Pohjois-Pohjanmaan hyvinvointialue

Lausunto

02.07.2026

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?

3

2.3 Arvio viranomaisohjeistuksen riittävyydestä ja selkeydestä

Ohjeistus ei ole riittävää

2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:

Ilmoitusvelvollisuuden kriteeristöä tulisi täsmentää, viranomaisohjausta yhdenmukaistaa ja kansallista konkretiaa lisätä, jotta sääntely olisi selkeämpää, paremmin kohdennettua ja käytännössä toteuttamiskelpoisempaa. Tarkennukset kohdassa 5.2.

Samoin riskienhallinnan toimintamallin osalta tulisi määritellä kansallinen, yhtenäinen viitekehys tai mallipohja, joka tukisi käytännön toimeenpanoa ja varmistaisi vaatimustenmukaisuuden yhdenmukaisella tavalla eri toimijoiden välillä sekä vertailtavuuden.

Toimitusketjujen riskienhallinnan käytännön toteuttaminen olisi myös tärkeä ohjeistaa tai vaatia kansallisesti samalla tavalla.

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

2

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

Kyberturvallisuusriskienhallinta osana organisaation normaalia toimintaa on saanut näkyvyyttä ja enemmän roolia. Euroopan komission täytäntöönpanoasetuksessa (EU) 2024/2690 määritellyt toimenpiteet kyberturvallisuuden parantamiseksi ovat antaneet tukea hankintojen vaatimuksien toteuttamiselle.

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

Merkittävän poikkeaman määritelmä jää epäselväksi, tai vastaavasti toimijan tulee ilmoittaa lähes kaikista tuotannollisistakin ICT-häiriöistä, joilla ei varmastikaan ole kansallisesti mitään merkitystä. Lain soveltaminen vaatii jatkuvasti resursseja, joita ei ole lain säätämisen aikana laskettu riittävällä tarkkuudella.

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

4

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

Perusasioiden ollessa kunnossa konkreettiset vaikutukset jäävät pieniksi. Laki antaa kuitenkin hyvää selkänojaa tietojärjestelmätoimittajien laadun parantamiseen ja myös jossain määrin organisaation toimintamallien kehittämiseksi.

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

4

4.1 Avoin tarkennus:

Ilmoitusvelvollisuuden epämääräisyys on lisännyt hallinnollista taakka. Riippuen tulkinnasta tavanomaisesta ICT-häiriöstä, jolla ei ole mitään tekemistä tietoturvan kanssa, tulee ilmoittaa usealle eri viranomaiselle ja vieläpä kolmella eri raportilla.

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

Kohtalaiset

4.2 Avoin tarkennus:

Pääasiassa organisaation omien työntekijöiden muutoksen toteuttamiseen käyttämä työaika.

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

Vähäiset

4.3 Avoin tarkennus:

Lain tullessa voimaan hyvinvointialueen budjetti oli jo suunniteltu ja soveltamisajan jäädessä lyhyeksi laki ei ole vielä vaikuttanut investointien tasoon. Laki, tai tarkemmin Euroopan komission täytäntöönpanoasetus (EU) 2024/2690, keskityy perusasioiden parantamiseen ja niitä kehitystoimenpiteitä olisi toteutettu joka tapauksessa, joten laki itsessään ei ole vaikuttanut investointien tasoon.

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

2

5.1 Avoin tarkennus:

Samalla lomakkeella tulisi pystyä toimittamaan vaadittavat ilmoitukset kaikille virastoille. Mikäli poikkeama on havaittu, käsitelty ja ratkaistu 24 sisällä, tulisi ilmoittajan pystyä raportoimaan poikkeama yhdellä lomakkeella ensi-ilmoituksen, jatko-ilmoituksen ja loppuraportin sijasta.

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

1 = erittäin tulkinnanvarainen

5.2 Avoin tarkennus:

Kyberturvallisuuslain ilmoitusvelvollisuuteen liittyy merkittäviä tulkinta- ja yhdenmukaisuushaasteita, jotka heikentävät sääntelyn käytännön toimivuutta ja aiheuttavat toimijoille epävarmuutta.

Keskeinen ongelma liittyy ilmoituskynnysten epäselvyyteen ja viranomaisten keskinäisiin tulkintaeroihin. Käytännön havaintojen perusteella eri valvovat viranomaiset ohjaavat ilmoittamista eri tavoin: Kyberturvallisuuskeskus ei välttämättä näe tarpeellisena ilmoittaa NIS2-direktiivin perusteella tiettyjä tuotannollisia ICT-häiriöitä, kun taas Lupa- ja valvontavirasto edellyttää ilmoituksia vastaavista tilanteista. Tämä johtaa epäyhtenäiseen raportointikäytäntöön ja lisää toimijoiden hallinnollista taakkaa ilman, että kyberturvallisuuden tilannekuva vastaavasti paranee.

Euroopan komission täytäntöönpanoasetus (EU) 2024/2690 konkretisoi ilmoitusvelvollisuutta, mutta sen soveltaminen hyvinvointialueiden kaltaisessa toimintaympäristössä johtaa käytännössä suureen ilmoitusmäärään. Asetuksen mukaiset merkittävän poikkeaman kriteerit ovat osittain liian laajoja ja tulkinnanvaraisia, minkä seurauksena suuri määrä operatiivisia häiriöitä tulkitaan ilmoitettaviksi tietoturvapoikkeamiksi.

Esimerkiksi asetuksen 37 kohta on ongelmallinen ja osittain päällekkäinen kansallisen sääntelyn kanssa (asiakastietolaki 82 § ja 90 §). Kohta sisältää tulkinnanvaraisen kriteerin poikkeamille, jotka “voivat aiheuttaa luonnollisten henkilöiden kuoleman tai huomattavaa vahinkoa terveydelle”. Tämä määrittely on liian avoin ja altis ylilavealle tulkinnalle, erityisesti sosiaali- ja terveydenhuollon toimintaympäristössä. Vastaavaa epäselvyyttä sisältyy myös asetuksen 39 kohtaan.

Ilmoitusvelvollisuuden kehittämisessä tulisi selkeämmin erottaa toisistaan kyberturvallisuuspoikkeamat, joissa korostuu vihamielinen tai tahallinen toiminta, sekä muut ICT- ja tuotannolliset häiriöt, jotka kuuluvat ensisijaisesti operatiiviseen häiriönhallintaan. Nykyinen sääntely ei riittävästi tue tätä erottelua, mikä heikentää raportoinnin vaikuttavuutta ja viranomaisten tilannekuvan laatua.

Lisäksi sääntelyssä on puutteita konkreettisuudessa ja kansallisen tason ohjauksessa. Euroopan komission täytäntöönpanoasetus (EU) 2024/2690 edellyttää muun muassa tietojärjestelmien turvallisuutta koskevia politiikkoja sekä aihekohtaisia politiikkoja (esimerkiksi pääsynhallinta). Näiden osalta olisi perusteltua luoda kansallisesti yhtenäinen vähimmäistaso joko lainsäädännöllä tai viranomaismääräyksillä, jotta vaatimukset toteutuvat johdonmukaisesti kaikissa organisaatioissa.

Ilmoitusvelvollisuuden kriteeristöä tulisi täsmentää, viranomaisohjausta yhdenmukaistaa ja kansallista konkretiaa lisätä, jotta sääntely olisi selkeämpää, paremmin kohdennettua ja käytännössä toteuttamiskelpoisempaa.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

2

5.3 Avoin tarkennus:

Ei merkittävää haittaa, mutta ei myöskään hyötyä.

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

3

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

2

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Laki on antanut hyvä selkänojan ICT-toimittajien tuotteiden ja toiminnan kyberturvallisuuden parantamiselle. Aiemmin ICT-toimittajat eivät kiinnittäneet välttämättä juurikaan mitään huomiota kyberturvallisuuteen, mutta nyt heidät on pakotettu siihen. Organisaation omassa kokonaisvaltaisessa riskienhallinnassa kyberturvallisuusriskienhallinta on saanut paremmin näkyvyyttä ja roolia.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

Tieto- ja kyberturvallisuuden kehittäminen on pitkäjänteistä työtä, jota Pohteella on tehty jo ennen kyberturvallisuuslain voimaantuloa osana normaalia riskienhallintaa, tietoturvan kehittämistä ja lakisääteisten velvoitteiden täyttämistä. Kyberturvallisuuslain edellyttämät riskienhallintatoimenpiteet ovat suurelta osin linjassa aiemmin toteutettujen käytäntöjen kanssa, eikä lain voimassaoloaikana ole tunnistettu merkittävää määrää sellaisia uusia toimenpiteitä, joita olisi toteutettu yksinomaan lain vaatimusten vuoksi.

Laajassa hyvinvointialueorganisaatiossa muutosten suunnittelu ja käyttöönotto ovat väistämättä pitkäkestoisia prosesseja. Erityisen haastavaa on toimitusketjujen riskienhallinta, sillä Pohteella on satoja erilaisia ICT-, teknologia-, laite- ja palvelusopimuksia. Näiden sopimusten sekä niihin liittyvien

kyberturvallisuusvaatimusten yhdenmukaistaminen ja valvonta edellyttävät merkittävää ja pitkäjänteistä kehitystyötä sekä yhteistyötä toimittajaverkoston kanssa.

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?

Ilmoitusvelvollisuuden kriteeristöä tulisi täsmentää, viranomaisohjausta yhdenmukaistaa ja kansallista konkretiaa lisätä, jotta sääntely olisi selkeämpää, paremmin kohdennettua ja käytännössä toteuttamiskelpoisempaa.

Samoin riskienhallinnan toimintamallin osalta tulisi määritellä kansallinen, yhtenäinen viitekehys tai mallipohja, joka tukisi käytännön toimeenpanoa ja varmistaisi vaatimustenmukaisuuden yhdenmukaisella tavalla eri toimijoiden välillä sekä vertailtavuuden.

Toimitusketjujen riskienhallinnan käytännön toteuttaminen olisi myös tärkeä ohjeistaa tai vaatia kansallisesti samalla tavalla.

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

5 = oikeasuhtaisia ja toteuttamiskelpoisia

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisudesta ja kehittämistarpeista

Sääntely kyberturvallisuuden alalla on tarpeellista ja näkisin, että tarvitsemme enemmän selkeitä pakottavia ja kansallisesti yhtenäisiä vaatimuksia. Hyvinvointialueiden taloustilanne on hankala ja tämä voi aiheuttaa ristiriitaisen tilanteen kyberturvallisuuslain noudattamisessa ja muiden lakisääteisten tehtävien hoitamisessa. Mitä enemmän pakottavia vaatimuksia on, sitä vähemmän toimijoiden tarvitsee neuvotella organisaation sisällä siitä, mitkä ovat tarpeellisia toimenpiteitä ja mitkä eivät. Eri hyvinvointialueet voivat nähdä tarpeelliset toimet eri tavalla riippuen siitä, mikä on taloustilanne ja millaiset henkilöt vastaavat kyberturvallisuudesta tai johtavat organisaatiota.

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

Valvovan viranomaisen pitäisi pystyä tekemään konkreettisia auditointeja lakia vastaan, jotta saisimme palautetta ja varmistettua kansallisesti, että toimenpiteet todellakin ovat toimeenpantu.

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

-

Borén Markku
Pohjois-Pohjanmaan hyvinvointialue

Huhtala Anssi
Pohjois-Pohjanmaan hyvinvointialue - Tietoturvapäällikkö