Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/37

2025 1 15

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (ES) 2025/37

2024 m. gruodžio 19 d.

kuriuo iš dalies keičiamas Reglamentas (ES) 2019/881, kiek tai susiję su valdomomis saugumo paslaugomis

(Tekstas svarbus EEE)

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

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

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

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

pasikonsultavę su Regionų komitetu,

laikydamiesi įprastos teisėkūros procedūros ([2]),

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 ([3]) sukurta Europos kibernetinio saugumo sertifikavimo schemų nustatymo sistema;

(2) siekiant užtikrinti Sąjungos atsparumą kibernetinėms atakoms ir užkirsti kelią bet kokiam pažeidžiamumui vidaus rinkoje, šiuo reglamentu siekiama papildyti horizontaliąją reguliavimo sistemą, kuria pagal Europos Parlamento ir Tarybos reglamentą (ES) 2024/2847 ([4]) nustatomi išsamūs kibernetinio saugumo reikalavimai, keliami produktams su skaitmeniniais elementais, nustatant saugumo tikslus valdomoms saugumo paslaugoms bei tų paslaugų taikymui ir patikimumui;

(3) valdomas saugumo paslaugas teikia valdomų saugumo paslaugų teikėjai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2022/2555 ([5]) 6 straipsnio 40 punkte. Valdomų saugumo paslaugų apibrėžtis šiame reglamente turėtų derėti su valdomų saugumo paslaugų teikėjų apibrėžtimi Direktyvoje (ES) 2022/2555. Tas paslaugas sudaro su klientų kibernetinio saugumo rizikos valdymu susijusios veiklos vykdymas arba parama tokiai veiklai, ir jos tampa vis svarbesnės incidentų prevencijai ir jų poveikio mažinimui. Todėl tų paslaugų teikėjai pagal Direktyvą (ES) 2022/2555 laikomi esminiais arba svarbiais subjektais, priklausančiais itin svarbiam sektoriui. Kaip pažymima tos direktyvos 86 konstatuojamojoje dalyje, valdomų 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 atakų taikiniai ir dėl jų glaudžios integracijos į klientų veiklą kyla specifinė rizika. Todėl svarbu, kad esminiai ir svarbūs subjektai, kaip tai suprantama Direktyvoje (ES) 2022/2555, rinkdamiesi valdomų saugumo paslaugų teikėjus veiktų atidžiau;

([1]) OL C 349, 2023 9 29, p. 167.
([2]) 2024 m. balandžio 24 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2024 m. gruodžio 2 d. Tarybos sprendimas.
([3]) 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).
([4]) 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas) (OL L, 2024/2847, 2024 11 20, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
([5]) 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).

(4) į valdomų saugumo paslaugų apibrėžtį pagal šį reglamentą įtrauktas nebaigtinis valdomų saugumo paslaugų, kurioms galėtų būti taikomos Europos kibernetinio saugumo sertifikavimo schemos, tokių kaip incidentų valdymas, skverbimosi testavimas, saugumo auditai ir konsultacijos, susijusios su techninė parama, sąrašas. Valdomos saugumo paslaugos galėtų apimti kibernetinio saugumo paslaugas, kuriomis remiamas pasirengimas incidentams, jų prevencija, nustatymas, analizė, poveikio mažinimas, reagavimas į juos ir atsigavimas po jų. Žvalgybos informacijos apie kibernetines grėsmes teikimas ir su techninė parama susijęs rizikos vertinimas taip pat galėtų būti laikomi valdomomis saugumo paslaugomis. Galėtų būti skirtingos Europos kibernetinio saugumo sertifikavimo schemos, skirtos skirtingoms valdomoms saugumo paslaugoms. Pagal tokias schemas išduotuose Europos kibernetinio saugumo sertifikatuose turėtų būti nurodytos konkrečios konkretaus paslaugų teikėjo teikiamos valdomos saugumo paslaugos;

(5) valdomų saugumo paslaugų teikėjai taip pat gali atlikti svarbų vaidmenį vykdant Sąjungos veiksmus, kuriais remiamas reagavimas ir pirminis atsigavimas reikšmingų ir didelio masto kibernetinio saugumo incidentų atveju, pasikliaujant patikimų privačių paslaugų teikėjų paslaugomis ir ypatingos svarbos subjektų galimo pažeidžiamumo testavimu remiantis Sąjungos mastu koordinuojamais saugumo rizikos vertinimais. Tas valdomų saugumo paslaugų sertifikavimas gali būti svarbus atrenkant patikimus valdomų saugumo paslaugų teikėjus, kaip apibrėžta Europos Parlamento ir Tarybos reglamente (ES) 2025/38 ([6]);

(6) valdomų saugumo paslaugų sertifikavimas yra aktualus ne vien atrankos į ES kibernetinio saugumo rezervą, įsteigtą Reglamentu (ES) 2025/38, 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 tvarkomų duomenų pažeidžiamumą, sertifikavimas galėtų suteikti potencialiems klientams svarbių gairių ir garantijų dėl tų paslaugų patikimumo. Valdomų saugumo paslaugų Europos kibernetinio saugumo sertifikavimo schemomis siekiama padėti išvengti vidaus rinkos susiskaidymo. Taigi, šiuo reglamentu siekiama gerinti vidaus rinkos veikimą;

(7) valdomoms saugumo paslaugoms skirtos Europos kibernetinio saugumo sertifikavimo schemos turėtų paskatinti naudojimąsi tomis paslaugomis ir padidinti valdomų saugumo paslaugų teikėjų konkurenciją. Todėl, nedarant poveikio tikslui užtikrinti pakankamą ir tinkamą tokių paslaugų teikėjų atitinkamų techninių žinių ir profesinio sąžiningumo lygį, tokios sertifikavimo schemos turėtų sudaryti palankesnes sąlygas patekti į rinką ir siūlyti valdomas saugumo paslaugas, kuo labiau supaprastinant galimą reguliavimo, administracinę ir finansinę naštą, su kuria galėtų susidurti paslaugų teikėjai, visų mažosios ir vidutinės įmonės (MVĮ), įskaitant labai mažas įmones, siūlydami valdomas saugumo paslaugas. Be to, siekiant skatinti valdomų saugumo paslaugų naudojimą ir didinti jų paklausą, Europos kibernetinio saugumo schemos turėtų prisidėti prie jų prieinamumo, visų pirma mažesniems subjektams, pavyzdžiui, MVĮ, įskaitant labai mažas įmones, taip pat vietos ir regionų institucijoms, kurių pajėgumai ir ištekliai yra riboti, tačiau kurių atžvilgiu kibernetinio saugumo pažeidimų, dėl kurių patiriami finansiniai ir teisiniai padariniai bei pasekmės reputacijai ir veiklai, rizika yra didesnė;

(8) svarbu teikti paramą MVĮ, įskaitant labai mažas įmones, įgyvendinant šį reglamentą ir įdarbinant darbuotojus, turinčius specializuotų kibernetinio saugumo įgūdžių ir ekspertinių žinių, būtinų valdomoms saugumo paslaugoms teikti laikantis šiame reglamente nustatytų reikalavimų. Skaitmeninės Europos programoje, sukurtoje Europos Parlamento ir Tarybos reglamentu (ES) 2021/694 ([7]), ir kitose atitinkamose Sąjungos programose numatyta, kad Komisija turi nustatyti finansinę ir techninę paramą, kuri sudarytų sąlygas toms įmonėms prisidėti prie Sąjungos ekonomikos augimo ir bendro kibernetinio saugumo lygio stiprinimo Sąjungos aplinkoje, be kita ko, supaprastinant Skaitmeninės Europos programos ir kitų atitinkamų Sąjungos programų finansinės paramos procesą ir remiant MVĮ, įskaitant labai mažas įmones;

(9) valdomoms saugumo paslaugoms skirtos Europos kibernetinio saugumo sertifikavimo schemos turėtų padidinti galimybę naudotis saugiomis ir aukštos kokybės paslaugomis, kuriomis užtikrinama saugi skaitmeninė pertvarka ir siekiama 2030 m. Skaitmeninio dešimtmečio politikos programoje, sukurtoje Europos Parlamento ir Tarybos sprendimu (ES) 2022/2481 ([8]), nustatytų tikslų, visų pirma susijusių su tikslu, kad 75 % Sąjungos įmonių pradėtų naudotis debesijos kompiuterijos paslaugų, didžiųjų duomenų ar dirbtinio intelekto technologijomis, kad daugiau

([6]) 2024 m. gruodžio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2025/38, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Kibernetinio solidarumo aktas) (OL L, 2025/38, 2025 1 15, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) 2021 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/694, kuriuo nustatoma Skaitmeninės Europos programa ir panaikinamas Sprendimas (ES) 2015/2240 (OL L 166, 2021 5 11, p. 1).

([8]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos sprendimas (ES) 2022/2481, kuriuo nustatoma 2030 m. Skaitmeninio dešimtmečio politikos programa (OL L 323, 2022 12 19, p. 4).

kaip 90 % MVĮ, įskaitant labai mažas įmones, pasiektų bent bazinį skaitmeninio intensyvumo lygį ir kad pagrindinės viešosios paslaugos būtų prieinamos internetu;

(10) be IRT produktų, IRT paslaugų ar IRT procesų diegimo, valdomos saugumo paslaugos dažnai apima ir papildomas paslaugų funkcijas, kurios priklauso nuo tokių paslaugų teikėjų darbuotojų kompetencijos, ekspertinių žinių ir patirties. Siekiant užtikrinti labai aukštą teikiamų valdomų saugumo paslaugų kokybę, į saugumo tikslus turėtų būti įtrauktas labai aukštas tos kompetencijos, ekspertinių žinių bei patirties lygis ir atitinkamos vidaus procedūros. Todėl, siekiant užtikrinti, kad specialios Europos kibernetinio saugumo sertifikavimo schemos galėtų apimti visus valdomų saugumo paslaugų aspektus, būtina iš dalies pakeisti Reglamentą (ES) 2019/881. Reikėtų atsižvelgti į Reglamente (ES) 2019/881 numatyto vertinimo ir peržiūros rezultatus ir rekomendacijas;

(11) siekiant sudaryti palankesnes sąlygas patikimos vidaus rinkos augimui, kartu kuriant partnerystes su bendramintėmis trečiosiomis valstybėmis, Europos kibernetinio saugumo sertifikavimo sistemoje, numatytoje Reglamente (ES) 2019/881, nustatytas sertifikavimo procesas turėtų būti įgyvendinamas taip, kad būtų sudarytos palankesnės sąlygos tarptautiniam pripažinimui ir suderinimui su tarptautiniais standartais;

(12) Sąjunga susiduria su talentų trūkumu, nes trūksta kvalifikuotų specialistų, ir sparčiai kintančia grėsmių panorama, kaip pripažinta 2023 m. balandžio 18 d. Komisijos komunikate „Kibernetinio saugumo srities talentų trūkumo problemos sprendimas siekiant didinti ES konkurencingumą ir atsparumą bei skatinti jos augimą (Kibernetinio saugumo įgūdžių akademija)“. Švietimo ištekliai ir formaliųjų mokymų formos skiriasi, o žinios gali būti įgyjamos įvairiais būdais – formaliai, pvz., universitetuose ar kursuose, arba neformaliai, pvz., mokantis darbo vietoje arba kaupiant darbo patirtį atitinkamoje srityje. Todėl, siekiant sudaryti palankesnes sąlygas aukštos kokybės valdomų saugumo paslaugų atsiradimui ir geriau apžvelgti Sąjungos kibernetinio saugumo srities darbo jėgos sudėtį, svarbu stiprinti valstybių narių, Komisijos, Europos Sąjungos kibernetinio saugumo agentūros, įsteigtos Reglamentu (ES) 2019/881, (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. Toks bendradarbiavimas taip pat sudarytų 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 programose. Svarbu, kad tokiu bendradarbiavimu būtų siekiama į tą sritį pritraukti daugiau moterų ir mergaičių ir padėti mažinti lyčių nelygybę gamtos mokslų, technologijų, inžinerijos ir matematikos srityse ir kad privatusis sektorius siektų rengti mokymus darbo vietoje, kuriuose būtų atsižvelgiama į labiausiai paklausius įgūdžius, įtraukiant viešojo administravimo įstaigas ir startuolius, taip pat MVĮ, įskaitant labai mažas įmones. Taip pat svarbu, kad paslaugų teikėjai ir valstybės narės bendradarbiautų ir prisidėtų renkant duomenis apie kibernetinio saugumo darbo rinkos padėtį ir raidą;

(13) ENISA atlieka svarbų vaidmenį pasirengiant potencialioms Europos kibernetinio sertifikavimo schemoms. Rengdama Sąjungos bendrojo biudžeto projektą Komisija turėtų įvertinti ENISA etatų planui reikalingus biudžeto išteklius pagal Reglamento (ES) 2019/881 29 straipsnyje nustatytą procedūrą;

(14) šiuo reglamentu numatomi tiksliniai Reglamento (ES) 2019/881 daliniai pakeitimai, kad būtų galima sukurti valdomoms saugumo paslaugoms skirtas Europos kibernetinio saugumo sertifikavimo schemas. Šiuo reglamentu taip pat patikslinamos ir paaiškinamos tam tikros to reglamento nuostatos, susijusios su visų Europos kibernetinio saugumo sertifikavimo schemų rengimu ir veikimu, siekiant užtikrinti jų skaidrumą ir atvirumą. Pastarieji pakeitimai, susiję tik su Reglamento (ES) 2019/881 patikslinimu ar paaiškinimu, visų pirma pakeitimai dėl informacijos, kurią ENISA turi pateikti perduodama potencialią schemą, dėl kiekvienai potencialiai schemai įsteigtos *ad-hoc* darbo grupės ir konsultacijų dėl Europos kibernetinio sertifikavimo schemų, jokiu būdu neturėtų daryti poveikio platesniam to reglamento vertinimui ir peržiūrai, kurio reikalaujama pagal to reglamento 67 straipsnį, visų pirma to reglamento antraštinės dalies, susijusios su kibernetinio saugumo sertifikavimo schemomis, poveikio, veiksmingumo ir efektyvumo vertinimą. Tos antraštinės dalies vertinimas ir peržiūra turėtų būti grindžiami plačiomis konsultacijomis su suinteresuotaisiais subjektais ir išsamia bei nuodugnia susijusių procedūrų analize;

(15) kadangi šio reglamento tikslo, t. y. kad būtų galima sukurti valdomoms saugumo paslaugoms skirtas Europos kibernetinio saugumo sertifikavimo schemas, valstybės narės negali deramai pasiekti, o dėl jo masto arba poveikio to tikslo geriau siekti Sąjungos lygmeniu, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šiuo reglamentu neviršijama to, kas būtina nurodytam tikslui pasiekti;

(16) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([9]) 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę 2024 m. sausio 10 d.,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Reglamento (ES) 2019/881 daliniai 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 vidaus 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 konkretiems IRT produktams, IRT paslaugoms, IRT procesams ar valdomoms saugumo paslaugoms sertifikuoti arba atitikčiai vertinti, rinkinys;

10) nacionalinė kibernetinio saugumo sertifikavimo schema – išsamus taisyklių, techninių reikalavimų, standartų ir procedūrų, kuriuos parengė ir priėmė nacionalinė valdžios institucija, rinkinys, taikomas IRT produktams, IRT paslaugoms, IRT procesams ar valdomoms saugumo paslaugoms, kuriems taikoma ta konkreti schema, sertifikuoti arba atitikčiai vertinti;

11) Europos kibernetinio saugumo sertifikatas – atitinkamos įstaigos išduotas dokumentas, 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, kurią sudaro su kibernetinio saugumo rizikos valdymu susijusios veiklos, tokios kaip incidentų valdymas, skverbimosi testavimas, saugumo auditai ir konsultacijos, įskaitant ekspertų rekomendacijas, susijusias su technine parama, vykdymas arba pagalba tokiai veiklai;“;

c) 20, 21 ir 22 punktai pakeičiami taip:

„20) techninė specifikacija – 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;

([9]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

21) saugumo užtikrinimo lygis – pagrindas pasitikėti, kad IRT produktas, IRT paslauga, IRT procesas ar valdoma saugumo paslauga atitinka konkrečios Europos kibernetinio saugumo sertifikavimo schemos saugumo reikalavimus; juo nurodoma, kokiu lygiu IRT produktas, IRT paslauga, IRT procesas ar valdoma saugumo paslauga yra įvertinti, tačiau juo pačiu nenurodomas atitinkamo IRT produkto, IRT paslaugos, IRT proceso ar valdomos saugumo paslaugos saugumas;

22) savarankiškas atitikties vertinimas – IRT produktų gamintojo, IRT paslaugų, IRT procesų arba valdomų saugumo paslaugų teikėjo atliekamas veiksmas, kuriuo įvertinama, ar tie IRT produktai, IRT paslaugos, IRT procesai ar 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 nustatymo ir priežiūros pagal šio reglamento III antraštinę dalį, siekiant didinti IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų kibernetinio saugumo skaidrumą, taip sustiprinant pasitikėjimą skaitmenine vidaus rinka ir jos konkurencingumą.“;

4) 8 straipsnis iš dalies keičiamas taip:

a) 1 dalis iš dalies keičiama taip:

i) įžanginė formuluotė pakeičiama taip:

„1. ENISA remia ir skatina Sąjungos politikos IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų kibernetinio saugumo sertifikavimo srityje plėtojimą ir įgyvendinimą, kaip nustatyta šio reglamento III antraštinėje dalyje:“;

ii) b punktas pakeičiamas taip:

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

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 straipsnis pakeičiamas taip:

„*46 straipsnis*

Europos kibernetinio saugumo sertifikavimo sistema

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, ir patvirtinti, kad pagal tokias schemas įvertinti IRT produktai, IRT paslaugos ir IRT 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, ekspertines žinias ir patirtį turintys darbuotojai, kurie yra įgiję atitinkamų pakankamo ir tinkamo lygio techninių žinių ir laikosi profesinio sąžiningumo principų.“;

6) 47 straipsnis iš dalies keičiamas taip:

a) 2 dalis pakeičiama taip:

„2. Į tęstinę Sąjungos darbo programą visų pirma įtraukiamas IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų, arba jų kategorijų, kurie gali būti įtraukti į Europos kibernetinio saugumo sertifikavimo schemos taikymo sritį, sąrašas.“;

b) 3 dalis iš dalies keičiama taip:

i) įžanginė formuluotė pakeičiama taip:

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

ii) a punktas pakeičiamas taip:

„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;“;

iii) įterpiamas šis punktas:

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

7) 49 straipsnis iš dalies keičiamas taip:

a) 1–4 dalys pakeičiamos taip:

„1. Gavusi Komisijos prašymą pagal 48 straipsnį, ENISA parengia potencialią schemą, atitinkančią taikytinus 51, 51a, 52 ir 54 straipsniuose nustatytus reikalavimus.

2. Gavusi EKSSG prašymą pagal 48 straipsnio 2 dalį, ENISA gali parengti potencialią schemą, atitinkančią taikytinus 51, 51a, 52 ir 54 straipsniuose nustatytus reikalavimus. Jei ENISA atsisako vykdyti tokį prašymą, ji nurodo savo atsisakymo priežastis. Sprendimus dėl atsisakymo vykdyti tokį prašymą priima Valdančioji taryba.

3. Rengdama potencialią schemą, ENISA laiku konsultuojasi su visais atitinkamais suinteresuotaisiais subjektais, taikydama oficialią, atvirą, skaidrią ir įtraukią konsultacijų procedūrą. Pagal 6 dalį perduodama potencialią schemą Komisijai, ENISA pateikia informaciją apie tai, kaip ji įvykdė šios dalies reikalavimus.

4. Kiekvienos potencialios schemos atveju ENISA pagal 20 straipsnio 4 dalį įsteigia *ad hoc* darbo grupę, kad ENISA būtų teikiamos specialios rekomendacijos ir ekspertinės žinios. Į tas *ad hoc* darbo grupes prireikus ir nedarant poveikio 20 straipsnio 4 dalyje pateiktoms procedūroms ir diskrecijai įtraukiami valstybių narių viešojo administravimo institucijų, Sąjungos institucijų, organų, įstaigų ir agentūrų bei privačiojo sektoriaus ekspertai.“;

b) 7 dalis pakeičiama taip:

„7. Komisija, remdamasi ENISA parengta potencialia schema, gali priimti įgyvendinimo aktus, kuriuose būtų numatytos atitinkamus 51, 51a, 52 ir 54 straipsnių reikalavimus atitinkančios IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų Europos kibernetinio saugumo sertifikavimo schemos. Tie įgyvendinimo aktai priimami laikantis 66 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.“;

8) įterpiamas šis straipsnis:

„49a straipsnis

Informacija apie Europos kibernetinio saugumo schemas ir konsultavimasis dėl jų

1. Komisija viešai skelbia informaciją apie savo 48 straipsnyje nurodytą prašymą ENISA parengti potencialią schemą arba peržiūrėti esamą Europos kibernetinio saugumo sertifikavimo schemą.

2. ENISA rengiant potencialią schemą pagal 49 straipsnį, Europos Parlamentas, Taryba arba Europos Parlamentas ir Taryba gali prašyti Komisijos, kaip EKSSG pirmininkės, ir ENISA kas ketvirtį pateikti atitinkamą informaciją apie potencialios schemos projektą. Europos Parlamento arba Tarybos prašymu ENISA, susitarusi su Komisija ir nedarant poveikio 27 straipsniui, gali pateikti Europos Parlamentui ir Tarybai atitinkamas potencialios schemos projekto dalis tokiu būdu, kuris atitiktų reikalaujamą konfidencialumo lygį, ir, kai taikytina, su naudojimo apribojimais.

3. Siekiant stiprinti Sąjungos institucijų tarpusavio dialogą ir prisidėti prie oficialaus, atviro, skaidraus ir įtraukaus konsultacijų proceso, Europos Parlamentas, Taryba arba Europos Parlamentas ir Taryba gali paprašyti Komisijos ir ENISA aptarti klausimus, susijusius su IRT produktų, IRT paslaugų, IRT procesų ar valdomų saugumo paslaugų Europos kibernetinio saugumo sertifikavimo schemų veikimu.

4. Vertindama šį reglamentą pagal 67 straipsnį, Komisija, kai tinkama, atsižvelgia į elementus, išreikštus Europos Parlamento ir Tarybos nuomonėse šio straipsnio 3 dalyje nurodytais klausimais.“;

9) 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:“;

10) 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) valdomos saugumo paslaugos turi būti teikiamos turint reikiamą kompetenciją, ekspertines žinias ir patirtį, be kita ko, už tų paslaugų teikimą atsakingi darbuotojai turi turėti pakankamo ir tinkamo lygio techninių žinių ir gebėjimų toje konkrečioje srityje bei pakankamos ir tinkamos patirties ir laikytis aukščiausių profesinio sąžiningumo standartų;

b) paslaugų teikėjas turi taikyti tinkamas vidaus procedūras, siekiant užtikrinti, kad valdomos saugumo paslaugos visada būtų pakankamos ir tinkamos kokybės;

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

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

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

f) turi būti saugomas registras, kad būtų 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) turi būti užtikrintas IRT produktų, IRT paslaugų ir IRT procesų, naudojamų teikiant valdomas saugumo paslaugas, standartizuotasis ir integruotasis saugumas ir, kai taikytina, naujausių saugumo naujinių įdiegimas, taip pat neturi būti viešai žinomų pažeidžiamumo spragų.“;

11) 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 ar 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 incidentų ir kibernetinių atakų rizika. Atliktini įvertinimo veiksmai turi apimti bent techninių dokumentų peržiūrą. Jei 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 ar 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 incidentų bei kibernetinių atakų, kuriuos vykdo ribotų įgūdžių ir ribotų išteklių turintys subjektai, rizika. Atliktini įvertinimo veiksmai turi apimti bent šiuos veiksmus: įvertinimą, ar nėra viešai žinomų pažeidžiamumo spragų, ir testavimą, 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 ar 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 naujausiomis technologijomis pagrįstų kibernetinių atakų, kurias 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; testavimą, ar IRT produktais, IRT paslaugomis, IRT procesais ar valdomomis saugumo paslaugomis tinkamai įgyvendinamos būtinos naujausiomis technologijomis pagrįstos saugumo funkcinės galimybės; ir, atliekant skverbimosi testavimą, jų atsparumo aukšto lygio įgūdžių turinčių subjektų išpuoliams įvertinimą. Jei tokie vertinimo veiksmai netaikytini, turi būti atlikti pakaitiniai lygiavertį poveikį turintys vertinimo veiksmai.“;

12) 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, IRT procesų arba valdomų saugumo paslaugų teikėjo atsakomybe. Savarankiškas atitikties vertinimas taikytinas tik tiems IRT produktams, IRT paslaugoms, IRT procesams ar valdomoms saugumo paslaugoms, kurie kelia nedidelę riziką, atitinkančią bazinį saugumo užtikrinimo lygį.

2. IRT produktų gamintojas, IRT paslaugų, IRT procesų ar 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, IRT procesų ar valdomų saugumo paslaugų teikėjas prisiima atsakomybę už IRT produkto, IRT paslaugos, IRT proceso ar valdomos saugumo paslaugos atitiktį toje schemoje nurodytiems reikalavimams.

3. IRT produktų gamintojas, IRT paslaugų, IRT procesų ar 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, IRT procesų ar valdomų saugumo paslaugų atitiktimi tai schemai, kad galėtų juos pateikti pagal 58 straipsnį paskirtai nacionalinei kibernetinio saugumo sertifikavimo institucijai. ES atitikties pareiškimo kopija pateikiama nacionalinei kibernetinio saugumo sertifikavimo institucijai ir ENISA.“;

13) 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) g punktas pakeičiamas taip:

„g) naudojami specifiniai vertinimo kriterijai ir metodai, įskaitant vertinimo rūšis, siekiant įrodyti, kad yra pasiekti 51 ir 51a straipsniuose nurodyti taikytini saugumo tikslai;“;

c) j punktas pakeičiamas taip:

„j) IRT produktų, IRT paslaugų, IRT procesų ar 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;“;

d) l punktas pakeičiamas taip:

„l) taisyklės, susijusios su padariniais IRT produktams, IRT paslaugoms, IRT procesams ar valdomoms saugumo paslaugoms, kurie buvo sertifikuoti arba kuriems išduotas ES atitikties pareiškimas, tačiau kurie neatitinka schemos reikalavimų;“;

e) 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 ar valdomoms saugumo paslaugoms, saugumo reikalavimus, vertinimo kriterijus bei metodus ir saugumo užtikrinimo lygius;“;

f) 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, IRT procesų ar valdomų saugumo paslaugų teikėjas turi galėti pateikti susipažinti;“;

14) 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 tokios 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, o nuo 2025 m. vasario 4 d. – 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:

— a punktas pakeičiamas taip:

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

— 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, IRT procesų ar valdomų saugumo paslaugų teikėjams, įskaitant konkrečius MVĮ, įskaitant labai mažas įmones, interesus ir poreikius;“;

c) 7 ir 8 dalys pakeičiamos taip:

„7. IRT produktus, IRT paslaugas, IRT procesus ar valdomas saugumo paslaugas sertifikuoti teikiantis fizinis arba juridinis asmuo pagal 58 straipsnį paskirtai nacionalinei kibernetinio saugumo sertifikavimo institucijai, kai ta 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 valdoma saugumo paslauga 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.“;

15) 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 įgyvendinimo 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, skirtų IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms, kuriems jau taikoma galiojanti Europos kibernetinio saugumo sertifikavimo schema.“;

16) 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 taisyklės dėl IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų atitikties sertifikatų, kurie buvo išduoti jų atitinkamose teritorijose, reikalavimams stebėsenos, ir užtikrina jų įgyvendinimą;

b) stebi, kaip jų atitinkamose teritorijose įsisteigę ir savarankišką atitikties vertinimą atliekantys IRT produktų gamintojai, IRT paslaugų, IRT procesų ar 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 ar 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 keisdamosi informacija, patirtimi ir geriausios praktikos pavyzdžiais, susijusiais su kibernetinio saugumo sertifikavimu ir IRT produktų, IRT paslaugų, IRT procesų ir valdomų saugumo paslaugų kibernetinio saugumo techniniais klausimais.“;

17) 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, IRT procesų ar valdomų saugumo paslaugų teikėjų pareigos, ir užtikrinti jų vykdymą pagal 58 straipsnio 7 dalies b punktą;“;

18) 67 straipsnio 2 ir 3 dalys pakeičiamos taip:

„2. Taip pat įvertinamas šio reglamento III antraštinės dalies nuostatų, be kita ko, procedūrų, po kurių patvirtinamos Europos kibernetinio saugumo sertifikavimo schemos, ir jų įrodymų bazių 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. Įvertinama, ar prieigai prie vidaus rinkos taikomi esminiai kibernetinio saugumo reikalavimai yra būtini siekiant užkirsti kelią IRT produktams, IRT paslaugoms, IRT procesams ir valdomoms saugumo paslaugoms, kurie neatitinka pagrindinių kibernetinio saugumo reikalavimų, patekti į vidaus rinką.“;

19) priedas iš dalies keičiamas pagal šio reglamento priedą.

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 Briuselyje 2024 m. gruodžio 19 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas*
R. METSOLA	BÓKA J.

PRIEDAS

Reglamento (ES) 2019/881 priedas iš dalies keičiamas taip:

1) 2–5 punktai pakeičiami taip:

„2. Atitikties vertinimo įstaiga yra trečioji šalis, nepriklausoma nuo vertinamos organizacijos ar vertinamų IRT produktų, IRT paslaugų, IRT procesų ar valdomų saugumo paslaugų.

3. Įstaiga, priklausanti verslo asociacijai arba profesinei federacijai, atstovaujančiai įmonėms, susijusioms su jos vertinamų IRT produktų, IRT paslaugų, IRT procesų ar valdomų saugumo paslaugų projektavimu, gamyba, tiekimu, surinkimu, naudojimu ar priežiūra, gali būti laikoma atitikties vertinimo įstaiga, jeigu įrodoma, kad ji yra nepriklausoma ir nėra jokio interesų konflikto.

4. Atitikties vertinimo įstaigos, jų vyresnioji vadovybė ir už atitikties vertinimo užduočių atlikimą atsakingi darbuotojai negali būti nei vertinamo IRT produkto, IRT paslaugos, IRT proceso ar valdomos saugumo paslaugos projektuotojai, gamintojai, tiekėjai, montuotojai, pirkėjai, savininkai, naudotojai ar priežiūros teikėjai, nei tų šalių įgaliotieji atstovai. Šis draudimas netrukdo atitikties vertinimo įstaigai naudoti vertinamų IRT produktų, kurie yra būtini jos veiklai, arba tokius IRT produktus naudoti asmeniniais tikslais.

5. Atitikties vertinimo įstaigos, jų vyresnioji vadovybė ir už atitikties vertinimo užduočių atlikimą atsakingi darbuotojai tiesiogiai nedalyvauja projektuojant, gaminant ar konstruojant, tiekiant, parduodant, įrengiant, naudojant arba prižiūrint tuos vertinamus IRT produktus, IRT paslaugas, IRT procesus ar valdomas saugumo paslaugas, taip pat negali atstovauti toje veikloje dalyvaujančioms šalims. Atitikties vertinimo įstaigos, jų vyresnioji vadovybė ir už atitikties vertinimo užduočių atlikimą atsakingi darbuotojai nesiima jokios veiklos, kuri jiems galėtų trukdyti nepriklausomai ir sąžiningai priimti sprendimus, susijusius su atitikties vertinimo veikla. Šis draudimas visų pirma taikomas konsultavimo paslaugoms.“;

2) 10 punktas iš dalies keičiamas taip:

a) įžanginė formuluotė pakeičiama taip:

„10. Visais atvejais kiekvienai atitikties vertinimo procedūrai vykdyti ir kiekvienos rūšies, kategorijos ar pakategorės IRT produktams, IRT paslaugoms, IRT procesams ar valdomoms saugumo paslaugoms atitikties vertinimo įstaiga turi turėti reikiamus (-as):“;

b) c punktas pakeičiamas taip:

„c) procedūras, pagal kurias ji galėtų vykdyti savo veiklą tinkamai atsižvelgdama į įmonės dydį, jos veiklos sektorių ir struktūrą, atitinkamo IRT produkto, IRT paslaugos, IRT proceso ar valdomos saugumo paslaugos technologijos sudėtingumo lygį ir į tai, ar gamybos procesas yra masinis, ar serijinis.“;

3) 19 ir 20 punktai pakeičiami taip:

„19. Atitikties vertinimo įstaigos atitinka reikalavimus pagal susijusį suderintą standartą, kaip apibrėžta Reglamento (EB) Nr. 765/2008 2 straipsnio 9 punkte, atitikties vertinimo įstaigų, vykdančių IRT produktų, IRT paslaugų, IRT procesų ar valdomų saugumo paslaugų sertifikavimą, akreditavimo tikslais.

20. Atitikties vertinimo įstaigos užtikrina, kad atitikties vertinimo tikslais naudojamos testavimo laboratorijos atitiktų reikalavimus pagal susijusį suderintą standartą, kaip apibrėžta Reglamento (EB) Nr. 765/2008 2 straipsnio 9 punkte, bandymus atliekančių laboratorijų akreditavimo tikslais.“

Dėl šio akto buvo padarytas pareiškimas; jį galima rasti OL C, C/2025/307, 2025 1 15, ELI: http://data.europa.eu/eli/C/2025/307/oj.