Liikenne- ja viestintäministeriö Perusmuistio EU/385/2026-LVM-22

Vuorinen Eevi 12.11.2026

U-jatkokirjelmä; Euroopan komission ehdotukset Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi

Eduskuntatunnus
U 17/2026 vp

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Euroopan komissio antoi 20.1.2026 ehdotuksen (COM(2026) 11 final) Euroopan parlamentin ja neuvoston asetukseksi Euroopan kyberturvallisuusvirasto ENISA:sta, Euroopan kyberturvallisuuden sertifiointikehyksestä ja ICT-toimitusketjujen turvallisuudesta) ja asetuksen (EU) 2019/881 kumoamisesta (CSA2, kyberturvallisuusasetus). Samanaikaisesti komissio antoi ehdotuksen (COM(2026) 13 final) NIS 2-direktiivin muuttamisesta (NIS 2-muutosdirektiivi).

CSA2-asetusehdotuksen käsittely aloitettiin Kyproksen puheenjohtajuuskaudella tammikuussa 2026 neuvoston horisontaalisessa kybertyöryhmässä. Ensimmäiset kompromissitekstit ENISA:n mandaatista (II osasto) ja kyberturvallisuuden sertifioinneista (III osasto) julkaistiin toukokuussa 2026. Televiestintäneuvosto otti puheenjohtajan ti-lanneselvityksen kyberturvallisuusasetuksesta ja NIS 2-muutosdirektiivistä tiedoksi 9.6.2026.

Irlannin puheenjohtajakaudella CSA2-ehdotusta on käsitelty kybertyöryhmässä aktiivisesti. Ensimmäinen kompromissiteksti ICT-toimitusketjujen turvallisuudesta (IV osasto) julkaistiin syyskuussa ja toinen kompromissi lokakuussa 2026. Muista osioista on julkaistu kompromissimuutoksia pitkin syksyä. NIS 2-muutosdirektiiviä ei ole käsitelty ensimmäisen toukokuussa 2026 käydyn läpiluvun jälkeen. Puheenjohtajan tavoitteena on löytää neuvoston kesken yhteisymmärrys molemmista ehdotuksista vuoden 2026 loppuun mennessä.

Euroopan parlamentin on tarkoitus äänestää kannastaan CSA2-ehdotuksesta helmikuussa 2027.

CSA2-asetusehdotuksesta ja NIS 2-muutosdirektiivistä annettiin valtioneuvoston U-kirjelmä (U 17/2026 vp) eduskunnalle 12.3.2026. Tämän U-jatkokirjelmän tarkoituksena on antaa tietoja eduskunnalle neuvottelujen etenemisestä sekä täydentää Suomen kantoja jatkoneuvotteluja varten erityisesti koskien ICT-toimitusketjujen turvallisuutta koskevia säännöksiä.

Suomen kanta

Valtioneuvosto on muodostanut kantoja asiakokonaisuuteen U-kirjelmällä U 17/2026 vp.

Valtioneuvosto täydentää ja täsmentää valtioneuvoston kirjelmässä (U 17/2026 vp) esitettyä kantaa ehdotuksen ICT-toimitusketjujen turvallisuutta koskevien säännösten osalta seuraavasti:

Valtioneuvosto katsoo, että asetuksen tai sen nojalla annettavien täytäntöönpanosäädösten vaihtamisvelvoitteiden valmistelussa tulee huomioida perustuslain 15 §:ssä suojattu omaisuuden suoja, jonka arvioinnin kannalta merkityksellisiä voivat olla siirtymäajat ja viestintäverkkojen osalta lisäksi vaihdettavien ICT-komponenttien käyttöiät, uusimissykli, niiden jäljellä oleva taloudellinen arvo ja saatavilla olevat vaihtoehdot. Valtioneuvosto katsoo, että ehdotuksen hyväksyttävyyteen voi suhtautua myönteisesti erityisesti, kun otetaan huomioon ehdotuksen myönteiset vaikutukset kyberturvallisuuden tasoon, teknologiseen suvereniteettiin ja Euroopan unionin sisämarkkinoiden häiriöttömään toimintaan.

Pääasiallinen sisältö

<u>Komission asetusehdotus</u>

Ehdotusten sisältöä on selostettu tarkemmin U-kirjelmässä U 17/2026 vp. Alla annetaan tiivistetty selostus alkuperäisten ehdotusten sisällöstä.

CSA2-asetusehdotuksella uudistettaisiin ENISA:n tehtävät ja mandaatti sekä kyberturvallisuuden sertifiointikehys. Lisäksi täysin uutena asiana ehdotetaan säädettäväksi ICT-toimitusketjujen turvallisuudesta ei-teknisten riskien hallitsemiseksi.

ENISA:n tehtäviä täydennettäisiin operatiivisen toiminnan, tilannekuvan tuottamisen sekä tietojärjestelmien haavoittuvuuksiin liittyvien palveluiden osalta. Lisäksi uudeksi tehtäväksi esitetään kyberosaamiseen liittyvien sertifikaattien kehittäminen ja myöntäminen. Ehdotus lisäisi tarvetta kasvattaa ENISA:n budjettia ja henkilöstömäärää merkittävästi. Jäsenvaltioiden tulisi myös nimetä kaksi jäsenvaltion rahoittamaa kansallista asiantuntijaa ENISA:n toiminnan tueksi.

Sertifiointikehyksen osalta asetusehdotuksessa esitetään, että sertifiointeja voitaisiin tulevaisuudessa antaa tieto- ja viestintätekniikan tuotteiden, palveluiden ja prosessien sekä tietoturvapalveluiden tarjoajien lisäksi organisaatioiden kybertasosta ja EU-sääntelyn vaatimustenmukaisuudesta. Lisäksi ENISA:n ylläpitämillä sertifiointijärjestelmillä tulisi olla ylläpitostrategia. Sertifiointijärjestelmien kehittämiseen ja ylläpitoon liittyvistä prosesseista säädettäisiin myös tiukemmin aikarajoin.

Asetusehdotuksessa esitetään uutena osa-alueena NIS 2-direktiivin kriittisten toimialojen ICT-toimitusketjujen ei-teknisten riskien hallintatoimenpiteitä. Tavoitteena on hallintatoimien yhdenmukaistaminen EU:ssa, joilla varmistettaisiin sisämarkkinoiden toiminta, edistettäisiin teknologista suvereniteettia ja vahvistettaisiin EU:n yhteistä kyberturvallisuuden ja resilienssin tasoa. Ehdotuksen mukaan ICT-toimitusketjuista voisi laatia yhteisiä riskiarviointeja, joiden pohjalta komissio voisi täytäntöönpanoasetuksilla tunnistaa kriittiset ICT-osat, nimetä kolmansia maita, jotka aiheuttavat kyberturvallisuushuolia ja nimetä niiden korkean riskin toimittajia ICT-toimitusketjuissa. Riskiarvion pohjalta komissio voisi kieltää korkean riskin toimittajien ICT-komponenttien käytön, asentamisen ja integroinnin NIS2-direktiivin toimialoilla. Korkean riskin toimittajille kohdistuisi erilaisia rajoituksia sisämarkkinoilla toimimiseen. Ehdotuksen pohjalta NIS2-direktiivin toimialoille olisi mahdollista osoittaa siirtymäajat kiellettyjen ICT-komponenttien vaihtamiseksi. Matkaviestintäverkkojen osalta komissio esittää enintään 36 kuukauden siirtymäaikaa kiellettyjen ICT-komponenttien vaihtamiseksi. Kiinteiden verkkojen, satelliittiviestintäverkkojen sekä muiden toimialojen osalta siirtymäajasta päätettäisiin erikseen täytäntöönpanoasetuksella. Ehdotuksen mukaan komissio voisi myöntää korkean riskin toimittajaksi tunnistetulle toimittajalle poikkeuksen rajoitusten kohdentamiseen tietyin ehdoin.

NIS 2-muutosdirektiivillä muutettaisiin direktiivin soveltamisalaa lisäämällä esimerkiksi digi-identiteettilompakot ja merenalainen datainfrastruktuuri sen piiriin ja poistamalla esimerkiksi DNS-palveluita tarjoavat mikro- ja pienyritykset sekä pitkäaikaista hoitoa tarjoavat terveyspalveluiden tuottajat. Komission riskienhallintatoimia koskevat täytäntöönpanoasetukset olisivat jatkossa täysharmonisoivia. Lisäksi NIS 2-muutosdirektiivillä säädettäisiin kiristyshaittaohjelmiin ja merkittäviin poikkeamiin liittyvien tietojen ilmoittamisesta kansallisesti ja komissiolle.

Keskeiset neuvoston käsittelyssä ehdotetut muutokset

ENISA:n mandaatin osalta puheenjohtajan uusimmassa kompromissiehdotuksessa on osin karsittu alkuperäisen asetusehdotuksen sisältämiä tehtäviä, jotka olisivat olleet jäsenvaltioiden viranomaisten tehtävien kanssa päällekkäisiä tai heikosti ENISA:lle sopivia, kuten kiristyshaittaohjelmiin ja varhaisiin varoituksiin liittyvät tehtävät. Suomi on korostanut, että ENISA:n tehtävien tulee olla erillisiä kansalliseen turvallisuuteen, mukaan lukien tiedusteluviranomaisten toimintaan nähden. Kompromissiehdotuksessa on lisäksi poistettu jäsenvaltioiden velvoite nimittää kaksi lähetettyä kansallista asiantuntijaa ENISA:an. Kansallisen asiantuntijan lähettämisen sijaan säilytettäisiin nykyinen toimintamalli kansallisen yhteyshenkilön nimeämisessä. Kompromissiehdotukset ovat menneet tältä osin Suomen kantojen mukaiseen suuntaan.

Suomi on pyrkinyt vaikuttamaan siihen, että ENISA:n mandaatin kokonaisvaltainen uudistus tehtäisiin ENISA:n toiminnan tehostamiseksi, tehtävien priorisoimiseksi ja läpinäkyvyyden lisäämiseksi. Suomi on pitkin neuvotteluita korostanut, että ENISA:n tehtävissä tulisi tehdä laajaa priorisointia ENISA:n toiminnan rahoittamisen ollessa riippuvainen monivuotisen rahoituskehyksen ja budjettineuvotteluiden ratkaisuista. Suomi on peräänkuuluttanut vastuullista lähestymistä ENISA:n tehtävien järjestämisessä ja budjettikeskusteluissa. Alkuperäisessä asetusehdotuksessa esitetyt ENISA:n keräämät maksut mm. kyberturvallisuuden sertifioinneista on poistettu, millä on vaikutuksia ENISA:n toiminnan rahoittamiseen.

Suomi on kyberturvallisuuden sertifiointijärjestelmien osalta kannattanut prosessien tehostamista, jotta sertifiointeja saataisiin valmisteltua ja otettua käyttöön nopeammin.

Suomi on pitänyt hyvänä sertifiointien vapaaehtoisuutta sekä jäsenvaltioiden roolia Euroopan kyberturvallisuuden sertifiointiryhmässä (ECCG) sekä sen riittävää osallistamista osana sertifiointikehyksen prosesseja. Kompromissiteksteissä tehdyt muutokset selkeyttävät ja tehostavat sertifiointikehyksen prosesseja ja ovat Suomen kannan mukaisia.

ICT-toimitusketjujen turvallisuuden osalta Suomi on kantojensa mukaisesti korostanut, että toimenpiteiden tulee olla oikeasuhtaisia, riskiperustaisia ja ennakoitavia sekä perustua asianmukaiseen kuulemiseen ja vaikutusarviointiin. Suomi on tukenut ehdotuksen tavoitteita hakea ehdotuksen pohjalta yhteisiä ICT-toimitusketjuja koskevia velvoittavampia ratkaisuja. Samalla Suomi on korostanut jäsenvaltioiden roolia ja unionin ja jäsenvaltioiden toimivaltajaon selkeyttä.

ICT-toimitusketjujen turvallisuudesta annetussa uusimmassa kompromississa on pyritty säilyttämään alkuperäisen tekstin tavoitteet ja vaikutukset. Kompromississa tehdyt muutokset ovat kohdistuneet pitkälti tekstin ja prosessien selkeyttämiseen sekä oikeusvarmuuden lisäämiseen. Kompromissiteksti on lisännyt ehdotuksen riskiperusteisuutta ja oikeasuhtaisuutta sekä jäsenvaltioiden roolia ICT-toimitusketjuja koskevassa unionin riskiarviointiprosessissa.

Viestintäverkkoja koskevien siirtymäaikojen osalta mobiiliviestintäverkoille osoitettu suora 36 kuukauden siirtymäaika on poistettu ja tarvittava siirtymäaika arvioitaisiin myös näiden osalta erikseen. Kompromissitekstin mukaan tarvittavat siirtymäajat kaikkien viestintäverkkotyyppien osalta arvioitaisiin arvioidun riskitason, tuotteiden ja infrastruktuurin elinkaarten, laitteiden vaihtosyklin sekä relevanttien tuotteiden ja infrastruktuurin jäljellä olevan taloudellisen arvon pohjalta. Siirtymäaikoja määriteltäessä tulee huomioida yhteentoimivuusvaatimukset sekä saatavilla olevat vaihtoehdot. Lisäksi siirtymäaikoja määriteltäessä tulee varmistaa keskeisten palvelujen tarjoamisen jatkuvuus siirtymän aikana. Lisäksi siirtymäajan päättymiseen saakka saisi tehdä käytössä olevien ICT-komponenttien ylläpitoa, korjausta tai turvallisuustoimenpiteitä, jos se on välttämätöntä viestintäverkkojen asianmukaisen toiminnan turvaamiseksi.

Riskiarvioinneissa on tarkennettu kriittisiä ICT-komponentteja koskevaa arviointia sekä edellytettäisiin selkeää riskiarviointimetodologiaa. Riskiarviointiprosessissa tulisi myös ennakolta arvioida toimenpiteiden vaikutuksia. Huolta aiheuttavan kolmannen maan nimeäminen on muutettu vakavia ja rakenteellisia ei-teknisiä riskejä aiheuttavien kolmansien maiden nimeämiseksi. Kyseisen toimenpiteen vaikutuksia tulisi myös arvioida ennakolta.

Suomi on pitänyt tärkeänä selkeää toimivallanjakoa sekä sitä, että kansalliseen turvallisuuteen liittyvät kysymykset kuuluvat jäsenvaltioiden yksinomaiseen toimivaltaan. Suomi on kantansa mukaisesti korostanut, että on tärkeää, että jäsenvaltiot voivat jatkossakin asettaa asetusehdotusta pidemmälle meneviä kansallisia velvoitteita ja toimenpiteitä, erityisesti viestintäverkkojen turvallisuuden varmistamiseksi. Ehdotus jättää edelleen jäsenvaltioille mahdollisuuden mennä kansallisesti asetusta pidemmälle sekä mahdollisuuden ottaa käyttöön myös kansallisia toimia, jotka ovat linjassa unionin oikeuden kanssa.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

CSA2-asetusehdotuksen ja NIS 2 -muutosdirektiiviehdotuksen oikeusperustana 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.

Valtioneuvosto on U-kirjelmässään U 17/2026 vp katsonut oikeusperustan olevan asianmukainen. Suuri valiokunta on ehdotusta koskevassa lausunnossaan todennut, että jatkoneuvotteluissa on syytä varmistua ehdotuksen oikeusperustan asianmukaisuudesta (SuVL 6/2026 vp), ja perustuslakivaliokunta on korostanut tarvetta varmistua vielä siitä, että ehdotetulla sääntelyllä on kaikkinensa riittävä liityntä sisämarkkinoiden toimintaan SEUT 114 artiklassa tarkoitetulla tavalla (PeVL 21/2026 vp). Perustuslakivalio-kunta on muun muassa todennut, että säädösehdotusten keskeiset tavoitteet liittyvät kyberturvallisuuteen, minkä vuoksi vailla merkitystä ei ole myöskään Euroopan unionista tehdyn sopimuksen (SEU) 4 artiklan 2 kohta, jonka mukaan kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla. Valtioneuvosto tuo esille, että CSA2-asetusehdotuksen kohdetta ja soveltamisalaa koskevassa artiklassa 1 on todettu, että se ei vaikuta jäsenvaltioiden keskeisiin valtiollisiin tehtäviin, kuten valtion alueellisen koskemattomuuden varmistamiseen, yleisen järjestyksen ylläpitämiseen ja kansallisen turvallisuuden turvaamiseen, ja että kansallinen turvallisuus pysyy yksinomaan kunkin jäsenvaltion vastuulla. Muutettavan NIS2-direktiivin 2 artiklaan sisältyy vastaava kirjaus. NIS2-direktiivi sekä asetus (EU) 2019/881 ENISA:sta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (CSA) on hyväksytty SEUT 114 artiklan nojalla.

Valtioneuvosto katsoo oikeusperustan olevan asianmukainen U-kirjelmässä (U 17/2026) todetulla tavalla.

Valtioneuvosto on U-kirjelmässään (U 17/2026 vp) on tarkemmin selostanut päätöksentekomenettelyä ja komissiolle delegoitua toimivaltaa. Kompromissiteksteissä on vahvistettu jäsenvaltioiden roolia komitologiamenettelyssä. Päätöksentekomenettelyn osalta valtioneuvosto tulee neuvotteluissa edelleen korostamaan asetustekstin täsmällisyyttä ja jäsenvaltioiden riittävää roolia päätöksentekomenettelyssä.

Käsittely Euroopan parlamentissa

Vastuuvaliokuntana on Euroopan parlamentin teollisuus-, tutkimus- ja energiavaliokunta (ITRE). Ehdotuksen raportöörinä toimii Markéta Gregorová (Greens/EFA).

Vastuuvaliokunnan luonnosraportti CSA2-asetusehdotuksesta julkaistiin 18.09.2026 ja NIS2-muutosdirektiivistä 24.09.2026. Valiokunta äänestää raporteista tämänhetkisen tiedon mukaan 2.2.2027.

Kansallinen valmistelu

Tämä valtioneuvoston U-jatkokirjelmä on valmisteltu liikenne- ja viestintäministeriössä.

U-jatkokirjelmä on käsitelty kirjallisessa menettelyssä viestintäjaostossa (EU19) ja hybridiuhat-jaostoissa (EU13) 9.-10.11.2026.

Eduskuntakäsittely

Liikenne- ja viestintävaliokunta 24.3.2026
Perustuslakivaliokunta 7.4.2026

Suuri valiokunta 8.4.2026
Puolustusvaliokunta ja hallintovaliokunta 21.4.2026

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

Ehdotuksen vaikutuksia kansalliseen lainsäädäntöön ja Ahvenanmaan toimivaltaa on selostettu U-kirjelmässä U 17/2026 vp.

Ehdotuksen suhde perustuslakiin

Perustuslakivaliokunta on lausunnossaan PeVL 21/2026 vp edellyttänyt, että CSA2-asetusehdotuksen jatkovalmistelussa on välttämätöntä selventää sääntelyn suhdetta perustuslain 15 §:ään.

Valtioneuvosto täydentää kirjelmässä U 17/2026 vp esitettyä arviota kuvaamalla niitä seikkoja, joilla voi olla merkitystä perustuslain 15 §:ssä suojatun omaisuudensuojan arvioinnin kannalta.

Valtioneuvosto on kirjelmässään U 17/2026 vp arvioinut ehdotuksen suhdetta perustuslakiin sekä perus- ja ihmisoikeuksiin. Kirjelmässään valtioneuvosto on arvioinut, että ehdotettu sääntely on merkityksellistä perustuslain 15 §:ssä turvatun omaisuudensuojan kannalta. Perustuslakivaliokunnan lausuntokäytännössä on aiemmin katsottu, että perustuslain 15 §:n pakkolunastussäännöksen soveltamisala ei rajoitu ainoastaan sellaisiin tilanteisiin, joissa omistusoikeus siirtyy subjektilta toiselle. Niinpä omaisuuden käyttörajoitus voi olla niin merkittävä, että se rinnastuu tosiasiallisilta vaikutuksiltaan pakkolunastukseen. Tällöin sitä on arvioitava perustuslain 15 §:n 2 momentin kannalta (esim. PeVL 7/2018 vp, PeVL 32/2010 vp, PeVL 38/1998 vp). Tällainen tilanne on käsillä erityisesti silloin, kun käyttörajoitus estää kokonaan omaisuuden käyttämisen pääasialliseen käyttötarkoitukseensa (PeVL 35/2020 vp).

Perustuslakivaliokunta on aiemmassa lausuntokäytännössään 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. Erityisen vahvasti säännellyillä markkinoilla toimivat elinkeinonharjoittajat eivät perustuslakivaliokunnan aiemman lausuntokäytännön mukaan voi perustellusti odottaa lainsäädännön pysyvän kaikissa oloissa muuttumattomana (mm. PeVL 50 /2025 vp, PeVL 22/2013 vp, PeVL 31/2006 vp, PeVL 56/2005 vp).

Perustuslakivaliokunta on aikaisemmassa lausuntokäytännössään arvioinut rajoitustoimenpiteiden suhdetta tosiasialliseen pakkolunastukseen kokonaisvaltaisen harkinnan pohjalta (PeVL 7/2018 vp, s. 2 ja PeVL 61/2010 vp, s. 3). Perustuslakivaliokunta on katsonut, että sääntelyn oikeasuhtaisuuden kannalta merkitystä on myös siinä, millaisia mahdollisuuksia elinkeinoharjoittajalla on ollut sopeuttaa toimintaansa lainsäädännön muutoksiin (PeVL 18/2013 vp).

Viestintäverkkojen osalta arvioitavaksi tulee siirtymäaikojen lisäksi se, mikä merkitys sääntelyn ennakoitavuudelle on EU:n 5G-suosituksilla, joilla komissio on aiemmin pyrkinyt yhdenmukaistamaan viestintäverkkojen turvallisuuden toimenpiteitä ja joiden pohjalta on annettu myös kansallisesti velvoittavaa lainsäädäntöä. ICT-toimitusketjujen turvallisuutta koskevassa kokonaisvaltaisessa perusoikeusarvioinnissa tulisi antaa painoarvoa rajoitustoimenpiteiden oikeasuhtaisuudelle ja ennakoitavuudelle. Edellä todetun pohjalta valtioneuvosto katsoo, että viestintäverkkotoimiala on voinut ennakoida velvoittavampaa unionin tasoista sääntelyä, joka pohjautuu osin EU:n 5G-suosituksiin edellä ja valtioneuvoston kirjelmässä (U 17 / 2026 vp) todetusti. Näiden suositusten lisäksi EU:ssa on julkaistu EU:n 5G-suositusten rakennetta ja osin sisältöä seuraavia ICT-toimitusketjuja koskevia suosituksia (ICT toolbox), joita kuvataan myös valtioneuvoston kirjelmässä (U 17/2026 vp).

Puheenjohtajamaan uusimmassa kompromissitekstiehdotuksessa on alkuperäistä ehdotusta täsmällisemmin huomioitu niitä ICT-komponenttien vaihtamisvelvoitteita koske-via seikkoja, joilla voi olla merkitystä arvioitaessa toimenpiteiden suhdetta perustuslain 15 §:ssä suojattuun omaisuudensuojaan. Arvioinnin kannalta merkityksellisiä seikkoja voivat olla siirtymäajat sekä viestintäverkkojen kohdalla siirtymäaikojen lisäksi vaihdettavien ICT-komponenttien elinkaaret, niiden uusimissykli sekä niiden jäljellä oleva taloudellinen arvo. Lisäksi omaisuudensuojaan myönteisesti voi vaikuttaa ICT-komponenttien välttämättömän ylläpidon salliminen poistettavaksi määrättyjen, mutta vielä käytössä olevien ICT-komponenttien osalta. Näiden seikkojen voidaan arvioida olevan omiaan lieventämään toimenpiteiden vaikutuksia ja parantavan mahdollisuuksia ottaa perustuslain 15 §:n omaisuudensuoja huomioon.

Perustuslakivaliokunta on lausuntokäytännössään todennut, ettei kysymystä siitä, merkitseekö jokin rajoitustoimenpide omaisuuden tosiasiallista pakkolunastusta, voida ratkaista minkään selkeän säännön pohjalta. Kyseessä on kokonaisvaltainen harkinta, jossa merkityksellisiä seikkoja voivat olla muun muassa, kuinka erityisestä rajoitustoimen-piteestä on kyse, kuinka kokonaisvaltaiseksi rajoituksesta aiheutuva omaisuuden arvonmenetys muodostuu sekä kuinka vahingollisen toiminnan rajoittamisesta on kysymys. Lisäksi harkinnassa voi olla merkitystä myös esimerkiksi toimenpiteen kohtuullisuudella sekä sen tarkoitusperän painavuudella, jonka vuoksi rajoitus asetetaan (PeVL 61/2010 vp).

Arvio siitä, voiko ehdotettu tiettyyn korkean riskin toimijaan kohdistuva käyttörajoitus muodostua perustuslain 15 §:n 2 momentissa tarkoitettuun pakkolunastukseen rinnastuvaksi toimenpiteeksi perustuu viime kädessä tapauskohtaiseen kokonaisarviointiin. Arvioinnin kannalta merkityksellisiä seikkoja ovat muun muassa kieltopäätöksen hetkellä käytössä olevien kiellettyjen ICT-komponenttien määrä, niiden käyttöikä, korvaavien ICT-komponenttien saatavuus, ICT-komponenttien poistamisen vaikutukset tuotteiden ja palvelujen tarjoamiseen sekä toimenpiteen kokonaisvaikutus kyseisen toimijan liiketoimintaan. Vaikutukset voivat eri toimijoiden välillä vaihdella huomattavasti. Merkittävä osa arvioinnin kannalta olennaisista tiedoista on yritysten hallussa olevaa liikesalaisuuksien suojaamaa tietoa.

Säädösehdotuksen soveltamisala on ICT-toimitusketjuja koskevan kappaleen osalta laaja, sillä se kattaa NIS2-direktiivin soveltamisalaan kuuluvia toimialoja, joista esimerkkeinä energia, liikenne, vesihuolto, avaruus, elintarvike, julkishallinto ja viestintäverkot. Näiden toimialojen välillä voidaan olettaa olevan eroja käytettävien ICT-komponenttien osalta, minkä lisäksi erot voivat olla huomattavia myös saman toimialan sisällä toimivien yritysten välillä. Mahdollisten käyttörajoitusten vaikutukset voivat siten vaihdella toimialasta toiseen sekä toimialan sisällä toimijasta toiseen, minkä lisäksi vaikutukset riippuvat olennaisesti siitä, missä määrin yksittäisellä toimijalla on käytössään sellaisia ICT-komponentteja, joihin käyttörajoitus kohdistuisi. Osalle toimijoista vaikutukset voivat jäädä vähäisiksi tai jopa merkityksettömiksi, jos niillä ei ole käytössään rajoituksen kohteeksi

joutuvia ICT-komponentteja, kun taas toisille toimijoille vaikutukset voivat olla merkittävämpiä, jos kyseisiä ICT-komponentteja on käytössä käyttökiellon antamisen hetkellä.

Mahdolliset omaisuudensuojan kannalta merkitykselliset vaikutukset konkretisoituvat viestintäverkkojen osalta vasta siinä vaiheessa, kun komissio nimeää täytäntöönpanoasetuksella korkean riskin toimittajat, joiden ICT-komponentteihin pääsäädöksen käyttörajoitukset kohdistuvat ja on esittänyt siirtymäajat tällaisten korkean riskin toimittajien ICT-komponenttien vaihtamiselle. Muiden NIS2-direktiivin soveltamisalaan kuuluvien toimialojen osalta säädösehdotus puolestaan antaa komissiolle toimivallan esittää täytäntöönpanoasetuksilla mahdollisia riskiarviointeihin ja vaikutustenarviointeihin pohjautuvia käyttörajoituksia ja viime kädessä poistovelvoitteita. Näiden laadintaan ja arvioon osallistuu sekä komissio että jäsenvaltiot. Omaisuudensuojan kannalta merkitykselliset vaikutukset riippuvat siten paitsi myöhemmistä täytäntöönpanotoimista myös niiden sisällöstä, kohteesta, ajankohdasta sekä siitä, missä määrin yksittäisillä toimijoilla on kyseisiä komponentteja käytössään kyseisellä hetkellä. Arviointiin vaikuttavat lisäksi muun muassa käyttörajoitusten ja poistovelvoitteiden voimaantulolle asetettujen siirtymäaikojen pituus, rajoituksen kohteena olevien ICT-komponenttien jäljellä oleva käyttöikä, korvaavien ICT-komponenttien saatavuus sekä käyttörajoituksen tosiasialliset vaikutukset toimijan kykyyn tarjota tuotteita ja palveluita. Näillä seikoilla on merkitystä siihen, missä määrin käyttörajoitus vaikuttaa toimijan omaisuuden käyttöön tuotteiden ja palvelujen tarjoamiseksi.

Asiassa C-354/24 Elisa Eesti julkisasiamies katsoi ratkaisuehdotuksessaan, että tapauksen käyttörajoitukset ovat lähtökohtaisesti oikeutettuja omaisuuden käytön rajoituksia, eivät omaisuuden menettämistä. Tästä seuraa, ettei julkisasiamies katso toimenpidettä lähtökohtaisesti sellaisena puuttumisena omaisuudensuojaan, joka edellyttäisi korvausta perusoikeuskirjan 17 artiklan 1 kohdan nojalla. Julkisasiamiehen mukaan omaisuuden käytön rajoittaminen on tapauksessa kuitenkin mahdollista vain siinä määrin kuin se on yleisen edun mukaan välttämätöntä. Julkisasiamiehen arvioinnin mukaan tämän jälkeen merkitystä on sillä, aiheutuuko käyttörajoituksesta yksittäiselle toimijalle suhteettoman raskas taakka. Ratkaisuehdotuksen mukaan tämän arviointi kuuluu viime kädessä kansalliselle tuomioistuimelle osana tapauskohtaista kokonaisarviointia. Julkisasiamies myös korostaa, että merkitystä on myös riittävän pitkällä siirtymäajalla ja toimijan mahdollisuudella ennakoida tulevaa sääntelyä, ja että kansallisen tuomioistuimen tulisi huomioida nämä kokonaisarvioinnissaan. Julkisasiamies katsoo, että jos kansallinen tuomioistuin arvioi, että siirtymäajat eivät ole olleet riittävän pitkiä, silloin olisi harkittava aiheutuneen vahingon asianmukaista korvausjärjestelmää. Unionin tuomioistuin ei ole vielä antanut ratkaisuaan asiassa.

Arvioitaessa toimenpiteiden suhdetta perustuslain 15 §:ssä turvattuun omaisuudensuojaan merkitystä voidaan antaa siten useille sellaisille sääntelyn rakenteellisille ominaisuuksille, jotka ovat omiaan lieventämään toimenpiteistä aiheutuvia vaikutuksia yksittäisille toimijoille. Täytäntöönpanoasetusehdotuksia edeltävissä vaikutusarvioinneissa tulisi arvioida muun muassa toimenpiteiden vaikutuksia toimenpiteen kohteena olevien NIS2-toimijoiden palvelujen ja tuotteiden tarjoamisen jatkuvuudelle sekä saatavilla olevat korvaavat ICT-komponentit, joilla on vastaava toiminnallisuus ja suorituskyky kuin vaihdettavilla ICT-komponenteilla. Erityistä merkitystä voidaan antaa myös sille, että poistamista koskeviin velvoitteisiin kytkeytyy siirtymäajat, joiden avulla toimenpiteen kohteena olevilla toimijoilla on mahdollisuus ennakoida ja sopeuttaa toimintaansa uusiin vaatimuksiin siirtymäajan loppuun saakka. Mobiiliviestintäverkkojen osalta siirtymäaikojen lisäksi merkitystä on myös sillä, että toimijoilla on ollut EU:n 5G-suosituksista lähtien mahdollisuus ennakolliseen varautumiseen. Näiden lisäksi rajoittavat toimenpiteet olisivat määräaikaisia ja niitä tulisi arvioida 36 kuukauden välein. Toimenpiteen tarpeellisuutta ja oikeasuhtaisuutta arvioitaisiin siten määräajoin uudelleen.

Myös asiassa C-354/24 julkisasiamies antoi edellä todetusti omaisuudensuojan arvioinnissa merkitystä muun muassa sääntelyn ennakoitavuudelle, siirtymäaikojen riittävyydelle sekä sille, aiheutuuko rajoituksesta yksittäiselle toimijalle suhteettoman raskas taakka. Ratkaisuehdotus tukee siten näkemystä, jonka mukaan omaisuudensuojan kannalta merkitystä ei ole ainoastaan käyttörajoituksen olemassaololla, vaan myös sillä, miten käyttörajoitus toteutetaan, millaisia vaikutuksia sillä on yksittäisiin toimijoihin sekä millaisia vaikutuksia lieventäviä seikkoja sääntelyyn sisältyy.

Vaihtovelvoitteiden perusoikeusvaikutuksia lieventävillä seikoilla on merkitystä myös sen arvioinnissa, estyykö rajoituksen kohteena olevan omaisuuden käyttäminen pääasialliseen käyttötarkoitukseensa. ICT-komponenttien poistamisvelvoitteeseen voisi kytkeytyä siirtymäajat. Lisäksi viestintäverkkojen osalta velvoitteisiin kytkeytyisi siirtymäaikojen lisäksi ICT-komponenttien käyttöikä, niiden uusimissyklit, niiden jäljellä oleva taloudellinen arvo sekä se, että vaihdettavaksi määrättyjen, vielä käytössä olevien ICT-komponenttien välttämätön ylläpito olisi sallittua. Tarvittavat siirtymäajat arvioitaisiin ja määriteltäisiin edellä todetut kriteerit huomioiden erikseen täytäntöönpanosäädöksissä. Edellä todetuilla seikoilla voidaan arvioida olevan myönteinen vaikutus omaisuudensuojaan, kun rajoituksen kohteena olevaa omaisuutta saisi käyttää pääasialliseen käyttötarkoitukseensa siirtymäajan loppuun saakka.

Viranomaisvaikutukset

Komission ehdotuksen vaikutuksia viranomaisten toimintaan on kuvattu valtioneuvoston kirjelmässä U 17/2026 vp.

Puheenjohtajan kompromissiehdotuksissa ENISA:n tehtäviin ehdotetut muutokset eivät merkittävästi muuta aiempaa arviota viranomaistoiminnan vaikutuksista Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen osalta. Tehtäviin ehdotetut selvennykset ja päällekkäisten tehtävien poistaminen selventävät ENISA:n roolia suhteessa kansallisiin kyberturvallisuusviranomaisiin.

ICT-toimitusketjujen turvallisuutta koskevien säännösten pohjalta kansallisille toimivaltaisille viranomaisille esitettäisiin uusia valvonta- ja täytäntöönpanotehtäviä NIS2-direktiivin (2022/2555) liitteiden I ja II toimijoille kattaen myös NIS2-direktiivin soveltamisalan ulkopuolella olevat pienet ja mikroyritykset. Huomionarvoista on, että ICT-toimitusketjujen turvallisuutta koskevan ehdotuksen soveltamisalan laajuus vaikuttaa valvovien viranomaisten resurssitarpeeseen, jos uusien valvonta- ja täytäntöönpanotehtävien lisäksi valvottavien toimijoiden määrä kasvaa nykyisestään. Ehdotuksen mukaan jäsenvaltioiden on varmistettava, että toimivaltaisilla viranomaisilla on riittävät toimivaltuudet, riittävät resurssit sekä tarvittava asiantuntemus tehtäviensä tehokkaaseen hoitamiseen. On huomioitava, että ICT-toimitusketjujen turvallisuutta koskevien velvoitteiden osalta edellytetään uudenlaista erikoisosaamista vaativien strategisten riskien arvioinnissa. Tarkemmat arviot viranomaisten resurssivaikutuksista esimerkiksi NIS2-direktiivin valvovien viranomaisten lisähenkilötyövuosien osalta ovat toistaiseksi suuntaa antavia ja varmistuvat myöhemmin valmistelun aikana. Korkean riskin toimittajien velvoitteisiin kytkeytyvissä vaikutusarvioinneissa on tarpeen huomioida myös mahdolliset vaikutukset lainvalvontaviranomaisiin

Taloudelliset vaikutukset

Ehdotuksen taloudellisia vaikutuksia on kuvattu U-kirjelmässä U 17/2026 vp. Kuten kirjelmässä on selitetty, ehdotetut muutokset ENISA:n tehtäviin vaatisivat komission arvion mukaan ENISA:n toimintamenojen merkittävää kasvattamista. Puheenjohtajan

kompromissiehdotuksissa ENISA:lle ehdotettuja tehtäviä on joiltakin osin selvennetty ja ehdotettu poistettavaksi, mutta ehdotettujen muutosten ei voitaisi arvioida vähentävän merkittävällä tavalla tarvetta kasvattaa ENISA:n toimintamenoja. Lisäksi puheenjohtajan ehdotus poistaa ENISA:lta mahdollisuus periä maksuja joidenkin tehtävien kustannuksien osittaiseksi kattamiseksi vähentäisi osaltaan ENISA:n toiminnan rahoituksen lähteitä ja näin kasvattaisi näiden tehtävien rahoittamiseksi tarvittavan budjettirahoituksen osuutta. Puheenjohtajan ehdotus poistaa komission alkuperäiseen ehdotukseen sisältynyt jäsenvaltioiden velvollisuus lähettää kansallisia asiantuntijoita ENISA:an vähentäisi ehdotuksesta aiheutuneita kustannuksia kansallisille kyberturvallisuusviranomaisille (kustannukseksi on aiemmin arvioitu noin 200 000 euroa vuosittain).

Komissio on alkuperäisen asetusehdotuksen osalta arvioinut, että 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. Puheenjohtajamaan kompromissitekstiehdotuksen pohjalta voidaan arvioida viestintäverkkojen osalta, että viestintäverkkojen toimialaan kohdistuvat taloudelliset vaikutukset voisivat olla alkuperäistä ehdotusta rajatummat.

Suomi on neuvotteluissa pyytänyt toistuvasti komissiolta tarkentavaa arviota siitä, millaisia taloudellisia vaikutuksia kohdistuisi myös muille soveltamisalaan kuuluville NIS2-direktiivin toimialoille. Komissio ei ole tarkentanut arviotaan edellä todetun lisäksi. Suomi on kiinnittänyt neuvotteluissa huomiota siihen, että ehdotuksella voi olla potentiaalisia taloudellisia vaikutuksia myös muihin NIS2-toimialoihin kuin viestintäverkkoihin.

Muut asian käsittelyyn vaikuttavat tekijät

CSA2-ehdotus on osa EU:n komission laajempaa kokonaisuutta kyberturvallisuuden tason, teknologisen suvereniteetin ja Euroopan unionin sisämarkkinoiden häiriöttömään toiminnan turvaamiseksi. Kokonaisuuteen kuuluvat myös komission ehdotukset digitaalisia verkkoja koskeva säädökseksi (Digital Networks Act, DNA) ja pilvipalvelujen ja tekoälyn kehittämistä koskevaksi säädökseksi (Cloud and AI Development Act, CADA).

Asiakirjat

COM(2026) 11 final
COM(2026) 13 final

Laatijan ja muiden käsittelijöiden yhteystiedot

Liikenne- ja viestintäministeriö TIO/TDL:
Eevi Vuorinen +358 29 5342080
Marième Korhonen-Cara +358 295342134
Maija Rönkä +358 29 5342235
Veikko Vauhkonen +358 295342168

VAHVA-tunnus

EU/385/2026
EU/388/2026

Liitteet Napsauta tähän ja kirjoita liitteet

Viite Napsauta tähän ja kirjoita viite