Euroopan unionin neuvosto

Bryssel, 22. toukokuuta 2026
(OR. en)

9399/26

Toimielinten väliset asiat:
2026/0011(COD)
2026/0012(COD)

LIMITE

CYBER 229
JAI 606
DATAPROTECT 161
TELECOM 239
MI 489
IND 342
CADREFIN 220
FIN 697
BUDGET 19
CSC 316
CODEC 937

ILMOITUS

Lähettäjä:	Neuvoston pääsihteeristö
Vastaanottaja:	Pysyvien edustajien komitea / Neuvosto
Asia:	Ehdotus Euroopan parlamentin ja neuvoston asetukseksi Euroopan unionin kyberturvallisuusvirastosta (ENISA), eurooppalaisesta kyberturvallisuuden sertifiointikehyksestä ja tieto- ja viestintätekniikan toimitusketjun turvallisuudesta sekä asetuksen (EU) 2019/881 kumoamisesta (kyberturvallisuussäädös 2) Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi direktiivin (EU) 2022/2555 muuttamisesta siltä osin kuin on kyse yksinkertaistamistoimenpiteistä sekä direktiivin saattamisesta linjaan [kyberturvallisuusasetusta koskevan ehdotuksen] kanssa – Tilanneselvitys

Puheenjohtajavaltio on laatinut tilanneselvityksen, joka koskee ehdotusta Euroopan parlamentin ja neuvoston asetukseksi Euroopan unionin kyberturvallisuusvirastosta (ENISA), eurooppalaisesta kyberturvallisuuden sertifiointikehyksestä ja tieto- ja viestintätekniikan toimitusketjun turvallisuudesta sekä asetuksen (EU) 2019/881 kumoamisesta (kyberturvallisuussäädös 2), raportoidakseen neuvoston valmisteluelinten tähän mennessä tekemästä työstä ja ehdotuksen käsittelyn tilanteesta.

JOHDANTO

1. Komissio ehdotti 20. tammikuuta 2026 uutta kyberturvallisuuspakettia, jolla vahvistetaan EU:n kyberresilienssiä ja -valmiuksia. Paketti koostuu Euroopan unionin kyberturvallisuusvirastoa (ENISA), eurooppalaista kyberturvallisuuden sertifiointikehystä ja tieto- ja viestintätekniikan toimitusketjun turvallisuutta koskevasta **asetuksesta**, jolla kumotaan asetus (EU) 2019/881 (kyberturvallisuusasetus). Tätä asetusta, jäljempänä ’kyberturvallisuussäädös 2’, täydennetään **direktiivillä**, jolla muutetaan direktiiviä (EU) 2022/2555, jäljempänä ’NIS 2 -direktiivi’, yksinkertaistamistoimenpiteiden ja [kyberturvallisuussäädöstä koskevan ehdotuksen] noudattamisen osalta.

2. Ennen ehdotuksen antamista neuvosto pyysi ENISAsta 6. joulukuuta 2024 antamissaan päätelmissä[1] komissiota tarkastelemaan ja vahvistamaan ENISAn roolia operatiivisen yhteistyön tukena EU:n tasolla ja jäsenvaltioiden välillä kyberuhkien sietokyvyn parantamiseksi ottaen huomioon jäsenvaltioiden toimivallan tällä alalla. Komissiota pyydettiin myös varmistamaan, että ENISAn toimeksianto tukea jäsenvaltioita on kohdennettu ja määritelty selkeästi ja että sillä on konkreettiset strategiset tavoitteet ja ensisijaiset tehtävät sen lisäksi, että tehtävät ja toimivaltuudet jaetaan tarkemmin muihin toimijoihin nähden. Neuvosto myös kehotti komissiota hyödyntämään kyberturvallisuusasetuksen arvioinnin tarjoamaa tilaisuutta etsiä tapoja, joilla EU:n kyberturvallisuuden sertifiointijärjestelmiä voitaisiin kehittää kevyemmin, riskiperusteisin sekä avoimemmin ja nopeammin toimintatavoin. Lisäksi neuvosto korosti kyberturvallisuuden tulevaisuudesta 21. toukokuuta 2024 antamissaan päätelmissä[2] olevansa sitoutunut varmistamaan turvalliset tieto- ja viestintätekniikan toimitusketjut ja korosti muiden kuin teknisten riskitekijöiden merkitystä, mukaan lukien kolmansien valtioiden sopimaton vaikuttaminen toimittajiin ja palveluntarjoajiin. Tieto- ja viestintätekniikan toimitusketjun turvallisuudesta 17. lokakuuta 2022 annetuissa neuvoston päätelmissä[3] korostettiin tarvetta vahvistaa tieto- ja viestintätekniikan toimitusketjujen häiriönsietokykyä ja turvallisuutta ottaen huomioon geopoliittisten jännitteiden sekä tieto- ja viestintätekniikan tuotteisiin ja palveluihin liittyvien riippuvuuksien vaikutukset.

---

1 16527/24.
2 10133/24.
3 13664/22.

3. SEUT 114 artiklaan perustuvan asetusehdotuksen tarkoituksena on vahvistaa unionin kyberturvallisuuskehystä. Sillä vahvistetaan Euroopan unionin kyberturvallisuusviraston (ENISA) roolia ja tehtäviä jäsenvaltioiden ja unionin toimijoiden tukemiseksi kyberturvallisuuden, häiriönsietokyvyn ja luottamuksen korkean tason saavuttamisessa unionissa. Sen tavoitteena on tehdä eurooppalaisesta kyberturvallisuuden sertifiointikehyksestä vaikuttavampi ja tehokkaampi, jotta järjestelmän kehittämistä ja täytäntöönpanoa voidaan nopeuttaa. Ehdotuksella luodaan myös luotettavan tieto- ja viestintätekniikan toimitusketjun turvallisuutta koskeva unionin kehys, jolla puututaan muihin kuin teknisiin riskitekijöihin ja riippuvuuksiin, jotka vaikuttavat kriittisen tieto- ja viestintätekniikan infrastruktuurin ja palvelujen turvallisuuteen. Siihen liittyy kohdennettuja yksinkertaistamistoimenpiteitä, jotka liittyvät NIS 2 -direktiivin[4] täytäntöönpanoon ja joilla pyritään yksinkertaistamaan vaatimusten noudattamista koskevia vaatimuksia, vähentämään tarpeetonta hallinnollista rasitetta ja lisäämään oikeudellista selkeyttä.

4. Kyproksella 24. huhtikuuta 2026 pidetyn valtion- tai hallitusten johtajien epävirallisen kokouksen yhteydessä allekirjoitettu yhden Euroopan yhdet markkinat -etenemissuunnitelma[5] sisältää tämän ehdotuksen yhtenä ensisijaisista tavoitteista.

5. Euroopan parlamentti nimitti Gregorová Markétan (Vihreät/EVA) esittelijäksi käsittelyä johtavaan teollisuus-, tutkimus- ja energiavaliokuntaan.

6. Euroopan talous- ja sosiaalikomitea antoi lausuntonsa[6] ehdotuksesta 29. huhtikuuta 2026.

---

4 EUVL L 333, 27.12.2022, s. 80.
5 8473/26.
6 8980/26.

KÄSITTELYN TILANNE NEUVOSTON VALMISTELUELIMISSÄ

7. Kyberturvallisuuspaketti esiteltiin yleisesti kyberkysymysten horisontaalisen työryhmän kokouksessa 26. tammikuuta 2026 ja pysyvien edustajien komitean kokouksessa 28. tammikuuta 2026.

8. Kyberkysymysten horisontaalinen työryhmä aloitti ehdotuksen käsittelyn 2. helmikuuta 2026 komission yksityiskohtaisella esittelyllä. Komissio esitteli tuolloin myös arviointikertomukseen, rahoitusselvitykseen ja vaikutustenarviointiin liittyvät havainnot.

9. Kyberkysymysten horisontaalinen työryhmä aloitti asetusehdotuksen käsittelyn 23. helmikuuta 2026.

10. Jäsenvaltiot suhtautuivat ehdotukseen myönteisesti ja kannattivat yleisesti sen yleisiä tavoitteita, erityisesti ENISAn jäsenvaltioiden operatiiviselle yhteistyölle antaman tuen vahvistamista ja sertifiointikehyksen virtaviivaistamista. Keskusteluissa kävi kuitenkin myös ilmi, että useita ehdotuksen osa-alueita olisi tarkasteltava lähemmin. Valtuuskunnat pyysivät lisäselvennyksiä ENISAlle suunnitellusta suuremmasta operatiivisesta roolista ja laajemmista tehtävistä, mukaan lukien varhaisvaroitusten antaminen, kiristysohjelmia käsittelevän neuvontapalvelun perustaminen ja ENISAn rooli CSIRT-verkostossa. Useat valtuuskunnat kyseenalaistivat resurssivaikutukset, joita jäsenvaltioille aiheutuisi ehdotetusta kahden kansallisen asiantuntijan osallistumisesta ENISAn tehtävien tukemiseen. Hallintoneuvoston äänestyssäännöistä on myös käytävä lisäkeskusteluja. Valtuuskunnat korostivat tarvetta selkeyttää ja täsmentää ehdotuksessa käytettyjä määritelmiä ja käsitteitä. ENISAn talousarvion koostumusta, erityisesti maksujen perimistä, on myös selvennettävä.

11. Uudet säännökset, joilla lisätään sertifiointiprosessin vaikuttavuutta ja tehokkuutta, saivat yleisesti ottaen myönteisen vastaanoton, vaikka yleisesti todettiin, että jäsenvaltioiden osallistumista sertifiointiprosessiin on lisättävä kauttaaltaan. Sertifioinnin vapaaehtoisuuteen suhtauduttiin yleisesti ottaen myönteisesti. Valtuuskunnat kuitenkin kyseenalaistivat joitakin sertifiointikehyksessä ehdotettuja määräaikoja.

12. Keskusteluissa luotettavan tieto- ja viestintätekniikan toimitusketjun kehyksestä tuotiin esiin useita jäsenvaltioiden huolenaiheita. Valtuuskunnat pyysivät lisäselvennyksiä menetelmistä ja menettelyistä, jotka koskevat keskeisen TVT-omaisuuden ja suuririskisten toimittajien määrittämistä, sekä ehdotettujen toimenpiteiden soveltamisalasta ja mahdollisista vaikutuksista. Valtuuskunnat korostivat, että on tärkeää varmistaa jäsenvaltioiden asianmukainen osallistuminen.

13. Useat valtuuskunnat tekivät tarkasteluvaraumia ehdotuksen eri osiin, joita olivat erityisesti hallintonäkökohdat, täytäntöönpanosäädösten käyttö ja ehdotettu mekanismi suuririskisten toimittajien tunnistamiseksi sekä tieto- ja viestintätekniikan toimitusketjun turvallisuus.

14. Kyberkysymysten horisontaalisessa työryhmässä käytyjen keskustelujen jälkeen jäsenvaltioita pyydettiin toimittamaan kirjallisia huomautuksia liittyen säännöksiin, jotka koskevat I osastoa (yleiset säännökset) ja II osastoa (ENISA). Vastauksia saatiin 23 jäsenvaltiolta. Jäsenvaltioita pyydettiin myöhemmin myös esittämään kirjallisia huomautuksia eurooppalaista kyberturvallisuuden sertifiointikehystä koskevasta III osastosta. Jäsenvaltioista 20 tarttui tilaisuuteen ja toimitti kantansa kirjallisena.

15. Puheenjohtajavaltio laatii jäsenvaltioiden kirjallisten huomautusten ja kyberkysymysten horisontaalisessa työryhmässä tehdyn työn pohjalta II osastoa (ENISA) ja III osastoa (eurooppalainen kyberturvallisuuden sertifiointikehys) koskevan kompromissitekstin, joka esitetään kyberkysymysten horisontaalisen työryhmän kokouksessa kesäkuun 2026 alussa.

16. Useat jäsenvaltiot pyysivät neuvoston oikeudellista yksikköä tarkastelemaan oikeusperustan asianmukaisuutta.

17. Puheenjohtajavaltio aloittaa NIS 2 -direktiiviä koskevien yksinkertaistamistoimenpiteiden läpikäynnin toukokuun 2026 lopussa.

18. Kaiken kaikkiaan kyberkysymysten horisontaalinen työryhmä on pitänyt Kyproksen puheenjohtajakaudella 15 kokousta kyberresilienssisäädöstä 2 koskevasta ehdotuksesta.

19. Seuraava puheenjohtajavaltio Irlanti aikoo jatkaa työtä tässä tärkeässä asiakokonaisuudessa nykyisen puheenjohtajavaltion Kyproksen saavuttaman edistymisen pohjalta.

20. Edellä esitetyn perusteella pysyvien edustajien komiteaa ja neuvostoa pyydetään panemaan merkille edistyminen asetusehdotuksen tarkastelussa.