

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

Mikäli tarvittava arviointien viitekehys tullaan myös valmistelemaan, ajatus varautumisen lisäämisestä arviointilain piiriin on hyvä ja kannatettava. Viranomaisia velvoittava ohjeistus on varautumisen osalta varsin yltäsoista, eikä sisällä riittävän yksityiskohtaisia vaatimuksia, jotta niiden perusteella voitaisiin arvioida objektiivisesti varautumisen tilaa.

Turvaluokittelu, jolla tavoitellaan erityisesti tietojen luottamuksellisuudesta varmistumista, ei myöskään lähtökohtaisesti määrittele varautumisen tasoa tai vaatimuksia. Turvaluokitusten ympärille rakennettujen kriteeristöjen sisältämät yksittäiset varautumista koskevat vaatimukset eivät lähtökohtaisesti myöskään johda varautumisen tilan kattavaan arviointiin.

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

Esitetty muutos johtaa todennäköisesti siihen, että teetätämme aiempaa enemmän palveluntarjoajan viranomaisen toimeksiannosta toteuttamia arviointeja. Niissä voimme määritellä arviointien laajuuden, sisällön sekä toteuttamistavan. Samanaikaisesti on käytettävissä aiempaa laajempi joukko palveluja tarjoavia yrityksiä. Tämä edesauttaa arviointitoiminnan kohdentamista oikeisiin kohteisiin ja mahdollistaa arviointien järjestämisen aiempaa tuottavammalla tavalla.

Koska itsearviointien laatu on helppo kyseenalaistaa, niitä tultaneen tekemään harvoin. Itsearviointien laatu vaihtelee voimakkaasti arviointia tekevän organisaation kypsyystason mukaan. Kun arviointia tekee organisaatio, jonka toiminta on osin arvioinnin kohteena, riskit erilaisista vääristymistä sekä puutteista ovat merkittävät.

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

Ei lausuttavaa tähän kohtaan.

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

Turvallisuuskriittisillä ratkaisuilla viitataan käytännössä tietoliikenne-, tiedosto-, levyjärjestelmä- ja linjasalaimiin. Salaustoteutusten turvallisuuden arvioiminen on voimakkaasti sidoksissa esitettyyn turvallisuuskriittisyyteen.

Kaikissa viranomaisten tietojärjestelmissä on nykyään tarpeita salaukselle, kuten esimerkiksi webbipalvelimen tietoliikenteen salaukselle, sähköisille allekirjoituksille asiakirjoihin tai Virtuverkoston allekirjoitusavaimien hallinnalle. Tähän mennessä näihin ratkaisuihin ei ole ollut käytännössä mahdollista hankkia arviointilaitoksilta tai arviointiviranomaiselta arviointeja.

Ehdotettu priorisointi johtaa siihen, että jatkossakaan yksittäinen viranomainen, jonka tietojärjestelmä ei menesty priorisoinnissa, ei voi saada salaustoteutusten arviointia lainsäädännön puitteissa. Kun jo yksin turvallisuusviranomaisten arviointipyynnöt ylittävät käytettävissä olevan arviointikapasiteetin, muiden ratkaisut jäävät arvioimatta. Viranomainen voi riskiarvionsa perusteella käytännössä lähinnä hankkia palveluntarjoajan viranomaisen toimeksiannosta toteuttaman arvioinnin ilman, että mahdollisuudesta toimia siten on säädetty.

Turvallisuuskriittisten ratkaisujen arvioinnin ja hyväksynnän ei periaatteessa pitäisi erota muusta tietoturvallisuuden arvioinnista. Alemmilla turvaluokitustasoilla viranomaisten pitäisi voida hankkia palveluntarjoajilta salausratkaisujen arvioinnit ja tämä mahdollisuus tulisi kirjata lakiin. Arviointiviranomaisen suorittama arviointi ja kansallinen hyväksyntä pitäisi rajata vain toteutuksiin, joilta edellytetään sitä erityislainsäädännössä, kansainvälisissä sopimuksissa tai vastaavissa muissa tilanteissa.

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

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Ei lausuttavaa tähän kohtaan.

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

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

On hyvä ja kannatettava ajatus lisätä lakiin kirjaus siitä, että Liikenne- ja viestintävirasto voi antaa tietoturvallisuustoimenpiteisiin ja tietoturvallisuuden arviointiin liittyvää neuvontaa.

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

Ei lausuttavaa tähän kohtaan.

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

Ei lausuttavaa tähän kohtaan.

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

Ei lausuttavaa tähän kohtaan.

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

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Turvallisuuskriittisten ratkaisujen osalta vaikutusten arviointi on puutteellista ja sitä on selvästi valmisteltu lähinnä arviointiviranomaisten näkökulmasta.

Jos salaustuotteiden arviointia siirrettäisiin palveluntarjoajille, ainakin alempien turvaluokitusten osalta ja kun kansallista hyväksyntää ei ole veloitettu, se todennäköisesti kasvattaisi kotimaisen yrityskentän osaamista pitkällä aikavälillä. Salausteknologiat eivät sinänsä erotu muista teknologioista, vaan mitä enemmän osaamiselle on kysyntää sitä enemmän yritykset ja korkeakoulut tuottavat uusia asiantuntijoita.

Esitetyn prioriteettilistan perusoikeusvaikutusten arviointiin on kiinnitettävä erityistä huomiota. Esitetty priorisointi tekee mahdollisesti osan tehtävistä tosiasiassa suorittamattomiksi. Tosiasialliset vaikutukset voivat johtaa siihen, että osan viranomaisista, jotka eivät menesty esitetystä priorisoinnista, tietojärjestelmät ovat tietoturvaltaan heikompia. Tämä voi välillisesti vaarantaa ko. viranomaisten hallinnon asiakkaiden subjektiivisen perusoikeuden yksityisyydensuojaan.

Laine Eelis
Oikeusrekisterikeskus

Lehtisalo Mikko
Oikeusrekisterikeskus - Turvallisuuspalvelut