Porvoon kaupunki

Lausunto

21.01.2026

Asia: VN/36127/2023

Lausuntopyyntö ehdotuksesta viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia koskevan lainsäädännön muuttamisesta

Huomiot ehdotetusta soveltamisalan laajenemisesta varautumisen arviointiin sekä muutoksen mahdollisista vaikutuksista/ Kommentarer om föreslaget att utvidga tillämpningsområdet så att det omfattar bedömningen av beredskapen och om ändringarnas konsekvenser:

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Lakia sovelletaan kunnassa, jossa käsitellään turvallisuusluokiteltuja tietoja tietojärjestelmissä tai tietoliikennejärjestelyissä

Uusien tietojärjestelmien ja ratkaisujen osalta tehdään tiedonhallintalain mukainen muutosvaikutusten arviointi, jonka tavoitteena on tunnistaa kriittiset järjestelmät sekä NIS2-direktiivin piiriin kuuluvat tehtävät.

Kriittiset järjestelmät ja toimintamallit arvioidaan varautumisen ja palautumisen näkökulmasta joko itsearviona tai ostopalveluna.

Kuntien työmäärää keventäisi keskitetty arviointimenettely tai toimittajan tekemä sertifiointi, joka on hyväksytty arviointilaitoksen toimesta.

Huomiot ehdotetuista arviointimenettelyjä koskevista muutoksista sekä uusista viranomaisia koskevista arviointivelvollisuuksista ja niiden vaikutuksista organisaatiosi toimintaan (3–3 c §)/ Kommentarer om de föreslagna ändringarna i bedömningsförfarandena och om de nya bedömningsskyldigheterna för myndigheterna samt konsekvenserna av dessa för din organisation (3–3 c §):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Keskisuuressa kunnassa turvallisuusluokiteltuja tietoja käsittelevät järjestelmät on arvioitava säännöllisesti, mikä lisää kehitystyötä ja edellyttää huomioimaan muuttuvat teknologiat. Muutoksella on vaikutus sekä tehtäviin ja henkilöresursseihin.

Hallinnollinen työ kasvaisi kunnassa sillä organisaation on määriteltävä selkeät tulkinnat, toimintamallit ja ohjeistus siitä, milloin itsearviointi on riittävä ja milloin tarvitaan laajempi arviointi. Myös tiedon dokumentointi laajenee ja syvenee.

Huomiot ehdotetuista arviointiviranomaistehtävien ja tiedonsaanti- ja tarkastusoikeuksien muutoksista (3 d–6 §)/ Kommentarer om de föreslagna ändringarna i bedömningsmyndigheternas uppgifter och rätt att få information och utföra inspektioner (3 d–6 §):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Tiedonsaanti ja tarkastusoikeudet tarvittavien käyttöoikeuksien kautta selkeyttävät auditointeja, jotka kohdistuvat organisaatioon.

Välttämättömyysperuste turvaa liikesalaisuudet ja yksityisyydensuojan, vaikka tarkastuksia tehdään.

Aiemmat tietoturvatarkastukset on toteutettu vaihtelevasti, eivätkä ne ole kunnassa olleet vuosittaisia. Jos markkinoilla toimii useampi tarkastuslaitos, se tuo kuntakentälle uuden kilpailutettavan kumppaniratkaisun.

Huomiot ehdotetusta uudesta turvallisuuskriittisten ratkaisujen ja niiden valmistuksen arviointien kokonaisuudesta/ Kommentarer om de nya bestämmelserna om bedömningen av säkerhetskritiska lösningar och produktionen av dem:

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Turvallisuusluokiteltujen tietojen ja palveluiden osalta julkinen hallinta yhdenmukaistuu, ja hankinnoissa voidaan edellyttää tietoturvaan liittyvien palveluiden arviointia sekä hyväksyntää. Kunnan on hankintaprosessiin lisättävä vaatimus, että toimittajan ratkaisu täyttää tietoturvakriteerit.

Arviointilaitosten tai viranomaisten tuottamat yhdenmukaiset raportit helpottavat kuntien työtä ja vähentävät päällekkäisiä tarkastuksia.

Huomiot ehdotetuista siirtymäsäännöksistä ja -ajoista/ Kommentarer om de föreslagna övergångsbestämmelserna och övergångstiderna:

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Kunnassa tulee arvioida turvallisuusluokitellut tiedot uudelleen, luoda hallintamalli sekä vuosittaiset suunnitelmat arviointien toteuttamiseksi ja priorisoida tehtävät luokitusten perusteella.

Hyväksyttyjen ratkaisujen päätökset on oltava helposti saatavilla, jotta niitä voidaan hyödyntää ja välttää pitkät sekä päällekkäiset odotusajat.

Yhteishankinnat tarjoavat lähinnä yhden kanavan markkinoille, mutta eivät poista päällekkäistä työtä.

Tarvitaan kokonaistarkastelu uusista vaatimuksista, jotka kohdistuvat kunnan tietohallintoon ja sen pohjalta on tehtävä realistinen arvio siirtymäajan riittävyydestä.

Muut arviointilakia koskevat huomiot, pyydämme yksilöimään pykälän/ Övriga kommentarer om bedömningslagen (specificera vilken paragraf som avses):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

3b§ Muiden kuin valtionhallinnon viranomaisten arviointivelvollisuudet

Kunnat voivat ajautua eriarvoiseen asemaan tietoturvan ja käytäntöjen osalta.

Turvallisuusluokiteltujen tietojen tulkinta vaihtelee kunnittain, mikä voi johtaa merkittäviin poikkeamiin tietoturvatasoissa ja käytännöissä.

Huomiot ehdotetusta tietoturvallisuuden arviointilaitosten luotettavuuden varmistamista koskevista muutoksista (4–5 §)/ Kommentarer om de föreslagna ändringarna angående säkerställandet av tillförlitligheten hos bedömningsorganen för informationssäkerhet (4–5 §):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Arviointilaitosten luotettavuuden varmistamiseksi tulisi edellyttää FINAS-akkreditointia aina, kun pätevyysalue kattaa Katakri-vaatimukset tai ISO 27001 -standardin.

Huomiot ehdotetusta tietoturvallisuuden arviointilaitosten lisäpätevyyksien hyväksymisprosessista (5 § 3 mom)/ Kommentarer om processen för godkännande av bedömningsorganens specialbehörigheter (5 § 3 mom.):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Arviointilaitosten luotettavuuden varmistamiseksi tulisi edellyttää FINAS-akkreditointia aina, kun pätevyysalue kattaa Katakri-vaatimukset tai ISO 27001 -standardin. Jos valvonta on muuten säännöllistä, uusinta-arvioinnit voidaan kohdentaa lisäpätevyyksien osalta.

Muussa tapauksessa arviointilaitos voi tehdä ISO 27001 arviointeja – ilman että FINAS akkreditointi on tehty.

Muut arviointilaitoslakia koskevat huomiot, pyydämme yksilöimään pykälän/ Övriga kommentarer om lagen om bedömningsorgan (specificera vilken paragraf som avses):

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

13 a § Turvallisuusselvitysrekisteriin merkittävät tiedot

Tuleeko kunnille käyttöön esimerkiksi DVV:n Suomi.fi-valtuudet, ja sitä kautta pääsy turvallisuusselvitysrekisteriin ajantasaisen tiedon saamiseksi?

Huomiot esityksen vaikutusten arvioinnista/ Kommentarer om bedömningen av propositionens konsekvenser:

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Arviointilaitosten määrän kasvu tarjoaa kunnille mahdollisuuden tiukentaa järjestelmähankintojen vaatimuksia edellyttämällä, että järjestelmät on arvioitu ja hyväksytty.

Lakiesityksen mukaan myös kuntien on arvioitava omat tietojärjestelmänsä ja tietoliikennejärjestelynsä, joissa käsitellään turvallisuusluokkaan III luokiteltuja tietoja (3 a §:n 2 kohdan mukaisesti). Tämä koskee laajasti kriittisiä toimintoja, kuten vesihuoltoa ja liikennejärjestelmiä.

On varmistettava riittävät siirtymäajat ja koulutus, jotta kunnat voivat toteuttaa vaatimukset hallitusti.

Lakiesityksen toimeenpanossa on riski, että kunnat tulkitsevat vaatimuksia eri tavoin, mikä voi johtaa eritasoisiin käytäntöihin. Tarvitaan valtakunnalliset ohjeet ja rahoitusmalli, joka tukee yhdenmukaista toteutusta.

Nykyinen sirpaleinen ja epävarma asetelma heikentää kyberturvallisuusstrategian mukaista vastetta. Lakiesityksen tulee vahvistaa yhtenäisyyttä ja selkeyttä.

On arvioitava, miten avoimen lähdekoodin ratkaisut soveltuvat vaatimuksiin. Lisäksi tiedonhallintalain implementointi on vielä monissa kunnissa kesken, mikä voi vaikeuttaa tiedon luokittelua ja siirtymävaihetta.

Kunnat toimivat jo nyt vaihtelevissa kyberturvallisuusympäristöissä, mikä luo uhkia ja heikentää vastekykyä. Lakiesityksen vaikutuksia on tarkasteltava suhteessa tähän lähtötilanteeseen ja realistiseen siirtymäaikaan.

Grönqvist Charlotta
Porvoon kaupunki - Kehitys ja digitalisaatio