät välttämättä ole kiinnostuneita kansallisten erityisvaatimusten täyttämisestä. Tarkka kansallinen säätely voidaan tulkita kilpailun esteeksi.

Palvelutarpeisiin vastataan yhä enemmän pilvipalveluilla, joissa hankinta kohdistuu palveluun (mm. SaaS-malli) eikä tietojärjestelmään. Vaarana on, että tietojärjestelmiin kohdistuva sääntely joko estää tällaisten palvelujen hankinnan tai sitten jättää näin hankitut palvelut kokonaan sääntelyn ulkopuolelle.

Sosiaali- ja terveydenhuollon tietojärjestelmiä säädellään jo nyt runsaasti sekä kansainvälisten säädösten (mm. lääkintälaitedirektiivi ja -laki) että kansallisten säädösten (mm. asiakastietolaki) kautta. Kokonaisuutta on kuvattu lyhyesti mm. arviomuistion kohdassa 9.1.7.

Useimpiin lausuntopyynnössä esitettyihin kysymyksiin ja myös uusiin tietojärjestelmäpalvelujen tuottamismalleihin kuten pilvipalvelut on jo olemassa tai on tulossa erityisesti sosiaali- ja

terveydenhuollon toimintaympäristöön kehitettyjä tai sovellettuja malleja, jotka osin voivat olla joko suoraan samoja tai sovellettavissa myös julkiseen hallintoon. Keskeistä on kuitenkin välttää liiallista sääntelyä sellaisten seikkojen suhteen, joiden yhtenäistämiseen, rajoittamiseen tai turvaamiseen säädösten kautta ei kohdistu merkittävää tarvetta.

Sosiaali- ja terveydenhuollon tietojärjestelmäympäristöön kohdistuvassa sääntelyssä on huomioitu toimijakentän ja palvelujen moninaisuus, julkisten ja yksityisten toimijoiden ratkaisut sekä kotimaisten ja kansainvälisten tietojärjestelmämarkkinoiden kyvykkyyksien hyödyntäminen. Asiakastietolaissa säädetään mm. sosiaali- ja terveydenhuollon asiakastietojen käsittelyyn tarkoitettujen tietojärjestelmien luokittelusta, olennaisista vaatimuksista, sertifioinnista ja rekisteröinnistä. Lakiin perustuvat Terveyden ja hyvinvoinnin laitoksen antamat määräykset säätelevät tarkemmin eri käyttötarkoituksiin tarkoitetuilta tietojärjestelmiltä edellytettäviä vähimmäisvaatimuksia. Olennaisia tietojärjestelmiin kohdistuvia vaatimuksia asetetaan järjestelmien toiminnallisuudelle, yhteentoimivuudelle ja tietoturvallisuudelle. Lisäksi asiakastietolaissa ja määräyksissä säädetään käyttäjäorganisaatioiden (sote-palvelunantajat) tietoturvallisuuteen ja tietojärjestelmien käyttöön liittyvästä suunnitteluvelvoitteesta ja suunnitelman sisällöstä.

Sosiaali- ja terveydenhuollon tietojärjestelmäympäristössä säädökset asettavat merkittäviä vaatimuksia sekä tietojärjestelmien valmistajille että käyttäjäorganisaatioille, erityisesti liittyen tietoturvallisuuteen sekä valtakunnallisten tietojärjestelmäpalvelujen (Kanta-palvelut) käyttöön. Sekä yleis- että erityislainsäädännöstä nousevien vaatimusten täyttäminen ja niiden todentaminen aiheuttavat kustannuksia tietojärjestelmätoimittajille ja sote-organisaatioille. Sosiaali- ja terveydenhuollon tietojärjestelmien sertifioinnin lähtökohtana on tuotesertifiointi, jossa järjestelmän valmistajan sertifioitu ja/tai rekisteröity järjestelmä voidaan ottaa käyttöön eri sote-organisaatioissa. Sertifiointi ei siis kohdistu suoraan rekisterinpitäjänä tai tiedon käsittelijänä toimivaan sote-organisaatioon.

Moninaisiin sote-palveluja tuottaviin julkisiin ja yksityisiin organisaatioihin ei kohdistu pakollisia ulkoisen vaatimusten todentamisen velvoitteita, mutta niiden on suunniteltava toimintansa tietoturvallisesti ja käytettävä sertifioituja ja rekisteröityjä järjestelmiä. Sosiaali- ja terveydenhuollon tietojärjestelmien sääntely on edellyttänyt toimivaa tarkempiin määrittelyihin ja määräyksiin perustuvan ohjauksen organisointia, yhteentoimivuuden testauksen organisointia, tietoturvallisuuden auditoinnin organisointia, järjestelmien rekisteröinnin ja valvonnan uskottavaa järjestämistä, laajaa viranomais- ja sidosryhmäyhteistyötä sekä toimijoiden osaamistason varmistamista. Viranomaisten ohjaus-, todentamis-, rekisteröinti- ja valvontatoiminnan riittävästä resursoinnista on huolehdittava. Sosiaali- ja terveydenhuollossa keskeisiä viranomaistoimijoita tältä osin ovat STM, THL, Kela, Valvira, Fimea ja Traficom.

3. Millaisia yleisiä vaatimuksia tietojärjestelmien toiminnallisuuksille pitäisi lainsäädännöllä asettaa?

Yksityiskohtaisten vaatimusten asettaminen tietojärjestelmille ja niiden testaamiselle sekä verifioimiselle ei ole välttämättä tarkoituksenmukaista muun muassa sen vuoksi, että teknologiat kehittyvät ja muuttuvat nopeasti ja siten muuttuvat myös testaamisen ja verifioinnin menettelyt. Myös tietojärjestelmien käyttötarkoitus vaikuttaa siihen, mitkä verifiointimenetelmät ovat ylipäätään tarpeellisia. Lainsäädännöllisesti onkin riittävää vaatia, että tietojärjestelmän on

toimittava joka hetki sille asetettujen vaatimusten mukaisesti siten, että viranomaisen tuottama palvelu ja tiedot eivät vaarannu.

Sääntelyä voitaisiin suunnata niin, että se asettaisi yleiset raamit niille palveluille ja tiedoille, jotka pitäisi olla aina käytössä, erotuksena niihin palveluihin ja tietoihin, joiden häiriötilanteessa riittää että informoidaan käyttäjiä häiriöstä.

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

Teknisten vaatimusten tuominen lainsäädäntöön aiheuttaisi helposti lain jäämisen kehityksestä jälkeen ja siten jatkuvaa lain päivittämisen tarvetta. Tämän vuoksi lainsäädännön tasolla on syytä pitäytyä pääasiassa toiminnallisissa vaatimuksissa. Vaatimukset on asetettava ensisijaisesti palvelun tasolle ja saatavuudelle, ei niille keinoille joilla näihin päästään.

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

Tietojärjestelmien teknologien sääntelyä kestävämpi tie on säädellä prosessin alkupäätä eli hankintaprosessia, tai jos tietojärjestelmä kehitetään itse, kehitysprosessia.

Kehittämiseen, käyttöönottoon ja hankintaan voitaisiin lainsäädännössä vaatia tietty dokumentaatio, koska sellainen on laadukkaasti toimittaessa tuotettava jo ilman lainsäädäntöäkin. Sellaisista tietojärjestelmistä, jotka kehitetään itse tai joiden kehitys ostetaan toimittajalta, pitäisi edellyttää riittävät tiedot mm. käyttötarkoitustarkoituksen, käytön, arkkitehtuurin ja jatkokehityksen kannalta.

Sääntelyn tulisi huomioida myös valmisohjelmistojen osittainen räätälöinti ja sen dokumentoiminen.

Useilla tietojärjestelmillä on ulkomainen toimittaja ja tuotekehitys tehdään ulkomailla, vaikka toimittajalla suomalainen edustaja tai paikallisorganisaatio olisikin. Suomalainen toimittaja voi myös päätyä yritysjärjestelyjen kautta ulkomaisen päämiehen omistukseen. Tämän vuoksi tietojärjestelmän hankintayksikön voisi olla hyödyllistä laatia hankintavaiheen dokumentaatio englanniksi. Jos näin ei tehdä, ulkomainen toimittaja käännättää dokumentaation itse, usein nopealla aikataululla ja asiaa tuntemattomalla kääntäjällä. Virkavastuun kohdentaminen helpottuu, hankinta nopeutuu ja hankintavaiheen laatu paranee, kun dokumentaatio on molemmin puolin ymmärrettävää.

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

Lainsäädännössä on mahdollista kirkastaa virkavastuun laajuus ja merkitys tietojärjestelmien osalta.

Tietojärjestelmien kehityksen osalta vastuullinen voisi olla projektipäällikkö, käytön osalta taas järjestelmän tai tietovarannon nimetty omistaja. Keskeistä on, että se mitä vastuu tarkoittaa, on täysin selvä, ja että vastuulliselle henkilölle kerrotaan hänen olevan virkavastuussa.

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

Automaattista päätöksentekoa tulisi edistää myös lainsäädännöllisin keinoin, koska samanaikaisesti viranomaisia velvoitetaan kehittämään digitaalisia asiointipalveluja (mm. hallitusohjelma, digipalvelulaki). Tästä syystä tietojärjestelmille ja tietovarannoille lainsäädännössä asetettavat määräykset eivät saisi olla ristiriidassa muun lainsäädännön, kuten digitalisaatiota ja asiointia edistävien säädösten ja linjausten, kanssa.

Automaattisessa päätöksenteossa korostuu tietovarantojen, tietojärjestelmien ja prosessien laatu. Automaattisessa päätöksenteossa kerättävien tai käytettävien tietojen tulee olla riittävän varmasti oikein. Tällöin myös tietojen antajan rooli korostuu. Ymmärrys annetuista tiedoista ja niiden laatutasosta tulee olla selvä. Tietojen laatuun pitäisi kohdistaa jatkuvan laadunhallinnan lisäksi sekä säännöllisiä että satunnaisia tarkastuksia, jotta voitaisiin varmistua niiden luotettavuudesta.

Kopiorekisterit ovat tiedon ajantasaisuuden kannalta haaste. Tiedon huollon prosessein tulisi varmistaa tietojen ajantasaisuus kopiorekistereissä.

Sekä automaattisessa päätöksenteossa käytettävä data että itse päätöksenteon prosessi tulisi mahdollisuuksien mukaan avata. Silloin kuin päätöksenteko kohdistuu henkilöön, henkilöllä tulisi ideaalitilanteessa olla mahdollisuus tarkastaa yhdessä paikassa kaikki häntä koskevat päätöksentekoon käytetyt tiedot ja nähdä päätöksenteon prosessi.

Kun tekoälyä käytetään päätöksenteossa, julkisen vallan käyttö saattaa siirtyä ainakin osittain tietojärjestelmälle ja sen toimittajalle.

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

Arviointilaitosten osaaminen tulee varmistaa siten, että arvioijat tuntevat arvioinnin pohjana käytettävät säädökset, arvioitavaa kohdetta koskevat vaatimukset ja että arvioinneissa on riittävä ymmärrys arvioitavan kohteen toiminnasta ja toimintaympäristöstä. Sosiaali- ja terveydenhuollosta saatujen kokemusten mukaan tietoturvallisuuden arviointilaitoksilla ei esimerkiksi nykyisellään ole aitoja edellytyksiä arvioida sosiaali- ja terveydenhuollon tietojärjestelmien yhteentoimivuutta tai järjestelmien käyttötarkoituksen näkökulmasta niihin kohdistuvien toiminnallisten vaatimusten oikeellista toteuttamista laajassa tietojärjestelmäkokonaisuudessa.

Arviointilaitosten roolia on asiakastietolain uudistuksessa edelleen selkiytetty keskittymään vain tietoturvallisuuteen, mutta myös tähän liittyvien säädösten ja kriteerien yksityiskohtaisessa tuntemuksessa on havaittu parannettavaa.

Sosiaali- ja terveydenhuollon tietojärjestelmiin kohdistuvien toiminnallisten vaatimusten ulkoista arviointia ei ole säädösten nojalla edellytetty eikä organisoitu Suomessa, vaan niiden täyttämisestä vastaa tietojärjestelmäpalvelun tuottaja.

Sosiaali- ja terveydenhuollon tietojärjestelmätuotteiden sertifiointiin kuuluu Kansaneläkelaitoksen kanssa suoritettava yhteistestaus Kanta-palveluihin liittyville järjestelmille ja/tai hyväksytyn arviointilaitoksen suorittama tietoturvallisuusvaatimusten arviointi. Yhteistestaus nojautuu tarkkoihin Kelan ja THL:n tuottamiin rajapinta- ja yhteentoimivuusmäärittelyihin. Tietoturva-auditointi nojautuu THL:n määräyksen kautta asetettuihin kriteereihin. Vain pieni osa tietoturva-auditoinnissa ja yhteentoimivuustestauksessa todennettavista vaatimuksista linkittyy järjestelmiltä edellytettäviin toiminnallisiin vaatimuksiin. Yhteentoimivuuden todentaminen raskaalla yhteistestausmenettelyllä on nähty tarpeelliseksi sosiaali- ja terveydenhuollossa, jotta asiakas- ja potilastietojen saatavuus, säilyttäminen ja hyödyntäminen laajan palveluntuottajakirjon toimijoiden välillä lukuisia eri tietojärjestelmätuotteita käyttäen pystytään riittävällä tasolla varmistamaan. Julkisen hallinnon virastokohtaisiin tai keskitettyihin palveluihin ja järjestelmiin perustuvassa tiedonhallinnassa asetelma ja tarpeet poikkeavat merkittävästi näistä lähtökohdista.

9. Kommenttinne muistiossa todetuista sääntelytarpeista yleensä

Palvelun mahdollistavien tietojärjestelmien sääntelyn sijaan hyödyllisempää on kiinnittää huomio palvelun käyttäjän saaman palvelun toteutumiseen ja palvelun laatuun. Jos sääntelyssä mennään teknisiin yksityiskohtiin, sääntelyn noudattaminen ei onnistu tai se vaikeutuu, kun huomio siirtyy palvelusta toteutusratkaisuihin, käyttäjistä järjestelmätoimittajiin.

Vaatimusten voimaantulon määräajoissa on pystyttävä huomioimaan se, että laajan tietojärjestelmäkokonaisuuden uudistaminen vie useita vuosia. Vaatimusten toimeenpanon aikataulut tulisi sallia liitettäväksi järjestelmien muutenkin tapahtuvan uusimisen ja päivittämisen rytmiin ylimääräisten kustannusten ja organisaatioiden perustoiminnalle koituvien häiriöiden vähentämiseksi.

Mikäli sääntelyä lisätään ja tarkennetaan, on erityisesti huolehdittava siitä, että julkisille sote-palvelujen järjestäjille ja tuottajille ei luoda päällekkäisiä arviointi- tai todentamismenettelyjä nykyisten erityislainsäädännöstä kuten asiakastietolaista nousevien velvoitteiden ja menettelyjen lisäksi.

Sosiaali- ja terveydenhuollosta saatujen kokemusten mukaan yleisiä säädöksiä tarkemmat kriteerit ja riittävän yksiselitteisesti tulkittavat vaatimukset ovat välttämättömiä toimivan arviointikokonaisuuden aikaansaamiseksi. Määräysten ja määrittelyjen soveltamisala on kuitenkin

pystyttävä rajaamaan vain niihin käyttökohteisiin, joihin ne on nimenomaisesti tarkoitettu. Esimerkiksi suun terveydenhuollon graafisia hammaskarttoja ei voida edellyttää kaikilta sähköisiä reseptejä tuottavilta tietojärjestelmiltä. Sosiaali- ja terveydenhuollon määräyksissä tähän on pyritty mm. hyödyntämällä profiileja, joilla tiettyyn käyttötarkoitukseen suunniteltujen tietojärjestelmien olennaiset vaatimukset kootaan yhteen viitaten tarkempiin määrittelydokumentteihin. Vastaavasti kuin lääkinnällisten laitteiden sääntelyssä, järjestelmän käyttötarkoituksen on toimittava avaimena siihen, mitkä viranomaisvaatimukset ja minkä tasoinen riskejä vähentävä menettely on tarpeen.

Sallituista poikkeamista säätämisen (muistion kohta 9.2.5) sijaan vaatimusten lähtökohtana tulee olla vaadittavien ominaisuuksien riittävän tarkka määrittely. Käytännössä esimerkiksi vanhojen järjestelmien arvioinnissa ja vaatimusten todentamisessa joudutaan tekemään riskiarvioita ja mahdollisesti hyväksymään vaatimusten täyttymättömyyden kompensoivia toimenpiteitä (esimerkiksi käyttäjäohjeistus) vähintäänkin väliaikaisesti.

10. Muut yleiset kommentit arviomuistiosta

Arviomuistio on kattava ja sisältää paljon yksityiskohtaista asiaa. Arviomuistioon kirjatun pohdinnan perusteella näyttää olevan olemassa merkittävä riski siitä, että mennään toisaalta teknologioita koskevaan sääntelyyn ja toisaalta liian yksityiskohtaiseen säätelyyn.

Virkavastuun tuominen tietojärjestelmien kehittämistasolle ja tietojärjestelmätoteutukseen tulisi jäämään väistämättä hieman vajaaksi. Vastuu on luontevampaa kohdentaa mm. palvelun toteutumiseen ja tehtävien täyttämiseen.

Siltala Heikki
Terveyden ja hyvinvoinnin laitos THL