PAKEITIMAI 001-001
pateikė Pramonės, mokslinių tyrimų ir energetikos komitetas

Pranešimas
Josianne Cutajar **A9-0307/2023**
Valdomos saugumo paslaugos

Pasiūlymas dėl reglamento (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Pakeitimas 1

EUROPOS PARLAMENTO PAKEITIMAI*

Komisijos pasiūlymui dėl

2023/0108(COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

kuriuo dėl valdomų saugumo paslaugų iš dalies keičiamas Reglamentas (ES) 2019/881

(Tekstas svarbus EEE)

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 114 straipsnį,

---

* Pakeitimai: naujas ar pakeistas tekstas žymimas pusjuodžiu kursyvu, o išbrauktas tekstas nurodomas simboliu ▌.

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę[1],

atsižvelgdami į Regionų komiteto nuomonę,

laikydamiesi įprastos teisėkūros procedūros[2],

[1] ***OL C 349, 2023 9 29, p. 167.***

[2] ***… m. … … d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir … m. … … d. Tarybos sprendimas.***

kadangi:

(1) siekiant užtikrinti tinkamą ***informacinių ir ryšių technologijų*** (IRT) produktų, IRT paslaugų ir IRT procesų kibernetinio saugumo lygį Sąjungoje, taip pat išvengti vidaus rinkos susiskaidymo Sąjungoje kibernetinio saugumo sertifikavimo schemų srityje, Europos Parlamento ir Tarybos reglamentu (ES) 2019/881[1] sukurta Europos kibernetinio saugumo sertifikavimo schemų kūrimo sistema;

(1a) siekiant užtikrinti Sąjungos atsparumą kibernetiniams išpuoliams ir užkirsti kelią bet kokiam pažeidžiamumui Sąjungos rinkoje, šiuo reglamentu siekiama papildyti horizontaliąją reguliavimo sistemą, kuria nustatomi išsamūs kibernetinio saugumo reikalavimai visiems produktams su skaitmeniniais elementais pagal Europos Parlamento ir Tarybos reglamentą (ES) .../...[2] (2022/0272(COD)), nustatant esminius reikalavimus dėl valdomų kibernetinio saugumo paslaugų, jų taikymo ir patikimumo;

(2) valdomos saugumo paslaugos, t. y. paslaugos, apimančios su klientų kibernetinės rizikos valdymu susijusios veiklos vykdymą arba paramą tokiai veiklai***, įskaitant incidentų aptikimą, reagavimą į juos ar veiklos atkūrimą jiems įvykus***, tampa vis svarbesnės kibernetinių incidentų prevencijai ir jų poveikio mažinimui. ***Valdomų saugumo paslaugų teikėjų veikla apima paslaugas, susijusias su prevencija, identifikavimu, apsauga, aptikimu, analize, apribojimu, reagavimu ir veiklos atkūrimu, įskaitant, be kitų, žvalgybos informacijos apie kibernetines grėsmes teikimą, grėsmių stebėseną realiuoju laiku taikant proaktyvius metodus, be kita ko, pritaikytąjį saugumą, rizikos vertinimą, išplėstinį aptikimą, ištaisymą ir reagavimą.*** Todėl tų paslaugų teikėjai pagal Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555[3] laikomi esminiais arba svarbiais subjektais, priklausančiais itin svarbiam sektoriui. Kaip pažymima tos direktyvos 86 konstatuojamojoje dalyje, valdomų

---

1 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).

2 … m. … … d. Europos Parlamento ir Tarybos reglamentas (ES) .../... dėl ... (OL L ..., ..., ELI: ...).

3 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva) (OL L 333, 2022 12 27, p. 80).

saugumo paslaugų teikėjams tokiose srityse kaip reagavimas į incidentus, skverbimosi testavimas, saugumo auditai ir konsultacijos tenka itin svarbus vaidmuo padėti subjektams užkirsti kelią incidentams, juos aptikti, į juos reaguoti ar po jų atkurti veiklą. Tačiau valdomų saugumo paslaugų teikėjai ir patys yra kibernetinių išpuolių taikiniai ir dėl jų glaudžios integracijos į klientų veiklą kyla specifinė rizika. Todėl esminiai ir svarbūs subjektai, kaip jie aiškinami Direktyvoje (ES) 2022/2555, rinkdamiesi valdomų saugumo paslaugų teikėją turėtų veikti atidžiau;

(3) valdomų saugumo paslaugų teikėjams tenka svarbus vaidmuo ir ES kibernetinio saugumo rezerve, kurio laipsniškas kūrimas remiamas Reglamentu (ES) …/…. [kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės]. ES kibernetinio saugumo rezervą numatoma naudoti teikiant paramą reaguoti ir imtis neatidėliojamų atkuriamųjų veiksmų reikšmingų ir didelio masto kibernetinių incidentų atvejais. Reglamentu (ES) …/… [kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės] nustatomas paslaugų teikėjų atrankos į ES kibernetinio saugumo rezervą procesas, kuriame, *inter alia*, turėtų būti atsižvelgiama į tai, ar paslaugų teikėjas yra įgijęs Europos arba nacionalinį kibernetinio saugumo sertifikatą. Atitinkamos paslaugos, kurias teikia patikimi paslaugų teikėjai pagal Reglamentą (ES) …./…. [kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės], atitinka valdomų saugumo paslaugų sampratą pagal šį reglamentą;

(4) valdomų saugumo paslaugų sertifikavimas yra aktualus ne vien atrankos į ES kibernetinio saugumo rezervą proceso metu – tai taip pat yra svarbus kokybės rodiklis privačiojo ir viešojo sektorių subjektams, ketinantiems pirkti tokias paslaugas. Atsižvelgiant į valdomų saugumo paslaugų svarbą ir į pažeidžiamumą, siejamą su duomenimis, tvarkomais teikiant tas paslaugas, sertifikavimas gali suteikti potencialiems klientams svarbių gairių ir garantijų dėl tų paslaugų patikimumo. Valdomų saugumo paslaugų Europos sertifikavimo schemomis padedama išvengti bendrosios rinkos susiskaidymo. Taigi, šiuo reglamentu siekiama gerinti vidaus rinkos veikimą;

(4a) valdomų saugumo paslaugų Europos sertifikavimo schemos turėtų paskatinti naudojimąsi tomis paslaugomis ir padidinti konkurenciją šioje srityje, atsižvelgiant į konkrečius paslaugų teikėjų ir naudos gavėjų poreikius. Todėl tomis schemomis turėtų būti užtikrinta pusiausvyra tarp jų tikslo ir galimos reguliavimo, administracinės ir finansinės naštos, su kuria gali susidurti paslaugų teikėjai, ypač labai mažos įmonės arba mažosios ir vidutinės įmonės (MVĮ). Be to, šiomis schemomis turėtų būti skatinamas sertifikuotų valdomų saugumo paslaugų naudojimas, padedant didinti jų prieinamumą, visų pirma mažesniems subjektams, pavyzdžiui, labai mažoms įmonėms ir MVĮ, taip pat vietos ir regionų valdžios institucijoms, kurių pajėgumai ir ištekliai yra riboti, tačiau kurios dažniau susiduria su kibernetinio saugumo pažeidimais, dėl kurių patiriami finansiniai ir teisiniai padariniai bei pasekmės reputacijai ir veiklai;

(4b) valdomų saugumo paslaugų Sąjungos sertifikavimo schema turėtų užtikrinti galimybę naudotis saugiomis ir aukštos kokybės paslaugomis, kuriomis užtikrinama saugi skaitmeninė pertvarka ir padedama siekti Skaitmeninio dešimtmečio politikos programoje nustatytų tikslų, visų pirma susijusių su tikslu, kad 75 proc. Sąjungos įmonių pradėtų naudotis debesijos, DI ar didžiųjų duomenų technologijomis, kad daugiau kaip 90 proc. labai mažų įmonių ir MVĮ pasiektų bent bazinį skaitmeninio intensyvumo lygį ir kad pagrindinės viešosios paslaugos būtų teikiamos internetu;

(4c) dabartinėje sparčiai kintančioje skaitmeninėje ir technologinėje aplinkoje švietimo išteklių ir formaliųjų mokymų pasiūla skiriasi, o žinios gali būti įgyjamos įvairiais būdais – tiek formaliai, pvz., universitetuose ar kursuose, tiek neformaliai, pvz., mokantis darbo vietoje arba kaupiant ilgalaikę darbo patirtį atitinkamoje srityje;

(5) be IRT produktų, IRT paslaugų ar IRT procesų diegimo, valdomos saugumo paslaugos dažnai apima ir papildomas paslaugų funkcijas, kurios priklauso nuo jas teikiančių darbuotojų kompetencijos, kvalifikacijos ir patirties. Siekiant užtikrinti labai aukštą teikiamų valdomų saugumo paslaugų kokybę, į saugumo tikslus turėtų būti įtrauktas labai aukštas šios kompetencijos, kvalifikacijos bei patirties lygis ir atitinkamos vidaus procedūros. Todėl, siekiant užtikrinti, kad ***speciali*** sertifikavimo schema galėtų apimti visus valdomos saugumo paslaugos aspektus, būtina iš dalies pakeisti Reglamentą (ES) 2019/881***. Plėtojant pagal šį reglamentą nustatytas***

sertifikavimo schemas turėtų būti atsižvelgiama į šiame reglamente numatyto vertinimo ir peržiūros rezultatus ir rekomendacijas;

(5a) siekiant sudaryti palankesnes sąlygas patikimos Sąjungos rinkos augimui, kartu mezgant partnerystes su bendramintėmis trečiosiomis šalimis, be kita ko, atsižvelgiant į Europos Parlamento ir Tarybos reglamento (ES) .../...[1] (2023/0109(COD)) nuostatas dėl prieigos prie ES kibernetinio saugumo rezervo, šiuo reglamentu nustatytoje sistemoje nustatytas sertifikavimo procesas turėtų būti supaprastintas, kad būtų užtikrintas tarptautinis pripažinimas ir suderinimas su tarptautiniais standartais;

(5b) siekiant užtikrinti patikimos valdomų saugumo paslaugų Sąjungos rinkos plėtrą, paslaugų teikėjai ir valstybės narės turėtų bendradarbiauti ir prisidėti renkant duomenis apie kibernetinio saugumo darbo rinkos padėtį ir raidą;

(5c) Sąjungos suderintas požiūris į ypatingos svarbos infrastruktūros objektų atsparumo didinimą grindžiamas valstybių narių pajėgumų stiprinimu. Tačiau Sąjunga susiduria su talentų trūkumu, nes trūksta kvalifikuotų specialistų, ir sparčiai kintančia grėsmių panorama, kaip pripažinta 2023 m. balandžio 18 d. Komisijos komunikate dėl Kibernetinio saugumo įgūdžių akademijos. Todėl, siekiant sudaryti palankesnes sąlygas aukštos kokybės esminių valdomų saugumo paslaugų atsiradimui ir geriau apžvelgti Sąjungos kibernetinio saugumo srities darbo jėgos sudėtį, reikėtų stiprinti valstybių narių, Komisijos, ENISA ir suinteresuotųjų subjektų, įskaitant privatųjį sektorių ir akademinę bendruomenę, bendradarbiavimą plėtojant viešojo ir privačiojo sektorių partnerystę, remiant mokslinių tyrimų ir inovacijų iniciatyvas, plėtojant ir abipusiškai pripažįstant bendrus kibernetinio saugumo įgūdžių standartus ir sertifikavimą, be kita ko, pasitelkiant Europos kibernetinio saugumo įgūdžių sistemą. Be to, tai turėtų sudaryti palankesnes sąlygas kibernetinio saugumo specialistų judumui Sąjungoje, taip pat kibernetinio saugumo žinių ir mokymo integravimui į švietimo programas, kartu užtikrinant, kad jaunimas, įskaitant asmenis, gyvenančius nepalankioje padėtyje esančiuose regionuose, pvz., salose, retai apgyvendintose, kaimo ir atokiose vietovėse, turėtų galimybę dalyvauti pameistrystės ir stažuočių

[1] … m. … … d. Europos Parlamento ir Tarybos reglamentas (ES) .../... dėl ... (OL L ..., ..., ELI: ...).

programose. Tomis priemonėmis taip pat turėtų būti siekiama pritraukti daugiau moterų ir mergaičių į šią sritį ir padėti mažinti lyčių nelygybę mokslo, technologijų, inžinerijos ir matematikos srityse. Privatusis sektorius taip pat turėtų siekti užtikrinti mokymą darbo vietoje, atsižvelgiant į paklausiausius įgūdžius, įtraukiant viešojo administravimo institucijas ir startuolius, taip pat labai mažas įmones ir MVĮ;

(5d) turėtų būti užtikrintas tinkamas finansavimas ir ištekliai papildomoms užduotims, kurios pavestos ENISA šiuo reglamentu padarytais Reglamento (ES) 2019/881 pakeitimais, vykdyti;

(5e) siekiant papildyti tam tikrus neesminius šio reglamento elementus, pagal Sutarties dėl Europos Sąjungos veikimo 290 straipsnį Komisijai turėtų būti suteikti įgaliojimai priimti teisės aktus, kuriais būtų nustatyta Europos kibernetinio saugumo sertifikavimo schema, skirta IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms. Ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat ir su ekspertais, ir kad tos konsultacijos būtų vykdomos vadovaujantis 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros[1] nustatytais principais. Visų pirma siekiant užtikrinti vienodas galimybes dalyvauti atliekant su deleguotaisiais aktais susijusį parengiamąjį darbą, Europos Parlamentas ir Taryba visus dokumentus gauna tuo pačiu metu kaip ir valstybių narių ekspertai, o jų ekspertams sistemingai suteikiama galimybė dalyvauti Komisijos ekspertų grupių, kurios atlieka su deleguotaisiais aktais susijusį parengiamąjį darbą, posėdžiuose;

(5e) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 42 straipsnio 1 dalimi buvo pasikonsultuota su Europos duomenų apsaugos priežiūros pareigūnu ir [MMMM MM DD] jis pateikė savo nuomonę[2],

PRIĖMĖ ŠĮ REGLAMENTĄ:

---

1 OL L 123, 2016 5 12, p. 1.

2 ***OL C .../...***

1 straipsnis

Reglamento (ES) 2019/881 pakeitimai

Reglamentas (ES) 2019/881 iš dalies keičiamas taip:

1) 1 straipsnio 1 dalies pirmos pastraipos b punktas pakeičiamas taip:

„b) Europos kibernetinio saugumo sertifikavimo schemų nustatymo sistema, siekiant užtikrinti tinkamą IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų kibernetinio saugumo lygį Sąjungoje, taip pat išvengti rinkos susiskaidymo Sąjungoje kibernetinio saugumo sertifikavimo schemų srityje.“;

2) 2 straipsnis iš dalies keičiamas taip:

a) 9, 10 ir 11 punktai pakeičiami taip:

„9) Europos kibernetinio saugumo sertifikavimo schema – išsamus Sąjungos lygmeniu nustatytų taisyklių, techninių reikalavimų, standartų ir procedūrų, kurie taikomi konkrečių IRT produktų, IRT paslaugų, IRT procesų ar valdomų saugumo paslaugų sertifikavimui arba atitikties vertinimui, rinkinys;

10) nacionalinė kibernetinio saugumo sertifikavimo schema – išsamus taisyklių, techninių reikalavimų, standartų ir procedūrų, kuriuos parengė ir priėmė nacionalinė valdžios institucija, rinkinys, taikomas IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų, kuriems taikoma ta konkreti schema, sertifikavimui arba atitikties vertinimui;

11) Europos kibernetinio saugumo sertifikatas – dokumentas, kurį išdavė atitinkama įstaiga ir kuriuo patvirtinama, kad tam tikras IRT produktas, IRT paslauga, IRT procesas ar valdoma saugumo paslauga buvo įvertinti dėl atitikties Europos kibernetinio saugumo sertifikavimo schemoje nustatytiems konkretiems saugumo reikalavimams;“;

b) įterpiamas šis punktas:

„14a) valdoma saugumo paslauga – ***trečiajai šaliai teikiama*** paslauga, apimanti su kibernetinio saugumo rizikos valdymu susijusios veiklos (įskaitant ***incidentų valdymą***, skverbimosi testavimą, saugumo auditus ir

konsultacijas) vykdymą***,*** paramą tokiai veiklai ***arba konsultavimą dėl jos***;“;

c) 20, 21 ir 22 punktai pakeičiami taip:

„20) techninės specifikacijos – dokumentas, kuriame nustatyti techniniai reikalavimai, kuriuos turi atitikti IRT produktas, IRT paslauga, IRT procesas ar valdoma saugumo paslauga, arba su IRT produktu, IRT paslauga, IRT procesu ar valdoma saugumo paslauga susijusios atitikties vertinimo procedūros;

21) saugumo užtikrinimo lygis – pagrindas pasitikėti, kad IRT produktas, IRT paslauga, IRT procesas ar valdoma saugumo paslauga atitinka tam tikros Europos kibernetinio saugumo sertifikavimo schemos saugumo reikalavimus: juo nurodoma, kokiu lygiu IRT produktas, IRT paslauga, IRT procesas ar valdoma saugumo paslauga yra įvertinti, tačiau jis pats nerodo atitinkamo IRT produkto, IRT paslaugos, IRT proceso ar valdomos saugumo paslaugos saugumo;

22) savarankiškas atitikties vertinimas – IRT produktų gamintojo, IRT paslaugų ar procesų teikėjo arba valdomų saugumo paslaugų teikėjo atliekamas veiksmas, kuriuo įvertinama, ar tie IRT produktai, paslaugos ar procesai arba valdomos saugumo paslaugos atitinka konkrečios Europos kibernetinio saugumo sertifikavimo schemos reikalavimus.“;

3) 4 straipsnio 6 dalis pakeičiama taip:

„6. ENISA skatina naudoti Europos kibernetinio saugumo sertifikavimą siekiant išvengti vidaus rinkos susiskaidymo. ENISA prisideda prie Europos kibernetinio saugumo sertifikavimo sistemos sukūrimo ir taikymo pagal šio reglamento III antraštinę dalį, siekiant didinti IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų kibernetinio saugumo skaidrumą ir taip sustiprinti pasitikėjimą skaitmenine vidaus rinka ir jos konkurencingumą.“;

4) 8 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. ENISA remia ir skatina IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų kibernetinio saugumo sertifikavimo

Sąjungos politikos plėtojimą ir įgyvendinimą, kaip nustatyta šio reglamento III antraštinėje dalyje:

a) tais atvejais, kai standartų nėra, nuolat stebėdama pokyčius susijusiose standartizacijos srityse ir rekomenduodama atitinkamas technines specifikacijas, skirtas Europos kibernetinio saugumo sertifikavimo schemoms rengti, pagal 54 straipsnio 1 dalies c punktą;

b) rengdama potencialias IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų Europos kibernetinio saugumo sertifikavimo schemas (potenciali schema) pagal 49 straipsnį;

c) vertindama patvirtintas Europos kibernetinio saugumo sertifikavimo schemas pagal 49 straipsnio 8 dalį;

d) dalyvaudama tarpusavio peržiūrose pagal 59 straipsnio 4 dalį;

e) padėdama Komisijai teikti sekretoriato paslaugas Europos kibernetinio saugumo sertifikavimo grupei pagal 62 straipsnio 5 dalį.“;

b) 3 dalis pakeičiama taip:

„3. ENISA rengia ir skelbia gaires ir formuoja gerąją praktiką, susijusią su IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms taikomais kibernetinio saugumo reikalavimais, formaliai, struktūrizuotai ir skaidriai bendradarbiaudama su nacionalinėmis kibernetinio saugumo sertifikavimo institucijomis ir pramonės sektoriumi.“;

c) 5 dalis pakeičiama taip:

„5. ENISA palengvina Europos ir tarptautinių rizikos valdymo ir IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų saugumo standartų nustatymą ir įdiegimą.“;

5) 46 straipsnio 1 ir 2 dalys pakeičiamos taip:

„1. Siekiant gerinti vidaus rinkos veikimo sąlygas didinant kibernetinio saugumo lygį Sąjungoje ir sudarant sąlygas Sąjungos lygmeniu suderintai taikyti

Europos kibernetinio saugumo sertifikavimo schemas, kad būtų sukurta IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų bendroji skaitmeninė rinka, nustatoma Europos kibernetinio saugumo sertifikavimo sistema.

2. Europos kibernetinio saugumo sertifikavimo sistemoje nustatomas mechanizmas, skirtas Europos kibernetinio saugumo sertifikavimo schemoms sukurti. Juo patvirtinama, kad pagal tokias schemas įvertinti IRT produktai, paslaugos ir procesai atitinka nustatytus saugumo reikalavimus siekiant apsaugoti saugomų, perduodamų ar tvarkomų duomenų arba tais produktais, paslaugomis ir procesais arba per juos prieinamų funkcijų ar paslaugų prieinamumą, autentiškumą, vientisumą ar konfidencialumą viso jų gyvavimo ciklo metu. Juo taip pat patvirtinama, kad pagal tokias schemas įvertintos valdomos saugumo paslaugos atitinka nustatytus saugumo reikalavimus siekiant apsaugoti duomenų, kurie gaunami, tvarkomi, saugomi ar perduodami teikiant tas paslaugas, prieinamumą, autentiškumą, vientisumą ir konfidencialumą, ir kad tas paslaugas nuolat teikia reikiamą kompetenciją, kvalifikaciją ir patirtį turintys darbuotojai, kurie yra įgiję atitinkamų labai aukšto lygio techninių žinių ir laikosi profesinio sąžiningumo principų.“;

6) 47 straipsnio 2 ir 3 dalys pakeičiamos taip:

„2. Į tęstinę Sąjungos darbo programą visų pirma įtraukiamas IRT produktų, paslaugų ir procesų arba jų kategorijų, taip pat valdomų saugumo paslaugų, kurie gali būti įtraukti į Europos kibernetinio saugumo sertifikavimo schemos taikymo sritį, sąrašas. ***Atsižvelgdama į tai, Komisija gali įtraukti išsamų esamų mokymo trajektorijų vertinimą, kad pašalintų nustatytas įgūdžių spragas, ir pasiūlymų, kaip patenkinti kvalifikuotų darbuotojų poreikį ir suteikti reikiamų rūšių įgūdžių, sąrašą.***

3. Konkrečių IRT produktų, paslaugų ir procesų ar jų kategorijų arba valdomų saugumo paslaugų įtraukimas į tęstinę Sąjungos darbo programą grindžiamas vienu iš šių pagrindų:

a) tuo, kad yra sukurtos ir plėtojamos nacionalinės kibernetinio saugumo sertifikavimo schemos, apimančios konkrečią IRT produktų, IRT paslaugų, IRT procesų ar valdomų saugumo paslaugų kategoriją, ypač

kiek tai susiję su susiskaidymo rizika;

b) atitinkama Sąjungos arba valstybės narės politika ar teisės aktais;

c) rinkos paklausa;

ca) technologine plėtra ir tarptautinių kibernetinio saugumo sertifikavimo schemų bei tarptautinių ir pramonės standartų prieinamumu ir plėtojimu;

d) kibernetinių grėsmių raidos pokyčiais;

e) EKSSG prašymu parengti konkrečią potencialią schemą.“;

7) 49 ***straipsnis iš dalies keičiamas*** taip:

a) 7 dalis pakeičiama taip:

„7. ***Remiantis*** ENISA pasiūlyta potencialia schema, Komisijai ***suteikiami įgaliojimai pagal 65a straipsnį*** priimti ***deleguotuosius*** aktus, ***kuriais šis reglamentas papildomas numatant*** 51, 52 ir 54 straipsnių reikalavimus ***atitinkančias*** IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų Europos kibernetinio saugumo sertifikavimo ***schemas****.****“;***

b) įterpiama ši dalis:

„7a. Prieš priimdama tokius deleguotuosius aktus, Komisija, bendradarbiaudama su ENISA, atlieka ir paskelbia siūlomos Europos kibernetinio saugumo sertifikavimo schemos poveikio vertinimą. Rengdama poveikio vertinimą, Komisija rengia viešas konsultacijas ir konsultuojasi su Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupe ir Europos kibernetinio saugumo sertifikavimo grupe.“;

8) 51 straipsnis iš dalies keičiamas taip:

a) pavadinimas pakeičiamas taip:

„IRT produktų, IRT paslaugų ir IRT procesų Europos kibernetinio saugumo sertifikavimo schemų saugumo tikslai“;

b) įvadinis sakinys pakeičiamas taip:

„IRT produktų, IRT paslaugų ar IRT procesų Europos kibernetinio saugumo sertifikavimo schema turi būti parengta taip, kad būtų pasiekti atitinkamai bent šie saugumo tikslai:“***;***

9) įterpiamas šis straipsnis:

„51a straipsnis
Valdomų saugumo paslaugų Europos kibernetinio saugumo sertifikavimo schemų saugumo tikslai

Valdomų saugumo paslaugų Europos kibernetinio saugumo sertifikavimo schema turi būti parengta taip, kad būtų pasiekti atitinkamai bent šie saugumo tikslai:

a) būtų užtikrinta, kad valdomos saugumo paslaugos būtų teikiamos turint reikiamą kompetenciją, kvalifikaciją ir patirtį, taip pat kad už tų paslaugų teikimą atsakingi darbuotojai turėtų labai aukšto lygio techninių žinių ir gebėjimų toje konkrečioje srityje bei pakankamai tinkamos patirties ir laikytųsi aukščiausių profesinio sąžiningumo standartų;

b) būtų užtikrinta, kad paslaugų teikėjas taikytų tinkamas vidaus procedūras, skirtas užtikrinti, kad valdomos saugumo paslaugos būtų visada teikiamos labai kokybiškai;

c) teikiant valdomas saugumo paslaugas gaunami, saugomi, perduodami ar kitaip tvarkomi duomenys būtų apsaugoti nuo atsitiktinio ar neteisėto jų gavimo, saugojimo, atskleidimo, sunaikinimo, kitokio tvarkymo, praradimo, pakeitimo ar neprieinamumo;

d) būtų užtikrinta, kad įvykus fiziniam ar techniniam incidentui būtų laiku atkurta galimybė naudotis duomenimis, paslaugomis bei funkcijomis ir prieiga prie jų;

e) būtų užtikrinta, kad leidimą turintys asmenys, programos ar mašinos galėtų gauti prieigą tik prie tų duomenų, paslaugų ar funkcijų, su kuriais yra susijusios jų prieigos teisės;

f) būtų užfiksuota ir galima patikrinti, prie kurių duomenų, paslaugų ar funkcijų buvo gauta prieiga, kuriais jų buvo pasinaudota ar jie buvo kitaip tvarkomi, kada ir kas tai padarė;

g) būtų užtikrintas IRT produktų, paslaugų ir procesų, naudojamų teikiant valdomas saugumo paslaugas, standartizuotasis ir integruotasis saugumas, ***jų***

aprūpinimas naujausia programine ir aparatine įranga, žinomų pažeidžiamumo spragų nebuvimas ir naujausių saugumo naujinių įdiegimas.“;

10) 52 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Europos kibernetinio saugumo sertifikavimo schemoje gali būti nurodytas vienas ar daugiau iš šių IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms taikomų saugumo užtikrinimo lygių: bazinis, pakankamai aukštas arba aukštas. Saugumo užtikrinimo lygis turi atitikti su IRT produkto, IRT paslaugos, IRT proceso ar valdomos saugumo paslaugos numatomu naudojimu susijusios rizikos lygį, apibrėžiamą atsižvelgiant į incidento tikimybę ir poveikį.“;

b) 3 dalis pakeičiama taip:

„3. Kiekvieną saugumo užtikrinimo lygį atitinkantys saugumo reikalavimai nustatomi atitinkamoje Europos kibernetinio saugumo sertifikavimo schemoje, įskaitant atitinkamas saugumo funkcines galimybes ir atitinkamą IRT produkto, IRT paslaugos, IRT proceso ar valdomos saugumo paslaugos vertinimo griežtumą ir išsamumą.“;

c) 5, 6 ir 7 dalys pakeičiamos taip:

„5. Europos kibernetinio saugumo sertifikatu arba ES atitikties pareiškimu, kuriame nurodytas bazinis saugumo užtikrinimo lygis, garantuojama, kad IRT produktai, IRT paslaugos, IRT procesai ir valdomos saugumo paslaugos, dėl kurių išduotas tas sertifikatas ar ES atitikties pareiškimas, tenkina atitinkamus saugumo reikalavimus, įskaitant saugumo funkcines galimybes, ir kad jie buvo įvertinti tokiu lygiu, kad būtų kuo labiau sumažinta žinoma bazinė kibernetinių incidentų ir kibernetinių išpuolių rizika. Atliktini įvertinimo veiksmai turi apimti bent techninių dokumentų peržiūrą. Kai tokia peržiūra netaikytina, turi būti atlikti pakaitiniai lygiavertį poveikį turintys įvertinimo veiksmai.

6. Europos kibernetinio saugumo sertifikatu, kuriame nurodytas pakankamai aukštas saugumo užtikrinimo lygis, garantuojama, kad IRT

produktai, IRT paslaugos, IRT procesai ir valdomos saugumo paslaugos, dėl kurių išduotas tas sertifikatas, tenkina atitinkamus saugumo reikalavimus, įskaitant saugumo funkcines galimybes, ir kad jie buvo įvertinti tokiu lygiu, kad būtų kuo labiau sumažinta žinoma kibernetinė rizika ir kibernetinių incidentų bei kibernetinių išpuolių, kuriuos vykdo ribotų gebėjimų ir ribotų išteklių turintys subjektai, pavojus. Atliktini įvertinimo veiksmai turi apimti bent šiuos veiksmus: įvertinimą, ar nėra viešai žinomų pažeidžiamumo spragų, ir išbandymą, ar IRT produktais, IRT paslaugomis, IRT procesais ar valdomomis saugumo paslaugomis tinkamai įgyvendinamos reikiamos saugumo funkcinės galimybės. Jei tokie įvertinimo veiksmai netaikytini, turi būti atlikti pakaitiniai lygiavertį poveikį turintys įvertinimo veiksmai.

7. Europos kibernetinio saugumo sertifikatu, kuriame nurodytas aukštas saugumo užtikrinimo lygis, garantuojama, kad IRT produktai, IRT paslaugos, IRT procesai ir valdomos saugumo paslaugos, dėl kurių išduotas tas sertifikatas, tenkina atitinkamus saugumo reikalavimus, be kita ko, saugumo funkcinių galimybių atžvilgiu, ir kad jie buvo įvertinti tokiu lygiu, kad būtų kuo labiau sumažinta naujausiomis technologijomis pagrįstų kibernetinių išpuolių, kuriuos vykdo aukšto lygio įgūdžių ir didelių išteklių turintys subjektai, rizika. Atliktini įvertinimo veiksmai turi apimti bent šiuos veiksmus: įvertinimą, ar nėra viešai žinomų pažeidžiamumo spragų; išbandymą, ar IRT produktais, IRT paslaugomis, IRT procesais ar valdomomis saugumo paslaugomis tinkamai įgyvendinamos būtinos naujausiomis technologijomis pagrįstos saugumo funkcinės galimybės; ir, atliekant skverbimosi bandymą, jų atsparumo aukšto lygio įgūdžių turinčių subjektų išpuoliams įvertinimą. Jei tokie vertinimo veiksmai netaikytini, turi būti atlikti pakaitiniai lygiavertį poveikį turintys vertinimo veiksmai.“;

11) 53 straipsnio 1, 2 ir 3 dalys pakeičiamos taip:

„1. Europos kibernetinio saugumo sertifikavimo schemoje gali būti numatyta galimybė, kad savarankiškas atitikties vertinimas atliekamas tik IRT produktų gamintojo, IRT paslaugų ar procesų teikėjo arba valdomų saugumo paslaugų teikėjo atsakomybe. Savarankiškas atitikties vertinimas taikytinas tik nedidelės

rizikos IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms, atitinkantiems bazinį saugumo užtikrinimo lygį.

2. IRT produktų gamintojas, IRT paslaugų ar procesų teikėjas arba valdomų saugumo paslaugų teikėjas gali išduoti ES atitikties pareiškimą, kuriame nurodoma, kad yra įrodyta atitiktis schemoje nurodytiems reikalavimams. Parengdamas tokį pareiškimą IRT produktų gamintojas, IRT paslaugų ar procesų teikėjas arba valdomų saugumo paslaugų teikėjas prisiima atsakomybę už IRT produkto, paslaugos ar proceso arba valdomos saugumo paslaugos atitiktį toje schemoje nurodytiems reikalavimams.

3. IRT produktų gamintojas, IRT paslaugų ar procesų teikėjas arba valdomų saugumo paslaugų teikėjas privalo atitinkamoje Europos kibernetinio saugumo sertifikavimo schemoje nurodytą laikotarpį saugoti ES atitikties pareiškimą, techninę dokumentaciją ir visą kitą aktualią informaciją, susijusią su IRT produktų, IRT paslaugų ar valdomų saugumo paslaugų atitiktimi tai schemai, kad galėtų juos pateikti nacionalinei kibernetinio saugumo sertifikavimo institucijai, nurodytai 58 straipsnyje. ES atitikties pareiškimo kopija pateikiama nacionalinei kibernetinio saugumo sertifikavimo institucijai ir ENISA.“;

12) 54 straipsnio 1 dalis iš dalies keičiama taip:

a) a punktas pakeičiamas taip:

„a) sertifikavimo schemos dalykas ir apimtis, įskaitant sertifikuojamų IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų rūšį arba kategorijas;“;

b) j punktas pakeičiamas taip:

„j) IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų atitikties Europos kibernetinio saugumo sertifikatų arba ES atitikties pareiškimų reikalavimams stebėsenos taisyklės, įskaitant mechanizmus, kuriais įrodoma, kad nuolat laikomasi nurodytų kibernetinio saugumo reikalavimų;“;

c) l punktas pakeičiamas taip:

„l) taisyklės, susijusios su padariniais IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms, kurie buvo

sertifikuoti arba kuriems išduotas ES atitikties pareiškimas, tačiau kurie neatitinka schemos reikalavimų;“;

d) o punktas pakeičiamas taip:

„o) informacija apie nacionalines arba tarptautines kibernetinio saugumo sertifikavimo schemas, taikomas tos pačios rūšies ar kategorijų IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms, saugumo reikalavimus, vertinimo kriterijus bei metodus ir saugumo užtikrinimo lygius;“;

e) q punktas pakeičiamas taip:

„q) laikotarpis, kurį turi būti prieinamas ES atitikties pareiškimas, techninė dokumentacija ir visa kita aktuali informacija, kurią IRT produktų gamintojas, IRT paslaugų ar procesų teikėjas arba valdomų saugumo paslaugų teikėjas turi galėti pateikti susipažinti;“;

13) 56 straipsnis iš dalies keičiamas taip:

a) 1 dalis pakeičiama taip:

„1. Laikoma, kad pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal 49 straipsnį, sertifikuoti IRT produktai, IRT paslaugos, IRT procesai ir valdomos saugumo paslaugos atitinka tos schemos reikalavimus.“;

b) 3 dalis iš dalies keičiama taip:

i) pirma pastraipa pakeičiama taip:

Komisija reguliariai vertina priimtų Europos kibernetinio saugumo sertifikavimo schemų veiksmingumą bei naudojimą ir tai, ar kuri nors konkreti Europos kibernetinio saugumo sertifikavimo schema atitinkamais Sąjungos teisės aktais turi būti nustatyta kaip privaloma siekiant užtikrinti tinkamą IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų kibernetinio saugumo lygį Sąjungoje ir pagerinti vidaus rinkos veikimą. Pirmas toks vertinimas atliekamas ne vėliau kaip 2023 m. gruodžio 31 d., o vėlesni vertinimai atliekami bent kas dvejus metus. Remdamasi tų vertinimų rezultatais Komisija nustato tuos IRT produktus, IRT paslaugas, IRT procesus ir valdomas saugumo

paslaugas, kuriems taikoma esama sertifikavimo sistema, tačiau kuriems turėtų būti taikoma privaloma sertifikavimo schema.“;

ii) trečia pastraipa iš dalies keičiama taip:

aa) a punktas pakeičiamas taip:

„a) atsižvelgia į su sąnaudomis susijusį priemonių poveikį tokių IRT produktų gamintojams, IRT paslaugų ar procesų teikėjams ir valdomų saugumo paslaugų teikėjams bei naudotojams, taip pat į numatomo tikslinių IRT produktų, paslaugų, procesų ar valdomų saugumo paslaugų didesnio saugumo visuomeninę ar ekonominę naudą;“;

bb) d punktas pakeičiamas taip:

„d) atsižvelgia į įgyvendinimo terminus, pereinamojo laikotarpio priemones ir laikotarpius, visų pirma dėl galimo priemonės poveikio IRT produktų gamintojams, IRT paslaugų ar procesų teikėjams arba valdomų saugumo paslaugų teikėjams, įskaitant ***konkrečius labai mažų įmonių ir MVĮ interesus ir poreikius***;“;

iii) pridedama ši pastraipa:

„Kiek tai susiję su šio straipsnio trečios pastraipos d punktu, Komisija užtikrina tinkamą finansinę paramą pagal esamų Sąjungos programų reguliavimo sistemą, visų pirma siekdama palengvinti finansinę naštą labai mažoms įmonėms ir MVĮ, įskaitant startuolius, veikiančius valdomų saugumo paslaugų srityje.“;

c) 7 ir 8 dalys pakeičiamos taip:

„7. IRT produktus, IRT paslaugas, IRT procesus ar valdomas saugumo paslaugas sertifikuoti teikiantis fizinis arba juridinis asmuo 58 straipsnyje nurodytai nacionalinei kibernetinio saugumo sertifikavimo institucijai, kai ši institucija yra Europos kibernetinio saugumo sertifikatą išduodanti įstaiga, arba 60 straipsnyje nurodytai atitikties vertinimo įstaigai leidžia susipažinti su visa sertifikavimo procedūrai atlikti reikalinga informacija.

8. Europos kibernetinio saugumo sertifikato turėtojas informuoja 7 dalyje

nurodytą instituciją arba įstaigą apie su sertifikuotu IRT produktu, IRT paslauga, IRT procesu ar valdomomis saugumo paslaugomis susijusias vėliau nustatytas pažeidžiamumo spragas ar neatitikties atvejus, kurie gali daryti poveikį atitikčiai su sertifikavimu susijusiems reikalavimams. Ta institucija ar įstaiga nepagrįstai nedelsdama perduoda tą informaciją atitinkamai nacionalinei kibernetinio saugumo sertifikavimo institucijai.“;

14) 57 straipsnio 1 ir 2 dalys pakeičiamos taip:

„1. Nedarant poveikio šio straipsnio 3 daliai, nacionalinės kibernetinio saugumo sertifikavimo schemos ir susijusios procedūros, taikomos IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms, kuriems taikoma Europos kibernetinio saugumo sertifikavimo schema, netenka galios nuo datos, nustatytos pagal 49 straipsnio 7 dalį priimtame ***deleguotajame akte***. Nacionalinės kibernetinio saugumo sertifikavimo schemos ir susijusios procedūros, taikomos IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms, kuriems netaikoma Europos kibernetinio saugumo sertifikavimo schema, galioja ir toliau.

2. Valstybės narės neįveda naujų nacionalinių kibernetinio saugumo sertifikavimo schemų IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms, kuriems jau taikoma galiojanti Europos kibernetinio saugumo sertifikavimo schema.“;

15) 58 straipsnis iš dalies keičiamas taip:

a) 7 dalis iš dalies keičiama taip:

i) a ir b punktai pakeičiami taip:

„a) bendradarbiaudamos su kitomis atitinkamomis rinkos priežiūros institucijomis prižiūri, kaip įgyvendinamos į Europos kibernetinio saugumo sertifikavimo schemas pagal 54 straipsnio 1 dalies j punktą įtrauktos IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų atitikties sertifikatų, kurie buvo išduoti jų atitinkamose teritorijose, reikalavimams stebėsenos taisyklės, ir užtikrina jų įgyvendinimą;

b) stebi, kaip jų atitinkamose teritorijose įsisteigę ir savarankišką atitikties vertinimą atliekantys IRT produktų gamintojai, IRT paslaugų ar procesų teikėjai arba valdomų saugumo paslaugų teikėjai vykdo savo pareigas, visų pirma 53 straipsnio 2 ir 3 dalyse ir atitinkamoje Europos kibernetinio saugumo sertifikavimo schemoje nustatytas tokių gamintojų ar teikėjų pareigas, ir užtikrina jų vykdymą;“;

ii) h punktas pakeičiamas taip:

„h) bendradarbiauja su kitomis nacionalinėmis kibernetinio saugumo sertifikavimo institucijomis ar kitomis valdžios institucijomis, be kita ko, dalydamosi informacija apie galimą IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų neatitiktį šio reglamento arba konkrečių Europos kibernetinio saugumo sertifikavimo schemų reikalavimams, ir“;

b) 9 dalis pakeičiama taip:

„9. Nacionalinės kibernetinio saugumo sertifikavimo institucijos bendradarbiauja tarpusavyje ir su Komisija, visų pirma keičiasi informacija, patirtimi ir gerąja praktika, susijusiomis su kibernetinio saugumo sertifikavimu ir IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų kibernetinio saugumo techniniais klausimais.“;

16) 59 straipsnio 3 dalies b ir c punktai pakeičiami taip:

„b) procedūros, skirtos prižiūrėti, kaip įgyvendinamos taisyklės dėl IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų atitikties Europos kibernetinio saugumo sertifikatams stebėsenos, ir užtikrinti jų įgyvendinimą pagal 58 straipsnio 7 dalies a punktą;

c) procedūros, skirtos stebėti, kaip vykdomos IRT produktų gamintojų, IRT paslaugų ar procesų teikėjų arba valdomų saugumo paslaugų teikėjų pareigos, ir užtikrinti jų vykdymą pagal 58 straipsnio 7 dalies b punktą;“;

16a) įterpiamas šis straipsnis:

„65a straipsnis

Įgaliojimų delegavimas

1. *Įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami šiame straipsnyje nustatytomis sąlygomis.*

2. *49 straipsnio 7 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami penkerių metų laikotarpiui nuo … [iš dalies keičiančio reglamento įsigaliojimo data]. Likus ne mažiau kaip devyniems mėnesiams iki penkerių metų laikotarpio pabaigos Komisija parengia naudojimosi deleguotaisiais įgaliojimais ataskaitą. Deleguotieji įgaliojimai savaime pratęsiami tokios pačios trukmės laikotarpiams, išskyrus atvejus, kai Europos Parlamentas arba Taryba pareiškia prieštaravimų dėl tokio pratęsimo likus ne mažiau kaip trims mėnesiams iki kiekvieno laikotarpio pabaigos.*

3. *Europos Parlamentas arba Taryba gali bet kada atšaukti 49 straipsnio 7 dalyje nurodytus deleguotuosius įgaliojimus. Sprendimu dėl įgaliojimų atšaukimo nutraukiami tame sprendime nurodyti įgaliojimai priimti deleguotuosius aktus. Sprendimas įsigalioja kitą dieną po jo paskelbimo Europos Sąjungos oficialiajame leidinyje arba vėlesnę jame nurodytą dieną. Jis nedaro poveikio jau galiojančių deleguotųjų aktų galiojimui.*

4. *Prieš priimdama deleguotąjį aktą Komisija konsultuojasi su kiekvienos valstybės narės paskirtais ekspertais vadovaudamasi 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros nustatytais principais.*

5. *Apie priimtą deleguotąjį aktą Komisija nedelsdama vienu metu praneša Europos Parlamentui ir Tarybai.*

6. *Pagal 49 straipsnio 7 dalį priimtas deleguotasis aktas įsigalioja tik tuo atveju, jeigu per du mėnesius nuo pranešimo Europos Parlamentui ir Tarybai apie šį aktą dienos nei Europos Parlamentas, nei Taryba nepareiškia prieštaravimų arba jeigu dar nepasibaigus šiam laikotarpiui ir Europos Parlamentas, ir Taryba praneša Komisijai, kad prieštaravimų nereikš. Europos Parlamento arba Tarybos iniciatyva šis laikotarpis pratęsiamas dviem mėnesiais.“;*

17) 67 straipsnis pakeičiamas taip:

„67 straipsnis

Vertinimas ir peržiūra

1. *Ne vėliau kaip 2024 m. birželio 28 d., o vėliau kas trejus metus Komisija įvertina ENISA ir jos darbo metodų poveikį, veiksmingumą bei efektyvumą ir galimą poreikį keisti ENISA įgaliojimus bei tokio pakeitimo finansinį poveikį. Atliekant vertinimą atsižvelgiama į grįžtamąją informaciją, pateiktą ENISA reaguojant į jos veiklą. Jei Komisija mano, kad tolesnė ENISA veikla nebepateisinama jai pavestų tikslų, įgaliojimų ir uždavinių atžvilgiu, Komisija gali siūlyti su ENISA susijusias šio reglamento nuostatas iš dalies pakeisti.*

2. *Vertinime vertinamas šio reglamento III antraštinės dalies nuostatų poveikis, veiksmingumas ir efektyvumas siekiant tikslų užtikrinti tinkamą IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų Sąjungoje kibernetinio saugumo lygį ir gerinti vidaus rinkos veikimą.*

3. *Vertinime taip pat vertinama:*

   a) *procedūrų, pagal kurias konsultuojamasi dėl Europos kibernetinio saugumo sertifikavimo schemų, jos rengiamos ir priimamos, veiksmingumas ir efektyvumas, taip pat būdai, kaip tas procedūras patobulinti ir paspartinti;*

   b) *ar prieigai prie vidaus rinkos taikomi esminiai kibernetinio saugumo reikalavimai yra būtini siekiant, kad į Sąjungos rinką nepatektų IRT produktai, IRT paslaugos, IRT procesai ir valdomos saugumo paslaugos, kurie neatitinka pagrindinių kibernetinio saugumo reikalavimų.*

4. *Ne vėliau kaip 2024 m. birželio 28 d., o vėliau kas trejus metus Komisija vertinimo ataskaitą kartu su savo išvadomis perduoda Europos Parlamentui, Tarybai ir valdančiajai tarybai. Tos ataskaitos išvados skelbiamos viešai.“*

2 straipsnis

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo Europos Sąjungos oficialiajame leidinyje.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta ...

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas / Pirmininkė*