Helsingin kaupunki

Lausunto

12.06.2026

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**

-

## 2. Lain soveltaminen ja velvoitteiden selkeys

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

5 = erittäin ymmärrettävästi

**2.2 Kuinka selkeinä pidätte lain velvoitteita organisaationne näkökulmasta?**

4

**2.3 Arvio viranomaisohjeistuksen riittävyydestä ja selkeydestä**

Kyllä, ohjeistus on riittävää

**2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:**

Laki antaa selkeät ohjeet siitä, miten riskienhallintaa ja raportointia voidaan toteuttaa organisaatiossa. Riskienhallinnan toimintamallin ja hallintatoimenpiteiden listaus (9§) on selkeä ja velvoitteet organisaatiolle ovat selkeät ja ymmärrettävät.

## 3. Kyberturvallisuuslain vaikutukset organisaatioonne

**3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne**

3

**3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne**

4

**3.3 Arvioikaa lain toimeenpanon vaikutuksia: Toimintaan vaikuttavien häiriöiden väheneminen organisaatiossanne**

2

**3.4 Arvioikaa lain toimeenpanon vaikutuksia: Yhteistyön lisääntyminen viranomaisten kanssa riskienhallinnassa**

2

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

1 = ei vaikutusta

**3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta**

Positiivisena vaikutuksena on havaittu erityisesti riskienhallinnan parantuminen ja selkeytyminen sekä johdon vastuun määrittely uudistettujen tietoturvalinjausten kautta. Lisäksi poikkeamailmoitukset viranomaisille sekä valvovan viranomaisen rooli ovat nyt selkeämmät kuin aikaisemmin. On myös positiivista, että lain alkuun on laitettu määritelmät, koska laki kattaa laajan joukon toimijoita, jolloin myös yhteentoimivuuden kannalta yhteiset määritelmät auttavat kokonaisuuden ymmärtämisessä. Määritelmistä puuttuu kuitenkin häiriön määritelmä. Laki ei määrittele suoraan mitä tarkoitetaan häiriöllä, vaikkakin sen riskienhallinnan kautta tulee määritellyksi, mutta olisi hyvä, jos laissa olisi määritelty mitä yleisesti tarkoitetaan pienellä häiriöllä tai vakavalla häiriöllä. 11§ annetaan kuitenkin viittaus siihen mitä laaja häiriö voi olla ja se on siinä hyvin määritelty.

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

Merkittäviä haasteita tai kielteisiä vaikutuksia ei lain toimeenpanosta ole havaittu.

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

3

**3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne**

Kyberturvallisuuslain vaikutus organisaatiossa on ollut, että se on tuonut selkeyttä tietoturvan ja kyberturvallisuuden hallintaan. Laki antaa hyvän selkänojan toteuttaa tietoturvallisuutta ja kyberturvallisuutta ja se tukee hyvin tiedonhallintalain velvoitteiden toteuttamista. Kyberturvallisuuslaki on ensimmäinen laki, josta voidaan suoraan nähdä mitä teknisiä ja hallinnollisia velvoitteita organisaation tulee toteuttaa riskienhallinnan kautta ja miten häiriötilanteissa tulee raportointivelvoite täyttää. Laki vaatii tuekseen esim. tiedonhallintalautakunnan suosituksia häiriöiden hallinnasta, mutta jo lain perusteella voidaan arvioida sekä osaamisen, että resurssien tarvetta velvoitteiden toteuttamiseksi.

# 4. Hallinnollinen taakka ja kustannukset

**4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne**

3

**4.1 Avoin tarkennus:**

Lain selkeät velvoitteet ovat mahdollistaneet myös laajemmin tietoturvan ja kyberturvallisuuden ohjeistuksen, joka vaatii hallinnollisia panostuksia ohjeiden tuottamiseen ja päätöksentekoon. Samalla myös riskienhallinnan systematisoiminen on lisännyt hallinnollista taakkaa jonkin verran.

**4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä**

Kohtalaiset

**4.2 Avoin tarkennus:**

Vaikea arvioida, koska Helsingin kaupungissa oli jo aloitettu ennen lain voimaan tuloa laaja tietoturvajohtamisen muutoshanke, jonka kustannuksia ei voi suoraan laskea laista johtuviksi. Laki kuitenkin velvoittaa vastaavien uudistusten tekemistä, joten voidaan sanoa, että ainakin osa uudistuksen kustannuksista on laista johtuvia

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

Erittäin merkittävät

**4.3 Avoin tarkennus:**

Helsingin kaupunki on aloittanut historiansa suurimman tietoturvan kehittämishankkeen missä tietoturvan ja kyberturvallisuuden muutokset ja parantaminen vuosina 2025-2028 ovat merkittäviä sekä toiminnallisesti että kustannuksiltaan.

# 5. Viranomaisyhteistyö ja raportointi

**5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus**

5 = erittäin hyvin toimiva

**5.1 Avoin tarkennus:**

Viranomaisraportointi on kirjattu lakiin hyvin selvästi ja valvovan viranomaisen tehtävä on myös selkeästi lakiin kirjattu.

**5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa**

5 = erittäin täsmällinen

**5.2 Avoin tarkennus:**

Laki on tältä osin selkeä ja ymmärrettävä.

**5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys**

4

**5.3 Avoin tarkennus:**

Viranomaisen tuen suhteen ei ole suoraa kokemusta, joten emme sitä pysty arvoimaan, mutta Kyberturvallisuuskeskus tuottaa hyvää ohjemateriaalia, jota organisaatiossa voidaan hyödyntää. Samoin tiedonhallintalautakunnan tuottamat suositukset ovat laajasti hyödynnettävissä.

## 6. Lain tavoitteiden toteutuminen

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

3

**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**

2

**6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle**

Parhaiten on vaikutusta ollut riskienhallintaan sekä uudistettuihin tietoturvalinjauksiin, jossa tietoturvatyön tavoitteet ovat selkeät. Riskienhallinnan toimintamallin tavoitteet nousevat esille riskien hallintatoimenpiteiden kautta, jotka ovat tietoturvan osalta osittain kytkettynä tietoturvajohtamisen muutoshankkeeseen, jolla tietoturvaa parannetaan systemaattisesti. Myös tietoturvan tilannekuvaa koskeva tavoitteet ovat parantuneet, mutta eivät vielä riittävän hyvällä tasolla.

**6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle**

Heikoimmin on toteutunut tietoturvan raportointiin liittyvät velvoitteet. Tietoturvan raportointiin ei ole vielä vuosikelloa eikä seuranta ole vielä vakiintunut johtamisen toimintatavan ja -kulttuurin osaksi.. Raportoinnin avulla johdon tulisi tehdä tietoturvaa koskevia päätöksiä, mutta se edellyttää raportoinnin lisäksi sitä, että tietoturva otetaan huomioon johtamisen tavoitteissa sekä hankintojen ja projektien alkuvaiheessa.

## 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?**

4

**7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisudesta ja kehittämistarpeista**

Sääntely on onnistunutta ja sen avulla voidaan lain velvoitteet toteuttaa. Riskienhallinta on olennainen osa kaupungin tietoturvallisuutta ja vaikka sen suhteen on joitakin asiantuntijoiden saatavuushaasteita, on riskit kuitenkin hyvin hallinnassa ja riskienhallinta resurssoitu. Riskienhallinnan toimenpiteet (9§) vaativat monenlaista osaamista ja kaikkea ei ole tarkoituksenmukaista toteuttaa omin voimin, mutta lopulta vastuu on aina organisaatiolla ja vastuu edellyttää hallinnollisen vastuun lisäksi teknistä ja toiminnallista vastuuta, jonka kantaminen vaatii monipuolista osaamista ja monipuolisia osaajia sekä selkeän tilannekuvan tuottamista johdolle päätöksenteon tueksi. Kaikki tämä edellyttää vahvaa tietoturvan ja kyberturvallisuuden organisoitumista ja mukanaoloa päätösten teossa.

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

Tietoturvaa koskevien standardien ”pakollisuus” osana kyberturvallisuuslain velvoitteiden toteuttamista voisi vielä kirkastaa lain toimeenpanoa. Asiaa voidaan aina tehostaa sanktioilla, mutta ne ovat reaktiivisia keinoja, kun sen sijaan esim. tietoturvan hallintamallin ISO 27001 tai varautumisen standardi ISO 42001 antavat organisaatiolle hyvän pohjan lain toteuttamiselle konkreettisella tasolla.

## 8. Muut huomiot ja avoin palaute

**8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista**

Ei muita huomioita.

Inkinen Mikael
Helsingin kaupunki - Tietoturvapäällikkö, kaupunginkanslia, digitalisaatio-osasto.