Teknologiateollisuus

Finnish Information Security Cluster Kyberala

Viite: U 23/2026 vp

Lausunto: Valtioneuvoston kirjelmä eduskunnalle

Teknologiateollisuus ry kiittää mahdollisuudesta lausua valtioneuvoston kirjelmään. Tämä lausunto on yhteinen Kyberala ry kanssa. Lausuntomme pohjautuu ja rajautuu jäsentemme edustamiin toimialoihin, joihin teleoperaattorit eivät kuulu. Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyberturvallisuusalaa. Yhdistyksen tarkoituksena on edistää digitaalisten teknologioiden riskienhallintaa, toimialan kilpailukykyä ja toimintaedellytyksiä sekä digitaalista turvallisuutta Suomessa ja EU:ssa yhteistyössä julkishallinnon, yritysten ja kansalaisyhteiskunnan kanssa.

Tiivistelmä

- Pidämme valtioneuvoston kantaa yleisesti ottaen hyvänä ja oikean suuntaisena. Asetusehdotuksen tavoitteet digitaalisten verkkojen turvallisuuden, toimintavarmuuden ja häiriönsietokyvyn vahvistamiseksi ovat kannatettavia elinkeinoelämän digitalisaatiolle sekä Euroopan kilpailukyvylle.
- Ehdotuksen turvallisuutta koskevien osioiden tulee tukea investointeja ja innovaatioita eikä lisätä epävarmuutta tai päällekkäisiä velvoitteita jo valmiiksi laajasti säännellyssä ja riskiperusteisessa toimintaympäristössä ja säännösten tulee olla saumattomasti yhteensopivia olemassa olevan EU:n kyberturvallisuussääntelyn kanssa.
- Sääntelyn on oltava johdonmukaista suhteessa olemassa olevaan EU-lainsäädäntöön sekä jäsenvaltioiden vastuisiin kansallisen turvallisuuden alueella, kuitenkaan estämättä yhteisten turvallisuus- ja resilienssitavoitteiden edistämistä.
- Verkkojen resilienssi ja toimintavarmuus ovat liiketoiminnan kannalta kriittisiä, sillä ne tukevat palveluiden jatkuvuutta, tuotantoketjuja ja digitaalisia riippuvuuksia eri toimialoilla.
- Varautumisvelvoitteiden tulee olla selkeästi määriteltyjä, teknisesti toteuttamiskelpoisia ja suhteutettuja todellisiin riskeihin, jotta ne eivät hidasta verkkojen modernisointia tai lisää hallinnollista taakkaa ilman vastaavaa turvallisuushyötyä.
- ICT-toimitusketjujen turvallisuuden huomioiminen on perusteltua, mutta vaatimusten on oltava ennakoitavia, teknologianeutraaleja ja riskiperusteisia sekä tuettava vakaata investointiympäristöä.
- Asetuksen verkkoviipaloinnin sääntely ja taajuuksien hallinnan keskittäminen EU tasolle ei saa vaarantaa teollisuuden jo rakentamia 5G-privaattiverkkoja.
- Sääntelyn tulisi keventää eikä lisätä hallinnollista taakkaa, ja keskeisten turvallisuusvelvoitteiden on oltava määriteltyjä jo asetustasolla, jotta oikeusvarmuus vahvistuu ja yritykset voivat kohdentaa resurssinsa varsinaiseen turvallisuustyöhön.
- Delegoitujen säädösten käyttöalan rajaamista tulee harkita tarkkaan, jotta se ei lisää yritysten epävarmuutta tulevasta sääntelystä.

Teknologiateollisuus ry

Eteläranta 10, PL 10, 00131 Helsinki
Puhelin 09 192 31
www.teknologiateollisuus.fi
Y-tunnus: 0215289-2

Yleinen arvio ja elinkeinoelämän lähtökohdat

Yhdymme valtioneuvoston kantaan, jossa kannatetaan EU:n sähköisen viestinnän sisämarkkinoiden kehittämistä digitaalisen siirtymän investointien vauhdittamiseksi, teletoimialan toimintaympäristön kehittämiseksi ja Euroopan globaalin kilpailukyvyn vahvistamiseksi. Suomella on maailman johtavaa osaamista verkkoteknologioissa, jotka ovat myös osa EU:n määrittelemiä kriittisiä teknologioita.

Pidämme Digital Networks Act -asetuksen tavoitteita vahvistaa digitaalisten verkkojen turvallisuutta, toimintavarmuutta ja häiriönsietokykyä lähtökohtaisesti kannatettavina. Turvallinen, ennustettava ja luotettava verkkoinfrastruktuuri on edellytys elinkeinoelämän digitalisaatiolle, investoinneille, kriittisille kyberturvallisuuspalveluille sekä Euroopan kilpailukyvylle globaalissa toimintaympäristössä.

Elinkeinoelämän kannalta keskeistä on kuitenkin, että turvallisuutta koskeva sääntely tukee investointeja ja innovaatioita eikä lisää epävarmuutta tai päällekkäisiä velvoitteita toimijoille, jotka jo toimivat laajasti säännellyssä ja riskiperusteisessa toimintaympäristössä. Samalla katsomme, että sääntelyn tulee olla johdonmukaista suhteessa olemassa olevaan EU-lainsäädäntöön sekä jäsenvaltioiden vastuisiin kansallisen turvallisuuden alueella. Jäsenvaltioiden yhteisiä turvallisuuden ja resilienssin päämääriä ei tule estää lyhytnäköisesti vain siksi, että kansallinen turvallisuus on jäsenvaltioiden toimivallan aluetta.

Näemme, että säädösehdotus voi parhaimmillaan vahvistaa Euroopan digitaalisten verkkojen turvallisuutta ja samalla tukea kyberalan, verkko-operaattoreiden ja digitaalisten palveluiden kasvua. Tämä edellyttää, että turvallisuutta koskeva sääntely on johdonmukaista, oikeasuhtaista ja investointiystävällistä. Asetuksen jatkovalmistelussa on olennaista varmistaa, että säädösehdotus tukee kyberturvallisuuden ja verkkojen resilienssin kehittämistä käytännössä ilman, että se lisää päällekkäistä sääntelyä, epävarmuutta tai tarpeetonta hallinnollista kuormaa elinkeinoelämälle.

Verkkojen resilienssi ja jatkuvuus liiketoiminnan näkökulmasta

Tuemme tavoitteita parantaa viestintäverkkojen ja -palvelujen resilienssiä sekä varautumista häiriöihin ja kriiseihin. Elinkeinoelämän näkökulmasta kriittistä on, että verkkojen toimintavarmuus tukee palveluiden jatkuvuutta, tuotantoketjujen toimivuutta ja digitaalisia riippuvuuksia eri toimialoilla.

Samalla painotamme, että säädöksellä asetettavien varautumisvelvoitteiden tulee olla selkeästi määriteltyjä, teknisesti toteuttamiskelpoisia ja suhteutettuja todellisiin riskeihin. Epäselvästi rajatut velvoitteet tai laajasti tulkittavat resilienssivaatimukset voivat hidastaa verkkojen modernisointia ja lisätä yritysten hallinnollista kuormaa ilman vastaavaa turvallisuushyötyä.

Johdonmukaisuus EU:n olemassa olevan kyberturvallisuussääntelyn kanssa

Pidämme välttämättömänä, että säädösehdotuksen turvallisuutta ja kyberturvallisuutta koskevat säännökset ovat saumattomasti yhteensopivia NIS2-direktiivin, CER-direktiivin sekä kyberturvallisuusasetuksen ja niihin ehdotettujen tuoreiden mahdollisten uudistusten kanssa. Kyberturvallisuusalan yritykset ja verkko--operaattorit toimivat jo nyt laajan riskienhallinta-, raportointi- ja velvoitekehikon piirissä.

Elinkeinoelämän näkökulmasta päällekkäiset tai osittain toisiaan vastaavat velvoitteet eivät paranna kokonaisturvallisuutta, vaan vievät resursseja varsinaisesta riskienhallinnasta ja turvallisuustyöstä. Säädösehdotuksen tulee täydentää olemassa olevaa sääntelykehikkoa eikä luoda uutta, erillistä turvallisuus- tai raportointikerrosta.

Investoinnit valokuituun ja kupariverkkojen poisto

Valtioneuvoston kanta kupariverkkojen poiston vähäisistä vaikutuksista Suomeen on oikea, mutta Euroopan tasolla kupariverkkojen poisto asetuksen avulla on perusteltua. Eurooppa kaipaa kipeästi lisää investointeja verkkoinfrastruktuuriin valokuidusta 5G/6G-verkkoihin ja tämän vauhdittaminen on Suomen etujen mukaista.

Verkkoviipalointi

Teollisuus on rakentanut viime vuosina 5G-privaattiverkkoja. Uusi ehdotettu sääntely ei saa vaarantaa näiden toimintaa, tai vaikeuttaa uusi privaattiverkkojen rakentamisia. Asetuksen ehdotus keskittää taajuushallinta EU tasolle saattaa myös pidentää käsittelyaikoja privaattiverkkojen osalta, joka olisi teollisuudelle haitallista.

ICT-toimitusketjujen turvallisuus ja investointiympäristö

Pidämme perusteltuna, että säädösehdotus tunnistaa ICT-toimitusketjujen turvallisuuden keskeiseksi osaksi verkkojen ja palveluiden luotettavuutta. Toimitusketjuriskien hallinta on keskeinen kysymys erityisesti verkko-, pilvi- ja kyberturvapalveluja tarjoaville yrityksille.

Samalla korostamme, että toimitusketjuvaatimusten tulee olla ennakoitavia, teknologianeutraaleja ja riskiperusteisia. Elinkeinoelämän investointipäätökset edellyttävät vakaata ja johdonmukaista sääntely-ympäristöä, jossa vaatimukset ovat selkeästi määriteltyjä eikä niitä laajenneta jälkikäteen ainakaan ilman vaikutusarvioita tai riittäviä siirtymäaikoja.

Kansallisen turvallisuuden rajapinnat ja yritysten toimintavarmuus

Pidämme tärkeänä, että säädösehdotus kunnioittaa jäsenvaltioiden vastuuta kansallisesta turvallisuudesta ja siihen liittyvistä ratkaisuista. Kyberturvallisuusalan ja verkko-operaattoreiden näkökulmasta on olennaista, että turvallisuuskriittisiä tietoja,

toimintatapoja tai infrastruktuurien yksityiskohtia ei edellytetä luovutettavaksi EU tasolle tavalla, joka vaarantaa luottamuksellisuutta tai yritysten sopimusvelvoitteita.

Erityisesti turvallisuusluokiteltuja tai liiketoiminnallisesti arkaluonteisia tietoja koskevien velvoitteiden tulee olla selkeästi rajattuja ja perusteltuja, jotta ne eivät heikennä yritysten kykyä toimia tehokkaasti tai kilpailla kansainvälisillä markkinoilla.

Hallinnollinen taakka, ohjeistusten määrä ja luottamuksen suoja

Elinkeinoelämän näkökulmasta on keskeistä, että säädösehdotus edistää sääntelyn yksinkertaistamista eikä lisää hallinnollista taakkaa uusilla raportointi-, tietopyyntö- tai koordinointivelvoitteilla, elleivät ne ole ehdottoman välttämättömiä. Erityisesti laaja riippuvuus delegoiduista säädöksistä, täytäntöönpanosäädöksistä ja viranomaisohjeista heikentää ennakoitavuutta ja vaikeuttaa pitkän aikavälin investointisuunnittelua. 198 artiklan delegointivaltuutus on erittäin laaja, ja pelkkä "lisäselvitysten saamista neuvottelujen aikana" ei voida pitää riittävän selkeänä neuvottelupositiona. Tuemme valtioneuvoston kantaa, jossa sääntelyn sujuvoittamiseen ja uudistamiseen johtavia toimia voitaisiin toteuttaa komission esittämää rohkeammin ja kunnianhimoisemmin.

Keskeisten turvallisuus- ja kyberturvallisuusvelvoitteiden tulisi olla mahdollisimman pitkälle määriteltyjä jo asetustasolla sekä, kuten aiemmin todettua, nojata kattavasti ja pääosin olemassa olevaan kyberturvallisuussääntelyyn (mm. NIS2-direktiivi, CER-direktiivi, kyberturvallisuusasetus (2.0) sekä kyberkestävyyssäädös (CRA). Tämä vahvistaa oikeusvarmuutta, tukee investointeja ja mahdollistaa yritysten resurssien kohdentamisen tehokkaaseen turvallisuustyöhön sääntelyhallinnan sijaan.

Helsingissä 14.4.2026

Peter Sund
Toimitusjohtaja
Kyberala ry
peter.sund@teknologiateollisuus.fi
050 565 0621

Ville Peltola
Päällikkö
Teknologiateollisuus ry
ville.peltola@teknologiateollisuus.fi
040 553 9941