Europos Sąjungos Taryba

**Briuselis, 2026 m. sausio 22 d.**
**(OR. en)**

**5611/26**
**ADD 2**

**Tarpinstitucinės bylos:**
**2026/0011 (COD)**
**2026/0012 (COD)**

**CYBER 29**
**JAI 85**
**DATAPROTECT 22**
**TELECOM 29**
**MI 58**
**IND 48**
**CADREFIN 26**
**FIN 100**
**BUDGET 3**
**CODEC 90**

**PRIDEDAMAS PRANEŠIMAS**

| | |
|---|---|
| nuo: | Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ |
| gavimo data: | 2026 m. sausio 21 d. |
| kam: | Europos Sąjungos Tarybos generalinei sekretorei Thérèse BLANCHET |
| Komisijos dok. Nr.: | SWD(2026) 12 final |
| Dalykas: | KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS<br>POVEIKIO VERTINIMO ATASKAITOS SANTRAUKA<br>[…]<br>pridedamas prie<br>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)<br>ir<br>Pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos, kuria iš dalies keičiama Direktyva (ES) 2022/2555 dėl supaprastinimo priemonių ir suderinimo su [pasiūlymu dėl Antrojo kibernetinio saugumo akto] |

Delegacijoms pridedamas dokumentas SWD(2026) 12 final.

Pridedama: SWD(2026) 12 final

EUROPOS
KOMISIJA

Strasbūras, 2026 01 20
SWD(2026) 12 final

**KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS**

# POVEIKIO VERTINIMO ATASKAITOS SANTRAUKA

**[…]**

***pridedamas prie***

**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)**

**ir**

**Pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos, kuria iš dalies keičiama Direktyva (ES) 2022/2555 dėl supaprastinimo priemonių ir suderinimo su [pasiūlymu dėl Antrojo kibernetinio saugumo akto]**

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

# Poveikio vertinimo santrauka

## Tikslas

Pagrindinis šio poveikio vertinimo tikslas – įvertinti dabartinių taisyklių tinkamumą reaguojant į kintančias kibernetinio saugumo grėsmes visoje ES. Jame siūlomas integruotas politikos galimybių rinkinys, kuriuo siekiama stiprinti Europos Sąjungos kibernetinio saugumo agentūrą (ENISA), reformuoti Europos kibernetinio saugumo sertifikavimo sistemą (EKSSS) ir supaprastinti atitiktį esamai kibernetinio saugumo srities teisės aktų sistemai. Šiame vertinime pabrėžiama, kad svarbu keisti valdymą kibernetinio saugumo srityje, siekiant jį suderinti su technologine pažanga ir rinkos poreikiais, kartu užtikrinant konkurencingumą ir atsižvelgiant į poveikį aplinkai.

## Problemos išdėstymas

Nepaisant dedamų pastangų, grėsmėms tampant vis sudėtingesnėms, ES kibernetinio saugumo aplinkoje vis dar susiduriama su dideliais iššūkiais. Nepakankamas valstybių narių ir kitų ES lygmens subjektų veiklos koordinavimas, sulėtėjęs politikos priemonių įgyvendinimas, reguliavimo kliūtys ir sudėtingumas trukdo veiksmingai valdyti kibernetinį saugumą. Dėl šių problemų didėja įmonių ir valdžios institucijų išlaidos, kibernetinių incidentų rizika, o piliečių apsaugos lygis yra nenuoseklus.

## ES veiksmų pagrindimas

Kibernetinio saugumo grėsmės peržengia valstybių sienas; todėl tvirtam atsakui būtinas vienodas požiūris. ES lygmens intervencija užtikrinama nuosekli apsauga, sudarant vienodas sąlygas didinamas konkurencingumas ir palengvinamas laisvas skaitmeninių paslaugų ir produktų judėjimas bendrojoje rinkoje. ES lygmens suderinimo veiksmais taip pat sumažinama administracinė našta, nes supaprastinamas reikalavimų laikymasis ir racionalizuojamos procedūros.

## Politikos galimybės ir tinkamiausia galimybė

Šioje ataskaitoje analizuojamos keturios intervencijos sritys, kurių kiekviena apima politikos galimybes, apsvarstytas atsižvelgiant į konkrečius siektinus tikslus: 1) ENISA įgaliojimai (taip pat dabartinio Kibernetinio saugumo akto dalis), 2) EKSSS (taip pat dabartinio Kibernetinio saugumo akto dalis) ir 3) tiksliniai TIS 2 direktyvos pakeitimai, kuriais siekiama supaprastinimo ir kurie taip pat yra susiję su ENISA įgaliojimais ir EKSSS. Kiekvienas galimybių rinkinys yra atskira intervencinė sritis, bet kartu yra tarpusavyje susiję ir svarbūs vienas kitam.

### *Galimybės spręsti ES kibernetinio saugumo politikos sistemos ir suinteresuotųjų subjektų poreikių nesuderinamumo vis labiau priešiškoje aplinkoje problemą*

A.1 galimybė. *Aiškiau išdėstyti ENISA įgaliojimus ir nustatyti prioritetus*. Pagal šią galimybę būtų užtikrintas aiškus ir stabilus ENISA užduočių pagrindas, nes į ją būtų įtrauktos kituose teisės aktuose nustatytos užduotys.

A.2 galimybė. *ENISA įgaliojimų reforma.* Pagal šią galimybę būtų panaikintas ir pakeistas Kibernetinio saugumo aktas, iš esmės pakeičiant Agentūros įgaliojimus.

A.3 galimybė. *ENISA įgaliojimų reforma daug dėmesio skiriant operatyvinei paramai.* Ši galimybė būtų grindžiama A.2 galimybe. Be to, ENISA valstybės narės prašymu plėtotų pajėgumus, kad padėtų TIS 2 direktyvos subjektams tiesiogiai reaguoti į kibernetinio saugumo incidentą ir atkurti veiklą po jo.

***Europos kibernetinio saugumo sertifikavimo sistemos galimybės***

B.1 galimybė. *Patikslinti EKSSS taikymo sritį, elementus ir tikslus ir nustatyti priežiūros mechanizmą.* Pagal šią galimybę bus numatytas naujas priimtų schemų priežiūros mechanizmas, kurį turės įgyvendinti ENISA.

B.2 galimybė. *Reformuoti EKSSS peržiūrint jos procedūras ir išplečiant taikymo sritį, kad būtų lengviau supaprastinti atitiktį teisės aktams.* Pagal šią galimybę Kibernetinio saugumo aktas būtų panaikintas ir pakeistas nauju reglamentu. Be B.1 galimybės, būtų peržiūrėta procedūra, susijusi su prašymu parengti schemas, jų rengimu ir priėmimu, siekiant pagerinti atskaitomybę ir veiksmingumą.

B.3 galimybė. *Reformuoti EKSSS, kaip numatyta pagal B.2 galimybę, ir nustatyti privalomą kibernetinio saugumo būklės sertifikavimą.* Ši galimybė būtų grindžiama B.2 galimybe, tačiau ja siekiama dar labiau stiprinti sistemos poveikį, nustatant privalomą esminių subjektų sertifikavimą pagal TIS 2 direktyvą, atsižvelgiant į konkrečius rizikos scenarijus, o ne pasikliauti vien savanorišku subjektų sertifikavimu.

***Supaprastinimo galimybės***

C.1 galimybė. *Taikyti privalomos teisinės galios neturinčiais teisės aktais ir ne teisėkūros priemonėmis grindžiamą požiūrį, įskaitant naudojimąsi esamais įgaliojimais (įgyvendinimo aktų priėmimas pagal TIS 2 direktyvos 21 straipsnio 5 dalį ir 23 straipsnio 11 dalį).* Pagal šią galimybę numatoma priimti įgyvendinimo aktus naudojantis esamais TIS 2 direktyva suteiktais įgaliojimais, kad būtų užtikrintas didesnis kibernetinio saugumo rizikos valdymo priemonių, pranešimo apie incidentus ribų, taip pat informacijos, formatų ir notifikavimo procedūrų suderinimas, kartu priimant gairių rinkinį, kuriuo siekiama padidinti teisinį tikrumą ir suderintą įgyvendinimą.

C.2 galimybė. *Tikslinė intervencija – tolesnis atitikties atitinkamai Sąjungos kibernetinio saugumo srities teisės aktų sistemai supaprastinimas.* Ši galimybė apima ribotą intervenciją keičiant Kibernetinio saugumo aktą ir TIS 2 direktyvą, siekiant supaprastinti konkrečius kibernetinio saugumo sistemos aspektus, įskaitant taikymo srities pritaikymą, didžiausią įgyvendinimo aktų suderinimą, atitikties įrodymą atliekant sertifikavimą ir gairių rinkinio priėmimą, kaip numatyta pagal C1 galimybę.

C.3 galimybė. *Sąjungos teisės aktuose nustatytų su kibernetiniu saugumu susijusių priemonių suderinimas.* Ši galimybė būtų grindžiama C.2 galimybe ir pagal ją būtų panaikintos visos kibernetinio saugumo rizikos valdymo priemonės ar įgaliojimai, susiję su priemonėmis ar įgaliojimais, įtrauktais į sektorių teisės aktus. Vietoj to TIS 2 direktyvos ekosistema būtų iš

dalies pakeista, kad būtų numatyti supaprastinti reikalavimai visų tipų subjektams ir tokiu būdu būtų užtikrintas didesnis suderinimas.

## *IRT tiekimo grandinės saugumo galimybės*

D.1 galimybė. *Taikyti privalomos teisinės galios neturinčiais teisės aktais grindžiamą požiūrį į kibernetinio saugumo rizikos IRT tiekimo grandinėms mažinimą.* Pagal šią galimybę nebūtų numatyta reguliavimo priemonių ES lygmeniu. Vietoj to Komisija padidintų koordinuotų rizikos vertinimų ir savanoriškų priemonių rinkinių skaičių.

D.2 galimybė. *Ad hoc reguliavimo intervencinė priemonė, kuria kodifikuojamas 5G priemonių rinkinys.* Pagal šią galimybę būtų kodifikuojamos 5G priemonių rinkinio priemonės. Ja valstybės narės būtų įpareigotos užtikrinti, kad didelės rizikos tiekėjų komponentai nebūtų naudojami pagrindiniuose tinklo objektuose.

D.3 galimybė. *Visapusiška ir horizontali sistema, skirta IRT tiekimo grandinių kibernetinio saugumo rizikai mažinti.* Pagal šią galimybę būtų sukurta horizontali, technologijų ir sektorių atžvilgiu neutrali reguliavimo sistema, skirta netechninio pobūdžio kibernetinio saugumo rizikai IRT tiekimo grandinėse mažinti.

***Atlikus išsamią analizę, tinkamiausias politikos priemonių rinkinys apima:*** A.2 galimybę (ENISA įgaliojimų pertvarkymas); B.2 galimybę (EKSSS reforma peržiūrint jos procedūras ir išplečiant taikymo sritį, kad būtų lengviau supaprastinti atitiktį teisės aktams) ir C.2 galimybę (tikslinė intervencija – tolesnis atitikties atitinkamai Sąjungos kibernetinio saugumo srities teisės aktų sistemai supaprastinimas), taip pat D.3 galimybę (visapusiška ir horizontali sistema, skirta IRT tiekimo grandinių kibernetinio saugumo rizikai mažinti).

Šiuo deriniu užtikrinamas subalansuotas atsakas į nustatytas politikos problemas ir gerokai padidinamas veiksmingumas, efektyvumas ir nuoseklumas visoje ES.

**Pagrindinis poveikis**

**Sąnaudų ir naudos analizė.** Dėl perėjimo prie siūlomos reguliavimo sistemos ENISA patirs iki 161,3 mln. EUR išlaidų per penkerius metus, kad galėtų vykdyti savo naujas užduotis, o valdžios institucijos visoje ES per penkerius metus patirs iki 80 mln. EUR priežiūros išlaidų (atsižvelgiant į atitinkamas sutaupytas išlaidas). Kalbant apie įmones, per trejų metų pereinamąjį laikotarpį dėl laipsniško konkrečios didelės rizikos įrangos atsisakymo judriojo ryšio tinklų operatoriai galėtų patirti 3,4–4,3 mlrd. EUR metinių išlaidų, o investicijos į patikimus tiekėjus kartu galėtų išaugti iki 2 mlrd. EUR per metus. Be to, tikimasi, kad supaprastinus ir sumažinus prievoles užtikrinti atitiktį įmonės sutaupys iki 14,6 mlrd. EUR. Taip pat piliečiai, valdžios institucijos ir įmonės gautų didelę naudą pagerinus bendrą ES kibernetinio saugumo būklę ir technologinį suverenumą bei skatinant inovacijas ir konkurencingumą, kaip tikimasi, ilgainiui iš esmės kompensuosiančius pradines išlaidas.

***Konkurencingumas.*** Tinkamiausios galimybės, kuriomis mažinamas rinkos susiskaidymas ir suderinamas reguliavimas, didina konkurencinę lygybę visoje ES, nes įmonėms sudaromos aiškesnės sąlygos laikytis reikalavimų ir diegti inovacijas.

***Suderinamumo su klimato srities tikslais patikrinimas.*** Atliekant vertinimą nagrinėtas galimas kiekvienos galimybės poveikis aplinkai. Ypatingas dėmesys buvo skiriamas energijos vartojimo efektyvumui, su kelionėmis susijusiems išmetamiesiems teršalams ir infrastruktūros konsolidavimui. Tinkamiausių A.2, B.2 ir C.2 galimybių poveikis aplinkai yra ribotas, o D.3 galimybe atsižvelgiama į poveikio aplinkai neutralumą, skiriant dėmesį produkto gyvavimo ciklui ir pereinamiesiems laikotarpiams, kai yra keičiami pagrindiniai ištekliai. Tai atitinka ES įsipareigojimą siekti tvarumo.

***Standartinis procesų skaitmenizavimas.*** Tai, kad pabrėžiami supaprastinti skaitmeniniai procesai, rodo ES įsipareigojimą laikytis požiūrio, pagal kurį pirmenybė teikiama skaitmeniniams procesams, užtikrinant greitesnį ir patikimesnį keitimąsi duomenimis ir sprendimų priėmimą. D.3 galimybė taip pat galėtų turėti didelį poveikį skaitmenizavimui, nes reikėtų pakeisti subjektų, kurie yra įsisteigę kibernetinio saugumo problemų keliančiose trečiosiose valstybėse arba yra kontroliuojami tų trečiųjų valstybių subjektų, tiekiamus komponentus.

***Supaprastinimas ir naštos mažinimas.*** Tinkamiausiomis galimybėmis prisidedama prie supaprastinimo nustatant taikymo srities paaiškinimus ir priemones, kuriomis siekiama supaprastinti reikalavimų laikymąsi ir priežiūrą, o dėl to mažėja administracinė našta. Svarstoma taikyti principą „kiek plius, tiek minus“ ir užtikrinti, kad naujas prievoles atsvers kitose srityse sumažintos prievolės.

**Išvada**

Šiame poveikio vertinime pateikiama išsami strategija, kuria siekiama didinti ES kibernetinį saugumą, šalinti reguliavimo neveiksmingumą ir parengti skaitmeninę aplinką būsimiems uždaviniams. Jame rekomenduojama laikytis bendradarbiavimu grindžiamo ir nuoseklaus požiūrio, pagal kurį politikos reformos būtų grindžiamos esamomis sistemomis, kartu prisitaikant prie naujų technologinių realijų. Šiomis priemonėmis ES siekia užtikrinti atsparią, konkurencingą ir tvarią skaitmeninę ekonomiką.