

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Keskisuuri yritys

1.2 Pääasiallinen toimialanne

Muu kuin KTL:n liitteissä tarkoitettu toimiala

1.3 KTL:n mukainen toimijatyyppi

Keskeinen toimija

2. Lain soveltaminen ja velvoitteiden selkeys

2.1 Miten ymmärrettävästi riskienhallintaa ja raportointia koskevat velvoitteet on säädetty KTL-laissa?

3

2.2 Kuinka selkeinä pidätte lain velvoitteita organisaationne näkökulmasta?

4

2.3 Arvio viranomaisohjeistuksen riittävydestä ja selkeydestä

Ohjeistus on riittävää joiltain osin

2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:

-

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

5 = erittäin merkittävä vaikutus

3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne

4

3.3 Arvioikaa lain toimeenpanon vaikutuksia: Toimintaan vaikuttavien häiriöiden väheneminen organisaatiossanne

3

3.4 Arvioikaa lain toimeenpanon vaikutuksia: Yhteistyön lisääntyminen viranomaisten kanssa riskienhallinnassa

4

3.5 Arvioikaa lain toimeenpanon vaikutuksia: Kumppanuus- ja toimitusketjuriskien hallinnan parantuminen organisaatiossanne

4

3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta

Kyberturvallisuuden näkyvyyden lisääntyminen johdon tasolla. Vastuiden ja toimintamallien selkeytyminen.

3.7 Kuvaus merkittävimmistä haasteista tai kielteisistä vaikutuksista, joita olette havainneet lain toimeenpanosta

Euroports Finland Oy toimii osana kansainvälistä konsernia, jossa kyberturvallisuuden hallinta, politiikat ja valvonta toteutetaan keskitetysti. Suomen kansallisten NIS2-vaatimusten yhteensovittaminen konsernin toimintamallien kanssa on aiheuttanut lisäselvitystarpeita sekä paikallisella että konsernitasolla.

3.8 Missä määrin arvioitte, että edellä kuvatut vaikutukset johtuvat nimenomaan KTL-laista?

4

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

-

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

4

4.1 Avoin tarkennus:

-

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

Merkittävät

4.2 Avoin tarkennus:

-

4.3 Miten arvioitte KTL-lain soveltamisen aikaista investointien tasoa kyberturvallisuuden kehittämiseen organisaatiossanne?

Kohtalaiset

4.3 Avoin tarkennus:

-

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

4

5.1 Avoin tarkennus:

-

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

3

5.2 Avoin tarkennus:

Ilmoittaminen on selkeää ja helppoakin. Missä menee raja milloin poikkeama on merkittävä on vaikeammin tulkittava asia.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

4

5.3 Avoin tarkennus:

-

6. Lain tavoitteiden toteutuminen

6.1 Arvio KTL-lain tavoitteiden toteutumisesta: Kyberturvallisuuden tason nousu organisaatiossanne

4

6.2 Arvio KTL-lain tavoitteiden toteutumisesta: Toimintaan vaikuttavien poikkeamien ennaltaehkäisy organisaatiossanne

3

6.3 Arvio KTL-lain tavoitteiden toteutumisesta: Organisaationne resilienssin paraneminen

4

6.4 Arvio KTL-lain tavoitteiden toteutumisesta: Riskienhallinnan kehitys organisaatiossanne

6.5 Arvio KTL-lain tavoitteiden toteutumisesta: Raportoinnin laadun parantuminen organisaatiossanne

3

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Kyberturvallisuusriskit käsitellään osana organisaation riskienhallintaprosessia, ja niiden merkitys liiketoiminnan jatkuvuudelle tunnustetaan aiempaa systemaattisemmin.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

NIS2-direktiivin kansalliset toimeenpanot eroavat jäsenvaltioiden välillä, mikä aiheuttaa haasteita konsernitason toimintamallien ja paikallisten vaatimusten yhteensovittamisessa.

7. Kyberturvallisuuslain ajantasaisuus, oikeasuhtaisuus ja kehittämistarpeet

7.1 Vastaako laki nykyisiin kyberuhkiin ja teknologiseen kehitykseen?

4

7.2 Onko lainsäädäntöön tarpeen tehdä muutoksia?

Ei

7.2 Jos kyllä, miten kehittäisitte sääntelyä?

-

7.3 Minkälaisia KTL:n velvoitteet ovat suhteessa arvioonne toimialanne riskeistä ja organisaationne resursseista?

3

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisuudesta ja kehittämistarpeista

Sääntelyä voidaan pääosin pitää ajantasaisena ja tarkoituksenmukaisena. Käytännön toimeenpanossa haasteita aiheuttavat kuitenkin kansallisten tulkintojen ja viranomaiskäytäntöjen erot eri EU-maissa. Kansainvälisissä konserneissa tämä voi johtaa tilanteeseen, jossa samoja NIS2-vaatimuksia joudutaan toteuttamaan ja dokumentoimaan osittain eri tavoin eri jäsenvaltioissa.

Kansainvälisten organisaatioiden näkökulmasta olisi myös hyödyllistä, että kyberturvallisuuslaista ja siihen liittyvistä viranomaisohjeista olisi saatavilla viralliset englanninkieliset versiot. Nykytilanteessa suomalaisen lainsäädännön ja viranomaisvaatimusten tulkitseminen sekä viestiminen konsernitason asiantuntijoille aiheuttaa ylimääräistä työtä ja lisää tulkintariskejä organisaatioissa, joissa kyberturvallisuuden hallinta toteutetaan kansainvälisesti.

7.4 Näettekö vaihtoehtoisia sääntely- tai ohjauskeinoja, jotka voisivat toimia paremmin kuin nykyinen malli?

-

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

-

Kärkkäinen Jari
Euroports Finland Oy