FiCom ry | Asko Metsola
11.2.2022

FiComin lausunto NIS 2.0 -jatkokirjeestä

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt FiComilta lausuntoa valtioneuvoston jatkokirjelmästä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi (COM (2020) 823 final) kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja direktiivin 2016/1148 kumoamisesta (verkko- ja tietoturvadirektiivi). FiCom kiittää mahdollisuudesta tulla kuulluksi ja esittää kunnioittavasti seuraavaa:

FiComin keskeiset viestit

- Direktiiviehdotus on kehittynyt oikeaan suuntaan, mutta kansallinen liikkumavara on silti tärkeää.
- Päällekkäistä sääntelyä ja raportointia on vältettävä.
- Kansallisten ja EU-viranomaisten toimivaltuuksien rajat tulee määritellä tarkasti.
- Direktiivin voimaansaattamiseksi annettu lisäaika on välttämätön.

FiCom kiinnitti aiemmassa, komission ehdotuksesta antamassaan lausunnossa huomiota muun muassa ehdotetun sääntelyn soveltamisalan epäselvyyteen, velvoitteiden epäsuhtaisuuteen, päällekkäiseen sääntelyyn ja raportointiin sekä sektori- ja toimijakohtaisten erityispiirteiden huomioimiseen. Onkin hyvä, että ehdotukseen sisällytettiin muutoksia, joilla vahvistetaan velvoitteiden oikeasuhtaisuutta, riskiperustaisuutta ja kriittisyyden arviointia. Suomen kanta ja kansallinen pyrkimys vaikuttaa soveltamisalan selkeyteen ovat koko käsittelyn ajan olleet kannatettavia.

Kansallinen liikkumavara soveltamisalan ja seuraamusjärjestelmän osalta on tärkeää. Mikäli Suomi kuitenkin haluaa ottaa käyttöön muita toimenpiteitä ja lainsäädännöllisiä muutoksia, jotka takaavat direktiiviehdotuksen minimitasoa korkeamman kyberturvallisuustason, tulee niissä huomioida sektori- ja toimijakohtaiset erityispiirteet.

On hyvä, että ehdotuksessa on selkeytetty sääntelyn suhdetta muuhun lainsäädäntöön, joka koskee direktiiviehdotuksen soveltamisalaan kuuluvia toimijoita. Tällaista on erityisesti tietosuojalainsäädäntö sekä eräät keskeneräiset säädösehdotukset, jotka liittyvät läheisesti direktiiviehdotukseen. Erityisesti suuriin toimijoihin kohdistuu tulevaisuudessa velvoitteita lukuisista muistakin säädöksistä, jolloin sääntelykokonaisuudella voi olla jo kilpailullisiakin vaikutuksia.

Alkuperäisessä ehdotuksessa esitettiin velvoitteiden laiminlyönnistä huomattavia hallinnollisia sanktioita. FiCom pitää oikeansuuntaisena, että hallinnollisia sanktioita on madallettu alkuperäisestä ehdotuksesta.

Kompromissitekstiin tehdyt muutokset raportointivelvoitteisiin ovat kannatettavia. Vapaaehtoisen kyberuhista raportoinnin lisäksi on hyvä, että ehdotuksessa kannustetaan jäsenvaltioita sellaisiin kansallisiin ratkaisuihin, jotka virtaviivaistavat raportointia ja joilla vältetään päällekkäinen raportointi. On myös hyvä, että toimijoilla on raportointivelvoitteiden ohella mahdollisuus vapaaehtoisesti ilmoittaa havainnoistaan,

uhkista ja häiriöistä. Tiukan ilmoitusvelvollisuuden sijaan tulee tarkemmin arvioida, mitkä häiriöt ja uhat ovat sellaisia, että niistä tarvitsee ylipäätään ilmoittaa valvontaviranomaiselle.

FiCom kannattaa direktiivin johdanto-osan 56 kappaleessa mainittua keskitettyä asiointikanavaa (single entry point). Keskitetty asiointikanava ilmoituksille on välttämätön, koska jo nyt lainsäädäntö velvoittaa tiukkoihin määräaikoihin. Jos joistain tilanteista on velvollisuus ilmoittaa kahdelle tai jopa kolmelle eri viranomaiselle, se on pystyttävä tekemään kaikille samalla kertaa ja samojen määräaikojen mukaisesti. Nykyisellään palveluntarjoajat joutuvat esimerkiksi yleisestä tietosuoja-asetuksesta aiheutuvan ilmoitusvelvollisuuden vuoksi ilmoittamaan tietoturvaloukkauksista useammalle viranomaiselle. Tämä lisää hallinnollista taakkaa tilanteessa, jossa voimavarat tulisi kohdistaa tietoturvaloukkauksen selvittämiseen. Keskitetty asiointikanava vähentäisi myös palveluntarjoajille uudesta sääntelystä aiheutuvia kustannuksia. Päällekkäistä sääntelyä ja raportointia tulee välttää.

On askel oikeaan suuntaan, että ehdotuksessa komission toimivaltaa on rajattu niin, että komissio voisi antaa ainoastaan täytäntöönpanosäädöksiä, jotka liittyvät riskienhallintatoimenpiteiden ja raportoinnin teknisiin ja metodologisiin tarkennuksiin. Tämä ei kuitenkaan ota huomioon yrityksissä riskienhallinnasta säännöllisesti käytävää tapauskohtaista arviointia. Keinojen ja teknologioiden tulee jäädä toimijoiden itsensä valittaviksi. Kansallisten ja EU-viranomaisten toimivaltuuksien rajat tulee määritellä tarkasti, ja niissä on vältettävä päällekkäisyyttä.

Kompromissitekstin mukaan NIS2-direktiivi tulee saattaa osaksi kansallista lainsäädäntöä 24 kuukauden kuluessa direktiivin voimaantulopäivästä. Annettu lisäaika on direktiivin laajuuden vuoksi tervetullut ja välttämätön.