



Kirje

8.10.2025

 VN/784/2025
 VN/784/2025-VM-3

Jakelun mukaisesti

EU:n kyberturvallisuusedirektiivin hyödyntäminen kunnissa

Tausta

EU:n kyberturvallisuusedirektiivin (NIS2-direktiivi) tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa. Direktiivissä osoitetaan yhteiskunnan kriittisille sektoreille kyberturvallisuutta vahvistavia riskienhallintavelvollisuuksia sekä merkittäviä poikkeamia koskevia raportointivelvollisuuksia.

Tukea NIS2-direktiivin toimeenpanoon löytyy Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen (KTK) [verkkosivuilta](#). Viranomaiset ovat järjestäneet toimeenpanosta sidosryhmätilaisuuksia. Valtiovarainministeriö lähetti kirjeen julkisen hallinnon toimijoille NIS2-direktiivin kansallisesta toimeenpanosta 4.4.2025. Tämä kirje täydentää julkiselle hallinnolle lähetettyä kirjettä kuntasektorin näkökulmasta. Kuntia pyydetään välittämään kirje myös liikelaitoksiinsa ja omistamiinsa yhtiöihin sekä muihin yhteisöihin.

Kuntasektorin toimijoiden kuulumisesta NIS2-direktiivin soveltamisalaan

NIS2-direktiivi on pantu kansallisesti täytäntöön direktiivin julkinen hallinto -toimialaan kuuluvien toimijoiden osalta säätämällä **julkisen hallinnon tiedonhallinnasta annettuun lakiin** (906/2019, jatkossa tiedonhallintalaki) uusi 4 a luku sekä muiden toimialojen toimijoiden osalta säätämällä edellytetyistä velvollisuuksista keskitetysti uudessa **kyberturvallisuuslaissa** (124/2025). Muutokset tiedonhallintalakiin ja kyberturvallisuuslaki tulivat voimaan 8.4.2025. Tiedonhallintalain 4 a luvun ja kyberturvallisuuslain vaatimukset ovat yhtenevät.

Kuntia ei ole direktiivin kansallisessa toimeenpanossa sisällytetty julkinen hallinto -toimialaan. Siten uusia kyberturvallisuusvelvoitteita ei sovelleta kuntiin viranomaisina eivätkä tiedonhallintalain 4 a luvun vaatimukset koske kuntia lukuun ottamatta Helsingin kaupunkia, johon sovelletaan 4 a lukua sen hoitaessa hyvinvointialueiden

Postiosoite
 Postadress
 Postal Address
 Valtiovarainministeriö

PL 28
 00023 Valtioneuvosto

Käyntiosoite
 Besöksadress
 Office

Snellmaninkatu 1 A
 Helsinki

Puhelin
 Telefon
 Telephone

0295 16001
 +358 295 16001

Faksi
 Fax
 Fax

s-posti, internet
 e-post, internet
 e-mail, internet

kirjaamo.vm@gov.fi

järjestämisvastuulle lailla säädettyjä tehtäviä. Kunta, kuntayhtymä, kunnallinen liikelaitos tai kunnan yksin tai yhdessä muiden kuntien kanssa omistama yhtiö tai muu yhteisö voi kuitenkin tarjota kyberturvallisuuslain soveltamisalaan kuuluvia palveluita, jolloin toimija saattaa tulla uusien velvoitteiden soveltamisalan piiriin. Lisäksi vaikka kunta ei kuuluisi kyberturvallisuuslain soveltamisalaan, niin se voi toimia palveluntarjoajana soveltamisalaan kuuluvalla toimijalla, esimerkiksi IT- palveluntarjoajana vesihuoltolaitokselle. Tällöin soveltamisalaan kuuluvan toimijan tulee varmistaa, että kunnan tarjoama palvelu on huomioitu kyberturvallisuuslain mukaisessa riskienhallinnassa ja riskienhallintatoimenpiteissä lain edellyttämällä tavalla.

Kyberturvallisuuslain **soveltamisalaan** kuuluvat NIS2-direktiivissä määriteltyjen toimialojen suuret ja keski-suuret toimijat. Suuren toimijan palveluksessa on vähintään 250 työntekijää tai sen vuosiliikevaihto ylittää 50 miljoonaa euroa ja taseen loppusumma ylittää 43 miljoonaa euroa. Keski-suuren toimijan palveluksessa on 50–249 työntekijää tai vuosiliikevaihto ja taseen loppusumma ylittävät 10 miljoonaa euroa. Toimijoiden, myös kunnallisten monialatoimijoiden, tulee itse arvioida, kuuluvatko ne soveltamisalaan ja mikä viranomainen heitä valvoo.

Kyberturvallisuuslain soveltamisalaan kuuluvat lisäksi kaikki CER (Critical Entities Resilience) -direktiivin mukaan määritellyt kriittiset toimijat riippumatta toimijan koosta. CER-direktiivi eli **kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi** on pantu kansallisesti täytäntöön lailla yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (310/2025). Kunkin CER-direktiivin toimialan¹ vastuuministeriö määrittää kriittiset toimijat sektorikohtaisesti. Ministeriön päätös kriittisistä toimijoista tulee tehdä ensimmäisen kerran 17.7.2026 mennessä.

NIS2-direktiivin toimialoista erityisesti **vesi-, jäte- ja energiahuolto** ovat toimialoja, joihin liittyvien palvelujen tuotannosta kunnat vastaavat. NIS2-direktiivin toimialojen toimijoihin kohdistuu kokokriteerejä siten, että vain suurimmat toimialojen yhteisöt ja toiminnot kuuluvat sääntelyn soveltamisalaan. Kyberturvallisuuslain 4 §:n 6 momentin mukaan lakia sovelletaan kuntalaissa (410/2015) tarkoitettuun kuntaan vain liitteessä I tai II tarkoitettun toiminnan osalta. Soveltamisalaan kuulumisen kriteerit määritellään siten, että tunnuslukuja tarkastellaan kunnan sisällä toimivan liikelaitoksen / taseyksikön, kuntayhtymän tai kuntaomisteisen yhteisön osalta. Soveltamisalaan kuulumisen arvioinnissa ei siten tarkastella yhtiömuotoisen toiminnan osalta koko kuntakonsernin tunnuslukuja eikä kunnan alla tapahtuvan toiminnan, kuten liikelaitokset ja taseyksiköt, kohdalla koko peruskunnan tunnuslukuja. Esimerkiksi vesihuoltosektorilla kyberturvallisuuslain soveltamisalaan kuuluu noin 30 vesihuoltolaitosta Suomen yli tuhannesta vesihuoltolaitoksesta. Ne ovat kaikki valvojan viranomaisen tiedossa ja informoitu. Jätehuollossa on suuria yhtiöitä, joilla on useita pieniä kuntia omistajana.

NIS2-direktiivin edellyttämistä toimenpiteistä

Tiedonhallintalain 4 a luvun tai kyberturvallisuuslain soveltamisalaan kuuluvien toimijoiden on laadittava kyberturvallisuuden **riskienhallinnan toimintamalli** ja käytävä läpi tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi säädetyt riskienhallintatoimenpiteet ja toteutettava ne riskienhallinnan perusteella omassa toiminnassaan. Lisäksi nämä toimenpiteet tulee dokumentoida riskienhallinnan toimintamalliin. Toimintamalliin muodostavista asiakirjoista ja muista tiedoista muodostuu toimijalle uusi hallittava tietoaaineisto ja velvollisuus ylläpitää tietoaaineistoa. Tiedonhallintalain 4 a luvun tai

¹ [Vastauksia kysymyksiin CER-laista - Sisäministeriö](#)

kyberturvallisuuslain soveltamisalaan kuuluvan tiedonhallintayksikön tulee sisällyttää tai liittää kyberturvallisuuden riskienhallinnan toimintamalli osaksi tiedonhallintamalliaan².

Kyberturvallisuuslain 10 §:n 2 momentin mukaan toimijan johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan. Lain 32 §:n 1 momentissa säädetään johdon toiminnan rajoittamismahdollisuudesta eli siitä, että valvova viranomainen voi kieltää määrääjäksi henkilöä toimimasta keskeisen toimijan hallituksen jäsenenä tai varajäsenenä, hallintoneuvoston jäsenenä tai varajäsenenä, toimitusjohtajana tai muussa siihen rinnastettavassa asemassa, jos tämä on toistuvasti ja vakavasti rikkonut 10 §:ssä säädettyjä velvollisuuksia. Lain 32 §:n 2 momentin mukaan johdon toimintaa ei kuitenkaan saa rajoittaa, jos kyse on esimerkiksi kunnallisesta viranomaisesta.

Kyberturvallisuuslain 5 luvussa säädetään hallinnollisesta seuraamusmaksusta. Seuraamusmaksua ei lain 35 §:n 2 momentin mukaan voi määrätä esimerkiksi kunnallisille viranomaisille. Säännöksen perustelujen mukaan: *”Kunnallisella viranomaisella tarkoitetaan kunnan tai kuntayhtymän toimielimiä, kunnan liikelaitosta sekä kunnan taseyksikköä. Rajoitus koskisi kuitenkin vain julkishallinnon toimijoita, eli esimerkiksi vesihuoltopalvelua tarjoavan, kunnan omistamalle osakeyhtiölle hallinnollisen seuraamusmaksun voisi määrätä samalla tavalla, kuin muillekin lain soveltamisalaan kuuluville osakeyhtiöille.”*

Soveltamisalaan kuuluvan toimijan on huomioitava, että kyberturvallisuuslain 11-13:ssä veloitetaan toimija **ilmoittamaan merkittävästä poikkeamasta** valvovalle viranomaiselle ja lain 14 §:ssä säädetään lisäksi ilmoitusvelvollisuudesta asiakkaille sekä yleisestä tiedotusvelvollisuudesta.

Tieto- ja kyberturvallisuus kuntasektorilla

Kuntien tiedonhallintaan liittyvistä **tietoturvallisuusvaatimuksista** säädetään tiedonhallintalain 4 luvussa, joka on jatkossakin olennaisin kuntien tietoturvallisuutta sääntelevä yleislaki. Valtiovarainministeriön yhteydessä toimivan [Tiedonhallintalautakunnan](#) tehtävänä on edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tiedonhallintalain vaatimusten toteuttamista. Tiedonhallintalautakunnan suositukset tukevat tiedonhallintalain 4 luvun tietoturvallisuutta koskevien vaatimusten toteuttamisessa.

Kuntien näkökulmasta tiedonhallintalain tietoturvallisuuteen liittyvien vaatimusten - eli lähinnä lain 4 luvun - ja kyberturvallisuuslain kyberturvallisuusvaatimusten välinen olennaisin ero on se, että kyberturvallisuuslain kyberturvallisuuden riskien hallintatoimenpiteet ovat yksityiskohtaisempia kuin tiedonhallintalain 4 luvun tietoturvallisuuteen liittyvät vaatimukset. Kyberturvallisuusvaatimuksiin sisältyvät riskienhallinnan veloitteet aiheuttavat jonkin verran muutoksia tiedonhallintaan.

Vaikka kunta, sen toiminto tai sen omistama yhteisö ei kuuluisikaan NIS2-direktiivin soveltamisalaan, niin niiden on **suositeltavaa tutustua NIS2-direktiivin** kyberturvallisuusvaatimuksiin ajankohtaisina kyberturvallisuuden ylläpitämisen ja kehittämisen hyvinä käytänteinä ja toteuttaa vaatimukset toiminnassaan.

² https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_57+2024.pdf

Kyberturvallisuuden olennainen merkitys on huomioitu Euroopan unionin tasolla. EU on rakentanut eurooppalaista kyberturvallisuutta kehittävän ja tukevan säädöskokonaisuuden, jonka olennaisimpiin säädöksiin NIS2-direktiivi lukeutuu. **EU arvioi ja kehittää** direktiivin soveltamista ja sisältöä pitkäjänteisesti. Toisin kuin Suomessa, useissa verrokki-maissamme kuten Ruotsissa ja Tanskassa kunnat kuuluvat NIS2-direktiivin soveltamisalaan. Näiden maiden kokemuksia pyritään hyödyntämään myös Suomen kyberturvallisuuslainsäädännön toimeenpanon kehittämisessä jatkossa.

Tukea tieto- ja kyberturvallisuuden toteuttamiseen

Kyberturvallisuuskeskus tarjoaa palveluita tieto- ja kyberturvallisuuden edistämiseksi kuntasektorilla. Valtiovarainministeriö suosittelee Kyberturvallisuuskeskuksen [Hyöky-palvelun](#) ja [Havaro-palvelun](#) käyttöönottoa. Hyöky-palvelu auttaa organisaatioita ennakkoimaan tietoturva- ja kyberuhkia kartoittamalla niiden digitaalista hyökkäyspinta-alaa. Hyöky-palvelua tarjotaan veloituksetta julkisen hallinnon toimijoille. Havaro-palvelu tunnistaa ja hälyttää vakavista tietoturvauhista. Hyöky-palvelun ja Havaro-palveluun käyttöönottoa tulisi harkita osana kokonaisvaltaista tieto- ja kyberturvallisuuden kehittämistä.

Valtiovarainministeriö suosittelee hyödyntämään tieto- ja kyberturvallisuuden kehittämisessä **Digi- ja väestötietoviraston (DVV)** tarjoamia palveluja. Liitteenä on DVV:n valmis-telema muistio: Vinkkejä kyber- ja digiturvan kehittämiseen syksyllä 2025. Julkisen hallinnon toimijoita pyydetään harkitsemaan liittymistä **Digiturvan kokonaiskuvapalveluun**, jonka avulla voi arvioida, seurata ja raportoida hallinnollisen kyberturvallisuuden tilannekuvaa sekä suunnitella toimenpiteitä sen edelleen kehittämiseksi. Julkri-työkalut ovat hyödynnettävissä asetettaessa tietojärjestelmän hankintavaatimuksia ja tietoturvallisuuden vaatimustenmukaisuuden arviointivaatimuksia.

Marraskuussa 2025 järjestetään jo kahdeksas **Taisto-harjoitus**, jossa organisaatiot voivat turvallisesti harjoitella toimintaa poikkeamatilanteissa ja siten varmistaa myös valmiutensa uusien NIS2-direktiin mukaisten raportointivaatimusten noudattamiseen. Organisaatiot ja asiantuntijat voivat kehittää kyberturvallisuutta ja siihen liittyvää osaamistaan hyödyntämällä Suomi.fi-kehittäjille -alustan **Digiturvan tietopankkia**. Tietopankkiin on koottu eri viranomaisten ja muiden toimijoiden tuottamia hyödyllisiä työkaluja, materiaaleja sekä palveluita kyberturvallisuuden kehittämiseen. **VAHTI-asiantuntijaverkoston** työryhmissä pääsee jakamaan ja saamaan tietoa sekä vertaistukea oman ja organisaation toiminnan kehittämiseen. Lisätietoa palveluista löytää DVV:n [verkkosivuilta](#) sekä [palveluhakemistosta](#).

ICT-johtaja, ylijohtaja

Jarkko Levasma

Tietohallintoneuvos

Tuija Kuusisto

Jakelu	Kunnat, pl Ahvenanmaa
Tiedoksi	Valtiovarainministeriö
	ELY Kyberturvallisuus Jätehuolto
	ELY Kyberturvallisuus Vesihuolto
	Liikenne- ja viestintävirasto
	Kuntaliitto

VN/784/2025-VM-3

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons: