Google

Lausunto

26.06.2026

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Suuri yritys

1.2 Pääasiallinen toimialanne

Digitaalinen infrastruktuuri

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?

-

2.2 Kuinka selkeinä pidätte lain velvoitteita organisaationne näkökulmasta?

-

2.3 Arvio viranomaisohjeistuksen riittävyydestä ja selkeydestä

-

2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:

-

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

-

3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne

-

3.3 Arvioikaa lain toimeenpanon vaikutuksia: Toimintaan vaikuttavien häiriöiden väheneminen organisaatiossanne

-

3.4 Arvioikaa lain toimeenpanon vaikutuksia: Yhteistyön lisääntyminen viranomaisten kanssa riskienhallinnassa

-

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

-

3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta

Google kiittää mahdollisuudesta saada antaa palautetta liikenne- ja viestintäministeriölle kyberturvallisuuslain (124/2025) täytäntöönpanosta ja vaikutuksista. Euroopan unionin laajuisena sähköisten viestintäpalvelujen (ECS) tarjoajana olemme sitoutuneet NIS2-direktiivin tavoitteisiin ja korkean tietoturvatason varmistamiseen. Toimintakokemuksemme perusteella haluamme antaa palautetta, joka keskittyy erityisesti auditointivelvoitteisiin, rajat ylittävään sääntely-yhteistyöhön ja poikkeamien raportointijärjestelmiin.

1. Riskipohjaisten auditointimekanismien tukeminen

Kannatamme vahvasti sitä käytännönläheistä lähestymistapaa, jota Suomessa on noudatettu NIS2-direktiivin saattamisessa osaksi kansallista lainsäädäntöä ulkoisen validoinnin ja auditointien osalta. Välttämällä pakollisia, toistuvia itsearviointeja tai auditointeja ja varaamalla auditoinnit sen sijaan tiettyihin tilanteisiin (kuten 30 §:n mukaisiin merkittäviin tapahtumiin) Suomen sääntelykehys noudattaa oikeasuhteista, riskilähtöistä lähestymistapaa.

Tämä lähestymistapa edistää virtaviivaista sääntöjen noudattamisympäristöä, joka minimoi hallinnollisen päällekkäisyyden. Asettamalla etusijalle käytännön turvallisuutta koskevat lopputulemat varmistetaan, että organisaation toimet ovat täysin linjassa kyberkestävyyden parantamisen päätavoitteen kanssa, ja tuetaan periaatetta, jonka mukaan sääntöjen noudattamisen puitteiden tulisi mahdollistaa, eikä vaikeuttaa, aktiivisten uhkien torjuntaa ja ennakoivia turvallisuusparannuksia. Suhtaudumme myönteisesti tähän kantaan ja suosittelemme sitä parhaaksi käytännöksi.

2. Sääntely-yhteistyö ja rajat ylittävä yhdenmukaistaminen

Nykyinen EU:n kyberturvallisuusympäristö on hajanainen, erityisesti 27 jäsenvaltion erilaisten auditointi- ja arviointivaatimusten osalta. Päällekkäisten toimien estämiseksi ja yhdenmukaisen sääntöjen noudattamisen varmistamiseksi kannatamme yhdenmukaistettua sääntelylähestymistapaa.

Google tukee erityisesti keskitetyn auditointikehyksen käyttöönottoa. Tämä malli antaisi organisaatioille mahdollisuuden hyödyntää olemassa olevia, kansainvälisesti tunnustettuja vaatimustenmukaisuusinvestointeja, kuten ISO/IEC 27001 -standardin mukaista tietoturvan hallintajärjestelmää (ISMS) keskitettynä lähtökohtana, ja suorittaa lisäarviointeja erityisten kansallisten vaatimusten osalta vain silloin, kun se on ehdottomasti tarpeen. NIS2-direktiivin 25 artiklan ja johdanto-osan 80 kohdan nojalla jäsenvaltioilla ja komissiolla on selkeä mandaatti koordinoida yhtenäisiä auditointiohjeita. Google kannustaa ottamaan käyttöön ohjeita, joissa tunnustetaan, että vankat, jo olemassa olevat sertifioinnit täyttävät 21 artiklan riskienhallinnan perusvaatimukset.

Tehokkaan sääntely-yhteistyön edistämiseksi kannatamme voimakkaasti sitä, että NIS2-säännösten noudattamisen valvonta ja yhteisten auditointilaajuuksien sopimus sidotaan EU:n päätoimipaikan jäsenvaltioon (Googlen tapauksessa Irlantiin). Kannustamme Traficomia hyödyntämään NIS2:n mukaisia sääntely-yhteistyömekanismeja tukeakseen päävalvontaviranomaisen valvonnassa suoritettujen keskitettyjen auditointien vastavuoroista tunnustamista. Tämä lähestymistapa vähentää merkittävästi teknisten tiimien sääntelytaakkaa, optimoi rajat ylittävän toiminnan ja varmistaa yhdenmukaisen korkean turvallisuustason koko EU:ssa.

3. Poikkeamien raportointi

Päättämällä sovittaa poikkeamien raportointirajoja direktiivin mukaisiksi sen sijaan, että olisi otettu käyttöön jäykkiä ja mielivaltaisia numeerisia raja-arvoja, Suomi on osoittanut esimerkillistä lähestymistapaa kyberkestävyyden hallintaan. Sen sijaan, että organisaatioita pakotettaisiin navigoimaan maakohtaisten mittareiden monimutkaisessa labyrintissä – kuten tarkat laskelmat yhteyskatkoksia kokevien käyttäjämäärien osuuksista – Suomen viitekehys perustuu merkittävän poikkeaman laadulliseen arviointiin.

Tällaisista mielivaltaisista kansallisista vertailuarvoista luopuminen antaa palveluntarjoajille mahdollisuuden sovittaa poikkeamanhallintaprosessinsa saumattomasti yhteen komission yleisten standardien kanssa, minkä ansiosta organisaatiot voivat keskittää resurssinsa varsinaiseen torjuntaan. Tekniset tiimit voivat asettaa riskienhallinnan etusijalle mittareiden kynnysarvojen laskemisen sijaan.

Lopuksi

Google kiittää Suomen tasapainoista sääntelykehystä ja odottaa innolla yhteistyön jatkumista, jotta näitä riskilähtöisiä ja yhdenmukaistettuja parhaita käytäntöjä voidaan edistää laajemmin Euroopan digitaalisen ekosysteemin piirissä.

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

-

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

-

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

-

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

-

4.1 Avoin tarkennus:

-

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

-

4.2 Avoin tarkennus:

-

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

-

4.3 Avoin tarkennus:

-

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

-

5.1 Avoin tarkennus:

-

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

-

5.2 Avoin tarkennus:

-

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

-

5.3 Avoin tarkennus:

-

6. Lain tavoitteiden toteutuminen

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

-

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

-

6.3 Arvio KTL-lain tavoitteiden toteutumisesta: Organisaationne resilienssin paraneminen

-

6.4 Arvio KTL-lain tavoitteiden toteutumisesta: Riskienhallinnan kehitys organisaatiossanne

-

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

-

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

-

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?

-

7.2 Onko lainsäädäntöön tarpeen tehdä muutoksia?

-

7.2 Jos kyllä, miten kehittäisitte sääntelyä?

-

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

-

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisudesta ja kehittämistarpeista

-

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

-

Jern Heidi
Google