

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Muu

1.2 Pääasiallinen toimialanne

Julkishallinto

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?

4

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:

Lain soveltaminen ja velvoitteet ovat suhteellisen selkeitä. Lainsäädännön lisäksi käytännön toiminnan tueksi on kuitenkin tärkeää saada myös tarkentavaa viranomaisohjeistusta.

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

2

3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne

2

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

3

3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta

Positiivisena vaikutuksena on havaittu muun ohella lainsäädännön tasoinen tuki vaatimusten esittämiseen, joka näkyy positiivisesti toimitusketjuissa. Toisin sanoen lain toimeenpano on helpottanut jossain määrin yhteistyötä muiden toimijoiden kanssa.

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

Lain toimeenpanon ei ole havaittu aiheuttavan kielteisiä vaikutuksia.

Yhtenä haasteena on koettu olemassa olevien sopimusten läpikäynti sekä mahdollinen päivittäminen, johon julkishallinnossa voi liittyä edellytys uudelleenkilpailutukselle.

Koemme haasteellisena myös kyberturvallisuuslain (julkishallinnon osalta tiedonhallintalain 4 a luku) sekä lakisääteisten yhteisten palvelujen yhteensovittamisen. Toisin sanoen kyberturvallisuuslaki asettaa meille kyberturvallisuutta koskevia velvollisuuksia, joita meidän täytyy toiminnassamme noudattaa. Samaan aikaan olemme lain nojalla velvollisia käyttämään tiettyjä yhteisiä palveluja, joiden sisältöön emme kuitenkaan useinkaan voi vaikuttaa.

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

2

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

Huomiona, että kaikissa vastauksissa (3.1 - 3.5) on jo huomioitu nimenomaan kyberturvallisuuslain vaikutukset.

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

3

4.1 Avoin tarkennus:

Uusi ilmoituskanava, joita odotetaan jatkossa tulevan vielä lisää, on lisännyt hallinnollista taakkaa, joka heijastuu myös kasvavina kustannusvaikutuksina. Toisaalta DigiOmnibus-ehdotuksen odotetaan vähentävän hallinnollista taakkaa, mikäli useat ilmoituskanavat saadaan yhdistettyä yhdeksi.

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

-

4.2 Avoin tarkennus:

Kustannusten määrää ei ole mahdollista arvioida tällaisessa aikataulussa.

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

-

4.3 Avoin tarkennus:

Emme ymmärtäneet, mitä kysymyksellä haetaan. Näin ollen emme osaa arvioida.

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

4

5.1 Avoin tarkennus:

Ennen kyberturvallisuuslain (julkishallinnon osalta tiedonhallintalain 4 a luku) ei ollut olemassa selkeitä toimintatapoja ja vaatimuksia taikka kanavaa KTK:n suuntaan tehtäville ilmoituksille.

Nettilomake ei kuitenkaan ole yhdenmukainen muiden ilmoituskanavien kanssa, joka lisää osaltaan hallinnollista taakkaa.

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

3

5.2 Avoin tarkennus:

Ilmoitusvelvollisuus itsessään on selkeä, mutta merkittävän poikkeaman määritelmään liittyy edelleen tulkinnanvaraisuuksia ja epäselvyyksiä.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

5.3 Avoin tarkennus:

Mikäli kysymyksessä tarkoitetaan kyberturvallisuuslain soveltamiseen liittyvää ohjeistusta, niin se on kehittynyt hieman viiveellä ja on ollut osittain puutteellista. Viranomaisten ohjeistus ja tuki koetaan kuitenkin hyödylliseksi ja niiden tuottamista myös tulevaisuudessa kannatetaan.

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

1 = erittäin vähäinen vaikutus

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

Kysymykset ovat nähdäksemme osittain päällekkäisiä otsikon 3 alla olevien kysymysten kanssa.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

-

7. Kyberturvallisuuslain ajantasaisuus, oikeasuhtaisuus ja kehittämistarpeet

7.1 Vastaako laki nykyisiin kyberuhkiin ja teknologiseen kehitykseen?

3

7.2 Onko lainsäädäntöön tarpeen tehdä muutoksia?

Kyllä

7.2 Jos kyllä, miten kehittäisitte sääntelyä?

Lainsäädäntö on antanut hyvän perustason, mutta toimintaympäristön ja teknologian muutosnopeus vaatii lainsäädännön päivitystarpeen säännöllistä arviointia.

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

5 = oikeasuhtaisia ja toteuttamiskelpoisia

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisuudesta ja kehittämistarpeista

-

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

Lainsäädäntö kykenee vastaamaan ja reagoimaan suhteellisen huonosti nopeasti muuttuviin kyberturvallisuutta koskeviin kysymyksiin, joihin voidaan vastata paremmin esimerkiksi erilaisilla ohjeistuksilla ja suosituksilla. Kannatamme tarkentavien ohjeistusten lisäämistä. Lisäksi valvovalla viranomaisella on mahdollisuus antaa velvoittavia määräyksiä, joiden lisäämistä kannatamme.

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

Lausuntovastauksessa toimialaksi on mahdollista valita julkishallinto, vaikka julkishallinnon osalta vastaavat velvoitteet on säädetty osaksi tiedonhallintalakia, ei kyberturvallisuuslakia. Koska NIS2-direktiivistä johtuvat velvoitteet ovat identtisiä tiedonhallintalaissa ja kyberturvallisuuslaissa, vastaa Verohallinto lausuntopyyntöön julkishallinnon näkökulmasta.

Alakangas Tarja
Verohallinto