

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

Metropolia Ammattikorkeakoulu kiittää mahdollisuudesta lausua asiassa.

Arviointilaitosten määrän laajentaminen on tarpeenmukaista. Korkeakoulusektori kuuluu tiedonhallintalain sääntelyn piiriin, ja sitä ohjaavat samat velvoitteet kuin julkishallintoa, kuntia ja hyvinvointialueita tietoturvahäiriöiden hallinnan sekä riskienhallinnan osalta. Valtion viralliset arviointilaitokset tukevat korkeakoulujen tietoturvatyötä paikkaamalla tarvittavaa tietoturvaosaamista, esimerkiksi varautumisen ja teknisen turvallisuuden alueilla.

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

Ehdotettu malli on järkevä ja linjassa kansainvälisten käytäntöjen kanssa, kuten kyberturvallisuuslain periaatteiden, joissa toimijalla on myös velvollisuus arvioida itseään. Ehdotetun lain vaikutukset korkeakouluille, esimerkiksi kustannusten ja hallinnollisen työkuorman näkökulmasta ovat minimaaliset. On kuitenkin huomioitava, että laki ei ota kantaa julkisuuslaissa määriteltujen salassa pidettävien tietojen suojausvaatimukseen, joka on sensitiivisintä tietoa korkeakoululla.

Korkeakouluilla harvemmin on hallussaan turvaluokiteltua tietoa. Mielestämme viranomaisia koskevien arviointivelvoitteiden tulisi käsitellä nykyistä tarkemmin myös salassa pidettävän tiedon suojausvaatimuksia, esimerkiksi itsearvioinnin osalta.

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

Tiedonvaihto ja tarkastusoikeus lisäävät julkishallinnon läpinäkyvyyttä, kun arviointiviranomaisella on pääsy arviointikohteen varautumis- ja suojautumiskäytänteisiin. Valtiovarainministeriölle kaavailtu koordinoivampi rooli tilannekuvan luomisessa viranomaisten tietoturva- ja varautumistasosta edistää kansallisen turvallisuuden toteutumista sekä näiden organisaatioiden hallintaa (Governance) toivottuun suuntaan. Kuitenkin varautumiskyky- ja tietoturvatöiden tiedonsaanti- ja tarkastusoikeus tulisi ulottaa salassa pidettävään tietoon vahvemmin.

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

Ehdotus on kokonaisuudessaan tarpeenmukainen. Valtion viralliseksi hyväksytty sala- ja hajasäteilysuojaukset helpottavat myös korkeakoulun käytössä olevien tietoturvaratkaisujen valitsemista.

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

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

-

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

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

-

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

Ehdotettu toimintatapa noudattaa tietoturvan hyviä käytäntöjä, joissa varmistetaan, että arviointilaitosten henkilöstö on soveltuva niihin rooleihin, joihin heitä harkitaan, ja että he säilyttävät kelpoisuutensa ja soveltuvuutensa koko työsuhteen ajan. Korkeakoulut luottavat tähän seikkaan, jossa viranomainen on vahvistanut arviointilaitoksen pätevyyden ja osaamisen arvioida korkeakoulun tietoturvaa ja keskeisiä IT-palveluita, kuten opintotietojärjestelmää.

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

Keskitetty rooli Liikenne- ja viestintävirastolle uusien pätevyysalueiden lisäämisessä on kannatettava, sillä se mahdollistaa hyväksytyille arviointilaitoksille uusien kompetenssien hankkimisen virallisten arviointiprosessien toteuttamiseksi. Arviointilaitokselta edellytettävä, esimerkiksi ISO 27000 -standardisarjan mukainen akkreditointi varmistaa pätevyyksien vertailtavuuden kansainvälisesti toisen maan vastaaviin vaatimuksiin, esimerkiksi tietoturvan johtamisjärjestelmän tai auditoiden kelpoisuusvaatimusten osalta.

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

-

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

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

Korkeakoulun näkökulmasta virallisten arviointilaitosten määrän laajentuminen on positiivinen asia.

Nykyistä laaja-alaisempi arviointilaitosten tarjonta pienentää korkeakoulun keskeisten IT-järjestelmien ja tietoturvan auditointikuluja lisääntyneen tarjonnan myötä. Lisäksi korkeakoululla on mahdollisuus hyödyntää valtion viranomaisen vahvistamaa auditointipalvelua joustavammin, koska palveluntarjoajia on enemmän.

Nykyinen esitys ei kuitenkaan huomioi riittävästi julkisuuslain mukaisten salassa pidettävien tietojen suojaus- ja varautumiskäytäntöjä, vaan keskittyy enemmän turvaluokiteltuun tietoon.

Korkeakouluilla on harvoin hallussaan kansalliseen turvallisuuteen liittyvää turvaluokiteltua tietoa, mutta niiden sensitiivisin tieto on pääasiassa salassa pidettävää tietoa julkisuuslain määrittelemällä tavalla. Julkisuuslain mukaan salassa pidettäviä tietoja ovat, muun muassa:

- potilasasiakirjat,

- tiedot sosiaalihuollon asiakkuudesta,
- psykologiset testit ja soveltuvuuskokeet,
- varautumisasiakirjat,
- opinnäytetöiden ja tieteellisten tutkimusten suunnitelmat ja perusaineistot,
- pääsykoetiedot,
- opiskelua koskevat yksilöivät arvioinnit.

Korkeakoululla on suojattavanaan yllä mainittua tieto-omaisuutta, johon kohdistuu normaalia korkeampi tietoturva- ja varautumiskyvykyys. Virallisia arviointilaitoksia hyödynnetään näiden tietojenkäsittely-ympäristöjen ja tietopalveluiden tietoturvallisuuden arvioinneissa, jotta toivotunlainen suojaustaso voidaan korkeakoulun toimesta saavuttaa.

Saarnia Sanna
Metropolia Ammattikorkeakoulu Oy