

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Suuri yritys

1.2 Pääasiallinen toimialanne

Terveys

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?

4

2.2 Kuinka selkeinä pidätte lain velvoitteita organisaationne näkökulmasta?

4

2.3 Arvio viranomaisohjeistuksen riittävydestä ja selkeydestä

Kyllä, ohjeistus on riittävää

2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:

-

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

3

3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne

3

3.3 Arvioikaa lain toimeenpanon vaikutuksia: Toimintaan vaikuttavien häiriöiden väheneminen organisaatiossanne

1 = ei vaikutusta

3.4 Arvioikaa lain toimeenpanon vaikutuksia: Yhteistyön lisääntyminen viranomaisten kanssa riskienhallinnassa

1 = ei vaikutusta

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

2

3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta

Ylimmän johdon ja koko henkilöstön tietoturvakoulutukset.

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

Ei ole havaittu.

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

5 = erittäin merkittävä vaikutus

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

Ennen lain voimaantuloa aihetta pidettiin runsaasti esillä, erityisesti erilaisten kaupallisten toimijoiden esityksissä, joiden taustalla todennäköisesti konsulttityön myymismotivaatio. Se toi kyberturvallisuudelle näkyvyyttä.

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

3

4.1 Avoin tarkennus:

Erilaisista häiriöistä tuli uusi ilmoitusvelvollisuus siten, että jokaisesta häiriöstä tehtävä yhdeksän viranomaisilmoitusta (kolme valvovaa viranomaista, joista kullekin tulee tehdä kolme ilmoitusta).

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

-

4.2 Avoin tarkennus:

Säätelyn noudattaminen itsessään tuo lähinnä hallinnollista työtä. HUSin toiminnan ja potilaiden yksityisyyden suojan turvaaminen edellyttävät joka tapauksessa panostamista tietoturvallisuuteen/kyberturvallisuuteen.

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

Kohtalaiset

4.3 Avoin tarkennus:

Taloussuunnittelu hyvinvointialueilla ja hyvinvointiyhtymissä tehdään n. 1,5 vuotta etukäteen. Siten lain voimassaoloaikana tehdyt investointisuunnitelmat eivät ole vielä käytössä ennen vuotta 2027 ja vuoden 2027 budjettia ei ole vielä vahvistettu. HUSin osalta suunniteltu investointibudjetti on tehty muun tarvearvioinnin kuin KTL-lain pohjalta, eikä siihen ole tehty lain pohjalta erikseen muutoksia.

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

3

5.1 Avoin tarkennus:

NIS2 ilmoituskaavakkeen tiedot eivät mene yhdellä kaavakkeella suoraan kaikille viranomaisille, mm FIMEAlle pitää erikseen lähettää kaavakkeen tiedot sähköpostilla.

5.2 Ilmoittamista koskevan veloitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

4

5.2 Avoin tarkennus:

-

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

2

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

2

6.3 Arvio KTL-lain tavoitteiden toteutumisesta: Organisaationne resilienssin paraneminen

2

6.4 Arvio KTL-lain tavoitteiden toteutumisesta: Riskienhallinnan kehitys organisaatiossanne

2

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

2

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Tietoturvatietoisuuden parantaminen riskienhallintakeinona, joka johtaa parempaan kyberturvallisuuden tasoon. Henkilöstön kouluttaminen suuressa organisaatiossa on iso kustannus ja lain vaatimus tuo asiaan selkeän selkänöjan.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

Tieto/kyberturvallisuuden kehittäminen on pitkäjänteistä työtä, jota HUSissa on tehty pitkään. Tämä työ on jo ennestään sisältänyt paljon kyberturvallisuuslain mukaisten riskienhallintatoimenpiteiden rakentamista. HUS tietohallinnolla on myös jo vuosia ollut ISO27001-sertifikaatti. Merkittävien parannusten tekeminen laajassa organisaatiossa on hidasta, eikä lain voimassaoloaikana ole havaittu juurikaan selkeitä lain vaatimusten perusteella toteutettuja toimenpiteitä, joita ei muuten olisi tehty.

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?

Poikkeamailmoitusprosessi tulisi virtaviivaistaa siten, että eri valvoville viranomaisille tehtävät ilmoitukset tulisi määrätä samaan kanavaan ja siten, että ilmoitukset jaetaan viranomaisten toimesta tarvittaville viranomaisille. Muita ilmoituksia, kuten rikosilmoituksen sekä ilmoitus tietosuojavaltuutetun toimistolle tulisi myös yhdistää samaan ilmoitukseen. Lisäksi terveyssektorilla on merkittävä määrä muuta ilmoitusvelvollisuutta erilaisista häiriöistä ja nämä sektorikohtaiset ilmoitusvelvollisuudet tulisi pystyä tekemään samoilla ilmoituksilla. Tavoite ilmoitusten tekoprosessia määriteltäessä tulisi olla viranomaisten tiedonsaantinäkökulman lisäksi se, että poikkeaman kohteena olevan organisaation toimintaa ei poikkeamatilanteessa rasiteta ylimääräisillä ilmoitusvaatimuksilla, vaan organisaation tulisi pystyä tilanteessa keskittymään itse poikkeamatilanteen hallitsemiseen.

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

4

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisuudesta ja kehittämistarpeista

Lain lähtökohta, jossa riskienhallinta on pohja hallintakeinojen valintaan, on ajantasainen ja oikeasuhtainen. Se ei myöskään vanhene kovinkaan nopeasti.

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

-

Karvo Jouni
HUS-Yhtymä