Tuomioistuinvirasto

Lausunto

19.01.2026 TIV/1660/2025

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

Turvallisuusluokitus on tiedon ominaisuudesta johtuva tiedon laatijan tai omistajan subjektiivinen näkemys tiedon arvosta, ja sen aiheuttamista haitoista, mikäli se paljastuu asiattomalle.

Tämä on vastaava ominaisuus kuin esimerkiksi henkilötiedon tyyppi, vaikka sille ei ole vastaavanlaista luokittelujärjestelmää luotu.

Tällä luokittelulla ei ole mitään tekemistä sen kanssa, miten luokiteltu tieto tai sitä käsittelevä järjestelmä olisi kriittinen tilanteessa, johon vaadittaisiin varautumista. Tällä ei ole suoranaista yhteyttä siihen mitä toiminta edellyttää tällaisessa tilanteessa. Varautumisen tarkoituksena, kun on varmistaa toiminnan, toiminnan edellytysten sekä toimintakyvyn ylläpitäminen. Turvallisuusluokitus ei käsittele näitä asioita. Välttämättä ei varautuminen edes edellytä tietojärjestelmiä vaan toiminnan luonne voi tarjota muita vaihtoehtoja.

Tietoturvallisuudella tarkoitetaan perinteisesti tiedon, tiedon käsittelyn ja tietojärjestelmien luottamuksellisuutta, saatavuutta sekä eheyttä. Turvallisuusluokittelu näkee vain luottamuksellisuuden suureena, jopa niin että se asettaa muut ominaisuudet varjoonsa – tuntuu kuin ei olisi väliä, vaikka tieto ei olisi saatavilla eikä sitä ylläpidettäisi kuten tulisi.

Useimman erilaisen organisaation, kuten myös esimerkiksi tuomioistuinten, toiminnan ja sen jatkuvuuden kannalta saatavuus ja eheys huomattavasti keskeisemmässä asemassa, kuin koskaan tiedon tai sen käsittelyn luottamuksellisuus. Eheyden osalta oleellinen kysymys on, voidaanko luottaa siihen, että tieto ja päätös ovat oikeita, muuttumattomia ja todistettavia. Perustuvatko nämä tietoon, joka on kontekstissaan eheää. Ja vastaavasti saatavuuden osalta, onko tieto käytettävissä silloin, kun laki ja prosessit sitä edellyttävät.

Varautumisen menetelmät ja tarpeet lähtevät organisaation toiminnasta. Tämän tarpeen muodostaminen arviointikriteeristöksi ei käytännössä ole mahdollista. Organisaatio muodostaa ja huolehtii varautumisestaan itse omasta toimintakyvystään sekä omista hallintatoimistaan priorisoiden tehtäviään ja toimintaedellytysten käyttöä. Tätä ei ulkopuolinen arvioija kykene järkevästi tehdä. Tästä syystä on hyvä asia, että itsearvioinnin mahdollisuus kirjataan myös lakiin.

Laajentamista koskemaan myös varautumista ei voida suoraan nähdä johtavan muuhun kuin kustannusten nousuun sekä järjestelmien käyttöönoton pitkittymiseen. Itse tarkoitus, eli varautumiskyvyn parannukseen ei arviointien tekemisellä ole kuin marginaalista vaikutusta. Vaikutus on silloin lähinnä konsultaatiota antava. Tämän voi organisaatio toteuttaa monella muullakin tavalla.

Toiminnan sekä sen edellytysten ja toimintakyvyn säilyttämisen onnistuminen selviää todellisuudessa vain tilanteessa, johon varaudutaan. Harjoittelulla sekä organisaation tekemillä simulaatioilla voidaan parhaiten kehittää kykyä toimia.

Ei sinänsä ole huono asia, mikäli esimerkiksi Liikenne- ja viestintävirasto tai jokin muu taho tuottaisi erilaisia listoja tukemaan varautumisen suunnittelua ja toteuttamista. Tosin näiden tulisi olla huomattavasti laajempia kuin vain tietotekniikkaan ja tiedon käsittelyyn keskittyviä, koska vaikka ollaan usein hyvinkin riippuvaisia näistä, eivät ne loppujen lopuksi tarvitse olla toiminnassa ratkaisevassa asemassa, varsinkaan lyhyellä aikaperspektiivillä.

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

Turvaluokittelu ei kuvaa tarvetta varautumiseen, ellei jälkimmäisellä tarkoiteta sitä, että varaudutaan suojaamaan luokiteltua tietoa. Toiminnan kannalta ei lisäyksellä turvallisuutta parantavaa merkitystä. Voi olla kustannusvaikutuksia.

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

4§ Kuten edellä, turvallisuuskriittinen (vain luottamuksellisuus!) ei välttämättä ole toimintakriittistä.

6§: Kohdassa määritetään asiantuntijalle oikeus tehdä järjestelmiin myös teknisiä arviointitoimenpiteitä. Tässä yhteydessä tulee myös säätää arviointia tekevän vastuusta ja mahdollisen aiheutetun vahingon korvaamisesta.

Kriittisten järjestelmien kaikkinainen muuttaminen ja samalla alustalla ajettavat ohjelmat tulee olla selkeästi testatut ja muutoshallintaprosessin kautta järjestelmään tuodut. Mikäli arvioijille annetaan oikeus suorittaa omia käskyjä tai ajoja, rikotaan hallinnointiprosesseja, joiden tehtävänä on varmistaa järjestelmän eheys. Eli tämän tulisi arvioissa merkitä vakavaksi havainnoksi.

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

7§ Arviointiperusteista.

Lähtökohtana kaikelle arvioinneille ja niiden sisältämille vaatimuksille tulee asettaa organisaation riskienhallinnan. Kaikki käytettävät kontrollit tulee hyvin rakennetussa turvallisuusarkkitehtuurissa olla johdettavissa organisaation toiminnasta sekä tarpeesta edellyttää joitain toimenpiteitä. Sekä myös toisin päin. Jokainen käytettävä kontrolli ja toimenpide pitää voida perustella organisaation toiminnasta ja sen tarpeesta.

Toiminnasta irrallisesti luotuja ”temppulistoja” ja niiden käyttöä auditoinnin tarkastuslistoina ei tulisi tehdä. Turvallisuuden kannalta kokonaisuus ja sen toimivuus on tärkeämpää kuin komponentit, josta se koostuu.

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

Arviointia suorittavalle asiantuntijalle tulee asettaa vaatimukset osaamisesta.

Arviointitoimien aiheuttamisien suorien kustannusten kohdistumisesta ja toimien vastuusta tulee säätää.

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

-

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

-

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

10§ Arviointiperusteista.

Lähtökohtana kaikelle arvioinneille ja niiden sisältämille vaatimuksille tulee asettaa organisaation riskienhallinnan. Kaikki käytettävät kontrollit tulee hyvin rakennetussa turvallisuusarkkitehtuurissa olla johdettavissa organisaation toiminnasta sekä tarpeesta edellyttää joitain toimenpiteitä. Sekä myös toisin päin. Jokainen käytettävä kontrolli ja toimenpide pitää voida perustella organisaation toiminnasta ja sen tarpeesta.

Toiminnasta irrallisesti luotuja ”temppulistoja” ja niiden käyttöä auditoinnin tarkastuslistoina ei tulisi tehdä. Turvallisuuden kannalta kokonaisuus ja sen toimivuus on tärkeämpää kuin komponentit, josta se koostuu.

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

Pyydämme kirjoittamaan lausuntonne tähän/ Skriv ert utlåtande här

-

Helaskoski Kimmo
Tuomioistuinvirasto - Riskienhallintapäällikkö