FiCom ry | Janne Hälinen
7.4.2026

FiComin lausunto valtioneuvoston kirjelmästä U 17/2026 vp

Ehdotukset Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi

FiCom ry:n lausunto suurelle valiokunnalle valtioneuvoston kirjelmästä U 17/2026 vp, joka koskee komission 20.1.2026 antamia ehdotuksia Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) sekä NIS 2 -direktiivin muuttamisesta.

FiComin jäsenyritykset ovat keskeisiä toimijoita NIS 2 -direktiivin liitteissä I ja II tarkoitetuilla kriittisillä sektoreilla, erityisesti sähköisten viestintäverkkojen ja -palveluiden tarjoajina. Sääntely vaikuttaa siten välittömästi jäsentemme toimintaedellytyksiin, investointiympäristöön ja kilpailukykyyn.

FiCom pitää valtioneuvoston U-kirjelmässä esitettyjä päälinjauksia pääosin asianmukaisina ja tukee EU-tasoisten kyberturvallisuusrakenteiden kehittämistä. Kirjelmässä on kuitenkin eräitä avoimia kohtia, joihin valiokunnan on perusteltua kiinnittää huomiota omassa lausunnossaan.

FiComin keskeiset viestit

- ICT-toimitusketjuja koskevien rajoitusten ja teknisten velvoitteiden on oltava riskiperusteisia, oikeasuhtaisia ja teknisesti toteuttamiskelpoisia. Verkkolaitteiden elinkaari sekä palvelujen kapasiteetti ja jatkuvuus on otettava huomioon siirtymäaikoja ja velvoitteita asetettaessa.

- Komissiolle siirrettävän täytäntöönpanovallan on oltava tarkkarajaista. Täysharmonisoivat täytäntöönpanosäädökset riskienhallintatoimenpiteistä ovat ongelmallisia ja edellyttävät neuvotteluissa kriittistä arviointia.

- ENISA:lle ja komissiolle osoitettaviin tiedonluovutusvelvoitteisiin on sovellettava tietojen minimointia ja korkeaa luottamuksellisuussuojaa, mukaan lukien kriittistä verkkoarkkitehtuuria koskevat tiedot.

- Kyberturvallisuussertifioinnin käytännön pakollistumista on vältettävä. Sertifioinnin edellyttäminen vaatimustenmukaisuuden osoittamiseksi on sidottava asianmukaiseen vaikutusarviointiin ja riskiperusteiseen tarveharkintaan.

- Komission henkilöstöresurssien merkittävä lisäys ja ehdotuksen laaja komitologiamenettelyjen käyttö korostavat valmistelun läpinäkyvyyden ja toimialan asiantuntemuksen merkitystä.

1. ICT-toimitusketjujen tekninen toteutettavuus ja oikeasuhtaisuus

FiCom pitää hyvänä, että valtioneuvoston kanta korostaa ICT-toimitusketjuja koskevien toimenpiteiden riskiperusteisuutta ja oikeasuhtaisuutta. Kirjelmä jää kuitenkin tältä osin yleiselle tasolle eikä ota riittävästi kantaa käytännön toimeenpanon kannalta keskeisiin kysymyksiin.

Ehdotuksen mukaan matkaviestinverkkojen korkean riskin toimittajien ICT-komponentit tulisi vaihtaa 36 kuukauden kuluessa komission listan julkaisemisesta. Kiinteiden viestintäverkkojen ja satelliittiviestintäverkkojen siirtymäajat täsmennettäisiin myöhemmin täytäntöönpanoasetuksilla. Muutosten toteuttamisessa tulee huomioida verkkojen teknistaloudelliset ja toiminnalliset tekijät, kuten verkkolaitteiden elinkaari, sekä turvallisuustilanne. Sääntely ei saa vaarantaa palvelujen kapasiteettia, laatua tai jatkuvuutta. Tähän liittyy myös perustuslain 15 §:ssä turvatun omaisuudensuojan kannalta merkityksellisiä kysymyksiä, jotka kirjelmä tunnistaa mutta joihin valtioneuvoston kanta ei erikseen ota kantaa.

Komissio ei kirjelmän mukaan ole arvioinut EU-tasoisia korvausjärjestelyjä, jotka liittyisivät korkean riskin toimittajien komponenttien pakkovaihtoon. Myöskään muiden NIS 2 -direktiivin toimialojen kustannusvaikutuksia ei ole arvioitu riittävästi. Tämä on merkittävä puute.

Rajoituksia ja siirtymäaikoja koskevien täytäntöönpanoasetusten valmistelussa on varmistettava jäsenvaltioiden ja toimialan asianmukainen kuuleminen sekä läpinäkyvät tekniset ja taloudelliset vaikutusarvioinnit. Sääntelyn ennakoitavuus on edellytys sille, ettei viestintäpalvelujen kapasiteetti, laatu tai jatkuvuus vaarannu.

FiCom esittää, että valiokunta kiinnittää lausunnossaan huomiota siihen, että valtioneuvoston on neuvotteluissa varmistettava verkkolaitteiden elinkaaren huomioiminen siirtymäaikoja asetettaessa, läpinäkyvät vaikutusarvioinnit sekä toimialan kuuleminen ennen rajoittavia täytäntöönpanoasetuksia.

2. Komission täytäntöönpanovalta ja kansallinen liikkumavara

CSA2-ehdotus ja NIS 2 -muutosdirektiivi lisäävät merkittävästi komissiolle siirrettävää säädösvaltaa. Kirjelmässä todetaan perustellusti, että komissiolle delegoitavien toimivaltuuksien tulisi olla tarkkarajaisia, oikeasuhtaisia, tarkoituksenmukaisia ja perusteltuja. FiCom katsoo kuitenkin, että tätä linjausta on tarpeen vahvistaa.

NIS 2 -muutosdirektiivissä komissiolle ehdotetaan mahdollisuutta antaa riskienhallintatoimenpiteistä täysharmonisoivia täytäntöönpanosäädöksiä. Tämä poikkeaisi NIS 2

-direktiivin luonteesta vähimmäisharmonisoivana säädöksenä ja kaventaisi merkittävästi jäsenvaltioiden liikkumavaraa. Kirjelmä suhtautuu tähän alustavan varauksellisesti. FiCom pitää perusteltuna, että valtioneuvoston kanta muotoillaan neuvotteluissa tältä osin selkeämmin.

Lopullisessa kirjelmässä komissiolle ehdotettu henkilöstölisäys on kasvanut luonnoksen 8 henkilötyövuodesta 50 henkilötyövuoteen. Merkittävä osa lisäresursseista kohdistuu ICT-toimitusketjujen riskiarviointeihin ja sertifiointeihin, eli juuri niihin toimintoihin, joissa komissio käyttää teknistä säädösvaltaa. Tämä korostaa jäsenvaltioiden osallistumisen ja toimialan asiantuntemuksen merkitystä.

Kirjelmä toteaa lisäksi, että ehdotus sisältää huomattavan määrän täytäntöönpanosäädöksiä, joita valmisteltaisiin komitologiamenettelyissä. Teknisten täytäntöönpanoasetusten markkinavaikutukset voivat olla välittömiä, minkä vuoksi valmistelun läpinäkyvyys, perustelut ja toimialan kuuleminen ovat olennaisia.

FiCom esittää, että valiokunta kiinnittää lausunnossaan huomiota siihen, että valtioneuvoston on neuvotteluissa suhtauduttava kriittisesti täysharmonisoiviin täytäntöönpanosäädöksiin riskienhallintatoimenpiteistä, varmistettava ENISA:n, jäsenvaltioiden ja toimialan asiantuntemuksen hyödyntäminen komission teknisten säädösten valmistelussa sekä huolehdittava siitä, että komissiolle siirrettävä täytäntöönpanovalta on tarkkarajaista ja komitologiamenettelyt läpinäkyviä.

3. Tietojen minimointi ja luottamuksellisuussuoja

CSA2-ehdotus laajentaa merkittävästi tiedonluovutusvelvoitteita suhteessa ENISA:an, komissioon ja kansallisiin valvontaviranomaisiin. Sääntely vaikuttaa suoraan viestintäverkkojen tarjoajiin, jotka ovat NIS 2 -direktiivin keskeisiä toimijoita.

Valtioneuvoston kanta ei sisällä nimenomaisia kirjauksia tietojen minimoinnista eikä kriittistä verkkoarkkitehtuuria koskevien tietojen erityisestä suojaamisesta. FiCom pitää tätä olennaisena puutteena.

Kirjelmässä todetaan, että ENISA:n vahvempi rooli valvonnan tukena edellyttäisi jäsenvaltioilta lisääntynyttä raportointia ja voisi kuormittaa viranomaisia. Vastaava kuormitus kohdistuu kuitenkin myös yrityksiin. Tiedonluovutusvelvoitteiden tulee koskea vain lainsäädännön tarkoituksen kannalta välttämättömiä tietoja, ja niihin on sovellettava korkeaa luottamuksellisuussuojaa, mukaan lukien liike- ja ammattisalaisuuksien suoja.

Erityisen tärkeää on varmistaa, ettei sääntelyn toimeenpano edellytä verkkoarkkitehtuurin tai muiden kriittisten teknisten yksityiskohtien tarpeettoman yksityiskohtaista luovuttamista. Tällaisen tiedon laajamittainen kerääntyminen EU-tason rakenteisiin voi itsessään muodostaa kyberturvallisuusriskin.

FiCom esittää, että valiokunta kiinnittää lausunnossaan huomiota siihen, että valtioneuvoston on neuvotteluissa varmistettava tietojen minimointi ja korkea luottamuksellisuussuoja, mukaan lukien verkkoarkkitehtuuriin liittyvät tiedot, sekä se, ettei tiedonluovutusvelvoitteista muodostu yrityksille kohtuutonta hallinnollista taakkaa.

4. Sertifiointikehyksen kustannukset ja soveltamisalan hallinta

Valtioneuvoston kanta pitää lähtökohtaisesti hyvänä, että eurooppalaisten kyberturvallisuussertifiointijärjestelmien mukaisia sertifiointeja voitaisiin hyödyntää NIS 2 -direktiivin asettamien vaatimusten täyttämisen osoittamisessa. Sertifiointia on kuitenkin arvioitava huolellisesti myös sen käytännön vaikutusten kannalta.

NIS 2 -muutosdirektiivin mukaan jäsenvaltiot voisivat edellyttää toimijoita hankkimaan sertifioinnin vaatimustenmukaisuuden osoittamiseksi. Sertifioinnin hankkineeseen toimijaan ei lisäksi kohdistettaisi säännöllisiä turvallisuusauditointeja. Tämä luo rakenteen, jossa sertifioinnista voi muodostua käytännössä pakollinen: ilman sertifikaattia toimija voi altistua jatkuvalle valvonnalle, jonka kustannukset voivat ylittää sertifioinnin hankkimisen kustannukset.

Komission arvion mukaan kybertason sertifiointi maksaa yritykselle noin 30 000 euroa sertifiointia kohti. Lisäksi sertifiointijärjestelmien kehittäminen rahoitettaisiin ainakin osin ENISA:n keräämillä maksuilla. Näiden kustannusvaikutusten kokonaisarviointi jää kirjelmässä puutteelliseksi.

FiCom korostaa, että sertifiointivaatimusten on oltava aidosti riskiperusteisia. Sertifiointijärjestelmää ei tule käyttää epäsuorana keinona de facto -pakollisiin sertifiointeihin tai muihin markkinoihin olennaisesti vaikuttaviin velvoitteisiin ilman asianmukaista vaikutusarviointia ja riskiperusteista tarveharkintaa.

FiCom esittää, että valiokunta kiinnittää lausunnossaan huomiota siihen, että sertifioinnin hyödyntäminen vaatimustenmukaisuuden osoittamisessa on sidottava asianmukaiseen vaikutusarviointiin. Lisäksi on varmistettava, ettei sertifioinnista muodostu epäsuoraa pakkoa eikä siitä aiheudu toimijoille kohtuuttomia kustannuksia.

Lopuksi

FiCom pitää valtioneuvoston U-kirjelmässä esitettyjä linjauksia yleisesti oikeansuuntaisina. Kirjelmässä on kuitenkin avoimia kohtia, joihin valiokunnan on perusteltua kiinnittää huomiota eduskunnan EU-valvonnan puitteissa. Sääntelyn tulee olla riskiperusteista, ennakoitavaa ja oikeasuhtaista. Sen on tuettava viestintäpalveluiden jatkuvuutta ja toimintavarmuutta sekä oltava sopusoinnussa perusoikeusjärjestelmän, erityisesti omaisuudensuojan ja elinkeinovapauden, sekä jäsenvaltioiden toimivallan kanssa.