Lausunto
Asianumero: U 17/2026 vp
Päivämäärä: 2.4.2026

Eevi Vuorinen, Marième Korhonen-Cara
TIO/TDL

Perustuslakivaliokunta

U 17/2026 vp Valtioneuvoston kirjelmä komission ehdotuksista EU:n kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi

Perustuslakivaliokunta on pyytänyt liikenne- ja viestintäministeriön asiantuntijalausuntoa valtioneuvoston kirjelmästä eduskunnalle (U 17/2026 vp) komission ehdotukseksi Euroopan parlamentin ja neuvoston asetukseksi Euroopan unionin kyberturvallisuusvirasto ENISA:sta, Euroopan kyberturvallisuuden sertifiointikehyksestä ja tieto- ja viestintätekniikan toimitusketjujen turvallisuudesta (COM(2026) 11 final, CSA2) sekä Euroopan parlamentin ja neuvoston direktiiviksi direktiivin (EU) 2022/2055 (NIS 2) muuttamisesta (COM(2026 13 final). Liikenne- ja viestintäministeriö kiittää mahdollisuudesta lausua asiassa ja esittää lausuntonaan kunnioittavasti seuraavan.

1. Lausunnon alasta

Lausunnossa keskitytään Euroopan komission 20.1.2026 antamiin ehdotuksiin EU:n kyberturvallisuusasetukseksi ja NIS 2-muutosdirektiiviksi erityisesti niiltä osin kuin valtioneuvoston kirjelmässä on tunnistettu perustuslakiin, perusoikeuksiin, kansalliseen liikkumavaraan tai julkisen vallan järjestämiseen liittyviä kysymyksiä.

2. Ehdotuksen pääasiallisesta sisällöstä ja käsittelyvaiheesta

Kyberturvallisuusasetuksen uudistamisen tavoitteena on kyberturvallisuuden kyvykkyyksien ja resilienssin lisääminen sekä sisämarkkinoiden pirstaloitumisen ehkäiseminen. Tavoitteena on 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.

Asetusehdotuksen 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.

NIS2-muutosdirektiivin tavoitteet ovat osa kyberturvallisuusasetuksen uudelleentarkastelun tavoitteiden toteuttamista. NIS2-muutosdirektiivin kohdennetuilla muutoksella tavoitellaan NIS2-

direktiivin vaatimuksenmukaisuuden yksinkertaistamista sekä johdonmukaisempaa täytäntöönpanoa.

Asetusehdotuksen ja muutosdirektiivin käsittely on käynnissä neuvoston horisontaalisessa kybertyöryhmässä. Puheenjohtajamaa Kypros pyrkii käsittelemään kyberturvallisuuspakettia tehokkaalla aikataululla ja ehdotustekstien ensimmäinen läpiluku saataneen tehtyä toukokuussa. Euroopan parlamentissa CSA2-asetusehdotuksen ja NIS 2-muutosdirektiivin pääkäsittelystä vastaava valiokunta on ITRE. Mietinnön esittelijät ovat Markéta Gregorová (Greens/EFA/CZ) ja Tomas Tobé (EPP, SE).

3. Valtioneuvoston kanta ehdotukseen

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 huomio, että muutoksiin sisältyy perusoikeusvaikutuksia, joita tulee arvioida tarkemmin erityisesti suhteessa julkisuusperiaatteeseen ja omaisuudensuojaan. Lisäksi valtioneuvosto katsoo, että jatkoneuvotteluissa olisi huolehdittava siitä, että säädös- ja täytäntöönpanovallan delegointi komissiolle on tarkoituksenmukaista sekä riittävän tarkkarajaista ja täsmällistä.

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 suhtautuu myönteisesti NIS 2-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 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.

Ehdotusten suhteesta perustuslakiin

Yksityiselämän suoja (PL 10 §): Valtioneuvosto huomioi, että 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. Ehdotuksen mukaisilla toimenpiteillä komissio pyrkisi ennaltaehkäisemään tämäntyyppisiä riskejä.

Valtioneuvosto katsoo, että ehdotus voi edistää perusoikeuskirjan perustuslain 10 §:ssä turvattua henkilötietojen suojaa.

Julkisuusperiaate (PL 12 §): 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 kiinnittää jatkovalmistelussa huomiota perustuslain 12 §:ään ja tiedonvaihtoon liittyvän sääntelyn tarkkarajaisuuteen ja täsmällisyyteen. Sääntelyä tulisi tältä osin mahdollisesti täydentää.

Omaisuudensuoja (PL 15 §): 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.

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).

Toimivallan siirto EU-tasolle ja sääntelyvallan delegointi: Valtioneuvoston kirjelmässä on käsitelty myös ehdotuksen oikeusperustaa sekä toimivallan siirtoa komissiolle. Komission ehdotuksen perustuva SEUT 114 artiklaan (sisämarkkinoiden toteuttaminen ja toimintaa koskevien toimenpiteiden antaminen). SEUT 114 artiklan nojalla annettavat säädökset hyväksytään tavallisessa lainsäätämisjärjestyksessä. Neuvosto tekee päätöksensä määräenemmistöllä.

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 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.