

Helsingin kaupungin lausunto viranomaisten tietojärjestelmien tietoturvallisuuden arviointia koskevan lainsäädännön muuttamiseen

Arviointilain muutokseen liittyvät kysymykset lausuntopyynnössä

Huomiot ehdotetusta soveltamisalan laajenemisesta varautumisen arviointiin sekä muutoksen mahdollisista vaikutuksista

Helsingin kaupunki näkee hyvänä asiana laajentaa arviointia varautumiseen sekä turvallisuuskriittisten ratkaisujen valmistuksen tietoturvallisuuteen. Helsingin kaupungin mielestä arvioinnissa on hyvä huomioida koko järjestelmän / ratkaisun elinkaari eri tilanteissa ja eri toimintaympäristöissä. Lisäksi järjestelmän toimintaa arvioitaessa tulisi huomioida nykypäivän monitoimijaympäristöt sekä valmistajan ja käyttäjäorganisaation rooli.

Valmistajaa ei ole lain luonnosesityksen määritelmässä määritelty. Muutenkin tällaisenaan ehdotus on muotoiltu siten, että tietojärjestelmä valmistetaan kerran ja sen jälkeen se on valmis ja käytetään elinkaaren loppuun sellaisenaan, ilman muutoksia tai jatkokehitystä. Tämä ei ole nykypäivän tietoteknisissä ratkaisuissa vallitseva tilanne. Järjestelmiin liittyen on useampia rooleja kuin vain valmistus. Tietojärjestelmiä ja tietoliikennetarkaisuja ylläpidetään, niiden käyttöä seurataan ja valvotaan tuotannossa (palveluhallinta), niihin tehdään muutoksia, toimittajat vaihtuvat esim. kilpailutusten tai yrityskauppojen seurauksena. Tämän takia Helsingin kaupunki toivoo, että laissa esitettäisiin ratkaisun hallinta sen koko elinkaarta ajatellen paremmin ja otettaisiin myös kantaa arvioinnin uusimistarpeeseen tai viitattaisiin siihen jotenkin, kuten esim. viitattaisiin tiedonhallintalain muutosvaikutusten arviointiin tekemisen ehtoihin (Laki julkisen hallinnon tiedonhallinnasta).

Arvioinnin laajeneminen mahdollisesti nostaa työmäärää ja siten myös arviointikohtaiset kustannukset saattavat nousta merkittävästi. Tämä on myös pitkälti riippuvainen siitä, paljonko hyväksytyjä palvelun tarjoajia markkinoilla arviointiviranomaisten lisäksi on. Lisäksi mahdollisia lisäkustannuksia hallitaan myös sillä, että ehdotus antaa mahdollisuuden myös itsearviointiin tietyissä tapauksissa.

Huomiot ehdotetuista arviointimenettelyjä koskevista muutoksista sekä uusista viranomaisista koskevista arviointivelvollisuuksista ja niiden vaikutuksista organisaatiosi toimintaan

Esitetyissä arviointimenettelyissä Helsingin kaupunki pitää hyvänä, että arviointimenettelyitä on määritelty useampia. Tämä tarjoaa varsinkin omaehtoiseen arviointiin mahdollisuuden hallita arvioinnin kustannuksia ja hyötyä riskiperusteisesti. Toisaalta arviointimenettelyjen kohdentamisen rajoitukset estävät ”yliarvioinnin” ja todennäköisesti myös auttavat arviointiviranomaisia hallitsemaan arviointipyyntöjä ja arviointiresurssien käyttöä.

Kunnalliselle toimijalle ehdotettu muutos tuo vähintäänkin itsearvioinnin velvoitteen niihin ratkaisuihin, joissa käsitellään turvallisuusluokkaan III luokiteltuja tietoja. Lainsäädäntö laajentaa kunnan, ja muiden kuin valtion viranomaisten, tehtäviä. Lisäksi ulkoisen arvioinnin edellytysten täyttyessä lisää ulkoisia kustannuksia. Muuten kunnallisella toimijalla säilyy itsenäisyys arviointitoimenpiteiden valinnasta, suorittamisesta ja laajuudesta asianmukaisesti.

Tässä kohtaa lain muutosvalmistelussa on hyvä varmistaa, että lainsäädännöllisesti ei jäisi ristiriidan mahdollisuutta ehdotetun lain 3b§ toisen momentin mukaan tehdyn arviointimenettelyn ja 1101/2019 6§ mukaisesti turvallisuusluokitellun luovutettavan aineiston suojaamisen välillä. Luovuttajan on varmistuttava luovutettavan asiakirjan suojaamisesta ja suojaustoimenpiteet voitaisiin tarvittaessa osoittaa jo tehdyllä arvioinnilla.

Huomiot ehdotetuista arviointiviranomaistehtävien ja tiedonsaanti- ja tarkastusoikeuksien muutoksista (3 d–6 §)

Helsingin kaupungin kannalta ehdotuksessa on hyvin huomioitu, että arviointiviranomaisia on useampia ja muutos edellyttää heiltä yhteistyötä sekä vuoropuhelua, vaikka toimivalta onkin arviointikohteiden perusteella jaettu. Myös yhteistyön ohjaaminen on määritelty selkeästi.

Toimivaltajako on yleistasolla selkeästi määritelty. Ehdotuksen kohta 3d§ 5 momentti tai 4§ toisen momentin ensimmäinen kohta vaatii täsmentämistä. 3d§ 5 momentissa säädetään pääesikunnan määrätyn turvallisuusviranomaisen toimivaltaan kuuluva ”arviointi koskee Puolustusvoimien tietojärjestelmien tai tietoliikennejärjestelyjen taikka niihin kuuluvien turvallisuuskriittisten ratkaisujen tietoturvallisuutta ja varautumista.” Toisaalta 4§ toisen momentin ensimmäisessä kohdassa määritellään liikenne- ja viestintäviraston tehtäväksi arvioida Suomeen sijoittautuneen turvallisuuskriittisten ratkaisujen valmistajan hakemusta. Entä jos tässä tapauksessa valmistajan ratkaisu onkin tuon 3d§ 5 momentin piirissä?

4a§ määritellään arviointiviranomaisen mahdollisuutta käyttää ulkopuolisia asiantuntijoita, jos heidän koulutuksensa ja kokemuksensa vastaavat arviointi tehtävän vaatimuksia. Lisäksi ulkopuolisiin asiantuntijoihin sovellettaisiin virkavastuuta koskevia säännöksiä. Se mitä ko. kohdassa ei mainita on, mitä 3§ toisessa momentissa säädetään hankkiessaan arviointi suoraan palveluntarjoajalta: ”Viranomaisen on tällöin ennakolta varmistuttava palveluntarjoajan luotettavuudesta toimeksiannon edellyttämässä laajuudessa.” Arviointiviranomaiselta olisi syytä tässä kohtaa edellyttää aivan samaa ulkopuolisen tahon luotettavuuden ja riippumattomuuden edellytyksiä suhteessa arvioitavaan järjestelmään ja sen toimittajaan kuin viranomaisella on toteuttaessaan arvioinnin palveluntarjoajalta.

Arviointiviranomaisten laaja tiedonvaihto- ja tiedonsaantioikeus on tehtävien suorittamiseksi perusteltua. Sitä olisi hyvä pohtia, pitääkö tässä sääntelyssä mainita myös arvioinnin kohteen oikeuksista saada tietää häntä koskevien tietojen vaihdosta ja luovutuksista tai viitata asianomaisiin jo olemassa oleviin lainkohtiin, jonka nojalla tämä informointivelvollisuus on olemassa.

Huomiot ehdotetusta uudesta turvallisuuskriittisten ratkaisujen ja niiden valmistuksen arviointien kokonaisuudesta

Yleisesti ottaen muutokset kautta linjan täsmentävät ja asettavat monelta osin uusia, tiukempiakin vaatimuksia toiminnalle ja arviointikohteille sekä eri viranomaisille.

Pääsääntöisesti nämä vaatimukset ovat kuitenkin perusteltuja ja antavat yhtenäisemmän pohjan arviointien tekemiseen ja hallintaan.

Ratkaisujen elinkaaren huomioiminen tulisi nostaa valmistelutyössä vielä pohdittavaksi asiaksi. Nyt ehdotus laajenee järjestelmän käytön osalta varautumiseen, ei normaaliin toimintaympäristön tilanteeseen ja ratkaisun valmistajaan, mutta jää vajavaiseksi muiden toimijoiden tai järjestelmässä tapahtuvien muutosten huomioimisessa järjestelmän eri elinkaaren vaiheissa.

Huomiot ehdotetuista siirtymäsäännöksistä ja -ajoista

3 vuoden siirtymäaika on luultavasti muulle kuin valtion viranomaiselle riittävä siirtymäaika, koska arviointivelvoite koskee suhteellisen vähäistä järjestelmien ja käsiteltävien tietojen lukumäärää.

- Muut arviointilakia koskevat huomiot, pyydämme yksilöimään pykälän

Yksittäisenä huomiona Helsingin kaupunki nostaa esiin sen, että olisi hyvä selkeyttää 3§, 3a§ ja 3b§ mainittuja velvollisuuksia ja mahdollisuuksia tehdä tai toteuttaa arviointeja eri menetelmillä. Esim. 3§ kolmas momentti toteaa, että viranomainen **voi toteuttaa** arvioinnin **vain** menetelmällä ja 3b§ vastaavasti velvoite ilmaistaan: ”viranomaisen **on arvioitava** tietojärjestelmänsä tai tietoliikennejärjestelynsä...”

2§ Lain määritelmissä tietojärjestelmän määritelmää olisi hyvä tarkastella kriittisesti. Nykyinen määritelmä: ”tietojärjestelmällä tarkoitetaan tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä”, on ongelmallinen erityisesti muusta tietojenkäsittelystä olevalla maininnalla. Siinä ei muuta käsittelyä rajata millään tavoin teknisiin ratkaisuihin. Muu tietojenkäsittely voi näin ollen myös vaikkapa manuaalista lyijykynän ja paperin käyttöä tietojen käsittelyyn sisältäen myös ihmisten tekemiä tehtäviä.

Esim. tiedonhallintalain 906/2019 määritelmissä tietojärjestelmälle on tämä sama, turhan tulkinnanvarainen määritelmä, mutta myös toinen (määritelmä nro 17), joka on teknisessä mielessä täsmällisempi:

”b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; ja

c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään näiden järjestelmien toimintaa, käyttöä, suojausta tai ylläpitoa varten;”

Arviointilaitoslain muutokset

Laki koskee keskeisesti liikenne- ja viestintäviraston ja arviointilaitokseksi hakeutuvan tai sellaisena toimivan yrityksen toimintaa ja luvan hallintaprosessia. Näin ollen Helsingin kaupungilla ei ole sen muutoksiin lausuttavaa.

Huomiot ehdotetusta tietoturvallisuuden arviointilaitosten luotettavuuden varmistamista koskevista muutoksista (4–5 §)

Huomiot ehdotetusta tietoturvallisuuden arviointilaitosten lisäpätevyyksien hyväksymisprosessista (5 § 3 mom)

Muut arviointilaitoslakia koskevat huomiot, pyydämme yksilöimään pykälän

Huomiot esityksen vaikutusten arvioinnista

Lainmuutos mahdollistaa yrityksille myös mahdollisuuden hakea arviointia itsenäisesti tarjoamilleen ratkaisuille.

Arviointivelvollisuuden laajeneminen muille viranomaisille, kuin valtion, vaikkakin rajatusti ja itsearviointi mahdollistaen tuo kuitenkin taloudellisiin vaikutuksiin markkinoiden potentiaalista kasvua arviointilaitosten kannalta ja toisaalta taas kasvavia kuluja viranomaisille ainakin jossain määrin. Näitä kustannuksia ei vaikutusten arvioinnissa ole esitetty kovinkaan täsmällisesti.

Esittelijän perustelut

Valtiovarainministeriö on pyytänyt Helsingin kaupunkia antamaan lausunnon ehdotuksesta viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia koskevan lainsäädännön muuttamisesta.

Hallintosäännön 9 luvun 1 §:n 7 kohdan mukaan pormestari tekee esityksiä ja antaa kaupunginhallitukselta pyydettyjä lausuntoja sekä huolehtii näihin rinnastettavista muista tehtävistä, jollei asiaa sen periaatteellisen tai taloudellisen merkityksen johdosta ole saatettava kaupunginhallituksen käsiteltäväksi.