U 17/2026 vp

Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi

Perustuslain 96 §:n 2 momentin perusteella lähetetään eduskunnalle komission 20 päivänä tammikuuta 2026 tekemä ehdotus Euroopan parlamentin ja neuvoston asetukseksi Euroopan unionin kyberturvallisuusvirasto ENISA:sta, Euroopan kyberturvallisuuden sertifiointikehyksestä ja tieto- ja viestintätekniikan toimitusketjujen turvallisuudesta sekä Euroopan parlamentin ja neuvoston direktiiviksi direktiivin (EU) 2022/2055 (NIS 2) muuttamisesta toimenpiteiden yksinkertaistamiseksi ja yhdenmukaistamiseksi [kyberturvallisuusasetuksen 2 kanssa, *myöhemmin CSA2*].

Helsingissä 12.3.2026

Liikenne- ja viestintäministeri Lulu Ranne

Ylitarkastaja Eevi Vuorinen

LIIKENNE- JA VIESTINTÄMINISTERIÖ

MUISTIO

12.3.2026

EU/385/2026
EU/388/2026

EHDOTUS EUROOPAN PARLAMENTIN JA NEUVOSTON KYBERTURVALLISUUSASETUKSEKSI (CSA2) JA NIS 2-MUUTOSDIREKTIIVIKSI

1 Tausta

Euroopan komissio antoi 20.1.2026 ehdotuksen (COM(2026) 11 final) Euroopan parlamentin ja neuvoston asetukseksi Euroopan unionin kyberturvallisuusvirasto ENISA:sta, Euroopan kyberturvallisuuden sertifiointikehyksestä ja ICT-toimitusketjujen turvallisuudesta sekä asetuksen (EU) 2019/881 kumoamisesta (CSA2-ehdotus). CSA2-ehdotuksella kumotaan vuonna 2019 voimaan tullut Euroopan parlamentin ja neuvoston asetus (EU) 2019/881 Euroopan unionin kyberturvallisuusvirasto ENISA:sta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (kyberturvallisuusasetus, CSA). Voimassa olevan CSA:n mukaan komissio arvioi viimeistään 28 päivänä kesäkuuta 2024 ja sen jälkeen viiden vuoden välein ENISA:n ja sen työtapojen vaikutuksen, tehokkuuden ja tuloksellisuuden sekä mahdollisen tarpeen muuttaa ENISA:n toimeksiantoa ja tällaisten muutosten taloudellisia vaikutuksia. Lisäksi arvioinnissa on ollut tarkoitus arvioida säännösten vaikutusta, tehokkuutta ja tuloksellisuutta suhteessa tavoitteisiin varmistaa tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberturvallisuuden riittävää tasoa unionissa ja parantaa sisämarkkinoiden toimintaa (kyberturvallisuuden sertifiointijärjestelmät).

CSA:n uudelleentarkastelun myötä havaittiin, että ENISA:n tehtävät ja resurssit eivät vastanneet tosiasiallista tarvetta esimerkiksi jäsenvaltioita ja organisaatioita tukeville toiminnoille. Eurooppalaisen kyberturvallisuuden sertifiointikehyksen osalta uudelleentarkastelu osoitti, että sertifiointikehyksen hyödyntäminen ei tarvittavalla tavalla estänyt sisämarkkinoiden pirstaloitumista ja siihen liittyvät prosessit katsottiin tehottomiksi. CSA2-ehdotuksen julkaisuajankohtana vain yksi kyberturvallisuuden sertifiointijärjestelmä (*EU Cybersecurity Certification Scheme on Common Criteria*) oli käytössä ja neljä valmisteluvaiheessa.

CSA2-ehdotuksen taustalla on jatkuva kyberturvallisuuden uhkaympäristön muutos, jonka myötä Eurooppa kohtaa päivittäin kyber- ja hybridiuhkia, jotka kohdistuvat kriittisiin palveluihin ja demokraattisiin instituutioihin. Sekä Euroopan varautumisunionin strategiassa että sisäisen turvallisuuden strategiassa (*ProtectEU*) kyberturvallisuus asetetaan EU:n resilienssin ytimeen. Myös EU:n taloudellista turvallisuutta koskevassa tiedonannossa painotetaan, että arkaluonteisten tietojen suojaaminen sekä kriittisen infrastruktuurin häiriöiden ehkäisy ovat turvallisuuden keskeisiä tavoitteita. Vastatakseen kasvaviin ja muuttuviin kyberturvallisuuden uhkiin ja kyberhyökkäyksiin Euroopan komissio on esittänyt uutta kyberturvallisuuden asetusta, jolla vahvistettaisiin kyberturvallisuutta ja toimintakykyä. Lisäksi ehdotuksen taustalla on ollut tarve yhdenmukaistaa ja yksinkertaistaa jäsenvaltioiden käyttämiä keinoja kyberturvallisuuden häiriöihin ja uhkiin vastaamiseksi.

Vuonna 2019 EU:ssa arvioitiin 5G-verkkojen turvallisuusriskejä. Riskiarvioinnissa jäsenvaltiot tunnistivat sekä teknisiä että strategisia riskejä. EU-tason koordinoitu riskiarviointi tehtiin NIS-yhteistyöryhmän (*Network and Information Security Cooperation Group*) 5G-alatyöryhmässä jäsenvaltioiden, komission ja EU:n kyberturvallisuusviraston (myöhemmin ENISA) yhteistyönä. Vuonna 2020 samassa yhteistyörakenteessa jäsenvaltiot laativat riskiarvioinnin

pohjalta yhteiset 5G-suositukset, jotka NIS-yhteistyöryhmä hyväksyi tammikuussa 2020. Suositusten tavoitteena on hallita riskiarvioinnissa tunnistettuja strategisia ja teknisiä riskejä 5G-verkoissa. Jäsenvaltiot ovat täytäntöönpanneet suosituksia osin erilaisilla ratkaisuilla. Komissio on pyrkinyt edistämään 5G-suositusten toimeenpanoa jäsenvaltioissa, erityisesti strategista suositusta koskien korkean riskin laitetoimittajien riskien hallitsemiseksi. Komissio antoi 15.6.2023 tiedonannon 5G-välineistön toimeenpanon tilanteesta ja korosti tiettyjen matkaviestinverkkojen laitetoimittajien unionin turvallisuudelle aiheuttamia riskejä sekä kehotti jäsenvaltioita toimenpiteisiin riskien hallitsemiseksi. EU:n sisäisen turvallisuuden strategiassa ja varautumisunionistrategiassa tieto- ja viestintätekniikan (*ICT*) toimitusketjujen vahvistaminen katsotaan tärkeäksi tavoitteeksi.

EU:ssa on valmisteltu 5G-suositusten (ns. 5G-työkalupakki eli *5G Toolbox*) rakennetta seuraavia ICT-toimitusketjuja koskevia suosituksia (ns. ICT-työkalupakki eli *ICT Toolbox*) ICT-toimitusketjujen turvallisuuden vahvistamiseksi. ICT-toimitusketjuja koskevat suositukset on valmisteltu NIS-yhteistyöryhmän toimitusketjujen turvallisuutta arvioivassa alatyöryhmässä jäsenvaltioiden, komission ja EU:n kyberturvallisuusvirasto ENISA:n yhteistyönä. Suositukset kohdistuvat pääasiassa jäsenvaltioihin. ICT-toimitusketjuja koskevat suositukset liittyvät myös NIS 2 -direktiivin 22 artiklaan, sillä ne luovat kehyksen artiklan mukaisten kriittisiä ICT-toimitusketjuja koskevien unionin tason koordinoitujen turvallisuusriskinarviointien laatimiselle. Vaikka suositukset kohdistuvat pääasiassa jäsenvaltioihin, voivat myös esimerkiksi NIS 2 -direktiivin soveltamisalaan kuuluvat toimijat hyödyntävät niitä arvioidessaan ICT-toimitusketjuihin kohdistuvia riskejä ja arvioivat tarvittavia toimenpiteitä. Suositukset on hyväksytty ja julkaistu alkuvuonna 2026.

Komissio antoi CSA2-ehdotuksen kanssa samanaikaisesti ehdotuksen (COM(2026) 13 final) Euroopan parlamentin ja neuvoston direktiiviksi direktiivin (EU) 2022/2055 (NIS 2) muuttamisesta sen yksinkertaistamiseksi ja yhdenmukaistamiseksi CSA2-ehdotuksen kanssa (NIS2-muutosehdotus). Koska NIS 2-muutosehdotus linkittyy tiiviisti CSA2-ehdotukseen, käsitellään ehdotukset samassa kirjelmässä. NIS 2-direktiivin soveltamisalaa ehdotetaan laajennettavaksi merenalaisen tiedonsiirtoinfrastruktuurin tarjoajiin, energia- ja kemianteollisuuden toimijoihin sekä eurooppalaisten digitaalisten identiteetti- ja yrityslompakoiden tarjoajiin.

2 Ehdotuksen tavoite

Kyberturvallisuusasetuksen uudistamisella on kaksi keskeistä tavoitetta: kyberturvallisuuden kyvykkyyksien ja resilienssin lisääminen sekä sisämarkkinoiden pirstaloitumisen ehkäiseminen. Tavoitteena on ensinnäkin vahvistaa Euroopan unionin kyberturvallisuuden hallinnointia sekä varmistaa, että asiaankuuluvilla toimielimillä, viranomaisilla ja muilla sidosryhmillä on paremmat edellytykset estää, havaita ja torjua kyberturvallisuusuhkia koordinoidulla ja tehokkaalla tavalla. Lisäksi kyberturvallisuusasetuksen uudelleentarkastelun tavoitteena on tukea unionin yhteisten kyberturvallisuusinstrumenttien kuten sertifiointijärjestelmien kehittämistä, täytäntöönpanoa ja käyttöönottoa sekä tarjota yhdenmukaistettuja keinoja rakentaa luottamusta ja yhteen toimivuutta jäsenvaltioiden välillä. Ehdotuksella pyritään kehittämään Euroopan kyberturvallisuuden sertifiointikehystä, ratkaisemaan kyberturvallisuuteen liittyviä monimutkaisia ja hajanaisia prosesseja, sekä puuttumaan lisääntyviin ICT-toimitusketjujen turvallisuusriskeihin. Tavoitteena on ICT-toimitusketjuihin, mukaan lukien viestintäverkkoihin, liittyvien ei-teknisten kyberturvallisuusriskien hallintatoimien yhdenmukaistaminen EU:ssa, joilla varmistettaisiin sisämarkkinoiden toiminta, edistettäisiin teknologista suvereniteettia ja vahvistettaisiin EU:n yhteistä kyberturvallisuuden ja resilienssin tasoa. Kyse olisi vähimmäistason velvoitteista.

Jäsenvaltioiden olisi mahdollista asettaa ehdotuksen velvoitteiden tasoa korkeampia kansallisia toimenpiteitä, jotka ovat linjassa unionin oikeuden kanssa.

Komission mukaan NIS2-muutosdirektiivin tavoitteet ovat osa kyberturvallisuusasetuksen uudelleentarkastelun tavoitteiden toteuttamista. NIS2-muutosdirektiivin kohdennetuilla muutoksella tavoitellaan NIS2-direktiivin vaatimuksenmukaisuuden yksinkertaistamista sekä johdonmukaisempaa täytäntöönpanoa. Tämä pitää sisällään tarkennuksia NIS2-direktiivin soveltamisalaan, määritelmiin, kiristyshaittaohjelmista ilmoittamiseen ja rajat ylittäviä palveluja tarjoavien toimijoiden valvontaan. Tavoitteena on lisäksi sääntelyn yksinkertaistaminen ja toimijoille sääntelystä aiheutuvien kustannuksien alentaminen.

3 Ehdotuksen pääasiallinen sisältö

3.1 Kyberturvallisuusasetusehdotuksen (CSA2) pääasiallinen sisältö

3.1.1 Euroopan kyberturvallisuusvirasto ENISA:n mandaatti ja tehtävät

Asetusehdotuksessa ehdotetaan EU:n kyberturvallisuusvirasto ENISA:n tehtävien selkeyttämistä ja päivittämistä kyberturvallisuuden uhkaympäristöön sopivaksi. Tulevaisuudessa ENISA:n toiminnan tavoitteena olisi vahvistaa EU:n ja jäsenmaiden kyberturvallisuutta, kyberresilienssiä ja luottamusta. Virasto toimisi koko unionin keskeisenä kyberturvallisuuden neuvonantajana ja asiantuntijakeskuksena. ENISA:n tehtävänä olisi muun muassa tukea jäsenvaltioita ja EU-toimielimiä kyberturvallisuuteen liittyvän EU-lainsäädännön ja politiikkojen kehittämisessä ja toimeenpanossa, vahvistaa kyberturvallisuusvalmiuksia ja resilienssiä koko EU:ssa, edistää operatiivista yhteistyötä ja tiedonvaihtoa, osallistua EU:n kyberturvallisuussertifiointijärjestelmän kehittämiseen ja ylläpitoon, sekä edistää kyberturvallisuusosaamista ja -koulutusta.

ENISA:n tehtävät

ENISA:n tehtäväkenttä jakautuu asetusehdotuksessa unionin lainsäädännön ja politiikkojen toimeenpanon tukeen, operatiiviseen yhteistyöhön, kyberturvallisuussertifiointeihin ja standardointiin, sekä kyberturvallisuuden osaamisakatemian toimeenpanoon.

Lainsäädännön toimeenpanon tukemisen osalta esitetään, että ENISA voisi muun muassa antaa jäsenmaille ja organisaatioille teknistä ohjeistusta, raportteja, neuvoja ja jakamalla parhaita käytäntöjä sekä tukea viranomaisten välistä tiedonvaihtoa. Se edistäisi kyberturvallisuustiedon jakamista eri toimialojen sisällä ja välillä, erityisesti NIS 2-direktiivin toimialoilla. Komission pyynnöstä ENISA voisi myös antaa kohdennettua teknistä tukea jäsenmaille esimerkiksi riskienhallinnassa ja kyberkyvykkyyden arvioinnissa. Suhteessa aiempiin tehtäviin ENISA:lle esitetään uusia laaja-alaisia tehtäviä koskien kyberturvallisuuden kapasiteetin rakennusta sisältäen myös hyvin yksityiskohtaisia tehtäviä, kuten organisaatioiden tukeminen kybervalmennusten järjestämisessä. NIS2-direktiivin mukaisesti ENISA voisi tukea jäsenmaita niiden tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden (*Computer Security Incident Response Team, CSIRT*) kehittämisessä ja kyberturvallisuusstrategioiden valmistelussa.

Operatiivisten kyberturvallisuustehtävien osalta ENISA:n mandaattiin esitetään merkittävää laajennusta. Jatkossa ENISA tukisi erityisesti jäsenmaiden CSIRT-yksiköistä koostuvan CSIRT-verkoston ja Euroopan kyberkriisien yhteysorganisaatioiden verkoston (*European Cyber Crisis Liaison Organisation Network*, *EU-CyCLONe)* kautta jäsenmaita tarjoamalla asiantuntija-arvioita ja tukea jäsenvaltioiden pyynnöstä kyberuhkatilanteisiin, analysoisi

haavoittuvuuksia sekä avustaisi laajamittaisten EU-tason kyberkriisien hallinnassa sekä tiedonvaihdon koordinoinnissa. Lisäksi ehdotuksessa esitetään tarkennuksia ENISA:n käyttämiin turvallisiin viestintävälineisiin.

ENISA:n tilannekuvan tuottamiseen esitetään myös tarkennuksia. ENISA tuottaisi jatkossa muun muassa varhaisia varoituksia kyberuhista, analysoisi uhkia ja riskejä, antaisi teknisiä analyysejä sekä tuottaisi laajempia raportteja uhkamaisemasta. ENISA voisi myös tukea jäsenmaita kyberturvallisuusharjoitusten järjestämisessä.

Lisäksi uutena kyvykkyytenä ENISA:n tehtävänä olisi kehittää koko EU:ta palveleva yhteinen tietojärjestelmien haavoittuvuuksien hallintakyvykkyys. ENISA ylläpitäisi NIS2-direktiivin perusteella perustettua Euroopan haavoittuvuustietokantaa, joka kokoaisi tiedot tunnetuista ICT-haavoittuvuuksista, tukisi jäsenmaita ja sidosryhmiä haavoittuvuuksiin liittyvässä työssä.

Kyberturvallisuuden sertifiointien osalta ENISA laatisi jatkossakin ehdotuksia eurooppalaisiksi kyberturvallisuuden sertifiointijärjestelmiksi. ENISA:n tulisi myös jatkossa ylläpitää hyväksyttyjä sertifiointijärjestelmiä ja valmistella niiden mahdollisia tarkistuksia ja edistää hyväksyttyjen järjestelmien käyttöönottoa. ENISA myös seuraisi ja tarvittaessa osallistuisi kyberturvallisuuteen liittyvään standardointityöhön EU-tasolla ja kansainvälisesti ja edistäisi eurooppalaisten ja kansainvälisten kyberturvallisuusstandardien käyttöönottoa.

Neljäntenä osa-alueena ehdotuksessa esitetään ENISA:lle vahvempaa roolia kyberturvallisuusosaamisen vahvistamisessa ja Euroopan kyberturvallisuusakatemian (*Cybersecurity Skills Academy* COM(2023) 207 final) toimeenpanossa. Ehdotuksella vahvistettaisiin, että ENISA laatisi ja ylläpitäisi eurooppalaista kyberturvallisuusosaamiskehystä (*European Cybersecurity Skills Framework, ECSF*), jossa määritellään kyberturvallisuusammattilaisten tehtävien roolit sekä niihin liittyvät taidot ja osaamisvaatimukset. ENISA:n tulisi tehdä tiivistä yhteistyötä jäsenmaiden kanssa kehystä valmistellessaan. Jatkossa erikseen valtuutetut osaamisen todentajat voisivat osaamiskehyksen perusteella myöntää eurooppalaisia osaamistodistuksia kyberturvallisuuden ammattilaisille. ENISA voisi myös kerätä valtuutetuilta osaamisen todentajilta maksuja. Osaamiskehyksen hyödyntäminen olisi jäsenmaille ja kyberturvallisuuden ammattilaisille vapaaehtoista.

ENISA:n hallintoa koskeva sisältö

Ehdotus sisältää ENISA:n toimintaan liittyviä säännöksiä, jotka koskevat budjetointia, henkilöstöasioita sekä viraston johtamista. Viraston hallinnolliseen rakenteeseen kuuluisi jatkossa johtokunta, hallitus, pääjohtaja, varapääjohtaja, neuvoa-antava ryhmä sekä valituslautakunta. Uusina rakenteina olisivat varapääjohtaja sekä valituslautakunta. Sen sijaan kansallisten yhteyshenkilöiden verkosto lakkautettaisiin.

ENISA:n johtokunta määrittelisi jatkossakin viraston toiminnan yleiset suuntaviivat ja nimittäisi pääjohtajan. Pääjohtaja vastaisi viraston päivittäisestä johtamisesta ja raportoisi johtokunnalle. Hallitus valmistelisi johtokunnan päätökset. Neuvoa-antava ryhmä olisi asiantuntijaelin, jossa olisi edustettuna yksityinen sektori, kuluttajajärjestöt ja muut keskeiset sidosryhmät. Ehdotus vastaa tältä osin pääpiirteissään viraston nykyistä toimintaa.

Uutena ENISA:n johtokunnan päätöksenteon osalta ehdotetaan, että jatkossa johtokunnassa Euroopan komissiolla olisi budjetti- ja henkilöstöasioihin liittyviin päätöksiin veto-oikeus. Lisäksi jatkossa jäsenmaiden tulisi ensisijaisesti nimittää johtokunnan edustajakseen NIS2-direktiivin mukaisen kansallisen toimivaltaisen viranomaisen johtaja tai muu korkean tason edustaja kyseisestä viranomaisesta. Johtokunta voisi myös päättää perustaa virastoon uuden

varapääjohtajan tehtävän. Varapääjohtajan tehtävänä olisi tukea pääjohtajaa viraston johdossa ja tehtävien hoidossa, sekä toimia pääjohtajan sijaisena.

Ehdotuksessa esitetään uutena toimintona myös riippumattoman valituslautakunnan perustamista. Valituslautakunta voisi käsitellä valtuutettujen osaamisen todentamisen palveluntarjoajien hakemuksiin liittyviä valituksia. ENISA voisi myös jatkossa kerätä maksuja valtuutetuilta osaamisen todentajilta kyberturvallisuustaitoihin liittyvien osaamisen todentamisen hakemuksista, vaatimustenmukaisuuden arviointilaitoksilta niiden osallistuessa Euroopan kyberturvallisuussertifikaattien myöntämiseen sekä julkisilta viranomaisilta tai yksityisiltä toimijoilta työkalujen testaamisesta. Maksuilla katettaisiin näistä toiminnoista aiheutuvia kuluja.

Ehdotuksessa esitetyt muutokset viraston toimintakenttään edellyttäisivät myös merkittävissä määrin ENISA:n resursoinnin ja henkilömäärän kasvattamista. Jäsenmaiden tulisi jatkossa nimittää kaksi kansallista asiantuntijaa, jotka toimisivat jäsenmaan yhteyshenkilönä (*liaison officer*) virastossa. Näiden asiantuntijoiden palkkakustannukset katettaisiin ensisijaisesti jäsenmaiden varoista. ENISA voisi hyödyntää lähetettyjä kansallisia asiantuntijoita vapaasti eri tehtävissä. EU:n virkamiehiä koskevat henkilöstösäännöt ja palvelussuhteen ehdot eivät koskisi kansallisia asiantuntijoita.

3.1.2 Eurooppalainen kyberturvallisuuden sertifiointikehys

Tavoitteet, soveltamisala ja prosessit

Asetusehdotuksessa esitetään uudistuksia eurooppalaisen kyberturvallisuuden sertifiointiin koskevaan sääntelyyn. EU:n laajuisella kyberturvallisuussertifikaatilla voisi osoittaa, että sertifioinnin kohde täyttää soveltuvassa sertifiointijärjestelmässä määritellyt tekniset kyberturvallisuusvaatimukset. Asetuksella säädettäisiin jatkossakin eurooppalaisten kyberturvallisuussertifiointien kehittämisestä ja käytöstä, mutta asetuksella ei asetettaisi sertifiointivelvollisuuksia. Eurooppalaisten kyberturvallisuuden sertifikaattien hakeminen ja hyödyntäminen olisi lähtökohtaisesti siis vapaaehtoista, ellei siitä ole erikseen muuten säädetty. Lisäksi eurooppalainen kyberturvallisuussertifikaatti ja osoitus vaatimustenmukaisuudesta tunnustettaisiin automaattisesti kaikissa jäsenvaltioissa.

Ehdotuksella uudistettaisiin eurooppalainen kyberturvallisuuden sertifiointikehys, jonka nojalla sertifiointijärjestelmissä arvioitaisiin tieto- ja viestintätekniikan tuotteiden, palvelujen, prosessien ja tietoturvapalvelujen kyberturvallisuusvaatimusten täyttymistä. Lisäksi ehdotus mahdollistaisi organisaatioiden kyberturvallisuustason (*cyber posture*) arvioinnin sekä sertifioinnin hyödyntämisen Euroopan unioin lainsäädännön vaatimustenmukaisuuden osoittamisessa. Ehdotuksessa esitetään, että vaatimustenmukaisuutta arvioitaessa kyberturvallisuuden sertifiointijärjestelmien arviointitoimet (*evaluation activities*) tulisivat olla yhdenmukaisia soveltuvien Euroopan unionin säädösten kanssa, minkä myötä syntyisi vaatimustenmukaisuusolettama (*presumption of conformity*). Jos tiettyjä arviointitoimia ei olisi määritelty unionin oikeudessa, sertifiointijärjestelmällä voitaisiin tarkentaa kriteerejä. Esityksen mukaan vaatimustenmukaisuuden arviointi tulee tehdä lähtökohtaisesti kolmannen osapuolen toimesta.

Ehdotuksen myötä lisättäisiin toiminnan läpinäkyvyyttä ja eri toimijoiden osallistamista. Komissio järjestäisi vähintään joka vuosi ENISA:n tuella kyberturvallisuuden sertifiointikokouksen (*European Cybersecurity Certification Assembly*), johon kutsuttaisiin Euroopan kyberturvallisuuden sertifiointiryhmän (*ECCG*) jäseniä, asiantuntijoita jäsenvaltioista ja unionin yhteisöistä sekä asiaankuuluvia sidosryhmiä. Lisäksi komissio

ylläpitäisi ja päivittäisi nettisivustoa, jolla asetettaisiin saataville kehitettävät eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät sekä strategiset prioriteetit tieto- ja viestintätekniikan tuotteiden, palveluiden ja prosessien, sekä kybertason ja EU-lainsäädännön turvallisuusvaatimusten harmonisoimiseksi. Myös ENISA ylläpitäisi nettisivustoa, jossa julkaistaisiin eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät, niiden ylläpitoon liittyvät maksut, myönnetyt eurooppalaiset kyberturvallisuuden sertifikaatit ja vaatimustenmukaisuuden vakuutukset, vertaisarvioinnit, tekniset eritelmät ja relevantit lisätiedot.

Ehdotuksen mukaan komissio voisi pyytää ENISA:a valmistelemaan tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja sekä tietoturvapalveluja ja kybertasoa koskevia kyberturvallisuuden sertifiointijärjestelmiä. ENISA:n tulisi laatia kyberturvallisuuden sertifiointijärjestelmä 12 kuukauden kuluessa komission pyynnöstä. Sertifiointijärjestelmää valmisteltaessa ENISA:n tulisi tehdä tiivistä yhteistyötä Euroopan kyberturvallisuuden sertifiointiryhmän kanssa sekä osallistaa asiaankuuluvia jäsenvaltioiden viranomaisia.

Lisäksi ehdotuksessa esitettäisiin, että jokaisella kyberturvallisuuden sertifiointijärjestelmällä olisi ylläpitostrategia (*maintenance strategy*) sekä sen mukaiset ylläpitokeinot. Ehdotuksen mukaan ENISA ylläpitäisi eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä yhteistyössä komission, Euroopan kyberturvallisuuden sertifiointiryhmän sekä jäsenvaltioiden kanssa. Ehdotuksessa esitettäisiin, että ENISA arvioisi kyberturvallisuuden sertifiointijärjestelmän vaikutuksia ja tehokkuutta vähintään joka neljäs vuosi järjestelmän käyttöönotosta. Lisäksi ENISA voisi kehittää teknisiä eritelmiä tulevia eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä tai niiden ylläpitoa varten.

Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien sisältö

Ehdotuksessa annetaan ehdotuksia eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän turvallisuustavoitteiksi esimerkiksi komponenttien, haavoittuvuuksien, poikkeamanhallinnan sekä sisäisten prosessien osalta. Lisäksi ehdotuksessa asetettaisiin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vähimmäisvaatimukset kuten järjestelmän kohteen, soveltamisalan ja toimintojen kuvaaminen; selostus sertifiointijärjestelmän tarkoituksesta; ylläpitostrategia; kyberturvallisuusvaatimukset, arviointikriteerit ja metodit. Tämän ohella ehdotuksessa ehdotetaan kyberturvallisuuden sertifiointikehyksiä ohjaavia vähimmäissääntöjä ja ehtoja muun muassa vaatimustenmukaisuuden seuraamisen, seuraamusten määräämisen ja tiedon luottamuksellisen käsittelyn osalta.

Ehdotuksen mukaan eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voitaisiin asettaa yksi tai useampi varmuustaso tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille sekä tietoturvapalveluille ja kybertasolle. Varmuustasot ”perus”, ”korotettu” ja ”korkea” tulisivat olla yhdenmukaisia tuotteiden, palveluiden ja prosessien sekä tietoturvapalvelun käyttötarkoitukseen, toiminnan luonteeseen ja olosuhteisiin liittyvien riskien kanssa. Ehdotuksessa esitettäisiin varmuustasojen vähimmäistasot, ja tarkemmat vaatimukset määriteltäisiin sertifiointijärjestelmissä. Eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä voitaisiin mahdollistaa vaatimustenmukaisuuden itsearviointi silloin, kun kyse on ”perustason” sertifikaatista.

Eurooppalaisen kyberturvallisuuden sertifiointikehyksen hallinnointi

Komission ehdotuksen mukaan tieto- ja viestintätekniikan tuotteiden, palveluiden ja prosessien, tietoturvapalvelujen ja kybertason sertifiointi loisi vaatimustenmukaisuusolettaman sertifiointijärjestelmän soveltamisalan osalta. Vaatimustenmukaisuuden arviointilaitokset

myöntäisivät kyberturvallisuuden sertifikaatteja kyseessä olevan kyberturvallisuuden sertifiointijärjestelmän vaatimusten mukaisesti. Ehdotuksen liitteessä 1 määriteltäisiin vaatimustenmukaisuuden arviointilaitoksille asetettavia vaatimuksia muun muassa niiden puolueettomuuden osalta. Kyberturvallisuuden sertifiointijärjestelmässä voitaisiin edellyttää, että sertifikaatteja voisi myöntää vain akkreditoitu kansallinen kyberturvallisuussertifioinnin viranomainen tai akkreditoitu julkinen elin.

Ehdotuksen mukaan kansalliset kyberturvallisuuden sertifiointijärjestelmät, jotka koskevat eurooppalaisia kyberturvallisuuden sertifiointijärjestelmien aihepiirejä ja soveltamisalaa, lakkaisivat eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vahvistamisesta annetun ehdotuksen myötä. Jäsenvaltiot eivät saisi luoda uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä, jos kyseisestä aihealueesta ja soveltamisalasta on jo olemassa eurooppalainen kyberturvallisuuden sertifiointijärjestelmä. Lisäksi kolmannen maan sertifikaatit voitaisiin tunnustaa eurooppalaista kyberturvallisuussertifikaattia vastaavaksi, jos sertifikaattien vaatimukset ovat yhdenmukaisia.

Komission ehdotuksen mukaan jokaisen jäsenvaltion olisi nimettävä yksi tai useampi kansallinen kyberturvallisuussertifioinnin viranomainen. Vaihtoehtona olisi pyynnöstä nimetä yksi tai useampi kyberturvallisuuden sertifiointiviranomainen toisessa jäsenvaltiossa vastaamaan pyynnön esittävän jäsenvaltion valvontatehtävistä.

Kansallisten kyberturvallisuussertifioinnin viranomaisten tulisi valvoa ja ilmoittaa vaatimustenmukaisuuden arviointilaitoksia; osallistua muun muassa Euroopan kyberturvallisuuden sertifiointiryhmään; valvoa ja seurata eurooppalaisen kyberturvallisuuden sertifiointijärjestelmien toimeenpanoa ja noudattamista; käsitellä kyberturvallisuuden sertifikaatteihin liittyviä valituksia sekä tuottaa vuosittaisia raportteja komissiolle, ENISA:lle ja Euroopan kyberturvallisuuden sertifiointiryhmälle. Lisäksi kansallisille kyberturvallisuuden sertifiointiviranomaisille esitettäisiin toimivaltuuksia esimerkiksi tiedonsaantioikeuksien, tutkintojen (*audits*) ja seuraamusten määräämisen osalta. Ehdotuksen mukaan kansalliset kyberturvallisuussertifioinnin viranomaiset tulisivat olemaan osana jäsenvaltioiden välisiä vertaisarviointeja, joissa arvioitaisiin viranomaisten yleistä, valvovaa ja täytäntöönpanevaa toimintaa ja menettelyjä. Vertaisarviointi toteutettaisiin vähintään kerran viidessä vuodessa kahden toisen kansallisen kyberturvallisuussertifioinnin viranomaisen toimesta.

Komission ehdotuksessa esitetään, että Euroopan kyberturvallisuuden sertifiointiryhmä (*ECCG*) koostuisi kansallisten kyberturvallisuussertifioinnin viranomaisten sertifiointiviranomaisten tai muiden relevanttien kansallisten viranomaisten edustajista. Euroopan kyberturvallisuuden sertifiointiryhmä avustaisi komissiota sertifiointikehykseen liittyvien normien implementoinnissa ja soveltamisessa sekä eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä koskevien pyyntöjen valmistelussa. Lisäksi muiden tehtävien ohessa Euroopan kyberturvallisuuden sertifiointiryhmä avustaisi ENISA:a valmistelemaan ehdotuksen sertifiointijärjestelmäksi ja määrittelemään sertifiointijärjestelmien teknisiä eritelmiä, sekä toimisi yhteistyössä komission ja ENISA:n kanssa sertifiointijärjestelmien ylläpitoon liittyvissä asioissa.

Oikeusturva ja seuraamukset

Komission esityksen mukaan luonnollisilla henkilöillä ja oikeushenkilöillä olisi oikeus tehdä valitus eurooppalaisen kyberturvallisuussertifikaatin myöntäjälle. Valittajalla olisi oikeus saada tietoa valituksen etenemisestä, päätöksestä ja oikeudesta hakea muutosta tuomioistuimesta.

Ehdotuksen mukaan jäsenvaltioiden tulisi asettaa seuraamuksia kyberturvallisuuden sertifiointikehykseen ja eurooppalaisen kyberturvallisuuden sertifiointiin liittyvien velvoitteiden rikkomisesta sekä tehdä tarvittavat toimenpiteet niiden täytäntöönpanemiseksi. Jäsenvaltioiden tulisi viivytyksettä ilmoittaa komissiolle näistä säännöistä ja menettelyistä.

3.1.3 ICT-toimitusketjujen turvallisuus

Ehdotuksessa esitetään velvoitteita ICT-toimitusketjujen ei-teknisten riskien hallitsemiseksi EU:ssa. Ehdotuksella luotaisiin luotettujen ICT-toimitusketjujen turvallisuusjärjestelmä (*security mechanism/framework*), jolla hallittaisiin ei-teknisiä riskejä NIS2-direktiivin (2022/2555) liitteiden I ja II sektoreilla. Komissio voisi täytäntöönpanoasetuksella määritellä kriittiset ICT-osat kriittisissä ICT-toimitusketjuissa. Se voisi ehdotuksen mukaisten riskiarviointien pohjalta esittää täytäntöönpanoasetuksilla asianmukaisia ja oikeasuhtaisia riskienhallintatoimia, jotka osoitettaisiin NIS2-direktiivin liitteiden I ja II toimialoille.

Turvallisuusriskien arviointi, kriittisten ICT-osien tunnistaminen ja riskienhallintatoimet

Ehdotuksen mukaan komissio tai ainakin kolmesta jäsenvaltiosta koostuva ryhmittymä voisi pyytää NIS2-direktiivin (2022/2555) 14 artiklan nojalla perustettua NIS-yhteistyöryhmää (*NIS Cooperation Group*) laatimaan NIS2-direktiivin 22 artiklan mukaisen riskiarvioinnin ICT-toimitusketjusta. Riskiarvioinnissa tulisi huomioida tarkasteltavan ICT-toimitusketjun kriittiset ICT-osat sekä näihin liittyvät keskeiset uhkatekijät, riskit ja haavoittuvuudet. Riskiarvioinnin pohjalta tulisi laatia riskiskenaariot ja ehdottaa toimenpiteet arvioinnissa tunnistettujen riskien hallitsemiseksi. Riskiarviointi tulisi laatia kuuden kuukauden sisällä sellaisen laadintapyynnöstä, tai komission pyynnöstä ja NIS yhteistyöryhmän näin sovittua myös tätä lyhyemmässä ajassa.

Mikäli komissiolla on riittävät perusteet epäillä, että ICT-toimitusketjussa olisi unionin turvallisuuteen vaikuttava merkittävä kyberuhka, joka edellyttäisi toimenpiteitä sisämarkkinoiden toiminnan turvaamiseksi, komissio voisi viipymättä konsultoida jäsenvaltioita tarvittavista ehdotuksen mukaisista riskienhallintatoimenpiteistä sekä laatia riskiarvioinnin, jossa komissio huomioisi havainnot jäsenvaltioiden konsultoinnista.

Jos edellä esitetty riskiarviointi osoittaisi merkittäviä kyberturvallisuusriskejä ICT-toimitusketjussa, komissio voisi täytäntöönpanoasetuksella määritellä kriittiset ICT-osat (*key ICT-assets*), joita NIS2-direktiivin liitteiden I ja II sektoreiden toimijat käyttävät tuotteidensa tai palvelujensa tuottamiseen. Arvioidessaan kriittisiä ICT-osia komissio ottaisi huomioon erilaisia seikkoja, kuten sen, onko ICT-osilla keskeisiä ja kriittisiä toimintoja, mahdolliset poikkeamat, mahdolliset riippuvuudet ja ehdotuksen mukaisen riskiarvioinnin tulokset.

Ehdotuksen mukaan komissio voisi täytäntöönpanoasetuksella kieltää NIS 2-direktiivin liitteiden I ja II toimijoita käyttämästä, asentamasta tai integroimasta tunnistettuihin kriittisiin ICT-osiin korkean riskin toimittajien ICT-komponentteja tai komponentteja, jotka sisältävät ICT-komponentteja. Näissä täytäntöönpanoasetuksissa määriteltäisiin soveltuvat siirtymäajat, joiden aikana komissio julkaisisi listan tähän liittyvistä korkean riskin toimittajista. Lisäksi täytäntöönpanoasetuksissa määriteltäisiin siirtymäajat kiellettyjen ICT-komponenttien vaihtamiseksi.

Komissio voisi täytäntöönpanoasetuksilla asettaa yhden tai useamman riskienhallintavelvoitteen ICT-toimitusketjuihin ja erityisesti kriittisiin ICT-osiin tietyille NIS2-direktiivin liitteiden I ja II toimialojen toimijoille riskiarvioinnin pohjalta. Näihin toimenpiteisiin lukeutuisi velvoite ICT-toimitusketjujen läpinäkyvyydestä toimivaltaiselle

valvovalle viranomaiselle, rajoitukset datan siirtämisestä kolmanteen maahan tai datan prosessointiin kolmannessa maassa, teknisiä toimenpiteitä, joita ulkopuolinen taho auditoisi, operatiiviseen toimintaan ja sopimussuhteisiin liittyviä rajoituksia sekä toimitusketjun monipuolistamiseen liittyviä toimia. Ennen näiden riskienhallintatoimien osoittamista komissio arvioisi mahdollisia riskejä ja riippuvuuksia. Varmistaakseen sisämarkkinoiden toiminnan komissio voisi myös poikkeuksellisessa tilanteessa kieltää NIS2-direktiivin liitteiden I ja II toimialojen toimijoita käyttämästä sellaisia toimittajia, joista aiheutuu merkittävä ei-tekninen kyberturvallisuusriski vähintään kolmelle jäsenvaltiolle.

Sähköisten viestintäverkkojen ICT-toimitusketjujen turvallisuus

Ehdotuksessa esitetään viestintäverkkojen ICT-toimitusketjuille vastaavia riskienhallintavelvoitteita ei-teknisten riskien hallitsemiseksi. Viestintäverkkoihin on kiinnitetty ehdotuksessa kuitenkin erityistä huomiota (110–111 artiklat). Ehdotuksen liitteessä II esitetään viestintäverkkojen kriittiset ICT-osat matkaviestintäverkoille, kiinteille viestintäverkoille ja satelliittiviestintäverkoille. Komissio voisi delegoidulla säädöksellä päivittää kyseistä listausta vastaamaan teknologista kehitystä. Ehdotuksen mukaan matkaviestintäverkoissa olevien korkean riskin laitetoimittajien ICT-komponentit tulisi vaihtaa viimeistään 36 kuukauden kuluessa siitä, kun komissio on julkaissut listan näiden viestintäverkkotyyppien korkean riskin toimittajista. Komissio voisi antaa täytäntöönpanoasetuksia, joissa se tarkentaisi siirtymäaikoja ICT-komponenttien vaihtamiselle kiinteiden viestintäverkkojen ja satelliittiviestintäverkkojen osalta. Ehdotuksen mukaan edellä todettujen viestintäverkkojen tarjoajien ei tulisi käyttää, asentaa tai integroida asetusehdotuksen liitteen II mukaisissa kriittisissä ICT-osissa korkean riskin toimittajien ICT-komponentteja tai komponentteja, jotka sisältävät ICT-komponentin.

Kyberturvallisuushuolia aiheuttavien kolmansien maiden osoittaminen

Asetusehdotuksessa esitetään, että komissio voisi nimetä kyberturvallisuushuolia aiheuttavia kolmansia maita (*third countries posing cybersecurity concerns*) pohjautuen edellä todettuihin riskiarvioihin tai pohjautuen muihin lähteisiin, kuten unionin tai jäsenvaltion julkilausumaan. Komissio arvioisi tällaisen kolmannen maan aiheuttaman riskin huomioiden 100 artiklan 1 kohdan a-e alakohdissa esitetyt seikat.

Mikäli komissio päätyisi arvioinnissaan toteamaan, että jokin kolmas maa aiheuttaisi vakavan ja rakenteellisen ei-teknisen riskin ICT-toimitusketjuissa, se voisi täytäntöönpanoasetuksella nimetä tällaisen kolmannen maan ICT-toimitusketjuihin kyberturvallisuushuolia aiheuttavaksi kolmanneksi maaksi.

Kyberturvallisuushuolia aiheuttavan kolmannen maan korkean riskin toimittajien tunnistaminen ja niitä koskevat rajoitukset

Ehdotuksen mukaan komissio voisi täytäntöönpanoasetuksella laatia listan korkean riskin toimittajista, joihin komissio voisi kohdistaa ehdotuksessa esitetyt rajoitteet täytäntöönpanosäädösten kautta. Rajoitusten osoittamista varten komissio selvittäisi ensin ICT-toimitusketjun toimittajat ja laatisi alustavan arvion sellaisista toimittajista, jotka olisivat perustettu kyberturvallisuushuolia aiheuttavaan kolmanteen maahan, tai olisivat tällaisen maan tai sinne perustetun toimijan tai maan kansalaisen hallinnassa. Komissio arvioisi toimittajien sijoittautumispaikan, omistussuhteen ja hallintajärjestelmän. Komissiolla olisi oikeus pyytää toimittajilta tietoja arvioinnin laatimiseksi. Mikäli jokin toimittaja ei luovuttaisi arviointiin tarvittavia tietoja määräajassa, komissio voisi sen perusteella päättää, että toimittaja on perustettu kyberturvallisuushuolia aiheuttavaan kolmanteen maahan tai sen olevan tällaisen

kolmannen maan, sen toimijan tai sen kansalaisten hallinnassa. Komissio kuulisi prosessissa tarkastelun alla olevaa toimittajaa ja kävisi tämän kanssa läpi alustavat havainnot. Komissio voisi myös pyytää toimivaltaista valvontaviranomaista laatimaan vastaavan arvioinnin ja toimivaltaisen valvovan viranomaisen tulisi ilmoittaa komissiolle, mikäli jokin toimittaja tulisi lisätä korkean riskin toimittajien listalle. Komissio päivittäisi säännöllisesti korkean riskin toimittajien listausta.

Komissio voisi myöntää poikkeuksen korkean riskin toimittajalle osoitettuihin rajoituksiin, mikäli tällainen toimittaja pystyisi todistetusti osoittamaan tehokkaat riskienhallintakeinot ei-teknisten riskien hallitsemiseksi ja varmistamaan, ettei kyberturvallisuushuolia aiheuttava kolmas maa vaikuta haitallisesti kyseisen toimittajan ICT-komponenttien toimitukseen. Komissio voisi tarvittaessa täytäntöönpanoasetuksilla asettaa tätä tarkempia ehtoja. Komissio kuulisi prosessissa poikkeusta hakenutta toimittajaa ja antaisi asiasta päätöksen yhdeksän kuukauden sisällä poikkeushakemuksesta. Se voisi asettaa määräajan myönnetyn poikkeuksen voimassaololle sekä määräajan poikkeuksen ehtoina olevien riskienhallintatoimenpiteiden toimeenpanolle. Komissio ylläpitäisi julkisesti saatavilla olevaa rekisteriä niistä päätöksistä, joissa se on myöntänyt poikkeuksen. Komissio voisi periä maksuja poikkeushakemuksista ja antaisi täytäntöönpanoasetuksilla tarkemmat tiedot maksutiedoista.

Toimivaltaisten valvontaviranomaisten valvontatehtävät

Jäsenvaltioiden tulisi nimetä NIS2-direktiivin 8 artiklan mukaiset toimivaltaiset valvovat viranomaiset asetusehdotuksen ICT-toimitusketjuja koskevien velvoitteiden valvoviksi viranomaisiksi. Tämän asetusehdotuksen valvontatoimet kohdistuisivat NIS2-direktiivin liitteiden I ja II toimijoihin. Ehdotuksen artiklassa 114 säädetään toimivaltaisten valvontaviranomaisten valvontatehtävistä. Toimivaltaisilla viranomaisilla olisi oikeus pyytää tarvittavia tietoja, toteuttaa valvontatoimenpiteitä sekä määrätä oikeasuhteisia ja tehokkaita korjaavia tai rajoittavia toimenpiteitä asetuksen noudattamisen varmistamiseksi. Valvontatoimenpiteiden tulisi olla tehokkaita, oikeasuhteisia ja johdonmukaisia. Ennen valvontatoimenpiteiden toimeenpanoa toimivaltaiset valvovat viranomaiset ilmoittaisivat valvontatoimenpiteiden kohteena olevaa toimijaa mahdollisista havainnoistaan. Toimijalla olisi mahdollisuus vastata näihin havaintoihin. Valvovat viranomaiset noudattaisivat valvontatehtävissään luottamuksellisuuden sekä liike- ja ammattisalaisuuden periaatteita.

Asetusehdotuksen mukaisten valvontatehtäviensä hoitamiseksi toimivaltaisten valvovien viranomaisten tulisi olla rakenteellisesti ja toiminnallisesti täysin itsenäisiä ja vapaita ulkoisista vaikutteista. Niiden ei tulisi saada ohjeistusta toiselta viranomaiselta tai yksityiseltä toimijalta. Komissio perustaisi näille valvoville viranomaisille yhteistyöverkoston tarvittavan yhteistyön edistämiseksi ja tietojenvaihdon edistämiseksi sekä korkean riskin toimittajien tunnistamista koskevan prosessin tueksi.

Jos NIS2-direktiivin I tai II liitteeseen kuuluva toimija tarjoaisi palveluita useassa jäsenvaltiossa tai sen kriittiset ICT-osat sijaitsevat useassa jäsenvaltiossa, toimivaltaisten valvontaviranomaisten olisi tehtävä yhteistyötä keskenään ja komission kanssa asetuksen tehokkaan ja yhdenmukaisen soveltamisen varmistamiseksi. Ehdotuksessa säädettäisiin myös valvontatehtävien hoitamista varten lainkäyttövallasta, johon NIS2-direktiivin liitteiden I ja II toimijat kuuluisivat tämän säädösehdotuksen mukaisten valvontatoimenpiteiden kohdistamiseksi.

Seuraamukset

Ehdotuksessa esitetään, että jäsenvaltioiden tulisi säätää seuraamusmaksuista (*penalties*) asetusehdotuksen velvoitteiden rikkomisesta. Seuraamusmaksujen tulisi olla tehokkaita, suhteellisia ja varoittavia, ja ne voisi määrätä asetusehdotuksen 114 artiklan 3 kohdan a-c toimien lisäksi. Ehdotuksessa säädettäisiin, että 103 artiklan 2 kohdan a alakohdan rikkomisesta voisi määrätä enintään 1% suuruinen seuraamusmaksu edellisen vuoden maailmanlaajuisesta liikevaihdosta. Asetusehdotuksen 103 artiklan 2 kohdan b-g alakohtien rikkomisesta voisi määrätä enintään 2% suuruinen seuraamusmaksu ja 103 artiklan 1 kohdan ja 111 artiklan rikkomisesta enintään 7 % suuruinen seuraamusmaksu.

3.1.4 Loppusäännökset

Ehdotuksessa ehdotetaan, että komissio arvioisi viimeistään xx.yy.zzzz ja sen jälkeen viiden vuoden välein ENISA:n tuloksellisuutta suhteessa sen tavoitteisiin, toimeksiantoon, tehtäviin, hallintoon ja sijaintiin; EU:n yksittäisten kyberturvallisuusosaamisen todentamisjärjestelmien vaikuttavuutta, tehokkuutta ja EU:n tuomaa lisäarvoa; tieto- ja viestintätekniikan tuotteiden, palveluiden ja prosessien sekä tietoturvapalvelujen vaikutuksia, vaikuttavuutta ja tehokkuutta asetettuihin tavoitteisiin ja turvallisuustasoihin nähden; tieto- ja viestintätekniikan toimitusketjujen turvallisuutta ja toteutuneita toimia.

3.2 NIS 2 -muutosdirektiivi

Direktiivillä ehdotetaan kohdennettuja muutoksia NIS 2 -direktiivin (EU) 2022/2555. Kohdennetuilla muutoksilla pyritään selventämään ja tarkentamaan direktiivin soveltamisalaa, edistämään täytäntöönpanon yhdenmukaisuutta jäsenvaltioissa, helpottamaan vaatimustenmukaisuuden osoittamista sekä vähentämään sääntelystä toimijoille aiheutuvia kustannuksia. Ehdotetut muutokset koskevat direktiivin soveltamisalaa, toimijoiden luokittelua keskeisiksi ja tärkeiksi, komission täytäntöönpanosäädöksiä riskienhallinnasta ja merkittävistä poikkeamista ilmoittamisesta, kiristyshaittaohjelmatietojen ilmoittamista, ENISA:n tehtävää jäsenvaltioiden valvonnan tukena sekä eurooppalaisen kyberturvallisuussertifioinnin hyödyntämistä riskienhallintavaatimuksen vaatimustenmukaisuuden osoittamisessa.

Direktiivin soveltamisalaan ehdotetaan lisättäväksi uusina toimijatyyppeinä eurooppalaisten digi-identiteettilompakoiden ja eurooppalaisten yrityslompakoiden tarjoajat. Lisäksi soveltamisalaan ehdotetaan uusina toimijatyyppeinä toimijoita, jotka omistavat, hallinnoivat tai käyttävät strategista kaksikäyttöinfrastruktuuria. Nämä toimijat kuuluisivat koosta riippumatta direktiivin soveltamisalaan keskeisinä toimijoina. Direktiivin soveltamisalaan ehdotetaan uutena toimijatyyppinä lisäksi merenalaisen datainfrastruktuurin operaattoreita silloin kun ne ovat kooltaan keskisuuria tai suurempia. Direktiivin soveltamisalasta ehdotetaan poistettavaksi DNS-palveluita tarjoavat mikro- ja pienyritykset, sellaiset sähköntuottajat, joiden tuotantokapasiteetti on alle 1 MW sekä sellaiset terveyspalveluiden tuottajat, jotka tarjoavat ainoastaan pitkäaikaista hoitoa. Lisäksi soveltamisalaa määrittäviin käsitteisiin ehdotetaan eräitä tarkennuksia vetytoimijoiden, älykkäiden liikennejärjestelmien tarjoajien sekä kemianteollisuuden osalta. Lisäksi direktiivin 26 artiklaan ehdotetaan eräitä täsmennyksiä jäsenvaltioiden lainkäyttövallasta lentoyhtiöitä ja kolmansiin valtioihin sijoittautuneita toimijoita koskien. Lisäksi direktiivin 27 ja 3 artikloihin ehdotetaan eräitä tarkennuksia, jotka koskevat ENISA:n ylläpitämää toimijaluetteloa sekä toimijoiden velvollisuutta ilmoittaa tietonsa valvovalle viranomaiselle.

Komissio ehdottaa, että keskeisen toimijan määrittämisessä sovellettavaa kokorajaa korotettaisiin. Direktiivin tarkoittamia keskeisiä toimijoita olisivat jatkossa sellaiset direktiivin liitteessä I tarkoitettua toimintaa harjoittavat toimijat, jotka ylittävät pienen midcap-yrityksen kokorajan. Pienen midcap-yrityksen määritelmään sovellettaisiin komission asiasta antamaa

suositusta (EU) 2025/1099). Suosituksen liitteen 2 kohdan mukaisesti pienten midcap-yrityksien luokka koostuu yrityksistä, joiden palveluksessa on vähemmän kuin 750 työntekijää ja joiden vuosiliikevaihto on enintään 150 miljoonaa euroa tai taseen loppusumma on enintään 129 miljoonaa euroa. Nykyisin sovellettava kokoraja on perustunut komission suositukseen 2003/361/EY mikroyritysten ja pienten yritysten määritelmistä, ja vastaavana kokorajana on sovellettu raja-arvojen ylittymistä sellaisesta yritysluokasta, joka koostuu yrityksistä, joiden palveluksessa on vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa tai taseen loppusumma on enintään 43 miljoonaa euroa.

Komissio ehdottaa strategian sisällöllisiä vaatimuksia koskevaa muutosta, jonka nojalla jäsenvaltioiden tulisi jatkossa hyväksyä kansallisissa kyberturvallisuusstrategioissa muun ohella myös kvantinkestävän salauksen (*post-quantum cryptography, PQC*) käyttöönottoa koskevat politiikat.

Komissio voi nykyisin antaa täytäntöönpanoasetuksia, joilla tarkennetaan riskienhallintavaatimukseen liittyviä toimenpiteitä. Komissio voisi jatkossa antaa riskienhallinnasta täytäntöönpanoasetuksia, jotka ovat täysharmonisoivia, ja siltä osin kuin sellaisia on annettu, jäsenvaltiot eivät saisi edellyttää niistä poikkeavia riskienhallintatoimia. Ehdotus olisi poikkeus NIS 2 -direktiivin luonteeseen vähimmäisharmonisoivana säädöksenä ja käytännössä laajentaisi komissiolle siirrettyä täytäntöönpanovaltaa riskienhallinnasta.

Ehdotuksen mukaan komission tulisi merkittävästä poikkeamasta ilmoittamista koskevalla täytäntöönpanosäädöksellä edellyttää, että toimijan on ilmoitettava, onko toimija havainnut kiristyshaittaohjelmahyökkäystä, -hyökkäyksen alan ja sitä koskevat hallintatoimet. Vaikka ehdotus ei perustaisi uutta velvollisuutta täytäntöönpanosäädöksen antamiseen, se soveltuisi merkittävästä poikkeamasta ilmoittamista koskeviin täytäntöönpanosäädöksiin uutena sisällöllisenä vaatimuksena. Lisäksi ehdotuksen mukaan jäsenvaltioiden tulisi edellyttää toimijoita ilmoittamaan merkittävän poikkeaman johtuessa kiristyshaittaohjelmasta siitä, onko se vastaanottanut lunnasvaatimuksen, keneltä se on vastaanottanut lunnasvaatimuksen, sekä tiedot siitä lunnaiden maksamisesta ja vastaanottajasta.

Ehdotuksen mukaan ENISA:n tulisi laatia analyysi rajat ylittävistä kyberturvallisuusriskeistä keskittyen erityisesti poikkeamien rajat ylittäviin vaikutuksiin. Tämän arvioinnin perusteella ENISA voisi antaa ohjeita tai suosituksia jäsenvaltioiden valvoville viranomaisille sekä jäsenvaltion valvovan viranomaisen pyynnöstä osallistua valvontatoimiin tai toimijan riskienhallintatoimenpiteiden riittävyyden arviointiin. Valvonnan tukemiseksi jäsenvaltioita edellytettäisiin toimittamaan tietoja ENISA:lle valvonnasta ja sen kohteista. Lisäksi komissio ehdottaa, että ENISA lisättäisiin CSIRT-verkoston jäseneksi.

Ehdotuksen mukaan jäsenvaltiot voisivat edellyttää toimijoita hankkimaan eurooppalaisen kyberturvallisuussertifiointijärjestelmän mukaisen sertifioinnin riskienhallinnan vaatimustenmukaisuuden osoittamiseksi. Jäsenvaltioiden tulisi pitää sertifioitua toimijaa riskienhallintaa koskevien velvoitteiden mukaisena, jos toimija olisi hankkinut siihen soveltuvan sertifioinnin. Lisäksi sertifioituun toimijaan ei saisi kohdistaa valvonnassa säännöllisiä turvallisuusauditointeja tai -tarkastuksia.

Ehdotuksen mukaan jäsenvaltioiden olisi saatettava NIS 2 -muutosdirektiivi osaksi kansallista lainsäädäntöä 12 kuukauden kuluessa sen voimaantulosta.

4 Ehdotuksen oikeusperusta ja suhde suhteellisuus- ja toissijaisuusperiaatteisiin

4.1 Oikeusperusta

CSA2-ehdotuksen ja NIS 2 -muutosdirektiivin oikeusperusteena on Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artikla, joka mahdollistaa sisämarkkinoiden toteuttamista ja toimintaa koskevien toimenpiteiden antamisen. SEUT 114 artiklan nojalla annettavat säädökset hyväksytään tavallisessa lainsäätämisjärjestyksessä. Neuvosto tekee päätöksensä määräenemmistöllä.

Komission mukaan ehdotuksella pyritään välttämään sisämarkkinoiden pirstoutumista.

Komissio kiinnittää huomiota siihen, että asetus (EU) 2019/881 ENISA:sta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (CSA) hyväksyttiin tämän SEUT 114 artiklan nojalla.

Komission mukaan ICT-toimitusketjujen turvallisuuden osalta kansallisen lainsäädännön hajanaisuus erityisesti ei-teknisten riskien osalta voisi johtaa sisämarkkinoiden pirstoutumiseen. Eriävät kansalliset lähestymistavat voisivat lisätä joidenkin jäsenvaltioiden haavoittuvuutta ja aiheuttaa rajat ylittäviä heijastevaikutuksia, mikä heikentäisi koko Euroopan Unionin kyberturvallisuuden resilienssiä ja luotettavuutta. Näistä syistä komissio katsoo, että SEUT 114 artikla säilyy asianmukaisena oikeusperustana CSA:n uudelleentarkastelulle. Valtioneuvosto pitää oikeusperustaa asianmukaisena.

NIS 2 -muutosdirektiivin osalta SEUT 114 artiklan soveltumista perustellaan sillä, että muutettavaksi ehdotettu direktiivi on annettu samalla oikeusperustalla. Valtioneuvosto pitää oikeusperustaa asianmukaisena.

4.2 Suhteellisuus- ja toissijaisuusperiaatteet

Euroopan unionista tehdyn sopimuksen toissijaisuus- ja suhteellisuusperiaatteita koskevan 5 artiklan mukaan unioni voi antaa säädöksiä ainoastaan silloin, kun se on tarpeen ja ainoastaan siinä laajuudessa, kun se on tarpeen. Toissijaisuusperiaatteen mukaisesti unioni toimii aloilla, jotka eivät kuulu sen yksinomaiseen toimivaltaan, ainoastaan jos ja siltä osin kuin jäsenvaltiot eivät voi keskushallinnon tasolla tai alueellisella taikka paikallisella tasolla riittävällä tavalla saavuttaa suunnitellun toiminnan tavoitteita, vaan ne voidaan suunnitellun toiminnan laajuuden tai vaikutusten vuoksi saavuttaa paremmin unionin tasolla.

Komissio katsoo, että toissijaisuusperiaatteen täyttyminen on tunnustettu jo voimassa olevaa kyberturvallisuusasetusta hyväksyttäessä. Komissio katsoo, että unionin tasoinen puuttuminen on edelleen ratkaisevan tärkeää, koska kyberturvallisuusuhat ja niihin liittyvät haasteet ovat rajat ylittäviä. Pirstaloituneet kansalliset ratkaisut eivät ole osoittautuneet riittäväksi markkinoiden laajuisen luottamuksen ja koordinoinnin saavuttamiseksi. Lainsäädännön uudelleenarviointia tarvitaan, jotta varmistetaan sen johdonmukainen täytäntöönpano ja tuetaan jäsenvaltioita yhä monimutkaisemmassa sääntely- ja uhkaympäristössä. Lisäksi komissio katsoo, että ehdotetut toimenpiteet eivät ylitä sitä, mikä on tarpeen ehdotuksen tavoitteiden saavuttamiseksi, eivätkä ne estä jäsenvaltioita toteuttamasta omia toimiaan kansallista turvallisuutta koskevissa asioissa. Komissio siis katsoo toiminnan olevan toissijaisuus- ja suhteellisuusperiaatteiden mukaista.

Euroopan kyberturvallisuusvirasto ENISA:n osalta ehdotus sisältää virastolle joitakin uusia tehtäviä, joiden tarkoituksena on tukea jäsenvaltioita niissä toimissa, joissa on kyberturvallisuuden hallinnan näkökulmasta nähty puutteita. Komission arvion mukaan ehdotus ei toissijaisuuden näkökulmasta poikkea aiemmasta kyberturvallisuusasetuksesta.

Valtioneuvosto yhtyy pääosin komission arvioon toissijaisuudesta ja suhteellisuusperiaatteesta ENISA:n mandaatin osalta. Neuvotteluiden aikana on kuitenkin arvioitava ENISA:n tehtävien suhdetta jäsenmaiden kyberturvallisuustehtäviin ja varmistettava toimien täydentävyys sekä jäsenmaiden riittävä mahdollisuus osallistua ENISA:n toimintaa koskevaan päätöksentekoon. ENISA:lle ehdotettujen uusien kyberturvallisuusosaamiseen liittyvien tehtävien osalta komissio ei ole esittänyt tarkempaa arviota toimien toissijaisuus- ja suhteellisuusperiaatteiden täyttymisestä. Valtioneuvosto pyytää käsittelyn aikana komissiolta lisätietoja näiden toimien vaikutuksista jäsenmaihin.

Komissio on aiemmin pyrkinyt yhdenmukaistamaan viestintäverkkojen turvallisuuden toimenpiteitä EU:n 5G-suosituksilla. Jäsenvaltiot ovat viime vuosina toimeenpanneet näitä suosituksia erilaisilla kansallisilla ratkaisuilla, mikä on johtanut toimenpiteiden pirstaloitumiseen unionissa. Komissio katsoo ehdotuksessaan, että ICT-toimitusketjujen kyberturvallisuuden osalta kansallisten, ei-teknisiin riskitekijöihin vaikuttavien toimenpiteiden pirstaleisuudella on sisämarkkinoiden toimintaa heikentävä vaikutus. Komissio katsoo, että jäsenvaltioiden erilaiset lähestymistavat voisivat johtaa joidenkin jäsenvaltioiden lisääntyneeseen haavoittuvuuteen, mikä voi heijastua koko unioniin. Komissio katsoo, että ICT-toimitusketjujen turvallisuus on rajat-ylittävää. ICT-toimitusketjujen rajat ylittävän luonteen vuoksi komissio katsookin, että eriävät kansalliset ratkaisut heikentäisivät oikeusvarmuutta sisämarkkinoilla. Komissio katsoo, että kyberturvallisuushuolia aiheuttavien kolmansien maiden tunnistaminen ja ICT-toimitusketjujen turvallisuus voidaan varmistaa tehokkaimmin ehdotuksen mukaisilla vähimmäistason toimenpiteillä unionin tasolla. Ehdotuksen mukaan ICT-toimitusketjuja koskevat säännökset ovat vähimmäistason velvoitteita, jotka eivät rajoittaisi jäsenvaltioiden mahdollisuutta antaa näiden yli meneviä kansallisia toimenpiteitä, erityisesti kansallisen turvallisuuden osalta, jossa jäsenvaltioilla on yksinomainen toimivalta SEU 4(2) mukaisesti.

Jäsenvaltiot eivät yksin pysty tehokkaasti varmistamaan ICT-toimitusketjujen turvallisuutta näiden ollessa luonteeltaan rajat-ylittäviä ja alihankintaketjujen ollessa monitasoisia. Valtioneuvoston alustava näkemys on, että ehdotuksen ICT-toimitusketjuja koskevat säännökset ovat suhteellisuus- ja toissijaisuusperiaatteiden mukaisia ja komission perustelut asianmukaisia. Neuvotteluissa on kuitenkin keskeistä varmistua siitä, että ehdotuksen toimenpiteet edistävät sisämarkkinoiden toimintaa, unionin laajempia strategisia tavoitteita ja lisäävät yhdenmukaisilla toimenpiteillä unionin oikeusvarmuutta eivätkä johda äkillisiin, ennakoimattomiin tai vaikeasti toteutettaviin muutoksiin jäsenvaltioissa. Lisäksi neuvotteluissa on tärkeää huolehtia siitä, että jäsenvaltiot voivat jatkossakin esittää ehdotuksen velvoitteita pidemmälle meneviä kansallisia toimenpiteitä, ja että SEU 4(2) artiklaa noudatetaan.

Komissio arvioi, että NIS 2 -muutosdirektiivi täyttää toissijaisuus- ja suhteellisuusperiaatteiden vaatimukset. Toissijaisuusperiaatteen osalta ehdotusta perustellaan sillä, että muutoksien kohteena oleva direktiivi on todettu toissijaisuusperiaatteen mukaiseksi. Lisäksi muutoksilla selkeytetään ja parannetaan lainsäädäntökehyksen toimivuutta. Suhteellisuusperiaatteen osalta komissio katsoo, että ehdotukset ovat oikeassa suhteessa niiden tavoitteiden kannalta ottaen huomioon erityisesti, että kysymys on muun ohella jäsenvaltioiden ja sidosryhmien esittämiin sääntelyn kehittämisen tarpeisiin puuttumisesta.

Valtioneuvosto yhtyy pääosin komission arvioon siitä, että NIS 2 -muutosdirektiivi täyttää toissijaisuus- ja suhteellisuusperiaatteiden vaatimukset. Neuvotteluiden aikana on kuitenkin arvioitava yksityiskohtaisemmin näiden periaatteiden kannalta komission ehdotusta siitä, että se voisi antaa kyberturvallisuuden riskienhallintatoimenpiteistä täysharmonisoivia täytäntöönpanosäädöksiä.

4.3 Toimivallan siirto sekä komissiolle ehdotetut tehtävät

Ehdotettuun kyberturvallisuusasetukseen (CSA2) ja NIS 2 -muutosdirektiiviin sisältyy täytäntöönpanovallan siirtämistä komissiolle.

Asetusehdotuksen mukaan komissio voisi antaa täytäntöönpanosäädöksiä, joissa vahvistetaan ENISA:n perimien maksujen määrittämistä koskevat yksityiskohtaiset säännöt, kuten maksujen määrät ja niiden edellytykset.

Ehdotuksen mukaan komissio voisi antaa täytäntöönpanosäädöksistä tieto- ja viestintätekniikan tuotteista, palveluista ja prosesseista sekä tietoturvapalvelujen tarjoajista ja kybertasosta annetun eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vahvistamiseksi. Lisäksi komissio voisi antaa täytäntöönpanosäädöksiä, joilla vahvistetaan yhteisiä periaatteita ja mallisäännöksiä eurooppalaisen kyberturvallisuuden sertifiointijärjestelmien elementtien osalta. Komissiolla olisi valtuudet antaa täytäntöönpanoasetuksia, joilla vahvistettaisiin vähintään viiden vuoden vertaisarviointisuunnitelma.

Komissio voisi antaa täytäntöönpanosäädöksiä, joilla se voisi riskiarvioinnin pohjalta nimetä kolmannen maan maaksi, joka aiheuttaa kyberturvallisuushuolia *(country posing cybersecurity concerns)* ICT-toimitusketjuille. Komissio voisi täytäntöönpanoasetuksella laatia listan korkean riskin toimittajista, joihin ehdotuksen rajoitukset kohdistuisivat. Komissio voisi täytäntöönpanoasetuksella määritellä tarkemmin ehdot, joilla korkean riskin toimittajalle voidaan myöntää poikkeus siihen kohdistuvista rajoituksista. Komissio voisi antaa täytäntöönpanoasetuksia, joilla se voisi määritellä kriittiset ICT-osat, joita NIS 2 -direktiivin liitteiden I ja II toimijat käyttävät tuotteidensa tai palvelujensa tarjoamiseen. Komissio voisi antaa täytäntöönpanoasetuksia, joilla se voisi kieltää NIS 2 -direktiivin liitteiden I ja II toimijoita käyttämästä, asentamasta tai integroimasta kriittisiin ICT-osiin korkean riskin toimittajien ICT-komponentteja tai komponentteja sisältäen ICT-komponentteja. Komissio määrittelisi täytäntöönpanoasetuksilla asianmukaiset siirtymäajat. Komissio voisi esittää täytäntöönpanoasetuksilla riskienhallintatoimenpiteitä ICT-toimitusketjuihin ja keskeisiin ICT-osiin NIS 2 -direktiivin liitteiden I ja II tietyille toimijoille. Komissio voisi huomioida näiden toimijoiden koon täytäntöönpanoasetuksia laatiessaan. Täytäntöönpanoasetukset koskettaisivat myös EU:n instituutioita, elimiä, toimistoja ja virastoja.

NIS 2 -muutosdirektiiviä koskevan ehdotuksen mukaan komissio voisi antaa täytäntöönpanosäädöksiä riskienhallintaa koskevista teknisistä ja metodologisista vaatimuksista sekä toimialakohtaisista vaatimuksista. Ehdotuksen mukaan komission antamat täytäntöönpanosäädökset olisivat täysharmonisoivia. Lisäksi muutosdirektiivillä ehdotetaan laajennettavaksi komissiolle siirrettyä säädösvaltaa merkittävistä poikkeamista ilmoittamista koskevien täytäntöönpanosäädöksien antamisesta siten, että komission tulisi täytäntöönpanosäädöksissä edellyttää toimijoita ilmoittamaan kiristyshaittaohjelmahyökkäykseen liittyviä tietoja.

5 Ehdotuksen vaikutukset.

5.1 Taloudelliset vaikutukset

Komission arvion mukaan Euroopan kyberturvallisuusvirasto ENISA:n toimintakentän laajentamisella voitaisiin saavuttaa tarkastelujaksolla 14,6 miljardin euron säästöt unionin alueella toimiville yrityksille. Lisäksi mahdollisuus torjua kyberuhkia ja niiden vaikutuksia nopeammin ja tehokkaammin voisi tuoda unionin tasolla noin 3,7–4,4 miljardin euron säästöt.

Ehdotuksella kasvatettaisiin ENISA:n toimintamenoja merkittävästi. ENISA:n toimintamenot vuosien 2028–2034 aikana olisivat keskimäärin 50 miljoonaa euroa vuodessa. Vuonna 2025 ENISA:n toimintamenot olivat noin 26 miljoonaa euroa ja henkilöstömäärä noin 131 henkilötyövuotta. Vuoteen 2031 mennessä ENISA:n henkilöstömäärän esitetään kasvavan noin 260 henkilötyövuoteen. Ehdotuksella olisi vaikutuksia myös Liikenne- ja viestintävirasto Traficomin tai muun lähettävän kansallisen viranomaisen toimintamenoihin. Ehdotettu velvoite nimittää kaksi jäsenmaiden maksamaa kansallista asiantuntijaa aiheuttaisi noin 200 000 euron kustannuksen vuosittain.

Myös Euroopan komissiolle ehdotetaan ehdotuksessa esitettyjen tehtävien hoitoon lisäresursointia yhteensä 50 henkilötyövuoden verran. Lisäresursoinnilla hoidettaisiin operatiiviseen yhteistyöhön, Euroopan kyberturvallisuuden osaamisen viitekehykseen (ECSF), sertifiointeihin sekä ICT-toimitusketjujen riskiarviointeihin liittyviä tehtäviä.

Komission arvion mukaan sertifiointikehyksestä aiheutuva kustannusarvio jäsenvaltioiden henkilöstövaikutusten osalta on noin 2–10 henkilötyövuotta riippuen valmisteltavista kyberturvallisuuden sertifiointijärjestelmistä ja olemassa olevasta henkilöstöstä tai sen mahdollisesta lisäämisestä. Komission arvion mukaan kybertason sertifiointi kustantaisi yritykselle noin 30 000 euroa kunkin sertifioinnin osalta. Komission laskelmien mukaan sertifiointijärjestelmien laatiminen, ylläpito ja myöntäminen rahoitettaisiin tulevaisuudessa kokonaan tai osittain ENISA:n keräämillä maksuilla. Muutos maksulliseen toimintaan tapahtuisi portaittain.

Komissio on arvioinut, että tiettyjen korkean riskin toimittajien osien vaihtamisesta aiheutuvat vuosittaiset kustannukset kolmen vuoden aikajänteellä olisivat 3,4–4,3 miljardin euron luokassa matkaviestinverkkojen operaattoreille. Samalla investoinnit luotettuihin toimittajiin kasvaisivat vuosittain enimmillään 2 miljardiin euroon vuodessa. Ehdotuksella saattaa olla vaikutusta jäsenvaltioiden mahdolliseen korvausvelvollisuuteen. Komissio ei ole asetusehdotuksessaan eikä sitä koskevassa vaikutustenarvioinnissa arvioinut EU-tasoisesti niitä korvausjärjestelyjä tai -mahdollisuuksia, jotka liittyvät korkean riskin toimittajien ICT-komponenttien vaihtamiseen. Komissio ei ole tarkemmin arvioinut mahdollisia kustannuksia muille NIS2-direktiivin toimialoille, joihin ICT-toimitusketjuja koskevat velvoitteet kohdistuisivat. Vaikutukset riippuvat myös siitä, milloin verkkolaitteiden käyttöä koskevat rajoituksen tulisivat voimaan.

NIS 2 -muutosdirektiivin ehdotuksilla voi olla taloudellisia vaikutuksia direktiivin soveltamisalaan kuuluville toimijoille, joita ovat Suomessa kyberturvallisuuslain tai julkisen hallinnon tiedonhallinnasta annetun lain 4 a luvun soveltamisalaan kuuluvat toimijat ja viranomaiset. Muutoksilla tavoitellaan muun muassa sääntelyn noudattamisesta ja vaatimustenmukaisuuden osoittamisesta aiheutuvien kustannuksien alentamista. Osa ehdotuksista, kuten kiristyshaittaohjelmatietojen raportointia koskeva säännös, voi sinänsä aiheuttaa myös sääntelyn noudattamisesta aiheutuvien kustannuksien kasvua. Taloudelliset vaikutusten määrä vaihtelee toimijakohtaisesti. Vaikutukset olisivat merkittävimpiä sellaisille toimijoille, jotka saatettaisiin uusina direktiivin soveltamisalaan.

5.2 Vaikutukset kansalliseen lainsäädäntöön

Kyberturvallisuusasetuksen säännöksiä eurooppalaista kyberturvallisuuden sertifiointikehystä täydentävät kansalliset säännökset sisältyvät nykyisin sähköisen viestinnän palveluista annettuun lakiin (917/2014). Eduskunnassa on vireillä hallituksen esitys HE 179/2025 vp, jolla kyberturvallisuussertifiointeihin liittyviä kansallisia säännöksiä on esitetty täydennettäviksi sekä siirrettäväksi sähköisen viestinnän palveluista annetusta laista uuteen, esityksellä eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista ehdotettuun lakiin.

Kyberturvallisuusasetuksen uudistus edellyttänee kyberturvallisuussertifiointia täydentävien kansallisten säännösten arviointia ja muuttamista.

Ehdotuksessa esitetyt ICT-toimitusketjuja koskevat säännökset edellyttäisivät ainakin sähköisen viestinnän palveluista annetun lain säännösten tarkastelua. Ehdotukset saattavat aiheuttaa muutoksia myös kyberturvallisuuslakiin (124/2025). Ehdotus voisi edellyttää myös hankintalain tarkastelua julkisiin ICT-hankintoihin kohdistuvien velvoitteiden osalta. Kansallisen lainsäädännön osalta tulisi varmistaa, että sääntely on yhdenmukainen asetusehdotuksen ICT-toimitusketjuja koskevien säännösten kanssa, jotta kansallinen lainsäädäntö ei ole päällekkäistä tai ristiriidassa unionin oikeuden kanssa.

NIS 2 -direktiivin muutoksien saattaminen osaksi kansallista lainsäädäntöä edellyttänee muutoksia kyberturvallisuuslakiin (124/2025) ja julkisen hallinnon tiedonhallinnasta annettuun lakiin (906/2019). Muutokset saattavat aiheuttaa myös muita vaikutuksia kansalliseen lainsäädäntöön.

Euroopan kyberturvallisuusvirasto ENISA:a koskevilla ehdotuksilla ei ole tunnistettu olevan merkittäviä vaikutuksia kansalliseen lainsäädäntöön. Ehdotukset voivat aiheuttaa tarvetta arvioida viranomaisten tiedonvaihtoon ja yhteistyöhön liittyviä säännöksiä.

5.3 Vaikutukset viranomaistoimintaan

Ehdotuksella voisi olla vaikutuksia viranomaistoimintaan, erityisesti Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen osalta. ENISA:n suurempi rooli operatiivisessa yhteistyössä vaikuttaisi koko unionin vakiintuneiden kyberturvallisuusverkostojen (kuten CSIRT-verkosto ja EU-CyCLONe) toimintaan ja niissä tehtävään tiedonvaihtoon. ENISA:n vahvempi rooli tilannekuvan tuottamisessa voisi jossain määrin vähentää kansallisesti tuotettujen tilannekuvatuotteiden tarvetta pidemmällä aikavälillä. Ehdotus voisi kuitenkin myös kuormittaa viranomaisia, mikäli viranomaisilta edellytetään lisääntynyttä raportointia ja tiedonjakoa ENISA:lle.

Eurooppalaisen kyberturvallisuuden sertifiointikehyksen uudistukset vaikuttavat kansallisten toimivaltaisten viranomaisten tehtäviin ja toimivaltuuksiin. Ehdotuksessa asetettaisiin tehtäviä ja vaatimuksia kansallisille kyberturvallisuuden sertifiointiviranomaisille ja vaatimustenmukaisuuden arviointilaitoksille. Suomessa ei ole vielä kyberturvallisuusasetuksen mukaisia vaatimustenmukaisuuden arviointilaitoksia. Ehdotuksen mukaan jäsenvaltioiden on huolehdittava kansallisten kyberturvallisuuden sertifiointiviranomaisten riittävästä resursoinnista niiden tehtävien ja toimivallan hoitamiseksi.

ICT-toimitusketjujen turvallisuutta koskevien säännösten pohjalta kansallisille toimivaltaisille viranomaisille esitettäisiin uusia valvonta- (*supervisory*) ja täytäntöönpanotehtäviä (*enforcement*) NIS2-direktiivin (2022/2555) liitteiden I ja II toimijoille. Ehdotuksen mukaan toimivaltaisten viranomaisten tulisi olla rakenteellisesti ja toiminnallisesti täysin puolueettomia ja vapaita kaikesta ulkoisesta vaikuttamisesta. Niiden ei tulisi hakea eikä vastaanottaa ohjeita miltään muulta viranomaiselta tai yksityiseltä taholta. Ehdotuksen mukaan jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on riittävät toimivaltuudet, riittävät resurssit sekä tarvittava asiantuntemus tehtäviensä tehokkaaseen hoitamiseen.

NIS 2 -muutosdirektiiviin sisältyvillä ehdotuksilla olisi vaikutuksia kansallista täytäntöönpanevaa sääntelyä eli kyberturvallisuuslakia ja julkisen hallinnon tiedonhallinnasta annetun lain 4 a lukua valvoville viranomaisille. Soveltamisalaa ja keskeisen toimijan kokorajaa

koskevat ehdotukset vaikuttavat soveltamisalaan ja valvonnan alaan kuuluvien toimijoiden määriin.

Esitykseen sisältyvä huomattava määrä täytäntöönpanosäädöksiä aiheuttaisi vaikutuksia niille ministeriöille, joiden toimialaan liittyen delegoituja säädöksiä valmisteltaisiin komitologiamenettelyissä.

5.4 Muut vaikutukset

Ehdotuksella ENISA:n toiminnan täydentämiseksi voidaan vahvistaa koko unionin kyberturvallisuutta. Ehdotus erityisesti vahvistaa NIS2-direktiivissä luotujen EU-tason kyberturvallisuuden yhteistyö- ja tiedonvaihtoverkostojen (CSIRT-verkosto ja EU-CyCLONe) toimintaa kyberuhkien havainnoinnissa, uhkiin reagoinnissa ja kyberhäiriöistä toipumisessa. Ehdotus selkeyttää näiden verkostojen toimintaa kyberpoikkeamatilanteissa sekä ENISA:n roolia näissä tilanteissa. Ehdotuksella voidaan myös ennaltaehkäistä kyberturvallisuushäiriötä paremman, laajemman ja ajankohtaisemman tilannekuvan ansiosta. Ehdotus todennäköisesti vaikuttaisi erityisesti matalamman kypsyystason maiden kyberturvallisuuden kehittymiseen, sillä jatkossa ENISA tarjoaisi selkeämmin esimerkiksi tukea harjoitteluun sekä häiriöistä toipumiseen. Paremmat tilannekuvatuotteet sekä tehokkaampi yhteistyö unionin tasolla voi myös tukea EU:n alueella toimivia yrityksiä kyberuhkiin varautumisessa ja niihin reagoinnissa, ja siten pienentää vakavien ja laaja-alaisten kyberhäiriöiden todennäköisyyttä.

Ehdotus ENISA:n roolista EU-tason tietojärjestelmien haavoittuvuuksien tietokannan ylläpidossa ja haavoittuvuuksien hallinnassa vahvistaa unionin strategista autonomiaa ja riippumattomuutta unionin ulkopuolisista palveluntarjoajista.

Euroopan kyberturvallisuuden osaamiskehyksen ylläpitoon ja sen perusteella myönnettävien osaamistodistusten vaikutuksia työmarkkinoihin tai kyberturvallisuuden osaajamäärän kasvattamiseen on vain osittain arvioitu ehdotuksessa. Komission arvion mukaan ehdotus voisi lisätä eurooppalaisten osaamisen todentajien määrää sekä parantaisi eurooppalaisten yritysten ymmärrystä erilaisista kyberturvallisuuden osaamistarpeista. Sen sijaan ehdotuksen vaikutuksia kyberturvallisuusosaajien määrään tai tasoon ei ole erikseen arvioitu.

ICT-toimitusketjujen turvallisuutta koskevilla säännöksillä voi olla myös erilaisia kauppapoliittisia ja ulkopoliittisia vaikutuksia.

6 Ehdotuksen suhde perustuslakiin sekä perus- ja ihmisoikeuksiin

Komissio arvioi, että ENISA:n mandaatti edistäisi kyberturvallisuutta koko talousalueella ja yleisesti yhteiskunnassa sekä parantaisi henkilöiden yksityisyyttä ja henkilötietojen suojaa. Ehdotus tukisi myös kyberturvallisuuteen liittyvää koulutusta ja harjoittelua, sillä se selkeyttäisi ENISA:n roolia kyberturvallisuuden parissa työskentelevien kykyjen kehittämisessä.

Eurooppalaisen kyberturvallisuuden sertifiointikehyksen osalta komissio toteaa, että se lisäisi yleisön ja yritysten luottamusta tieto- ja viestintäteknologian ratkaisuihin erityisesti, kun kriittinen sektori voisi sertifioinneilla osoittaa korkeaa kyberturvallisuuden tasoa. Lisäksi komissio toteaa, että luottamusta arkaluonteisten tietojen suojaamiseen voitaisiin lisätä harmonisoimalla kiristyshaittaohjelmatapausten raportointia ja edistämällä siirtymistä kvantinkestävään salaukseen.

Komission arvion mukaan ehdotuksen ICT-toimitusketjujen turvallisuutta koskevilla säännöksillä on jonkinasteista vaikutusta perusoikeuksien suojaan, sillä ne rajoittavat EU:n

ulkopuolista vaikuttamista. Ehdotuksen mukaisilla toimenpiteillä voisi komission mukaan lisätä siten luottamusta, turvallisuutta ja yksityisyyden suojaa eri teknologioissa ja digitaalisissa ratkaisuissa.

Ehdotuksella voisi olla myönteisiä vaikutuksia perusoikeuksien suojaamiseen, kuten perustuslain 10 §:n yksityiselämän suojaan ja luottamuksellisen viestinnän suojaan. Ehdotus koskettaa sellaisia yhteiskunnan kannalta kriittisiä toimialoja, jotka toiminnassaan käsittelevät laajasti erilaisia tietoja, mukaan lukien henkilötietoja sekä välittävät luottamuksellista viestintää. Ehdotuksen mukaan kyberturvallisuushuolia aiheuttavien maiden korkean riskin toimittajat voisivat aiheuttaa ICT-toimitusketjuissa erilaisia riskejä, kuten tietojen vuotamisen tällaisiin maihin. Ehdotuksen mukaisilla toimenpiteillä komissio pyrkisi ennaltaehkäisemään tämäntyyppisiä riskejä.

Komissio on ennen ehdotuksen antamista pyrkinyt ensin edistämään ehdotuksessa esitettyjä tavoitteita erityisesti 5G-viestintäverkkojen turvallisuuden varmistamiseksi vuonna 2020 julkaistuilla EU:n 5G-suosituksilla. Komissio on arvioinut, että jäsenvaltioiden erilaiset ratkaisut eivät ole olleet riittäviä varmistamaan 5G-viestintäverkkojen turvallisuus EU:n 5G-suosituksissa tarkoitetulla tavalla ja esittää osin tästä syystä ehdotuksessa esitettyjä toimenpiteitä.

Ehdotettu sääntely on merkityksellistä perustuslain 15 §:ssä turvatun omaisuudensuojan kannalta, sillä käsillä oleva ehdotus voisi kieltää NIS2-direktiivin toimialoihin kuuluvia toimijoita käyttämästä, asentamasta ja integroimasta missään muodossa korkean riskin toimittajien ICT-komponenttien käytön tuotteidensa ja palvelujensa tarjoamiseksi unionissa. Lisäksi ehdotettu sääntely on merkityksellistä perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta, sillä ehdotuksella voisi asettaa korkean riskin toimittajille rajoituksia sisämarkkinoilla toimimiselle.

Edellä todettuihin perusoikeuksiin kohdistuvan puuttumisen perusteena olisi ehdotuksen mukaan ICT-toimitusketjujen häiriöttömän toiminnan turvaaminen unionissa ja ICT-toimitusketjuihin kohdistuvien ei-teknisten riskien hallinta. Ehdotuksen mukaan ICT-toimitusketjuihin kohdistuvat häiriöt voivat vaikuttaa haitallisesti sisämarkkinoiden toimintaan, aiheuttaa taloudellisia menetyksiä, rapauttaa käyttäjien luottamusta palveluihin ja tuotteisiin sekä aiheuttaa vakavaa vahinkoa unionin talousalueelle ja jäsenvaltioiden toimintaan.

EU:n perusoikeuskirjan 52 artiklan 1 kohdan mukaan oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

Ehdotuksen mukaan mahdollista kieltoa käyttää korkean riskin toimittajien ICT-komponentteja edeltäisi erilaiset oikeasuhtaisuutta lisäävät toimenpiteet. Ensiksi jäsenvaltiot ja komissio laatisivat yhteisen riskiarvion ICT-toimitusketjuun kohdistuvista riskeistä, keskeisistä uhkatoimijoista sekä haavoittuvuuksista, jotka kohdistuisivat arvioinnissa tunnistettuihin kriittisiin ICT-osiin. Mikäli tällaisessa riskiarvioinnissa, tai jäsenvaltion julkilausuman pohjalta, olisi näyttöä siitä, että kolmas maa aiheuttaisi vakavan ja rakenteellisen ei-teknisen riskin ICT-toimitusketjuille, komissio laatisi tämän pohjalta erillisen arvion ehdotuksessa esitettyjen kriteerien pohjalta. Komissio ottaisi arvioinnissa huomioon mahdollisten rajoitusten vaikutukset NIS2-direktiivin toimialojen toimintaan ja vaihtoehtoisten toimittajien saatavuus, joilla korkean riskin toimittajien ICT-komponentit voisi korvata.

Täytäntöönpanoasetuksia laatiessaan komissio kuulisi prosessissa jäsenvaltioita tarkastelumenettelyssä. Lisäksi komissio kävisi alustavat havaintonsa läpi arvioinnin korkean riskin arvioinnin kohteena olevan toimijan kanssa ja varaisi tälle mahdollisuuden tulla kuulluksi. Toimija, joka on perustettu tai jota kontrolloidaan kyberturvallisuushuolia aiheuttavasta kolmannesta maasta voisi hakea poikkeusta korkean riskin toimittajille asetettaviin rajoituksiin ehdotuksessa mainituin ehdoin. Korkean riskin toimittajien listauksessa oleva toimija voisi pyytää komissiota laatimaan uuden arvion, mikäli toimija toimittaa näyttöä muutoksista.

Perustuslakivaliokunta on aiemmissa lausunnoissaan todennut, että omaisuus ei ole perustuslain suojaama kaikkia käyttörajoituksia vastaan, ja että omistajan oikeuksia voidaan rajoittaa lailla, joka täyttää perusoikeutta rajoittavalta laita vaaditut yleiset edellytykset (PeVM 25/1994 vp). Perustuslakivaliokunnan lausuntokäytännön (10/2007 vp) mukaan lainsäätäjän liikkumavara omaisuudensuojan rajoittamisessa on suurempi, kun sääntelykohteella on erityispiirteitä, kuten teknologian monimutkaisuus ja kansainvälinen toimintaympäristö, velvoitteet kohdistuvat pörssiyhtiöihin tai varallisuusmassaltaan huomattaviin oikeushenkilöihin ja kysymys on EU-tason sääntelystä, joihin edellä todettujen yritysten tulee varautua. Lisäksi Euroopan unionin tuomioistuimen oikeuskäytännön (C-292/97) mukaan perusoikeuksien käyttämiseen voidaan asettaa rajoituksia, edellyttäen että nämä rajoitukset tosiasiallisesti vastaavat yhteisön (unionin) tavoittelemaa yleistä etua eivätkä ne muodosta tavoiteltavaan päämäärään nähden suhteetonta ja kohtuutonta puuttumista, joka vaarantaa perusoikeuksien ytimen. Perustuslain 15 §:n 2 momentin mukaan omaisuuden pakkolunastuksesta yleiseen tarpeeseen täyttä korvausta vastaan säädetään lailla. Ehdotuksen mukaiset toimenpiteet, joissa kielletään NIS2-direktiivin toimialoihin kuuluvia toimijoita käyttämästä korkean riskin toimittajien ICT-komponentteja, voisi olla merkityksellinen perustuslain 15 §:n 2 momentissa tarkoitetun pakkolunastuksen kannalta. Perustuslakivaliokunta on lausuntokäytännössään (35/2020 vp) katsonut, että edellä todetun säännöksen soveltamisala ei rajoitu ainoastaan sellaisiin tilanteisiin, joissa omistusoikeus siirtyy subjektilta toiselle. Perustuslakivaliokunnan mukaan omaisuuden käyttörajoitus voi olla niin merkittävä, että se rinnastuu tosiasiallisilta vaikutuksiltaan pakkolunastukseen, jolloin sitä on arvioitava perustuslain 15 §:n 2 momentin kannalta. Omaisuudensuojaan puuttuvaa sääntelyä arvioidaan perusoikeuksien yleisten rajoitusedellytysten, kuten sääntelyn tarkoituksen hyväksyttävyyden ja sääntelyn oikeasuhtaisuuden kannalta (PeVL 31/2006 vp).

Komission ehdotuksen voidaan arvioida olevan merkityksellinen perustuslain 12 §:n 2 momentin mukaisen julkisuusperiaatteen ja salassa pidettävien tietojen luovuttamisen kannalta. Asetuksen mukainen tietojen luovuttaminen saattaisi edellyttää salassa pidettävien tietojen luovuttamista ENISA:lle, EU:n komissiolle sekä muille jäsenmaille. Komissio ei ole tarkemmin arvioinut salassa pidettävien tietojen ja tiedonvaihdon merkitystä.

Perustuslakivaliokunta on aiemmissa lausunnoissaan kiinnittänyt huomiota muun muassa siihen, mihin ja ketä koskeviin tietoihin tiedonsaantioikeus ulottuu ja miten tiedonsaantioikeus sidotaan tietojen välttämättömyyteen. Viranomaisen tietojensaantioikeus ja tietojenluovuttamismahdollisuus ovat valiokunnan mukaan voineet liittyä jonkin tarkoituksen kannalta ”tarpeellisiin tietoihin”, jos tarkoitetut tietosisällöt on pyritty luettelemaan laissa tyhjentävästi. Jos taas tietosisältöjä ei ole samalla tavoin luetteloitu, sääntelyyn on pitänyt sisällyttää vaatimus ”tietojen välttämättömyydestä” jonkin tarkoituksen kannalta (esim. PeVL 13/2023 vp ja PeVL 92/2022)). Valiokunta ei kuitenkaan ole pitänyt hyvin väljiä ja yksilöimättömiä tietojensaantioikeuksia perustuslain kannalta mahdollisina edes silloin, kun ne on sidottu välttämättömyyskriteeriin (esim. 96/2022 vp). Tiedonluovutussäännösten täsmällisyyden ja sisällön arvioinnissa on annettu erityistä merkitystä luovutettavien tietojen luonteelle arkaluonteisina tietoina (esim. PeVL 96/2022).

Valtioneuvosto yhtyy pääosin komission näkemyksiin. Ehdotus voi edistää perusoikeuskirjan 8 artiklan ja perustuslain 10 §:ssä turvattua henkilötietojen suojaa. Valtioneuvosto katsoo, että ehdotus hyödyttää julkista sektoria, mutta toisaalta lisää yksityisten henkilöiden luottamusta kyberturvallisuuden toimintakenttään ja henkilötietojen suojaan. Valtioneuvosto kiinnittää jatkovalmistelussa huomiota perustuslain 12 §:ään ja tiedonvaihtoon liittyvän sääntelyn tarkkarajaisuuteen ja täsmällisyyteen. Sääntelyä tulisi tältä osin mahdollisesti täydentää.

7 Ahvenanmaan toimivalta

Kyberturvallisuusasetuksen uudistuksessa ja NIS2-muutosdirektiivissä säädettäisiin kyberturvallisuuteen liittyvistä toimista, joilla yksinkertaistettaisiin, tehostettaisiin ja selkeytettäisiin jäsenvaltioiden ja unionin elinten välistä yhteistyötä ja luotaisiin yhdenmukaisemmat markkinat kyberturvallisuuden saralta. Toimivalta valtakunnan ja maakunnan lainsäädäntövallan välillä jakautuu Ahvenanmaan itsehallintolain (1144/1991, jäljempänä itsehallintolaki) mukaisesti. Itsehallintolaissa ei säädetä erikseen kyberturvallisuutta tai tietoturvallisuutta koskevan lainsäädäntövallan jaosta. Näin ollen asiaa on arvioitava muiden itsehallintolain mukaisten maakunnan ja valtakunnan välistä toimivaltajakoa koskevien perusteiden mukaisesti.

Itsehallintolain 27 §:n mukaan valtakunnalla on lainsäädäntövalta asioissa, jotka koskevat muun ohella valtion viranomaisten järjestysmuotoa ja toimintaa, standardisointia, teletoimintaa sekä muita kuin pykälässä erityisesti mainittuja yksityisoikeudellisia kysymyksiä, jollei kysymys välittömästi liity sellaiseen oikeudenalaan, joka itsehallintolain mukaan kuuluu maakunnan lainsäädäntövaltaan. Itsehallintolain 18 §:n mukaan maakunnalla on lainsäädäntövalta asioissa, jotka koskevat muun ohella maakunnan hallitusta sekä sen alaisia viranomaisia ja laitoksia, terveyden- ja sairaanhoitoa eräin poikkeuksin sekä elinkeinotoimintaa eräin poikkeuksin.

Valtioneuvosto katsoo, että ehdotukset jakautuvat osin valtakunnan ja osin maakunnan lainsäädäntövaltaan. Kyberturvallisuusasetusta koskevan ehdotuksen osalta esitys kuuluu pääosin valtakunnan lainsäädäntövaltaan. Kyberturvallisuusasetuksen ICT-toimitusketjujen turvallisuutta koskevien ehdotuksien osalta sekä NIS 2 -direktiivin muuttamista koskevien ehdotuksien osalta esitys jakautuu valtakunnan ja maakunnan lainsäädäntövaltaan siltä osin kuin ehdotukset koskevat toimialoja, joissa maakunnalla on itsehallintolain nojalla lainsäädäntövalta.

8 Ehdotuksen käsittely Euroopan unionin toimielimissä ja muiden jäsenvaltioiden kannat

Komissio antoi asetusehdotuksen 20.1.2026.

Ehdotuksen käsittely on alkanut neuvoston horisontaalisessa kybertyöryhmässä 26.1.2026. Ehdotuksen käsittely Euroopan parlamentissa ei ole vielä alkanut.

9 Ehdotuksen kansallinen käsittely

U-kirjelmä on valmisteltu liikenne- ja viestintäministeriössä virkatyönä.

U-kirjelmä käsitellään raha-asianvaliokunnassa 12.3.2026. Luonnos U-kirjelmäksi on käsitelty jaostoissa viestintä- ja hybridijaostoissa 13.-16.2.2026. Lisäksi ehdotuksesta järjestettiin kuulemistilaisuudet viranomaisille ja yksityiselle sektorille 4.2.2026.

10 Valtioneuvoston kanta

Kyberturvallisuusasetus (CSA2)

Valtioneuvosto katsoo kyberturvallisuuden olevan olennainen osa EU:n sisämarkkinoiden häiriöttömän toiminnan ja yhteiskuntavakauden sekä kansalaisten yksityisyyden turvaamista. Valtioneuvosto kannattaa EU:n lainsäädännön tavoitetta vahvistaa kyberturvallisuuden hallinnointia sekä sitä, että asiaankuuluvilla toimielimillä, viranomaisilla ja muilla sidosryhmillä olisivat paremmat edellytykset estää, havaita ja torjua kyberturvallisuusuhkia koordinoidulla ja tehokkaalla tavalla.

Valtioneuvosto suhtautuu myönteisesti Euroopan kyberturvallisuusvirasto ENISA:n mandaatin kokonaisvaltaiseen uudelleentarkasteluun muuttunut uhkaympäristö sekä unionin kyberturvallisuuslainsäädäntö huomioiden. Valtioneuvosto katsoo, että ENISA:n toiminnan tulee olla tehokasta, priorisoitua ja läpinäkyvää. ENISA:n toiminnan ja tehtävien tulisi ensisijaisesti täydentää jäsenmaiden viranomaisten kyberturvallisuustehtäviä.

Valtioneuvosto suhtautuu myönteisesti ENISA:n toiminnan laajentamiseen operatiivisen yhteistyön tukeen sekä tilannekuvan tuottamiseen huomioiden kuitenkin, että ensisijainen vastuu kyberturvan tasoa varmistavissa ja yhteiskunnan toimijoita tukevissa viranomaistehtävissä on jäsenmailla ja sen viranomaisilla. Tiedonvaihtoon, jolla voisi olla negatiivisia vaikutuksia kansalliseen turvallisuuteen, suhtaudutaan varauksellisesti. Valtioneuvosto suhtautuu kuitenkin myönteisesti ENISA:n yhteistyön tiivistämiseen kumppanimaiden ja kansainvälisten organisaatioiden, kuten NATO:n kanssa.

Valtioneuvosto pitää ENISA:n tehtävien laajentamista tietojärjestelmähaavoittuvuuksien hallintaan liittyviin palveluihin erityisen tärkeänä. Unionin omien kyvykkyyksien vahvistaminen tietojärjestelmähaavoittuvuuksien hallinnassa vahvistaa unionin strategista autonomiaa.

Valtioneuvosto pitää tärkeänä, että jäsenmaat ja komissio ovat jatkossakin tasa-arvoisessa asemassa ENISA:n toimintaan liittyvässä päätöksenteossa. Jäsenmaiden tulee itse voida päättää viraston toimielimiin nimitettävistä edustajista sekä virastoon lähetettävistä asiantuntijoista.

Valtioneuvosto pitää tärkeänä, että tällä asetuksella ei ennakoida tulevan rahoituskehyksen (2028–2034) rahoitusta. Tulevan kauden rahoituksen mitoitukseen otetaan kantaa erikseen osana rahoituskehysneuvottelujen kokonaisuutta.

Valtioneuvosto korostaa, että EU:n toimielinten ja virastojen hallintomenojen taso sekä henkilöstömäärä on pidettävä maltillisena. Valtioneuvosto pyytää jatkovalmistelussa tarkennuksia ENISA:n keräämiin maksuihin ja toiminnan rahoittamiseen liittyen.

Valtioneuvosto suhtautuu kyberturvallisuuden osaamiseen liittyvän tarkemman sääntelyn kehittämiseen varauksellisesti. Valtioneuvosto pitää tärkeänä varmistaa, että osaamisen liittyvät toimenpiteet ovat jäsenvaltioille vapaaehtoisia ja resurssineutraaleja.

Valtioneuvosto tukee yleisesti eurooppalaisen kyberturvallisuuden sertifiointikehyksen uudistamista, tehostamista ja selkeyttämistä. Valtioneuvosto suhtautuu lähtökohtaisesti myönteisesti kybertason ja EU:n lainsäädännön vaatimustenmukaisuusolettaman sisällyttämistä sertifiointijärjestelmien soveltamisalaan. Lisäksi valtioneuvosto kannattaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ylläpitostrategian ja -toimien lisäämistä osaksi sertifiointikehystä. Valtioneuvosto pitää tärkeänä, että jäsenvaltioilla on mahdollisuus osallistua eurooppalaisen kyberturvallisuuden sertifiointikehyksen prosesseihin. Lisäksi valtioneuvosto katsoo, että sertifiointien tulee säilyä lähtökohtaisesti vapaaehtoisina.

Valtioneuvosto pitää kannatettavana, että EU:ssa haetaan ehdotuksen pohjalta yhteisiä ICT-toimitusketjuja koskevia ratkaisuja, jotka vahvistavat näiden turvallisuutta, edistävät sisämarkkinoiden toimintaa ja EU:n teknologista suvereniteettia. Toimenpiteiden tulee olla ennakoitavia ja hallittuja sekä perustua asianmukaiseen kuulemiseen ja vaikutusarviointiin. Valtioneuvosto katsoo, että ehdotuksessa esitettyjen toimenpiteiden tulee olla myös oikeasuhtaisia ja riskiperustaisia. Valtioneuvosto pitää tärkeänä, että jäsenvaltiot voivat jatkossakin asettaa asetusehdotusta pidemmälle meneviä kansallisia velvoitteita ja toimenpiteitä, erityisesti viestintäverkkojen turvallisuuden varmistamiseksi. Valtioneuvosto tukee ehdotuksen tavoitetta ja pitää samalla tärkeänä, että unionin ja jäsenvaltioiden toimivallan rajat säilyvät selkeinä erityisesti kansallista turvallisuutta koskevissa asioissa. Valtioneuvosto myös korostaa jäsenvaltioiden keskeistä roolia ICT-toimitusketjujen riskien arvioinnissa.

Valtioneuvosto edellyttää, että komissiolle delegoitavat toimivaltuudet ovat tarkkarajaisia, oikeasuhtaisia, tarkoituksenmukaisia ja perusteltuja.

Suomen kantoja komission ja korkean edustajan tiedonantoon unionin taloudellisen turvallisuuden vahvistamiseksi on muodostettu selvityksessä E 3/2026 vp. Selvitys sisältää nyt kyseessä olevan ehdotuksen näkökulmasta olennaisen kirjauksen kansainvälisestä yhteistyöstä haitallisten riippuvuuksien vähentämiseksi:

Haitallisten riippuvuuksien vähentämiseksi EU:n tulee edetä nopeasti kauppaneuvotteluissa sekä kumppanuuksissa esimerkiksi kriittisten raaka-aineiden, teollisuuden, energian ja kriittisten teknologioiden toimitus- ja arvoketjuissa. EU:n tulisi kartoittaa standardipohjaisten markkinoiden luomisen edut ja mahdollisuudet ja panostaa sääntely-yhteistyöhön kolmasmaakumppaneiden kanssa. EU:n tulee hyödyntää unionin olemassa olevia välineitä laajasti myös kolmasmaayhteistyössä haitallisten riippuvuuksien purkamiseksi.

Lisäksi Suomen kantoja komission tiedonantoon osaamisunionista on muodostettu selvityksessä E 56/2025 vp, jonka osalta huomioidaan nyt kyseessä olevan ehdotuksen osalta seuraava kirjaus:

Suomi pitää tärkeänä, että komission ehdotukset perustuvat riittävän kattaviin vaikutusarviointeihin. Suomi korostaa, että EU-tason toimenpiteet on tärkeää suunnitella siten, että ne ovat kustannustehokkaita, eivät lisää hallinnollista taakkaa, huomioivat jäsenmaiden erilaiset koulutusjärjestelmät sekä työvoimapoliittiset painotukset ja hyödyntävät mahdollisimman paljon olemassa olevia rakenteita.

NIS 2 -muutosdirektiivi

Valtioneuvosto kannattaa muutosehdotuksien tavoitteita sääntelyn yksinkertaistamiseksi, sujuvoittamiseksi ja sääntelystä aiheutuvien hallinnollisten kustannuksien alentamiseksi. Valtioneuvosto suhtautuu myönteisesti muutosehdotuksiin, jotka edistävät näitä tavoitteita ja turvaavat samalla kyberturvallisuuden korkeaa tasoa.

Valtioneuvosto pitää tarpeellisena, että osana neuvotteluita arvioidaan tarkemmin ehdotuksen vaikutuksia sääntelystä toimijoille aiheutuviin kustannuksiin ja ehdotuksen tavoitteisiin.

Valtioneuvosto suhtautuu myönteisesti direktiivin soveltamisalaa koskeviin muutosehdotuksiin sekä ehdotukseen keskeisen toimijan kokorajan korottamisesta. Valtioneuvosto pitää tarpeellisena soveltamisalan tarkentamista erityisesti tuotantomäärältään vähäisten sähköntuottajien sekä kemianteollisuuden osalta. Valtioneuvosto pitää tarpeellisena, että neuvotteluissa arvioidaan yksityiskohtaisemmin komission ehdotusta strategisen

kaksikäyttöinfrastruktuurin omistajien ja operaattoreiden sisällyttämisestä direktiivin soveltamisalaan erityisesti maanpuolustuksen ja kansallisen turvallisuuden kannalta.

Valtioneuvosto pitää tärkeänä, että NIS 2 -direktiivin vaatimukset ovat oikeasuhtaisia ja riskiperusteisia. Valtioneuvosto suhtautuu alustavan varauksellisesti ehdotukseen komission toimivallasta täysharmonisoida riskienhallintatoimenpiteitä täytäntöönpanosäädöksillä. Valtioneuvosto pitää tarkoituksenmukaisena, että jäsenvaltioilla on riittävä kansallinen liikkumavara riskienhallintaa koskevien vaatimuksien asettamisessa.

Valtioneuvosto pitää lähtökohtaisesti hyvänä, että eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisia sertifiointeja voitaisiin hyödyntää NIS 2 -direktiivin vaatimustenmukaisuuden osoittamisessa.

Valtioneuvosto suhtautuu myönteisesti ehdotukseen ENISA:n tehtävästä laatia rajat ylittäviä kyberturvallisuusriskien arviointeja. Valtioneuvosto pitää kuitenkin tärkeänä, että ENISA:n toimivaltuus valvovien viranomaisten tukemisessa ja sitä koskevien tietojen saamisessa perustuu jäsenvaltion viranomaisen suostumukseen.

Valtioneuvosto suhtautuu alustavan varauksellisesti ehdotukseen kiristyshaittaohjelmatietojen ilmoittamiseen liittyviin uusiin velvollisuuksiin sekä ehdotukseen komissiolle siirretyn säädösvallan laajennuksesta kiristyshaittaohjelmatietojen ilmoittamista koskien. Valtioneuvosto pitää tältä osin tarpeellisena, että neuvotteluissa arvioidaan tarkemmin, miten ehdotus vaikuttaa sääntelystä toimijoille aiheutuviin kustannuksiin ja hallinnolliseen taakkaan.