Helsingin kaupunki, Kaupunginkanslia

Lausunto

06.09.2021 HEL 2021-008280

Asia: VN/4400/2021

Arviomuistio julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista

Lausuntonne arviomuistiosta

1. Kommenttinne arviomuistiossa tehdystä nykytilan kuvauksesta

Helsingin kaupunki yhtyy arviomuistiossa esitettyyn näkemykseen siitä, että tietojärjestelmien kehittämistä ja käyttöä koskevaa sääntelyä ja vastuita tulisi täsmentää sekä selkeyttää, jotta voidaan turvata hyvän hallinnon takeet, oikeusturvan toteutuminen ja hallinnon läpinäkyvyys erityisesti automaattisessa päätöksenteossa. Samalla on huomioitava, että tiedonhallintalaki asettaa hyvän lähtökohdan tietojärjestelmäsääntelylle ja lain tasoisen sääntelyn lisäämistä tulee huolellisesti harkita.

2. Kommenttinne tietojärjestelmistä sääntelykohteena

Sääntelykohteena tietojärjestelmissä käytettävä tieto- ja viestintäteknologia on nopeasti kehittyvää ja muuttuvaa, mikä asettaa erityisvaatimuksia sääntelylle. Tietojärjestelmä sääntelykohteena ei myöskään ole vakiintunut. Tietojärjestelmän käsitteen yhdenmukaistaminen lainsäädännössä on kannatettava tavoite.

Tietojärjestelmiä koskevan sääntelyn tulisi olla joustavaa ja teknologianeutraalia, kuten työryhmä on katsonut. Sääntelyn ei tulisi olla liian yksityiskohtaista tai asettaa vaatimuksia tietynlaisille teknisille vaatimuksille, mikä tekisi sääntelystä helposti samalla helposti vanhentuvaa. Sääntelyn tulee mahdollistaa viranomaisille uusien teknologioiden kehittäminen ja käyttöönotto.

Sääntelyn taso olisi harkittava tarkkaan, jotta asioista ei tarpeettomasti säädettäisi mahdollisen uuden yleislain tasolla. Tarkempia vaatimuksia voitaisiin antaa alemmalla tasolla esimerkiksi toimivaltaisten virastojen toimesta ja huomioida alan soft law -tyyppinen itsesääntely.

Yksityiskohtaista laintasoista teknistä sääntelyä keskeisempää on asianmukaisuuden ja muiden olennaisten hallinnolle lailla asetettujen vaatimusten huomiointi tietojärjestelmien elinkaaressa ja selkeä ilmaisu tiedonhallintaa koskevassa sääntelyssä, jotta hyvän hallinnon takeet on turvattu hallinnon tietojärjestelmällä toteutettavassa asiankäsittelyssä, eli toimintaprosessissa.

Tietojärjestelmien vaatimukset tulisi kytkeä kiinteämmin tietojärjestelmien ja toimintaprosessin kehittämiseen ja suunnitteluun, jossa välineenä toimii tiedonhallintalain velvoittama

muutosvaikutusten arviointi (TiHL 5§). Arviomuistion luku 5. ja erityisesti 5.5 mainitsevat asian, mutta kytkös toiminnan kehittämisen ohjauksen ja tietojärjestelmien vaatimustenmukaisuuden välillä jää avonaiseksi. Mahdollisia uuden yleislain tietojärjestelmille tuomia velvoitteita tultaneen jatkossakin ohjaamaan osana tiedonhallintayksikön muutosvaikutusarviointiprosessia.

Koordinoinnin tarve on selvä lain, mahdollisesti edelleen tarkentuvien, tavoitteiden saavuttamiseksi, eikä lain tasoisella sääntelyllä voitane ratkaista kaikkia eteen tulevia tiedonhallinnan tai spesifimmin tietojärjestelmien haasteita. Julkisen hallinnon tiedonhallintalautakunnalla tai vastaavalla toimielimellä voisi olla rooli ja toimivalta sitovan ohjeistuksen antamiseen erityisesti teknisten vaatimusten osalta.

3. Millaisia yleisiä vaatimuksia tietojärjestelmien toiminnallisuuksille pitäisi lainsäädännöllä asettaa?

Tiedonhallintalaissa jo eri yhteyksissä mainitut tietoturvallisuus, saatavuus, käytettävyys, eheys ja vikasietoisuus ovat yleiset vaatimukset myös tietojärjestelmien toiminnallisuuksille, jotta varsinainen tavoite, eli asianmukainen hallintotoiminta ja hallintomenettely ovat mahdollisia. Työryhmän näkemys, että kehitettävän sääntelyn pitäisi sisältää säännökset tietojärjestelmien kehittämiseen liittyvistä riittävistä kontrolleista, dokumentoinnista ja virkavastuusta, on kannatettava.

Tietojärjestelmästä tulisi voida riittävällä tavalla selvittää, mihin automatisoitu päätös on perustunut jo viranomaisen päätöksen perusteluvelvollisuuden vuoksi. Toistaiseksi automatisoitu päätöksenteko niissä viranomaisissa, joissa sääntely on mahdollistanut sen käytön, on ainakin pääosin perustunut yksilöitävissä oleviin päätöksentekosääntöihin (perusteena olevat selvitykset ja oikeussäännöt). Hallintolakiin luonnostellut lisäykset koskien automaattista päätöksentekoa edellyttävät selkeitä päätöksentekosääntöjä sekä sitä, että asianosaista informoidaan automatisoidusta päätöksenteosta (prosessin sisällöstä) ymmärrettävällä tavalla. Tekoäly ei tällaisessa automaattisessa päätöksenteossa käytä itsenäistä harkintaa.

Kuten muistiossa todetaan, automaattisen päätöksenteon perustana olevan koodin selvittäminen asianosaiselle ei ole tarpeen, eikä tuone asianosaiselle perusteluna lisäarvoa. Tältä osin vireillä oleva hallintolain automaattista päätöksentekoa koskevien säännösten laatiminen on keskeinen asiakkaan näkökulmasta.

Hallintotoiminnan sujuvuuden näkökulmasta järjestelmän tulisi olla looginen ja ohjata käyttäjää, jotta virheet minimoidaan. Toiminnallisuuksien tulee olla yksiselitteisiä, jotta henkilötietoja käsitellään vain siihen tarkoitukseen, johon järjestelmä on tarkoitettu.

Uudistetun tiedonhallintalain toimintavelvoitteista lienee osin mahdollista johtaa tarkempia vaatimuksia tietojärjestelmille ilman uutta sääntelyä.

Arviomuistiossa esitetty näkemys, että sääntelyä ei ole tarkoituksenmukaista kohdistaa nimenomaan tekoälyyn tai tekoälyksi tulkittavia teknologioita käyttäviin järjestelmiin, on kannatettava. Tekoälyä koskeva oikeustila on tällä hetkellä vielä voimakkaasti kehittyvässä tilassa, minkä vuoksi sitä koskevan erillisen sääntelyn valmisteluun ei ole perusteltua nyt ryhtyä.

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

Muistion 6. lukuun on kattavasti koottu niitä vaatimuksia, jotka tietojärjestelmille vähintään tulisi lain tasolla asettaa, kuten tietojen siirtämiseen, käyttäjien tunnistamiseen, käyttöoikeuksiin ja

lokitietojen keräämiseen liittyvät vaatimukset. Nämä ovat osin jo olemassa olevasta lainsäädännöstä johdettavia vaatimuksia, eivätkä välttämättä vaadi täysin uutta sääntelyä.

On kannatettavaa, että EU:n yleisen tietosuoja-asetuksen 35 artiklan mukaista tietosuojan vaikutustenarviointia hyödynnetään muistiossa esitetyllä tavalla myös tietojärjestelmien teknisten vaatimusten asianmukaisuuden ja järjestelmiin liittyvien riskien arvioinnissa, osana perusoikeuksien turvaamista henkilötietojen käsittelyssä. Arvioitavaksi jää, onko asiasta säädettävä kansallisella lailla erikseen, ottaen huomioon, että tietosuoja-asetus on suoraan sovellettavaa oikeutta.

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

Lähtökohdan kehittämisen vaatimuksille asettavat samat asianmukaisuuden vaatimukset (kohta 3 ja 4) kuin tietojärjestelmille yleensä. Lain tasolla tulisi siten huolehtia siitä, että myös tietojärjestelmien kehittämisessä otettaisiin riittävällä tavalla huomioon perustuslain, hallintolain ja tiedonhallintalain sekä muun asiaa koskevan lainsäädännön asian käsittelyyn kohdistamat vaatimukset. Osin kyse on myös virkavastuun tehokkaasta kohdentamisesta, jonka keinoja on käsitelty kohdassa 6.

Tiedonhallintalaki velvoittaa tiedonhallintayksikköä ylläpitämään tiedonhallintamallia sekä toteuttamaan ns. muutosvaikutusten arviointia (ts. muutoksen suunnittelu ja arviointi) aina, kun tiedonhallintamalliin kohdistuu muutoksia. Kyseessä on käytännössä tiedonhallintaan liittyvien tietojärjestelmien ym. kehittämistoiminnan ohjauksesta. Olisi suositeltavaa selkeyttää ja täsmentää vaatimuksia, jotka tiedonhallintalaki asettaa tietojärjestelmien suunnittelulle, kehittämiselle ja käyttöönotolle muutosvaikutusten arvioinnin kautta, sekä kytkeä lain tarkoittamat muutoksenhallinnan ja suunnittelun velvoitteet osaksi tietojärjestelmiin kohdistuvia teknisiä ja toiminnallisia vaatimuksia, jotta ne muodostavat kokonaisuuden.

Tiedonhallintalain edellyttämä muutosvaikutusten arvioinnin vaatimuksen sisällöllinen huomioiminen tietojärjestelmiä koskevan yleislain yhteydessä edistäisi hyvän hallinnon toteutumista, kun viranomaisen olisi helpompi arvioida sekä toimintansa, eli tietojärjestelmän kehittämisen, lainmukaisuutta että ennakoida tietojärjestelmien kehittämisen vaikutuksia organisaation tiedonhallintamalliin ja tätä kautta myös toimintaprosesseihin. Selkeä, yhdenmukainen ja systemaattinen arviointi tietojärjestelmäkehittämisen yhteydessä vähentää tiedonhallintamallin laatuun ja sisällölliseen luotettavuuteen kohdistuvia riskejä, sekä selkeyttäisi ja yhdenmukaistaisi toimintatapoja myös kansallisella tasolla.

Syntyvän dokumentaation tulisi kattaa kaikki tiedonhallintalain ja mahdollisesti muun lain tai sitovan ohjeen asettamat vaatimukset selkeällä ja ymmärrettävällä tavalla. Dokumentaatiota tulisi tarpeen vaatiessa täydentää ja päivittää, ja sen tulisi olla helposti löydettävissä.

Dokumentoinnin tulisi olla niin kattavaa ja selkeää, että sen perusteella voidaan tosiasiallisesti arvioida järjestelmän toimintaa ja ominaisuuksia tietosuojan vaikutustenarvioinnin yhteydessä. Dokumentaatiota tulee tarvittaessa täydentää tietosuojan vaikutustenarvioinnissa tehtyjen havaintojen perusteella. Uutta järjestelmää kehitettäessä vaikutustenarvioinnin tulee olla tehty ennen käyttöönottoa. Dokumentoinnin perusteella tulee pystyä selvittämään järjestelmän virhetilanteet.

Arviomuistiossa esitettyjä tietojärjestelmän käyttöönottovaiheeseen liittyviä varmistustoimenpiteitä (huolellinen testaus, tietojärjestelmän käytön koulutus ja käyttöönoton suunnittelu) on pidettävä kannatettavina sääntelyn kehittämisen näkökulmasta. Voidaan katsoa, että asianmukaisen ja huolellisen järjestelmäkehityksen olemassa olevien vaatimusten (alan parhaiden käytäntöjen) tulisi

toteutua myös viranomaisen tietojärjestelmiä suunniteltaessa ja kehitettäessä. Arvioitavaksi jää, kuinka yksityiskohtaisesti nämä vaatimukset on asetettava lain tasolla.

Huomionarvoinen on myös palvelun käsitteen liityntä tietojärjestelmiin. Tiedonhallintalaki (27 §) asettaa tietoaineistojen hallinnalle palveluja tuotettaessa vaatimuksia. Näitä palveluja tuotetaan tietojärjestelmillä. Palvelun käsitteen määrittely toisi selkeyttä tietojärjestelmiinkin kohdistuvien vaatimusten osalta.

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

Tosiasiallisen virkavastuun tulee aina kohdistua luonnolliseen henkilöön. On tärkeää kansalaisten oikeusturvan kannalta, että virkavastuu tietojärjestelmien kehittämisessä ja käytössä on selvästi määritelty. Tämä vaatii lainsäädännön tarkentamista.

Virkavastuu voitaisiin esimerkiksi automaattisen päätöksenteon osalta kohdistaa päätöksentekosääntöjen hyväksyjiin ja päätöksenteon valvonnasta vastaaviin. Virkavastuun tulee siten selkeästi olla yhdistettävissä johonkin tiettyyn virkatoimeen tai ratkaisuun. Vastuu tulisi myös organisaatiossa asettaa oikealle tasolle, suhteessa virkatoimen merkittävyyteen. Esimerkiksi päätöksentekosääntöjen hyväksyminen on nähtävä julkisen vallan käytöksi, jonka toimivalta ja vastuu kuuluu riittävän korkealle tasolle. Automatisoituihin toimintaprosesseihin kohdistettavan virkavastuun tulisi siten olla oikeassa suhteessa ihmisen tekemän päätöksenteon vastaaviin vastuisiin.

Lainsäädännöllä voitaneen asettaa vaatimus, että viranomaisen on esimerkiksi hallintosäännössä tai vastaavassa määrättävä tietojärjestelmien kehittämiseen, käyttöönottoon ja käyttöön liittyvät vastuut.

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

Vaatimukset ovat sinällään samat saatavuus, käytettävyys, eheys ja vikasietoisuus ja näiden johdannaiset kuin tietojärjestelmissä ja tietosuoja-asetuksen 5 artiklan periaatteet. Erityisesti korostuvat riittävä luotettavuus ja ajantasaisuus. Tiedonhallintalain vaatimukset tietovarannoille ja niiden yhteen toimivuudelle ovat hyvä lähtökohta mahdollisesti tarkennettaville vaatimuksille.

Arviomuistiossa esitetyt alustavat laatukriteerit, jotka perustuvat ISO 25012 –standardiin, muodostavat kokonaisuutena kattavan ja hyvän pohjan arvioida tietovarantojen, niiden laadun sekä käytön asianmukaisuutta myös automaattisen päätöksenteon osalta.

Viranomaisten yhteisten tietovarantojen luotettavuuden tulisi vastata käytännössä ns. julkista luotettavuutta, kun kyse tietovarantoon sisältyvistä automaattiseen päätöksentekoon käytettävistä tiedoista, jotta päätöksenteko olisi tehokasta ja viranomaisen selvitysvelvollisuuden täyttäminen joutuisaa. Tietovarannon on oltava hyödynnettävissä niin ihmisen kuin automatisoidun tietojärjestelmän toiminnassa. Konkreettisesti esimerkiksi muutoksenhakuasiaa käsittelevän ihmisen tulee olla mahdollista löytää automaattisen päätöksenteon perusteena olleet tiedot tietovarannosta täydellisinä sekä mahdollisimman vaivattomasti.

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

Helsingin kaupunki yhtyy arviomuistiossa esitettyyn näkemykseen siitä, että viranomaisella itsellään on paras asiantuntemus arvioida ja varmistua sen käytössä olevien tietojärjestelmien päätöksentekosääntöjen virheettömyydestä ja tietoturvallisuudesta.

Ulkopuolisen asiantuntemuksen hyödyntämiseksi teknisten vaatimusten arvioinnissa ja arviointijärjestelmän joustavuuden näkökulmasta olisi kuitenkin kannatettavaa, että yksityiset toimijat voisivat sertifioinnin perusteella tehdä arviointeja julkishallinnon tietojärjestelmistä.

Viranomaisen on silti kannettava virkavastuu sen toiminnassaan hyödyntämien päätöksentekosääntöjen laatimisesta ja niiden vaatimustenmukaisuudesta kokonaisuudessaan, kuten arviomuistiossakin todetaan.

Muistiossa on esitetty, että vaatimustenmukaisuuden osoittamista koskevassa sääntelyssä yksi vaihtoehto voisi olla vaatimusten ja kriteeristöjen joustavuus, jolloin poikkeamisen määrästä ja laadusta riippuen palvelu voitaisiin ottaa käyttöön tai sen käyttöä voitaisiin jatkaa ehdollisesti, jos näin on palvelun vaatimuksia koskevassa säädännössä todettu ja sallittu. Helsingin näkemyksen mukaan tämä olisi erityisesti ei-henkilötietoja sisältävien tietovarantojen kohdalla järkevää, koska riskiarvioinnin pohjalta voitaisiin tällöin tapauskohtaisesti arvioida, onko mahdollinen poikkeama korjattava.

Itsesääntelyn ja muiden soft law -sääntelykeinojen hyödyntämistä tietoturvallisuuden suhteen täydentävinä normeina tulee vielä tarkastella säädösvalmistelussa erikseen. Itsesääntely, kuten standardeihin sidotut tietoturvavaatimukset, tarjoaa joustavan ja ketterän tavan ohjata tietojärjestelmien tietoturvallisuutta.

9. Kommenttinne muistiossa todetuista sääntelytarpeista yleensä

Yleisesti voidaan todeta, että hallinnon tietojärjestelmiä koskeva tarkentava lainsäädäntö tulee tarpeeseen. Uuden lain tasoisen sääntelyn laajuus ja suhde hallinnon yleislakeihin on kuitenkin tarkkaan harkittava. Tähän asti tietojärjestelmät toiminnallisuuksineen on mielletty vain viranomaisen valmistelun ja päätöksenteon teknisen toteuttamisen välineiksi. Ei ole riittävästi ymmärretty, että tosiasiassa järjestelmiä hyödynnetään paikoin hyvinkin oleellisena osana viranomaisen hallintomenettelyä ja sillä, miten ne on hankittu ja toteutettu, voidaan joko heikentää tai vahvistaa menettelyn lainmukaisuutta ja hallinnon asiakkaan oikeusturvaa.

10. Muut yleiset kommentit arviomuistiosta

Ei kommentteja.

Eid Terttu
Helsingin kaupunki, Kaupunginkanslia