Anh Tran

Lausunto

16.05.2026

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Muu

1.2 Pääasiallinen toimialanne

Muu kuin KTL:n liitteissä tarkoitettu toimiala

1.3 KTL:n mukainen toimijatyyppi

Ei KTL:n soveltamisalaan kuuluva vastaaja

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?

3

2.3 Arvio viranomaisohjeistuksen riittävyydestä ja selkeydestä

Ohjeistus on riittävää joiltain osin

2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:

Kyberturvallisuuslain tavoitteita ja yleistä rakennetta voidaan pitää pääosin selkeinä, ja sääntely vastaa pitkälti NIS2-direktiivin keskeisiä tavoitteita. Riskienhallintaa ja raportointia koskevat velvoitteet ovat kuitenkin osittain yleisluonteisia, mikä jättää käytännön soveltamisessa tulkintavaraa.

Erityisesti seuraavat osa-alueet ovat aiheuttaneet epäselvyyttä:

merkittävän poikkeaman arviointikriteerit,

toimitusketjuriskien hallinnan käytännön laajuus,

johdon vastuiden konkreettinen sisältö,

sekä velvoitteiden suhteuttaminen organisaation kokoon ja toiminnan kriittisyyteen.

Viranomaisohjeistus on tukenut toimeenpanoa, mutta käytännön soveltamista helpottaisi nykyistä yksityiskohtaisempi toimialakohtainen ohjeistus sekä esimerkkitapaukset erityisesti raportointivelvollisuuksista ja riskienhallinnan vähimmäistasosta.

Lisäksi olisi hyödyllistä varmistaa mahdollisimman yhdenmukaiset tulkintakäytännöt eri valvontaviranomaisten välillä.

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

4

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

3

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

4

3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta

Lain toimeenpano on lisännyt organisaatioiden tietoisuutta kyberriskeistä ja vahvistanut riskienhallinnan systemaattisuutta. Erityisesti:

johdon osallistuminen kyberturvallisuuden hallintaan,

dokumentoitujen riskienhallintamenettelyjen kehittäminen,

sekä toimitusketjujen arviointi

ovat monissa organisaatioissa vahvistuneet.

Laki on myös lisännyt kyberturvallisuuden näkyvyyttä osana organisaatioiden jatkuvuudenhallintaa ja strategista johtamista.

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

Keskeisiä haasteita ovat olleet:

velvoitteiden tulkinnanvaraisuus,

raportointivelvoitteiden käytännön soveltaminen,

resurssitarpeiden kasvu,

sekä toimitusketjuihin liittyvien vaatimusten hallinta.

Erityisesti pienemmille organisaatioille sääntelyn toimeenpano voi muodostaa suhteellisen raskaan hallinnollisen kokonaisuuden.

Lisäksi joidenkin velvoitteiden suhde olemassa oleviin tietoturva- ja jatkuvuusvaatimuksiin on jäänyt osittain epäselväksi.

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

4

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

Vaikutukset johtuvat merkittävältä osin juuri KTL-laista ja siihen liittyvästä NIS2-sääntelyn toimeenpanosta. Vaikka kyberturvallisuuden kehittäminen oli monissa organisaatioissa käynnissä jo ennen lain voimaantuloa, laki on lisännyt kehittämistoimien systemaattisuutta, johdon sitoutumista sekä dokumentointi- ja raportointivaatimuksia.

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

4

4.1 Avoin tarkennus:

Hallinnollinen taakka on lisääntynyt erityisesti:

dokumentointivaatimusten,

riskienhallintaprosessien,

toimitusketjuarviointien,

sekä raportointivelvoitteiden vuoksi.

Lisäksi henkilöstön koulutukseen ja sisäisten toimintamallien kehittämiseen on tarvittu aiempaa enemmän resursseja.

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

Kohtalaiset

4.2 Avoin tarkennus:

Kustannuksia on aiheutunut erityisesti:

asiantuntijapalveluista,

tietoturvakartoituksista,

teknisistä suojausratkaisuista,

sekä henkilöstön koulutuksesta.

Kustannusten taso vaihtelee kuitenkin merkittävästi organisaation koon ja lähtötason mukaan.

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

Merkittävät

4.3 Avoin tarkennus:

Lain toimeenpano on lisännyt investointeja erityisesti:

valvonta- ja tunnistusjärjestelmiin,

jatkuvuudenhallintaan,

varautumiseen,

sekä toimitusketjujen turvallisuuden arviointiin.

Investoinnit ovat osaltaan vahvistaneet organisaatioiden kykyä tunnistaa ja hallita kyberuhkia.

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

-

5.1 Avoin tarkennus:

Ilmoitusprosessi toimii pääosin kohtuullisesti, mutta käytännön menettelyissä on edelleen kehittämistarpeita erityisesti:

ilmoitusten yhdenmukaisuudessa,

aikataulujen tulkinnassa,

sekä eri viranomaisten roolien selkeydessä.

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

3

5.2 Avoin tarkennus:

Merkittävän poikkeaman määrittelyyn liittyy edelleen tulkinnanvaraisuutta. Käytännössä organisaatiot joutuvat tekemään tapauskohtaista arviointia siitä, milloin ilmoituskynnys ylittyy.

Lisäohjeistus konkreettisista esimerkkitilanteista olisi hyödyllistä.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

4

5.3 Avoin tarkennus:

Viranomaisten tuella ja ohjeistuksella on ollut tärkeä rooli lain toimeenpanossa. Erityisen hyödyllisiä ovat olleet:

yleiset soveltamisohjeet,

koulutustilaisuudet,

sekä yhteistyöverkostot.

Jatkossa toimialakohtainen ohjeistus ja käytännön esimerkit voisivat edelleen parantaa toimeenpanon yhdenmukaisuutta.

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

4

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

4

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Parhaiten ovat toteutuneet:

riskienhallinnan systematisointi,

johdon sitoutumisen vahvistuminen,

sekä kyberturvallisuuden integrointi osaksi organisaation jatkuvuudenhallintaa.

Laki on myös lisännyt kyberturvallisuuden näkyvyyttä strategisella tasolla.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

Heikoimmin ovat toteutuneet:

velvoitteiden yhdenmukainen tulkinta,

raportointikynnyksen selkeys,

sekä toimialakohtaisen soveltamisen ennakoitavuus.

Osin tämä liittyy siihen, että laki on vielä suhteellisen uusi ja soveltamiskäytäntö on vasta muodostumassa.

7. Kyberturvallisuuslain ajantasaisuus, oikeasuhtaisuus ja kehittämistarpeet

7.1 Vastaako laki nykyisiin kyberuhkiin ja teknologiseen kehitykseen?

4

7.2 Onko lainsäädäntöön tarpeen tehdä muutoksia?

Kyllä

7.2 Jos kyllä, miten kehittäisitte sääntelyä?

Jatkossa olisi hyödyllistä:

täsmentää raportointikynnyksiä,

selkeyttää toimitusketjuvastuiden laajuutta,

sekä lisätä toimialakohtaisia soveltamisohjeita.

Lisäksi olisi tärkeää arvioida jatkuvasti:

tekoälyyn liittyviä kyberriskejä,

pilvipalveluiden turvallisuutta,

sekä kansainvälisiin palveluketjuihin liittyviä riippuvuuksia.

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

3

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisudesta ja kehittämistarpeista

Sääntelyä voidaan pitää pääosin ajantasaisena ja tavoitteiden kannalta perusteltuna. Velvoitteiden käytännön toteuttaminen voi kuitenkin olla raskasta erityisesti keskisuurille ja pienemmille toimijoille.

Jatkossa olisi hyödyllistä painottaa:

riskiperusteisuutta,

suhteellisuusperiaatetta,

sekä toimialakohtaisia erityispiirteitä.

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

Pelkkää velvoitesääntelyä täydentäisivät hyvin:

vapaaehtoiset kyberturvallisuuden kehittämismallit,

toimialakohtaiset suositukset,

sertifiointimallit,

sekä viranomaisten ja toimialojen yhteiset harjoitukset ja yhteistyöverkostot.

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

Kyberturvallisuuslain tavoitteita voidaan pitää yhteiskunnan toimintavarmuuden näkökulmasta tärkeinä ja perusteltuina. Laki on lisännyt kyberturvallisuuden painoarvoa organisaatioiden johtamisessa ja riskienhallinnassa.

Jatkokehittämisessä olisi kuitenkin tärkeää:

varmistaa sääntelyn ennakoitavuus ja oikeasuhtaisuus,

kehittää viranomaisohjeistuksen käytännönläheisyyttä,

sekä huolehtia siitä, ettei hallinnollinen kuormitus muodostu suhteettomaksi erityisesti pienemmille toimijoille.

Lisäksi olisi hyödyllistä seurata aktiivisesti EU-tason sääntelyn kehitystä ja varmistaa kansallisen sääntelyn yhteensopivuus muun digitaalisen sääntelyn kanssa.

Anh Tran
YDHV lakitiimi