Europos Sąjungos Taryba

Briuselis, 2026 m. gegužės 22 d.
(OR. en)

9399/26

Tarpinstitucinės bylos:
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

PRANEŠIMAS

nuo:	Tarybos generalinio sekretoriato
kam:	Nuolatinių atstovų komitetui / Tarybai
Dalykas:	Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl Europos Sąjungos kibernetinio saugumo agentūros (ENISA), Europos kibernetinio saugumo sertifikavimo sistemos ir IRT tiekimo grandinės saugumo, kuriuo panaikinamas Reglamentas (ES) 2019/881, (Antrasis kibernetinio saugumo aktas) Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos, kuria dėl supaprastinimo priemonių ir suderinimo su [Pasiūlymu dėl kibernetinio saugumo akto] iš dalies keičiama Direktyva (ES) 2022/2555 – Pažangos ataskaita

Pirmininkaujanti valstybė narė parengė pažangos ataskaitą dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl Europos Sąjungos kibernetinio saugumo agentūros (ENISA), Europos kibernetinio saugumo sertifikavimo sistemos ir IRT tiekimo grandinės saugumo, kuriuo panaikinamas Reglamentas (ES) 2019/881, (Antrasis kibernetinio saugumo aktas), kad informuotų apie iki šiol Tarybos parengiamųjų organų atliktą darbą ir pasiūlymo nagrinėjimo dabartinę padėtį.

ĮVADAS

1. 2026 m. sausio 20 d. Komisija pasiūlė naują kibernetinio saugumo dokumentų rinkinį, kuriuo siekiama stiprinti ES kibernetinio saugumo atsparumą ir pajėgumus. Rinkinį sudaro **Reglamentas** dėl Europos Sąjungos kibernetinio saugumo agentūros (ENISA), Europos kibernetinio saugumo sertifikavimo sistemos ir informacinių ir ryšių technologijų (IRT) tiekimo grandinės saugumo, kuriuo panaikinamas Reglamentas (ES) 2019/881, (Kibernetinio saugumo aktas). Šį reglamentą (Antrąjį kibernetinio saugumo aktą) papildo **Direktyva**, kuria dėl supaprastinimo priemonių ir suderinimo su [Pasiūlymu dėl kibernetinio saugumo akto] iš dalies keičiama Direktyva (ES) 2022/2555 (TIS 2 direktyva).

2. Prieš pateikiant pasiūlymą, 2024 m. gruodžio 6 d. išvadose dėl ENISA[1] Taryba paprašė Komisijos išnagrinėti ir toliau stiprinti ENISA vaidmenį remiant operacinį bendradarbiavimą ES lygmeniu ir tarp valstybių narių kibernetinio atsparumo didinimo srityje, atsižvelgiant į valstybių narių kompetenciją šioje srityje. Komisija taip pat buvo paraginta užtikrinti, kad ENISA įgaliojimai remti valstybes nares būtų orientuoti į rezultatus ir aiškiai apibrėžti, kad būtų nustatyti konkretūs strateginiai tikslai ir prioritetinės užduotys, taip pat tiksliau pasidalijamos užduotys ir kompetencija kitų subjektų atžvilgiu. Be to, Taryba paragino Komisiją pasinaudoti Kibernetinio saugumo akto vertinimo suteikta galimybe rasti būdų, kaip užtikrinti, kad ES kibernetinio saugumo sertifikavimo schemos būtų rengiamos taikant paprastesnį, rizika grindžiamą, skaidresnį ir spartesnį metodą. Be to, 2024 m. gegužės 21 d. išvadose[2] dėl kibernetinio saugumo ateities Taryba pabrėžė įsipareigojimą siekti, kad būtų užtikrintos saugios IRT tiekimo grandinės, ir akcentavo netechninių rizikos veiksnių, įskaitant nederamą trečiųjų valstybių įtaką tiekėjams ir paslaugų teikėjams, aktualumą. Galiausiai, 2022 m. spalio 17 d. Tarybos išvadose[3] dėl IRT tiekimo grandinių saugumo pabrėžta, kad reikia stiprinti IRT tiekimo grandinių atsparumą ir saugumą, atsižvelgiant į geopolitinės įtampos ir priklausomybės nuo IRT produktų ir paslaugų poveikį.

---

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

3. Pasiūlymo dėl reglamento, kuris grindžiamas SESV 114 straipsniu, tikslas – sustiprinti Sąjungos kibernetinio saugumo sistemą. Juo stiprinamas Europos Sąjungos kibernetinio saugumo agentūros (ENISA) vaidmuo ir užduotys siekiant padėti valstybėms narėms ir Sąjungos subjektams užtikrinti Sąjungoje aukšto lygio kibernetinį saugumą, atsparumą ir pasitikėjimą. Juo siekiama, kad Europos kibernetinio saugumo sertifikavimo sistema taptų veiksmingesnė ir efektyvesnė, kad šią schemą būtų galima greičiau sukurti ir įgyvendinti. Pasiūlymu taip pat nustatoma Sąjungos patikimo IRT tiekimo grandinių saugumo sistema, kuria sprendžiami klausimai, susiję su netechniniais rizikos veiksniais ir priklausomybe, darančiais poveikį ypatingos svarbos IRT infrastruktūros ir paslaugų saugumui. Kartu numatomos tikslinės supaprastinimo priemonės, susijusios su TIS 2 direktyvos[4] įgyvendinimu, kuriomis siekiama supaprastinti reikalavimų laikymosi reikalavimus, sumažinti bereikalingą administracinę naštą ir padidinti teisinį aiškumą.

4. Šis pasiūlymas, kaip vienas iš prioritetinių siektinų rezultatų, įtrauktas į veiksmų gaires „Viena Europa, viena rinka“[5], pasirašytas 2026 m. balandžio 24 d. Kipre įvykusio neformalaus valstybių ar vyriausybių vadovų susitikimo metu.

5. Europos Parlamento Pramonės, mokslinių tyrimų ir energetikos (ITRE) komitetas (už šį klausimą atsakingas komitetas) pranešėja paskyrė Gregorová Markéta (Verts/ALE).

6. 2026 m. balandžio 29 d. Europos ekonomikos ir socialinių reikalų komitetas pateikė nuomonę dėl šio pasiūlymo[6].

---

4 OL L 333, 2022 12 27, p. 80.
5 Dok. 8473/26.
6 Dok. 8980/26.

DARBO TARYBOS PARENGIAMUOSIUOSE ORGANUOSE PADĖTIS

7. Kibernetinio saugumo dokumentų rinkinys bendrai pristatytas 2026 m. sausio 26 d. Kibernetinių klausimų horizontaliosios darbo grupės (HWPCI) posėdyje ir 2026 m. sausio 28 d. Nuolatinių atstovų komiteto posėdyje.

8. HWPCI pasiūlymą pradėjo svarstyti 2026 m. vasario 2 d., Komisijai išsamiai jį pristačius. Per šį pristatymą Komisija taip pat darbo grupę supažindino su vertinimo ataskaitos, finansinės pažymos ir poveikio vertinimo išvadomis.

9. 2026 m. vasario 23 d. HWPCI pradėjo svarstyti siūlomą reglamentą.

10. Valstybės narės palankiai įvertino pasiūlymą ir iš esmės pritarė jo bendriems tikslams, visų pirma tam, kad būtų stiprinama ENISA parama valstybių narių operaciniam bendradarbiavimui, ir sertifikavimo sistemos supaprastinimui. Tačiau diskusijos taip pat parodė, kad keletą pasiūlymo aspektų reikės nagrinėti toliau. Delegacijos paprašė pateikti išsamesnius paaiškinimus dėl numatomo didesnio ENISA operacinio vaidmens ir užduočių, tokių kaip ankstyvųjų perspėjimų teikimas, pagalbos dėl išpirkos reikalavimo programinės įrangos tarnybos sukūrimas ir ENISA vaidmuo Reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinkle. Kelios delegacijos pareiškė abejonių dėl poveikio valstybių narių ištekliams, susijusio su siūlomu dviejų deleguotųjų nacionalinių ekspertų (DNE) iš kiekvienos valstybės narės indėliu vykdant ENISA užduotis. Taip pat reikia toliau svarstyti Valdančiosios tarybos balsavimo taisykles. Delegacijos pabrėžė, kad visame pasiūlyme vartojamos apibrėžtys ir sąvokos turi būti aiškesnės ir tikslesnės. Be to, reikia išsamiau paaiškinti ENISA biudžeto sudėtį, visų pirma mokesčių rinkimą.

11. Naujosios nuostatos, kuriomis siekiama, kad sertifikavimo procesas būtų veiksmingesnis ir efektyvesnis, įvertintos iš esmės palankiai, tačiau apskritai nurodyta, jog reikia, kad valstybės narės visame sertifikavimo procese dalyvautų aktyviau. Iš esmės palankiai įvertintas savanoriškas sertifikavimo pobūdis. Tačiau delegacijos suabejojo dėl kai kurių siūlomų sertifikavimo sistemos laiko terminų.

12. Diskusijose dėl patikimos IRT tiekimo grandinės sistemos išryškėjo keletas valstybėms narėms susirūpinimą keliančių klausimų. Delegacijos paragino išsamiau paaiškinti pagrindinio IRT turto nustatymo ir didelės rizikos tiekėjų identifikavimo metodiką ir procedūras, taip pat siūlomų priemonių taikymo sritį ir galimą poveikį. Delegacijos pabrėžė, kad svarbu užtikrinti tinkamo lygio valstybių narių dalyvavimą.

13. Kelios delegacijos pareiškė tikrinimo išlygas dėl įvairių pasiūlymo dalių, visų pirma dėl valdymo aspektų, įgyvendinimo aktų naudojimo ir siūlomo didelės rizikos tiekėjų identifikavimo bei IRT tiekimo grandinės saugumo užtikrinimo mechanizmo.

14. Po HWPCI vykusių diskusijų valstybių narių buvo paprašyta raštu pateikti pastabas dėl nuostatų, susijusių su I antraštine dalimi dėl bendrųjų nuostatų ir II antraštine dalimi dėl ENISA. Pastabas pateikė 23 valstybės narės. Vėliau valstybių narių taip pat buvo paprašyta raštu pateikti pastabas dėl III antraštinės dalies dėl Europos kibernetinio saugumo sertifikavimo sistemos. 20 valstybių narių pasinaudojo šia galimybe ir raštu išdėstė savo poziciją.

15. Remdamasi šiomis valstybių narių raštu pateiktomis pastabomis ir HWPCI atliktu darbu, pirmininkaujanti valstybė narė parengs kompromisinį II antraštinės dalies (ENISA) ir III antraštinės dalies (Europos kibernetinio saugumo sertifikavimo sistema) tekstą; jis bus pristatytas 2026 m. birželio mėn. pradžioje vyksiančiame HWPCI posėdyje.

16. Kelios valstybės narės paprašė Tarybos Teisės tarnybos išnagrinėti teisinio pagrindo tinkamumą.

17. 2026 m. gegužės mėn. pabaigoje pirmininkaujanti valstybė narė pradės TIS 2 direktyvoje numatytų supaprastinimo priemonių svarstymą.

18. Pirmininkaujant Kiprui HWPCI bus surengusi iš viso 15 posėdžių dėl pasiūlymo dėl Antrojo kibernetinio atsparumo akto.

19. Remdamasi Kipro pirmininkavimo laikotarpiu padaryta pažanga, pirmininkausianti Airija ketina tęsti su šiuo svarbiu dokumentu susijusį darbą.

20. Atsižvelgiant į tai, kas išdėstyta pirmiau, Nuolatinių atstovų komiteto ir Tarybos prašoma susipažinti su pažanga, padaryta nagrinėjant pasiūlymą dėl reglamento.