Suuren valiokunnan kirjallinen lausuntopyyntö 16.3.2026

DNA Oyj:n lausunto komission kyberturvallisuusasetusta koskevasta ehdotuksesta (U 17/2026 vp)

DNA Oyj (jäljempänä DNA) kiittää mahdollisuudesta lausua valtioneuvoston kirjelmästä U 17/2026 vp - Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi.

DNA yhtyy FiCom ry:n lausuntoon[1] ja korostaa lisäksi seuraavia näkökohtia:

TIIVISTELMÄ

- DNA pitää komission ehdotuksen tavoitetta kyberturvallisuuden vahvistamisesta tärkeänä. Samalla katsomme, että ehdotetut ICT-toimitusketjuja koskevat keinot ovat useilta osin ongelmallisia ja voivat toteutuessaan heikentää **Suomen ja EU:n kilpailukykyä**, digitalisaation etenemistä, innovaatioita ja verkkojen kehittämistä, kuten siirtymistä 6G-aikakauteen.

- DNA pitää kannatettavana valtioneuvoston näkemystä siitä, että ehdotuksen tulee olla **riskiperusteinen ja suhteellisuusperiaatteen** mukainen sekä sitä, että ehdotettujen toimenpiteiden tulee olla ennakoitavia ja hallittuja sekä perustua asianmukaiseen kuulemiseen ja vaikutusarviointiin. Samalla DNA katsoo kuitenkin, että **valtioneuvoston kantaa tulisi monelta osin tarkentaa**, erityisesti ehdotuksen ICT-toimitusketjua koskevien velvoitteiden soveltamisalan, siirtymäaikojen ja kustannusten korvaamisen näkökulmasta.

- Ehdotuksen velvoitteiden tulisi kohdistua riskiperusteisesti **vain korkeimman riskin laitteisiin** ja velvoitteiden tulisi olla myös käytännössä toteuttamiskelpoisia. Ehdotuksen liitteessä II määritelty keskeinen ICT-omaisuus tulisi rajata koskemaan vain kriittisimpiä laitteita, kuten ns. ydinverkon laitteita.

- Ehdotukseen sisältyvät **siirtymäajat ovat liian lyhyitä ja täysin epärealistisia** suhteessa verkkojen pitkään elinkaareen. Erityisesti 5G-verkoille ehdotettu kolmen

[1] FiComin lausunto kyberturvallisuusasetusta ja NIS2-muutosdirektiiviä koskevasta U-kirjelmästä - FiCom

vuoden määräaika EU:n komission määrittelemien korkean riskin laitetoimittajien laitteiden poistolle ei ole teknis-taloudellisesti toteuttamiskelpoinen, huomioiden myös että ehdotus on EU-laajuinen ja kaikissa maissa laitteiden poisto tulisi tehdä samanaikaisesti. Seuraava ajankohta mahdollisille verkkolaitteiden vaihdolle on 2030-luvun alkupuolella, kun nykyiset verkkotoimiluvat päättyvät ja siirryttäessä 6G-aikakauteen.

- Ehdotettu sääntely tulee arvioida myös perustuslain ja EU:n perusoikeuskirjan omaisuudensuojan, mukaan lukien investointien suojan, näkökulmasta. Laitteiden vaihdosta aiheutuvat **kustannukset tulee korvata teleyrityksille**, jos laitteiden vaihtoa edellytetään ennen laitteiden luonnollisen elinkaaren päättymistä.

- Ehdotuksessa **komissiolle annetaan merkittäviä toimivaltuuksia** jatkossa päättää muun muassa keskeisen ICT-omaisuuden määrittelystä ja korkean riskin toimittajista, mikä heikentää sääntelyn vaikutusten ennakoitavuutta ja oikeusvarmuutta. DNA pitää tärkeänä, että jatkovalmistelussa arvioidaan valtioneuvoston näkemyksen mukaisesti se, että komissiolle delegoitavat toimivaltuudet ovat tarkkarajaisia, oikeasuhtaisia, tarkoituksenmukaisia ja perusteltuja.

- DNA pitää hyvänä myös valtioneuvoston näkemystä siitä, että unionin ja jäsenvaltioiden toimivallan rajat tulee säilyä selkeinä erityisesti kansallista turvallisuutta koskevissa asioissa. DNA katsoo, että jatkovalmistelussa on olennaista arvioida komission toimivaltuuksien säädösperusta ja oikeasuhteisuus säädöksen sisämarkkinatavoitteisiin nähden.

- Ehdotuksen kanssa samanaikaisesti komissio antoi ehdotuksen myös Digital Networks Act -ehdotukseksi. Kyberturvallisuusasetuksen toimitusketjuvelvoitteiden seuraamukset tulisi pitää asetuksen omassa seuraamuskehikossa ja taajuustoimilupien ehdot tulisi rajata taajuuksien käyttöön liittyviin, ennakoitaviin ja yksiselitteisiin velvoitteisiin, eikä taajuustoimiluvissa tulisi olla kytkentää kyberturvallisuusasetuksen toimitusketjuvelvoitteiden noudattamiseen.

1. Lähtökohdat

DNA pitää kyberturvallisuutta ja resilienssin vahvistamista koko yhteiskunnan toimivuuden, kansalaisten luottamuksen, yritysten toimintakyvyn sekä kriittisten palvelujen jatkuvuuden kannalta erittäin tärkeänä. Suomessa sähköisen viestinnän palvelulaki yhdessä uuden kyberturvallisuuslain kanssa, jolla on toimeenpantu NIS2-direktiivi, sisältävät kattavan viestintäsektorin turvallisuutta ja resilienssiä koskevan sääntelykehikon.

Kyberturvallisuuden ja resilienssin jatkuva parantaminen on teleyritysten liiketoiminnan keskeinen lähtökohta ja perusta, jolle liiketoiminta rakentuu ja niiden merkitys on entisestään korostunut viime vuosien aikana. Tämä edellyttää jatkuvaa riskienhallintaa ja

kehittämistoimia, joita teleyritykset tekevät suunnitelmallisesti osana normaalia operatiivista toimintaansa.

DNA kannattaa komission kyberturvallisuusasetus-ehdotuksen tavoitetta vahvistaa kyberturvallisuutta ja resilienssiä, mutta korostaa, että sääntelyn on tuettava oikeusvarmuutta, oltava riskiperusteinen, soveltamisalaltaan rajattu ja hallittu, suhteellisuusperiaatteen mukainen ja taloudellisesti sekä operatiivisesti toteuttamiskelpoinen.

2. Keskeiset vaikutukset

Viestintäverkot ja digitaalinen infrastruktuuri muodostavat perustan Suomen kasvulle, tuottavuudelle ja digitaalisen talouden kehitykselle. Ehdotetulla sääntelyllä, joka voi vaikuttaa olennaisella tavalla verkkolaitteisiin ja nykyisten, jo tehtyjen investointien hyödyntämiseen, voi olla merkittäviä vaikutuksia uusien palvelujen ja innovaatioiden kehittämiseen sekä valmistautumiseen 6G-siirtymään, jos näiden sijaan teleyritysten fokus olisi EU-laajuisesti useiden vuosien ajan 5G-verkkolaitteiden vaihdossa.

Useissa maissa, kuten Suomessa, 5G-verkot on myös jo käytännössä rakennettu ja tällä hetkellä operaattorit kehittävät uuden verkon päälle uusia palveluita ja valmistautuvat tulevaan 6G-siirtymään. Toteutuessaan ehdotuksella voisi olla vaikutusta myös mahdollisten tulevien investointien ajoitukseen ja laajuuteen.

DNA:n näkökulmasta on tärkeää, että ehdotuksen velvoitteet eivät aiheuta negatiivisia vaikutuksia jo tehtyjen investointien hyödyntämiselle sekä uusien palvelujen ja innovaatioiden kehittämiselle. Toimitusketjua koskevilla velvoitteilla on merkittävä vaikutus teleyritysten liiketoimintaan ja toimintaedellytyksiin, jolloin on olennaista huolehtia siitä, että sääntely on selkeää, ennakoitavaa ja käytännössä toteuttamiskelpoista.

3. Soveltamisalan laajuus: riskiperusteisuus ja suhteellisuus

DNA pitää keskeisenä, että kyberturvallisuusasetuksen velvoitteet ovat riskiperusteisia siten, että ne kohdistuvat erityisesti korkeimman riskin verkkoelementteihin. Käsitteiden, kuten “keskeisen ICT omaisuuden” (key ICT assets), tulee olla täsmällisiä ja ennakoitavia, jotta toimijat pystyvät etukäteen arvioimaan velvoitteiden soveltumista. Samalla velvoitteiden tulee olla suhteellisuusperiaatteen mukaisia niin, etteivät matalamman riskin laitteet joudu samanlaisen velvoitetason piiriin kuin aidosti kriittiset laitteet.

Ehdotetussa sääntelyssä on mukana kattavasti sekä 5G- että kiinteä verkko ja soveltamisala on laajempi kuin esimerkiksi Suomen kansallisessa viestintäsektorin kriittistä infrastruktuuria koskevassa sääntelyssä, josta säädetään sähköisen viestinnän palveluja koskevassa laissa ja sen perusteella annetussa Traficomin tarkemmassa määräyksessä viestintäverkon kriittisistä osista.

Ehdotetun sääntelyn liitteessä II määriteltyjen mobiili- ja kiinteiden verkkojen komponentit tulisi rajata riskiperusteisesti vain kriittisimpään osaan verkosta, kuten 5G-ydinverkkoon, ja jättää soveltamisalan ulkopuolelle esimerkiksi 5G-radioverkkolaitteet ja liityntäverkon laitteet, kuten ns. CPE-laitteet (Customer Premises Equipment -laitteet). Tällä tavoin ehdotus olisi riskiperusteinen ja suhteellisuusperiaatteen mukainen koskiessaan kriittisimpiä osia verkosta ja sen vaikutukset olisivat myös kokonaisuutena hallitummat.

On myös huomattava, että ehdotuksessa komissiolle annetaan merkittäviä toimivaltuuksia jatkossa päättää muun muassa keskeisen ICT-omaisuuden määrittelystä ja korkean riskin toimittajista, mikä heikentää sääntelyn vaikutusten ennakoitavuutta ja oikeusvarmuutta. DNA pitää tärkeänä, että jatkovalmistelussa arvioidaan valtioneuvoston näkemyksen mukaisesti se, että komissiolle delegoitavat toimivaltuudet ovat tarkkarajaisia, oikeasuhtaisia, tarkoituksenmukaisia ja perusteltuja.

DNA pitää hyvänä myös valtioneuvoston näkemystä siitä, että unionin ja jäsenvaltioiden toimivallan rajat tulee säilyä selkeinä erityisesti kansallista turvallisuutta koskevissa asioissa. DNA katsoo, että jatkovalmistelussa on olennaista arvioida komission toimivaltuuksien säädösperusta ja oikeasuhteisuus säädöksen sisämarkkinatavoitteisiin nähden.

4. Toimitusketjuja koskevat vaatimukset edellyttävät riittävän pitkää siirtymäaikaa

DNA pitää välttämättömänä, että ehdotetun sääntelyn toimeenpanossa huomioidaan verkkojen ja niiden komponenttien pitkät elinkaaret sekä se, että muutokset vaativat huolellista suunnittelua, rakentamista, testausta ja hallittua käyttöönottoa. Liian nopea aikataulu voi lisätä riskejä verkkojen toimintavarmuudelle ja laadulle sekä kasvattaa kustannuksia.

Mobiiliverkoille ehdotettu 36 kuukauden (3 vuoden) siirtymäaika komission määrittelemien korkean riskin laitetoimittajien verkkolaitteiden poistolle on EU-laajuisestikin tarkasteltuna täysin epärealistinen. Toteutuessaan sillä voi olla hyvin merkittävät vaikutukset, kun teleyritykset samanaikaisesti käynnistäisivät laitehankinnat EU-laajuisesti, mikä kuormittaisi niin laitetoimittajia, asentajia kuin teleyrityksen omaa organisaatiota samanaikaisesti. Verkkolaitetoimittajien tuotantokapasiteetti ei todennäköisesti riittäisi ilman erillisiä toimenpiteitä EU-laajuiseen yhtäaikaiseen laitetoimittajan vaihtoon. Yhtäaikainen, regulaatiolla pakotettu, tiukka ja ehdoton aikataulu aiheuttaisi sellaisen kysyntäpiikin, joka voi vaikuttaa merkittävästi esimerkiksi verkkolaitteiden hintatasoon. Samalla fokus olisi EU-tasolla verkkolaitteiden vaihdossa uusien palvelujen ja innovaatioiden kehittämisen sijaan.

DNA katsoo, että siirtymäaikojen ja vaiheistuksen tulee olla riittävän pitkiä ja teknis-taloudellisesti realistisia ja laitteiden vaihtoa koskevat vaatimukset tulee kohdentaa edellisessä kohdassa 3 todetulla tavalla vain soveltamisalaltaan korkeimman riskin laitteisiin. Olennaista on, että siirtymäajat ajoitetaan verkkolaitteiden luonnollisen elinkaaren mukaan, huomioiden siirtymisen 6G-aikakauteen ja uuteen verkkotoimilupakauteen 2030-luvun

alkupuolella. Näin mahdolliset muutokset tehdään hallitusti ja varmistaen, että verkkojen toiminta ja palveluiden laatu säilyvät myös muutostilanteessa.

5. Kustannusten korvaaminen

Perustuslain 15 § ja EU:n perusoikeuskirjan 17 artikla turvaavat omaisuudensuojaa, huomioiden myös jo tehtyjen investointien suojan. On olennaista, että jatkovalmistelussa ehdotettu sääntely arvioidaan erityisesti perustuslain ja EU:n perusoikeuskirjan turvaaman omaisuudensuojan kannalta.

Jos ehdotetun sääntelyn toimeenpano edellyttää laajoja ja nopeita muutoksia toimitusketjuissa tai komponenttivalinnoissa ennen nykyisten verkkolaitteiden luonnollisen elinkaaren päättymistä, kustannusvaikutukset voivat olla huomattavia ja vaikuttaa investointikykyyn laajemmin koko EU-tasolla. Nämä huomattavat kustannukset maksavat viime kädessä siis veronmaksajat tai teleyritysten asiakkaat – jäsenvaltioiden kuluttajat ja yritykset.

DNA katsoo, että teleyrityksille tulee korvata verkkolaitteiden vaihdosta aiheutuneet kustannukset, jos laitteiden poistoa edellytetään ennen niiden luonnollisen elinkaaren päättymistä. Kustannusten korvaamista ei ole käsitelty komission ehdotuksessa ja on tärkeää, että kysymystä arvioidaan huolellisesti jatkovalmistelussa ja että ehdotukseen sisällytetään mukaan kompensaatiomekanismi, jos verkkolaitteiden poistoa edellytetään ennen niiden luonnollisen elinkaaren päättymistä.

6. Kytkentä Digital Networks Actiin ja taajuustoimilupiin

Samanaikaisesti komission antaman Digital Networks Act -ehdotuksen mukaan taajuustoimiluvan ehtona olisi ehdotetun kyberturvallisuusasetuksen toimitusketjuvelvoitteiden noudattaminen. On huomattava, että ehdotettu kyberturvallisuusasetus on luonteeltaan horisontaalinen sääntely ja sisältää jo omat kattavat sanktio- ja valvontamekanisminsa.

Taajuustoimiluvat ovat pitkäkestoisia ja investointiperusteisia, mutta ehdotetun kyberturvallisuussäänтelyn toimitusketjuja koskevat velvoitteet täsmentyvät riskiarviointien sekä täytäntöönpanotoimien kautta, mukaan lukien velvoitteet poistaa komission määrittelemien korkean riskin toimittajien laitteita. Kun toimiluvan jatkuvuus sidotaan tällaiseen kehikkoon, yrityksen oikeusasema voi muuttua olennaisesti kesken toimilupakauden. Lisäksi toimiluvan menettämisen uhka muodostaisi suhteettoman seuraamuksen, joka kohdistuu koko toiminnan edellytyksiin, vaikka ehdotetussa kyberturvallisuusasetuksessa on jo omat, kattavat ja kohdennetut seuraamuskeinonsa.

Ehdotettu kytkentä voi heikentää myös tehokasta oikeussuojaa. Toimitusketjuvelvoitteiden seuraamukset tulisi pitää kyberturvallisuusasetuksen omassa kehikossa ja taajuustoimilupien ehdot tulisi rajata taajuuksien käyttöön liittyviin, ennakoitaviin ja yksiselitteisiin velvoitteisiin. Jos kytkentä kuitenkin säilytetään, kyberturvallisuusasetukseen tulee sisällyttää selkeät

menettelytakeet, jotta toimiluvan menettämisen riski ei realisoidu ennen kuin mahdolliset uuden sääntelyn velvoitteiden tulkintaan ja soveltamiseen liittyvät oikeudelliset kysymykset on asianmukaisesti arvioitu.

7. Lopuksi

DNA pitää tärkeänä ja on sitoutunut parantamaan kyberturvallisuutta yhteistyössä viranomaisten, kumppaneiden ja koko yhteiskunnan kanssa. EU-tason sääntely voi parhaimmillaan vahvistaa turvallisuutta, kyberresilienssiä ja luottamusta sekä tukea sisämarkkinoiden toimivuutta ja EU:n ja Suomen kilpailukykyä. Tämä edellyttää kuitenkin, että velvoitteet ovat riskiperusteisia, suhteellisia, ennakoitavia ja käytännössä toimeenpantavissa, ja että keinojen muotoilussa on asianmukaisesti huomioitu niiden kilpailukyky-, investointi- ja kustannusvaikutukset.

Helsinki 7.4.2026

Elina Thorström
Regulatory Manager