EUROPOS
KOMISIJA

Strasbūras, 2023 04 18
COM(2023) 208 final

2023/0108 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

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

(Tekstas svarbus EEE)

AIŠKINAMASIS MEMORANDUMAS

1. PASIŪLYMO APLINKYBĖS

• Pasiūlymo pagrindimas ir tikslai

Šis aiškinamasis memorandumas pridedamas prie pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo dėl valdomų saugumo paslaugų iš dalies keičiamas Reglamentas (ES) 2019/881[1].

Siūlomo tikslinio pakeitimo tikslas – sudaryti galimybę Komisijos įgyvendinimo aktais tvirtinti Europos kibernetinio saugumo sertifikavimo schemas, skirtas ne tik informacinių ir ryšių technologijų (IRT) produktams, IRT paslaugoms ir IRT procesams, kuriuos jau apima Kibernetinio saugumo aktas, bet ir valdomoms saugumo paslaugoms. Valdomų saugumo paslaugų vaidmuo tampa vis svarbesnis kibernetinio saugumo incidentų prevencijai ir jų poveikio mažinimui.

2022 m. gegužės 23 d. išvadose[2] dėl Europos Sąjungos pozicijos kibernetiniais klausimais parengimo Taryba paragino Sąjungą ir jos valstybes nares dėti daugiau pastangų siekiant padidinti bendrą kibernetinio saugumo lygį, pavyzdžiui, sudarant palankesnes sąlygas rastis patikimiems kibernetinio saugumo paslaugų teikėjams, ir pabrėžė, kad tokių paslaugų teikėjų plėtros skatinimas turėtų būti Sąjungos pramonės politikos kibernetinio saugumo srityje prioritetas. Ji taip pat paprašė Komisijos pasiūlyti galimybių skatinti patikimų kibernetinio saugumo paslaugų pramonės atsiradimą. Valdomų saugumo paslaugų sertifikavimas yra veiksmingas būdas stiprinti pasitikėjimą tų paslaugų kokybe, taip sudarant palankesnes sąlygas formuotis patikimų Europos kibernetinio saugumo paslaugų pramonei.

2022 m. lapkričio 10 d. priimtame Komisijos ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai bendrame komunikate „ES kibernetinės gynybos politika“[3] pranešta, kad Komisija išnagrinės galimybes parengti ES lygmens kibernetinio saugumo sertifikavimo schemas, taikytinas kibernetinio saugumo pramonei ir privačioms įmonėms. Valdomų saugumo paslaugų teikėjai taip pat atliks svarbų vaidmenį ES lygmens kibernetinio saugumo rezerve, kurio laipsniškas kūrimas remiamas Kibernetinio solidarumo aktu (kurio pasiūlymas pateiktas kartu su šio reglamento pasiūlymu). ES lygmens kibernetinio saugumo rezervu numatoma naudotis teikiant paramą reaguoti ir imtis neatidėliojamų atkuriamųjų veiksmų reikšmingų ir didelio masto kibernetinio saugumo incidentų atvejais. Atitinkamos kibernetinio saugumo paslaugos, kurias teikia patikimi paslaugų teikėjai, nurodyti Kibernetinio solidarumo akte, atitinka „valdomų saugumo paslaugų“ sampratą šiame pasiūlyme.

Kai kurios valstybės narės jau pradėjo diegti valdomų saugumo paslaugų sertifikavimo schemas. Dėl įvairių Sąjungoje taikomų kibernetinio saugumo sertifikavimo schemų nesuderinamumo didėja valdomų saugumo paslaugų vidaus rinkos susiskaidymo rizika. Siekiant išvengti tokio susiskaidymo, šiuo pasiūlymu atveriama galimybė kurti Europos kibernetinio saugumo sertifikavimo schemas, skirtas toms paslaugoms.

---

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 151/15, 2019 6 7.

2 9364/22.

3 JOIN(2022) 49 *final*.

- **Suderinamumas su toje pačioje politikos srityje galiojančiomis nuostatomis**

Šis pasiūlymas dera su Kibernetinio saugumo aktu, kuris šiuo pasiūlymu iš dalies keičiamas. Pasiūlyme remiamasi to reglamento nuostatomis ir jos atitinkamai pritaikomos, kad apimtų ir valdomas saugumo paslaugas. Siūlomi tik būtini pakeitimai, kuriais nekeičiama Kibernetinio saugumo akto esmė ar veikimas.

Šis pasiūlymas taip pat dera su 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)[4]. Valdomų saugumo paslaugų teikėjai yra pagal Direktyvą (ES) 2022/2555 laikomi esminiais arba svarbiais subjektais, priklausančiais itin svarbiam sektoriui. Tos direktyvos 86 konstatuojamojoje dalyje pažymima, kad valdomų saugumo paslaugų teikėjai tokiose srityse, kaip reagavimas į incidentus, skverbimosi testavimas, saugumo auditai ir konsultacijos, atlieka itin svarbų vaidmenį padėdami subjektams užkirsti kelią incidentams, juos atskleisti, į juos reaguoti ar atstatyti po jų 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.

Šiuo pasiūlymu siekiama pagerinti valdomų saugumo paslaugų kokybę ir padidinti jų palyginamumą. Taigi, esminiams ir svarbiems subjektams jis teikia galimybę atidžiau rinktis valdomų saugumo paslaugų teikėją, kaip reikalaujama Direktyvoje (ES) 2022/2555. Be to, valdomų saugumo paslaugų apibrėžtis šiame pasiūlyme yra pagrįsta labai panašia valdomų saugumo paslaugų teikėjų apibrėžtimi Direktyvoje (ES) 2022/2555. Todėl šis pasiūlymas reikšmingai papildo TIS 2 direktyvą.

Galiausiai, šis pasiūlymas papildo ir siūlomą Kibernetinio solidarumo aktą. Siūlomu Kibernetinio solidarumo aktu nustatomas paslaugų teikėjų atrankos į ES lygmens kibernetinio saugumo rezervą procesas, kurį atliekant turėtų būti, *inter alia*, atsižvelgiama į tai, ar tie paslaugų teikėjai yra įgiję Europos arba nacionalinį kibernetinio saugumo sertifikatą. Taigi būsimos valdomų saugumo paslaugų sertifikavimo schemų vaidmuo bus svarbus įgyvendinant Kibernetinio solidarumo aktą.

- **Suderinamumas su kitomis Sąjungos politikos sritimis**

Šis pasiūlymas nedaro poveikio Kibernetinio saugumo akto suderinamumui su Reglamentu (ES) 2016/679 (Bendrasis duomenų apsaugos reglamentas, BDAR)[5] ir jo nuostatomis dėl sertifikavimo mechanizmų ir duomenų apsaugos ženklų bei žymenų, skirtų duomenų valdytojų ir tvarkytojų atliekamų duomenų tvarkymo operacijų atitikčiai tam reglamentui įrodyti, nustatymo. Kibernetinio saugumo aktas ir toliau nedaro poveikio duomenų tvarkymo operacijų sertifikavimui (taip pat tais atvejais, kai tokios operacijos yra susietos su produktais ir paslaugomis) pagal BDAR.

Be to, šis pasiūlymas nedaro poveikio Kibernetinio saugumo akto suderinamumui su Reglamentu (EB) Nr. 765/2008 dėl akreditavimo ir rinkos priežiūros reikalavimų[6], visų pirma kiek tai susiję su nacionalinių akreditacijos įstaigų ir atitikties vertinimo įstaigų sistema bei nacionalinėmis sertifikavimo priežiūros institucijomis.

---

4 OL L 333/810, 2022 12 27.
5 OL L 119/1, 2016 5 4.
6 OL L 218/30, 2008 8 13.

2. TEISINIS PAGRINDAS, SUBSIDIARUMO IR PROPORCINGUMO PRINCIPAI

- **Teisinis pagrindas**

Šiuo pasiūlymu iš dalies keičiamas Kibernetinio saugumo aktas, kurio teisinis pagrindas yra Sutarties dėl Europos Sąjungos veikimo (SESV) 114 straipsnis. Šiuo pasiūlymu, kaip ir Kibernetinio saugumo aktu, siekiama išvengti vidaus rinkos susiskaidymo ir tuo tikslu suteikiama galimybė tvirtinti Europos kibernetinio saugumo sertifikavimo schemas, skirtas valdomoms saugumo paslaugoms. Valstybės narės jau yra pradėjusios diegti nacionalines valdomų saugumo paslaugų sertifikavimo schemas. Taigi, yra konkreti šių paslaugų vidaus rinkos susiskaidymo rizika, o šiuo pasiūlymu siekiama ją pašalinti. Todėl SESV 114 straipsnis yra tinkamas šios iniciatyvos teisinis pagrindas.

- **Subsidiarumo principas (neišimtinės kompetencijos atveju)**

Tikslo, kad būtų galima tvirtinti Europos kibernetinio saugumo sertifikavimo schemas saugumo valdymo srityje, ir vidaus rinkos susiskaidymo prevencijos tikslo neįmanoma pasiekti nacionaliniu lygmeniu – tai gali būti pasiekta tik Sąjungos lygmeniu. Be to, valdomų saugumo paslaugų, kurios yra siūlomo pakeitimo dalykas, teikėjai ir didžiausi potencialūs jų klientai veikia Sąjungos mastu. Todėl reikia imtis veiksmų Sąjungos lygmeniu ir jie būtų efektyvesni už nacionalinio lygmens veiksmus.

- **Proporcingumo principas**

Šiuo pasiūlymu nustatomas Kibernetinio saugumo akto tikslinis pakeitimas. Juo neviršijama to, kas būtina jo tikslui – suteikti galimybę tvirtinti ne tik IRT produktams, IRT paslaugoms ir IRT procesams, bet ir valdomoms saugumo paslaugoms skirtas Europos kibernetinio saugumo sertifikavimo schemas – pasiekti. Siūlomais pakeitimais visų pirma pritaikoma Europos kibernetinio saugumo sertifikavimo sistemos apimtis, į ją įtraukiant valdomas saugumo paslaugas, pateikiama tų paslaugų apibrėžtis, paremta jų samprata TIS 2 direktyvoje, ir su saugumu susiję Europos kibernetinio saugumo sertifikavimo tikslai iš dalies pakeičiami juos pritaikant prie valdomų saugumo paslaugų. Visi kiti pakeitimai yra techninio pobūdžio, jais siekiama užtikrinti, kad atitinkami straipsniai būtų taikomi ir valdomoms saugumo paslaugoms. Taigi, siūloma iniciatyva yra proporcinga tikslui.

- **Priemonės pasirinkimas**

Šiuo pasiūlymu iš dalies keičiamas Reglamentas (ES) 2019/881, todėl tinkama teisinė priemonė yra reglamentas.

3. *EX POST* VERTINIMO, KONSULTACIJŲ SU SUINTERESUOTOSIOMIS ŠALIMIS IR POVEIKIO VERTINIMO REZULTATAI

- **Galiojančių teisės aktų *ex post* vertinimas / tinkamumo patikrinimas**

Netaikoma.

- **Konsultacijos su suinteresuotosiomis šalimis**

Surengtos tikslinės konsultacijos su valstybėmis narėmis ir ENISA. Šiose konsultacijose valstybės narės apibūdino dabartinę su valdomų saugumo paslaugų sertifikavimu susijusią savo veiklą ir požiūrį į tai. ENISA paaiškino savo požiūrį ir savo diskusijų su valstybėmis narėmis ir suinteresuotosiomis šalimis išvadas. Iš valstybių narių ir ENISA gautomis pastabomis ir informacija remtasi rengiant šį pasiūlymą.

- **Tiriamųjų duomenų rinkimas ir naudojimas**

Netaikoma.

- **Poveikio vertinimas**

Buvo paprašyta, kad poveikio vertinimo nereikėtų atlikti, nes šis pasiūlymas yra dėl Kibernetinio saugumo akto labai siauro ir tikslinio pobūdžio pakeitimo. Šiuo pakeitimu būtų suteikta galimybė Komisijai įgyvendinimo aktais tvirtinti ne tik IRT produktams, paslaugoms ir procesams, kuriuos jau apima Kibernetinio saugumo aktas, bet ir valdomoms saugumo paslaugoms skirtas sertifikavimo schemas. Tačiau šis pakeitimas turėtų poveikį tik vėliau, kai tokios sertifikavimo schemos būtų patvirtintos. Be to, šiuo pakeitimu nebūtų pakeistas savanoriškas sertifikavimo schemų pobūdis.

- **Reglamentavimo tinkamumas ir supaprastinimas**

Netaikoma.

- **Pagrindinės teisės**

Pasiūlymas neturi jokio numatomo poveikio pagrindinių teisių apsaugai.

4. POVEIKIS BIUDŽETUI

Nėra.

5. KITI ELEMENTAI

- **Įgyvendinimo planai ir stebėsena, vertinimas ir ataskaitų teikimo tvarka**

Nuostatos, kurias numatoma iš dalies pakeisti šiuo pasiūlymu, bus Komisijos įvertintos atliekant Kibernetinio saugumo akto periodinį vertinimą pagal jo 67 straipsnį. To vertinimo metu įvertinama, *inter alia*, nuostatų dėl kibernetinio saugumo sertifikavimo sistemos poveikis, veiksmingumas ir efektyvumas siekiant tikslų užtikrinti tinkamą IRT produktų, paslaugų ir procesų Sąjungoje kibernetinio saugumo lygį ir gerinti vidaus rinkos veikimą. Šiame pasiūlyme numatytas pakeitimas, kuriuo užtikrinama, kad tas vertinimas apimtų ir valdomas saugumo paslaugas. Komisija taip pat nusiunčia Europos Parlamentui, Tarybai ir ENISA valdančiajai tarybai to vertinimo ataskaitą su savo išvadomis ir paskelbia tos ataskaitos išvadas viešai.

- **Išsamus konkrečių pasiūlymo nuostatų paaiškinimas**

Pasiūlymą sudaro du straipsniai. 1 straipsnyje išdėstyti Reglamento (ES) 2019/881 pakeitimai, o 2 straipsnyje pateiktos nuostatos dėl įsigaliojimo. 1 straipsnyje išdėstyti tiksliniai pakeitimai, kuriais iš dalies keičiama Kibernetinio saugumo akte numatytos Europos kibernetinio saugumo sertifikavimo sistemos apimtis, į ją įtraukiant valdomas saugumo paslaugas (Kibernetinio saugumo akto 1 ir 46 straipsniai). Jame pateikiama tų paslaugų apibrėžtis, labai artima valdomų saugumo paslaugų teikėjų apibrėžčiai TIS 2 direktyvoje (Kibernetinio saugumo akto 2 straipsnis). Juo taip pat pridedamas naujas 51a straipsnis dėl valdomoms saugumo paslaugoms pritaikytų saugumo tikslų, kurių siekiama Europos kibernetinio saugumo sertifikavimu. Galiausiai pasiūlyme pateikti keli techninio pobūdžio

pakeitimai siekiant užtikrinti, kad atitinkami straipsniai būtų taikomi ir valdomoms saugumo paslaugoms.

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,

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę,

atsižvelgdami į Regionų komiteto nuomonę,

laikydamiesi įprastos teisėkūros procedūros,

kadangi:

(1) siekiant užtikrinti tinkamą 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[7] sukurta Europos kibernetinio saugumo sertifikavimo schemų kūrimo sistema;

(2) valdomos saugumo paslaugos, t. y. paslaugos, apimančios su klientų kibernetinio saugumo rizikos valdymu susijusios veiklos vykdymą arba paramą tokiai veiklai, tampa vis svarbesnės kibernetinio saugumo incidentų prevencijai ir jų poveikio mažinimui. Todėl tų paslaugų teikėjai pagal Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555[8] 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 išpuolių taikiniai ir dėl jų glaudžios integracijos į klientų veiklą kyla specifinė rizika.

---

[7] 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).

[8] 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).

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 priemonės siekiant stiprinti solidarumą ir pajėgumą Sąjungoje atskleisti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti]. ES kibernetinio saugumo rezervą numatoma naudoti teikiant paramą reaguoti ir imtis neatidėliojamų atkuriamųjų veiksmų reikšmingų ir didelio masto kibernetinio saugumo incidentų atvejais. Reglamentu (ES) …/… [kuriuo nustatomos priemonės siekiant stiprinti solidarumą ir pajėgumą Sąjungoje atskleisti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti] 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 priemonės siekiant stiprinti solidarumą ir pajėgumą Sąjungoje atskleisti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti], 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;

(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 sertifikavimo schema galėtų apimti visus valdomos saugumo paslaugos aspektus, būtina iš dalies pakeisti Reglamentą (ES) 2019/881;

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,

PRIĖMĖ ŠĮ REGLAMENTĄ:

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 – paslauga, apimanti su kibernetinio saugumo rizikos valdymu susijusios veiklos (įskaitant reagavimą į incidentus, skverbimosi testavimą, saugumo auditus ir konsultacijas) vykdymą arba paramą tokiai veiklai;“;

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 techninės 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.

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;

d) kibernetinių grėsmių raidos pokyčiais;

e) EKSSG prašymu parengti konkrečią potencialią schemą.“;

7) 49 straipsnio 7 dalis pakeičiama taip:

„7. Komisija, remdamasi ENISA pasiūlyta potencialia schema, gali priimti įgyvendinimo aktus, kuriuose būtų numatytos 51, 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 pagal 66 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.“;

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 [bei aparatinės įrangos], naudojamų teikiant valdomas saugumo paslaugas, standartizuotasis ir

integruotasis saugumas, 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 MVĮ;“;

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 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 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;“;

17) 67 straipsnio 2 ir 3 dalys pakeičiamos taip:

„2. Taip pat įvertinamas 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. 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 Sąjungos rinką.“

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 Strasbūre

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