Europos Sąjungos
Taryba

Briuselis, 2018 m. gegužės 29 d.
(OR. en)

9350/18

Tarpinstitucinė byla:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

PRANEŠIMAS

nuo:	Pirmininkaujančios valstybės narės
kam:	Tarybai
Ankstesnio dokumento Nr.:	8834/18
Komisijos dok. Nr.:	12183/17
Dalykas:	Pasiūlymas dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO dėl ES kibernetinio saugumo agentūros ENISA ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) - Bendras požiūris

I. ĮVADAS

1. 2017 m. rugsėjo 13 d. Komisija, vadovaudamasi savo bendrosios skaitmeninės rinkos strategija, priėmė ir perdavė Tarybai ir Europos Parlamentui pirmiau nurodytą pasiūlymą [1], kurio teisinė bazė – SESV 114 straipsnis. Šiuo pasiūlymu, kuris yra vadinamojo „kibernetinio saugumo dokumentų rinkinio dalis“, siekiama aukšto kibernetinio saugumo lygio, kibernetinio atsparumo ir pasitikėjimo Sąjungoje, kad būtų užtikrintas tinkamas vidaus rinkos veikimas.

2. Siūlomu reglamentu nustatomi ENISA – ES kibernetinio saugumo agentūros – tikslai, užduotys ir organizaciniai aspektai ir nustatoma Europos kibernetinio saugumo sertifikavimo schemų sistema, siekiant užtikrinti tinkamą IRT produktų ir paslaugų kibernetinio saugumo lygį Sąjungoje. Prie Komisijos pasiūlymo pridedamas poveikio vertinimas, kuriame nagrinėjamos aštuonios konkrečios politikos galimybės, apimančios ENISA peržiūrą ir IRT kibernetinio saugumo sertifikavimą.

3. Siūlomame reglamente galima išskirti du pagrindinius elementus:

   - nuolatinių apibrėžtos apimties įgaliojimų suteikimą Agentūrai, atsižvelgiant į poreikius, kylančius dėl naujų politikos prioritetų bei priemonių, ir atnaujintų užduočių ir funkcijų priskyrimą Agentūrai, kad būtų galima veiksmingai ir efektyviai remti valstybių narių, ES institucijų ir kitų suinteresuotųjų subjektų pastangas užtikrinti saugią kibernetinę erdvę;

   - IRT produktams ir paslaugoms skirta Europos kibernetinio saugumo sertifikavimo sistema ir Europos kibernetinio saugumo sertifikavimo schemas reglamentuojančios taisyklės, kurios suteikia galimybę pagal tas schemas išduotus sertifikatus laikyti galiojančiais ir pripažinti visose valstybėse narėse ir kurios padeda spręsti dabartinio rinkos susiskaidymo problemą.

[1] Dok. 12183/17; 12183/1/17 REV 1; 12183/2/17 REV 2.

4. 2017 m. spalio mėn. Europos Vadovų Taryba [2] paragino Komisijos pasiūlymus dėl kibernetinio saugumo rengti laikantis holistinio požiūrio, pateikti laiku ir nedelsiant nagrinėti remiantis veiksmų planu, kurį turės parengti Taryba.

5. 2017 m. gruodžio 12 d. Bendrųjų reikalų taryba priėmė Veiksmų planą [3] Tarybos išvadoms [4] dėl bendro komunikato [5] Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“ įgyvendinti. Veiksmų planas atspindėjo Tarybos užmojį iki 2018 m. birželio mėn. susitarti dėl bendro požiūrio.

6. Europos Parlamente pranešėja paskirta Angelika NIEBLER (ITRE komitetas, EPP). Suplanuota, kad ITRE komitetas dėl pranešimo balsuos 2018 m. birželio 19 d.

7. Europos ekonomikos ir socialinių reikalų komitetas nuomonę priėmė 2018 m. vasario 14 d.

II. DARBAS TARYBOJE

8. 2017 m. rugsėjo 26 d. Komisija šį pasiūlymą ir jo poveikio vertinimą pateikė Kibernetinių klausimų horizontaliajai darbo grupei (toliau – darbo grupė), o darbo grupė poveikio vertinimą nagrinėjo 2017 m. spalio 20 d. Tolesnėse diskusijose pagrindinės temos buvo Agentūros operacinis pajėgumas, sąveikos su nacionalinėmis kompetentingomis institucijomis apimtis ir sertifikavimo sistemos poveikis rinkai ir verslo konkurencingumui. Apskritai delegacijos teigiamai įvertino tiek poveikio vertinimą, tiek pasiūlymą.

---

[2] EUCO 14/17, 11 punktas.
[3] Dok. 15748/17.
[4] Dok. 14435/17.
[5] Dok. 12211/17.

9. Diskusijos dėl paties pasiūlymo darbo grupėje prasidėjo 2017 m. lapkričio mėn., pirmininkaujant Estijai, ir buvo tęsiamos pirmininkaujant Bulgarijai. Dėl šio pasiūlymo surengta 12 posėdžių, po kurių iš eilės parengtos aštuonios patikslintos pasiūlymo redakcijos, siekiant susitarti dėl bendro požiūrio būsimame TTE (telekomunikacijos) tarybos posėdyje, kurį numatoma surengti 2018 m. birželio 8 d.

10. Šio pranešimo priede pateikiami 2018 m. gegužės 14–15 d. darbo grupėje vykusių diskusijų rezultatai ir patikslintas pirmininkaujančios valstybės narės kompromisinis tekstas. Konstatuojamosios dalys buvo patikslintos, kad atspindėtų esminių nuostatų pakeitimus. Visi Komisijos pasiūlymo pakeitimai pažymėti **paryškintuoju šriftu** arba ženklu […]. Pakeitimai, palyginti su naujausiu darbo grupės dokumentu 8834/18, pažymėti **paryškintuoju šriftu ir pabraukti**, o visas išbrauktas tekstas pažymėtas ženklu **[…]**.

III. IŠVADA

11. Priede pateikiamas pirmininkaujančios valstybės narės kompromisinis tekstas atspindi pirmininkaujančios valstybės narės ir valstybių narių pastangas užtikrinti tekste tinkamą pusiausvyrą.

12. 2018 m. gegužės 25 d. Nuolatinių atstovų komitetas susitarė dėl priede pateikiamo pirmininkaujančios valstybės narės kompromisinio teksto su sąlyga, kad bus pakeista 19 straipsnio 5 dalis ir 48 straipsnio 5 dalis.

13. Todėl Tarybos prašoma 2018 m. birželio 8 d. posėdyje priimti bendrą požiūrį ir suteikti įgaliojimus pirmininkaujančiai valstybei narei pradėti derybas su Europos Parlamento ir Europos Komisijos atstovais dėl šio dokumento.

PRIEDAS

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

dėl *[…] Europos Sąjungos kibernetinio saugumo agentūros* ENISA ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas)

(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 [6],

atsižvelgdami į Regionų komiteto nuomonę [7],

laikydamiesi įprastos teisėkūros procedūros,

[6] OL C , , p. .
[7] OL C , , p. .

kadangi:

(1) tinklų ir informacinės sistemos bei telekomunikacijų tinklai ir paslaugos atlieka visuomenei gyvybiškai svarbų vaidmenį ir yra ekonomikos augimo pamatas. Informacinėmis ir ryšių technologijomis grindžiamos sudėtingos sistemos, kurias taikant remiama visuomeninė veikla, užtikrinamas mūsų ekonomikos pagrindinių sektorių, kaip antai sveikatos, energetikos, finansų ir transporto, funkcionavimas ir visų pirma remiamas vidaus rinkos veikimas;

(2) tinklų ir informacines sistemas piliečiai, įmonės ir valdžios institucijos visoje Sąjungoje dabar naudoja labai plačiai. Skaitmeninimas ir ryšys tampa pagrindinėmis vis didesnės produktų ir paslaugų dalies savybėmis, ir numatoma, kad, įsitvirtinus daiktų internetui, per ateinantį dešimtmetį ES bus įdiegta milijonai, jei ne milijardai susietųjų skaitmeninių įrenginių. Nors prie interneto prijungiama vis daugiau įrenginių, juos projektuojant neužtikrinamas pakankamas saugumas ir atsparumas, dėl to jų kibernetinis saugumas yra nepakankamas. Šiomis aplinkybėmis dėl nepakankamo sertifikavimo organizacijos ir pavieniai vartotojai negauna pakankamai informacijos apie IRT produktų ir paslaugų kibernetinį saugumą, o tai mažina pasitikėjimą skaitmeniniais sprendimais;

(3) dėl išaugusio skaitmeninimo ir ryšio padidėjo kibernetinio saugumo rizika, todėl visuomenė yra labiau pažeidžiama dėl kibernetinių grėsmių ir padidėjo gyventojams, įskaitant pažeidžiamus asmenis, pvz., vaikus, kylantys pavojai. Siekiant sumažinti šią riziką visuomenei būtina imtis visų reikiamų veiksmų, kad ES būtų padidintas kibernetinis saugumas ir geriau nuo kibernetinių grėsmių apsaugotos tinklų ir informacinės sistemos, telekomunikacijų tinklai ir skaitmeniniai produktai, paslaugos ir įrenginiai, kuriais naudojasi piliečiai, valdžios institucijos ir įmonės – nuo MVĮ iki ypatingos svarbos infrastruktūros operatorių;

(4) kibernetinių išpuolių daugėja, todėl susietajai ekonomikai ir visuomenei, labiau pažeidžiamai dėl kibernetinių grėsmių ir išpuolių, reikalinga didesnė apsauga. Vis dėlto, nors kibernetiniai išpuoliai dažnai yra tarpvalstybinio pobūdžio, kibernetinio saugumo institucijų atsakomosios politikos priemonės ir teisėsaugos institucijų kompetencijos daugiausia yra nacionalinės. Didelio masto kibernetiniai incidentai gali sutrikdyti esminių paslaugų visoje ES teikimą. Todėl būtinas veiksmingas ES lygmens atsakas ir krizių valdymas, paremtas specializuota politika ir bendresnio pobūdžio Europos solidarumo ir savitarpio pagalbos priemonėmis. Be to, politikos formuotojams, sektoriaus atstovams ir naudotojams yra svarbu, kad reguliariai būtų vykdomas patikimais Sąjungos duomenimis grindžiamas kibernetinio saugumo ir atsparumo būklės Sąjungoje vertinimas ir sistemingai prognozuojami Sąjungos ir pasaulinio masto ateities pokyčiai, sunkumai ir grėsmės;

(5) atsižvelgiant į padidėjusius kibernetinio saugumo iššūkius, su kuriais susiduria Sąjunga, būtina parengti išsamų ankstesniais Sąjungos veiksmais grindžiamų priemonių, kuriomis remiami vienas kitą papildantys tikslai, rinkinį. Tam būtina dar labiau gerinti valstybių narių ir įmonių pajėgumus bei parengtį, taip pat gerinti valstybių narių ir ES institucijų, agentūrų ir įstaigų bendradarbiavimą ir koordinavimą. Be to, dėl tarpvalstybinio kibernetinių grėsmių pobūdžio būtina didinti Sąjungos lygmens pajėgumus, kurie galėtų papildyti valstybių narių veiksmus, visų pirma didelių tarpvalstybinių kibernetinių incidentų ir krizių atveju. Taip pat reikia dėti daugiau pastangų siekiant didinti piliečių ir įmonių informuotumą apie kibernetinio saugumo problemas. Be to, reikėtų dar labiau didinti pasitikėjimą skaitmenine bendrąja rinka teikiant skaidrią informaciją apie IRT produktų ir paslaugų saugumo lygį. To siekti galėtų padėti ES masto sertifikavimas, numatant bendrus kibernetinio saugumo reikalavimus ir vertinimo kriterijus visose nacionalinėse rinkose ir sektoriuose;

(6) 2004 m. Europos Parlamentas ir Taryba priėmė Reglamentą (EB) Nr. 460/2004 [8], įsteigiantį ENISA, siekdami prisidėti prie šių tikslų įgyvendinimo: užtikrinti aukštą Sąjungos tinklų ir informacijos saugumo lygį ir piliečių, vartotojų, įmonių ir viešojo sektoriaus organizacijų labui formuoti tinklų ir informacijos saugumo kultūrą. 2008 m. Europos Parlamentas ir Taryba priėmė Reglamentą (EB) Nr. 1007/2008 [9], kuriuo Agentūros įgaliojimai pratęsti iki 2012 m. kovo mėn. Reglamentu (EB) Nr. 580/2011 [10] agentūros įgaliojimai buvo dar pratęsti iki 2013 m. rugsėjo 13 d. 2013 m. Europos Parlamentas ir Taryba priėmė Reglamentą (ES) Nr. 526/2013 [11] dėl ENISA, kuriuo panaikintas Reglamentas (EB) Nr. 460/2004 ir kuriuo Agentūros įgaliojimai buvo pratęsti iki 2020 m. birželio mėn.;

---

[8] 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 460/2004, įsteigiantis Europos tinklų ir informacijos apsaugos agentūrą (OL L 77, 2004 3 13, p. 1).

[9] 2008 m. rugsėjo 24 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1007/2008, iš dalies keičiantis Reglamentą (EB) Nr. 460/2004, įsteigiantį Europos tinklų ir informacijos apsaugos agentūrą, jos veiklos trukmės atžvilgiu (OL L 293, 2008 10 31, p. 1).

[10] 2011 m. birželio 8 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 580/2011, kuriuo iš dalies keičiamas Reglamentas (EB) Nr. 460/2004, įsteigiantis Europos tinklų ir informacijos apsaugos agentūrą, jos veiklos trukmės atžvilgiu (OL L 165, 2011 6 24, p. 3).

[11] 2013 m. gegužės 21 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 526/2013 dėl Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA), kuriuo panaikinamas Reglamentas (EB) Nr. 460/2004 (OL L 165, 2013 6 18, p. 41).

(7) Sąjunga jau ėmėsi svarbių veiksmų siekdama užtikrinti kibernetinį saugumą ir padidinti pasitikėjimą skaitmeninėmis technologijomis. 2013 m. buvo priimta ES kibernetinio saugumo strategija siekiant Sąjungos politikos atsaką nukreipti į kibernetinio saugumo grėsmes ir riziką. Siekdama geriau apsaugoti europiečius internete 2016 m. Sąjunga priėmė pirmąjį teisėkūros procedūra priimamą kibernetinio saugumo srities aktą – Direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyvą). TIS direktyva buvo nustatyti reikalavimai, susiję su kibernetinio saugumo srities nacionaliniais pajėgumais, sukurti pirmieji mechanizmai, kuriais siekiama stiprinti strateginį ir operatyvinį valstybių narių bendradarbiavimą, ir nustatyti įpareigojimai, susiję su saugumo priemonėmis ir pranešimais apie incidentus ypatingo svarbos ekonomikai ir visuomenei sektoriuose, pvz., energetikos, transporto, vandens, bankininkystės, finansų rinkų infrastruktūros, sveikatos priežiūros, skaitmeninės infrastruktūros, taip pat pagrindinių skaitmeninių paslaugų teikėjų (paieškos sistemų, debesijos kompiuterijos paslaugų ir elektroninių prekyviečių). Pagrindinis vaidmuo padėti įgyvendinti šią direktyvą buvo priskirtas ENISA. Be to, svarbus Europos saugumo darbotvarkės prioritetas – veiksmingai kovoti su kibernetiniais nusikaltimais, prisidedant prie bendro tikslo užtikrinti aukštą kibernetinio saugumo lygį;

(8) pripažįstama, kad nuo tada, kai 2013 m. buvo priimta ES kibernetinio saugumo strategija ir paskutinį kartą buvo persvarstyti Agentūros įgaliojimai, bendros politinės aplinkybės labai pasikeitė, taip pat dėl labiau nenuspėjamos ir nesaugesnės aplinkos visame pasaulyje. Šiomis sąlygomis ir remiantis nauja Sąjungos kibernetinio saugumo politika būtina peržiūrėti ENISA įgaliojimus, kad būtų apibrėžtas jos vaidmuo pasikeitusioje kibernetinio saugumo ekosistemoje ir užtikrinti, kad ji veiksmingai prisidėtų prie Sąjungos veiksmų reaguojant į kibernetinio saugumo problemas dėl radikaliai pasikeitusių grėsmių, kurioms spręsti, kaip pripažinta Agentūros vertinime, esamų įgaliojimų nepakanka;

(9) šiuo reglamentu įsteigta Agentūra turėtų pakeisti Reglamentu (ES) Nr. 526/2013 įsteigtą ENISA. Agentūra turėtų vykdyti šiuo reglamentu ir kibernetinio saugumo srities Sąjungos teisės aktais jai pavestas užduotis, be kita ko, teikdama ekspertines žinias ir konsultuodama bei atlikdama Sąjungos informacijos ir žinių centro funkcijas. Ji turėtų skatinti keistis geriausia patirtimi tarp valstybių narių ir privačių suinteresuotųjų subjektų, teikti politikos pasiūlymus Europos Komisijai ir valstybėms narėms, veikti kaip informacinis centras vykdant Sąjungos sektorių politikos iniciatyvas kibernetinio saugumo klausimais, skatinti operatyvinį valstybių narių tarpusavio ir valstybių narių bei Europos institucijų, agentūrų ir įstaigų bendradarbiavimą;

(10) Sprendimu 2004/97/EB, Euratomas, kuris buvo priimtas 2003 m. gruodžio 13 d. įvykusiame Europos Vadovų Tarybos susitikime, valstybių narių atstovai nusprendė, kad ENISA būstinė bus viename iš Graikijos miestų, dėl kurio nuspręs Graikijos vyriausybė. Agentūrą priimančioji valstybė narė turėtų užtikrinti kuo geresnes jos sklandžios ir veiksmingos veiklos sąlygas. Kad Agentūra tinkamai ir veiksmingai vykdytų savo užduotis, samdytų ir išsaugotų darbuotojus bei didintų tinklų kūrimo veiklos veiksmingumą, yra būtina Agentūrą įkurdinti tinkamoje vietovėje, be kita ko, užtikrinant tinkamas transporto jungtis ir infrastruktūrą Agentūros darbuotojus lydintiems sutuoktiniams ir vaikams. Agentūros ir priimančiosios valstybės narės susitarime, sudarytame gavus Agentūros Valdančiosios tarybos pritarimą, turėtų būti nustatytos reikiamos nuostatos;

(11) atsižvelgiant į didėjančius kibernetinio saugumo iššūkius, su kuriais susiduria Sąjunga, reikėtų padidinti Agentūrai skiriamus finansinius ir žmogiškuosius išteklius, kad būtų atsižvelgta į didesnį jos vaidmenį ir uždavinius, taip pat labai svarbų jos vaidmenį Europos skaitmeninę ekosistemą ginančių organizacijų ekosistemoje;

(12) Agentūra turėtų kurti ir išlaikyti aukšto lygio ekspertines žinias ir veikti kaip informacinis centras, skatinantis pasitikėti bendrąja rinka – visa tai ji galėtų pasiekti būdama nepriklausoma, teikdama kokybiškas konsultacijas ir skleisdama kokybišką informaciją, užtikrindama savo procedūrų ir veiklos būdų skaidrumą bei uoliai vykdydama savo užduotis. Vykdydama savo užduotis Agentūra turėtų **remti** […] nacionalinius veiksmus ir **aktyviai prisidėti prie** Sąjungos veiksmų, visapusiškai bendradarbiaudama su Sąjungos institucijomis, […] agentūromis **bei įstaigomis** ir valstybėmis narėmis. Be to, Agentūra turėtų remtis privačiojo sektoriaus ir kitų atitinkamų suinteresuotųjų subjektų indėliu ir bendradarbiavimu su jais. Užduočių sąraše turėtų būti nurodyta, kaip Agentūra turi siekti savo tikslų, tačiau jos veiklos sąlygos turėtų būti lanksčios;

(13) Agentūra turėtų padėti Komisijai teikdama patarimus, nuomones ir analizę visais Sąjungos klausimais, susijusiais su politikos ir teisės plėtojimu, atnaujinimu ir peržiūra kibernetinio saugumo srityje, **ir jų specifiniais sektorių aspektais, siekiant padidinti kibernetinio saugumo aspektą apimančios ES politikos ir teisės aktualumą ir sudaryti galimybę jas įgyvendinti nacionaliniu lygmeniu** […]. Rengiant Sąjungos sektorinę politiką ir teisės aktų iniciatyvas kibernetinio saugumo klausimais Agentūra turėtų veikti kaip informacinis centras, teikdama patarimus ir ekspertines žinias;

(14) pagrindinė Agentūros užduotis yra skatinti nuosekliai įgyvendinti atitinkamus teisės aktus, visų pirma veiksmingai įgyvendinti TIS direktyvą, nes tai itin svarbu siekiant padidinti kibernetinį atsparumą. Turint omeny sparčiai kintančias grėsmes kibernetiniam saugumui, akivaizdu, kad valstybėms narėms būtina padėti laikantis platesnio, įvairias politikos sritis apimančio požiūrio į kibernetinio atsparumo didinimą;

(15) Agentūra turėtų padėti valstybėms narėms ir Sąjungos institucijoms, […] agentūroms **ir įstaigoms** plėtoti ir stiprinti pajėgumą ir pasirengimą užkirsti kelią tinklų ir informacinių sistemų saugumo […] **grėsmėms** ir incidentams, juos nustatyti ir į juos reaguoti. Visų pirma Agentūra turėtų padėti plėtoti ir stiprinti nacionalines CSIRT, siekiant užtikrinti vienodą jų brandos Sąjungoje lygį. **ENISA vykdoma veikla, susijusi su valstybių narių operaciniais pajėgumais, turėtų tik papildyti veiksmus, kurių imasi pačios valstybės narės siekdamos vykdyti savo įpareigojimus, kylančius iš TIS direktyvos, ir todėl neturėtų jų pakeisti […]**;

(15a) Agentūra taip pat turėtų padėti rengti ir atnaujinti Sąjungos ir, gavus prašymą, valstybių narių tinklų ir informacinių sistemų saugumo, visų pirma kibernetinio saugumo, strategijas, skatinti jų sklaidą ir stebėti jų įgyvendinimą. Be to, Agentūra turėtų organizuoti viešiesiems subjektams skirtus mokymus ir teikti mokymo medžiagą bei, prireikus, mokyti instruktorius, siekiant padėti valstybėms narėms plėtoti jų pačių mokymo pajėgumus;

(16) Agentūra turėtų padėti pagal TIS direktyvą įsteigtai Bendradarbiavimo grupei vykdyti jos užduotis, visų pirma susijusias su valstybių narių esminių paslaugų teikėjų nustatymu, taip pat klausimais, susijusiais su tarpvalstybine priklausomybe, rizika ir incidentais, teikdama ekspertines žinias bei konsultuodama ir sudaryti palankesnes sąlygas keistis geriausia praktika;

(17) siekiant skatinti viešojo ir privačiojo sektorių bendradarbiavimą ir bendradarbiavimą privačiajame sektoriuje […], **Agentūra turėtų** remti **dalijimąsi informacija sektoriuose ir tarp sektorių, visų pirma išvardytųjų Direktyvos (ES) 2016/1148 II priede, dalydamasi geriausia patirtimi ir teikdama rekomendacijas dėl esamų priemonių ir procedūrų, taip pat rekomendacijas, kaip spręsti su dalijimusi informacija susijusius reguliavimo klausimus, pavyzdžiui, padėdama** […] steigti sektorių keitimosi informacija ir jos analizės centrus (ISAC) […];

(18) Agentūra turėtų apibendrinti ir analizuoti **savanoriškai pateiktas** nacionalines CSIRT ir CERT-EU ataskaitas, **siekdama padėti valstybėms narėms** nustatyti bendras keitimosi informacija […] **procedūras**, kalbą ir terminiją. Remdamasi TIS direktyva, kuria […] padėtas pamatas savanoriškiems techninės informacijos mainams **CSIRT tinkle** operatyviniu lygmeniu, Agentūra taip pat turėtų įtraukti privatųjį sektorių;

(19) Agentūra turėtų padėti ES lygmeniu reaguoti į didelio masto tarpvalstybinius kibernetinio saugumo incidentus ir krizes. Ši veikla turėtų **būti vykdoma laikantis jos įgaliojimų pagal šį reglamentą ir požiūrio, dėl kurio turi susitarti valstybės narės pagal Komisijos rekomendaciją dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes.** Vykdydama šią veiklą Agentūra **galėtų** rinkti svarbią informaciją ir prisiimti tarpininkės tarp CSIRT tinklo, techninės bendruomenės ir už krizių valdymą atsakingų sprendimus priimančių asmenų vaidmenį. Be to, Agentūra galėtų padėti valdyti incidentus techniniu požiūriu sudarydama palankesnes sąlygas valstybėms narėms keistis tinkamais techniniais sprendimais ir prisidėdama prie viešųjų ryšių. Agentūra turėtų palaikyti šį procesą, per […] **reguliarias** kibernetinio saugumo pratybas išbandydama tokio bendradarbiavimo būdus;

(20) [...] **remdama** operatyvinį **bendradarbiavimą**, Agentūra turėtų naudotis esamomis CERT-EU **techninėmis ir operatyvinėmis** ekspertinėmis žiniomis palaikydama struktūrinį bendradarbiavimą [...]. […] Jei tinkama, turėtų būti sudaryti specialūs šių dviejų organizacijų susitarimai, kuriuose nustatoma, kaip toks bendradarbiavimas bus įgyvendinamas praktiškai**, siekiant išvengti veiklos dubliavimo**;

(21) vykdydama savo užduotis [...]**, kuriomis remiamas operatyvinis bendradarbiavimas CSIRT tinkle,** Agentūra turėtų galėti **valstybėms narėms paprašius** teikti joms paramą, pavyzdžiui, teikdama konsultacijas**, kaip pagerinti jų pajėgumus užkirsti kelią incidentams, juos aptikti ir į juos reaguoti, palengvindama didelį arba esminį poveikį turinčių incidentų** techninį **valdymą** [...] arba užtikrindama grėsmių ir incidentų analizę. **[...] Didelį arba esminį poveikį turinčių incidentų techninio valdymo palengvinimas [...] visų pirma turėtų apimti ENISA paramą savanoriškam valstybių narių dalijimuisi techniniais sprendimais arba bendros techninės informacijos, kuri galėtų apimti, pavyzdžiui, valstybių narių savanoriškai pateiktus techninius sprendimus, rengimą.** Komisijos rekomendacijoje dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes rekomenduojama, kad valstybės narės geranoriškai bendradarbiautų ir nedelsdamos dalytųsi tarpusavyje bei su ENISA informacija apie didelio masto kibernetinio saugumo incidentus ir krizes. Tokia informacija turėtų dar labiau padėti ENISA […] **remti operatyvinį bendradarbiavimą**;

(22) reguliaraus techninio bendradarbiavimo, padedančio būti geriau informuotiems apie padėtį Sąjungoje, dalis turėtų būti Agentūros reguliariai**, glaudžiai bendradarbiaujant su valstybėmis narėmis,** rengiama ES kibernetinio saugumo techninės padėties ataskaita, kurioje apžvelgiami incidentai ir grėsmės ir kuri grindžiama viešai prieinama informacija, pačios Agentūros atliekama analize ir ataskaitomis, kurias Agentūrai pateikė valstybių narių CSIRT […] arba pagal TIS direktyvą įsteigti bendrieji informaciniai centrai **(tiek vieni, tiek kiti – savanoriškai)**, Europolo Europos kovos su elektroniniu nusikalstamumu centras (EC3), CERT-EU ir prireikus Europos išorės veiksmų tarnybai priklausantis Europos Sąjungos žvalgybos analizės centras (INTCEN). Ataskaita turėtų būti pateikta atitinkamoms Tarybos instancijoms, Komisijai, Sąjungos vyriausiajam įgaliotiniui užsienio reikalams ir saugumo politikai ir CSIRT tinklui;

(23) **Agentūrai** […] **susijusių** […] valstybių narių prašymu **remiant** didelį poveikį […] turinčių incidentų […] *ex post* techninius **tyrimus**, daugiausia dėmesio turėtų būti skiriama incidentų prevencijai […]. **Susijusios valstybės narės turėtų pateikti reikiamą informaciją, kad Agentūra galėtų veiksmingai prisidėti prie techninio tyrimo;**

(24) […]

(25) valstybės narės gali paraginti incidento paveiktas įmones bendradarbiauti ir teikti reikalingą informaciją ir pagalbą Agentūrai, nepažeidžiant jų teisės apsaugoti neskelbtiną komercinę informaciją;

(26) siekdama geriau suprasti kibernetinio saugumo srities problemas ir teikti strategines ilgalaikes rekomendacijas valstybėms narėms ir Sąjungos institucijoms Agentūra turi analizuoti esamą ir atsirandančią riziką. Šiuo tikslu Agentūra, bendradarbiaudama su valstybėmis narėmis ir prireikus su statistikos įstaigomis ir kitais subjektais, turėtų rinkti reikiamą informaciją**, kuri yra viešai prieinama arba savanoriškai pateikiama,** ir vykdyti naujausių technologijų analizę bei teikti teminius vertinimus, susijusius su numatomu tinklų ir informacijos saugumo, visų pirma kibernetinio saugumo, srities technologinių inovacijų visuomeniniu, teisiniu, ekonominiu ir reguliavimo poveikiu. Be to, Agentūra, vykdydama grėsmių ir incidentų analizę, turėtų padėti valstybėms narėms ir Sąjungos institucijoms, agentūroms ir įstaigoms nustatyti atsirandančias tendencijas ir išvengti […] kibernetinio saugumo **incidentų** […];

(27) kad padidintų Sąjungos atsparumą, Agentūra turėtų plėtoti mokslinę kompetenciją **infrastruktūros objektų, kurie užtikrina visų pirma TIS direktyvos II priede išvardytų sektorių veiklą ir kuriuos naudoja tos direktyvos III priede išvardyti skaitmeninių paslaugų teikėjai, kibernetinio** saugumo klausimais, […] konsultuodama, teikdama rekomendacijas ir dalydamasi geriausia patirtimi. Siekdama užtikrinti lengvesnę prieigą prie geriau struktūruotos informacijos apie kibernetinio saugumo riziką ir galimas taisomąsias priemones, Agentūra turėtų sukurti ir palaikyti Sąjungos informacijos centrą – vieno langelio principu veikiantį portalą, kuriame visuomenei būtų prieinama ES ir nacionalinių institucijų, agentūrų ir įstaigų teikiama informacija apie kibernetinį saugumą;

(28) Agentūra turėtų padėti didinti visuomenės informuotumą apie riziką, susijusią su kibernetiniu saugumu, ir piliečiams bei organizacijoms pateikti atskiriems naudotojams skirtas gerosios praktikos rekomendacijas. Agentūra taip pat turėtų padėti skatinti asmenis ir organizacijas taikyti geriausią patirtį ir sprendimus, šiuo tikslu rinkdama ir analizuodama viešai prieinamą informaciją apie didelius incidentus, taip pat rengti ataskaitas siekdama įmonėms ir piliečiams teikti rekomendacijas bei pagerinti bendrą pasirengimo ir atsparumo lygį. Agentūra, bendradarbiaudama su valstybėmis narėmis ir Sąjungos institucijomis, […] agentūromis **ir įstaigomis**, taip pat turėtų organizuoti reguliarias galutiniams vartotojams skirtas visuomenės švietimo kampanijas, kuriomis būtų siekiama propaguoti saugesnį asmens elgesį internetinėje aplinkoje ir skatinti informuoti apie galimas grėsmes kibernetinėje erdvėje, įskaitant elektroninius nusikaltimus, kaip antai duomenų vagystes, botnetus, finansinį ir bankinį sukčiavimą, taip pat skatinti teikti pagrindinę patariamojo pobūdžio informaciją apie autentiškumo patvirtinimą ir duomenų apsaugą. Agentūra turėtų atlikti pagrindinį vaidmenį spartindama galutinių vartotojų informuotumą apie įrenginių saugumą;

(29) siekdama padėti kibernetinio saugumo sektoriuje veikiančioms įmonėms bei kibernetinio saugumo sprendimų naudotojams Agentūra turėtų sukurti rinkos stebėjimo centrą ir palaikyti jo veiklą reguliariai analizuodama svarbiausias kibernetinio saugumo rinkos paklausos ir pasiūlos tendencijas ir skleisdama apie jas informaciją;

(30) kad Agentūra galėtų pasiekti visus savo tikslus, ji turėtų bendradarbiauti su atitinkamomis institucijomis, agentūromis ir įstaigomis, be kita ko, CERT-EU, Europolo Europos kovos su elektroniniu nusikalstamumu centru (EC3), Europos gynybos agentūra (EGA), Europos didelės apimties IT sistemų operacijų valdymo agentūra (eu-LISA), Europos aviacijos saugos agentūra (EASA), **Europos pasaulinės navigacijos palydovų sistemos agentūra (GNSS agentūra)**, Europos pasaulinės navigacijos palydovų sistemos priežiūros institucija ir kitomis su kibernetiniu saugumu susijusiomis ES agentūromis. Ji taip pat turėtų bendradarbiauti su duomenų apsaugos institucijomis siekiant keistis praktine patirtimi ir geriausia praktika ir teikti rekomendacijas dėl poveikį jų darbui galinčių daryti kibernetinio saugumo aspektų. Nacionalinių ir Sąjungos teisėsaugos ir duomenų apsaugos institucijų atstovams turėtų būti suteikta teisė dalyvauti Agentūros nuolatinės suinteresuotųjų subjektų grupės veikloje. Bendradarbiaudama su teisėsaugos įstaigomis tinklų ir informacijos saugumo aspektais, galinčiais turėti įtakos jų darbui, Agentūra turėtų naudotis esamais informacijos kanalais ir sukurtais tinklais;

(31) be visų TIS direktyvoje apibrėžtų atitinkamų CSIRT tinklo užduočių vykdymo, Agentūra, […] **vykdydama** CSIRT tinklo sekretoriato **funkciją**, turėtų remti valstybių narių CSIRT ir CERT-EU operatyvinį bendradarbiavimą. Be to, Agentūra turėtų skatinti ir remti atitinkamų CSIRT bendradarbiavimą incidentų, išpuolių arba tinklo ar infrastruktūros, kurią valdo ar saugo CSIRT ir kurioje dalyvauja ar potencialiai dalyvautų bent dvi CERT, sutrikimų atvejais, deramai atsižvelgdama į CSIRT tinklo standartines veiklos procedūras;

(32) kad Sąjunga būtų geriau pasirengusi reaguoti į kibernetinio saugumo incidentus, Agentūra turėtų organizuoti […] **reguliarias** Sąjungos lygmens kibernetinio saugumo pratybas ir valstybėms narių, ES institucijų, agentūrų ir įstaigų prašymu padėti joms organizuoti pratybas;

(33) kad galėtų prisidėti prie Sąjungos kibernetinio saugumo sertifikavimo politikos Agentūra turėtų toliau gerinti ir išlaikyti savo kompetenciją šiais klausimais. Agentūra turėtų skatinti kibernetinio saugumo sertifikavimo diegimą Sąjungoje, be kita ko, prisidėdama prie Sąjungos lygmens kibernetinio saugumo sertifikavimo sistemos sukūrimo ir taikymo, siekiant didinti IRT produktų ir paslaugų kibernetinio saugumo užtikrinimo skaidrumą ir taip sustiprinti pasitikėjimą skaitmenine vidaus rinka;

(34) veiksminga kibernetinio saugumo politika viešajame ir privačiajame sektoriuose turėtų būti grindžiama gerai parengtais rizikos vertinimo metodais. Įvairiais lygmenimis rizikos vertinimo metodai taikomi nesant bendros jų veiksmingo taikymo praktikos. Geriausių rizikos vertinimo ir sąveikiųjų rizikos valdymo sprendimų populiarinimas ir plėtojimas viešojo ir privačiojo sektoriaus organizacijose padidins kibernetinio saugumo Sąjungoje lygį. Todėl Agentūra turėtų remti suinteresuotųjų subjektų bendradarbiavimą Sąjungos lygmeniu, palaikydama jų pastangas nustatyti rizikos valdymo, taip pat elektroninių gaminių, sistemų, tinklų ir paslaugų, kurios kartu su programine įranga sudaro tinklų ir informacijos sistemas, išmatuojamojo saugumo Europos ir tarptautinius standartus ir jų laikytis;

(35) Agentūra turėtų skatinti valstybes nares ir paslaugų teikėjus griežtinti savo bendruosius saugumo standartus, kad visi interneto naudotojai galėtų imtis reikiamų veiksmų savo asmeniniam kibernetiniam saugumui užtikrinti. Visų pirma, paslaugų teikėjai ir produktų gamintojai turėtų atšaukti arba pakoreguoti kibernetinio saugumo standartų neatitinkančius produktus ir paslaugas. Bendradarbiaudama su kompetentingomis institucijomis ENISA gali skleisti informaciją apie vidaus rinkoje siūlomų produktų ir paslaugų kibernetinio saugumo lygį ir įspėti paslaugų teikėjus bei gamintojus ir reikalauti, kad jie pagerintų savo produktų saugumą, įskaitant kibernetinį saugumą;

(36) agentūra turėtų visiškai atsižvelgti į šiuo metu vykdomą mokslinių tyrimų, plėtros ir technologijų vertinimo veiklą, visų pirma atliekamą pagal įvairias Sąjungos mokslinių tyrimų iniciatyvas, siekdama teikti patarimus Sąjungos institucijoms, […] agentūroms **ir įstaigoms**, ir prireikus ir joms paprašius – valstybėms narėms – dėl mokslinių tyrimų poreikių tinklų ir […] kibernetinio saugumo srityje. **Kad nustatytų mokslinių tyrimų poreikius ir prioritetus, Agentūra taip pat turėtų konsultuotis su atitinkamomis naudotojų grupėmis;**

(37) kibernetinio saugumo […] **grėsmės** yra pasaulinės. Būtinas glaudesnis tarptautinis bendradarbiavimas, kad būtų patobulinti **kibernetinio** saugumo standartai, įskaitant bendrų elgesio normų apibrėžimą bei informacijos mainus, spartesnio tarptautinio bendradarbiavimo skatinimą reaguojant į tinklų ir informacijos saugumo problemas ir vadovaujantis visuotiniu požiūriu į jas. Tuo tikslu Agentūra turėtų remti tolesnį Sąjungos ryšių mezgimą ir bendradarbiavimą su trečiosiomis šalimis ir tarptautinėmis organizacijomis, prireikus teikdama atitinkamoms Sąjungos institucijoms, [...] agentūroms **ir įstaigoms** reikalingas specialiąsias žinias ir analizę;

(38) Agentūra turėtų būti pajėgi reaguoti į valstybių narių ir ES institucijų, agentūrų ir įstaigų *ad hoc* prašymus teikti patarimus ir paramą, susijusius su Agentūros tikslais;

(39) būtina įgyvendinti tam tikrus Agentūros valdymo principus, kad būtų laikomasi bendro pareiškimo ir bendro požiūrio, dėl kurių 2012 m. liepos mėn. susitarė Tarpinstitucinė darbo grupė ES decentralizuotų agentūrų klausimais; šiuo pareiškimu ir požiūriu siekiama racionalizuoti agentūrų veiklą ir pagerinti jų darbą. Prireikus į bendrą pareiškimą ir bendrą požiūrį taip pat turėtų būti atsižvelgta Agentūros darbo programose, Agentūros vertinimuose ir Agentūrai teikiant ataskaitas bei vykdant administracinę veiklą;

(40) iš valstybių narių ir Komisijos atstovų sudaryta Valdančioji taryba turėtų apibrėžti bendrąją Agentūros veiklos kryptį ir užtikrinti, kad savo užduotis ji vykdytų pagal šį reglamentą. Valdančiajai tarybai turėtų būti suteikti įgaliojimai, būtini sudaryti biudžetą, tikrinti, kaip jis vykdomas, priimti reikiamas finansines taisykles, sukurti skaidrias Agentūros sprendimų priėmimo procedūras, priimti Agentūros bendrąjį programavimo dokumentą, nustatyti savo darbo tvarkos taisykles, paskirti vykdomąjį direktorių ir nuspręsti dėl vykdomojo direktoriaus kadencijos pratęsimo bei jos nutraukimo;

(41) kad Agentūros veikla būtų tinkama ir veiksminga, Komisija ir valstybės narės turėtų užtikrinti, kad į Valdančiąją tarybą būtų skiriami tinkamos profesinės patirties ir patirties funkcinėse srityse turintys asmenys. Komisija ir valstybės narės taip pat turėtų stengtis riboti savo atstovų Valdančiojoje taryboje kaitą, kad būtų užtikrintas jos veiklos tęstinumas;

(42) kad Agentūra veiktų sklandžiai, jos vykdomasis direktorius turi būti skiriamas atsižvelgiant į privalumus ir į dokumentais pagrįstus administracinio ir vadovaujamojo darbo įgūdžius bei kompetenciją, kibernetiniam saugumui svarbią patirtį ir kompetenciją, o vykdomojo direktoriaus pareigos turi būti atliekamos visiškai nepriklausomai. Pasitaręs su Komisija vykdomasis direktorius turėtų parengti Agentūros veiklos programos pasiūlymą ir imtis visų būtinų veiksmų, kad užtikrintų tinkamą Agentūros veiklos programos vykdymą. Vykdomasis direktorius turėtų parengti Valdančiajai tarybai teikiamą metinę ataskaitą, **apimančią Agentūros metinės darbo programos įgyvendinimą**, Agentūros pajamų ir išlaidų sąmatos projektą ir įgyvendinti biudžetą. Be to, vykdomajam direktoriui turėtų būti leista steigti *ad hoc* darbo grupes konkretiems, visų pirma moksliniams, techniniams, teisiniams ar socialiniams ir ekonominiams, klausimams spręsti. Vykdomasis direktorius turėtų užtikrinti, kad *ad hoc* darbo grupės nariai būtų išrinkti pagal aukščiausius dalyko žinių standartus ir atsižvelgiant į nagrinėjamus klausimus būtų subalansuotai atstovaujama valstybių narių viešojo administravimo institucijoms, Sąjungos institucijoms ir privačiajam sektoriui, įskaitant pramonę, vartotojams ir tinklų bei informacijos apsaugos mokslo ekspertams;

(43) Vykdomoji valdyba turėtų prisidėti prie veiksmingo Valdančiosios tarybos veikimo. Atlikdama parengiamąjį darbą, susijusį su Valdančiosios tarybos sprendimais, ji turėtų išsamiai išnagrinėti atitinkamą informaciją ir apsvarstyti turimas galimybes bei teikti rekomendacijas ir sprendimus siekiant parengti atitinkamus Valdančiosios valdybos sprendimus;

(44) siekiant palaikyti nuolatinį dialogą su privačiuoju sektoriumi, vartotojų organizacijomis ir kitais atitinkamais suinteresuotaisiais subjektais Agentūroje turėtų būti įsteigta nuolatinė suinteresuotųjų subjektų grupė, veikianti kaip patariamasis organas. Vykdomojo direktoriaus pasiūlymu Valdančiosios tarybos įsteigta nuolatinė suinteresuotųjų subjektų grupė pagrindinį dėmesį turėtų skirti suinteresuotiesiems subjektams svarbiems klausimams ir į tuos klausimus atkreipti Agentūros dėmesį. Nuolatinės suinteresuotųjų subjektų grupės sudėtis ir šiai grupei, su kuria turi būti konsultuojamasi dėl veiklos programos projekto, priskirtos užduotys, turėtų užtikrinti pakankamą suinteresuotųjų subjektų atstovavimą Agentūros veikloje;

(45) Agentūra turėtų priimti interesų konfliktų prevencijos ir valdymo taisykles. Agentūra taip pat turėtų taikyti atitinkamas Sąjungos nuostatas dėl galimybės visuomenei susipažinti su dokumentais, kaip nustatyta Europos Parlamento ir Tarybos reglamente (EB) Nr. 1049/2001 [12]. Agentūra asmens duomenis turėtų tvarkyti laikydamasi 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo [13]. Agentūra turėtų laikytis Sąjungos institucijoms taikytinų nuostatų ir nacionalinės teisės aktų dėl informacijos, visų pirma neskelbtinos neįslaptintos ir ES įslaptintos informacija tvarkymo;

---

[12] 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais (OL L 145, 2001 5 31, p. 43).

[13] OL L 8, 2001 1 12, p. 1.

(46) siekiant užtikrinti visišką Agentūros autonomiją ir nepriklausomumą ir suteikti jai galimybę vykdyti papildomas ir naujas užduotis, įskaitant nenumatytas užduotis kritiniais atvejais, Agentūrai turėtų būti skiriamas pakankamas ir nepriklausomas biudžetas, kurio pajamas iš esmės sudarytų Sąjungos įnašas ir Agentūros veikloje dalyvaujančių trečiųjų šalių įnašai. Dauguma Agentūros darbuotojų turėtų tiesiogiai dalyvauti praktiškai vykdant Agentūros įgaliojimus. Agentūrą priimančiajai valstybei narei arba bet kuriai kitai valstybei narei turėtų būti leidžiama savanoriškais įnašais prisidėti prie Agentūros pajamų. Mokant subsidijas iš Sąjungos bendrojo biudžeto, turėtų būti taikoma Sąjungos biudžeto procedūra. Be to, Audito Rūmai turėtų atlikti Agentūros apskaitos auditą, kad būtų užtikrintas skaidrumas ir atskaitomybė;

(47) […]

(48) kibernetinio saugumo sertifikavimas yra labai svarbus didinant pasitikėjimą IRT produktais ir paslaugomis bei jų saugumą. Bendroji skaitmeninė rinka, visų pirma duomenų ekonomika ir daiktų internetas, ir gali klestėti tik jei visuomenė tikės, jog tokie produktai ir paslaugos užtikrina tam tikro lygio kibernetinį saugumą. Susietųjų ir automatizuotų automobilių, elektroninių medicinos priemonių, pramoninių automatizacijos valdymo sistemų ar pažangiųjų elektros energijos tinklų sektoriai yra tik keli sektorių, kuriuose sertifikavimas jau yra plačiai naudojamas arba gali būti naudojamas artimiausioje ateityje, pavyzdžiai. Kibernetinio saugumo sertifikavimas taip pat yra itin svarbus TIS direktyva reglamentuojamiems sektoriams;

(49) 2016 m. komunikate „Europos kibernetinio atsparumo sistemos stiprinimas ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimas“ Komisija nurodė kokybiškų, įperkamų ir sąveikių kibernetinio saugumo produktų ir sprendimų poreikį. IRT produktų tiekimas ir paslaugų teikimas bendrojoje rinkoje geografine prasme tebėra labai nevienodai išplėtotas. Taip yra dėl to, kad kibernetinio saugumo sektorius Europoje daugiausia vystėsi grindžiamas nacionalinės valdžios poreikiu. Kiti bendrąją kibernetinio saugumo rinką neigiamai veikiantys trūkumai, be kita ko, yra sąveikių sprendimų (techninių standartų), metodų ir ES masto sertifikavimo mechanizmų stoka. Viena vertus, tai apsunkina Europos įmonių galimybes konkuruoti nacionaliniu, Europos ir pasauliniu lygmenimis. Kita vertus, tai mažina perspektyvių ir tinkamų fiziniams asmenims bei įmonėms prieinamų kibernetinio saugumo technologijų pasirinkimo galimybes. Be to, Bendrosios skaitmeninės rinkos strategijos įgyvendinimo laikotarpio vidurio peržiūroje Komisija pabrėžė būtinybę turėti saugių susietųjų produktų ir sistemų ir nurodė, kad sukūrus Europos IRT saugumo sistemą, kurioje būtų nustatytos taisyklės, kaip Sąjungoje organizuoti IRT saugumo sertifikavimą, būtų galima išsaugoti pasitikėjimą internetu ir spręsti dabartinio kibernetinio saugumo rinkos susiskaidymo problemą;

(50) šiuo metu IRT **procesų,** produktų ir paslaugų kibernetinio saugumo sertifikavimas yra ribotas. Kai jie sertifikuojami, toks sertifikavimas dažniausiai vykdomas valstybių narių lygmeniu arba pagal pramonės iniciatyva pagrįstas schemas. Tai reiškia, kad vienos nacionalinės kibernetinio saugumo institucijos išduotas sertifikatas iš esmės kitose valstybėse narėse nepripažįstamas. Todėl bendrovėms gali reikėti savo produktus ir paslaugas sertifikuoti keliose valstybėse narėse, kuriose jos vykdo veiklą, pavyzdžiui, siekiant dalyvauti nacionalinėse viešųjų pirkimų procedūrose. Be to, nors atsiranda naujų schemų, atrodo, nėra nuoseklaus ir visapusiško požiūrio į horizontalius kibernetinio saugumo klausimus, pavyzdžiui, daiktų interneto srityje. Esamose schemose yra didelių trūkumų ir skirtumų, susijusių su sertifikuojamais produktais, saugumo užtikrinimo lygiais, esminiais kriterijais ir faktiniu naudojimu;

(51) jau anksčiau buvo imtasi tam tikrų veiksmų siekiant užtikrinti sertifikatų savitarpio pripažinimą Europoje. Tačiau jie tik iš dalies buvo veiksmingi. Svarbiausias pavyzdys šiuo požiūriu – vyresniųjų pareigūnų grupės informacinių sistemų saugumo klausimais (SOG-IS) tarpusavio pripažinimo susitarimas. Nors saugumo sertifikavimo srityje tai yra svarbiausias bendradarbiavimo ir tarpusavio pripažinimo modelis, […] SOG-IS apima tik dalį Sąjungos valstybių narių. Tai riboja SOG-IS tarpusavio pripažinimo susitarimą veiksmingumą vidaus rinkoje;

(52) atsižvelgiant į tai, kas išdėstyta pirmiau, būtina sukurti Europos kibernetinio saugumo sertifikavimo sistemą, kurioje būtų nustatyti pagrindiniai kuriamoms Europos kibernetinio saugumo sertifikavimo schemoms keliami horizontalieji reikalavimai ir kuria būtų sudarytos sąlygos IRT produktų ir paslaugų sertifikatus **bei ES atitikties pareiškimus** pripažinti ir taikyti visose valstybėse narėse. Europine sistema turėtų būti siekiama dvejopo tikslo. Viena vertus, ji turėtų padėti didinti pasitikėjimą IRT produktais ir paslaugomis, kurie buvo sertifikuoti pagal tas schemas. Kita vertus, ji turėtų padėti išvengti vienas kitai prieštaraujančių arba besidubliuojančių nacionalinių kibernetinio saugumo sertifikavimo schemų daugėjimo ir taip sumažinti bendrojoje skaitmeninėje rinkoje veikiančių įmonių išlaidas. Šios schemos turėtų būti nediskriminacinės ir pagrįstos tarptautiniais ir (arba) […] **Europos** standartais, išskyrus atvejus, kai tie standartai yra neveiksmingi arba netinkami siekiant įgyvendinti teisėtus šios srities ES tikslus;

(53) Komisija turėtų būti įgaliota tvirtinti konkrečioms IRT **procesų,** produktų ir paslaugų grupėms taikomas Europos kibernetinio saugumo sertifikavimo schemas. Įgyvendinti ir prižiūrėti šias schemas turėtų nacionalinės **kibernetinio saugumo** sertifikavimo [...] institucijos, o pagal šias schemas išduoti sertifikatai turėtų galioti ir būti pripažįstami visoje Sąjungoje. Šis reglamentas neturėtų būti taikomas pramonės ar kitų privačių organizacijų naudojamoms sertifikavimo schemoms. Tačiau tokias schemas naudojantys subjektai gali siūlyti Komisijai jų pagrindu patvirtinti europinę schemą;

(54) šio reglamento nuostatomis neturėtų būti daromas poveikis Sąjungos teisės aktams, kuriais nustatomos specialios IRT produktų ir paslaugų sertifikavimo taisyklės. Visų pirma Bendrajame duomenų apsaugos reglamente išdėstomos nuostatos dėl sertifikavimo mechanizmų ir duomenų apsaugos ženklų bei žymenų nustatymo, siekiant įrodyti duomenų valdytojų ir tvarkytojų vykdomų tvarkymo operacijų atitiktį to reglamento nuostatoms. Tokie sertifikavimo mechanizmai ir duomenų apsaugos ženklai ir žymenys turėtų sudaryti sąlygas duomenų subjektams greitai įvertinti atitinkamų produktų ir paslaugų duomenų apsaugos lygį. Šiuo reglamentu nedaromas poveikis duomenų tvarkymo operacijų sertifikavimui, taip pat kai tokios operacijos pagal Bendrąjį duomenų apsaugos reglamentą susietos su produktais ir paslaugomis;

(55) Europos kibernetinio saugumo sertifikavimo schemų tikslas turėtų būti užtikrinti, kad pagal tokią schemą sertifikuoti IRT **procesai,** produktai ir paslaugos atitiktų nustatytus reikalavimus […], siekiant **apsaugoti** saugomų, perduodamų ar tvarkomų duomenų arba tais produktais, procesais, paslaugomis ir sistemomis suteikiamų arba per juos prieinamų funkcijų ar paslaugų prieinamumą, autentiškumą, vientisumą ir konfidencialumą **viso jų gyvavimo ciklo metu**, kaip apibrėžta šiame reglamente. Šiame reglamente neįmanoma išsamiai nustatyti visiems IRT **procesams,** produktams ir paslaugoms keliamų kibernetinio saugumo reikalavimų. IRT **procesai,** produktai ir paslaugos bei susiję kibernetinio saugumo poreikiai yra tokie įvairūs, kad labai sunku nustatyti bendrus visiems produktams ir paslaugoms galiojančius kibernetinio saugumo reikalavimus. Todėl sertifikavimo tikslu reikalinga plati ir bendra kibernetinio saugumo samprata, kurią papildytų konkretūs kibernetinio saugumo tikslai, į kuriuos turi būti atsižvelgta rengiant Europos kibernetinio saugumo sertifikavimo schemas. Kaip tie tikslai bus pasiekti sertifikuojant konkrečius IRT **procesus,** produktus ir paslaugas, turėtų būti toliau išsamiai nurodyta atskiros Komisijos tvirtinamos sertifikavimo schemos lygmeniu, pavyzdžiui, nurodant standartus ar technines specifikacijas**, kai tinkamų standartų nėra**;

(55a) Europos kibernetinio saugumo sertifikavimo schemoje naudotinos techninės specifikacijos turėtų būti nustatytos laikantis Reglamento (ES) 1025/2012 II priede išdėstytų principų. Vis dėlto, tinkamai pagrįstais atvejais būtų galima laikyti, kad kai kurie nukrypimai nuo šių principų yra reikalingi, kai tos techninės specifikacijos turi būti naudojamos Europos kibernetinio saugumo sertifikavimo schemoje, patvirtinančioje aukštą saugumo užtikrinimo lygį. Tokių nukrypimų priežastys turi būti pateikiamos viešai;

(55b) sertifikuotas atitikties vertinimas – procesas, kurio metu vertinama, ar buvo įvykdyti nustatyti reikalavimai, susiję su IRT procesu, produktu arba paslauga. Šį procesą vykdo nepriklausoma trečioji šalis, kuri nėra produkto gamintoja arba paslaugos teikėja. Po sėkmingo IRT proceso, produkto ar paslaugos įvertinimo proceso vykdomas sertifikato išdavimo procesas. Jis turėtų būti laikomas patvirtinimu, kad atitinkamas įvertinimas buvo tinkamai atliktas. Priklausomai nuo saugumo užtikrinimo lygio, Europos kibernetinio saugumo schemoje turėtų būti nurodyta, ar sertifikatą išduoda privati ar vieša įstaiga. Pats atitikties vertinimas ir sertifikavimas negali užtikrinti, kad IRT produktai ir paslaugos kibernetiniu požiūriu yra saugūs. Tai greičiau procedūra ir techninė metodika, kuriomis patvirtinama, kad IRT produktai ir paslaugos buvo išbandyti ir kad jie atitinka tam tikrus kitur, pavyzdžiui, techniniuose standartuose, nustatytus kibernetinio saugumo reikalavimus;

(55c) sertifikatų naudotojai, rinkdamiesi tinkamą sertifikavimo lygį ir susijusius saugumo reikalavimus, turėtų remtis IRT proceso, produkto ar paslaugos naudojimo rizikos analize. Todėl saugumo užtikrinimo lygis turėtų priklausyti nuo rizikos, susijusios su IRT proceso, produkto arba paslaugos paskirtimi, lygio;

(55d) Europos kibernetinio saugumo sertifikavimo schemoje gali būti numatyta, kad atitikties vertinimas vykdomas tik IRT produktų gamintojo arba paslaugų teikėjo atsakomybe (savarankiškas atitikties vertinimas). Tokiais atvejais pakanka, kad gamintojas arba teikėjas pats atliktų visus patikrinimus siekdamas užtikrinti IRT proceso, produktų ar paslaugų atitiktį sertifikavimo schemai. Šios rūšies atitikties vertinimas turėtų būti laikomas tinkamu nesudėtingiems IRT produktams ir paslaugoms (pvz., paprastam projektavimo ir gamybos mechanizmui), kurie nekelia didelės grėsmės viešajam interesui. Be to, savarankiškas atitikties vertinimas gali būti taikomas tik IRT produktams ir paslaugoms, atitinkantiems bazinį saugumo užtikrinimo lygį;

(55e) Europos kibernetinio saugumo užtikrinimo schemoje galėtų būti numatytas tiek IRT produktų ir paslaugų sertifikavimas, tiek savarankiškas jų atitikties vertinimas. Tokiu atveju schemoje turėtų būti numatytos aiškios ir suprantamos priemonės, kad vartotojai ir kiti naudotojai galėtų produktus ir paslaugas, vertinamus gamintojo arba teikėjo atsakomybe, atskirti nuo produktų ir paslaugų, kuriuos sertifikuoja trečioji šalis;

(55f) IRT produktų gamintojas arba paslaugų teikėjas, kuris atlieka savarankišką atitikties vertinimą, vykdydamas atitikties vertinimo procedūrą turėtų parengti ir pasirašyti ES atitikties pareiškimą. ES atitikties pareiškimas – dokumentas, kuriame visų pirma pareiškiama, jog IRT produktas arba paslauga atitinka schemos reikalavimus. Parengęs ir pasirašęs ES atitikties pareiškimą, gamintojas arba teikėjas prisiima atsakomybę už IRT produkto ar paslaugos atitiktį teisiniams schemos reikalavimams. ES atitikties pareiškimo kopija turėtų būti pateikta nacionalinei kibernetinio saugumo sertifikavimo institucijai ir ENISA;

(55g) ES atitikties pareiškimą ir visos aktualios informacijos, susijusios su IRT produktų ar paslaugų atitiktimi schemai, techninę dokumentaciją IRT produktų gamintojas arba paslaugų teikėjas turėtų saugoti konkrečioje Europos kibernetinio saugumo sertifikavimo schemoje nurodytą laikotarpį, kad galėtų juos pateikti kompetentingai nacionalinei kibernetinio saugumo sertifikavimo institucijai. Techninėje dokumentacijoje turėtų būti nurodyti taikomi reikalavimai ir, jeigu tai svarbu vertinimui atlikti, aprašomi IRT produkto arba paslaugos projektas, gamyba ir naudojimas. Techniniai dokumentai turėtų būti parengti taip, kad būtų galima įvertinti IRT produkto ar paslaugos atitiktį atitinkamiems reikalavimams;

(55h) valstybės narės ir atitinkamos suinteresuotųjų subjektų organizacijos turėtų turėti teisę siūlyti Europos kibernetinio saugumo sertifikavimo grupei parengti potencialią schemą. Atitinkamos suinteresuotųjų subjektų organizacijos – pramonės ar vartotojų organizacijos, įskaitant MVĮ organizacijų atstovus, turinčios pagrįstą interesą parengti konkrečią Europos kibernetinio saugumo sertifikavimo schemą. Tokie pasiūlymai turėtų būti nagrinėjami atsižvelgiant į kriterijus, kuriuos parengė Europos kibernetinio saugumo sertifikavimo grupė remdamasi gairėmis, grindžiamomis skaidrumu, atvirumu, nešališkumu, konsensusu, veiksmingumu, aktualumu ir nuoseklumu;

(56) Komisijai **ir Grupei** turėtų būti suteikti įgaliojimai prašyti ENISA **nepagrįstai nedelsiant** parengti konkretiems IRT **procesams,** produktams ir paslaugoms taikomas potencialias schemas. Tada Komisija turėtų būti įgaliota agentūros ENISA pasiūlytos potencialios schemos pagrindu patvirtinti Europos kibernetinio saugumo sertifikavimo schemą priimdama įgyvendinimo aktą. Atsižvelgiant į bendrąjį šio reglamento tikslą ir jame nustatytus saugumo tikslus, Komisijos patvirtintose Europos kibernetinio saugumo sertifikavimo schemose turėtų būti nustatyti būtiniausi individualios schemos elementai, susiję su dalyku, taikymo sritimi ir veikimu. Jie, be kita ko, turėtų apimti kibernetinio saugumo sertifikavimo taikymo sritį ir tikslą, taip pat sertifikuojamų IRT **procesų,** produktų ir paslaugų kategorijas, išsamius kibernetinio saugumo reikalavimus, pavyzdžiui, nurodant standartus ar technines specifikacijas, konkrečius vertinimo kriterijus ir vertinimo metodus bei numatomą saugumo užtikrinimo lygį, kuris gali būti bazinis, pakankamas ir (arba) aukštas**, taip pat, kai tinkama, vertinimo lygius**;

(56a) Europos sertifikavimo schemos saugumo užtikrinimo lygis – pagrindas, kuriuo remiantis patvirtinama, kad IRT procesas, produktas ar paslauga atitinka tam tikros Europos kibernetinio saugumo sertifikavimo schemos saugumo reikalavimus. Siekiant užtikrinti sistemos nuoseklumą sertifikuotų IRT procesų, produktų ir paslaugų atžvilgiu, Europos kibernetinio saugumo sertifikavimo schemoje galėtų būti apibrėžiami pagal tą schemą išduodamų Europos kibernetinio saugumo sertifikatų ir ES atitikties pareiškimų saugumo užtikrinimo lygiai. Kiekvienas sertifikatas galėtų patvirtinti vieną iš saugumo užtikrinimo lygių: bazinį, pakankamą arba aukštą, o ES atitikties pareiškimas galėtų patvirtinti tik bazinį saugumo užtikrinimo lygį. Saugumo užtikrinimo lygiais nustatomos atitinkamo lygio pastangos vertinimui atlikti […] ir apibūdinamos su jais susijusios techninės specifikacijos, standartai ir procedūros, įskaitant technines kontrolės priemones, kurių tikslas – sušvelninti kibernetinio saugumo incidentus arba užkirsti jiems kelią. Kiekvienas saugumo užtikrinimo lygis įvairiose sektorių srityse, kuriose taikomas sertifikavimas, turėtų būti nuoseklus;

(56b) Europos kibernetinio saugumo sertifikavimo schemoje gali būti nustatyti keli vertinimo lygiai, priklausomai nuo taikomos vertinimo metodikos griežtumo ir išsamumo; ši metodika turėtų atitikti vieną iš saugumo užtikrinimo lygių ir turėtų būti susieta su tinkamu saugumo užtikrinimo komponentų deriniu. Visų saugumo užtikrinimo lygių atveju IRT produktas ar paslauga turėtų turėti tam tikrų saugių funkcijų, kaip apibrėžta schemoje, kurios, be kita ko, gali būti šios: saugi standartinė konfigūracija, pasirašytasis kodas, saugus naujinimas ir galimybių pasinaudoti saugumo spragomis sumažinimas ir visiškos dėklo / masyvo atminties apsaugos priemonės. Šios funkcijos turėtų būti sukurtos ir palaikomos naudojant į saugumą orientuotus kūrimo metodus ir susijusias priemones, kad būtų užtikrintas patikimas veiksmingų mechanizmų (tiek programinės, tiek aparatinės įrangos) integravimas. Bazinio saugumo užtikrinimo lygio atveju atliekant vertinimą turėtų būti remiamasi bent šiais saugumo užtikrinimo komponentais: vertinimas turėtų apimti bent atitikties vertinimo įstaigos atliekamą IRT produkto ar paslaugos techninių dokumentų peržiūrą. Jei sertifikuojami IRT procesai, techninė peržiūra taip pat turėtų būti taikoma IRT produktų ar paslaugų projektavimo, kūrimo ir palaikymo procesui. Tais atvejais, kai Europos kibernetinio saugumo sertifikavimo schemoje numatoma galimybė pačiam gamintojui ar tiekėjui atlikti atitikties vertinimą, turėtų pakakti, kad pats gamintojas arba paslaugų teikėjas būtų atlikęs IRT procesų, produktų ar paslaugų atitikties sertifikavimo schemai vertinimą. Pakankamo saugumo užtikrinimo lygio atveju atliekant vertinimą, be bazinio saugumo užtikrinimo lygio komponentų turėtų būti remiamasi bent patikrinimu, ar IRT produkto ar paslaugos saugumo funkcinės galimybės atitinka jų techninius dokumentus. Aukšto saugumo užtikrinimo lygio atveju atliekant vertinimą, be pakankamo saugumo užtikrinimo lygio komponentų turėtų būti remiamasi bent efektyvumo bandymu, kuriuo įvertinamas IRT produkto ar paslaugos saugumo funkcinių galimybių atsparumas sudėtingų kibernetinių išpuolių, kuriuos vykdo aukšto lygio įgūdžių ir didelių išteklių turintys subjektai, rizikai;

(56c) rengdama potencialią schemą ENISA turėtų konsultuotis su visais susijusiais suinteresuotaisiais subjektais, tokiais kaip Europos standartizacijos organizacijos, susijusios nacionalinės valdžios institucijos, pagal tarpusavio pripažinimo susitarimus veikiančios organizacijos, pavyzdžiui, Vyresniųjų pareigūnų grupės informacinių sistemų saugumo klausimais (SOG-IS) tarpusavio pripažinimo susitarimas, MVĮ, vartotojų organizacijos, taip pat aplinkosaugos ir socialinės srities suinteresuotieji subjektai;

(56d) ENISA turėtų administruoti interneto svetainę, kurioje būtų teikiama informacija apie Europos kibernetinio saugumo sertifikavimo schemas ir jų reklama, kuri turėtų, be kita ko, apimti prašymus parengti potencialią Europos kibernetinio saugumo sertifikavimo schemą, taip pat parengiamuoju etapu ENISA vykdyto konsultacijų proceso metu gautą grįžtamąją informaciją. Tokioje interneto svetainėje taip pat turėtų būti teikiama informacija apie pagal šį reglamentą išduotus sertifikatus ir ES atitikties pareiškimus;

(57) Europos kibernetinio saugumo sertifikavimas **ir ES atitikties pareiškimas** turėtų likti savanoriški, išskyrus atvejus, kai Sąjungos ar **pagal Sąjungos teisę priimtuose** nacionalinės teisės aktuose numatyta kitaip. **Jeigu nėra suderintų teisės aktų, valstybės narės gali pagal Direktyvą (ES) 2015/1535 priimti nacionalines technines taisykles, kuriose būtų numatytas privalomas sertifikavimas pagal Europos kibernetinio saugumo sertifikavimo schemą. Valstybės narės taip pat galėtų pasinaudoti Europos kibernetinio saugumo sertifikavimu viešųjų pirkimų ir Direktyvos 2014/214/ES kontekste;**[...]

(57a) tačiau, siekiant įgyvendinti šio reglamento tikslus ir išvengti vidaus rinkos susiskaidymo, nacionalinės kibernetinio saugumo sertifikavimo schemos arba procedūros, taikomos IRT produktams ir paslaugoms, kuriems taikoma Europos kibernetinio saugumo sertifikavimo schema, turėtų nustoti galioti nuo Komisijos priimtu įgyvendinimo aktu nustatytos dienos. Be to, valstybės narės turėtų nenustatyti naujų nacionalinių sertifikavimo schemų, kuriose numatomos kibernetinio saugumo sertifikavimo schemos, skirtos IRT produktams ir paslaugoms, kuriems jau taikoma galiojanti Europos kibernetinio saugumo sertifikavimo schema. Vis dėlto valstybėms narėms turėtų būti netrukdoma priimti arba toliau taikyti nacionalines sertifikavimo schemas nacionalinio saugumo tikslais;

(58) patvirtinus Europos kibernetinio saugumo sertifikavimo schemą IRT produktų gamintojai arba IRT paslaugų teikėjai turėtų turėti galimybę teikti prašymą savo pasirinkai atitikties vertinimo įstaigai savo produktams arba paslaugoms sertifikuoti. Tam tikrus šiame reglamente nustatytus reikalavimus atitinkančias atitikties vertinimo įstaigas turėtų akredituoti akreditacijos įstaiga. Akreditacija turėtų būti suteikiama ne ilgesniam kaip penkerių metų laikotarpiui ir gali būti pratęsta tomis pačiomis sąlygomis, jei atitikties vertinimo įstaiga toliau vykdo reikalavimus. Akreditacijos įstaigos turėtų **apriboti, laikinai sustabdyti arba** panaikinti atitikties vertinimo įstaigos akreditaciją, jeigu akreditacijos sąlygos nevykdomos arba nebevykdomos arba jeigu veiksmais, kurių imasi atitikties vertinimo įstaiga, pažeidžiamas šis reglamentas;

(59) **[...]** valstybės narės **[...] turėtų** paskirti vieną **ar kelias** kibernetinio saugumo sertifikavimo [...] **institucijas**, kurios prižiūrėtų, kaip laikomasi **iš šio reglamento kylančių įpareigojimų**. **Jeigu valstybė narė mano tai esant tikslinga, užduotys gali būti pavedamos jau veikiančioms institucijoms. Be to, valstybės narės turėtų galėti abipusiu susitarimu su kita valstybe nare nuspręsti paskirti vieną ar kelias priežiūros institucijas tos kitos valstybės narės teritorijoje. Ta institucija visų pirma turėtų stebėti, kaip jų atitinkamoje teritorijoje įsisteigę IRT produktų gamintojai arba tiekėjai arba IRT paslaugų teikėjai vykdo su ES atitikties pareiškimu susijusius įpareigojimus, ir užtikrinti jų vykdymą, padėti nacionalinėms akreditacijos įstaigoms vykdyti atitikties vertinimo įstaigų atliekamą stebėsenos ir priežiūros veiklą teikdama joms ekspertines žinias ir atitinkamą informaciją, įgalioti atitikties vertinimo įstaigas atlikti užduotis, kai jos tenkina papildomus schemoje nustatytus reikalavimus, ir stebėti svarbius pokyčius kibernetinio saugumo sertifikavimo srityje** [...]. Nacionalinės **kibernetinio saugumo** sertifikavimo [...] institucijos turėtų nagrinėti fizinių ar juridinių asmenų pateiktus skundus, susijusius su **jų** išduotais sertifikatais **arba atitikties vertinimo įstaigų išduotais sertifikatais, patvirtinančiais aukštą saugumo užtikrinimo lygį**[...], tirti, kiek tinkama, skundo dalyką ir per pagrįstą laikotarpį informuoti skundo teikėją apie tyrimo eigą ir rezultatus. Be to, jos turėtų bendradarbiauti su kitomis nacionalinėmis **kibernetinio saugumo** sertifikavimo [...] institucijomis ar kitomis valdžios institucijomis, be kita ko, dalydamosi informacija apie galimą IRT produktų ir paslaugų neatitiktį šio reglamento arba konkrečių kibernetinio saugumo schemų reikalavimams;

(60) siekiant užtikrinti nuoseklų Europos kibernetinio saugumo sertifikavimo sistemos taikymą reikėtų įsteigti iš nacionalinių **kibernetinio saugumo** sertifikavimo [...] institucijų **arba kitų atitinkamų nacionalinių institucijų atstovų** sudarytą Europos kibernetinio saugumo sertifikavimo grupę (toliau – grupė). Pagrindinės grupės užduotys turėtų būti konsultuoti Komisiją ir padėti jai užtikrinti nuoseklų Europos kibernetinio saugumo sertifikavimo sistemos įgyvendinimą ir taikymą, padėti Agentūrai ir glaudžiai su ja bendradarbiauti rengiant potencialias kibernetinio saugumo sertifikavimo schemas, rekomenduoti, kad Komisija paprašytų Agentūros parengti potencialią Europos kibernetinio saugumo sertifikavimo schemą ir priimti **Agentūrai** skirtas nuomones **dėl potencialių schemų ir** Komisijai skirtas nuomones, susijusias su esamų Europos kibernetinio saugumo sertifikavimo schemų palaikymas ir peržiūra;

(60a) grupė turėtų sudaryti palankesnes sąlygas nacionalinėms kibernetinio saugumo sertifikavimo institucijoms, atsakingoms už atitikties vertinimo įstaigų įgaliojimą ir sertifikatų išdavimą, keistis gerosios patirties pavyzdžiais ir ekspertinėmis žiniomis. Grupė turėtų remti tarpusavio vertinimo mechanizmo rengimą potencialios schemos kūrimo kontekste ir jo įdiegimą įstaigose, išduodančiose aukštą saugumo užtikrinimo lygį patvirtinančius Europos kibernetinio saugumo sertifikatus. Atliekant tokius tarpusavio vertinimus visų pirma turėtų būti įvertinama, ar atitinkamos įstaigos turi tinkamų ekspertinių žinių ir suderintai vykdo savo užduotis. Tarpusavio vertinimų rezultatai turėtų būti skelbiami viešai. Šios įstaigos gali patvirtinti atitinkamas savo praktikos ir ekspertinių žinių pritaikymo priemones;

(61) siekdama padidinti informuotumą ir būsimų ES kibernetinio saugumo schemų priimtinumą, Europos Komisija gali parengti bendras arba konkrečiam sektoriui skirtas kibernetinio saugumo rekomendacijas, pvz., dėl geros kibernetinio saugumo praktikos, arba atsakingo saugaus elgesio kibernetinėje erdvėje, ir pabrėžti teigiamą sertifikuotų IRT produktų ir paslaugų naudojimo poveikį;

(61a) siekiant dar labiau palengvinti prekybą ir pripažįstant, kad IRT tiekimo grandinės yra pasaulinio masto, pagal SESV 218 straipsnį Sąjunga gali sudaryti susitarimus dėl pagal Europos kibernetinio saugumo sertifikavimo sistemą nustatytas schemas išduotų tarpusavio sertifikatų pripažinimo. Komisija, atsižvelgdama į ENISA ir Europos kibernetinio saugumo sertifikavimo grupės nuomonę, gali rekomenduoti pradėti atitinkamas derybas. Kiekvienoje schemoje turėtų būti nustatytos konkrečios tarpusavio pripažinimo sąlygos su trečiosiomis šalimis;

(62) […]

(63) […]

(64) siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai, kai tai numatyta šiuo reglamentu. Tais įgaliojimais turėtų būti naudojamasi laikantis Reglamento (ES) Nr. 182/2011;

(65) turėtų būti naudojama nagrinėjimo procedūra siekiant priimti įgyvendinimo aktus dėl IRT produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo schemų, dėl Agentūros atliekamų tyrimų tvarkos, taip pat dėl aplinkybių, formatų ir procedūrų, susijusių su nacionalinių **kibernetinio saugumo** sertifikavimo [...] institucijų pranešimu Komisijai apie akredituotas atitikties vertinimo įstaigas;

(66) Agentūros veikla turėtų būti vertinama nepriklausomai. Atliekant vertinimą turėtų būti atsižvelgiama į Agentūros tikslų siekimą, jos darbo metodus ir jos užduočių aktualumą. Atliekant vertinimą taip pat turėtų būti įvertintas Europos kibernetinio saugumo sertifikavimo sistemos poveikis, veiksmingumas ir efektyvumas;

(67) Reglamentas (ES) Nr. 526/2013 turėtų būti panaikintas;

(68) kadangi šio reglamento tikslų valstybės narės negali deramai pasiekti, bet jų geriau siekti Sąjungos lygmeniu, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali priimti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šiuo reglamentu neviršijama to, kas būtina nurodytam tikslui pasiekti,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I ANTRAŠTINĖ DALIS
BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

1. Siekiant užtikrinti tinkamą vidaus rinkos veikimą ir kartu aukštą kibernetinio saugumo lygį, kibernetinį atsparumą ir pasitikėjimą Sąjungoje, šiame reglamente:

a) išdėstomi [...] **Europos Sąjungos kibernetinio saugumo** agentūros ENISA (toliau – Agentūra) tikslai, užduotys ir organizaciniai aspektai ir

b) nustatoma Europos kibernetinio saugumo sertifikavimo schemų nustatymo sistema, siekiant Sąjungoje užtikrinti tinkamą IRT **procesų,** produktų ir paslaugų kibernetinio saugumo lygį. Tokia sistema taikoma nepažeidžiant tam tikrų kitų Sąjungos aktų nuostatų dėl savanoriško arba privalomo sertifikavimo.

2. **Šis reglamentas nedaro poveikio valstybių narių kompetencijai kibernetinio saugumo srityje ir bet kuriuo atveju nedaro poveikio veiklai, susijusiai su visuomenės saugumu, gynyba, nacionaliniu saugumu, ir valstybės veiklai baudžiamosios teisės srityse.**

2 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) kibernetinis saugumas – bet kurios rūšies veikla, būtina tinklų ir informacinėms sistemoms, jų vartotojams ir susijusiems asmenims nuo kibernetinių grėsmių apsaugoti;

2) tinklų ir informacinė sistema – sistema, apibrėžta Direktyvos (ES) 2016/1148 4 straipsnio 1 punkte;

3) nacionalinė tinklų ir informacinių sistemų saugumo strategija – sistema, apibrėžta Direktyvos (ES) 2016/1148 4 straipsnio 3 punkte;

4) esminių paslaugų operatorius – viešojo arba privačiojo sektoriaus subjektas, apibrėžtas Direktyvos (ES) 2016/1148 4 straipsnio 4 punkte;

5) skaitmeninių paslaugų teikėjas – juridinis asmuo, kuris teikia skaitmenines paslaugas, apibrėžtas Direktyvos (ES) 2016/1148 4 straipsnio 6 punkte;

6) incidentas – įvykis, apibrėžtas Direktyvos (ES) 2016/1148 4 straipsnio 7 punkte;

7) incidentų valdymas – bet kuri procedūra, apibrėžta Direktyvos (ES) 2016/1148 4 straipsnio 8 punkte;

8) kibernetinė grėsmė – galima aplinkybė arba įvykis, kuris gali **pažeisti, sutrikdyti arba kitaip** neigiamai paveikti tinklų ir informacines sistemas, jų naudotojus ir susijusius asmenis;

9) Europos kibernetinio saugumo sertifikavimo schema – išsamus taisyklių, techninių reikalavimų, standartų ir procedūrų, nustatytų Sąjungos lygmeniu, rinkinys, taikomas informacinių ir ryšių technologijų (IRT) **procesų,** produktų ir paslaugų, kuriems taikoma ta konkreti schema, sertifikavimui **arba atitikties vertinimui**;

9a) nacionalinė kibernetinio saugumo sertifikavimo schema – išsamus taisyklių, techninių reikalavimų, standartų ir procedūrų, kuriuos parengė ir priėmė nacionalinė valdžios institucija, rinkinys, taikomas IRT procesų, produktų ir paslaugų, kuriems taikoma ta konkreti schema, sertifikavimui arba atitikties vertinimui;

10) Europos kibernetinio saugumo sertifikatas – [...] dokumentas, kuriuo patvirtinama, kad tam tikras IRT **procesas,** produktas arba paslauga [...] **buvo įvertinti dėl atitikties** Europos kibernetinio saugumo sertifikavimo schemoje nustatytiems konkretiems **saugumo** reikalavimams;

11) IRT produktas [...] – bet kuris tinklų ir informacinių sistemų elementas arba elementų grupė;

11a) IRT paslauga – paslauga, kurią visą arba jos dalį sudaro informacijos perdavimas, saugojimas, gavimas arba tvarkymas naudojantis tinklų ir informacinėmis sistemomis;

11b) IRT procesas – veikla, vykdoma siekiant projektuoti, kurti, pateikti ir palaikyti IRT produktą ar paslaugą;

12) akreditavimas – akreditavimas, apibrėžtas Reglamento (EB) Nr. 765/2008 2 straipsnio 10 punkte;

13) nacionalinė akreditacijos įstaiga – nacionalinė akreditacijos įstaiga, apibrėžta Reglamento (EB) Nr. 765/2008 2 straipsnio 11 punkte;

14) atitikties vertinimas – atitikties vertinimas, apibrėžtas Reglamento (EB) Nr. 765/2008 2 straipsnio 12 punkte;

15) atitikties vertinimo įstaiga – atitikties vertinimo įstaiga, apibrėžta Reglamento (EB) Nr. 765/2008 2 straipsnio 13 punkte;

16) standartas – standartas, apibrėžtas Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkte**;**

16a) techninė specifikacija – dokumentas, kuriame nustatyti techniniai reikalavimai, kuriuos turi atitikti IRT procesas, produktas ar paslauga;

16b) saugumo užtikrinimo lygis – pagrindas, kuriuo remiantis patvirtinama, kad IRT procesas, produktas ar paslauga atitinka tam tikros Europos kibernetinio saugumo sertifikavimo schemos saugumo reikalavimus, ir nurodoma, kokiu lygiu tai buvo įvertinta; saugumo užtikrinimo lygiu nevertinamas paties IRT proceso, produkto ar paslaugos saugumas.

II ANTRAŠTINĖ DALIS

ENISA – *[...] Europos Sąjungos kibernetinio saugumo agentūra*

I SKYRIUS

ĮGALIOJIMAI IR */...* TIKSLAI */...*

3 straipsnis

Įgaliojimai

1. Agentūra prisiima jai šiuo reglamentu paskirtas užduotis, kad padėtų užtikrinti aukštą Sąjungos kibernetinio saugumo lygį [...] **visoje** Sąjungoje, **visų pirma padėdama valstybėms narėms ir Sąjungos institucijoms, agentūroms ir įstaigoms gerinti kibernetinį saugumą. Agentūra veikia kaip informacinis centras teikdama konsultacijas ir ekspertines žinias Sąjungos institucijoms, agentūroms ir įstaigoms kibernetinio saugumo klausimais.**

2. Agentūra vykdo užduotis, kurios jai paskirtos Sąjungos aktais, kuriais nustatytos valstybių narių įstatymų ir kitų teisės aktų, susijusių su kibernetiniu saugumu, suderinimas.

2a. Vykdydama savo užduotis Agentūra veikia nepriklausomai ir kuo labiau atsižvelgia į valstybių narių atitinkamų institucijų nacionalines ekspertines žinias, kartu vengdama veiklos dubliavimo.

3. […]

4 straipsnis

Tikslai

1. Būdama nepriklausoma, teikdama kokybiškas mokslines ir technines konsultacijas, pagalbą ir informaciją, užtikrindama savo operacinių procedūrų ir veiklos būdų skaidrumą bei uoliai vykdydama savo užduotis, Agentūra veikia kaip kibernetinio saugumo kompetencijos centras.

2. Agentūra padeda Sąjungos institucijoms, agentūroms ir įstaigoms, taip pat valstybėms narėms rengti ir įgyvendinti su kibernetiniu saugumu susijusią **Sąjungos** politiką**, įskaitant sektorių kibernetinio saugumo srities politiką.**

3. Agentūra visoje Sąjungoje remia pajėgumų stiprinimą ir pasirengimą, padėdama Sąjungos **institucijoms, agentūroms ir įstaigoms**, **taip pat** valstybėms narėms ir viešiesiems bei privatiesiems suinteresuotiesiems subjektams didinti savo tinklų ir informacinių sistemų apsaugą ir plėtoti **bei gerinti kibernetinį atsparumą ir reagavimo pajėgumus, taip pat plėtoti** įgūdžius ir gebėjimus kibernetinio saugumo srityje [...].

4. Agentūra skatina valstybes nares, Sąjungos institucijas, agentūras ir įstaigas bei susijusius **privačiojo ir viešojo sektorių** suinteresuotuosius subjektus [...] bendradarbiauti ir koordinuoti su kibernetiniu saugumu susijusius klausimus Sąjungos lygmeniu.

5. Agentūra **prisideda prie** [...] Sąjungos lygmens kibernetinio saugumo pajėgumų **didinimo**, kad [...] **padėtų** valstybėms narėms [...] užkirsti kelią kibernetinėms grėsmėms ir reaguoti į jas, visų pirma tarpvalstybinių incidentų atveju.

6. Agentūra skatina sertifikavimo naudojimą **siekiant išvengti sertifikavimo schemų susiskaidymo Europos Sąjungoje. Visų pirma Agentūra** [...] **prisideda** prie Sąjungos lygmens kibernetinio saugumo sertifikavimo sistemos sukūrimo ir taikymo pagal šio reglamento III antraštinę dalį, siekiant didinti IRT produktų ir paslaugų kibernetinio saugumo užtikrinimo skaidrumą ir taip sustiprinti pasitikėjimą skaitmenine vidaus rinka.

7. Agentūra skatina aukšto lygio piliečių ir įmonių informavimą apie kibernetinį saugumą.

IA SKYRIUS
UŽDUOTYS

5 straipsnis

[...] Sąjungos politikos ir teisės formavimas ir įgyvendinimas

Agentūra padeda formuoti ir įgyvendinti Sąjungos politiką ir teisę:

1. padėdama ir konsultuodama, ypač teikdama nepriklausomą nuomonę ir atlikdama parengiamąjį darbą, susijusį su Sąjungos politikos ir teisės plėtojimu ir peržiūra kibernetinio saugumo srityje, taip pat su konkretiems sektoriams skirtomis politikos ir teisės iniciatyvomis, susijusiomis su kibernetinio saugumo klausimais;

2. padėdama valstybėms narėms nuosekliai įgyvendinti Sąjungos politiką ir teisės aktus, susijusius su kibernetiniu saugumu, visų pirma Direktyvą (ES) 2016/1148, be kita ko, teikdama nuomones, gaires, konsultuodama ir dalydamasi geriausia patirtimi tokiais klausimais, kaip rizikos valdymas, pranešimai apie incidentus ir keitimasis informacija, taip pat sudarydama kompetentingoms institucijoms palankias sąlygas keistis susijusia geriausia patirtimi;

3. prisidėdama prie Bendradarbiavimo grupės veiklos pagal Direktyvos (ES) 2016/1148 11 straipsnį ir teikdama ekspertines žinias ir pagalbą;

4. remdama:

    1) elektroninės atpažinties ir patikimumo užtikrinimo paslaugų srities Sąjungos politikos plėtojimą ir įgyvendinimą, visų pirma teikdama konsultacijas ir technines gaires, taip pat sudarydama kompetentingoms institucijoms palankias sąlygas keistis geriausia patirtimi;

    2) didesnio elektroninių ryšių saugumo propagavimą, įskaitant ekspertinių žinių teikimą ir konsultavimą, taip pat sudarydama kompetentingoms institucijoms palankias sąlygas keistis geriausia patirtimi;

5. remdama nuolatinę Sąjungos politinės veiklos peržiūrą, teikdama metinę atitinkamos teisinės sistemos įgyvendinimo padėties ataskaitą, susijusią su:

    a) pranešimais apie incidentus valstybėse narėse, kuriuos bendrieji informaciniai centrai teikia Bendradarbiavimo grupei pagal Direktyvos (ES) 2016/1148 10 straipsnio 3 dalį;

    b) iš patikimumo užtikrinimo paslaugų teikėjų gautais pranešimais apie saugumo ir vientisumo pažeidimą, kuriuos priežiūros įstaigos pateikė Agentūrai pagal Reglamento (ES) Nr. 910/2014 19 straipsnio 3 dalį;

    c) viešųjų ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjų perduotais pranešimais apie saugumo [...] **incidentus**, kuriuos kompetentingos institucijos pateikė Agentūrai pagal [Direktyvos, kuria nustatomas Europos elektroninių ryšių kodeksas] 40 straipsnį.

6 straipsnis

[...] ***Pajėgumų stiprinimas***

1. Agentūra padeda:

a) valstybėms narėms gerinti kibernetinių [...] **grėsmių** [...] ir incidentų prevencijos, nustatymo, analizės ir reagavimo į juos pajėgumus, suteikdama joms reikiamų ekspertinių ir kitų žinių;

b) Sąjungos institucijoms, [...] agentūroms **ir įstaigoms** gerinti kibernetinių [...] **grėsmių** [...] ir incidentų prevencijos, nustatymo, analizės ir reagavimo į juos pajėgumus, **visų pirma** tinkamai remdama Sąjungos institucijų, agentūrų ir įstaigų kompiuterinių incidentų tyrimo tarnybos (CERT-EU) veiklą;

c) valstybėms narėms – jų prašymu – suformuoti nacionalines reagavimo į kompiuterinius saugumo incidentus tarnybas (CSIRT) pagal Direktyvos (ES) 2016/1148 9 straipsnio 5 dalį;

d) valstybėms narėms – jų prašymu – parengti nacionalines tinklų ir informacinių sistemų saugumo strategijas pagal Direktyvos (ES) 2016/1148 7 straipsnio 2 dalį. Siekdama populiarinti geriausią patirtį, Agentūra taip pat skatina visoje Sąjungoje tų strategijų sklaidą ir stebi jų įgyvendinimo pažangą;

e) Sąjungos institucijoms rengti ir peržiūrėti Sąjungos kibernetinio saugumo strategijas, skatinti jų sklaidą ir stebėti jų įgyvendinimo pažangą;

f) nacionalinėms ir Sąjungos CSIRT didinti pajėgumus, taip pat skatindama palaikyti dialogą ir keistis informacija, kad būtų užtikrinta, jog, atsižvelgdama į naujausius technikos laimėjimus, kiekviena CSIRT turėtų būtiniausius bendrus pajėgumus ir vykdytų veiklą vadovaudamasi geriausia praktika;

g) valstybėms narėms, **reguliariai** [...] Sąjungos lygmeniu organizuodama didelio masto kibernetinio saugumo pratybas, nurodytas 7 straipsnio 6 dalyje, ir teikdama politines rekomendacijas, pagrįstas pratybų vertinimu ir po jų padarytomis išvadomis;

h) atitinkamoms viešosioms įstaigoms, siūlydama mokymus kibernetinio saugumo srityje, prireikus bendradarbiaudama su suinteresuotaisiais subjektais;

i) Bendradarbiavimo grupei, pagal Direktyvos (ES) 2016/1148 11 straipsnio 3 dalies l punktą [...]**keičiantis** geriausia praktika, susijusia su valstybių narių vykdomu esminių paslaugų operatorių identifikavimu, be kita ko, susijusiu su valstybių tarpusavio priklausomybe rizikos ir incidentų atveju.

2. Agentūra **remia dalijimąsi informacija sektoriuose ir tarp sektorių** [...], visų pirma išvardytųjų Direktyvos (ES) 2016/1148 II priede, dalydamasi geriausia patirtimi ir teikdama rekomendacijas dėl esamų priemonių ir procedūrų, taip pat rekomendacijas, kaip spręsti su dalijimusi informacija susijusius reguliavimo klausimus.

7 straipsnis

[...] ***Operatyvinis bendradarbiavimu Sąjungos lygmeniu***

1. Agentūra remia **valstybių narių, Sąjungos institucijų, agentūrų ir** [...] įstaigų, taip pat suinteresuotųjų subjektų operatyvinį bendradarbiavimą.

2. Agentūra operatyviniu lygmeniu bendradarbiauja su Sąjungos institucijomis, [...] agentūromis **ir įstaigomis**, įskaitant CERT-EU, tarnybas, atsakingas už kovą su elektroniniais nusikaltimais, ir priežiūros institucijas, atsakingas už privačių bei asmens duomenų apsaugą, ir užtikrina jų sąveiką, siekdama spręsti visuotinai svarbius klausimus, įskaitant:

a) keitimąsi praktine patirtimi ir geriausia praktika;

b) konsultavimą ir gairių teikimą su kibernetiniu saugumu susijusiais aktualiais klausimais;

c) praktinės konkrečių užduočių atlikimo tvarkos nustatymą pasikonsultavus su Komisija.

3. Agentūra vykdo CSIRT tinklo sekretoriato funkciją pagal Direktyvos (ES) 2016/1148 12 straipsnio 2 dalį ir **vykdydama šią funkciją** [...] padeda jo nariams tarpusavyje dalytis informacija ir bendradarbiauti.

4. Agentūra **remia** [...] operatyvinį bendradarbiavimą su CSIRT tinklo dalyviais, teikdama šią paramą valstybėms narėms **joms paprašius**:

a) patardama, kaip gerinti incidentų prevencijos, nustatymo ir reagavimo į juos pajėgumus;

b) [...] **palengvindama** [...] didelį arba esminį poveikį turinčių incidentų techninį **suvaldymą, be kita ko, visų pirma remdama valstybių narių savanorišką dalijimąsi techniniais sprendimais**;

c) analizuodama pažeidžiamumą [...] ir incidentus**;**

ca) teikdama paramą *ex post* techniniams didelį arba esminį poveikį turinčių incidentų tyrimams pagal Direktyvą (ES) 2016/1148.

Atlikdama šias užduotis Agentūra ir CERT-EU struktūriškai bendradarbiauja, kad pasinaudotų sinergija **ir išvengtų veiklos dubliavimo** [...].

5. […]

[…]

6. Agentūra [...] **reguliariai** Sąjungos lygmeniu organizuoja kibernetinio saugumo pratybas ir padeda jas organizuoti valstybėms narėms, ES institucijoms, agentūroms bei įstaigoms, kai jos to paprašo. **Tokios pratybos Sąjungos lygmeniu gali apimti techninius, operatyvinius arba strateginius elementus.** [...] **Kas dvejus metus organizuojamos didelio masto pratybos, apimsiančios visus tuos elementus.** Agentūra taip pat prisideda prie sektorinių kibernetinio saugumo pratybų ir prireikus padeda jas organizuoti kartu su susijusiomis [...] **organizacijomis, kurios** taip pat **gali** dalyvauti Sąjungos lygmens kibernetinio saugumo pratybose.

7. Agentūra, **glaudžiai bendradarbiaudama su valstybėmis narėmis,** reguliariai rengia ES kibernetinio saugumo techninės padėties ataskaitą, kurioje apžvelgiami incidentai ir grėsmės ir kuri grindžiama viešųjų šaltinių informacija, pačios Agentūros atliekama analize ir ataskaitomis, kurias Agentūrai, be kitų subjektų, pateikė valstybių narių CSIRT [...] arba pagal TIS direktyvą įsteigti bendrieji informaciniai centrai (**tiek vieni, tiek kiti – savanoriškai** [...]), Europolo Europos kovos su elektroniniu nusikalstamumu centras (EC3), CERT-EU.

8. Agentūra padeda Sąjungos ir valstybių narių lygmeniu rengti koordinuotą atsaką į didelio masto tarpvalstybinius kibernetinio saugumo incidentus arba krizes, daugiausia:

   a) apibendrindama **savanoriškai pateiktas** nacionalinių šaltinių ataskaitas, kad padėtų užtikrinti bendrą informuotumą apie padėtį;

   b) užtikrindama galimybę CSIRT tinklui ir techninius bei politinius sprendimus priimantiems subjektams Sąjungos lygmeniu veiksmingai keistis informacija ir suteikdama jiems eskalavimo mechanizmus;

c) [...] **valstybėms narėms paprašius, palengvindama** techninį incidento arba krizės valdymą, [...] be kita ko, **visų pirma remdama** valstybių narių **savanorišką** dalijimąsi techniniais sprendimais;

d) remdama **ES institucijų, agentūrų ir įstaigų, o valstybėms narėms paprašius – ir valstybių narių** su incidentu arba krize susijusių viešųjų ryšių veiklą;

e) **valstybėms narėms paprašius padėdama** išbandy**ti** [...] bendradarbiavimo reaguojant į tokius incidentus arba krizes planus.

8 straipsnis

[...] ***Rinka, kibernetinio saugumo sertifikavimas ir standartizavimas***

Agentūra:

a) remia ir skatina Sąjungos IRT **procesų,** produktų ir paslaugų kibernetinio saugumo sertifikavimo politikos plėtojimą ir įgyvendinimą, kaip nustatyta šio reglamento III antraštinėje dalyje:

1) rengdama potencialias IRT **procesų,** produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo schemas **bendradarbiaudama su sektoriumi ir** pagal šio reglamento 44 straipsnį;

2) padėdama Komisijai teikti sekretoriato paslaugas Europos kibernetinio saugumo sertifikavimo grupei pagal šio reglamento 53 straipsnį;

3) rengdama ir skelbdama gaires ir formuodama gerąją patirtį, susijusią su IRT produktų ir paslaugų kibernetinio saugumo reikalavimais, bendradarbiaudama su nacionalinėmis **kibernetinio saugumo** sertifikavimo [...] institucijomis ir sektoriaus atstovais;

3a) [...] **tais atvejais, kai standartų nėra – rekomenduodama atitinkamas technines specifikacijas, skirtas Europos kibernetinio saugumo sertifikavimo schemoms kurti, kaip nurodyta 47 straipsnio 1 dalies b punkte**;

3b) **prisidėdama prie pakankamų pajėgumų stiprinimo, susijusio su vertinimo ir sertifikavimo procesais: rengdama ir skelbdama gaires, taip pat teikdama paramą valstybėms narėms joms paprašius;**

b) padeda nustatyti ir įgyvendinti Europos ir tarptautinius rizikos valdymo ir IRT **procesų,** produktų ir paslaugų saugumo standartus [...]**;**

ba) taip pat bendradarbiaudama su valstybėmis narėmis parengia rekomendacijas ir gaires dėl techninių sričių, susijusių su saugumo reikalavimais esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams, taip pat dėl jau galiojančių standartų, įskaitant valstybių narių nacionalinius standartus, pagal Direktyvos (ES) 2016/1148 19 straipsnio 2 dalį;

c) reguliariai analizuoja pagrindines kibernetinio saugumo rinkos paklausos ir pasiūlos tendencijas ir skleidžia informaciją apie jas, siekdama remti kibernetinio saugumo rinką Sąjungoje.

9 straipsnis

[...] ***Žinios ir informavimas*** [...]

Agentūra:

a) analizuoja naujausias technologijas ir teikia teminius vertinimus, susijusius su numatomu kibernetinio saugumo srities technologinių inovacijų visuomeniniu, teisiniu, ekonominiu ir reguliavimo poveikiu;

b) atlieka ilgalaikę strateginę kibernetinio saugumo grėsmių ir incidentų analizę, kad galėtų nustatyti naujausias tendencijas ir padėtų užkirsti kelią [...] kibernetinio saugumo **incidentams**;

c) bendradarbiaudama su ekspertais iš valstybių narių institucijų, pateikia tinklų ir informacinių sistemų, visų pirma [...] infrastruktūros, kuria naudojasi Direktyvos (ES) 2016/1148 II priede išvardyti sektoriai **ir tos direktyvos III priede išvardyti skaitmeninių paslaugų teikėjai,** saugumo užtikrinimo rekomendacijų, gairių ir geriausią praktiką;

d) renka, telkia informaciją apie kibernetinį saugumą, kurią pateikė Sąjungos institucijos, agentūros ir įstaigos, **o savanoriškai – valstybės narės ir privačiojo bei viešojo sektorių suinteresuotieji subjektai,** ir pateikia ją specialiame portale visuomenei susipažinti;

e) […]

f) renka ir analizuoja viešai prieinamą informaciją apie didelius incidentus, taip pat rengia ataskaitas, siekdama visoje Sąjungoje teikti rekomendacijas įmonėms ir piliečiams;

g) […].

9a straipsnis

Informuotumo didinimas ir švietimas

Agentūra:

a) didina visuomenės informuotumą apie kibernetinio saugumo riziką ir teikia piliečiams bei organizacijoms skirtas atskirų naudotojų gerosios patirties rekomendacijas;

b) bendradarbiaudama su valstybėmis narėmis ir Sąjungos institucijomis, agentūromis, įstaigomis ir sektoriaus atstovais, reguliariai organizuoja informavimo kampanijas, kuriomis siekiama didinti kibernetinį saugumą ir šios problemos matomumą Sąjungoje;

c) remia valstybių narių pastangas didinti informuotumą apie kibernetinį saugumą ir skatinti švietimą kibernetinio saugumo klausimais;

d) remia glaudesnį valstybių narių veiksmų koordinavimą ir keitimąsi geriausios patirties pavyzdžiais su kibernetiniu saugumu susijusio švietimo ir informuotumo didinimo srityje, padėdama sukurti ir palaikyti nacionalinių švietimo informacinių centrų tinklą.

10 straipsnis

*[...] **Moksliniai tyrimai ir inovacijos***

Mokslinių tyrimų ir inovacijų srityje Agentūra:

a) konsultuoja Sąjungą ir valstybes nares dėl poreikio atlikti mokslinius tyrimus kibernetinio saugumo srityje ir dėl šios srities prioritetų, siekiant sudaryti sąlygas veiksmingai reaguoti į esamą ir naują riziką bei grėsmes, įskaitant susijusias su naujomis ir kuriamomis informacinėmis ir ryšių technologijomis, bei veiksmingai taikyti rizikos prevencijos technologijas;

b) jei Komisija yra delegavusi Agentūrai atitinkamus įgaliojimus, ši dalyvauja mokslinių tyrimų ir inovacijų finansavimo programų įgyvendinimo etape arba kaip gavėja.

11 straipsnis

*[...]**Tarptautinis bendradarbiavimas***

Agentūra padeda Sąjungai bendradarbiauti su trečiosiomis šalimis ir tarptautinėmis organizacijomis, kad būtų skatinamas tarptautinis bendradarbiavimas kibernetinio saugumo klausimais:

a) prireikus, būdama stebėtoja organizuojant tarptautines pratybas, ir analizuodama tokių pratybų rezultatus ir teikdama Valdančiajai tarybai jų ataskaitas;

b) [...]**atitinkamose tarptautinio bendradarbiavimo sistemose** sudarydama palankesnes sąlygas keistis geriausia patirtimi[...];

c) Komisijai paprašius, teikdama Komisijai ekspertines žinias**;**

ca) bendradarbiaujant su pagal 53 straipsnį įsteigta Europos kibernetinio saugumo sertifikavimo grupe teikdama rekomendacijas ir paramą Komisijai klausimais, susijusiais su susitarimais dėl kibernetinio saugumo sertifikatų savitarpio pripažinimo su trečiosiomis šalimis.

II SKYRIUS
AGENTŪROS ORGANIZACINĖ STRUKTŪRA

12 straipsnis

Struktūra

Agentūros administracinę ir valdymo struktūrą sudaro:

a) Valdančioji taryba, atliekanti 14 straipsnyje nustatytas funkcijas;

b) Vykdomoji valdyba, atliekanti 18 straipsnyje nustatytas funkcijas;

c) vykdomasis direktorius, atliekantis 19 straipsnyje nustatytas pareigas;[...]

d) nuolatinė suinteresuotųjų subjektų grupė, atliekanti 20 straipsnyje nustatytas funkcijas**;**

da) nacionalinių ryšių palaikymo pareigūnų tinklas, atliekantis 20a straipsnyje nustatytas funkcijas.

1 SKIRSNIS
VALDANČIOJI TARYBA

13 straipsnis

Valdančiosios tarybos sudėtis

1. Valdančiąją tarybą sudaro po vieną kiekvienos valstybės narės atstovą ir du Komisijos paskirti atstovai. Kiekvienas narys turi balsavimo teisę.

2. Kiekvienas Valdančiosios tarybos narys turi pakaitinį narį, kuris atstovauja nariui šiam nedalyvaujant.

3. Valdančiosios tarybos nariai ir jų pakaitiniai nariai skiriami atsižvelgiant į jų žinias kibernetinio saugumo srityje, taip pat į valdymo, administracinio darbo ir biudžeto valdymo įgūdžius. Komisija ir valstybės narės deda pastangas apriboti savo atstovų Valdančiojoje taryboje kaitą, siekiant užtikrinti jos veiklos tęstinumą. Komisija ir valstybės narės siekia užtikrinti vyrų ir moterų atstovavimo pusiausvyrą Valdančiojoje taryboje.

4. Valdančiosios tarybos narių ir jų pakaitinių narių kadencija – ketveri metai. Ta kadencija gali būti pratęsta.

14 straipsnis

Valdančiosios tarybos funkcijos

1. Valdančioji taryba:

a) apibrėžia bendrą Agentūros veiklos kryptį ir taip pat užtikrina, kad Agentūra veiktų pagal šiame reglamente nustatytas taisykles ir principus. Ji taip pat užtikrina, kad Agentūros darbas būtų suderinamas su valstybių narių ir Sąjungos lygmeniu vykdoma veikla;

b) priima 21 straipsnyje nurodyto Agentūros bendrojo programavimo dokumento projektą iki jis pateikiamas Komisijos nuomonei gauti;

c) atsižvelgdama į Komisijos nuomonę, dviejų trečdalių narių balsų dauguma ir pagal 17 straipsnį priima Agentūros bendrąjį programavimo dokumentą;

ca) prižiūri į bendrąjį programavimo dokumentą įtrauktų daugiamečių ir metinių veiklos programų įgyvendinimą;

d) dviejų trečdalių narių balsų dauguma priima Agentūros metinį biudžetą ir vykdo kitas su Agentūros biudžetu susijusias funkcijas pagal III skyrių;

e) įvertina ir priima konsoliduotą metinę Agentūros veiklos ataskaitą ir ne vėliau kaip kitų metų liepos 1 d. pateikia tą ataskaitą ir jos vertinimą Europos Parlamentui, Tarybai, Komisijai ir Audito Rūmams. Metinę ataskaitą sudaro finansinės ataskaitos ir joje aprašoma, kaip Agentūra pasiekė savo veiklos rezultatų rodiklius. Metinė ataskaita skelbiama viešai;

f) vadovaudamasi 29 straipsniu priima Agentūrai taikomas finansines taisykles;

g) atsižvelgdama į įgyvendintinų priemonių ekonominės naudos analizę, priima kovos su sukčiavimu strategiją, kuri proporcingai atitinka sukčiavimo riziką;

h) priima savo narių interesų konfliktų prevencijos ir valdymo taisykles;

i) užtikrina, kad būtų imtasi tinkamų tolesnių priemonių atsižvelgiant į Europos kovos su sukčiavimu tarnybos (OLAF) tyrimų ir įvairiose vidaus ar išorės audito ataskaitose bei vertinimuose pateiktas išvadas ir rekomendacijas;

j) priima savo darbo tvarkos taisykles;

k) laikydamasi 2 dalies nuostatų Agentūros darbuotojų atžvilgiu naudojasi įgaliojimais, kurie paskyrimų tarnybai ir tarnybai, įgaliotai sudaryti darbo sutartis, suteikti pagal Tarnybos nuostatus ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygas (toliau – paskyrimų tarnybos įgaliojimai);

l) priima Tarnybos nuostatų ir kitų tarnautojų įdarbinimo sąlygų įgyvendinimo taisykles laikydamasi Tarnybos nuostatų 110 straipsnyje numatytos tvarkos;

m) skiria vykdomąjį direktorių ir prireikus pratęsia jo kadenciją arba pašalina jį iš pareigų pagal šio reglamento 33 straipsnį;

n) skiria apskaitos pareigūną, kuris gali būti Komisijos apskaitos pareigūnas, kuris eidamas savo pareigas yra visiškai nepriklausomas;

o) atsižvelgdama į Agentūros veiklos poreikius ir patikimą finansų valdymą, priima visus sprendimus dėl Agentūros vidaus struktūrų sukūrimo ir prireikus – keitimo;

p) pagal 7 ir 39 straipsnius įgalioja sudaryti darbo susitarimus.

2. Vadovaudamasi Tarnybos nuostatų 110 straipsniu, Valdančioji taryba priima Tarnybos nuostatų 2 straipsnio 1 dalimi ir kitų tarnautojų įdarbinimo sąlygų 6 straipsniu grindžiamą sprendimą, kuriuo atitinkami paskyrimų tarnybos įgaliojimai perduodami vykdomajam direktoriui ir nustatomos tų įgaliojimų perdavimo sustabdymo sąlygos. Vykdomajam direktoriui leidžiama tuos įgaliojimus toliau deleguoti.

3. Prireikus dėl išskirtinių aplinkybių Valdančioji taryba gali priimti sprendimą laikinai sustabdyti paskyrimų tarnybos įgaliojimų perdavimą vykdomajam direktoriui bei vykdomojo direktoriaus perskirtus įgaliojimus, ir jais naudotis pati arba perduoti juos vienam iš savo narių arba darbuotojui, kitam nei vykdomasis direktorius.

15 straipsnis

Valdančiosios tarybos pirmininkas

Valdančioji taryba dviejų trečdalių narių balsų dauguma iš savo narių išrenka pirmininką ir pirmininko pavaduotoją ketverių metų kadencijai, kuri gali būti vieną kartą pratęsta. Tačiau jei bet kuriuo kadencijos metu jie netenka Valdančiosios tarybos nario statuso, tą pačią dieną automatiškai baigiasi ir jų kadencija. Pirmininko pavaduotojas *ex officio* pakeičia pirmininką, jei šis negali vykdyti savo pareigų.

16 straipsnis

Valdančiosios tarybos posėdžiai

1. Valdančiosios tarybos posėdžius sušaukia jos pirmininkas.

2. Valdančioji taryba į eilinius posėdžius renkasi bent du kartus per metus. Pirmininko, Komisijos arba ne mažiau kaip trečdalio Valdančiosios tarybos narių prašymu Valdančioji taryba taip pat rengia neeilinius posėdžius.

3. Valdančiosios tarybos posėdžiuose vykdomasis direktorius dalyvauja be balsavimo teisės.

4. Pirmininko kvietimu Valdančiosios tarybos posėdžiuose nuolatinės suinteresuotųjų subjektų grupės nariai gali dalyvauti be balsavimo teisės.

5. Pagal darbo tvarkos taisykles Valdančiosios tarybos nariams ir jų pakaitiniams nariams posėdžiuose gali padėti patarėjai arba ekspertai.

6. Agentūra vykdo Valdančiosios tarybos sekretoriato funkciją.

17 straipsnis

Valdančiosios tarybos balsavimo taisyklės

1. Valdančioji taryba sprendimus priima savo narių balsų dauguma.

2. Dviejų trečdalių visų Valdančiosios tarybos narių dauguma būtina bendrajam programavimo dokumentui, metiniam biudžetui priimti, vykdomajam direktoriui paskirti, jo kadencijai pratęsti arba jam atleisti.

3. Kiekvienas narys turi vieną balsą. Jei narys nedalyvauja, jo balsavimo teise turi teisę pasinaudoti jo pakaitinis narys.

4. Pirmininkas balsuoja.

5. Vykdomasis direktorius nebalsuoja.

6. Valdančiosios tarybos darbo tvarkos taisyklėse nustatoma išsamesnė balsavimo tvarka, visų pirma aplinkybės, kuriomis vienas narys gali veikti kito nario vardu.

2 SKIRSNIS
VYKDOMOJI VALDYBA

18 straipsnis

Vykdomoji valdyba

1. Valdančiajai tarybai padeda Vykdomoji valdyba.

2. Vykdomoji valdyba:

   a) rengia sprendimus, kuriuos turi priimti Valdančioji taryba;

   b) kartu su Valdančiąja taryba užtikrina, kad būtų imtasi tinkamų tolesnių priemonių atsižvelgiant į OLAF tyrimų ir įvairiose vidaus ar išorės audito ataskaitose bei vertinimuose pateiktas išvadas ir rekomendacijas;

   c) nedarant poveikio 19 straipsnyje nustatytoms vykdomojo direktoriaus pareigoms, padeda ir pataria vykdomajam direktoriui, kaip pagal 19 straipsnį įgyvendinti Valdančiosios tarybos sprendimus, susijusius su administraciniais ir biudžeto klausimais.

3. Vykdomąją valdybą sudaro penki nariai, paskirti iš Valdančiosios tarybos narių: vienas iš jų – Valdančiosios tarybos pirmininkas, kuris taip pat gali būti Vykdomosios valdybos pirmininkas, ir vienas Komisijos atstovas. Vykdomasis direktorius dalyvauja Vykdomosios valdybos posėdžiuose, tačiau neturi teisės balsuoti.

4. Vykdomosios valdybos narių kadencija yra ketveri metai. Ta kadencija gali būti pratęsta.

5. Vykdomoji valdyba posėdžiauja bent kartą kas tris mėnesius. Vykdomosios valdybos narių prašymu jos pirmininkas sušaukia papildomus posėdžius.

6. Valdančioji taryba nustato Vykdomosios valdybos darbo tvarkos taisykles.

7. […]

3 SKIRSNIS
VYKDOMASIS DIREKTORIUS

19 straipsnis

Vykdomojo direktoriaus pareigos

1. Agentūrai vadovauja vykdomasis direktorius; vykdydamas savo pareigas jis yra nepriklausomas. Vykdomasis direktorius yra atskaitingas Valdančiajai tarybai.

2. Gavęs prašymą, vykdomasis direktorius Europos Parlamentui pateikia savo pareigų vykdymo ataskaitą. Taryba gali paprašyti vykdomojo direktoriaus pateikti jo pareigų vykdymo ataskaitą.

3. Vykdomasis direktorius atsako už:

a) kasdienį Agentūros veiklos administravimą;

b) Valdančiosios tarybos priimtų sprendimų įgyvendinimą;

c) bendrojo programavimo dokumento projekto rengimą ir jo pateikimą tvirtinti Valdančiajai tarybai prieš jį pateikiant Komisijai;

d) bendrojo programavimo dokumento įgyvendinimą ir atsiskaitymą už jį Valdančiajai tarybai;

e) konsoliduotosios metinės Agentūros veiklos ataskaitos**, įskaitant metinės darbo programos įgyvendinimą,** rengimą ir jos pateikimą Valdančiajai tarybai vertinti ir tvirtinti;

f) tolesnių veiksmų plano rengimą atsižvelgiant į retrospektyvių įvertinimų išvadas ir ataskaitų apie pažangą teikimą Komisijai kas dvejus metus;

g) veiksmų plano, kuriuo atsižvelgiama į vidaus ar išorės audito ataskaitų išvadas, taip pat į Europos kovos su sukčiavimu tarnybos (OLAF) atliktus tyrimus, rengimą ir padarytos pažangos ataskaitų teikimą du kartus per metus – Komisijai ir reguliariai – Valdančiajai tarybai;

h) Agentūrai taikytinų finansinių taisyklių projekto rengimą;

i) Agentūros pajamų ir išlaidų sąmatos projekto rengimą bei jos biudžeto vykdymą;

j) Sąjungos finansinių interesų gynimą taikant prevencines kovos su sukčiavimu, korupcija ir bet kokia kita neteisėta veikla priemones, vykdant veiksmingus patikrinimus ir, nustačius pažeidimų, susigrąžinant neteisingai išmokėtas sumas bei prireikus taikant veiksmingas, proporcingas ir atgrasomąsias administracines ir finansines nuobaudas;

k) Agentūros kovos su sukčiavimu strategijos rengimą ir jos pateikimą Valdančiajai tarybai patvirtinti;

l) kontaktų su verslo bendruomene ir vartotojų organizacijomis plėtrą ir palaikymą, kad būtų užtikrintas nuolatinis dialogas su atitinkamais suinteresuotaisiais subjektais;

la) reguliarų keitimąsi informacija apie jų veiklą kibernetinio saugumo srityje su Sąjungos institucijomis, agentūromis ir įstaigomis, siekiant užtikrinti ES politikos rengimo ir įgyvendinimo nuoseklumą;

m) kitas šiuo reglamentu vykdomajam direktoriui priskirtas užduotis.

4. Prireikus ir atsižvelgdamas į Agentūros įgaliojimus, tikslus ir užduotis, vykdomasis direktorius gali įsteigti ekspertų, įskaitant ekspertus iš valstybių narių kompetentingų valdžios institucijų, *ad hoc* darbo grupes. Valdančiajai tarybai pranešama iš anksto. Procedūros, visų pirma susijusios su darbo grupių sudėtimi, vykdomojo direktoriaus vykdomu darbo grupių ekspertų paskyrimu ir darbo grupių veikla, išsamiai išdėstomos Agentūros vidaus veiklos taisyklėse.

5. **Kai to reikia siekiant veiksmingai ir efektyviai vykdyti Agentūros užduotis, remdamasis atitinkama sąnaudų ir naudos analize**, vykdomasis direktorius **gali** nuspręsti [...]**vienoje arba keliose valstybėse narėse steigti vieną arba kelis vietos skyrius.** Prieš nuspręsdamas įsteigti vietos skyrių, vykdomasis direktorius **prašo atitinkamos (-ų) valstybės (-ių) narės (-ių), įskaitant valstybę narę, kurioje yra Agentūros būstinė, nuomonės ir** gauna išankstinį Komisijos **ir** Valdančiosios tarybos pritarimą[...]. **Jei vykdomojo direktoriaus ir atitinkamų valstybių narių konsultavimosi procese kiltų nesutarimų, klausimas turi būti perduotas Tarybai svarstyti.** Veiklos, kurią vykdys vietos skyrius, sritis sprendime nustatoma taip, kad būtų išvengta nebūtinų išlaidų ir Agentūros administracinių funkcijų dubliavimo.[...]**Darbuotojų skaičius visuose vietos skyriuose turi būti kuo mažesnis, o bendras jų skaičius turi neviršyti 40 % darbuotojų skaičiaus [...] valstybėje narėje, kurioje yra Agentūros būstinė. Darbuotojų skaičius kiekviename vietos skyriuje turi neviršyti 10 % [...] darbuotojų skaičiaus valstybėje narėje, kurioje yra Agentūros būstinė.**

4 SKIRSNIS
NUOLATINĖ SUINTERESUOTŲJŲ SUBJEKTŲ GRUPĖ

20 straipsnis

Nuolatinė suinteresuotųjų subjektų grupė

1. Valdančioji taryba vykdomojo direktoriaus siūlymu įsteigia nuolatinę suinteresuotųjų subjektų grupę, sudarytą iš pripažintų specialistų, atstovaujančių atitinkamiems suinteresuotiesiems subjektams, pavyzdžiui, IRT sektoriui, visuomenei prieinamų elektroninių ryšių tinklų ar paslaugų teikėjams, **esminių paslaugų operatoriams,** vartotojų grupėms, kibernetinio saugumo mokslo ekspertams, ir kompetentingų institucijų, apie kurias pranešta pagal [Direktyvą, kuria nustatomas Europos elektroninių ryšių kodeksas], bei teisėsaugos ir duomenų apsaugos priežiūros institucijų atstovų.

2. Agentūros vidaus darbo tvarkos taisyklėse nustatomos ir viešai skelbiamos nuolatinės suinteresuotųjų subjektų grupės procedūros, visų pirma dėl šios grupės dydžio, sudėties, jos narių paskyrimo Valdančiosios tarybos sprendimu, vykdomojo direktoriaus pasiūlymu ir jos veiklos.

3. Nuolatinei suinteresuotųjų subjektų grupei pirmininkauja vykdomasis direktorius arba kitas vykdomojo direktoriaus kiekvienam atvejui atskirai paskirtas asmuo.

4. Nuolatinės suinteresuotųjų subjektų grupės narių kadencija – dveji su puse metų. Valdančiosios tarybos nariai negali būti nuolatinės suinteresuotųjų subjektų grupės nariais. Komisijos ir valstybių narių ekspertai turi teisę dalyvauti nuolatinės suinteresuotųjų subjektų grupės posėdžiuose ir jos veikloje. Kitų įstaigų, kurias vykdomasis direktorius laiko svarbiomis, atstovai, kurie nėra nuolatinės suinteresuotųjų subjektų grupės nariai, gali būti kviečiami dalyvauti nuolatinės suinteresuotųjų subjektų grupės posėdžiuose ir jos veikloje.

5. Nuolatinė suinteresuotųjų subjektų grupė pataria Agentūrai jos veiklos klausimais. Ji visų pirma pataria vykdomajam direktoriui dėl Agentūros veiklos programos pasiūlymo rengimo ir dėl to, kaip užtikrinti ryšius su atitinkamais suinteresuotaisiais subjektais visais su veiklos programa susijusiais klausimais.

5a. Nuolatinė suinteresuotųjų subjektų grupė apie savo veiklą nuolat informuoja Valdančiąją tarybą.

4A SKIRSNIS
NACIONALINIŲ RYŠIŲ PALAIKYMO PAREIGŪNŲ TINKLAS

20a straipsnis

Nacionalinių ryšių palaikymo pareigūnų tinklas

1. Valdančioji taryba, remdamasi vykdomojo direktoriaus pasiūlymu, sudaro iš valstybių narių atstovų sudarytą nacionalinių ryšių palaikymo pareigūnų tinklą.

2. Nacionalinių ryšių palaikymo pareigūnų tinklą sudaro visų valstybių narių atstovai. Kiekviena valstybė narė paskiria vieną atstovą. Tinklo susitikimai gali būti rengiami įvairių ekspertų sudėties.

3. Nacionalinių ryšių palaikymo pareigūnų tinklas visų pirma palengvina ENISA ir valstybių narių keitimąsi informacija. Jis visų pirma remia ENISA skleidžiant informaciją apie jos veiklą, išvadas ir rekomendacijas atitinkamiems suinteresuotiesiems subjektams visoje ES.

4. Nacionaliniai ryšių palaikymo pareigūnai veikia kaip ryšių punktai nacionaliniu lygmeniu, kad palengvintų ENISA ir nacionalinių ekspertų bendradarbiavimą ENISA darbo programos įgyvendinimo kontekste.

5. Kadangi nacionaliniai ryšių palaikymo pareigūnai turėtų glaudžiai bendradarbiauti su savo šalies atstovais Valdančiojoje taryboje, pats tinklas nedubliuoja nei Valdančiosios tarybos, nei kitų ES forumų darbo.

6. Nacionalinių ryšių palaikymo pareigūnų tinklo funkcijos ir procedūros nustatomos Agentūros vidaus veiklos taisyklėse ir paskelbiamos viešai.

5 SKIRSNIS
VEIKLA

21 straipsnis

Bendrasis programavimo dokumentas

1. Agentūra vykdo savo veiklą pagal bendrąjį programavimo dokumentą, kurį sudaro jos daugiametė ir metinė veiklos programos, kuriose numatyta visa jos planuojama veikla.

2. Vykdomasis direktorius kasmet parengia bendrojo programavimo dokumento projektą, kuriame, vadovaujantis Komisijos deleguotojo reglamento (ES) Nr. 1271/2013 [14] 32 straipsniu ir atsižvelgiant į Komisijos nustatytas gaires, nustatomos daugiametė ir metinė programos su atitinkamais žmogiškaisiais ir finansiniais ištekliais.

3. Valdančioji taryba kiekvienais metais iki lapkričio 30 d. priima 1 dalyje nurodytą bendrąjį programavimo dokumentą ir ne vėliau kaip kitų metų sausio 31 d. nusiunčia jį ir visas paskesnes atnaujintas to dokumento versijas Europos Parlamentui, Tarybai ir Komisijai.

4. Galutinai patvirtinus bendrąjį Sąjungos biudžetą bendrasis programavimo dokumentas prireikus atitinkamai pakoreguojamas ir tampa galutiniu.

5. Metinėje darbo programoje nustatomi išsamūs tikslai ir numatomi rezultatai, įskaitant veiklos rezultatų rodiklius. Į ją taip pat įtraukiamas finansuotinų veiksmų aprašas ir nurodomi kiekvienam veiksmui skiriami finansiniai ir žmogiškieji ištekliai, vadovaujantis veikla grindžiamo biudžeto sudarymo ir valdymo principais. Metinė darbo programa dera su 7 dalyje nurodyta daugiamete darbo programa. Joje aiškiai nurodoma, kokios užduotys nuo ankstesnių finansinių metų buvo pridėtos, pakeistos arba išbrauktos.

---

[14] 2013 m. rugsėjo 30 d. Komisijos deleguotasis reglamentas (ES) Nr. 1271/2013 dėl finansinio pagrindų reglamento, taikomo įstaigoms, nurodytoms Europos Parlamento ir Tarybos reglamento (ES, Euratomas) Nr. 966/2012 208 straipsnyje (OL L 328, 2013 12 7, p. 42).

6. Jei Agentūrai paskiriama nauja užduotis, Valdančioji taryba iš dalies keičia priimtą metinę darbo programą. Visi esminiai metinės darbo programos pakeitimai priimami laikantis tokios pačios tvarkos, kaip priimant pirminę metinę darbo programą. Valdančioji taryba gali perduoti vykdomajam direktoriui įgaliojimus atlikti neesminius metinės darbo programos pakeitimus.

7. Daugiametėje darbo programoje nustatomos bendro strateginio programavimo nuostatos, įskaitant tikslus, numatomus rezultatus ir veiklos rezultatų rodiklius. Joje taip pat nustatomas išteklių, įskaitant daugiametį biudžetą ir darbuotojus, programavimas.

8. Išteklių programavimas kasmet atnaujinamas. Strateginis programavimas prireikus atnaujinamas, visų pirma, kai reikia atsižvelgti į 56 straipsnyje nurodyto vertinimo rezultatus.

22 straipsnis

Interesų deklaravimas

1. Kiekvienas Valdančiosios tarybos narys, vykdomasis direktorius ir valstybių narių laikinai deleguotieji pareigūnai pateikia įsipareigojimų deklaraciją ir deklaraciją, iš kurios būtų aišku, kad jie neturi jokių arba turi tiesioginių arba netiesioginių interesų, kurie galėtų neigiamai paveikti jų nepriklausomumą. Deklaracijos turi būti tikslios ir išsamios, pateikiamos kasmet raštu ir, esant būtinybei, atnaujinamos.

2. Kiekvienas Valdančiosios tarybos narys, vykdomasis direktorius ir *ad hoc* darbo grupėse dalyvaujantys išorės ekspertai ne vėliau kaip kiekvieno posėdžio pradžioje tiksliai ir išsamiai deklaruoja visus su darbotvarkėje numatytais klausimais susijusius interesus, kurie galėtų neigiamai paveikti jų nepriklausomumą, ir nedalyvauja diskusijose bei balsavime dėl tokių klausimų.

3. Agentūra savo vidaus veiklos taisyklėse nustato praktines priemones 1 ir 2 dalyse nurodyto interesų deklaravimo taisyklėms įgyvendinti.

23 straipsnis

Skaidrumas

1. Agentūra vykdo savo veiklą itin skaidriai ir pagal 25 straipsnį.

2. Agentūra užtikrina, kad visuomenė ir suinteresuotosios šalys gautų tinkamą, objektyvią, patikimą ir lengvai prieinamą informaciją, ypač kai ji susijusi su Agentūros veiklos rezultatais. Ji taip pat viešai skelbia pagal 22 straipsnį pateiktas interesų deklaracijas.

3. Valdančioji taryba, vadovaudamasi vykdomojo direktoriaus siūlymu, gali leisti suinteresuotosioms šalims stebėti, kaip vykdoma tam tikra Agentūros veikla.

4. Agentūra savo vidaus veiklos tvarkos taisyklėse nustato praktines priemones 1 ir 2 dalyse nurodytoms skaidrumo taisyklėms įgyvendinti.

24 straipsnis

Konfidencialumas

1. Nedarant poveikio 25 straipsniui, Agentūra neatskleidžia trečiosioms šalims informacijos, kurią ji tvarko arba gauna ir kurią pateiktame pagrįstame prašyme prašoma laikyti visiškai ar iš dalies konfidencialia.

2. Valdančiosios tarybos nariams, vykdomajam direktoriui, nuolatinės suinteresuotųjų subjektų grupės nariams, *ad hoc* darbo grupėse dalyvaujantiems išorės ekspertams ir Agentūros darbuotojams, įskaitant valstybių narių laikinai deleguotuosius pareigūnus, taikomi konfidencialumo reikalavimai pagal Sutarties dėl Europos Sąjungos veikimo (SESV) 339 straipsnį, net jiems nustojus eiti savo pareigas.

3. Agentūra savo vidaus veiklos taisyklėse nustato praktines priemones 1 ir 2 dalyse nurodytoms konfidencialumo taisyklėms įgyvendinti.

4. Jei to reikia Agentūros užduotims vykdyti, Valdančioji taryba nusprendžia leisti Agentūrai tvarkyti įslaptintą informaciją. Tokiu atveju Valdančioji taryba priima su Komisijos tarnybomis suderintas vidaus veiklos taisykles, kaip taikyti Komisijos sprendimuose (ES, Euratomas) 2015/443 [15] ir 2015/444 [16] nustatytus saugumo principus. Tos taisyklės apima įslaptintos informacijos tvarkymo ir saugojimo bei keitimosi ja nuostatas.

---

[15] 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/443 dėl saugumo Komisijoje (OL L 72, 2015 3 17, p. 41).

[16] 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/444 dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (OL L 72, 2015 3 17, p. 53).

25 straipsnis

Galimybė susipažinti su dokumentais

1. Agentūros saugomiems dokumentams taikomas Reglamentas (EB) Nr. 1049/2001.

2. Valdančioji taryba per šešis mėnesius nuo Agentūros įsteigimo patvirtina Reglamento (EB) Nr. 1049/2001 įgyvendinimo priemones.

3. Sprendimai, kuriuos priima Agentūra pagal Reglamento (EB) Nr. 1049/2001 8 straipsnį, gali tapti skundo ombudsmenui pagal SESV 228 straipsnį ar Europos Sąjungos Teisingumo Teisme pareikšto ieškinio dalyku pagal SESV 263 straipsnį.

III SKYRIUS

BIUDŽETO SUDARYMAS IR STRUKTŪRA

26 straipsnis

Biudžeto sudarymas

1. Kasmet vykdomasis direktorius parengia Agentūros ateinančių finansinių metų pajamų ir išlaidų sąmatos projektą ir perduoda jį Valdančiajai tarybai kartu su etatų plano projektu. Pajamos ir išlaidos turi būti subalansuotos.

2. Valdančioji taryba, vadovaudamasi 1 dalyje nurodytu pajamų ir išlaidų sąmatos projektu, kasmet parengia Agentūros ateinančių finansinių metų pajamų ir išlaidų sąmatą.

3. 2 dalyje nurodytą sąmatą, kuri taip pat įtraukiama į bendrojo programavimo dokumento projektą, Valdančioji taryba iki kiekvienų metų sausio 31 d. nusiunčia Komisijai ir trečiosioms šalims, su kuriomis Sąjunga yra sudariusi susitarimus pagal 39 straipsnį.

4. Pagal tą sąmatą Komisija į Sąjungos biudžeto projektą įtraukia, jos manymu, etatų planui būtinų lėšų sąmatas ir įnašo į bendrąjį biudžetą, kurį ji pagal SESV 313 ir 314 straipsnius pateikia Europos Parlamentui ir Tarybai, sumą.

5. Europos Parlamentas ir Taryba patvirtina Agentūrai skiriamo įnašo asignavimus.

6. Europos Parlamentas ir Taryba tvirtina Agentūros etatų planą.

7. Valdančioji taryba Agentūros biudžetą priima kartu su bendruoju programavimo dokumentu. Jis tampa galutiniu galutinai priėmus Sąjungos bendrąjį biudžetą. Prireikus Valdančioji taryba tikslina Agentūros biudžetą ir bendrąjį programavimo dokumentą pagal Sąjungos bendrąjį biudžetą.

27 straipsnis

Biudžeto struktūra

1. Neatmetant kitų išteklių galimybės, Agentūros pajamas sudaro:

   a) įnašas iš Sąjungos biudžeto;

   b) asignuotosios pajamos, skirtos konkretiems išlaidų straipsniams pagal 29 straipsnyje nurodytas finansines taisykles;

   c) Sąjungos lėšos, skiriamos sudarant įgaliojimo susitarimus ar skiriant *ad hoc* dotacijas pagal 29 straipsnyje nurodytas Agentūros finansines taisykles ir pagal atitinkamų priemonių, kuriomis remiama Sąjungos politika, nuostatas;

   d) trečiųjų šalių, dalyvaujančių Agentūros veikloje, kaip numatyta 39 straipsnyje, įnašai;

   e) savanoriški valstybių narių įnašai pinigais arba natūra. Savanoriškus įnašus teikiančios valstybės narės dėl to negali reikalauti jokių ypatingų teisių ar paslaugų.

2. Agentūros išlaidas sudaro darbuotojų, administracinės ir techninės pagalbos, infrastruktūros ir veiklos išlaidos, taip pat išlaidos, atsirandančios dėl sutarčių, sudarytų su trečiosiomis šalimis.

28 straipsnis

Biudžeto įgyvendinimas

1. Už Agentūros biudžeto įgyvendinimą atsako vykdomasis direktorius.

2. Komisijos vidaus auditoriaus įgaliojimai Agentūros atžvilgiu yra tokie patys, kaip ir Komisijos departamentų atžvilgiu.

3. Ne vėliau kaip kovo 1 d. po kiekvienų finansinių metų (N + 1 m. kovo 1 d.) Agentūros apskaitos pareigūnas Komisijos apskaitos pareigūnui ir Audito Rūmams nusiunčia preliminarias finansines ataskaitas.

4. Gavęs Audito Rūmų pastabas dėl preliminarių finansinių Agentūros ataskaitų, Agentūros apskaitos pareigūnas, prisiimdamas atsakomybę, parengia galutines finansines Agentūros ataskaitas.

5. Vykdomasis direktorius pateikia galutines finansines ataskaitas Valdančiajai tarybai, kad ši pareikštų savo nuomonę.

6. Vykdomasis direktorius ne vėliau kaip N + 1 m. kovo 31 d. siunčia biudžeto ir finansų valdymo ataskaitą Europos Parlamentui, Tarybai, Komisijai ir Audito Rūmams.

7. Apskaitos pareigūnas ne vėliau kaip N + 1 m. liepos 1 d. siunčia galutines finansines ataskaitas kartu su Valdančiosios tarybos nuomone Europos Parlamentui, Tarybai, Komisijos apskaitos pareigūnui ir Audito Rūmams.

8. Tą pačią dieną, kurią apskaitos pareigūnas išsiunčia savo galutines finansines ataskaitas, jis taip pat išsiunčia ir tas galutines finansines ataskaitas patvirtinantį pareiškimo raštą Audito Rūmams ir jo kopiją Komisijos apskaitos pareigūnui.

9. Vykdomasis direktorius paskelbia galutines finansines ataskaitas iki kitų metų lapkričio 15 d.

10. Ne vėliau kaip N + 1 m. rugsėjo 30 d. vykdomasis direktorius išsiunčia Audito Rūmams atsakymą dėl jų pateiktų pastabų ir taip pat išsiunčia to atsakymo kopiją Valdančiajai tarybai ir Komisijai.

11. Europos Parlamento prašymu vykdomasis direktorius jam pateikia visą informaciją, kurios reikia sklandžiai sprendimo dėl atitinkamų finansinių metų biudžeto įvykdymo priėmimo procedūrai pagal Finansinio reglamento 165 straipsnio 3 dalį.

12. Europos Parlamentas, remdamasis Tarybos rekomendacija, iki N + 2 metų gegužės 15 d. vykdomajam direktoriui pateikia N metų biudžeto įvykdymo patvirtinimo sprendimą.

29 straipsnis

Finansinės taisyklės

Pasikonsultavusi su Komisija, Valdančioji taryba priima Agentūrai taikomas finansines taisykles. Jos negali nukrypti nuo Reglamento (ES) Nr. 1271/2013, išskyrus atvejus, kai taip nukrypti aiškiai reikia dėl Agentūros veiklos ir yra gautas išankstinis Komisijos sutikimas.

30 straipsnis

Kova su sukčiavimu

1. Siekiant sudaryti palankias sąlygas kovoti su sukčiavimu, korupcija ir kita neteisėta veikla pagal Europos Parlamento ir Tarybos reglamentą (ES, Euratomas) Nr. 883/2013 [17], Agentūra per šešis mėnesius nuo veiklos pradžios dienos prisijungia prie 1999 m. gegužės 25 d. Tarpinstitucinio susitarimo dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų vidaus tyrimų ir priima visiems Agentūros darbuotojams taikomas tinkamas nuostatas naudodamasi to susitarimo priede nustatytu modeliu.

2. Audito Rūmai turi įgaliojimus atlikti visų dotacijų gavėjų, rangovų ir subrangovų, kurie iš Agentūros yra gavę Sąjungos lėšų, auditą remdamiesi dokumentais ir auditą vietoje.

[17] 2013 m. rugsėjo 11 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) Nr. 883/2013 dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų tyrimų ir kuriuo panaikinami Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1073/1999 ir Tarybos reglamentas (Euratomas) Nr. 1074/1999 (OL L 248, 2013 9 18, p. 1).

3. OLAF gali atlikti tyrimus, įskaitant patikrinimus ir inspektavimus vietoje, laikydamasi Europos Parlamento ir Tarybos reglamento (ES, Euratomas) Nr. 883/2013 ir 1996 m. lapkričio 11 d. Tarybos reglamento (Euratomas, EB) Nr. 2185/96 [18] dėl Komisijos atliekamų patikrinimų ir inspektavimų vietoje siekiant apsaugoti Sąjungos finansinius interesus nuo sukčiavimo ir kitų pažeidimų nuostatų ir procedūrų, kad nustatytų sukčiavimo, korupcijos arba bet kurios kitos neteisėtos veiklos, susijusios su Agentūros finansuojamomis dotacijomis ar sutartimis ir turinčios neigiamą poveikį Sąjungos finansiniams interesams, atvejus.

4. Nedarant poveikio 1, 2 ir 3 dalims, su trečiosiomis šalimis ir tarptautinėmis organizacijomis sudarytuose bendradarbiavimo susitarimuose, Agentūros sutartyse, susitarimuose dėl dotacijų ir sprendimuose dėl dotacijų pateikiamos nuostatos, pagal kurias Audito Rūmams ir OLAF aiškiai suteikiami įgaliojimai atlikti tokį auditą ir tyrimus atsižvelgiant į jų atitinkamą kompetenciją.

IV SKYRIUS
AGENTŪROS DARBUOTOJAI

31 straipsnis

Bendrosios nuostatos

Agentūros darbuotojams taikomi Pareigūnų tarnybos nuostatai ir kitų tarnautojų įdarbinimo sąlygos ir Sąjungos institucijų tarpusavio susitarimu priimtos Pareigūnų tarnybos nuostatų įgyvendinimo taisyklės.

---

[18] 1996 m. lapkričio 11 d. Tarybos reglamentas (Euratomas, EB) Nr. 2185/96 dėl Komisijos atliekamų patikrinimų ir inspektavimų vietoje siekiant apsaugoti Europos Bendrijų finansinius interesus nuo sukčiavimo ir kitų pažeidimų (OL L 292, 1996 11 15, p. 2).

32 straipsnis

Privilegijos ir imunitetas

Agentūrai ir jos darbuotojams taikomas prie Europos Sąjungos sutarties ir SESV pridėtas Protokolas Nr. 7 dėl Europos Sąjungos privilegijų ir imunitetų.

33 straipsnis

Vykdomasis direktorius

1. Remiantis kitų tarnautojų įdarbinimo sąlygų 2 straipsnio a punktu, vykdomasis direktorius įdarbinamas kaip Agentūros laikinai priimtas tarnautojas.

2. Vykdomąjį direktorių iš Komisijos pasiūlytų kandidatų sąrašo skiria Valdančioji taryba, laikydamasi atviros ir skaidrios atrankos procedūros.

3. Sudarant sutartį su vykdomuoju direktoriumi, Agentūrai atstovauja Valdančiosios tarybos pirmininkas.

4. Prieš paskyrimą Valdančiosios tarybos atrinktas kandidatas pakviečiamas padaryti pranešimą atitinkamame Europos Parlamento komitete ir atsakyti į Parlamento narių klausimus.

5. Vykdomojo direktoriaus kadencija – **ketveri**[...] metai. To laikotarpio pabaigoje Komisija atlieka vertinimą, kuriame atsižvelgiama į vykdomojo direktoriaus veiklos vertinimą ir būsimas Agentūros užduotis ir iššūkius.

6. Sprendimus dėl vykdomojo direktoriaus skyrimo, kadencijos pratęsimo arba atleidimo iš pareigų Valdančioji taryba priima dviejų trečdalių balso teisę turinčių narių balsų dauguma.

7. Remdamasi Komisijos pasiūlymu, kuriame atsižvelgiama į 5 dalyje nurodytą vertinimą, Valdančioji taryba gali vieną kartą pratęsti vykdomojo direktoriaus kadenciją ne daugiau kaip **ketveriems**[...] metams.

8. Apie ketinimą pratęsti vykdomojo direktoriaus kadenciją Valdančioji taryba informuoja Europos Parlamentą. Per tris mėnesius iki tokio kadencijos pratęsimo vykdomasis direktorius, jei jo paprašoma, padaro pranešimą atitinkamame Europos Parlamento komitete ir atsako į Parlamento narių klausimus.

9. Vykdomasis direktorius, kurio kadencija buvo pratęsta, negali dalyvauti kitoje atrankos į tą pačią pareigybę procedūroje.

10. Vykdomasis direktorius gali būti pašalintas iš pareigų tik valdančiosios tarybos sprendimu[...].

34 straipsnis

Deleguotieji nacionaliniai ekspertai ir kiti darbuotojai

1. Agentūra gali naudotis deleguotųjų nacionalinių ekspertų ar kitų darbuotojų, neįdarbintų Agentūroje, paslaugomis. Tokiems darbuotojams netaikomi Pareigūnų tarnybos nuostatai ir kitų tarnautojų įdarbinimo sąlygos.

2. Valdančioji taryba priima sprendimą, kuriuo nustato nacionalinių ekspertų delegavimo į Agentūrą taisykles.

V SKYRIUS
BENDROSIOS NUOSTATOS

35 straipsnis

Agentūros teisinis statusas

1. Agentūra yra juridinio asmens statusą turinti Sąjungos įstaiga.

2. Kiekvienoje valstybėje narėje Agentūra turi didžiausios apimties veiksnumą, suteikiamą pagal nacionalinę teisę juridiniams asmenims. Visų pirma, Agentūra gali įsigyti kilnojamojo ir nekilnojamojo turto arba juo disponuoti, taip pat būti teismo proceso šalimi[...].

3. Agentūrai atstovauja jos vykdomasis direktorius.

36 straipsnis

Agentūros atsakomybė

1. Agentūros sutartinė atsakomybė reglamentuojama aptariamai sutarčiai taikytina teise.

2. Europos Sąjungos Teisingumo Teismas turi jurisdikciją priimti sprendimus pagal bet kurią Agentūros sudarytos sutarties arbitražinę išlygą.

3. Nesutartinės atsakomybės atveju Agentūra pagal bendrus valstybių narių teisės aktams būdingus principus atlygina žalą, kurią vykdydama savo pareigas padaro ji pati arba jos tarnautojai.

4. Europos Sąjungos Teisingumo Teismas turi jurisdikciją spręsti ginčus dėl tokios žalos atlyginimo.

5. Asmeninę tarnautojų atsakomybę Agentūros atžvilgiu reguliuoja atitinkamos Agentūros darbuotojams taikomos atitinkamos nuostatos.

37 straipsnis

Nuostatos dėl kalbų

1. Agentūrai taikomas Tarybos reglamentas Nr. 1 [19]. Valstybės narės ir kitos jų paskirtos įstaigos į Agentūrą gali kreiptis ir atsakymą gauti jų pasirinkta Sąjungos institucijų oficialiąja kalba.

2. Agentūros veiklai būtinas vertimo paslaugas teikia Europos Sąjungos įstaigų vertimo centras.

38 straipsnis

Asmens duomenų apsauga

1. Agentūros vykdomam asmens duomenų tvarkymui taikomas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 [20].

2. Valdančioji taryba priima Reglamento (EB) Nr. 45/2001 24 straipsnio 8 dalyje nurodytas įgyvendinimo priemones. Valdančioji taryba gali priimti papildomas priemones, kurių reikia, kad Agentūra taikytų Reglamentą (EB) Nr. 45/2001.

---

[19] Reglamentas Nr. 1, nustatantis kalbas, kurios turi būti vartojamos Europos ekonominėje bendrijoje (OL 17, 1958 10 6, p. 401).

[20] 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, 2001 1 12, p. 1).

39 straipsnis

Bendradarbiavimas su trečiosiomis šalimis ir tarptautinėmis organizacijomis

1. Tiek, kiek būtina šiame reglamente išdėstytiems tikslams pasiekti, Agentūra gali bendradarbiauti su trečiųjų šalių kompetentingomis valdžios institucijomis ir (arba) su tarptautinėmis organizacijomis. Todėl Agentūra gali, gavusi Komisijos patvirtinimą, sudaryti darbinius susitarimus su tomis trečiųjų šalių valdžios institucijomis ir tarptautinėmis organizacijomis. Tais susitarimais nesukuriami teisiniai įpareigojimai Sąjungai ir jos valstybėms narėms.

2. Agentūros veikloje gali dalyvauti trečiosios valstybės, kurios tuo tikslu yra sudariusios susitarimus su Sąjunga. Pagal atitinkamas tų susitarimų nuostatas susitariama ir nurodoma, visų pirma, tų šalių dalyvavimo Agentūros veikloje pobūdis, mastas ir būdai, įskaitant su dalyvavimu Agentūros vykdomose iniciatyvose, finansiniais įnašais ir personalu susijusias nuostatas. Tų susitarimų nuostatos dėl darbuotojų visais atvejais turi atitikti Tarnybos nuostatus.

3. Valdančioji taryba priima santykių su trečiosiomis šalimis ar tarptautinėmis organizacijomis Agentūros kompetencijai priklausančiais klausimais strategiją. Sudarydama tinkamą darbinį susitarimą su Agentūros vykdomuoju direktoriumi, Komisija užtikrina, kad Agentūra veiktų pagal savo įgaliojimus ir esamą institucinę struktūrą.

40 straipsnis

Įslaptintos informacijos ir neskelbtinos neįslaptintos informacijos apsaugai užtikrinti skirtos saugumo taisyklės

Pasikonsultavusi su Komisija, Agentūra priima savo pačios saugumo taisykles, pagrįstas saugumo principais, išdėstytais Komisijos saugumo taisyklėse, skirtose Europos Sąjungos įslaptintos informacijos ir neskelbtinos neįslaptintos informacijos apsaugai užtikrinti, kaip nustatyta Komisijos sprendimuose (ES, Euratomas) 2015/443 ir 2015/444. Tai apima, *inter alia*, tokios informacijos tvarkymo ir saugojimo bei keitimosi ja nuostatas.

41 straipsnis

Susitarimas dėl būstinės ir veiklos sąlygos

1. Susitarime dėl būstinės, kurį, pritarus Valdančiajai tarybai, Agentūra ne vėliau kaip [praėjus dviem metams nuo šio Reglamento įsigaliojimo], sudaro su priimančiąja valstybe nare, nustatomos reikiamos nuostatos dėl darbuotojų įkurdinimo ir Agentūros patalpų suteikimo priimančioje valstybėje narėje, taip pat toje valstybėje narėje Agentūros vykdomajam direktoriui, Valdančiosios tarybos nariams, personalui ir jų šeimos nariams taikytinos specialiosios taisyklės.

2. Agentūrą priimančioji valstybė narė sudaro[...] sąlygas, kad būtų užtikrintas tinkamas Agentūros veikimas, įskaitant vietos prieinamumą, tinkamas galimybes mokytis darbuotojų vaikams, tinkamas galimybes įsidarbinti, naudotis socialinės apsaugos ir medicininės priežiūros paslaugomis vaikams ir sutuoktiniams.

42 straipsnis

Administracinė kontrolė

Agentūros veiklą pagal SESV 228 straipsnį prižiūri ombudsmenas.

III ANTRAŠTINĖ DALIS
KIBERNETINIO SAUGUMO SERTIFIKAVIMO SISTEMA

43 straipsnis

***Europos kibernetinio saugumo sertifikavimo[...]* sistema**

1. **Siekiant pagerinti vidaus rinkos veikimo sąlygas padidinant kibernetinio saugumo lygį Sąjungoje, sukuriama Europos kibernetinio saugumo sertifikavimo sistema. Joje nustatomi valdymo principai, kuriais sudaromos sąlygos ES lygmeniu laikytis suderinto požiūrio į Europos kibernetinio saugumo sertifikavimo schemas siekiant sukurti bendrąją skaitmeninę rinką, skirtą IRT procesams, produktams ir paslaugoms.**

2. **Europos kibernetinio saugumo sertifikavimo sistemoje nustatomas mechanizmas, skirtas** [...]Europos kibernetinio saugumo sertifikavimo schem**oms sukurti** [...] **ir** patvirtinti, kad pagal toki**as** schem**as** [...]**įvertinti** IRT **procesai,** produktai ir paslaugos atitinka nustatytus **saugumo** reikalavimus[...], **siekiant apsaugoti** saugomų, perduodamų ar tvarkomų duomenų arba tais produktais, procesais **ir** paslaugomis arba per juos prieinamų funkcijų ar paslaugų prieinamumą, autentiškumą, vientisumą ar konfidencialumą[...] **viso jų gyvavimo ciklo metu**.

44 straipsnis

Europos kibernetinio saugumo sertifikavimo schemos rengimas ir tvirtinimas

1. Gavusi Komisijos **arba pagal 53 straipsnį įsteigtos Europos kibernetinio saugumo sertifikavimo grupės (toliau – grupė)** prašymą, ENISA parengia potencialią šio reglamento 45, 46 ir 47 straipsniuose nustatytus reikalavimus atitinkančią Europos kibernetinio saugumo sertifikavimo schemą.[...]

1a. Potencialios Europos kibernetinio saugumo sertifikavimo schemos rengimą grupei gali pasiūlyti valstybės narės arba atitinkamos suinteresuotųjų subjektų organizacijos. Grupė įvertina tokius pasiūlymus atsižvelgdama į grupės pagal 53 straipsnio 3 dalies ca punktą parengtose gairėse nustatytus kriterijus ir gali prašyti, kad ENISA parengtų potencialią Europos kibernetinio saugumo sertifikavimo schemą.

2. Rengdama šio straipsnio 1 dalyje nurodytas potencialias schemas ENISA konsultuojasi su visais atitinkamais suinteresuotaisiais subjektais **vesdama skaidrų konsultacijų procesą** ir glaudžiai bendradarbiauja su grupe. Grupė teikia ENISA pagalbą ir ekspertų konsultacijas[...], susijusias su potencialios schemos rengimu, **ir priima nuomonę dėl potencialios schemos prieš ją pateikiant Komisijai**[...]. **ENISA užtikrina, kad potencialios schemos atitiktų taikytiną darnųjį standartą, taikomą atitikties vertinimo įstaigų akreditavimui.**

3. ENISA **kuo labiau atsižvelgia į grupės nuomonę prieš išsiųsdama** [...]pagal šio straipsnio 2 dalį parengtą [...]potencialią schemą Komisijai.

4. Komisija, remdamasi ENISA pasiūlyta potencialia schema, pagal 55 straipsnio 2 dalį gali priimti įgyvendinimo aktus, kuriuose nustatomos šio reglamento 45, 46 ir 47 straipsnių reikalavimus atitinkančios IRT **procesų,** produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo schemos.

5. […]

44a straipsnis

Europos kibernetinio saugumo sertifikavimo schemos priežiūra

1. Agentūra administruoja specialią svetainę, kurioje pateikiama informacija apie Europos kibernetinio saugumo sertifikavimo schemas, sertifikatus ir ES atitikties pareiškimus, paskelbtus pagal 47a straipsnį, ir jų reklama.

2. Agentūra, glaudžiai bendradarbiaudama su grupe, bent kas 5 metus peržiūri priimtas Europos kibernetinio saugumo sertifikavimo schemas, atsižvelgdama į iš suinteresuotųjų šalių gautą grįžtamąją informaciją. Jei manoma, kad tai būtina, Komisija arba grupė gali prašyti Agentūros pradėti patikslintos potencialios schemos rengimo pagal 44 straipsnio 2 ir 3 dalis procesą.

45 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų saugumo tikslai

Europos kibernetinio saugumo sertifikavimo schema turi būti suprojektuota taip, **kad** būtų [...]**pasiekti** atitinkamai **bent** šie saugumo tikslai:

a) saugomi, perduodami ar kitaip tvarkomi duomenys būtų apsaugoti nuo atsitiktinio ar neteisėto jų saugojimo, tvarkymo, prieigos prie jų ar jų atskleidimo **viso proceso, produkto ar paslaugos gyvavimo ciklo metu**;

b) saugomi, perduodami ar kitaip tvarkomi duomenys būtų apsaugoti nuo atsitiktinio ar neteisėto jų sunaikinimo, [...]netekimo ar pakeitimo **arba jų neprieinamumo viso proceso, produkto ar paslaugos gyvavimo ciklo metu**;

c) [...]įgaliotieji asmenys, programos ar mašinos galėtų gauti prieigą tik prie tų duomenų, paslaugų ar funkcijų, su kuriais yra susijusios jų prieigos teisės;

d) būtų registruojama, prie kurių duomenų, funkcijų ar paslaugų [...]**buvo gauta prieiga, kuriais jų buvo pasinaudota ar jie buvo kitaip tvarkomi**, bei kada ir kas tai padarė;

e) [...]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;

f) įvykus fiziniam ar techniniam incidentui, laiku atkuriamas duomenų, paslaugų ir funkcijų prieinamumas ir prieigos prie jų galimybės;

g) [...]IRT **procesai,** produktai ir paslaugos būtų teikiami su atnaujinta programine įranga **ir aparatine įranga**, [...] kuriuose nėra **viešai** žinomų spragų ir kurie yra aprūpinti saugaus programinės įrangos atnaujinimo mechanizmais**;**

ga) IRT procesai, produktai ir paslaugos būtų kuriami, gaminami ir tiekiami laikantis konkrečioje schemoje nurodytų saugumo reikalavimų.

46 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų saugumo užtikrinimo lygiai

1. Europos kibernetinio saugumo sertifikavimo schemoje gali būti nurodytas vienas ar daugiau iš šių IRT **procesams,** produktams ir paslaugoms taikomų saugumo užtikrinimo lygių: bazinis, pakankamas ir (arba) aukštas[...]. **Saugumo užtikrinimo lygis turi atitikti rizikos, susijusios su numatoma IRT proceso, produkto arba paslaugos paskirtimi, rizikos lygį.**

2. Bazinis, pakankamas ir aukštas saugumo užtikrinimo lygiai [...]**patvirtinami pagal Europos kibernetinio saugumo sertifikavimo schemą išduotu sertifikatu arba ES atitikties pareiškimu, kuriame kiekvieno atitinkamo saugumo užtikrinimo lygio atveju nustatomi saugumo reikalavimai, įskaitant saugumo funkcijas ir atitinkamas IRT proceso, produkto arba paslaugos įvertinimo pastangų mastas. Sertifikatu arba ES atitikties pareiškimu apibūdinamos su juo susijusios techninės specifikacijos, standartai ir procedūros, įskaitant technines kontrolės priemones, kurių paskirtis – sumažinti kibernetinio saugumo incidentų riziką arba jų išvengti:**

a) **Europos kibernetinio saugumo sertifikatu arba ES atitikties pareiškimu, kuriuo patvirtinimas** bazinis saugumo užtikrinimo lygis**, garantuojama, kad IRT procesai, produktai ir paslaugos tenkina atitinkamus saugumo reikalavimus, įskaitant saugumo funkcines galimybes, ir buvo atliktas tokio lygmens jų įvertinimas, kad būtų kuo labiau sumažinta žinoma bazinė kibernetinių incidentų rizika. Vykdant įvertinimo veiksmus turi būti bent peržiūrėti techniniai dokumentai arba, kai tai netaikoma, vykdomi pakaitiniai tokio paties poveikio veiksmai**[...];

b) **Europos kibernetinio saugumo sertifikatu, kuriuo patvirtinimas** pakankamas saugumo užtikrinimo lygis, **garantuojama, kad IRT procesai, produktai ir paslaugos tenkina atitinkamus saugumo reikalavimus, įskaitant saugumo funkcines galimybes, ir buvo atliktas tokio lygmens jų įvertinimas, kad būtų kuo labiau sumažinta žinoma kibernetinė rizika, kibernetinių incidentų ir kibernetinių išpuolių, kuriuos vykdo ribotų gebėjimų ir ribotų išteklių turintys subjektai, pavojų. Vykdant įvertinimo veiksmus turi būti bent: įvertinama, ar nėra viešai žinomų spragų, ir išbandoma, ar IRT procesais, produktais arba paslaugomis tinkamai įgyvendinamos būtinos saugumo funkcinės galimybės;** arba, **jei tai netaikoma, turi būti vykdomi pakaitiniai tokio paties poveikio veiksmai[...].**

c) **Europos kibernetinio saugumo sertifikatu, kuriuo patvirtinimas „**aukštas**“** saugumo užtikrinimo lygis, **garantuojama, kad IRT procesai, produktai ir paslaugos tenkina atitinkamus saugumo reikalavimus, be kita ko, saugumo funkcinių galimybių atžvilgiu, ir buvo atliktas tokio lygmens jų įvertinimas, kad būtų kuo labiau sumažinta naujausiomis technologijomis pagrįstų kibernetinių išpuolių, kuriuos vykdo aukšto lygio įgūdžių ir didelių išteklių turintys subjektai, rizika. Atliekant vertinimo veiksmus mažų mažiausiai įvertinama, ar nėra viešai žinomų spragų, ir išbandoma, ar IRT procesuose, produktuose arba paslaugose tinkamai įgyvendinamos būtinos naujausiomis technologijomis pagrįstos saugumo funkcinės galimybės, ir, atliekant skverbties bandymą, įvertinamas jų atsparumas prieš aukšto lygio įgūdžių turinčių subjektų išpuolius; arba**, **jei tai netaikoma, atliekami pakaitiniai tokio paties poveikio veiksmai**[...]**.**

2a. Europos kibernetinio saugumo sertifikavimo schemoje gali būti nurodyti keli vertinimo lygiai, priklausomai nuo taikomos vertinimo metodikos griežtumo ir išsamumo. Kiekvienas vertinimo lygis turi atitikti vieną iš saugumo užtikrinimo lygių ir apibrėžiamas pagal tinkamą saugumo užtikrinimo komponentų derinį.

47 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų elementai

1. Europos kibernetinio saugumo sertifikavimo schemą sudaro **bent** šie elementai:

a) sertifikavimo **schemos** dalykas ir apimtis, įskaitant sertifikuojamų IRT **procesų**, produktų ir paslaugų rūšį arba kategorijas, **taip pat išaiškinimą, rodantį, kaip sertifikavimo schema atitinka tikėtinų tikslinių grupių poreikius**;

b) [...]nuoroda į [...]tarptautinius, **europinius ar nacionalinius** standartus**, kuriais vadovaujamasi vertinime**. **Jeigu tokių standartų nėra, daroma nuoroda į** [...]technines specifikacijas, **atitinkančias Reglamento 1025/2012 II priedo reikalavimus, arba, jeigu tokių nėra, į technines specifikacijas arba kitus kibernetinio saugumo reikalavimus, apibrėžtus schemoje**;

c) kai taikoma, vienas ar daugiau saugumo užtikrinimo lygiai;

ca) jei taikytina, specialūs ar papildomi reikalavimai, taikomi atitikties vertinimo įstaigoms, siekiant garantuoti jų techninę kompetenciją kibernetinio saugumo reikalavimų įvertinimo srityje;

d) naudojami specifiniai vertinimo kriterijai ir metodai, įskaitant vertinimo rūšis, siekiant įrodyti, kad konkretūs 45 straipsnyje nurodyti tikslai yra pasiekti;

e) **jei taikytina**, informacija, kurią pareiškėjas turi pateikti **arba su kuria turi kitaip leisti susipažinti** atitikties vertinimo įstaigoms ir kuri yra reikalinga sertifikavimui;

f) jeigu schemoje numatomas ženklų arba etikečių naudojimas, tokių ženklų arba etikečių naudojimo sąlygos;

g) [...]sertifikatų **arba ES atitikties pareiškimo** reikalavimų laikymosi stebėsenos taisyklės, įskaitant mechanizmus, kuriais įrodoma, kad nuolat laikomasi nurodytų kibernetinio saugumo reikalavimų;

h) **jei taikytina**, **sertifikato** suteikimo **ir atnaujinimo** sąlygos, **taip pat** sertifikavimo taikymo srities išlaikymo, tęsimo, išplėtimo **arba** sumažinimo sąlygos;

i) taisyklės, susijusios su sertifikuotų **ar savarankiško atitikties vertinimo** IRT produktų ir paslaugų neatitikties [...]**schemos** reikalavimams padariniais;

j) taisyklės, nustatančios, kaip turi būti pranešta apie anksčiau nenustatytas IRT **procesų,** produktų ir paslaugų kibernetinio saugumo spragas ir kaip jos turi būti šalinamos;

k) **jei taikytina,** taisyklės dėl atitikties vertinimo įstaigų įrašų laikymo;

l) informacija apie nacionalines **arba tarptautines** kibernetinio saugumo sertifikavimo schemas, taikomas tos pačios rūšies ar kategorijų IRT **procesams**, produktams ir paslaugoms, **saugumo reikalavimus ir vertinimo kriterijus bei metodus**;

m) išduoto sertifikato **arba ES atitikties pareiškimo** turinys;

ma) laikotarpis, kurį IRT produktų gamintojas ar paslaugų teikėjas turi saugoti ES atitikties pareiškimą ir techninę dokumentaciją, kurioje pateikiama visa susijusi informacija;

mb[...]) didžiausias sertifikatų galiojimo laikotarpis;

mc[...]) suteiktų, pakeistų ar atšauktų sertifikatų atskleidimo politika;

md[...]) sertifikavimo schemų tarpusavio pripažinimo susitarimų su trečiosiomis šalimis sąlygos;

me[...]) jei taikytina, taisyklės, susijusios su tarpusavio vertinimo mechanizmu, skirtu Europos kibernetinio saugumo sertifikatų išdavimo institucijoms, siekiant aukšto saugumo užtikrinimo lygio [...]pagal 48 straipsnio 4a dalį.

2. Nurodyti schemos reikalavimai neturi prieštarauti bet kokiems taikytiniems teisiniams reikalavimams, visų pirma suderintais Sąjungos teisės aktais nustatytiems reikalavimams.

3. Kai tai numatoma konkrečiame Sąjungos teisės akte, sertifikavimas **arba ES atitikties pareiškimas** pagal Europos kibernetinio saugumo sertifikavimo schemą gali būti naudojamas siekiant įrodyti atitikties to teisės akto reikalavimams prielaidą.

4. Nesant suderintų Sąjungos teisės aktų, valstybės narės teisės aktuose taip pat gali būti numatyta, kad siekiant įrodyti atitikties teisiniams reikalavimams prielaidą gali būti naudojama Europos kibernetinio saugumo sertifikavimo schema.

47a straipsnis

Savarankiškas atitikties vertinimas

1. Europos kibernetinio saugumo sertifikavimo schemoje gali būti nustatyta galimybė, kad atitikties vertinimas vykdomas tik IRT produktų gamintojo arba paslaugų teikėjo atsakomybe. Toks atitikties vertinimas taikomas tik nedidelės rizikos IRT produktams ir paslaugoms, atitinkant bazinį saugumo užtikrinimo lygį.

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

3. IRT produktų gamintojas arba paslaugų teikėjas privalo atitinkamoje Europos kibernetinio saugumo sertifikavimo schemoje nurodytą laikotarpį saugoti ES atitikties pareiškimą ir visos aktualios informacijos, susijusios su IRT produktų ar paslaugų atitiktimi schemai, techninę dokumentaciją, kad galėtų juos pateikti nacionalinei kibernetinio saugumo sertifikavimo institucijai, nurodytai 50 straipsnio 1 dalyje. ES atitikties pareiškimo kopija pateikiama nacionalinei sertifikavimo priežiūros institucijai ir ENISA.

4. ES atitikties pareiškimo išdavimas yra savanoriškas, išskyrus atvejus, kai Sąjungos ar valstybių narių teisėje nurodyta kitaip.

5. Pagal šį straipsnį išduotas ES atitikties pareiškimas pripažįstamas visose valstybėse narėse.

48 straipsnis

Kibernetinio saugumo sertifikavimas

1. Laikoma, kad pagal Europos kibernetinio saugumo sertifikavimo schemą, patvirtintą pagal 44 straipsnį, sertifikuoti IRT **procesai**, produktai ir paslaugos atitinka tos schemos reikalavimus.

2. Sertifikavimas yra savanoriškas, išskyrus atvejus, kai Sąjungos **ar valstybių narių** teisėje nustatyta kitaip.

3. Europos kibernetinio saugumo sertifikatą, pagal šį straipsnį **patvirtinantį bazinio arba pakankamo saugumo užtikrinimo lygį**, išduoda 51 straipsnyje nurodytos atitikties vertinimo įstaigos remdamosi kriterijais, įtrauktais į Europos kibernetinio saugumo sertifikavimo schemą, patvirtintą pagal 44 straipsnį.

4. [...]Nukrypstant nuo 3 dalies, tinkamai pagrįstais atvejais konkrečioje Europos kibernetinio saugumo **sertifikavimo** schemoje gali būti nustatyta, kad Europos kibernetinio saugumo sertifikatą pagal tą schemą gali išduoti tik viešoji įstaiga. Tokia [...]įstaiga yra viena iš šių įstaigų:

a) 50 straipsnio 1 dalyje nurodyta nacionalinė **kibernetinio saugumo** sertifikavimo [...]institucija;

b) **viešoji** įstaiga, kuri pagal 51 straipsnio 1 dalį yra akredituota kaip atitikties vertinimo įstaiga [...]

c) […].

4a. Tais atvejais, kai pagal 44 straipsnį Europos kibernetinio saugumo sertifikavimo schemoje reikalaujama užtikrinti aukštą saugumo užtikrinimo lygį, sertifikatą išduoti gali tik 50 straipsnio 1 dalyje nurodyta nacionalinė kibernetinio saugumo sertifikavimo institucija arba 51 straipsnyje nurodyta atitikties vertinimo įstaiga, laikantis toliau nurodytų sąlygų:

a) dėl kiekvieno atitikties vertinimo įstaigos išduodamo sertifikato turi būti gautas išankstinis nacionalinės kibernetinio saugumo sertifikavimo institucijos patvirtinimas; arba

b) nacionalinė kibernetinio sertifikavimo institucija turi būti iš anksto suteikusi bendrus įgaliojimus dėl šios užduoties atitikties vertinimo įstaigai.

5. Savo IRT **procesus**, produktus ir paslaugas sertifikuoti teikiantis fizinis arba juridinis asmuo [...]**leidžia susipažinti** 51 straipsnyje nurodytai atitikties vertinimo įstaigai **arba 50 straipsnyje nurodytai nacionalinei kibernetinio saugumo sertifikavimo institucijai, kai ši institucija yra sertifikatą išduodanti įstaiga, [...]**su visa sertifikavimo procedūrai atlikti reikalinga informacija.

5a. Sertifikato turėtojas informuoja sertifikatą išduodančią įstaigą apie su sertifikuotu IRT procesu, produktu ar paslauga susijusias vėliau nustatytas spragas ar pažeidimus, kurie gali daryti poveikį su sertifikavimu susijusiems reikalavimams. Ta įstaiga nepagrįstai nedelsdama perduoda šią informaciją nacionalinei kibernetinio saugumo sertifikavimo institucijai.

6. Sertifikatai išduodami [...]**konkrečios sertifikavimo schemos nustatytam laikotarpiui** ir gali būti atnaujinami, [...]jeigu ir toliau atitinkami susiję reikalavimai.

7. Pagal šį straipsnį išduotas Europos kibernetinio saugumo sertifikatas pripažįstamas visose valstybėse narėse.

49 straipsnis

Nacionalinės kibernetinio saugumo sertifikavimo schemos ir sertifikatai

1. Nedarant poveikio 3 dalies taikymui, nacionalinės kibernetinio saugumo sertifikavimo schemos ir susijusios procedūros, taikomos IRT **procesams**, produktams ir paslaugoms, kuriems taikoma Europos kibernetinio saugumo sertifikavimo schema, netenka galios nuo pagal 44 straipsnio 4 dalį priimtame įgyvendinimo akte nustatytos datos. **N**acionalinės kibernetinio saugumo sertifikavimo schemos ir susijusios procedūros, taikomos IRT **procesams**, produktams ir paslaugoms, kuriems Europos kibernetinio saugumo sertifikavimo schema netaikoma, galioja ir toliau.

2. Valstybės narės neįveda naujų nacionalinių kibernetinio saugumo sertifikavimo schemų IRT **procesams**, produktams ir paslaugoms, kuriems taikoma Europos kibernetinio saugumo sertifikavimo schema.

3. Esami pagal nacionalines kibernetinio saugumo sertifikavimo schemas išduoti sertifikatai, **kuriems taikoma Europos kibernetinio saugumo sertifikavimo schema**, toliau galioja iki jų galiojimo pabaigos datos.

50 straipsnis

Nacionalinės* kibernetinio *saugumo sertifikavimo[...] institucijos

1. Kiekviena valstybė narė **savo teritorijoje [...]paskiria vieną** nacionalinę **kibernetinio saugumo** sertifikavimo [...]instituciją **arba kelias** tokias institucijas, **arba, sudariusi abipusį susitarimą su kita valstybe nare, paskiria toje kitoje valstybėje narėje įsisteigusią instituciją arba kelias institucijas būti atsakinga (-omis) už priežiūros užduotis paskyrusioje valstybėje narėje**.

2. Kiekviena valstybė narė praneša Komisijai apie **paskirtas institucijas [...]ir joms pavestas užduotis**.

3. **Nedarant poveikio 48 straipsnio 4 dalies a punktui ir 48 straipsnio 4a daliai,** [...]**k**iekvienos nacionalinės **kibernetinio saugumo** sertifikavimo [...]institucijos veiklos organizavimas, finansavimo sprendimai, teisinė struktūra ir sprendimų priėmimas nepriklauso nuo prižiūrimų subjektų.

3a. Valstybės narės užtikrina, kad nacionalinė kibernetinio saugumo sertifikavimo institucija, vykdydama su sertifikatų išdavimu pagal 48 straipsnio 4 dalies a punktą ir 48 straipsnio 4a dalį susijusią veiklą, laikytųsi griežto savo funkcijų ir pareigų atskyrimo nuo šiame straipsnyje nustatytos priežiūros veiklos, ir kad abiejų rūšių veikla būtų vykdoma tarpusavyje nepriklausomai.

4. Valstybės narės užtikrina, kad nacionalinės **kibernetinio saugumo** [...]sertifikavimo institucijos turėtų pakankamai išteklių savo įgaliojimams ir pavestoms užduotims veiksmingai bei efektyviai vykdyti.

5. Siekiant užtikrinti veiksmingą šio reglamento įgyvendinimą, tikslinga, kad šios institucijos aktyviai, veiksmingai, efektyviai ir saugiai dalyvautų pagal 53 straipsnį įsteigtos Europos kibernetinio saugumo sertifikavimo grupės veikloje.

6. Nacionalinės **kibernetinio saugumo** [...]sertifikavimo institucijos:

a) […]

aa) stebi, kaip jų atitinkamose teritorijose įsisteigę IRT produktų gamintojai arba paslaugų teikėjai vykdo 47a straipsnio 2 ir 3 dalyse ir atitinkamoje Europos kibernetinio saugumo sertifikavimo schemoje nustatytus įpareigojimus, ir užtikrina jų vykdymą;

b) [...]**nedarant poveikio 51 straipsnio 1b daliai, padeda nacionalinėms akreditavimo įstaigoms vykdyti** atitikties vertinimo įstaigų veiksmų **stebėsenos ir priežiūros** veiklą, kaip nustatyta šiame reglamente[...];

ba) stebi ir prižiūri 48 straipsnio 4 dalyje nurodytų įstaigų veiklą;

bb) teikia įgaliojimus atitikties vertinimo įstaigoms, nurodytoms 51 straipsnio 1b dalyje, ir apriboja, sustabdo arba atšaukia suteiktus įgaliojimus šio reglamento reikalavimų nesilaikymo atveju;

c) nagrinėja fizinių ar juridinių asmenų pateiktus skundus, susijusius su [...]**nacionalinės kibernetinio saugumo sertifikavimo institucijos arba, remiantis 48 straipsnio 4a dalimi, atitikties vertinimo įstaigų** išduotais sertifikatais, tiria, kiek įmanoma, skundo dalyką ir per pagrįstą laikotarpį informuoja skundo teikėją apie tyrimo eigą ir rezultatus;

d) bendradarbiauja su kitomis nacionalinėmis **kibernetinio saugumo** sertifikavimo [...]institucijomis ar kitomis valdžios institucijomis, be kita ko, dalydamosi informacija apie galimą IRT **procesų**, produktų ir paslaugų neatitiktį šio reglamento arba konkrečių Europos kibernetinio saugumo sertifikavimo schemų reikalavimams;

e) stebi aktualius kibernetinio saugumo sertifikavimo srities pokyčius.

7. Kiekviena nacionalinė **kibernetinio saugumo** sertifikavimo [...]institucija turi bent šiuos įgaliojimus:

a) prašyti atitikties vertinimo įstaigų**,** [...]Europos kibernetinio saugumo sertifikatų turėtojų **ir ES atitikties pareiškimo išdavėjų** pateikti bet kokią informaciją, kurios jai reikia savo užduotims atlikti;

b) vykdyti tiriamąjį atitikties vertinimo įstaigų**,** [...]Europos kibernetinio saugumo sertifikatų turėtojų ir **ES atitikties pareiškimo išdavėjų** auditą siekiant patikrinti, ar laikomasi III antraštinės dalies nuostatų;

c) pagal nacionalinę teisę imtis atitinkamų priemonių siekiant užtikrinti, kad atitikties vertinimo įstaigos**,** [...]sertifikatų turėtojai **ir ES atitikties pareiškimo išdavėjai** laikytųsi šio reglamento arba Europos kibernetinio saugumo sertifikavimo schemos reikalavimų;

d) gauti leidimą patekti į visas atitikties vertinimo įstaigų ir Europos kibernetinio saugumo sertifikatų turėtojų patalpas, kad galėtų vykdyti tyrimus pagal Sąjungos arba valstybės narės proceso teisę;

e) pagal nacionalinę teisę panaikinti sertifikatus, **išduotus nacionalinės kibernetinio saugumo sertifikavimo institucijos arba pagal 48 straipsnio 4a dalį išduotus atitikties vertinimo įstaigų,** kurie neatitinka šio reglamento arba Europos kibernetinio saugumo sertifikavimo schemos reikalavimų;

f) pagal nacionalinę teisę taikyti sankcijas, kaip numatyta 54 straipsnyje, ir reikalauti nedelsiant nutraukti šiame reglamente nustatytų įpareigojimų nesilaikymą.

8. Nacionalinės **kibernetinio saugumo** sertifikavimo [...]institucijos bendradarbiauja tarpusavyje ir su Komisija ir, visų pirma, keičiasi informacija, patirtimi ir gerosios praktikos pavyzdžiais, susijusiais su kibernetinio saugumo sertifikavimu ir techniniais IRT **procesų**, produktų ir paslaugų kibernetinio saugumo klausimais.

51 straipsnis

Atitikties vertinimo įstaigos

1. Atitikties vertinimo įstaigas akredituoja pagal Reglamentą (EB) Nr. 765/2008 paskirta nacionalinė akreditacijos įstaiga tik jei jos atitinka šio reglamento priede išdėstytus reikalavimus.

1a. Tais atvejais, kai Europos kibernetinio saugumo sertifikatą išduoda nacionalinė kibernetinio saugumo sertifikavimo institucija pagal 48 straipsnį 4 dalies a punktą ir 48 straipsnio 4a dalį, nacionalinės kibernetinio saugumo sertifikavimo institucijos sertifikavimo įstaiga yra akredituota kaip atitikties vertinimo įstaiga pagal šio straipsnio 1 dalį.

1b. Jei taikytina, atitikties vertinimo įstaigos nacionalinės kibernetinio saugumo institucijos įgaliojamos vykdyti jos veiksmus, kai jos atitinka specialius ar papildomus reikalavimus, išdėstytus Europos sertifikavimo schemoje pagal 47 straipsnio 1 dalies ca punktą.

2. Akreditacija suteikiama ne ilgesniam kaip penkerių metų laikotarpiui ir gali būti pratęsta tomis pačiomis sąlygomis, jei atitikties vertinimo įstaiga toliau atitinka šiame straipsnyje nustatytus reikalavimus. Akreditacijos įstaigos **imasi visų tinkamų priemonių per pagrįstą terminą, siekdamos apriboti, sustabdyti arba** atšaukti atitikties vertinimo įstaigos akreditaciją pagal šio straipsnio 1 dalį, jeigu netenkinamas ar nebetenkinamos akreditacijos sąlygos, arba jeigu atitikties vertinimo įstaigos veiksmai pažeidžia šį reglamentą.

52 straipsnis

Notifikavimas

1. Kiekvienos pagal 44 straipsnį patvirtintos Europos kibernetinio saugumo sertifikavimo schemos atveju nacionalinės **kibernetinio saugumo** [...]sertifikavimo institucijos praneša Komisijai apie [...]atitikties vertinimo įstaigas, akredituotas **ir, jei taikytina, pagal 51 straipsnio 1b dalį įgaliotas** išduoti 46 straipsnyje nurodytų nustatytų saugumo užtikrinimo lygių sertifikatus ir, be reikalo nedelsdamos, apie visus vėlesnius jų pasikeitimus.

2. Praėjus vieniems metams po Europos kibernetinio saugumo sertifikavimo schemos įsigaliojimo Komisija Oficialiajame leidinyje paskelbia notifikuotųjų atitikties vertinimo įstaigų sąrašą.

3. Jei Komisija gauna pranešimą pasibaigus **2**[...] dalyje nurodytam laikotarpiui, ji per du mėnesius nuo to pranešimo gavimo dienos Europos Sąjungos oficialiajame leidinyje paskelbia 2 dalyje nurodyto sąrašo pakeitimus.

4. Nacionalinė **kibernetinio saugumo** sertifikavimo [...]institucija gali pateikti Komisijai prašymą iš šio straipsnio 2 dalyje nurodyto sąrašo išbraukti tos valstybės narės notifikuotą atitikties vertinimo įstaigą. Komisija atitinkamus sąrašo pakeitimus Europos Sąjungos oficialiajame leidinyje paskelbia per vieną mėnesį nuo nacionalinės **kibernetinio saugumo** sertifikavimo [...]institucijos prašymo gavimo dienos.

5. Komisija gali priimti įgyvendinimo aktus, kuriais apibrėžia pranešimo teikimo pagal šio straipsnio 1 dalį aplinkybes, formatus ir procedūras. Tie įgyvendinimo aktai priimami laikantis 55 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

53 straipsnis

Europos kibernetinio saugumo sertifikavimo grupė

1. Įsteigiama Europos kibernetinio saugumo sertifikavimo grupė (toliau – grupė).

2. Grupę sudaro nacionalinių **kibernetinio saugumo** sertifikavimo [...]institucijų **atstovai arba kitų susijusių nacionalinių institucijų atstovai**. [...]**Bet kuris grupės narys gali atstovauti ne daugiau kaip vienai kitai valstybei narei.**

3. Grupės užduotys yra šios:

a) konsultuoti Komisiją ir padėti jai užtikrinti nuoseklų šios antraštinės dalies įgyvendinimą ir taikymą, visų pirma susijusį su kibernetinio saugumo sertifikavimo politikos klausimais, politinių požiūrių koordinavimu ir Europos kibernetinio saugumo sertifikavimo schemų rengimu;

b) padėti, patarti ir bendradarbiauti su ENISA rengiant potencialią schemą pagal šio reglamento 44 straipsnį;

ba) priimti nuomonę dėl potencialios schemos pagal šio reglamento 44 straipsnį;

c) [...]**paprašyti** Agentūros parengti potencialią Europos kibernetinio saugumo sertifikavimo schemą pagal šio reglamento 44 straipsnį;

ca) parengti ir priimti gaires dėl vertinimo kriterijų, skirtų įvertinti pasiūlymus dėl potencialios schemos rengimo, teikiamus [...]grupei pagal 44 straipsnio 1a dalį;

d) priimti Komisijai skirtas nuomones, susijusias su esamų Europos kibernetinio saugumo sertifikavimo schemų priežiūra ir peržiūra;

e) nagrinėti aktualius kibernetinio saugumo sertifikavimo srities pokyčius ir keistis gerosios patirties pavyzdžiais, susijusiais su kibernetinio saugumo sertifikavimo schemomis;

f) sudaryti palankesnes sąlygas nacionalinėms **kibernetinio saugumo** sertifikavimo [...]institucijoms bendradarbiauti pagal šią antraštinę dalį pasitelkiant **pajėgumų stiprinimą ir keitimąsi informacija**, visų pirma nustatant efektyvaus keitimosi informacija visais kibernetinio saugumo sertifikavimo klausimais metodus**;**

fa) remti tarpusavio vertinimo mechanizmo įgyvendinimą pagal taisykles, nustatytas Europos kibernetinio saugumo sertifikavimo schemoje pagal šio reglamento 47 straipsnio 1 dalies md punktą.

4. Komisija pirmininkauja grupei, **atlikdama moderatoriaus funkcijas**, ir, kaip numatyta 8 straipsnio a punkte, padedama agentūros ENISA teikia sekretoriato paslaugas.

53a straipsnis

Teisė pateikti skundą nacionalinei **kibernetinio saugumo** ***sertifikavimo [...]institucijai***

1. Fiziniai ar juridiniai asmenys turi teisę pateikti skundą nacionalinei kibernetinio saugumo sertifikavimo institucijai dėl tos pačios institucijos arba, pagal 48 straipsnio 4a dalį, atitikties vertinimo įstaigų išduoto sertifikato.

2. Nacionalinė kibernetinio saugumo sertifikavimo institucija, kuriai pateiktas skundas, informuoja skundo pateikėją apie skundo nagrinėjimo pažangą ir rezultatus, be kita ko, apie galimybę imtis teisminių teisių gynimo priemonių pagal 53b straipsnį.

53b straipsnis

Teisė į veiksmingas teismines teisių gynimo priemones

1. Fiziniai ar juridiniai asmenys turi teisę į veiksmingas teismines teisių gynimo priemones, reaguojant į su jais susijusį teisiškai įpareigojantį nacionalinės kibernetinio saugumo sertifikavimo institucijos sprendimą.

2. Fiziniai ar juridiniai asmenys turi teisę į veiksmingas teismines teisių gynimo priemones tais atvejais, kai nacionalinė kibernetinio saugumo sertifikavimo institucija nenagrinėja skundo.

3. Teisminiai procesai prieš nacionalinę kibernetinio saugumo sertifikavimo instituciją pradedami valstybės narės, kurioje ta institucija yra įsisteigusi, teismuose.

54 straipsnis

Sankcijos

Valstybės narės nustato taisykles, kuriomis reglamentuojamos už šios antraštinės dalies ir Europos kibernetinio saugumo sertifikavimo schemų nuostatų pažeidimus taikytinos sankcijos, ir imasi visų reikiamų priemonių, kad užtikrintų jų įgyvendinimą. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos. Valstybės narės [ne vėliau kaip …/nedelsdamos] praneša apie tas taisykles ir tas priemones Komisijai ir jai praneša apie visus vėlesnius joms įtakos turinčius pakeitimus.

IV ANTRAŠTINĖ DALIS
BAIGIAMOSIOS NUOSTATOS

55 straipsnis

Komiteto procedūra

1. Komisijai padeda komitetas. Tas komitetas – tai komitetas, kaip nustatyta Reglamente (ES) Nr. 182/2011.

2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnio **4 dalies b punktas**.

56 straipsnis

Vertinimas ir peržiūra

1. Ne vėliau kaip po penkerių metų nuo 58 straipsnyje nurodytos datos, o vėliau kas penkerius metus Komisija įvertina Agentūros ir jos darbo metodų poveikį, veiksmingumą ir naudingumą ir galimą poreikį keisti Agentūros įgaliojimus bei tokio pakeitimo finansinį poveikį. Atliekant vertinimą atsižvelgiama į grįžtamąją informaciją, pateiktą Agentūrai reaguojant į jos veiklą. Jei Komisija mano, kad Agentūros veikla nebepateisinama jos tikslais, įgaliojimais ir uždaviniais, ji gali siūlyti su Agentūra susijusias šio reglamento nuostatas iš dalies pakeisti.

2. Taip pat įvertinamas III antraštinės dalies nuostatų poveikis, veiksmingumas ir naudingumas siekiant tikslų užtikrinti tinkamą IRT produktų ir paslaugų Sąjungoje kibernetinio saugumo lygį ir gerinti vidaus rinkos veikimą.

3. Komisija vertinimo ataskaitą kartu su savo išvadomis perduoda Europos Parlamentui, Tarybai ir Valdančiajai tarybai. Vertinimo ataskaitos išvados skelbiamos viešai.

57 straipsnis

Panaikinimas ir tęstinumas

1. Reglamentas (ES) Nr. 526/2013 panaikinamas nuo […].

2. Nuorodos į Reglamentą (ES) Nr. 526/2013 ir į ENISA laikomos nuorodomis į šį reglamentą ir Agentūrą.

3. Agentūra perima visą Reglamentu (ES) Nr. 526/2013 įsteigtos agentūros nuosavybę, susitarimus, teisinius įsipareigojimus, darbo sutartis, finansinius įsipareigojimus ir atsakomybę. Visi esami Valdančiosios tarybos ir Vykdomosios valdybos sprendimai lieka galioti, jei jie neprieštarauja šio reglamento nuostatoms.

4. Agentūra įsteigiama neterminuotam laikotarpiui nuo [...]

5. Pagal Reglamento (ES) Nr. 526/2013 24 straipsnio 4 dalį paskirtas vykdomasis direktorius yra Agentūros vykdomasis direktorius likusį savo kadencijos laiką.

6. Pagal Reglamento (ES) Nr. 526/2013 6 straipsnį paskirti Valdančiosios tarybos nariai ir jų pakaitiniai nariai yra Agentūros Valdančiosios tarybos nariai ir jų pakaitiniai nariai likusį savo kadencijos laiką.

58 straipsnis

Įsigaliojimas

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

1a. Šis reglamentas taikomas nuo [...], išskyrus 50, 51, 52, 53a, 53b ir 54 straipsnius, kurie taikomi nuo [24 mėnesiai nuo jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* dienos].

2. Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas	*Pirmininkas*

PRIEDAS

REIKALAVIMAI, KURIUOS TURI ATITIKTI ATITIKTIES VERTINIMO ĮSTAIGOS

Akreditacijos siekiančios atitikties vertinimo įstaigos turi atitikti šiuos reikalavimus:

1. Atitikties vertinimo įstaiga turi būti įsteigta pagal nacionalinę teisę ir turėti teisinį subjektiškumą.

2. Atitikties vertinimo įstaiga yra trečioji šalis, nepriklausoma nuo vertinamos organizacijos ar IRT produktų ar paslaugų.

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

4. Atitikties vertinimo įstaiga, jos aukščiausio lygio vadovai ir už atitikties vertinimo užduotis atsakingi darbuotojai negali būti vertinamo IRT produkto ar paslaugos projektuotojai, gamintojai, tiekėjai, montuotojai, pirkėjai, savininkai, naudotojai ar prižiūrėtojai arba tų šalių įgaliotieji atstovai. Tai netrukdo atitikties vertinimo įstaigai naudoti įvertintų produktų, kurie yra būtini jos veiklai, arba tokius produktus naudoti asmeniniais tikslais.

5. Atitikties vertinimo įstaiga, jos aukščiausiojo lygio vadovai ir už atitikties vertinimo užduočių atlikimą atsakingi darbuotojai tiesiogiai nedalyvauja projektuojant, gaminant ar konstruojant, parduodant, įrengiant, naudojant ar prižiūrint tuos IRT produktus ar paslaugas, taip pat negali atstovauti toje veikloje dalyvaujančioms šalims. Jie nesiima jokios veiklos, kuri jiems trukdytų nepriklausomai ir sąžiningai priimti sprendimus, susijusius su atitikties vertinimo veikla, dėl kurios apie juos pranešta. Tai visų pirma taikoma konsultacinėms paslaugoms.

6. Atitikties vertinimo įstaigos užtikrina, kad joms pavaldžių įstaigų ar subrangovų veikla neturėtų poveikio jų atitikties vertinimo veiklos konfidencialumui, objektyvumui ar nešališkumui.

7. Atitikties vertinimo įstaigos ir jų darbuotojai atitikties vertinimo veiklą vykdo laikydamiesi griežčiausių profesinio sąžiningumo reikalavimų, turi reikiamą konkrečios srities techninę kompetenciją ir jiems nedaromas joks spaudimas ir neteikiamos jokios paskatos, įskaitant finansinio pobūdžio, kurie galėtų paveikti jų sprendimą ar atitikties vertinimo veiklos rezultatus, ypač jei tai susiję su tos veiklos rezultatais suinteresuotais asmenimis ar asmenų grupėmis.

8. Atitikties vertinimo įstaiga turi pajėgti atlikti visas atitikties vertinimo užduotis, kurios jai paskirtos remiantis šiuo reglamentu, nesvarbu, ar tas užduotis vykdo pati atitikties vertinimo įstaiga, ar jos vykdomos jos vardu ir jos atsakomybe.

9. Visais atvejais kiekvienai atitikties vertinimo procedūrai vykdyti ir kiekvienos rūšies, kategorijos ar pakategorės IRT produktų ar paslaugų atitikčiai įvertinti atitikties vertinimo įstaiga turi turėti reikalingų:

a) darbuotojų, turinčių techninių žinių ir pakankamos bei tinkamos patirties atitikties vertinimo užduotims atlikti;

b) procedūrų, pagal kurias vertinama atitiktis, aprašymų, taip užtikrinant tų procedūrų skaidrumą ir galimybę jas pakartoti. Ji turi taikyti tinkamą politiką ir procedūras, kuriomis užtikrinamas užduočių, kurias ji atlieka kaip notifikuotoji įstaiga, ir kitos veiklos atskyrimas;

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

10. Atitikties vertinimo įstaiga turi turėti reikiamų priemonių su atitikties vertinimo veikla susijusioms techninėms ir administracinėms užduotims tinkamai atlikti ir galimybę naudotis visa reikiama įranga ir įrenginiais.

11. Už atitikties vertinimo veiklos vykdymą atsakingi darbuotojai turi:

a) turėti tinkamą techninį ir profesinį parengimą, apimantį visą atitikties vertinimo veiklą;

b) pakankamai gerai išmanyti atliekamo vertinimo reikalavimus ir turėti reikiamus įgaliojimus jį atlikti;

c) turėti reikiamų žinių ir išmanyti taikomus reikalavimus ir bandymo standartus;

d) turėti gebėjimų rengti sertifikatus, įrašus ir ataskaitas, kuriais patvirtinama, kad vertinimas atliktas.

12. Užtikrinamas atitikties vertinimo įstaigų, jų aukščiausio lygio vadovų ir vertinimą atliekančių darbuotojų nešališkumas.

13. Atitikties vertinimo įstaigos aukščiausio lygio vadovų ir vertinimą atliekančių darbuotojų atlyginimas nepriklauso nuo atliktų vertinimų skaičiaus ar tų vertinimų rezultatų.

14. Atitikties vertinimo įstaigos apsidraudžia atsakomybės draudimu, išskyrus atvejus, kai atsakomybę pagal nacionalinės teisės aktus prisiima valstybė arba kai pati valstybė narė tiesiogiai atsako už atitikties vertinimą.

15. Atitikties vertinimo įstaigos darbuotojai laikosi profesinio slaptumo reikalavimo, taikomo visai informacijai, kurią jie gauna atlikdami užduotis pagal šį reglamentą arba bet kurią nacionalinės teisės aktų nuostatą, kuria jis įgyvendinamas, išskyrus atvejus, susijusius su valstybės narės, kurioje vykdoma veikla, kompetentingomis institucijomis.

16. Atitikties vertinimo įstaigos atitinka reikalavimus pagal susijusį standartą, **kuris yra suderintas pagal Reglamentą (EB) 765/2008 atitikties vertinimo įstaigų, vykdančių procesų, produktų ar paslaugų sertifikavimą, akreditavimo[...] tikslais**.

17. Atitikties vertinimo įstaigos užtikrina, kad atitikčiai vertinti naudojamos bandymų laboratorijos atitiktų reikalavimus pagal **susijusį** standartą, **kuris yra suderintas pagal Reglamentą (EB) 765/2008 bandymus atliekančių laboratorijų akreditavimo tikslais**[...].