EUROPOS
KOMISIJA

Briuselis, 2018 02 22
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

dėl ES 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)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

AIŠKINAMASIS MEMORANDUMAS

1. PASIŪLYMO APLINKYBĖS

• Pasiūlymo pagrindimas ir tikslai

Europos Sąjunga ėmėsi veiksmų, kad taptų atsparesnė ir pagerintų savo kibernetinio saugumo pasirengimą. 2013 m. priimtoje pirmojoje ES kibernetinio saugumo strategijoje[1] nustatyti strateginiai tikslai ir konkretūs veiksmai, kuriais siekiama užtikrinti atsparumą, sumažinti kibernetinių nusikaltimų skaičių, parengti kibernetinės gynybos politiką ir plėtoti jos pajėgumus, didinti pramonės ir technologinius išteklius bei parengti ES nuoseklią tarptautinę kibernetinės erdvės politiką. Nuo to laiko, esant tokioms aplinkybėms, įvyko svarbių pokyčių, visų pirma Europos Sąjungos tinklų ir informacijos apsaugos agentūrai (ENISA)[2] antrąkart suteikti įgaliojimai ir priimta **Tinklų ir informacijos saugumo direktyva**[3] (TIS direktyva), kuri yra šio pasiūlymo pagrindas.

Be to, 2016 m. Europos Komisija priėmė **komunikatą „Europos kibernetinio atsparumo sistemos stiprinimas ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimas“**[4], kuriame pranešama apie tolesnes priemones, kad gerėtų bendradarbiavimas, būtų dalijamasi informacija ir žiniomis ir ES būtų atsparesnė bei geriau pasirengusi, taip pat ir atremti didelio masto incidentus ir galimą visos Europos kibernetinio saugumo krizę. Šiomis aplinkybėmis Komisija paskelbė, kad **įvertins** ir **peržiūrės** Europos Parlamento ir Tarybos reglamentą (ES) Nr. 526/2013 dėl ENISA, kuriuo panaikinamas Reglamentas (EB) Nr. 460/2004 (toliau – ENISA reglamentas). Po vertinimo būtų galima vykdyti Agentūros reformą ir padidinti jos galimybes ir pajėgumus tvariai remti valstybes nares. Taigi, Agentūrai būtų suteiktas operatyvesnis ir svarbesnis vaidmuo siekiant užtikrinti atsparumą kibernetinio saugumo srityje, o suteikiant naujus įgaliojimus būtų patvirtintos naujos jos pareigos pagal TIS direktyvą.

TIS direktyva yra pirmas esminis žingsnis, siekiant propaguoti rizikos valdymo kultūrą, nustatant saugumo reikalavimus kaip teisinius įpareigojimus pagrindiniams ekonominės veiklos vykdytojams, visų pirma esmines paslaugas teikiantiems operatoriams (esminių paslaugų operatoriams – EPO) ir kai kurių pagrindinių skaitmeninių paslaugų teikėjams (skaitmeninių paslaugų teikėjams – SPT). Atsižvelgiant į tai, kad saugumo reikalavimai yra svarbūs siekiant išsaugoti intensyvėjančio visuomenės skaitmeninimo teikiamą naudą, ir į spartų susietųjų įrenginių daugėjimą (daiktų internetas), 2016 m. komunikate taip pat pasiūlyta idėja sukurti IRT produktų ir paslaugų saugumo sertifikavimo sistemą, kad būtų užtikrintas didesnis pasitikėjimas ir saugumas bendrojoje skaitmeninėje rinkoje. IRT kibernetinio saugumo sertifikavimas tampa itin svarbus atsižvelgiant į tai, kad naudojama vis daugiau technologijų, kurių kibernetinio saugumo lygis turi būti aukštas (pvz., susietieji automatizuoti automobiliai, elektroninės sveikatos priežiūros arba pramoninės automatizacijos valdymo sistemos).

---

1 Europos Komisijos ir Europos išorės veiksmų tarnybos bendras komunikatas „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“, JOIN(2013).

2 Reglamentas (ES) Nr. 526/2013 dėl Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA), kuriuo panaikinamas Reglamentas (EB) Nr. 460/2004.

3 Direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

4 Komisijos komunikatas „Europos kibernetinio atsparumo sistemos stiprinimas ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimas“, COM/2016/0410 *final*.

Šios politikos priemonės ir pranešimai papildomai patvirtinti 2016 m. **Tarybos išvadose**, kuriose pripažįstama, kad „kibernetinės grėsmės ir pažeidžiamumas toliau vystosi ir stiprėja, ir dėl to būtinas nuolatinis ir glaudesnis bendradarbiavimas, visų pirma siekiant spręsti problemas, susijusias su didelio masto tarpvalstybiniais kibernetinio saugumo incidentais“. Išvadose dar kartą teigiama, kad „ENISA reglamentas yra vienas iš esminių ES kibernetinio atsparumo sistemos elementų“[5], o Komisija raginama imtis tolesnių veiksmų, kad sertifikavimo klausimas būtų sprendžiamas Europos lygmeniu.

Norint sukurti sertifikavimo sistemą, reikėtų ES lygmeniu nustatyti tinkamą valdymo sistemą, taip pat pasinaudojant nepriklausomos ES agentūros ekspertinėmis žiniomis. Atsižvelgiant į tai, šiame pasiūlyme ENISA nurodoma kaip savaime už kibernetinio saugumo klausimus atsakinga ES lygmens įstaiga, kuriai turėtų tekti funkcija telkti nacionalines kompetentingas sertifikavimo srities įstaigas ir koordinuoti jų darbą.

2017 m. gegužės mėn. komunikate **„Bendrosios skaitmeninės rinkos strategijos įgyvendinimo laikotarpio vidurio peržiūra“** Komisija papildomai patikslino, kad iki 2017 m. rugsėjo mėn. ji peržiūrės ENISA įgaliojimus. Taip siekiama apibrėžti jos vaidmenį pasikeitusioje kibernetinio saugumo ekosistemoje ir parengti priemones, susijusias su kibernetinio saugumo standartais, sertifikavimu ir ženklinimu, kad IRT pagrįstų sistemų, taip pat susietųjų objektų kibernetinis saugumas būtų didesnis[6]. 2017 m. birželio mėn. **Europos Vadovų Tarybos išvadose**[7] pritarta Komisijos ketinimui rugsėjo mėn. peržiūrėti Kibernetinio saugumo strategiją ir iki 2017 m. pabaigos pasiūlyti tolesnių tikslinių veiksmų.

Siūlomame reglamente numatomos ankstesniais veiksmais grindžiamos priemonės, kuriomis remiami vienas kitą papildantys konkretūs tikslai:

- didinti valstybių narių ir įmonių **pajėgumus bei pasirengimą**;
- gerinti valstybių narių ir ES institucijų, agentūrų bei įstaigų **bendradarbiavimą ir koordinavimą**;
- didinti **ES lygmens pajėgumus papildyti valstybių narių veiksmus**, ypač tarpvalstybinių kibernetinių krizių atveju;
- didinti piliečių ir įmonių **informuotumą** apie kibernetinį saugumą;
- didinti bendrą IRT produktų ir paslaugų **kibernetinio saugumo užtikrinimo skaidrumą**[8], siekiant stiprinti pasitikėjimą bendrąja skaitmenine rinka ir skaitmeninėmis inovacijomis; ir
- vengti **nereikalingos sertifikavimo schemų** ES ir susijusių reikalavimų bei vertinimo kriterijų visose valstybėse narėse ir sektoriuose gausos.

Tolesnėje aiškinamojo memorandumo dalyje išsamiau paaiškinama pagrindinė iniciatyvos priežastis, susijusi su siūlomais ENISA veiksmais ir kibernetinio saugumo sertifikavimu.

---

5 2016 m. lapkričio 15 d. Tarybos išvados dėl Europos kibernetinio atsparumo sistemos stiprinimo ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimo.

6 Komisijos komunikatas „Bendrosios skaitmeninės rinkos strategijos įgyvendinimo laikotarpio vidurio peržiūra“. COM(2017) 228.

7 Europos Vadovų Tarybos susitikimas (2017 m. birželio 22 ir 23 d.). Išvados EUCO 8/17.

8 Kibernetinio saugumo užtikrinimo skaidrumas reiškia, kad vartotojams suteikiama pakankamai informacijos apie kibernetinio saugumo savybes, ir tokiu būdu vartotojai gali objektyviai nustatyti atitinkamo IRT produkto, paslaugos ar proceso saugumo lygį.

ENISA

ENISA veikia kaip kompetencijos centras, kurio užduotis – stiprinti tinklų ir informacijos saugumą Sąjungoje ir remti valstybių narių pajėgumų stiprinimą.

ENISA įkurta 2004 m.[9], siekiant prisidėti prie bendro tikslo užtikrinti aukštą ES tinklų ir informacijos saugumo lygį įgyvendinimo. 2013 m. Reglamentu (ES) Nr. 526/2013 septynerių metų laikotarpiui iki 2020 m. nustatyti nauji Agentūros įgaliojimai. Agentūros biurai yra Graikijoje: administracinė buveinė įsikūrusi Heraklione (Kretoje), o pagrindinė veikla vykdoma Atėnuose.

ENISA yra nedidelė mažo biudžeto agentūra, kurioje, palyginti su visomis ES agentūromis, dirba nedaug darbuotojų. Jos įgaliojimai yra terminuoti.

ENISA padeda Europos institucijoms, valstybėms narėms ir verslo bendruomenei **spręsti tinklų ir informacijos apsaugos problemas, į jas reaguoti ir ypač užkirsti joms kelią**. Ji tai daro vykdydama įvairią, jos strategijoje nurodytų penkių sričių veiklą[10]:

- ekspertinės žinios: teikia informaciją ir ekspertines žinias pagrindiniais tinklų ir informacijos apsaugos klausimais;
- politika: remia politikos formavimą ir vykdymą Sąjungoje;
- pajėgumai: remia pajėgumų stiprinimą visoje Sąjungoje (pvz., rengdama mokymus, rekomendacijas, vykdydama informuotumo didinimo veiklą);
- bendruomenė: remia tinklų ir informacijos saugumo bendruomenę (pvz., teikia paramą kompiuterinių incidentų tyrimo tarnyboms (CERT), koordinuoja visos Europos kibernetines pratybas);
- galimybių užtikrinimas (pvz., suinteresuotųjų subjektų dalyvavimas ir tarptautiniai ryšiai).

Vykstant deryboms dėl TIS direktyvos, ES teisėkūros institucijos nusprendė skirti agentūrai ENISA svarbias šios direktyvos įgyvendinimo funkcijas. Visų pirma Agentūra atlieka CSIRT tinklo (įsteigto, siekiant skatinti greitą ir veiksmingą operatyvinį valstybių narių bendradarbiavimą įvykus tam tikriems kibernetinio saugumo incidentams ir dalytis informacija apie riziką) sekretoriato funkciją; į ją taip pat kreipiamasi, kai reikia padėti bendradarbiavimo grupei vykdyti savo užduotis. Be to, pagal direktyvą reikalaujama, kad ENISA padėtų valstybėms narėms ir Komisijai, teikdama ekspertines žinias ir konsultuodama bei padėdama keistis geriausia patirtimi.

Pagal ENISA reglamentą Komisija atliko Agentūros vertinimą, į kurį įtrauktas nepriklausomas tyrimas ir viešos konsultacijos. Vertinime įvertinta Agentūros svarba, poveikis, efektyvumas, veiksmingumas, suderinamumas ir papildoma nauda ES, visa tai susiejant su Agentūros veiklos rezultatais, valdymu, vidaus organizacine struktūra ir darbo praktika 2013–2016 m. laikotarpiu.

Viešose konsultacijose dauguma respondentų[11] (74 %) bendrą ENISA veiklą įvertino teigiamai. Dauguma respondentų taip pat manė, kad ENISA pasieks įvairius savo tikslus

---

9 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.

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy.

(kiekvieną tikslą įvykdys bent 63 %). ENISA paslaugomis ir produktais reguliariai (kartą per mėnesį arba dažniau) naudojasi beveik pusė respondentų (46 %); šios paslaugos ir produktai vertinami dėl to, kad gaunami iš ES lygmens įstaigos (83 %), ir dėl kokybės (62 %).

Vis dėlto didžioji dauguma respondentų (88 %) manė, kad dabartinės ES lygmens priemonės ir mechanizmai yra nepakankami arba tik iš dalies pakankami dabartinėms kibernetinio saugumo problemoms spręsti. Didžioji dauguma respondentų (98 %) nurodė, kad į šiuos poreikius turėtų atsižvelgti ES įstaiga, o 99 % iš jų manė, kad ENISA yra tam tinkama organizacija. Be to, 67,5 % respondentų išreiškė nuomonę, kad ENISA galėtų atlikti tam tikrą vaidmenį sukuriant suderintą IT produktų ir paslaugų saugumo sertifikavimo sistemą.

Po bendro vertinimo (grindžiamo ne tik viešomis konsultacijomis, bet ir keletu individualių pokalbių, papildomomis tikslinėmis apklausomis ir praktiniais seminarais) padarytos šios išvados:

- ENISA'os tikslai šiandien tebėra aktualūs. Atsižvelgiant į sparčią technologijų raidą ir kintančias grėsmes, taip pat didėjančią pasaulinę kibernetinio saugumo riziką, ES tikrai reikia skatinti ir toliau plėsti aukšto lygio technines ekspertines žinias kibernetinio saugumo klausimais. Valstybės narės turi stiprinti pajėgumus, kad galėtų suprasti grėsmes ir į jas reaguoti, o suinteresuotieji subjektai turi bendradarbiauti įvairiose teminėse srityse ir institucijose.
- Nepaisant nedidelio Agentūros biudžeto, ji veiksmingai naudojo savo išteklius ir įgyvendino užduotis. Tačiau buvo ir papildomų administracinių išlaidų, kadangi veikla vykdoma Atėnuose ir Heraklione.
- ENISA su veiksmingumu susijusius savo tikslus įvykdė iš dalies. Stiprindama pajėgumus 28 valstybėse narėse[12], gerindama valstybių narių ir tinklų ir informacijos saugumu suinteresuotų subjektų bendradarbiavimą bei teikdama ekspertines žinias, kurdama bendruomenę ir remdama politikos kūrimą, Agentūra sėkmingai prisidėjo prie tinklų ir informacijos saugumo gerinimo Europoje. Apskritai ENISA kruopščiai stengėsi įgyvendinti savo darbo programą ir kaip patikimas suinteresuotųjų subjektų partneris veikė tokioje srityje, kurios didelė tarpvalstybinė reikšmė pripažinta neseniai.
- ENISA sugebėjo padaryti nors šiokį tokį poveikį plataus masto tinklų ir informacijos saugumo srityje, tačiau jai ne visiškai pavyko sukurti patikimą prekės ženklą ir tapti pakankamai matomai, kad būtų pripažinta kaip kompetencijos centras Europoje. Tai galima paaiškinti plataus masto ENISA įgaliojimais, kuriems vykdyti nebuvo proporcingai skirta pakankamų išteklių. Be to, ENISA yra vienintelė ES agentūra,

---

11 Į konsultacijų klausimus atsakė 90 suinteresuotųjų subjektų iš 19 valstybių narių (88 atsakymai ir 2 pozicijos dokumentai), įskaitant nacionalines institucijas iš 15 valstybių narių ir 8 bendrąsias organizacijas, atstovaujančias daugeliui Europos įmonių.

12 Viešų konsultacijų respondentų buvo paprašyta pareikšti nuomonę apie tai, kas 2013–2016 m. buvo pagrindiniai ENISA pasiekimai. Visų grupių respondentai (iš viso 55, įskaitant 13 iš nacionalinių valdžios institucijų, 20 iš privačiojo sektoriaus ir 22 iš kitų sričių) kaip pagrindinius ENISA pasiekimus nurodė: 1) Europos kibernetinio saugumo pratybų („Cyber Europe“) koordinavimą; 2) paramos teikimą CERT / CSIRT rengiant mokymus ir praktinius seminarus, kuriais skatinamas koordinavimas ir keitimasis informacija; 3) ENISA leidinius (gaires ir rekomendacijas, grėsmių padėties ataskaitas, pranešimų apie incidentus ir krizių valdymo strategijas ir kt.), kurie buvo laikomi naudingais nacionalinėms saugumo sistemoms kurti ir atnaujinti, taip pat kaip atspirties taškas politikos formuotojams ir kibernetikos ekspertams; 4) pagalbą skatinant TIS direktyvos taikymą; 5) pastangas didinti informuotumą apie kibernetinį saugumą vykdant kibernetinio saugumo mėnesio iniciatyvą.

kurios įgaliojimai terminuoti – tai riboja jos gebėjimą parengti ilgalaikę viziją ir tvariai remti suinteresuotuosius subjektus. Tai taip pat prieštarauja TIS direktyvos nuostatoms, pagal kurias agentūrai ENISA pavedamos užduotys be galutinio termino. Galiausiai vertinime nustatyta, kad šį nedidelį veiksmingumą galima iš dalies paaiškinti tuo, kad buvo labai naudojamasi išorės ekspertų, o ne vidaus ekspertų žiniomis ir kad buvo sudėtinga įdarbinti ir išlaikyti specialistus.

- Galiausiai ne mažiau svarbu yra tai, kad vertinime padaryta išvada, kad ENISA papildoma nauda pirmiausia susijusi su jos gebėjimu stiprinti bendradarbiavimą, daugiausia tarp valstybių narių, o ypač su susijusiomis tinklų ir informacijos saugumo bendruomenėmis (visų pirma tarp CSIRT). ES lygmeniu nėra jokio kito subjekto, kuris remtų tiek įvairiausių tinklų ir informacijos saugumu suinteresuotų subjektų. Tačiau kadangi reikia nustatyti griežtus agentūros veiklos prioritetus, ENISA darbo programa daugiausia grindžiama valstybių narių poreikiais. Taigi, joje nepakankamai atsižvelgiama į kitų suinteresuotųjų subjektų, ypač įmonių, poreikius. Tai taip pat skatino Agentūrą tenkinti savo pagrindinių suinteresuotųjų subjektų poreikius, o tai neleido jai pasiekti didesnio poveikio. Todėl Agentūros teikiama papildoma nauda buvo nevienoda ir priklausė nuo skirtingų jos suinteresuotųjų subjektų poreikių ir nuo to, kiek ji galėjo tuos poreikius patenkinti (pvz., didelės valstybės narės, palyginti su mažomis valstybėmis narėmis; valstybės narės, palyginti su įmonėmis).

Apibendrinant, iš suinteresuotųjų subjektų konsultacijų rezultatų ir vertinimo matyti, kad ENISA išteklius ir įgaliojimus reikia pakoreguoti, kad ji galėtų imtis atitinkamo vaidmens sprendžiant dabartinius ir būsimus uždavinius.

Atsižvelgiant į šias išvadas, šiuo pasiūlymu peržiūrimi dabartiniai ENISA įgaliojimai ir atnaujinamos užduotys ir funkcijos, siekiant veiksmingai ir efektyviai remti valstybių narių, ES institucijų ir kitų suinteresuotųjų subjektų pastangas Europos Sąjungoje užtikrinti saugią kibernetinę erdvę. Naujaisiais siūlomais įgaliojimais siekiama suteikti Agentūrai svaresnį ir reikšmingesnį vaidmenį, visų pirma, kad ir ji padėtų valstybėms narėms įgyvendinti TIS direktyvą ir aktyviau atremti konkrečias grėsmes (operatyviniai pajėgumai) ir taptų kompetencijos centru, padėsiančiu valstybėms narėms ir Komisijai kibernetinio saugumo sertifikavimo srityje. Pagal šį pasiūlymą:

- Agentūrai ENISA būtų suteiktas nuolatinis įgaliojimas ir kartu stabilus pagrindas ateičiai. Vis dėlto įgaliojimą, tikslus ir užduotis reikėtų nuolat peržiūrėti.
- Siūlomais įgaliojimais išsamiau paaiškinamas ENISA, kaip ES kibernetinio saugumo agentūros ir kaip informacijos punkto ES kibernetinio saugumo ekosistemoje, glaudžiai bendradarbiaujančio su visomis kitomis atitinkamomis tokios ekosistemos įstaigomis, vaidmuo.
- Agentūros organizacinė struktūra ir valdymas, kurie buvo teigiamai įvertinti atliekant vertinimą, būtų nuosaikiai peržiūrimi, ypač siekiant įsitikinti, kad Agentūra dirbdama geriau atsižvelgtų į didesnės suinteresuotųjų subjektų bendruomenės poreikius.
- Apibrėžta siūloma įgaliojimų apimtis, sustiprinant tas sritis, kuriose Agentūra aiškiai įrodė savo papildomą naudą, ir įtraukiant tokias naujas sritis, kuriose reikalinga parama dėl naujų politikos prioritetų ir priemonių, ypač TIS direktyvos, ES kibernetinio saugumo strategijos peržiūros, būsimo ES kibernetinio saugumo projekto, skirto bendradarbiavimui kibernetinių krizių klausimais, ir IRT saugumo sertifikavimo:

- **ES politikos formavimas ir įgyvendinimas.** Agentūra ENISA gautų užduotį aktyviai prisidėti prie tinklų ir informacijos saugumo politikos kūrimo, taip pat prie kitų politikos iniciatyvų, susijusių su įvairių sektorių (pvz., energetikos, transporto, finansų) kibernetinio saugumo elementais. Šiuo tikslu jai tektų svarbi patariamoji funkcija, kurią ji galėtų vykdyti teikdama nepriklausomas nuomones ir atlikdama parengiamąjį politikos ir teisės plėtotės bei atnaujinimo darbą. Siekdama skatinti didesnį kibernetinio saugumo lygį, ENISA taip pat remtų ES politiką ir teisę elektroninių ryšių, elektroninės atpažinties ir patikimumo užtikrinimo paslaugų srityse. Įgyvendinimo etapu, ypač kiek tai susiję su TIS bendradarbiavimo grupe, ENISA padėtų valstybėms narėms nuosekliai įgyvendinti TIS direktyvą įvairiuose sektoriuose tarpvalstybiniu mastu, taip pat kitų atitinkamų politikos sričių ir teisės aktų klausimais. Siekdama padėti nuolat peržiūrėti kibernetinio saugumo srities politiką ir teisės aktus, ENISA taip pat teiktų reguliarias ES teisinės sistemos įgyvendinimo padėties ataskaitas.

- **Pajėgumų stiprinimas.** ENISA prisidėtų prie ES ir nacionalinių valdžios institucijų pajėgumų ir ekspertinių žinių (įskaitant reagavimo į incidentus ir su kibernetiniu saugumu susijusių reguliavimo priemonių priežiūros) gerinimo. Agentūra taip pat turėtų padėti įvairiuose sektoriuose steigti keitimosi informacija ir jos analizės centrus, dalydamasi geriausia patirtimi ir informuodama apie esamas priemones ir procedūras, taip pat tinkamai spręsdama reguliavimo klausimus, susijusius su keitimusi informacija.

- **Žinios ir informacija, informuotumo didinimas.** ENISA taptų ES informacijos centru. Tai reiškia, kad sutelkiant iš ES ir nacionalinių institucijų, agentūrų ir įstaigų gautą informaciją apie kibernetinį saugumą būtų populiarinama geriausia patirtis ir iniciatyvos ir jomis būtų dalijamasi visoje ES. Agentūra taip pat teiktų konsultacijas, gaires ir dalytųsi geriausia patirtimi, susijusia su ypatingos svarbos infrastruktūros objektų saugumu. Be to, po didelių tarpvalstybinių kibernetinio saugumo incidentų ENISA rinktų ataskaitas, kad galėtų konsultuoti įmones ir piliečius visoje ES. Toks darbas apimtų ir nuolatinį informuotumo didinimo veiklos organizavimą bendradarbiaujant su valstybių narių valdžios institucijomis.

- **Su rinka susijusios užduotys (standartizavimas, kibernetinio saugumo sertifikavimas).** Analizuodama atitinkamas kibernetinio saugumo rinkos tendencijas, kad geriau derėtų paklausa ir pasiūla, ir padėdama formuoti ES politiką IRT standartizavimo ir IRT kibernetinio saugumo sertifikavimo srityse, ENISA vykdytų keletą funkcijų, kuriomis būtų konkrečiai remiama vidaus rinka ir kurios apimtų kibernetinio saugumo rinkos stebėjimą. Kiek tai susiję su standartizavimu, ji sudarytų palankesnes sąlygas kibernetinio saugumo standartams nustatyti ir juos taikyti. ENISA taip pat vykdytų numatytas užduotis, susijusias su būsima sertifikavimo sistema (žr. tolesnį skirsnį).

- **Moksliniai tyrimai ir inovacijos.** ENISA pasidalytų ekspertinėmis žiniomis patardama ES ir nacionalinėms valdžios institucijoms dėl mokslinių tyrimų ir plėtros prioritetų nustatymo, taip pat dėl sutartimis grindžiamos viešojo ir privačiojo sektorių partnerystės kibernetinio saugumo srityje. Su moksliniais tyrimais susijusiomis ENISA konsultacijomis pasinaudotų naujasis Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centras pagal būsimą

daugiametę finansinę programą. Paprašyta Komisijos ENISA taip pat dalyvautų įgyvendinant mokslinių tyrimų ir inovacijų finansavimo ES lėšomis programas.

- **Operatyvinis bendradarbiavimas ir krizių valdymas.** Šis darbas turėtų būti grindžiamas esamų prevencinių operacinių pajėgumų stiprinimu, visų pirma atnaujinant visos Europos kibernetinio saugumo pratybas („Cyber Europe“), kurias reikėtų rengti kasmet, ir pagalbiniu CSIRT tinklo sekretoriato vaidmeniu operatyvinio bendradarbiavimo srityje (pagal TIS direktyvos nuostatas), be kitų dalykų, užtikrinant gerą CSIRT tinklo IT infrastruktūros ir ryšių kanalų veikimą. Šiomis aplinkybėmis CERT-EU, Europos kovos su elektroniniu nusikalstamumu centras (EC3) ir kitos susijusios ES įstaigos turėtų bendradarbiauti struktūrizuotai. Be to, fizinėje aplinkoje struktūrizuotai bendradarbiaujant su CERT-EU, turėtų būti įmanoma teikti techninę pagalbą įvykus dideliam incidentui ir padėti jį išanalizuoti. Siekiant stiprinti valstybių narių prevencijos ir reagavimo pajėgumus, jos paprašiusios gautų pagalbą incidentams suvaldyti ir paramą pažeidžiamumui, artefaktams ir incidentams analizuoti.
- Agentūrai ENISA taip pat būtų skirtas vaidmuo **ES kibernetinio saugumo projekte**, kuris pateikiamas kaip šio dokumentų rinkinio dalis ir kuriame pateikiama Komisijos rekomendacija valstybėms narėms, kaip koordinuotai reaguoti į didelio masto tarpvalstybinius kibernetinius incidentus ir krizes ES lygmeniu[13]. ENISA, analizuodama ir kaupdama nacionalines padėties ataskaitas, remdamasi informacija, kurią jai savanoriškai pateikė valstybės narės ir kiti subjektai, sudarytų atskiroms valstybėms narėms palankesnes sąlygas bendradarbiauti reaguojant į krizes.

- **IRT produktų ir paslaugų kibernetinio saugumo sertifikavimas**

Siekiant užtikrinti pasitikėjimą IRT produktais ir paslaugomis ir išlaikyti jų saugumą, reikia, kad jų saugumu būtų rūpinamasi nuo pat pirmųjų techninio projektavimo ir plėtojimo etapų (saugumo užtikrinimas projektuojant). Be to, klientai ir vartotojai turi galėti įvertinti produktų ir paslaugų, kuriuos įsigyja ar perka, saugumo užtikrinimo lygį.

Sertifikavimas, kurį sudaro oficialus produktų, paslaugų ir procesų įvertinimas, kurį atlieka nepriklausoma ir akredituota įstaiga pagal nustatytą kriterijų standartų rinkinį, ir sertifikato, kuriame nurodoma atitiktis, išdavimas, yra labai svarbus, siekiant didinti pasitikėjimą produktais ir paslaugomis bei jų saugumą. Nors saugumo vertinimai yra gana techninė sritis, sertifikavimo paskirtis – informuoti ir patikinti pirkėjus ir naudotojus, kad jų perkami ar naudojami IRT produktai ir paslaugos pasižymi konkrečiomis saugumo savybėmis. Kaip minėta pirmiau, tai ypač pasakytina apie tas naujas sistemas, kurioms intensyviai naudojamos skaitmeninės technologijos ir kurioms būtinas aukštas saugumo lygis. Tokių sistemų

[13] Šis projektas bus taikomas kibernetinio saugumo incidentams, kurių sukeliamų sutrikimų jokia valstybė narė negali pašalinti viena pati arba kurie dviem ar daugiau valstybių narių padaro tokį plataus masto ir didelį poveikį arba turi tokią politinę reikšmę, kad būtina laiku koordinuoti politiką ir reaguoti Sąjungos politiniu lygmeniu.

pavyzdžiai: susietieji automatizuoti automobiliai, elektroninės sveikatos priežiūros sistemos, pramoninės automatizacijos valdymo sistemos[14] ar pažangieji elektros energijos tinklai.

Šiuo metu IRT produktų ir paslaugų kibernetinio saugumo sertifikavimo padėtis ES yra gana nevienoda. Yra keletas tarptautinių iniciatyvų, pvz., informacinių technologijų saugumo vertinimo bendrieji kriterijai (ISO 15408) – kompiuterių saugumo vertinimo tarptautinis standartas. Jis grindžiamas trečiosios šalies atliekamu vertinimu ir pagal jį numatomi septyni vertinimo užtikrinimo lygiai (angl. EAL). Bendrieji kriterijai ir kartu taikoma Bendra informacinių technologijų saugumo vertinimo metodika (angl. CEM) yra techninis tarptautinio susitarimo dėl bendrųjų kriterijų pripažinimo (angl. CCRA) pagrindas, užtikrinantis, kad pagal bendruosius kriterijus išduotus sertifikatus pripažintų visos minėtąjį susitarimą pasirašančios šalys. Vis dėlto, remiantis naujausia CCRA redakcija, tarpusavyje pripažįstami tik ne aukštesnio kaip EAL 2 lygio vertinimai. Be to, susitarimą yra pasirašiusios tik 13 valstybių narių.

Dvylikos valstybių narių sertifikavimo institucijos sudarė tarpusavio pripažinimo susitarimą dėl sertifikatų, išduotų laikantis susitarimo, grindžiamo bendraisiais kriterijais[15]. Be to, valstybėse narėse šiuo metu vykdoma arba rengiama keletas IRT sertifikavimo iniciatyvų. Nors šios iniciatyvos ir svarbios, dėl jų gali būti suskaidyta rinka ir kilti sąveikumo problemų. Taigi, kad bendrovė galėtų siūlyti savo produktą keliose rinkose, jai gali prireikti jį sertifikuoti įvairiose valstybėse narėse. Pavyzdžiui, pažangiųjų skaitiklių gamintojas, norėdamas parduoti savo produktus trijose valstybėse narėse, pvz., Vokietijoje, Prancūzijoje ir Jungtinėje Karalystėje, šiuo metu turi laikytis trijų skirtingų sertifikavimo schemų: „Commercial Product Assurance“ (CPA) Jungtinėje Karalystėje, „Certification Sécuritaire de Premier Niveau“ (CSPN) Prancūzijoje ir bendraisiais kriterijais pagrįsto specialaus apsaugos profilio Vokietijoje.

Dėl šios situacijos keliose valstybėse narėse veikiančių įmonių išlaidos padidėja ir joms tenka didžiulė administracinė našta. Nors sertifikavimo išlaidos gali labai skirtis, priklausomai nuo atitinkamo produkto ir (arba) paslaugos, norimo užtikrinimo lygio ir (arba) kitų komponentų, paprastai įmonėms jos būna gana didelės. Pavyzdžiui, BSI „Smart Meter Gateway“ sertifikatas kainuoja daugiau kaip milijoną EUR (suteikia aukščiausią testavimo lygį ir užtikrinimą, apima ne tik vieną produktą, bet ir visą su juo susijusią infrastruktūrą). Pažangiųjų skaitiklių sertifikavimas JK kainuoja beveik 150 000 EUR. Prancūzijoje kaina panaši kaip JK – apie 150 000 EUR arba didesnė.

Pagrindiniai viešieji ir privatieji suinteresuotieji subjektai pripažino, kad, nesant ES masto kibernetinio saugumo sertifikavimo schemos, daugeliu atvejų įmonės savo produktus turi sertifikuoti kiekvienoje valstybėje narėje atskirai, o tai sudaro sąlygas rinkos susiskaidymui. Svarbiausia yra tai, kad, nesant IRT produktų ir paslaugų ES derinamųjų teisės aktų, dėl skirtingų kibernetinio saugumo sertifikavimo standartų ir praktikos valstybės narės ES praktiškai gali sukurti 28 atskiras saugumo rinkas, kiekvienoje iš kurių būtų taikomi atskiri

---

[14] Jungtinis tyrimų centras paskelbė ataskaitą, kurioje siūlomi pradiniai bendri Europos reikalavimai ir bendros gairės, susijusios su pramoninės automatizacijos valdymo sistemos komponentų kibernetinio saugumo sertifikavimu. Paskelbta https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[15] Vyresniųjų pareigūnų grupėje informacinių sistemų saugumo klausimais (angl. SOG-IS) dalyvauja 12 valstybių narių ir Norvegija. Grupė parengė kelis riboto skaičiaus produktų, pvz., skaitmeninio parašo, skaitmeninio tachografo ir lustinių kortelių, apsaugos profilius. Dalyviai bendradarbiauja siekdami koordinuoti bendraisiais kriterijais grindžiamos apsaugos profilių standartizavimą ir apsaugos profilių kūrimą. Valstybės narės dažnai prašo SOG-IS sertifikavimo nacionaliniuose viešųjų pirkimų konkursuose.

techniniai reikalavimai, testavimo metodikos ir kibernetinio saugumo sertifikavimo procedūros. Jeigu ES lygmeniu nebūtų imtasi tinkamų veiksmų, šie skirtingi nacionaliniu lygmeniu taikomi metodai gali tapti didele bendrosios skaitmeninės rinkos kūrimo kliūtimi – dėl to lėčiau augtų ekonomika, lėčiau būtų kuriamos darbo vietos arba tam būtų užkirstas kelias.

Remiantis pirmiau minėtais pokyčiais, siūlomame reglamente nustatoma IRT produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo sistema (toliau – **Sistema**) ir apibrėžiamos esminės ENISA funkcijos ir užduotys kibernetinio saugumo sertifikavimo srityje. Šiame pasiūlyme nurodoma bendra taisyklių, reglamentuojančių Europos kibernetinio saugumo sertifikavimo schemas, sistema. Pasiūlyme operacinės sertifikavimo schemos tiesiogiai nepateikiamos, bet sukuriama konkrečių IRT produktų ir (arba) paslaugų konkrečių sertifikavimo schemų (toliau – Europos kibernetinio saugumo sertifikavimo schemų) nustatymo sistema. Taikant pagal Sistemą sukurtas Europos kibernetinio saugumo sertifikavimo schemas, išduoti sertifikatai galios ir bus pripažįstami visose valstybėse narėse ir tai leis išspręsti dabartinę rinkos susiskaidymo problemą.

Bendra Europos kibernetinio saugumo sertifikavimo schemos paskirtis – patvirtinti, kad pagal tokią sistemą sertifikuoti IRT produktai ir paslaugos atitinka konkrečius kibernetinio saugumo reikalavimus. Pavyzdžiui, tai apimtų jų gebėjimą apsaugoti duomenis (laikomus, perduodamus ar kitaip tvarkomus) nuo atsitiktinio ar neteisėto jų laikymo, tvarkymo, prieigos prie jų, jų atskleidimo, sunaikinimo, atsitiktinio jų netekimo ar pakeitimo. Taikant ES kibernetinio saugumo sertifikavimo schemas, būtų panaudoti esami standartai, susiję su techniniais reikalavimais ir vertinimo procedūromis, kurias turi atitikti produktai, o pagal pačias schemas techniniai standartai kuriami nebūtų[16]. Pavyzdžiui, tokių produktų, kaip lustinės kortelės, kurios dabar testuojamos remiantis tarptautiniais bendrųjų kriterijų standartais pagal daugiašalę SOG-IS schemą (aprašytą pirmiau), ES masto sertifikavimas reikštų, kad ši schema tampa galiojanti visoje ES.

Pasiūlyme nurodoma ne tik keletas konkrečių saugumo tikslų, į kuriuos turi būti atsižvelgta rengiant konkrečią Europos kibernetinio saugumo sertifikavimo schemą, bet ir minimalus tokių schemų turinys. Be kitų dalykų, tokiose schemose turės būti apibrėžta keletas konkrečių elementų, nurodančių kibernetinio saugumo sertifikavimo taikymo sritį ir tikslą. Tai apima produktų ir paslaugų, kuriems taikoma schema, kategorijų nustatymą, išsamų kibernetinio saugumo reikalavimų nurodymą (pavyzdžiui, remiantis susijusiais standartais arba techninėmis specifikacijomis), konkrečius vertinimo kriterijus ir metodus, taip pat užtikrinimo lygį, kurį jais ketinama užtikrinti (t. y. bazinį, pakankamą arba aukštą).

Europos kibernetinio saugumo sertifikavimo schemas rengs ENISA, glaudžiai bendradarbiaudama su Europos kibernetinio saugumo sertifikavimo grupe (žr. toliau), jos padedama ir pasinaudodama jos ekspertų konsultacijomis, o schemas tvirtins Komisija, priimdama įgyvendinimo aktus. Atsiradus kibernetinio saugumo sertifikavimo schemos poreikiui, Komisija paprašys agentūros ENISA parengti schemą konkretiems IRT produktams arba paslaugoms. ENISA schemą rengs glaudžiai bendradarbiaudama su nacionalinėmis sertifikavimo priežiūros institucijomis, kurios atstovaujamos Grupėje. Valstybės narės ir Grupė gali siūlyti Komisijai, kad ši paprašytų agentūros ENISA parengti tam tikrą schemą.

Sertifikavimas gali būti labai brangus procesas, dėl kurio gali išaugti kainos klientams ir vartotojams. Poreikis sertifikuoti taip pat gali labai skirtis atsižvelgiant į konkrečias produktų ir paslaugų naudojimo aplinkybes ir greitą technologijų kitimą. Todėl Europos kibernetinio

[16] Europos standartus rengia Europos standartizacijos organizacijos ir tvirtina Europos Komisija, paskelbdama *Oficialiajame leidinyje* (žr. Reglamentą Nr. 1025/2012).

saugumo sertifikavimas turėtų likti savanoriškas, išskyrus atvejus, kai Sąjungos teisės aktuose, nustatančiuose IRT produktų ir paslaugų saugumo reikalavimus, numatyta kitaip.

Siekiant užtikrinti, kad būtų laikomasi suderintos praktikos ir išvengta rinkos susiskaidymo, nacionalinės kibernetinio saugumo sertifikavimo schemos arba procedūros, taikomos IRT produktams ir paslaugoms, kuriems taikoma Europos kibernetinio saugumo sertifikavimo schema, nebebus taikomos nuo įgyvendinimo akte, kuriuo priimama schema, nustatytos datos. Be to, valstybės narės turėtų neįvesti naujų nacionalinių kibernetinio saugumo sertifikavimo schemų IRT produktams ir paslaugoms, kuriems taikoma galiojanti Europos kibernetinio saugumo sertifikavimo schema.

Priėmus Europos kibernetinio saugumo sertifikavimo schemą IRT produktų gamintojai arba IRT paslaugų teikėjai turės galimybę savo pasirinktai atitikties vertinimo įstaigai teikti prašymą sertifikuoti savo produktus arba paslaugas. Atitikties vertinimo įstaigas, atitinkančias tam tikrus nustatytus reikalavimus, turėtų akredituoti akreditacijos įstaiga. Akreditacija bus suteikiama ne ilgesniam kaip penkerių metų laikotarpiui ir gali būti pratęsta tomis pačiomis sąlygomis, jei atitikties vertinimo įstaiga vykdo reikalavimus. Akreditacijos įstaigos panaikins atitikties vertinimo įstaigos akreditaciją, jeigu akreditacijos sąlygos nevykdomos arba nebevykdomos, arba jeigu veiksmais, kurių imasi atitikties vertinimo įstaiga, pažeidžiamas šis reglamentas.

Pagal šį pasiūlymą stebėjimo, priežiūros ir vykdymo užtikrinimo užduotys tenka valstybėms narėms. Valstybės narės turės paskirti vieną sertifikavimo priežiūros instituciją. Šiai institucijai bus pavesta prižiūrėti atitikties vertinimo įstaigų ir jų teritorijoje įsisteigusių atitikties vertinimo įstaigų išduotų sertifikatų atitiktį šio reglamento ir atitinkamų Europos kibernetinio saugumo sertifikavimo schemų reikalavimams. Nacionalinės sertifikavimo priežiūros institucijos bus kompetentingos nagrinėti fizinių ar juridinių asmenų pateiktus skundus, susijusius su jų teritorijose įsteigtų atitikties vertinimo įstaigų išduotais sertifikatais. Tiek, kiek tinkama, jos išnagrinės skundo dalyką ir per pagrįstą laikotarpį informuos skundo teikėją apie tyrimo eigą ir rezultatus. Be to, jos bendradarbiaus su kitomis sertifikavimo priežiūros institucijomis ar kitomis valdžios institucijomis, pavyzdžiui, dalydamosi informacija apie galimą IRT produktų ir paslaugų neatitiktį šio reglamento arba konkrečių Europos kibernetinio saugumo schemų reikalavimams.

Galiausiai pasiūlymu įsteigiama iš visų valstybių narių nacionalinių sertifikavimo priežiūros institucijų sudaryta Europos kibernetinio saugumo sertifikavimo grupė (toliau – Grupė). Pagrindinė Grupės užduotis – konsultuoti Komisiją su kibernetinio saugumo sertifikavimo politika susijusiais klausimais ir bendradarbiauti su ENISA rengiant Europos kibernetinio saugumo sertifikavimo schemų projektus. ENISA padės Komisijai užtikrinti Grupės sekretoriato funkciją ir atnaujinti viešąjį schemų, patvirtintų pagal Europos kibernetinio saugumo sertifikavimo sistemą, registrą. ENISA taip pat palaikys ryšius su standartizavimo įstaigomis, kad užtikrintų standartų, taikomų pagal patvirtintas schemas, tinkamumą ir nustatytų sritis, kur reikalingi kibernetinio saugumo standartai.

Europos kibernetinio saugumo sertifikavimo sistema (toliau – Sistema) užtikrins keleriopą naudą piliečiams ir įmonėms. Visų pirma:

- Tam tikriems produktams arba paslaugoms sukūrus ES masto kibernetinio saugumo sertifikavimo schemas, įmonėms bus teikiama ES kibernetinio saugumo sertifikavimo vieno langelio sistemos paslauga. Tokioms įmonėms užteks sertifikuoti savo produktus tik vieną kartą ir jos gaus visose valstybėse narėse galiojantį sertifikatą. Jos neprivalės pakartotinai sertifikuoti savo produktų įvairiose nacionalinėse sertifikavimo įstaigose. Tai labai sumažins įmonių išlaidas, palengvins

tarpvalstybines operacijas ir galiausiai sumažins ir pašalins atitinkamų produktų vidaus rinkos susiskaidymą.

- Sistema nustatoma Europos kibernetinio saugumo sertifikavimo schemų viršenybė prieš nacionalines schemas: pagal šią taisyklę Europos kibernetinio saugumo sertifikavimo schema esant tam tikram užtikrinimo lygiui pakeis visas esamas tų pačių IRT produktų ar paslaugų lygiagrečias nacionalines schemas. Sumažinant viena kitai prieštaraujančių arba besidubliuojančių nacionalinių kibernetinio saugumo sertifikavimo schemų paplitimą, bus užtikrintas papildomas aiškumas.
- Pasiūlymu remiamas ir papildomas TIS direktyvos įgyvendinimas, suteikiant įmonėms, atsižvelgiant į direktyvą, labai naudingą atitikties TIS reikalavimams visoje Sąjungoje įrodymo priemonę. Rengdamos naujas kibernetinio saugumo sertifikavimo schemas, Komisija ir ENISA kreips ypatingą dėmesį į poreikį užtikrinti, kad kibernetinio saugumo sertifikavimo schemose būtų atsižvelgta į TIS reikalavimus.
- Pasiūlymu, kuriuo suderinamos ES IRT produktų ir paslaugų kibernetinio saugumo sertifikavimo sąlygos ir esminiai reikalavimai, bus remiamas Europos kibernetinio saugumo politikos formavimas ir sudaromos tam palankesnės sąlygos. Europos kibernetinio saugumo sertifikavimo schemos bus grindžiamos bendrais standartais arba vertinimo kriterijais ir testavimo metodika. Nors ir netiesiogiai, tai labai padės įgyvendinti bendrus saugumo sprendimus ES ir kartu pašalins kliūtis patekti į vidaus rinką.
- Sistema parengta taip, kad būtų užtikrinta reikiama kibernetinio saugumo sertifikavimo schemų lankstumo galimybė. Priklausomai nuo konkrečių kibernetinio saugumo poreikių, produktas arba paslauga gali būti sertifikuojami užtikrinant didesnį arba mažesnį saugumo lygį. Europos kibernetinio saugumo sertifikavimo schemos bus rengiamos turint omenyje šią lankstumo galimybę ir todėl jomis remiantis bus numatyti skirtingi saugumo užtikrinimo lygiai (t. y. bazinis, pakankamas arba aukštas), kad jas būtų galima naudoti skirtingais tikslais arba skirtingomis aplinkybėmis.
- Dėl visų pirmiau nurodytų elementų kibernetinio saugumo sertifikavimas taps patrauklesnis įmonėms kaip veiksminga informavimo apie IRT produktų arba paslaugų kibernetinio saugumo užtikrinimo lygį priemonė. Jeigu kibernetinio saugumo sertifikavimas taps pigesnis, veiksmingesnis ir komerciškai patrauklesnis, įmonėms tai bus didesnės paskatos sertifikuoti savo produktus atsižvelgiant į kibernetinio saugumo riziką, taip prisidedant prie geresnės kibernetinio saugumo praktikos skleidimo kuriant IRT produktus ir paslaugas (kibernetinio saugumo užtikrinimas projektuojant).

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

Pagal TIS direktyvą operatoriai, veikiantys ypatingos svarbos mūsų ekonomikai ir visuomenei sektoriuose, pvz., energetikos, transporto, vandens, bankininkystės, finansų rinkų infrastruktūros, sveikatos priežiūros ir skaitmeninės infrastruktūros, taip pat skaitmeninių paslaugų teikėjai (t. y. paieškos sistemų, debesijos kompiuterijos paslaugų ir elektroninių prekyviečių) turi imtis priemonių, kad tinkamai valdytų saugumo riziką. Šio pasiūlymo naujos taisyklės papildo TIS direktyvos nuostatas ir užtikrina suderinamumą su jomis, kad būtų galima toliau didinti ES kibernetinį atsparumą gerinant pajėgumus, bendradarbiavimą, rizikos valdymą ir informuotumą apie kibernetinį saugumą.

Be to, kibernetinio saugumo sertifikavimo taisyklės yra esminė priemonė įmonėms, kurioms taikoma TIS direktyva, nes jos, atsižvelgdamos į riziką kibernetiniam saugumui, galės sertifikuoti savo IRT produktus ir paslaugas pagal visoje ES galiojančias ir pripažįstamas kibernetinio saugumo sertifikavimo schemas. Šios taisyklės taip pat papildys eIDAS reglamente[17] ir Radijo įrenginių direktyvoje[18] nurodytus saugumo reikalavimus.

- **Suderinamumas su kitomis Sąjungos politikos sritimis**

Reglamente (ES) 2016/679 (Bendrajame duomenų apsaugos reglamente, **BDAR**)[19] išdėstytos sertifikavimo mechanizmų ir duomenų apsaugos ženklų ir žymenų nustatymo nuostatos, kad būtų galima įrodyti, jog duomenų valdytojai ir duomenų tvarkytojai, tvarkydami duomenis, laikosi šio reglamento. Šiuo reglamentu nepažeidžiamas duomenų tvarkymo operacijų, įskaitant atvejus, kai tokios operacijos yra produktų ir paslaugų dalis, sertifikavimas pagal BDAR.

Siūlomu reglamentu bus užtikrintas suderinamumas su Reglamentu Nr. 765/2008 dėl akreditavimo ir rinkos priežiūros reikalavimų[20], remiantis nacionalinių akreditacijos įstaigų ir atitikties vertinimo įstaigų sistemos taisyklėmis. Kalbant apie priežiūros institucijas, pagal siūlomą reglamentą bus reikalaujama, kad valstybės narės paskirtų nacionalines sertifikavimo priežiūros institucijas, atsakingas už priežiūrą, stebėjimą ir taisyklių vykdymo užtikrinimą. Tos įstaigos liks atskirtos nuo atitikties vertinimo įstaigų, kaip nustatyta Reglamente Nr. 765/2008.

2. TEISINIS PAGRINDAS, SUBSIDIARUMO IR PROPORCINGUMO PRINCIPAI

- **Teisinis pagrindas**

ES veiksmų teisinis pagrindas – Sutarties dėl Europos Sąjungos veikimo (SESV) 114 straipsnis, kuriame kalbama apie valstybių narių įstatymų suderinimą siekiant SESV 26 straipsnio tikslų, visų pirma užtikrinti tinkamą vidaus rinkos veikimą.

Vidaus rinkos teisinį pagrindą agentūrai ENISA įsteigti patvirtino Teisingumo Teismas (byloje C-217/04, *Jungtinė Karalystė prieš Europos Parlamentą ir Tarybą*), vėliau jis papildomai patvirtintas 2013 m. reglamentu, kuriame nustatyti dabartiniai Agentūros įgaliojimai. Be to, veikla, kuri atspindėtų tikslus didinti valstybių narių bendradarbiavimą ir koordinavimą bei tuos papildomus ES lygmens pajėgumus papildyti valstybių narių veiksmus būtų priskirtos operatyvinio bendradarbiavimo kategorijai. Tai konkrečiai nurodyta TIS direktyvoje (kurios teisinis pagrindas – SESV 114 straipsnis) kaip tikslas, kurio turi būti siekiama kuriant CSIRT tinklą, kai „ENISA teikia sekretoriato paslaugas ir aktyviai remia

---

17 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.

18 2014 m. balandžio 16 d. Europos Parlamento ir Tarybos direktyva 2014/53/ES dėl valstybių narių įstatymų, susijusių su radijo įrenginių tiekimu rinkai, suderinimo, kuria panaikinama Direktyva 1999/5/EB.

19 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1–88).

20 Reglamentas (EB) Nr. 765/2008, nustatantis su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinantis Reglamentą (EEB) Nr. 339/93.

bendradarbiavimą“ (12 straipsnio 2 dalis). Visų pirma 12 straipsnio 3 dalies f punkte tiksliau nustatytos kitos CSIRT tinklo vykdomo operatyvinio bendradarbiavimo formos, be kita ko, susijusios su: i) rizikos ir incidentų kategorijomis, ii) išankstiniais įspėjimais, iii) savitarpio pagalba ir iv) koordinavimo principais ir tvarka tuo atveju, kai valstybės narės reaguoja į tarpvalstybinę riziką ir incidentus.

- Tokią dabartinę padėtį, kai naudojama daugybė IRT produktų ir paslaugų sertifikavimo schemų, lėmė ir tai, kad trūksta valstybėms narėms taikytino bendros teisiškai privalomos ir veiksmingos sistemos proceso. Tai neleidžia kurti IRT produktų ir paslaugų vidaus rinkos ir kenkia šio sektoriaus Europos įmonių konkurencingumui. Šiuo pasiūlymu siekiama pašalinti esamą vidaus rinkos susiskaidymą ir susijusias kliūtis, pateikiant bendrą visoje ES galiosiančią kibernetinio saugumo sertifikavimo schemų nustatymo sistemą.

Subsidiarumo principas (neišimtinės kompetencijos atveju)

Vadovaujantis subsidiarumo principu reikia įvertinti ES veiksmų būtinybę ir pridėtinę jų vertę. Vadovavimasis subsidiarumo principu šioje srityje jau buvo pripažintas priimant dabartinį ENISA reglamentą[21].

Kibernetinis saugumas yra Sąjungos bendros svarbos klausimas. Tinklų ir informacijos sistemos taip susijusios tarpusavyje, kad atskiri subjektai (viešieji ir privatieji, įskaitant piliečius) patys vieni labai dažnai negali kovoti su grėsmėmis, valdyti rizikos ir galimo kibernetinių incidentų poveikio. Viena vertus, dėl valstybių narių tarpusavio priklausomybės, be kita ko, susijusios su ypatingos svarbos infrastruktūros objektų (pvz., energetikos, transporto, vandens infrastruktūros ir kt.) veikimu, viešoji intervencija Europos lygmeniu yra ne tik naudinga, bet ir reikalinga. Kita vertus, ES intervencija gali turėti teigiamos įtakos, nes visose valstybėse narėse dalijamasi gerąja praktika ir tai gali lemti didesnį kibernetinį saugumą Sąjungoje.

Apibendrinant, esant dabartinėms aplinkybėms ir žvelgiant į ateities scenarijus, atrodo, kad, **norint padidinti bendrą** Sąjungos **kibernetinį atsparumą, pavienių ES valstybių narių veiksmų ir skirtingų požiūrių** nepakaks.

Siekiant pašalinti dabartinių kibernetinio saugumo sertifikavimo schemų gausą, taip pat reikia imtis ES veiksmų. Tuomet gamintojai turėtų galimybę visapusiškai naudotis vidaus rinka ir labai sumažintų testavimo ir pakartotinio projektavimo išlaidas. Pavyzdžiui, šiuo atžvilgiu dabartiniu vyresniųjų pareigūnų grupės informacinių sistemų saugumo klausimais (SOG-IS) tarpusavio pripažinimo susitarimu pasiekta svarbių rezultatų, tačiau kartu tapo akivaizdūs ir dideli trūkumai, dėl kurių jis negali būti tinkama priemonė, siekiant rasti ilgesnio laikotarpio tvarių sprendimų visapusiškai naudotis vidaus rinkos teikiamomis galimybėmis.

ES lygmens veiksmų pridėtinė vertė, ypač siekiant sustiprinti ne tik valstybių narių, bet ir tinklų ir informacijos saugumo bendruomenių bendradarbiavimą, pripažinta 2016 m. Tarybos išvadose[22], tai taip pat akivaizdu ir ENISA vertinime.

---

[21] 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.

[22] Tarybos išvados dėl Europos kibernetinio atsparumo sistemos stiprinimo ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimo. 2016 m. lapkričio 15 d.

- **Proporcingumo principas**

Siūlomomis priemonėmis neviršijama to, kas būtina politikos tikslams pasiekti. Be to, ES intervencijos mastas netrukdo imtis tolesnių nacionalinių veiksmų nacionalinių saugumo klausimų srityje. Todėl ES veiksmai grindžiami subsidiarumo ir proporcingumo principais.

- **Priemonės pasirinkimas**

Šiuo pasiūlymu peržiūrimas Reglamentas (ES) Nr. 526/2013, kuriame nustatyti dabartiniai ENISA įgaliojimai ir užduotys. Be to, atsižvelgiant į svarbų ENISA vaidmenį parengti ir valdyti ES kibernetinio saugumo sertifikavimo sistemą, geriausia naujuosius ENISA įgaliojimus ir minėtą sistemą nustatyti viena bendra teisine priemone – reglamentu.

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

Galiojančių teisės aktų *ex post* vertinimas / tinkamumo patikrinimas

Remdamasi vertinimo gairėmis[23] Komisija įvertino Agentūros **svarbą, poveikį, efektyvumą, veiksmingumą, suderinamumą ir pridėtinę vertę**, visa tai susiejant su Agentūros veiklos rezultatais, valdymu, vidaus organizacine struktūra ir darbo praktika 2013–2016 m. laikotarpiu. Pagrindines išvadas galima apibendrinti taip (daugiau informacijos ta tema pateikta prie poveikio vertinimo pridedamame Komisijos tarnybų darbiniame dokumente):

- **Svarba.** Technologiniai pokyčiai ir kintančios grėsmės, taip pat didesnio kibernetinio saugumo ES poreikis įrodė, kad ENISA tikslai yra svarbūs. Valstybės narės ir ES įstaigos iš tikrųjų pasikliauja jos gausiomis ekspertinėmis žiniomis kibernetinio saugumo klausimais. Be to, valstybės narės turi stiprinti pajėgumus, kad galėtų geriau suprasti grėsmes ir į jas reaguoti, o suinteresuotieji subjektai turi bendradarbiauti įvairiose teminėse srityse ir institucijose. Kibernetinis saugumas tebėra pagrindinis ES politinis prioritetas, į kurį turi atsižvelgti ENISA. Tačiau kadangi ENISA yra ES agentūra, kuriai suteikti terminuoti įgaliojimai: i) ji negali vykdyti ilgalaikio planavimo ir tvariai remti valstybių narių ir ES institucijų; ii) gali susidaryti teisinis vakuumas, kadangi TIS direktyvos nuostatos, kuriomis agentūrai ENISA pavedamos užduotys, yra nuolatinio pobūdžio[24]; iii) trūksta suderinamumo su vizija, pagal kurią ENISA siejama su patobulinta ES kibernetinio saugumo ekosistema.
- **Efektyvumas**. Apskritai ENISA įvykdė savo tikslus ir įgyvendino užduotis. Vykdydama savo pagrindinę veiklą (stiprindama pajėgumus, teikdama ekspertines žinias, kurdama bendruomenę ir remdama politiką), ji padėjo didinti tinklų ir informacijos saugumą Europoje. Tačiau kiekvienoje srityje jai dar yra kur tobulėti. Vertinime padaryta išvada, kad ENISA veiksmingai užmezgė stiprius ir pasitikėjimu pagrįstus ryšius su kai kuriais suinteresuotaisiais subjektais, ypač su valstybėmis narėmis ir CSIRT bendruomene. Pajėgumų stiprinimo priemonės įvertintos kaip veiksmingos, visų pirma mažesnių išteklių valstybėse narėse. Vienas iš svarbiausių dalykų buvo plataus masto bendradarbiavimo skatinimas – suinteresuotieji subjektai bendrai sutiko dėl teigiamo ENISA vaidmens suartinant žmones. Vis dėlto ENISA patyrė sunkumų siekdama padaryti didelį poveikį plataus masto tinklų ir informacijos

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

[24] Nuoroda į Tinklų ir informacijos saugumo direktyvos (TIS direktyvos) 7, 9, 11, 12 ir 19 straipsnius.

saugumo srityje. Tai lėmė ir tai, kad labai plataus masto įgaliojimams vykdyti ji turėjo labai ribotus žmogiškuosius ir finansinius išteklius. Vertinime taip pat padaryta išvada, kad ekspertinių žinių teikimo tikslą ENISA įvykdė iš dalies – tai susiję su tuo, kad buvo sudėtinga įdarbinti ekspertus (taip pat žr. tolesnį skirsnį apie veiksmingumą).

- **Veiksmingumas**. Nors ir turėjo nedidelį biudžetą – vieną iš mažiausių, palyginti su kitomis ES agentūromis – Agentūra, bendrai veiksmingai panaudodama savo išteklius, sugebėjo prisidėti prie tikslinių uždavinių įgyvendinimo. Vertinime padaryta išvada, kad procesai apskritai buvo veiksmingi ir kad organizacijoje aiškiai pasidalijus funkcijas, darbas buvo atliekamas tinkamai. Viena iš pagrindinių problemų, susijusių su Agentūros veiksmingumu, kyla dėl ENISA patiriamų sunkumų įdarbinti ir išlaikyti aukštos kvalifikacijos ekspertus. Remiantis išvadomis, tai galima paaiškinti keletu veiksnių: sunkumais, kuriuos apskritai patiria viešasis sektorius, konkuruodamas su privačiuoju sektoriumi, stengiantis įdarbinti aukštos kvalifikacijos ekspertus; sutarčių, kurias Agentūra daugiausia galėtų pasiūlyti, tipais (terminuotos sutartys) ir nelabai patrauklia ENISA veiklos vieta, pavyzdžiui, tai susiję su sunkumais, kuriuos gali patirti sutuoktiniai norėdami susirasti darbą. Kadangi veikla buvo vykdoma Atėnuose ir Heraklione, reikėjo papildomų koordinavimo pastangų ir buvo papildomų išlaidų, tačiau 2013 m. perkėlus pagrindinių operacijų departamentą į Atėnus, Agentūros operacinis veiksmingumas padidėjo.
- **Suderinamumas**. ENISA veikla iš esmės buvo suderinta su jos suinteresuotųjų subjektų politika ir veikla tiek nacionaliniu, tiek ES lygmenimis, tačiau reikalingas labiau koordinuotas požiūris į kibernetinį saugumą ES lygmeniu. ENISA ir kitų ES įstaigų bendradarbiavimo galimybės dar nėra išnaudotos. Dabartiniai įgaliojimai nedera su pakitusia ES teisine ir politine aplinka.
- **ES pridėtinė vertė**. ENISA pridėtinė vertė pirmiausia susijusi su Agentūros gebėjimu stiprinti bendradarbiavimą, daugiausia tarp valstybių narių, tačiau taip pat ir su susijusiomis tinklų ir informacijos saugumo bendruomenėmis. ES lygmeniu nėra jokio kito subjekto, kuris remtų tokios įvairovės suinteresuotųjų subjektų bendradarbiavimą tinklų ir informacijos saugumo klausimais. Agentūros teikiama papildoma nauda buvo nevienoda ir priklausė nuo skirtingų jos suinteresuotųjų subjektų poreikių (pvz., didelės valstybės narės, palyginti su mažomis; valstybės narės, palyginti su įmonėmis) ir Agentūros poreikio pagal darbo programą nustatyti savo veiklos prioritetus. Vertinime padaryta išvada, kad galimas ENISA veiklos nutraukimas būtų prarasta galimybė visoms valstybėms narėms. Valstybėse narėse nebus galima užtikrinti tokio paties lygio bendruomenės stiprinimo ir bendradarbiavimo kibernetinio saugumo srityje. Jeigu nebūtų labiau centralizuotos ES agentūros, rinka būtų dar labiau suskaidyta, ENISA veiklą pakeistų dvišalis arba regioninis bendradarbiavimas.

Konkrečiai atsižvelgiant į ankstesnius ENISA veiklos rezultatus ir į jos ateitį, po 2017 m. konsultacijų išryškėjo šios pagrindinės tendencijos[25]:

[25] Į konsultacijų klausimus atsakė 90 suinteresuotųjų subjektų iš 19 valstybių narių (88 atsakymai ir 2 pozicijos dokumentai), įskaitant nacionalines institucijas iš 15 valstybių narių, įskaitant Prancūziją, Italiją, Airiją ir Graikiją, bei 8 bendrąsias organizacijas, atstovaujančias daugeliui Europos organizacijų, pavyzdžiui, Europos bankų federaciją, Skaitmeninę Europą (atstovaujančią skaitmeninių technologijų pramonei Europoje), Europos telekomunikacijų tinklo operatorių asociaciją (ETNO). ENISA viešas

- Dauguma respondentų (74 %) bendrą ENISA veiklą 2013–2016 m. laikotarpiu įvertino teigiamai. Dauguma respondentų taip pat manė, kad ENISA pasieks įvairius savo tikslus (kiekvieną tikslą įvykdys bent 63 %). ENISA paslaugomis ir produktais reguliariai (kartą per mėnesį arba dažniau) naudojasi beveik pusė respondentų (46 %); šios paslaugos ir produktai vertinami dėl to, kad gaunami iš ES lygmens įstaigos (83 %), ir dėl kokybės (62 %).
- Respondentai nurodė keletą ES kibernetinio saugumo ateities spragų ir problemų, iš kurių penkios svarbiausios (iš 16) buvo šios: valstybių narių bendradarbiavimas; gebėjimas užkirsti kelią, aptikti didelio masto kibernetinius išpuolius ir juos suvaldyti; valstybių narių bendradarbiavimas kibernetinio saugumo klausimais; įvairių suinteresuotųjų subjektų bendradarbiavimas ir dalijimasis informacija, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą; ypatingos svarbos infrastruktūros apsauga nuo kibernetinių išpuolių.
- Didžioji dauguma respondentų (88 %) manė, kad dabartinės ES lygmens priemonės ir mechanizmai yra nepakankami arba tik iš dalies pakankami šiems klausimams spręsti. Didžioji dauguma respondentų (98 %) nurodė, kad į šiuos poreikius turėtų atsižvelgti ES įstaiga, o 99 % iš jų manė, kad ENISA yra tam tinkama organizacija.

Konsultacijos su suinteresuotaisiais subjektais

- 2016 m. balandžio 12 d. – liepos 5 d. Komisija surengė viešas konsultacijas dėl ENISA vertinimo ir gavo 421 atsakymą[26]. Vertinimo rezultatai tokie: 67,5 % respondentų išreiškė nuomonę, kad ENISA galėtų atlikti tam tikrą vaidmenį sukuriant suderintą IT produktų ir paslaugų saugumo sertifikavimo sistemą.

2016 m. konsultacijų dėl kibernetinio saugumo sutartinės viešojo ir privačiojo sektorių partnerystės[27] skirsnio dėl sertifikavimo rezultatai rodo, kad:

- 50,4 % (t. y. 121 iš 240) respondentų nežino, ar nacionalinės sertifikavimo schemos yra tarpusavyje pripažįstamos visose ES valstybėse narėse. 25,8 % (62 iš 240) atsakė „ne“, o 23,8 % (57 iš 240) atsakė „taip“;
- 37,9 % respondentų (91 iš 240) mano, kad esamos sertifikavimo schemos nepadeda tenkinti Europos pramonės poreikių. Kita vertus, 17,5 % respondentų (42 iš 240) – daugiausia pasaulinės bendrovės, veikiančios Europos rinkoje – išreiškė priešingą nuomonę;
- 49,6 % (119 iš 240) respondentų teigia, kad nelengva įrodyti standartų, sertifikavimo schemų ir etikečių lygiavertiškumą. 37,9 % (91 iš 240) atsakė „nežinau“ ir tik 12,5 % (30 iš 240) atsakė „taip“.

---

konsultacijas papildė keli kiti šaltiniai, įskaitant: i) išsamius pokalbius su maždaug 50 pagrindinių kibernetinio saugumo bendruomenės dalyvių; ii) apklausą, skirtą CSIRT tinklui; iii) apklausą, skirtą ENISA Valdančiajai tarybai, Vykdomajai valdybai ir Nuolatinei suinteresuotųjų subjektų grupei.

[26] 162 atsakymus pateikė piliečiai, o 33 atsakymus – pilietinės visuomenės atstovai ir vartotojų organizacijos. 186 atsakymus pateikė sektoriaus atstovai, o 40 atsakymų – valdžios institucijos, įskaitant kompetentingas institucijas, kurios užtikrina E. privatumo direktyvos vykdymą.

[27] Į skirsnio dėl sertifikavimo klausimus atsakė 240 suinteresuotųjų subjektų iš nacionalinių viešojo administravimo institucijų, didelių įmonių, MVĮ, labai mažų įmonių ir mokslinių tyrimų įstaigų.

Tiriamųjų duomenų rinkimas ir naudojimas

Komisija naudojosi šiomis išorės ekspertų rekomendacijomis:

- ENISA vertinimo tyrimas („Ramboll/Carsa“ 2017; SMART Nr. 2016/0077)
- IRT saugumo sertifikavimo ir ženklinimo tyrimas. Įrodymų rinkimas ir poveikio vertinimas („PriceWaterhouseCoopers“ 2017; SMART Nr. 2016/0029).

Poveikio vertinimas

- Šios iniciatyvos poveikio vertinimo ataskaitoje buvo nustatytos šios pagrindinės spręstinos problemos:
- kibernetinio saugumo politikos ir požiūrio į kibernetinį saugumą valstybėse narėse nenuoseklumas;
- išskaidyti ištekliai ir nevienodas požiūris į kibernetinį saugumą ES institucijose, agentūrose ir įstaigose ir
- nepakankamas piliečių ir įmonių informavimas, taip pat didėjanti nacionalinių ir sektorinių sertifikavimo schemų įvairovė.

Ataskaitoje įvertintos šios galimybės, susijusios su ENISA įgaliojimais:

- išlaikyti *status quo*, t. y. išplėsti įgaliojimai vis dar būtų ribotos trukmės (atskaitos scenarijaus galimybė);
- dabartinių ENISA įgaliojimų galiojimo pasibaigimas nepratęsiant įgaliojimų ir nenutraukiant ENISA veiklos (intervencinių politikos veiksmų nesiimama);
- pertvarkyta ENISA ir
- visišku operaciniu pajėgumu veikianti ES kibernetinio saugumo agentūra.

Ataskaitoje įvertintos šios galimybės, susijusios su kibernetinio saugumo sertifikavimu:

- nesiimti intervencinių politikos veiksmų (atskaitos scenarijaus galimybė);
- imtis ne teisėkūros priemonių (privalomos teisinės galios neturintys teisės aktai);
- ES teisėkūros procedūra priimamu teisės aktu sukurti privalomą sistemą visoms valstybėms narėms, paremtą vyresniųjų pareigūnų grupės informacinių sistemų klausimais (SOG-IS) sistema ir
- sukurti ES bendrą IRT kibernetinio saugumo sertifikavimo sistemą.

Atlikus analizę prieita prie išvados, kad tinkamiausia galimybė yra pertvarkyti ENISA ir sukurti ES bendrą IRT kibernetinio saugumo sertifikavimo sistemą.

Tinkamiausia galimybė buvo įvertinta kaip veiksmingiausia galimybė ES pasiekti nustatytus tikslus: padidinti kibernetinio saugumo pajėgumus, užtikrinti pasirengimą, bendradarbiavimą, informuotumą, skaidrumą ir išvengti rinkos suskaidymo. Ji taip pat buvo įvertinta kaip labiausiai atitinkanti ES kibernetinio saugumo strategijos bei susijusių politikos sričių (pvz., TIS direktyvos) ir bendrosios skaitmeninės rinkos strategijos politinius prioritetus. Per konsultacijas taip pat paaiškėjo, kad tinkamiausią galimybę palaiko dauguma suinteresuotųjų subjektų. Be to, rengiant poveikio vertinimą atlikta analizė parodė, kad pasirinkus tinkamiausią galimybę tikslai būtų pasiekti racionaliai panaudojant išteklius.

Komisijos reglamentavimo patikros valdyba iš pradžių liepos 24 d. pateikė neigiamą nuomonę, o vėliau, po pakartotinio ataskaitos pateikimo, 2017 m. rugpjūčio 25 d. pateikė teigiamą nuomonę. Į iš dalies pakeistą poveikio vertinimo ataskaitą buvo įtraukta papildomų įrodymų, galutinės ENISA vertinimo išvados ir papildomų paaiškinimų dėl politikos galimybių ir jų poveikio. Galutinės poveikio vertinimo ataskaitos 1 priede apibendrinama, kaip buvo atsižvelgta į valdybos antros nuomonės pastabas. Visų pirma ataskaita buvo atnaujinta siekiant išsamiau apibūdinti ES kibernetinio saugumo aplinką, įskaitant priemones, įtrauktas į bendrą komunikatą „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“ (JOIN(2017) 450) ir ypač svarbias agentūrai ENISA – ES kibernetinio saugumo projektą ir Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centrą, kuriems Agentūra teiks patarimus apie ES mokslinių tyrimų poreikius.

Ataskaitoje paaiškinama, kaip Agentūros pertvarka, susijusi, be kita ko, su naujomis užduotimis, geresnėmis įdarbinimo sąlygomis ir struktūriniu bendradarbiavimu su atitinkamos srities ES įstaigomis, padidintų jos kaip darbdavio patrauklumą ir padėtų spręsti problemas, susijusias su ekspertų samdymu. Ataskaitos 6 priede taip pat pateikiama patikslinta išlaidų, susijusių su ENISA politikos galimybėmis, sąmata. Sertifikavimo klausimu ataskaita buvo peržiūrėta siekiant išsamiau paaiškinti tinkamiausią galimybę (taip pat grafiškai) ir pateikti valstybėms narėms bei Komisijai tenkančių išlaidų, susijusių su nauja sertifikavimo sistema, sąmatą. Taip pat buvo išsamiau paaiškintas ENISA kaip pagrindinio sistemos subjekto pasirinkimas, susijęs su jos patirtimi šioje srityje ir tuo, kad ji yra vienintelė ES lygmens kibernetinio saugumo agentūra. Galiausiai buvo peržiūrėti sertifikavimui skirti skirsniai, siekiant išaiškinti skirtumus, palyginti su dabartine SOG-IS sistema, paaiškinti skirtingų politikos galimybių naudą bei tai, kad pačioje patvirtintoje Europos sertifikavimo schemoje bus apibrėžta IRT produktų ir paslaugų, kuriems taikoma ta schema, rūšis.

Reglamentavimo tinkamumas ir supaprastinimas

Netaikoma

Poveikis pagrindinėms teisėms

Kibernetinis saugumas yra būtinas norint apsaugoti asmenų privatumą ir asmens duomenis pagal ES pagrindinių teisių chartijos 7 ir 8 straipsnius. Įvykus kibernetiniam incidentui aiški grėsmė kyla privatumui ir asmens duomenų apsaugai. Taigi, kibernetinis saugumas yra būtina sąlyga privatumo ir asmens duomenų konfidencialumo apsaugai. Šiuo atžvilgiu, siekiant sustiprinti kibernetinį saugumą Europoje, pasiūlymu svariai papildomi galiojantys teisės aktai, kuriais užtikrinama pagrindinė teisė į privatumą ir asmens duomenis. Kibernetinis saugumas taip pat yra būtinas siekiant apsaugoti elektroninių ryšių konfidencialumą, taigi ir naudojimuisi žodžio laisve, informacijos laisve ir kitomis susijusiomis teisėmis, pavyzdžiui, minties, sąžinės ir religijos laisve.

4. POVEIKIS BIUDŽETUI

Žr. finansinę pažymą

5. KITI ELEMENTAI

- **Įgyvendinimo planai ir stebėjimo, vertinimo ir ataskaitų teikimo taisyklės**

Komisija stebės šio reglamento taikymą ir kas penkerius metus teiks vertinimo ataskaitą Europos Parlamentui, Tarybai ir Europos ekonomikos ir socialinių reikalų komitetui. Tose viešose ataskaitose bus pateikiama išsamios informacijos apie faktinį šio reglamento taikymą ir jo vykdymo užtikrinimą.

- **Išsamus konkrečių pasiūlymo nuostatų paaiškinimas**

Reglamento I antraštinėje dalyje išdėstomos bendrosios nuostatos: dalykas (1 straipsnis), apibrėžtys (2 straipsnis), įskaitant nuorodas į atitinkamas apibrėžtis kituose ES teisės aktuose, pavyzdžiui, Europos Parlamento ir Tarybos direktyvoje (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyva), Europos Parlamento ir Tarybos reglamente (EB) Nr. 765/2008, nustatančiame su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus gaminių pardavimo srityje ir panaikinančiame Reglamentą (EEB) Nr. 339/93, ir Europos Parlamento ir Tarybos reglamente (ES) Nr. 1025/2012 dėl Europos standartizacijos.

Reglamento II antraštinėje dalyje išdėstomos pagrindinės nuostatos, susijusios su ENISA, ES kibernetinio saugumo agentūra.

Šios antraštinės dalies I skyriuje nustatomi Agentūros įgaliojimai (3 straipsnis), tikslai (4 straipsnis) ir užduotys (5–11 straipsniai).

II skyriuje išdėstomas ENISA organizavimas ir pagrindinės nuostatos dėl jos struktūros (12 straipsnis). Jame nurodoma Valdančiosios tarybos (1 skirsnis, 13–17 straipsniai) ir Vykdomosios valdybos (2 skirsnis, 18 straipsnis) sudėtis, balsavimo taisyklės ir funkcijos bei vykdomojo direktoriaus (3 skirsnis, 19 straipsnis) funkcijos. Į jį taip pat įtrauktos nuostatos dėl nuolatinės suinteresuotųjų subjektų grupės (4 skirsnis, 20 straipsnis) sudėties ir vaidmens. Paskutiniame, bet ne mažiau svarbiame šio skyriaus 5 skirsnyje išdėstomos Agentūros veiklos taisyklės, susijusios, be kita ko, su Agentūros veiklos planavimu, interesų konfliktu, skaidrumu, konfidencialumu ir galimybe susipažinti su dokumentais (21–25 straipsniai).

III skyrius yra susijęs su Agentūros biudžeto sudarymu ir jo struktūra (26 ir 27 straipsniai) bei jo įgyvendinimo taisyklėmis (28 ir 29 straipsniai). Į jį taip pat įtrauktos nuostatos, kuriomis siekiama lengvinti kovą su sukčiavimu, korupcija ir kita neteisėta veikla (30 straipsnis).

IV skyrius yra susijęs su Agentūros darbuotojais. Jame pateikiamos bendrosios nuostatos dėl Tarnybos nuostatų ir įdarbinimo sąlygų ir taisyklės dėl privilegijų ir imuniteto (31 ir 32 straipsniai). Jame taip pat išdėstomos Agentūros vykdomojo direktoriaus įdarbinimo ir skyrimo taisyklės (33 straipsnis). Galiausiai jame pateikiamos nuostatos dėl deleguotųjų nacionalinių ekspertų ar kitų Agentūroje neįdarbintų darbuotojų (34 straipsnis).

Paskutiniame V skyriuje pateikiamos bendrosios su Agentūra susijusios nuostatos. Jame nurodomas teisinis statusas (35 straipsnis), taip pat nuostatos, reglamentuojančios atsakomybės, kalbų vartojimo ir asmens duomenų apsaugos klausimus (36–38 straipsniai), bei įslaptintos informacijos ir neskelbtinos neįslaptintos informacijos apsaugai užtikrinti skirtos saugumo taisyklės (40 straipsnis). Jame apibūdinamos Agentūros bendradarbiavimo su trečiosiomis šalimis ir tarptautinėmis organizacijomis taisyklės (39 straipsnis). Galiausiai jame pateikiamos nuostatos dėl Agentūros būstinės ir veiklos sąlygų, taip pat ombudsmeno administracinės kontrolės (41 ir 42 straipsniai).

Reglamento III antraštine dalimi kaip *lex generalis* įsteigiama IRT produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo sistema (toliau – **Sistema**) (1 straipsnis). Joje

nustatomas bendrasis Europos kibernetinio saugumo sertifikavimo schemų tikslas, t. y. užtikrinti, kad IRT produktai ir paslaugos atitiktų nustatytus kibernetinio saugumo reikalavimus, susijusius su jų pajėgumu tam tikru saugumo užtikrinimo lygiu išlikti atspariais veiksmams, keliantiems pavojų saugomų, perduodamų ar tvarkomų duomenų arba susijusių funkcijų arba paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui (43 straipsnis). Be to, joje nurodomi saugumo tikslai, kurių turi būti siekiama Europos kibernetinio saugumo sertifikavimo schemomis (45 straipsnis), be kita ko, gebėjimas apsaugoti duomenis nuo atsitiktinės arba neteisėtos prieigos ar atskleidimo, sunaikinimo ar pakeitimo, taip pat Europos kibernetinio saugumo sertifikavimo schemų turinys (t. y. elementai), kaip antai, išsamiai apibrėžta taikymo sritis, saugumo tikslai, vertinimo kriterijai ir kt. (47 straipsnis).

III antraštinėje dalyje taip pat nustatomas pagrindinis Europos kibernetinio saugumo sertifikavimo schemų teisinis poveikis, t. y. i) prievolė įgyvendinti schemą nacionaliniu lygmeniu ir savanoriškas sertifikavimas; ii) Europos kibernetinio saugumo sertifikavimo schemomis panaikinamas tiems patiems produktams ar paslaugoms taikomų nacionalinių schemų galiojimas (48 ir 49 straipsniai).

Šioje antraštinėje dalyje taip pat nustatomos Europos kibernetinio saugumo sertifikavimo schemų tvirtinimo procedūros ir atitinkami Komisijos, ENISA ir Europos kibernetinio saugumo sertifikavimo grupės (toliau – grupė) vaidmenys (44 straipsnis). Galiausiai šioje antraštinėje dalyje pateikiamos nuostatos dėl atitikties vertinimo įstaigų, įskaitant jų reikalavimus, įgaliojimus ir užduotis, nacionalines sertifikavimo priežiūros institucijas ir sankcijas.

Taip pat šia antraštine dalimi įsteigiama iš nacionalinių sertifikavimo priežiūros institucijų atstovų sudaryta grupė, kurios pagrindinė funkcija – bendradarbiauti su ENISA rengiant Europos kibernetinio saugumo sertifikavimo schemas ir patarti Komisijai bendro pobūdžio ar konkrečiais kibernetinio saugumo sertifikavimo politikos klausimais.

Reglamento IV antraštinėje dalyje pateikiamos baigiamosios nuostatos, apibrėžiančios įgaliojimų delegavimą, vertinimo reikalavimus, panaikinimą ir tęstinumą bei įsigaliojimą.

2017/0225 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

dėl ES 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[28],

atsižvelgdami į Regionų komiteto nuomonę[29],

laikydamiesi įprastos teisėkūros procedūros,

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

[28] OL C , , p. .
[29] OL C , , p. .

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[30], 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[31], kuriuo Agentūros įgaliojimai pratęsti iki 2012 m. kovo mėn. Reglamentu (EB) Nr. 580/2011[32] agentūros įgaliojimai buvo dar pratęsti iki 2013 m. rugsėjo 13 d. 2013 m. Europos Parlamentas ir Taryba priėmė Reglamentą (ES) Nr. 526/2013[33] dėl ENISA, kuriuo

---

30 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).

31 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).

32 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).

33 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).

panaikintas Reglamentas (EB) Nr. 460/2004 ir kuriuo Agentūros įgaliojimai buvo pratęsti iki 2020 m. birželio mėn.;

(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 nustatytos prievolės, susijusios 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 ES 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 ir visapusiškai bendradarbiaudama su Sąjungos institucijomis, įstaigomis, tarnybomis ir agentūromis bei valstybėmis narėmis Agentūra turėtų aktyviai prisidėti prie nacionalinių ir Sąjungos veiksmų. 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 su Sąjungos kibernetinio saugumo, taip pat ypatingos svarbos infrastruktūros apsaugos ir kibernetinio atsparumo politikos ir teisės plėtojimu, atnaujinimu ir peržiūra susijusiais klausimais. 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, įstaigoms, tarnyboms ir agentūroms plėtoti ir stiprinti pajėgumą ir pasirengimą užkirsti kelią tinklų ir informacijos saugumo problemoms 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. Agentūra taip pat turėtų padėti rengti ir atnaujinti Sąjungos ir valstybių narių tinklų ir informacinių sistemų saugumo, visų pirma kibernetinio saugumo, strategijas, skatinti jų sklaidą ir stebėti jų įgyvendinimo pažangą. 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, visų pirma siekiant padėti apsaugoti ypatingos svarbos infrastruktūros objektus, Agentūra turėtų padėti kurti sektorių keitimosi informacija ir jos analizės centrus (ISAC) dalydamasi geriausia praktika ir teikdama rekomendacijas apie esamas priemones ir procedūras, taip pat rekomendacijas sprendžiant su keitimusi informacija susijusius reguliavimo klausimus;

(18) Agentūra turėtų apibendrinti ir analizuoti nacionalines CSIRT ir CERT-EU ataskaitas ir nustatyti bendras keitimosi informacija taisykles, kalbą ir terminiją. Remdamasi TIS direktyva, kuria, sukūrus CSIRT tinklą, padėtas pamatas savanoriškiems techninės informacijos mainams 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. Vykdydama šią veiklą Agentūra turėtų 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 kasmetines kibernetinio saugumo pratybas išbandydama tokio bendradarbiavimo būdus;

(20) kad vykdydama savo veiklos užduotis Agentūra pasinaudotų CERT-EU ekspertinėmis žiniomis, jos turėtų palaikyti struktūrinį bendradarbiavimą būdamos netoli fizine prasme. Struktūrinis bendradarbiavimas paskatins reikiamą sinergiją ir ENISA ekspertinių žinių kaupimą. Jei tinkama, turėtų būti sudaryti specialūs šių dviejų organizacijų susitarimai, kuriuose turėtų būti nustatyta, kaip toks bendradarbiavimas bus įgyvendinamas praktiškai;

(21) vykdydama savo veiklos užduotis Agentūra turėtų teikti paramą valstybėms narėms, pavyzdžiui, konsultuoti ar teikti techninę pagalbą arba vykdyti grėsmių ir incidentų analizę. 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 vykdyti savo veiklos užduotis;

(22) reguliaraus techninio bendradarbiavimo, padedančio būti geriau informuotiems apie padėtį Sąjungoje, dalis turėtų būti Agentūros reguliariai 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 (savanoriškai) arba pagal TIS direktyvą įsteigti bendrieji informaciniai centrai, 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) atitinkamų valstybių narių prašymu arba su jomis sutarus didelį poveikį daugiau negu vienai valstybei narei padariusių incidentų *ex post* techniniuose tyrimuose, kuriuos vykdo arba jų vykdymą remia Agentūra, daugiausia dėmesio turėtų būti skiriama incidentų prevencijai, ir jie turėtų būti vykdomi nedarant poveikio bet kokiems teisminiams ar administraciniams procesams, kuriais siekiama nustatyti, kas yra kaltas ar atsakingas;

(24) atitinkamos valstybės narės turėtų teikti Agentūrai reikalingą informaciją ir pagalbą tyrimo vykdymo tikslais, nepažeidžiant Sutarties dėl Europos Sąjungos veikimo 346 straipsnio, arba dėl kitų viešosios politikos priežasčių;

(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 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 su kibernetiniu saugumu susijusių problemų;

(27) kad padidintų Sąjungos atsparumą, Agentūra turėtų plėtoti mokslinę kompetenciją interneto infrastruktūros ir ypatingos svarbos infrastruktūros objektų saugumo klausimais, konsultuodama, teikdama rekomendacijas ir dalydamasi geriausia praktika. 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, įstaigomis, tarnybomis ir agentūromis, 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) ir kitoms 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, kaip narė, kuri taip pat teikia CSIRT tinklo sekretoriato paslauga, 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 kasmetines 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, įstaigoms, tarnyboms ir agentūroms, ir prireikus ir joms paprašius – valstybėms narėms – dėl

mokslinių tyrimų poreikių tinklų ir informacijos saugumo, visų pirma kibernetinio saugumo, srityje;

(37) kibernetinio saugumo problemos yra pasaulinės. Būtinas glaudesnis tarptautinis bendradarbiavimas, kad būtų patobulinti 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, įstaigoms, tarnyboms ir agentūroms 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, 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[34]. 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[35]. Agentūra turėtų laikytis Sąjungos institucijoms taikytinų nuostatų ir nacionalinės teisės aktų dėl informacijos, visų pirma neskelbtinos neįslaptintos ir ES įslaptintos informacija tvarkymo;

(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) atitikties vertinimas – procesas, kuriuo nustatoma, ar produktas, procesas, paslauga, sistema, asmuo arba įstaiga atitinka jiems nustatytus reikalavimus. Šiame reglamente laikytina, jog sertifikavimas yra nepriklausomos trečiosios šalies, išskyrus produkto gamintoją ar paslaugos teikėją, atliekamas produkto, proceso, paslaugos, sistemos arba jų derinio (IRT produktų ir paslaugų) kibernetinio saugumo savybių atitikties vertinimas. Pats sertifikavimas savaime 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;

---

[34] 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).

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

(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 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 tarpusavio pripažinimo susitarimas turi didelių trūkumų, susijusių su didelėmis sąnaudomis ir ribota apimtimi. Iki šiol sukurti tik keli skaitmeninių produktų, pvz., skaitmeninio parašo, skaitmeninio tachografo ir lustinių kortelių, apsaugos profiliai. Svarbiausia, kad 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 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) Sąjungos 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 produktų ir paslaugų grupėms taikomas Europos kibernetinio saugumo sertifikavimo schemas. Įgyvendinti ir prižiūrėti šias schemas turėtų nacionalinės sertifikavimo priežiūros 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 produktai ir paslaugos atitiktų nustatytus reikalavimus. Tokie reikalavimai pagal šį reglamentą yra susiję su pajėgumu tam tikru saugumo užtikrinimo lygiu išlikti atspariems veiksmams, keliantiems pavojų saugomų, perduodamų ar tvarkomų duomenų arba naudojantis tais produktais, procesais, paslaugomis ir sistemomis siūlomų arba gaunamų funkcijų arba paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui. Šiame reglamente neįmanoma išsamiai nustatyti visiems IRT produktams ir paslaugoms keliamų kibernetinio saugumo reikalavimų. IRT 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 produktus ir paslaugas, turėtų būti toliau išsamiai nurodyta atskiros Komisijos tvirtinamos sertifikavimo schemos lygmeniu, pavyzdžiui, nurodant standartus ar technines specifikacijas;

(56) Komisijai turėtų būti suteikti įgaliojimai prašyti ENISA parengti konkretiems IRT 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 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;

(57) Europos kibernetinio saugumo sertifikavimas turėtų likti savanoriškas, išskyrus atvejus, kai Sąjungos ar nacionalinės teisės aktuose numatyta kitaip. 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 įgyvendinimo aktu Komisijos nustatytos datos. Be to, valstybės narės neturėtų nustatyti naujų nacionalinių kibernetinio saugumo sertifikavimo schemų, skirtų IRT produktams ir paslaugoms, kuriems jau taikoma esama Europos kibernetinio saugumo sertifikavimo schema;

(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 panaikinti atitikties vertinimo įstaigos akreditaciją, jeigu akreditacijos sąlygos nevykdomos arba nebevykdomos arba jeigu veiksmais, kurių imasi atitikties vertinimo įstaiga, pažeidžiamas šis reglamentas;

(59) būtina reikalauti, kad visos valstybės narės paskirtų po vieną kibernetinio saugumo sertifikavimo priežiūros instituciją prižiūrėti atitikties įvertinimo įstaigų ir jų teritorijoje įsisteigusių atitikties vertinimo įstaigų išduotų sertifikatų atitiktį šio reglamento ir atitinkamų kibernetinio saugumo sertifikavimo schemų reikalavimams. Nacionalinės sertifikavimo priežiūros institucijos turėtų nagrinėti fizinių ar juridinių asmenų pateiktus skundus, susijusius su jų teritorijose įsteigtų atitikties vertinimo įstaigų išduotais sertifikatais, 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 sertifikavimo priežiūros 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 priežiūros institucijų 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 Komisijai skirtas nuomones, susijusias su esamų Europos kibernetinio saugumo sertifikavimo schemų priežiūra ir peržiūra;

(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;

(62) Agentūra taip pat turėtų remti kibernetinio saugumo sertifikavimą bendradarbiaudama su Tarybos saugumo komitetu ir atitinkama nacionaline institucija dėl kriptografinio produktų, naudojamų įslaptintuose tinkluose, patvirtinimo;

(63) siekiant išsamiau nustatyti atitikties vertinimo įstaigų akreditavimo kriterijus, pagal Sutarties dėl Europos Sąjungos veikimo 290 straipsnį Komisijai turėtų būti suteikti įgaliojimai priimti deleguotuosius aktus. Atlikdama parengiamąjį darbą Komisija turėtų tinkamai konsultuotis, taip pat ekspertų lygmeniu. Šios konsultacijos turėtų būti vykdomos laikantis principų, išdėstytų 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros. Visų pirma, siekiant užtikrinti vienodas galimybes dalyvauti atliekant su deleguotaisiais aktais susijusį parengiamąjį darbą, Europos Parlamentas ir Taryba visus dokumentus turėtų gauti tuo pačiu metu kaip ir valstybių narių ekspertai, o jų ekspertams turėtų būti sistemingai suteikiama galimybė dalyvauti Komisijos ekspertų grupių, kurios atlieka su deleguotaisiais aktais susijusį parengiamąjį darbą, posėdžiuose;

(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 sertifikavimo priežiūros 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

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

(a) išdėstomi ES 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 produktų ir paslaugų kibernetinio saugumo lygį. Tokia sistema taikoma nepažeidžiant tam tikrų kitų Sąjungos aktų nuostatų dėl savanoriško arba privalomo sertifikavimo.

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 (-i) gali 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) produktų ir paslaugų, kuriems taikoma ta konkreti schema, sertifikavimui;

(10) Europos kibernetinio saugumo sertifikatas – atitikties vertinimo įstaigos išduotas dokumentas, kuriuo patvirtinama, kad tam tikras IRT produktas arba paslauga atitinka Europos kibernetinio saugumo sertifikavimo schemoje nustatytus konkrečius reikalavimus;

(11) IRT produktas ir paslauga – bet kuris tinklų ir informacinių sistemų elementas arba elementų grupė;

(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.

II ANTRAŠTINĖ DALIS

ENISA – ES kibernetinio saugumo agentūra

I SKYRIUS
ĮGALIOJIMAI, TIKSLAI IR UŽDUOTYS

3 straipsnis
Įgaliojimai

1. Agentūra prisiima jai šiuo reglamentu paskirtas užduotis, kad padėtų užtikrinti aukštą Sąjungos kibernetinio saugumo lygį.

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

3. Agentūros tikslai ir užduotys 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.

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 politiką.

3. Agentūra visoje Sąjungoje remia pajėgumų stiprinimą ir pasirengimą, padėdama Sąjungai, valstybėms narėms ir viešiesiems bei privatiesiems suinteresuotiesiems subjektams didinti savo tinklų ir informacinių sistemų apsaugą, lavinti įgūdžius ir gebėjimus kibernetinio saugumo srityje ir užtikrinti kibernetinį atsparumą.

4. Agentūra skatina valstybes nares, Sąjungos institucijas, agentūras ir įstaigas bei susijusius suinteresuotuosius subjektus, įskaitant privatųjį sektorių, bendradarbiauti ir koordinuoti su kibernetiniu saugumu susijusius klausimus Sąjungos lygmeniu.

5. Agentūra didina Sąjungos lygmens kibernetinio saugumo pajėgumus, kad papildytų valstybių narių veiksmus užkertant kelią kibernetinėms grėsmėms ir reaguojant į jas, visų pirma tarpvalstybinių incidentų atveju.

6. Agentūra skatina sertifikavimo naudojimą, be kita ko, prisidėdama 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.

5 straipsnis

Užduotys, susijusios su Sąjungos politikos ir teisės formavimu ir įgyvendinimu

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 pažeidimą, kuriuos kompetentingos institucijos pateikė Agentūrai pagal [Direktyvos, kuria nustatomas Europos elektroninių ryšių kodeksas] 40 straipsnį.

6 straipsnis

Užduotys, susijusios su pajėgumų stiprinimu

1. Agentūra padeda:

(a) valstybėms narėms gerinti kibernetinio saugumo problemų ir incidentų prevencijos, nustatymo, analizės ir reagavimo į juos pajėgumus, suteikdama joms reikiamų ekspertinių ir kitų žinių;

(b) Sąjungos institucijoms, įstaigoms, tarnyboms ir agentūroms gerinti kibernetinio saugumo problemų ir incidentų prevencijos, nustatymo, analizės ir reagavimo į juos pajėgumus, 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, kasmet 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 keisdamasi 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 padeda kurti sektorinius keitimosi informacija ir jos analizės centrus (ISAC), visų pirma Direktyvos (ES) 2016/1148 II priede išvardytuose sektoriuose, ir teikia jiems nuolatinę paramą, dalydamasi geriausia patirtimi ir teikdama rekomendacijas apie esamas priemones ir procedūras, taip pat rekomendacijas sprendžiant su keitimusi informacija susijusius reguliavimo klausimus.

7 straipsnis

Užduotys, susijusios su operatyviniu bendradarbiavimu Sąjungos lygmeniu

1. Agentūra remia kompetentingų viešųjų įstaigų, taip pat suinteresuotųjų subjektų operatyvinį bendradarbiavimą.

2. Agentūra operatyviniu lygmeniu bendradarbiauja su Sąjungos institucijomis, įstaigomis, tarnybomis ir agentūromis, 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 aktyviai padeda jo nariams tarpusavyje dalytis informacija ir bendradarbiauti.

4. Agentūra prisideda prie operatyvinio bendradarbiavimo su CSIRT tinklo dalyviais, teikdama šią paramą valstybėms narėms:

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

   (b) jų prašymu teikdama techninę pagalbą, įvykus didelį arba esminį poveikį turintiems incidentams;

   (c) analizuodama pažeidžiamumą, artefaktus ir incidentus.

Atlikdama šias užduotis Agentūra ir CERT-EU struktūriškai bendradarbiauja, kad pasinaudotų sąveika, visų pirma susijusia su operatyviniais aspektais.

5. Dviem arba daugiau susijusių valstybių narių paprašius ir tiktai vieninteliu tikslu – pakonsultuoti dėl būsimų incidentų prevencijos – Agentūra padeda atlikti arba atlieka incidentų, turinčių didelį arba esminį poveikį pagal Direktyvą (ES) 2016/1148, techninį *ex post* tyrimą pagal suinteresuotų įmonių pranešimus. Agentūra taip pat atlieka tokį tyrimą Komisijai pateikus tinkamai pagrįstą prašymą ir susijusioms valstybėms narėms pritarus, jeigu tokie incidentai paveikia daugiau nei dvi valstybes nares.

   Dėl tyrimo masto ir jo atlikimo procedūros susitaria susijusios valstybės narės ir Agentūra, ir jis neturi daryti poveikio jokiam vykdomam nusikalstamos veikos tyrimui, susijusiam su tuo pačiu incidentu. Tyrimas užbaigiamas galutine techninе ataskaita, kurią parengia Agentūra, visų pirma remdamasi susijusių valstybių narių ir įmonės (-ių) pateikta informacija ir pastabomis, ir su kuria sutinka susijusios valstybės narės. Ataskaitos santrauka, kurioje koncentruojamasi į rekomendacijas dėl būsimų incidentų prevencijos, išplatinama CSIRT tinklui.

6. Agentūra kasmet Sąjungos lygmeniu organizuoja kibernetinio saugumo pratybas ir padeda jas organizuoti valstybėms narėms, ES institucijoms, agentūroms bei įstaigoms, kai jos to paprašo. Metinės pratybos Sąjungos lygmeniu apima techninius, operatyvinius ir strateginius elementus ir padeda pasirengti koordinuotam Sąjungos

lygmens atsakui į didelio masto tarpvalstybinius kibernetinio saugumo incidentus. Agentūra taip pat prisideda prie sektorinių kibernetinio saugumo pratybų kartu su susijusiais ISAC ir prireikus padeda jas organizuoti, taip pat leidžia ISAC dalyvauti Sąjungos lygmens kibernetinio saugumo pratybose.

7. Agentūra 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 (savanoriškai) arba pagal TIS direktyvą įsteigti bendrieji informaciniai centrai (pagal TIS direktyvos 14 straipsnio 5 dalį), 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 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) padėdama techniškai suvaldyti incidentą arba krizę, taip pat sudarydama palankesnes sąlygas valstybėms narėms keistis techniniais sprendimais;

   (d) remdama su incidentu arba krize susijusių viešųjų ryšių veiklą;

   (e) išbandydama bendradarbiavimo reaguojant į tokius incidentus arba krizes planus.

8 straipsnis

Užduotys, susijusios su rinka, kibernetinio saugumo sertifikavimu ir standartizavimu

Agentūra:

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

   (1) rengdama potencialias IRT produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo schemas 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 praktiką, susijusią su IRT produktų ir paslaugų kibernetinio saugumo reikalavimais, bendradarbiaudama su nacionalinėmis sertifikavimo priežiūros institucijomis ir sektoriaus atstovais;

(b) padeda nustatyti ir įgyvendinti Europos ir tarptautinius rizikos valdymo ir IRT produktų ir paslaugų saugumo standartus, 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

Užduotys, susijusios su žiniomis, informavimu ir informuotumo didinimu

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 kibernetinio saugumo tendencijas ir padėtų užkirsti kelią problemoms;

(c) bendradarbiaudama su ekspertais iš valstybių narių institucijų, pateikia tinklų ir informacinių sistemų, visų pirma interneto infrastruktūros ir tos infrastruktūros, kuria naudojasi Direktyvos (ES) 2016/1148 II priede išvardyti sektoriai, saugumo užtikrinimo rekomendacijų, gairių ir geriausią praktiką;

(d) renka, sutelkia Sąjungos institucijų, agentūrų ir įstaigų pateiktą informaciją apie kibernetinį saugumą ir pateikia ją specialiame portale naudotis visuomenei;

(e) didina visuomenės informuotumą apie kibernetinio saugumo riziką ir piliečiams bei organizacijoms pateikia atskiriems naudotojams skirtas gerosios praktikos rekomendacijas;

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

(g) bendradarbiaudama su valstybėmis narėmis ir Sąjungos institucijomis, įstaigomis, tarnybomis ir agentūromis, organizuoja reguliarias informavimo kampanijas, kuriomis siekiama didinti kibernetinį saugumą ir šios problemos matomumą Sąjungoje.

10 straipsnis

Užduotys, susijusios su moksliniais tyrimais ir inovacijomis

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

Užduotys, susijusios su tarptautiniu bendradarbiavimu

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) Komisijos prašymu sudarydama susijusioms tarptautinėms organizacijoms palankias sąlygas keistis geriausia patirtimi;

(c) paprašius teikdama Komisijai ekspertines žinias.

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, kuris vykdo 19 straipsnyje nustatytas pareigas; ir

(d) nuolatinė suinteresuotųjų subjektų grupė, atliekanti 20 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;

(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. Jei reikia, skubiais atvejais Vykdomoji valdyba gali Valdančiosios tarybos vardu priimti tam tikrus laikinus sprendimus, visų pirma administracinio valdymo klausimais, įskaitant sprendimą sustabdyti paskyrimų tarnybos įgaliojimų perdavimą ir biudžeto reikalus.

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 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;

   (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. Vykdomasis direktorius sprendžia, ar būtina, kad vienoje arba daugiau valstybių narių dirbtų Agentūros darbuotojai, kad Agentūros užduotys būtų vykdomos veiksmingai ir efektyviai. Prieš nuspręsdamas įsteigti vietos skyrių vykdomasis direktorius gauna išankstinį Komisijos, Valdančiosios tarybos ir susijusios (-ių) valstybės narės (-ių) pritarimą. Veiklos, kurią vykdys vietos skyrius, sritis sprendime nustatoma taip, kad būtų išvengta nebūtinų išlaidų ir Agentūros administracinių funkcijų dubliavimo. Jei tinka arba būtina, susitariama su atitinkama (-omis) valstybe (-ėmis) nare (-ėmis).

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, 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.

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[36] 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.

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.

---

[36] 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).

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 (toliau – 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[37] ir 2015/444[38] nustatytus saugumo principus. Tos taisyklės apima įslaptintos informacijos tvarkymo ir saugojimo bei keitimosi ja nuostatas.

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.

[37] 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/443 dėl saugumo Komisijoje (OL L 72, 2015 3 17, p. 41).

[38] 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).

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[39], 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.

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[40] 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

[39] 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).

[40] 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).

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.

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. Vykdomasis direktorius skiriamas penkerių metų kadencijai. 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 penkeriems 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, kuri remiasi Komisijos siūlymu, 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, arba ji gali pasinaudoti abiem galimybėmis.

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[41]. 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[42].

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.

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.

---

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

42 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).

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 geriausias įmanomas 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 schemos

Europos kibernetinio saugumo sertifikavimo schema patvirtinama, kad pagal tokią schemą sertifikuoti IRT produktai ir paslaugos atitinka nustatytus reikalavimus, susijusius su jų pajėgumu tam tikru saugumo užtikrinimo lygiu išlikti atspariems veiksmams, keliantiems pavojų saugomų, perduodamų ar tvarkomų duomenų arba naudojantis tais produktais, procesais, paslaugomis ir sistemomis siūlomų arba gaunamų funkcijų arba paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui.

44 straipsnis

Europos kibernetinio saugumo sertifikavimo schemos rengimas ir tvirtinimas

1. Gavusi Komisijos prašymą, ENISA parengia potencialią šio reglamento 45, 46 ir 47 straipsniuose nustatytus reikalavimus atitinkančią Europos kibernetinio saugumo sertifikavimo schemą. Parengti potencialią Europos kibernetinio saugumo sertifikavimo schemą Komisijai gali pasiūlyti Valstybės narės arba Europos kibernetinio saugumo sertifikavimo grupė (toliau – Grupė), įsteigta pagal 53 straipsnį.
2. Rengdama potencialias šio straipsnio 1 dalyje nurodytas schemas ENISA konsultuojasi su visais suinteresuotaisiais subjektais ir glaudžiai bendradarbiauja su grupe. Grupė teikia ENISA pagalbą ir ekspertų konsultacijas, kurių jai reikia rengiant potencialią schemą, ir prireikus teikia nuomones.
3. ENISA pagal šio straipsnio 2 dalį parengtą potencialią Europos kibernetinio saugumo sertifikavimo schemą teikia 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 produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo schemos.
5. ENISA administruoja specialią interneto svetainę, kurioje teikiama informacija apie Europos kibernetinio saugumo sertifikavimo schemas ir jos viešinamos.

45 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų saugumo tikslai

Europos kibernetinio saugumo sertifikavimo schema turi būti parengta taip, kad būtų atsižvelgta į šiuos saugumo tikslus (jei taikomi):

(a) apsaugoti saugomus, perduodamus ar kitaip tvarkomus duomenis nuo atsitiktinio ar neteisėto jų saugojimo, tvarkymo, prieigos prie jų ar jų atskleidimo;

(b) apsaugoti saugomus, perduodamus ar kitaip tvarkomus duomenis nuo atsitiktinio ar neteisėto jų sunaikinimo, atsitiktinio jų netekimo ar pakeitimo;

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

(d) registruoti, kurie duomenys, funkcijos ar paslaugos buvo perduoti, kada ir kas juos perdavė;

(e) užtikrinti, kad būtų galima patikrinti, prie kokių duomenų, paslaugų ar funkcijų buvo gauta prieiga arba jais buvo pasinaudota, kada ir kas tai padarė;

(f) įvykus fiziniam ar techniniam incidentui, laiku atkurti duomenų, paslaugų ir funkcijų prieinamumą ir prieigos prie jų galimybes;

(g) užtikrinti, kad IRT produktai ir paslaugos būtų teikiami su atnaujinta programine įranga be žinomų saugumo spragų ir kad būtų teikiami saugaus programinės įrangos atnaujinimo mechanizmai.

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 produktams ir paslaugoms, sertifikuotiems pagal tą schemą, taikomų saugumo užtikrinimo lygių: bazinis, pakankamas ir (arba) aukštas.

2. Bazinis, pakankamas ir aukštas saugumo užtikrinimo lygiai atitinkamai turi atitikti šiuos kriterijus:

(a) bazinis saugumo užtikrinimo lygis patvirtinimas pagal Europos kibernetinio saugumo sertifikavimo schemą išduotu sertifikatu, kuriuo užtikrinamas ribotas pareikštų arba patvirtintų IRT produkto arba paslaugos kibernetinio saugumo savybių patikimumo laipsnis, ir apibūdinamas remiantis su juo susijusiomis techninėmis specifikacijomis, standartais ir procedūromis, įskaitant technines kontrolės priemones, kurių paskirtis – sumažinti kibernetinio saugumo incidentų riziką;

(b) pakankamas saugumo užtikrinimo lygis patvirtinimas pagal Europos kibernetinio saugumo sertifikavimo schemą išduotu sertifikatu, kuriuo užtikrinamas pakankamas pareikštų arba patvirtintų IRT produkto arba paslaugos kibernetinio saugumo savybių patikimumo laipsnis, ir apibūdinamas remiantis su juo susijusiomis techninėmis specifikacijomis, standartais ir procedūromis, įskaitant technines kontrolės priemones, kurių paskirtis – labai sumažinti kibernetinio saugumo incidentų riziką;

(c) aukštas saugumo užtikrinimo lygis patvirtinamas pagal Europos kibernetinio saugumo sertifikavimo schemą išduotu sertifikatu, kuriuo užtikrinamas aukštesnis pareikštų arba patvirtintų IRT produkto arba paslaugos kibernetinio saugumo savybių patikimumo laipsnis nei sertifikatais, kuriais patvirtinamas pakankamas saugumo užtikrinimo lygis, ir apibūdinamas remiantis su juo susijusiomis techninėmis specifikacijomis, standartais ir procedūromis, įskaitant technines kontrolės priemones, kurių paskirtis – išvengti kibernetinio saugumo incidentų.

47 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų elementai

1. Europos kibernetinio saugumo sertifikavimo schemą sudaro šie elementai:

   (a) sertifikavimo dalykas ir apimtis, įskaitant sertifikuojamų IRT produktų ir paslaugų rūšį arba kategorijas;

   (b) išsamūs kibernetinio saugumo reikalavimai, pagal kuriuos vertinami konkretūs IRT produktai ir paslaugos, pavyzdžiui, nurodant Sąjungos ar tarptautinius standartus arba technines specifikacijas;

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

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

   (e) informacija, kurią pareiškėjas turi pateikti atitikties vertinimo įstaigoms ir kuri yra reikalinga sertifikavimui;

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

   (g) jeigu pagal schemą numatoma stebėsena, sertifikatų reikalavimų laikymosi stebėsenos taisyklės, įskaitant mechanizmus, kuriais įrodoma, kad nuolat laikomasi nurodytų kibernetinio saugumo reikalavimų;

   (h) sertifikavimo taikymo srities suteikimo, išlaikymo, tęsimo, išplėtimo ir sumažinimo sąlygos;

   (i) taisyklės, susijusios su sertifikuotų IRT produktų ir paslaugų neatitikties sertifikavimo reikalavimams padariniais;

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

   (k) taisyklės dėl atitikties vertinimo įstaigų įrašų laikymo;

   (l) nustatytos nacionalinės kibernetinio saugumo sertifikavimo schemos, taikomos tos pačios rūšies ar kategorijų IRT produktams ir paslaugoms;

   (m) išduodamo sertifikato turinys.

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 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.

48 straipsnis

Kibernetinio saugumo sertifikavimas

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

2. Sertifikavimas yra savanoriškas, išskyrus atvejus, kai Sąjungos teisėje nustatyta kitaip.

3. Europos kibernetinio saugumo sertifikatą pagal šį straipsnį 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 schemoje gali būti nustatyta, kad Europos kibernetinio saugumo sertifikatą pagal tą schemą gali išduoti tik viešoji įstaiga. Tokia viešoji įstaiga yra viena iš šių įstaigų:

   (a) 50 straipsnio 1 dalyje nurodyta nacionalinė sertifikavimo priežiūros institucija;

   (b) įstaiga, kuri pagal 51 straipsnio 1 dalį yra akredituota kaip atitikties vertinimo įstaiga, arba

   (c) atitinkamos valstybės narės teisės aktais, įstatymo lydimaisiais teisės aktais ar kitomis oficialiomis administracinėmis procedūromis sukurta įstaiga, atitinkanti produktus, procesus ir paslaugas sertifikuojančioms įstaigoms pagal standartą ISO/IEC 17065:2012 keliamus reikalavimus.

5. Savo IRT produktus ir paslaugas sertifikuoti teikiantis fizinis arba juridinis asmuo pateikia 51 straipsnyje nurodytai atitikties vertinimo įstaigai visą sertifikavimo procedūrai atlikti reikalingą informaciją.

6. Sertifikatai išduodami ne ilgesniam kaip trejų metų laikotarpiui ir gali būti pratęsti tomis pačiomis sąlygomis, jei ir toliau atitinkami 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 produktams ir paslaugoms, kuriems taikoma Europos kibernetinio saugumo sertifikavimo schema, netenka galios nuo pagal 44 straipsnio 4 dalį priimtame įgyvendinimo akte nustatytos datos. Esamos nacionalinės kibernetinio saugumo sertifikavimo schemos ir susijusios procedūros, taikomos IRT produktams ir paslaugoms, kuriems Europos kibernetinio saugumo sertifikavimo schema netaikoma, ir toliau galios.

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

3. Esami pagal nacionalines kibernetinio saugumo sertifikavimo schemas išduoti sertifikatai toliau galioja iki jų galiojimo pabaigos datos.

50 straipsnis

Nacionalinės sertifikavimo priežiūros institucijos

1. Kiekviena valstybė narė paskiria nacionalinę sertifikavimo priežiūros instituciją.

2. Kiekviena valstybė narė praneša Komisijai apie paskirtą instituciją.

3. Kiekvienos nacionalinės sertifikavimo priežiūros institucijos veiklos organizavimas, finansavimo sprendimai, teisinė struktūra ir sprendimų priėmimas nepriklauso nuo prižiūrimų subjektų.

4. Valstybės narės užtikrina, kad nacionalinės sertifikavimo priežiūros 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 sertifikavimo priežiūros institucijos:

   (a) stebi ir užtikrina šioje antraštinėje dalyje nustatytų nuostatų taikymą nacionaliniu lygmeniu ir prižiūri atitinkamose savo teritorijose įsteigtų atitikties vertinimo įstaigų išduotų sertifikatų atitiktį šioje antraštinėje dalyje ir atitinkamoje Europos kibernetinio saugumo sertifikavimo schemoje nustatytiems reikalavimams;

   (b) stebi ir prižiūri įgyvendinant šį reglamentą atitikties vertinimo įstaigų vykdomą veiklą, be kita ko, susijusią su atitikties vertinimo įstaigų notifikavimu ir susijusiais uždaviniais, nustatytais šio reglamento 52 straipsnyje;

   (c) nagrinėja fizinių ar juridinių asmenų pateiktus skundus, susijusius su jų teritorijose įsteigtų 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 sertifikavimo priežiūros institucijomis ar kitomis valdžios institucijomis, be kita ko, dalydamosi informacija apie galimą IRT 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 sertifikavimo priežiūros institucija turi bent šiuos įgaliojimus:

   (a) prašyti atitikties vertinimo įstaigų ir Europos kibernetinio saugumo sertifikatų turėtojų pateikti bet kokią informaciją, kurios jai reikia savo užduotims atlikti;

   (b) vykdyti tiriamąjį atitikties vertinimo įstaigų ir Europos kibernetinio saugumo sertifikatų turėtojų auditą siekiant patikrinti, ar laikomasi III antraštinės dalies nuostatų;

   (c) pagal nacionalinę teisę imtis atitinkamų priemonių siekiant užtikrinti, kad atitikties vertinimo įstaigos arba sertifikatų turėtojai 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 atšaukti šio reglamento arba Europos kibernetinio saugumo sertifikavimo schemos reikalavimų neatitinkančius sertifikatus;

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

8. Nacionalinės sertifikavimo priežiūros institucijos bendradarbiauja tarpusavyje ir su Komisija ir, visų pirma, keičiasi informacija, patirtimi ir gerąja praktika, susijusia su kibernetinio saugumo sertifikavimu ir techniniais IRT 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.

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 panaikina atitikties vertinimo įstaigos akreditaciją pagal šio straipsnio 1 dalį, jeigu akreditacijos sąlygos nevykdomos arba nebevykdomos, arba jeigu veiksmais, kurių imasi atitikties vertinimo įstaiga, pažeidžiamas šis reglamentas.

52 straipsnis
Notifikavimas

1. Dėl kiekvienos pagal 44 straipsnį patvirtintos Europos kibernetinio saugumo sertifikavimo schemos nacionalinės sertifikavimo priežiūros institucijos praneša Komisijai apie akredituotas atitikties vertinimo įstaigas, akredituotas išduoti 46 straipsnyje nurodytų nustatytų saugumo užtikrinimo lygių sertifikatus ir, be reikalo nedelsdama, 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 sertifikavimo priežiūros institucija gali pateikti Komisijai prašymą iš šio straipsnio 2 dalyje nurodyto sąrašo išbraukti tos nacionalinės sertifikavimo priežiūros institucijos notifikuotą atitikties vertinimo įstaigą. Komisija atitinkamus sąrašo pakeitimus *Europos Sąjungos oficialiajame leidinyje* paskelbia per vieną mėnesį nuo nacionalinės sertifikavimo priežiūros 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 pagal 55 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.

53 straipsnis

Europos kibernetinio saugumo sertifikavimo grupė

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

2. Grupę sudaro nacionalinės sertifikavimo priežiūros institucijos. Nacionalinėms sertifikavimo priežiūros institucijoms atstovauja jų vadovai arba kiti aukšto lygio atstovai.

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;

   (c) pasiūlyti Komisijai, kad ji paprašytų Agentūros parengti potencialią Europos kibernetinio saugumo sertifikavimo schemą pagal šio reglamento 44 straipsnį;

   (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 gerąja patirtimi, susijusia su kibernetinio saugumo sertifikavimo schemomis;

   (f) keičiantis informacija sudaryti palankesnes sąlygas nacionalinėms sertifikavimo priežiūros institucijoms bendradarbiauti pagal šią antraštinę dalį, visų pirma nustatant efektyvaus keitimosi informacija visais kibernetinio saugumo sertifikavimo klausimais metodus.

4. Grupei pirmininkauja Komisija ir, kaip numatyta 8 straipsnio a punkte, padedama agentūros ENISA teikia sekretoriato paslaugas.

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. Nustatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomosios. Valstybės narės [iki ... / nedelsdamos] praneša Komisijai apie tas taisykles ir priemones ir ją informuoja apie visus vėlesnius joms įtakos turinčius pakeitimus.

IV ANTRAŠTINĖ DALIS
BAIGIAMOSIOS NUOSTATOS

55 straipsnis
Komiteto procedūra

1. Komisijai padeda komitetas. Tas komitetas – komitetas, apibrėžtas Reglamente (ES) Nr. 182/2011.
2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.

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*.

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

Priimta Briuselyje

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas	*Pirmininkas*

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

Europos Parlamento ir Tarybos reglamento dėl ENISA, ES kibernetinio saugumo agentūros, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013, ir ryšių technologijų kibernetinio saugumo sertifikavimo (Kibernetinio saugumo aktas / reglamentas), pasiūlymas

1.2. Atitinkama (-os) politikos sritis (-ys)

Politikos sritis: 09 - Ryšių tinklai, turinys ir technologijos

Veikla: 09.02 Skaitmeninė bendroji rinka

1.3. Pasiūlymo (iniciatyvos) pobūdis

☒ Pasiūlymas (iniciatyva) susijęs (-usi) su **nauja priemone (III antraštinė dalis – Sertifikavimas)**

☐ Pasiūlymas (iniciatyva) susijęs (-usi) su **nauja priemone, kuri bus priimta įgyvendinus bandomąjį projektą ir (arba) atlikus parengiamuosius veiksmus**[43]

☒ Pasiūlymas (iniciatyva) susijęs (-usi) su **esamos priemonės (II antraštinė dalis – ENISA įgaliojimas) galiojimo pratęsimu**

☐ Pasiūlymas (iniciatyva) susijęs (-usi) su **priemone, perorientuota į naują priemonę**

1.4. Tikslas (-ai)

1.4.1. Komisijos daugiametis (-čiai) strateginis (-iai) tikslas (-ai), kurio (-ių) siekiama šiuo pasiūlymu (šia iniciatyva)

1. Didinti valstybių narių, įmonių ir visos ES atsparumą.

2. Užtikrinti tinkamą IRT produktų ir paslaugų ES vidaus rinkos veikimą.

3. Didinti IRT srityje veikiančių ES bendrovių konkurencingumą pasaulyje.

4. Suderinti valstybių narių su kibernetiniu saugumu susijusius įstatymus ir kitus teisės aktus.

1.4.2. Konkretus (-ūs) tikslas (-ai)

Atsižvelgiant į bendruosius tikslus bei į platesnį peržiūrėtos kibernetinio saugumo strategijos kontekstą, priemone apibrėžiant ENISA įgaliojimų apimtį ir sukuriant Europos IRT produktų ir paslaugų sertifikavimo sistemą ketinama siekti šių konkrečių tikslų:

1. didinti valstybių narių ir įmonių **galimybes bei pasirengimą**;
2. gerinti valstybių narių ir ES institucijų, agentūrų bei įstaigų **bendradarbiavimą ir koordinavimą**;
3. didinti **ES lygmens galimybes papildyti valstybių narių veiksmus**, ypač tarpvalstybinių kibernetinių krizių atveju;
4. didinti piliečių ir įmonių **informuotumą** kibernetinio saugumo klausimais;
5. didinant bendrą IRT produktų ir paslaugų **kibernetinio saugumo užtikrinimo**

[43] Kaip nurodyta Finansinio reglamento 54 straipsnio 2 dalies a arba b punkte.

skaidrumą[44], sustiprinti pasitikėjimą bendrąja skaitmenine rinka ir skaitmeninėmis inovacijomis.

ENISA padės siekti pirmiau nurodytų tikslų šiomis priemonėmis:

Remdama politikos formavimą: teikdama rekomendacijas ir patarimus Komisijai ir valstybėms narėms atnaujinant ir plėtojant visapusišką kibernetinio saugumo srities sistemą, taip pat konkretiems sektoriams skirtas politikos ir teisėkūros iniciatyvas kibernetinio saugumo klausimais; prisidėdama prie Bendradarbiavimo grupės veiklos (Direktyvos (ES) 2016/1148 11 straipsnis) ir teikdama ekspertines žinias ir pagalbą; remdama elektroninės atpažinties ir patikimumo užtikrinimo paslaugų srities politikos plėtojimą ir įgyvendinimą; skatindama kompetentingas institucijas keistis geriausia patirtimi.

Remdama pajėgumų stiprinimą: teikdama paramą valstybėms narėms, Sąjungos institucijoms, įstaigoms, tarnyboms ir agentūroms plėtojant ir gerinant kibernetinio saugumo problemų ir incidentų prevenciją, nustatymą, analizę ir pajėgumą į juos reaguoti; valstybių narių prašymu padėdama joms kurti nacionalines CSIRT ir nacionalines kibernetinio saugumo strategijas; padėdama Sąjungos institucijoms rengti ir peržiūrėti Sąjungos kibernetinio saugumo strategijas; teikdama kibernetinio saugumo mokymus; padėdama valstybėms narėms Bendradarbiavimo grupėje keistis geriausia patirtimi; padėdama kurti sektorinius keitimosi informacija ir jos analizės centrus (ISAC).

Remdama operatyvinį bendradarbiavimą ir krizių valdymą: remdama kompetentingų viešųjų institucijų ir suinteresuotųjų subjektų bendradarbiavimą, šiuo tikslu sukuriant sistemingo bendradarbiavimo su Sąjungos institucijomis, įstaigomis, tarnybomis ir agentūromis, kurių veikla susijusi su kibernetiniu saugumu ir kova su elektroniniu nusikalstamumu bei privatumo ir asmens duomenų apsauga, mechanizmą; teikdama sekretoriato paslaugas CSIRT tinklui (Direktyvos (ES) 2016/1148 12 straipsnio 2 dalis) bei prisidėdama prie operatyvinio bendradarbiavimo tinkle, valstybių narių prašymu teikdama (bendradarbiaujant su CERT-EU) joms paramą; rengdama reguliarias kibernetinio saugumo pratybas; padėdama rengti koordinuotą atsaką į didelio masto tarpvalstybinius kibernetinio saugumo incidentus ir krizes; bendradarbiaujant su CSIRT tinklu vykdydama *ex post* techninį rimtų incidentų tyrimą ir teikdama rekomendacijas dėl tolesnių veiksmų.

Vykdydama su rinka susijusias užduotis (standartizavimo, sertifikavimo): atlikdama tam tikras funkcijas, visų pirma susijusias su vidaus rinkos rėmimu, t. y. kibernetinio saugumo rinkos stebėjimo centro funkciją ir analizuodama atitinkamas tendencijas kibernetinio saugumo rinkoje siekiant geriau suderinti paklausą ir pasiūlą; remdama ir skatindama kurti bei įgyvendinti Sąjungos IRT produktų ir paslaugų kibernetinio saugumo sertifikavimo politiką, šiuo tikslu rengdama Europos IRT produktų ir paslaugų saugumo sertifikavimo schemas, teikdama sekretoriato paslaugas Sąjungos kibernetinio saugumo sertifikavimo grupei, teikdama rekomendacijas ir gerąją patirtį, susijusią su IRT produktų ir paslaugų saugumo reikalavimais, bendradarbiaujant su nacionalinėmis sertifikavimo priežiūros institucijomis ir sektoriaus atstovais. **Prisidėdama prie žinių, informacijos bei sąmoningumo didinimo:** teikdama pagalbą ir patarimus Komisijai ir valstybėms narėms siekiant, kad visoje Sąjungoje būtų pasiektas aukštas TIS žinių ir jų taikymo sektoriuje veikiančiuose suinteresuotuosiuose subjektuose lygis. Ši veikla taip pat apima, per tam skirtą portalą, informacijos apie tinklų ir informacinių sistemų saugumą [arba kibernetinis saugumas] telkimą, organizavimą ir viešinimą; Kitas svarbus elementas yra plačiajai

[44] Kibernetinio saugumo užtikrinimo skaidrumas reiškia, kad vartotojams suteikiama pakankamai informacijos apie kibernetinio saugumo savybes, ir tokiu būdu vartotojai gali objektyviai nustatyti atitinkamo IRT produkto, paslaugos ar proceso saugumo lygį.

visuomenei skirtos informuotumo didinimo ir informavimo kampanijos apie kibernetinio saugumo riziką.

Remdama mokslinius tyrimus ir inovacijas: patardama klausimais, susijusiais su mokslinių tyrimų poreikiais ir kibernetinio saugumo srities prioritetų nustatymu.

Remdama tarptautinį bendradarbiavimą: remdama Sąjungos pastangas bendradarbiauti su trečiosiomis šalimis ir tarptautinėmis organizacijomis siekiant skatinti tarptautinį kibernetinio saugumo srities bendradarbiavimą.

SERTIFIKAVIMAS

Sertifikavimo sistema padės siekti tikslų didinant bendrą IRT produktų ir paslaugų kibernetinio saugumo užtikrinimo skaidrumą[45] ir taip sustiprinant pasitikėjimą bendrąja skaitmenine rinka ir skaitmeninėmis inovacijomis. Tai taip pat padės išvengti daugybės sertifikavimo schemų ES ir susijusių reikalavimų bei vertinimo kriterijų visose valstybėse narėse ir sektoriuose atsiradimo.

1.4.3. Numatomas (-i) rezultatas (-ai) ir poveikis

Nurodyti poveikį, kurį pasiūlymas (iniciatyva) turėtų padaryti tiksliniams gavėjams (tikslinėms grupėms).

Numatoma, kad sustiprinta ENISA (sustiprinant pajėgumus, prevenciją, bendradarbiavimą ir didinant informuotumą ES lygmeniu ir atitinamai didinant bendrą ES kibernetinį atsparumą) ir IRT produktų ir paslaugų ES sertifikavimo sistemos stiprinimas turėtų tokį poveikį (sąrašas nėra išsamus):

Bendras poveikis:

- bendras teigiamas poveikis vidaus rinkai dėl mažesnio rinkos susiskaidymo ir pasitikėjimo skaitmeninėmis technologijomis didinimas, užtikrinant geresnį bendradarbiavimą, labiau suderintą požiūrį į ES kibernetinio saugumo politiką ir didesnius ES lygmens pajėgumus. Tai turėtų teigiamą ekonominį poveikį, nes padėtų sumažinti kibernetinio saugumo incidentų / kibernetinių nusikaltimų, kurių įvertinta ekonominė vertė Sąjungoje siekia 0,41 % ES BVP (t. y. apie 55 mlrd. EUR), keliamas išlaidas.

Konkretūs rezultatai:

Didesni valstybių narių ir įmonių kibernetinio saugumo srities pajėgumai bei pasirengimas

- Didesni valstybių narių ir įmonių kibernetinio saugumo srities pajėgumai bei pasirengimas (dėl kibernetinių grėsmių ir incidentų ilgalaikės strateginės analizės, rekomendacijų ir ataskaitų, praktinių žinių ir gerosios patirties sklaidos, mokymų ir mokymo medžiagos prieinamumo, sustiprintų *CyberEurope* pratybų).

- Didesni privačių subjektų pajėgumai dėl įvairiuose sektoriuose sukurtų keitimosi informacija ir jos analizės centrų teikiamos paramos.

- Geresnis ES ir valstybių narių kibernetinio saugumo srities pasirengimas dėl gerai išbandytų ir sutartų planų reaguojant į didelius tarpvalstybinius kibernetinius incidentus, išbandytus per *CyberEurope* pratybas.

[45] Kibernetinio saugumo užtikrinimo skaidrumas reiškia, kad vartotojams suteikiama pakankamai informacijos apie kibernetinio saugumo savybes, ir tokiu būdu vartotojai gali objektyviai nustatyti atitinkamo IRT produkto, paslaugos ar proceso saugumo lygį.

Pagerintas valstybių narių ir ES institucijų, agentūrų bei įstaigų bendradarbiavimas ir koordinavimas

- Pagerintas bendradarbiavimas viešajame sektoriuje ir tarp viešojo ir privačiojo sektorių.

- Nuoseklesnis požiūris į TIS direktyvos įgyvendinimą tarpvalstybiniu mastu ir įvairiuose sektoriuose.

- Sustiprintas bendradarbiavimas sertifikavimo srityje dėl institucinės sistemos, kuria sudaromos sąlygos kurti Europos kibernetinio saugumo sertifikavimo schemas ir bendrą šios srities politiką.

Didesni ES lygmens pajėgumai, papildantys valstybių narių veiksmus

- Didesni ES operatyviniai pajėgumai, papildantys valstybių narių veiksmus ir sudarantys sąlygas valstybių narių prašymu teikti joms ribotos apimties ir iš anksto apibrėžtą paramą. Tai turėtų turėti teigiamos įtakos incidentų prevencijai, aptikimui ir reagavimui į juos tiek valstybių narių, tiek Sąjungos lygmeniu.

Didesnis piliečių ir įmonių informuotumas kibernetinio saugumo klausimais

- Didesnis bendras piliečių ir įmonių informuotumas kibernetinio saugumo klausimais.

- Dėl kibernetinio saugumo sertifikavimo daugiau galimybių priimti informacija pagrįstus IRT produktų ir paslaugų pirkimo sprendimus.

Didesnis pasitikėjimas bendrąja skaitmenine rinka ir skaitmeninėmis inovacijomis dėl didesnio IRT produktų ir paslaugų kibernetinio saugumo užtikrinimo skaidrumo

- Didesnis IRT produktų ir paslaugų kibernetinio saugumo užtikrinimo skaidrumas[46] dėl saugumo sertifikavimo procedūrų ES lygmens sistemoje supaprastinimo.

- Didesnis IRT produktų ir paslaugų saugumo savybių užtikrinimo lygis.

- Plačiau naudojamas saugumo sertifikavimas, kurį skatina supaprastintos procedūros, mažesnės išlaidos ir rinkos susiskaidymo nevaržomų ES masto verslo galimybių potencialas

- Didesnis konkurencingumas ES kibernetinio saugumo rinkoje dėl mažesnių sąnaudų ir administracinės naštos MVĮ, taip pat išvengiant galimų patekimo į rinką kliūčių, atsirandančių dėl įvairių nacionalinių sertifikavimo sistemų.

Kita

- Nė vienas iš tikslų neturėtų daryti didelio poveikio aplinkai.

- Kiek tai susiję su ES biudžetu, tikėtinas efektyvumo padidėjimas dėl didesnio bendradarbiavimo ir veiklos koordinavimo tarp ES institucijų, agentūrų ir įstaigų.

1.4.4. Rezultatų ir poveikio rodikliai

Nurodyti pasiūlymo (iniciatyvos) įgyvendinimo stebėjimo rodiklius.

(g)

[46] Kibernetinio saugumo užtikrinimo skaidrumas reiškia, kad vartotojams suteikiama pakankamai informacijos apie kibernetinio saugumo savybes, ir tokiu būdu vartotojai gali objektyviai nustatyti atitinkamo IRT produkto, paslaugos ar proceso saugumo lygį.

Tikslas – didinti valstybių narių ir įmonių pajėgumus bei pasirengimą:

- ENISA organizuojamų mokymų skaičius
- ENISA teikiamos tiesioginės paramos geografinė aprėptis (šalių ir teritorijų skaičius)
- Valstybių narių pasiektas pasirengimo lygis CSIRT brandos ir su kibernetiniu saugumu susijusių reguliavimo priemonių priežiūros atžvilgiu
- ES mastu taikomos gerosios patirties, susijusios su ENISA teikiama ypatingos svarbos infrastruktūros objektų apsauga, atvejų skaičius
- ES mastu taikomos gerosios patirties, susijusios su MVĮ, atvejų skaičius
- ENISA paskelbta metinė strateginė kibernetinių grėsmių ir incidentų analizė siekiant nustatyti atsirandančias tendencijas
- Reguliarus ENISA įnašas į Europos standartizacijos organizacijų kibernetinio saugumo darbo grupių darbą.

Tikslas – gerinti valstybių narių ir ES institucijų, agentūrų bei įstaigų bendradarbiavimą ir koordinavimą:

- valstybių narių, kurios formuodamos politiką pasinaudojo ENISA rekomendacijomis ir nuomonėmis, skaičius
- ES institucijų, agentūrų ir įstaigų, kurios formuodamos politiką pasinaudojo ENISA rekomendacijomis ir nuomonėmis, skaičius
- Reguliarus CSIRT tinklo darbo programos įgyvendinimas ir gerai veikianti CSIRT tinklo IT infrastruktūra ir ryšių kanalai
- Bendradarbiavimo grupei suteiktų ir jos pasinaudotų techninių ataskaitų skaičius
- Nuoseklus TIS direktyvos įgyvendinimas tarpvalstybiniu lygmeniu ir skirtinguose sektoriuose
- ENISA vykdomų reglamentavimo atitikties vertinimų skaičius
- Įvairiuose sektoriuose, visų pirma susijusiuose su ypatingos svarbos infrastruktūros objektais, veikiančių ISACS skaičius
- Informacinės platformos, skleidžiančios iš ES institucijų, agentūrų ir įstaigų gautą informaciją apie kibernetinį saugumą, sukūrimas ir nuolatinis administravimas
- Reguliari pagalba rengiant ES mokslinių tyrimų ir inovacijų darbo programas
- ENISA, EC3 ir CERT-EU sudarytas bendradarbiavimo susitarimas
- Į sistemą įtrauktų ir parengtų sertifikavimo sistemų skaičius

Tikslas – didinti ES lygmens pajėgumus papildant valstybių narių veiksmus, ypač tarpvalstybinių kibernetinių krizių atveju:

- ENISA paskelbta metinė strateginė kibernetinių grėsmių ir incidentų analizė siekiant nustatyti atsirandančias tendencijas
- ENISA paskelbta apibendrinta informacija apie incidentus, apie kuriuos pranešama pagal TIS direktyvą
- Agentūros koordinuojamų Europos masto pratybų skaičius ir jose dalyvaujančių valstybių narių ir organizacijų skaičius

- Valstybių narių ENISA pateiktų prašymų padėti reaguoti į incidentus ir Agentūros priimtų prašymu skaičius
- Bendradarbiaujant su CERT-EU ENISA įvykdytų pažeidžiamumo, artefaktų ir incidentų analizės skaičius
- Parengtos ES masto padėties ataskaitos, pagrįstos valstybių narių ir kitų subjektų ENISA pateikta informacija didelio masto tarpvalstybinio kibernetinio incidento atveju.

Tikslas – didinti piliečių ir įmonių informuotumą kibernetinio saugumo klausimais

- Reguliariai organizuojamos visos ES ir nacionalinės informuotumo didinimo kampanijos ir nuolat atnaujinamos temos pagal atsirandančius mokymosi poreikius
- ES piliečių kibernetinio informuotumo didinimas
- Reguliariai organizuojama informuotumo apie kibernetinį saugumą viktorina ir su laiku didėjanti teisingų atsakymų dalis
- Reguliariai publikuojama darbuotojams ir organizacijoms skirta kibernetinio saugumo ir kibernetinės higienos geroji patirtis

Tikslas – pasitikėjimo bendrąja skaitmenine rinka ir skaitmeninėmis inovacijomis stiprinimas didinant bendrą IRT produktų ir paslaugų kibernetinio saugumo užtikrinimo skaidrumą[47]

- ES sistemai priklausančių schemų skaičius
- Mažesnės išlaidos gauti IRT saugumo sertifikatą
- IRT sertifikavimo srityje besispecializuojančių atitikties vertinimo įstaigų skaičius valstybėse narėse
- Europos kibernetinio saugumo sertifikavimo grupės sukūrimas ir reguliarus posėdžių rengimas
- Sertifikavimo gairės pagal galiojančią ES sistemą
- Reguliariai skelbiamos pagrindinių ES kibernetinio saugumo rinkos tendencijų analizės
- Pagal europinės IRT saugumo sertifikavimo sistemos taisykles sertifikuotų IRT produktų ir paslaugų skaičius
- Daugiau galutinių paslaugų gavėjų, žinančių apie IRT produktų ir paslaugų saugumo savybes

(h)

1.4.5. Trumpalaikiai arba ilgalaikiai poreikiai

Atsižvelgiant į reguliavimo reikalavimus ir sparčiai kintančias kibernetines grėsmes reikia peržiūrėti ENISA įgaliojimus, kad būtų atnaujintos užduotys ir funkcijos ir kad ji veiksmingai ir efektyviai galėtų remti valstybių narių, ES institucijų ir kitų suinteresuotųjų subjektų pastangas Europos Sąjungoje užtikrinti saugią kibernetinę erdvę. Apibrėžta siūloma įgaliojimų apimtis, sustiprinant tas sritis, kuriose Agentūra aiškiai įrodė savo

[47] Kibernetinio saugumo užtikrinimo skaidrumas reiškia, kad vartotojams suteikiama pakankamai informacijos apie kibernetinio saugumo savybes, ir tokiu būdu vartotojai gali objektyviai nustatyti atitinkamo IRT produkto, paslaugos ar proceso saugumo lygį.

papildomą naudą, ir įtraukiant tokias naujas sritis, kuriose reikalinga parama dėl naujų politikos prioritetų ir priemonių, ypač TIS direktyvos, ES kibernetinio saugumo strategijos peržiūros, ES kibernetinio saugumo projekto, skirto bendradarbiavimui kibernetinių krizių klausimais, ir IRT saugumo sertifikavimo. Naujaisiais siūlomais įgaliojimais siekiama suteikti Agentūrai svaresnį ir reikšmingesnį vaidmenį, visų pirma, kad ji padėtų valstybėms narėms aktyviau atremti konkrečias grėsmes (operatyviniai pajėgumai) ir taptų kompetencijos centru, padėsiančiu valstybėms narėms ir Komisijai kibernetinio saugumo sertifikavimo srityje.

Kartu pasiūlymu nustatoma IRT produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo sistema ir apibrėžiamos esminės ENISA funkcijos ir užduotys kibernetinio saugumo sertifikavimo srityje. Sistemoje nustatomos bendrosios nuostatos ir procedūros, sudarančios sąlygas sukurti ES masto kibernetinio saugumo sertifikavimo schemas, taikomas konkretiems IRT produktams ir (arba) paslaugoms ar kibernetinio saugumo rizikai. Pagal sistemą sukūrus Europos kibernetinio saugumo sertifikavimo schemas bus galima tvirtinti pagal tas schemas išduotus sertifikatus ir juos pripažinti visose valstybėse narėse bei išspręsti dabartinę rinkos susiskaidymo problemą.

1.4.6. Papildoma Sąjungos dalyvavimo nauda

Kibernetinis saugumas yra pasaulinio masto klausimas, kuris savo esme yra tarpvalstybinis ir vis labiau tampa tarpsektorinis dėl tinklų ir informacinių sistemų tarpusavio priklausomybės. Kibernetinio saugumo incidentų ilgainiui daugėja, jie sudėtingėja, jų mastas ir poveikis ekonomikai ir visuomenei didėja; numatoma, kad vykstant technologijų plėtrai, pvz., įsigalint daiktų internetui, jų daugės. Tai reiškia, kad bendros valstybių narių, ES institucijų ir privačiojo sektoriaus suinteresuotųjų subjektų pastangos atremti kibernetiniam saugumo grėsmes ateityje neturėtų mažėti.

Nuo pat įsteigimo 2004 m. ENISA siekė stiprinti valstybių narių ir TIS suinteresuotųjų subjektų bendradarbiavimą, be kita ko, remdama viešojo ir privačiojo sektorių bendradarbiavimą. Remiant bendradarbiavimą vykdytas techninio pobūdžio darbas siekiant suteikti ES lygmens grėsmių padėties vaizdą, sukurtos ekspertų grupės ir organizuotos viešajam ir privačiajam sektoriams skirtos visos Europos kibernetinių incidentų ir krizių valdymo pratybos (visų pirma „Cyber Europe“). TIS direktyva ENISA buvo suteikti įgaliojimai vykdyti papildomas užduotis, be kita ko CSIRT tinklui teikti sekretoriato paslaugas, susijusias su valstybių narių operatyviniu bendradarbiavimu.

2016 m. Tarybos išvadose[48] buvo pripažinta pridėtinė ES lygmens veiksmų vertė, visų pirma stiprinant bendradarbiavimą tarp valstybių narių bei tarp TIS bendruomenių, o iš 2017 m. ENISA vertinimo taip pat aiškiai matyti, kad Agentūros pridėtinė vertė visų pirma glūdi jo gebėjime didinti šių suinteresuotųjų subjektų bendradarbiavimą. Nėra jokio kito ES lygmens subjekto, kuris remtų tokios įvairovės suinteresuotųjų subjektų bendradarbiavimą TIS klausimais.

ENISA teikiama pridėtinė vertė, susijusi su kibernetinio saugumo bendruomenių ir suinteresuotųjų subjektų sutelkimu, taip pat yra jos teikiama ir sertifikavimo srityje. Dėl padažnėjusių elektroninių nusikaltimų ir padidėjusių saugumo grėsmių atsirado nacionalinių iniciatyvų, kuriomis siekiama nustatyti aukšto lygio kibernetinio saugumo ir sertifikavimo reikalavimus tradicinėje infrastruktūroje naudojamiems IRT komponentams. Nors šios iniciatyvos yra svarbios, dėl jų kyla bendrosios rinkos

[48] Tarybos išvados dėl Europos kibernetinio atsparumo sistemos stiprinimo ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimo. 2016 m. lapkričio 15 d.

susiskaidymo rizika ir atsiranda kliūčių sąveikai. IRT pardavėjui gali tekti atlikti kelis sertifikavimo procesus, kad galėtų prekiauti keliose valstybėse narėse. Mažai tikėtina, kad dabartinių sertifikavimo schemų neveiksmingumo ir (arba) neefektyvumo problema būtų išspręsta, jei ES nesiims veiksmų. Labai tikėtina, kad nesiimant veiksmų rinkos susiskaidymas atsirandant naujoms sertifikavimo schemoms trumpuoju ar vidutiniu laikotarpiu (per ateinančius 5–10 metus) padidėtų. Nepakankamas tokių schemų koordinavimas ir sąveika yra tai, kas mažina bendrosios skaitmeninės rinkos potencialą. Tai įrodo pridėtinę IRT produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo sistemos sukūrimo vertę, nes ja būtų sudarytos reikiamos sąlygos veiksmingai spręsti problemą, susijusią su daugelio sertifikavimo procedūrų įvairiose valstybėse narėse koegzistavimu, ir taip sumažinti sertifikavimo išlaidas ir komerciniu bei konkurenciniu požiūriu ES sertifikavimą padaryti patrauklesnį.

1.4.7. Panašios patirties išvados

Pagal ENISA teisinį pagrindą Komisija atliko Agentūros vertinimą, į kurį įtrauktas nepriklausomas tyrimas ir viešos konsultacijos. Vertinime padaryta išvada, kad ENISA tikslai šiandien tebėra aktualūs. Atsižvelgiant į technologijų raidą ir kintančias grėsmes bei didelį poreikį ES didinti tinklų ir informacijos saugumą (TIS), reikalingos techninės ekspertinės žinios tinklų ir informacijos saugumo pokyčių klausimais. Valstybės narės turi stiprinti pajėgumus, kad galėtų suprasti grėsmes ir į jas reaguoti, o suinteresuotieji subjektai turi bendradarbiauti įvairiose teminėse srityse ir institucijose.

Agentūra sėkmingai prisidėjo prie tinklų ir informacijos saugumo Europoje didinimo siūlydama pajėgumą didinančias priemones 28 valstybėse narėse bei stiprindama bendradarbiavimą tarp valstybių narių ir TIS suinteresuotųjų subjektų, teikdama ekspertine žinias ir įgyvendindama bendruomenės stiprinimo ir politikos rėmimo priemones.

Nors ENISA sugebėjo padaryti nors šiokį tokį poveikį plataus masto TIS saugumo srityje, jai ne visiškai pavyko sukurti patikimą prekės ženklą ir tapti pakankamai matomai, kad būtų pripažinta kaip kompetencijos centras Europoje. Tai galima paaiškinti plataus masto ENISA įgaliojimais, kuriems vykdyti nebuvo skirta proporcingai didelių išteklių. Be to, ENISA lieka vienintele ES agentūra, kuriai suteiktas terminuotas įgaliojimas – tai riboja jos gebėjimą parengti ilgalaikę viziją ir tvariai remti suinteresuotuosius subjektus. Tai taip pat prieštarauja TIS direktyvos nuostatoms, pagal kurias ENISA pavedamos užduotys be galutinio termino.

Kalbant apie IRT produktų ir paslaugų kibernetinio saugumo sertifikavimą šiuo metu nėra jokios Europos sistemos. Tačiau dėl padažnėjusių elektroninių nusikaltimų ir padidėjusių saugumo grėsmių atsirado nacionalinių iniciatyvų, keliančių bendrosios rinkos susiskaidymo riziką.

1.4.8. Suderinamumas ir galima sąveika su kitomis atitinkamomis priemonėmis

Ši iniciatyva visiškai dera su esama politika, visų pirma vidaus rinkos srities politika. Iš tiesų ji parengta laikantis bendro požiūrio į kibernetinį saugumą, kaip apibrėžta bendrosios skaitmeninės rinkos strategijos peržiūroje, siekiant papildyti išsamų rinkinį priemonių, kaip antai, ES kibernetinio saugumo strategiją, bendradarbiavimo kibernetinių krizių klausimais projektą ir iniciatyvas, skirtas kovoti su kibernetiniais nusikaltimais. Taip būtų užtikrintas derėjimas su esamų kibernetinio saugumo srities teisės aktų, visų pirma TIS direktyvos, nuostatomis, siekiant toliau didinti ES kibernetinį atsparumą stiprinant pajėgumus, bendradarbiavimą, rizikos valdymą ir didinant kibernetinį informuotumą.

Siūlomomis sertifikavimo priemonėmis turėtų būti sprendžiama galimo susiskaidymo dėl esamų ir kuriamų nacionalinių sertifikavimo schemų problema, taip prisidedant prie bendrosios skaitmeninės rinkos vystymo. Iniciatyva taip pat remiamas ir papildomas TIS direktyvos įgyvendinimas, pagal direktyvą suteikiant įmonėms priemonę įrodyti atitiktį TIS reikalavimams visoje Sąjungoje.

Pasiūlyta Europos IRT saugumo sertifikavimo sistema nedaro poveikio Bendrajam duomenų apsaugos reglamentui[49] ir visų pirma atitinkamoms sertifikavimo nuostatoms[50], taikomoms asmens duomenų tvarkymo saugumui. Galiausiai, pagal Europos sistemą ateityje pasiūlytos schemos turėtų kuo labiau remtis tarptautiniais standartais siekiant išvengti prekybos kliūčių sukūrimo ir užtikrinti derėjimą su kitomis tarptautinėmis iniciatyvomis.

[49] 2016 m. balandžio 27 d. Reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).

[50] Pavyzdžiui, 42 straipsnis (sertifikavimas) ir 43 straipsnis (sertifikavimo įstaigos), taip pat 57, 58 ir 70 straipsniai dėl atitinkamų nepriklausomų priežiūros institucijų užduočių bei galių ir Europos duomenų apsaugos valdybos užduočių.

1.5. Trukmė ir finansinis poveikis

☐ Pasiūlymo (iniciatyvos) **trukmė ribota**

– ☐ Pasiūlymas (iniciatyva) galioja nuo MMMM [MM DD] iki MMMM [MM DD]

– ☐ finansinis poveikis nuo MMMM iki MMMM

☒ Pasiūlymo (iniciatyvos) **trukmė neribota**

– įgyvendinimo pradinis laikotarpis – nuo 2019 iki 2020 m.;

– vėliau – visuotinis taikymas.

1.6. Numatytas (-i) valdymo būdas (-ai)[51]

☒ **Tiesioginis valdymas,** vykdomas Komisijos (III antraštinė dalis – Sertifikavimas)

– ☐ vykdomųjų įstaigų

☐ **Pasidalijamasis valdymas** kartu su valstybėmis narėmis

☒ **Netiesioginis valdymas**, biudžeto vykdymo užduotis perduodant:

☐ tarptautinėms organizacijoms ir jų agentūroms (nurodyti);

☐ EIB ir Europos investicijų fondui;

☒ įstaigoms, nurodytoms 208 ir 209 straipsniuose (II antraštinė dalis – ENISA);

☐ viešosios teisės įstaigoms;

☐ įstaigoms, kurių veiklą reglamentuoja privatinė teisė, veikiančioms viešųjų paslaugų srityje, jeigu jos pateikia pakankamų finansinių garantijų;

☐ įstaigoms, kurių veiklą reglamentuoja valstybės narės privatinė teisė, kurioms pavesta įgyvendinti viešojo ir privačiojo sektorių partnerystę ir kurios pateikia pakankamų finansinių garantijų;

☐ asmenims, kuriems pavestas konkrečių BUSP veiksmų vykdymas pagal ES sutarties V antraštinę dalį ir kurie nurodyti atitinkamame pagrindiniame teisės akte.

Pastabos

Šio reglamento taikymo sritis: - Siūlomo reglamento II antraštinėje dalyje peržiūrimas Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA) įgaliojimas, jai suteikiant svarbų su sertifikavimu susijusį vaidmenį, o - III antraštinėje dalyje nustatomas IRT produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo schemų sukūrimo pagrindas, kuriame ENISA atlieka itin svarbų vaidmenį.

[51] Informacija apie valdymo būdus ir nuorodos į Finansinį reglamentą pateikiamos svetainėje „BudgWeb“: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir atskaitomybės taisyklės

Nurodyti dažnumą ir sąlygas.

Stebėsena bus pradedama vykdyti iš karto priėmus teisinę priemonę ir daugiausia dėmesio bus skiriama tos priemonės taikymui. Komisija surengs susitikimus su ENISA, valstybių narių atstovais (pvz., ekspertų grupe) ir su susijusiais suinteresuotaisiais subjektais, visų pirma siekdama padėti lengviau įgyvendinti su sertifikavimu susijusias taisykles, pvz., dėl valdybos įsteigimo.

Pirmas vertinimas turėtų būti atliekamas praėjus 5 metams nuo teisinės priemonės įsigaliojimo, su sąlyga, kad yra pakankamai duomenų. Teisinė priemonė apima išsamaus vertinimo ir peržiūros išlygą [XXX str.], kuria remdamasi Komisija atliks nepriklausomą vertinimą. Komisija vėliau pateiks ataskaitą Europos Parlamentui ir Tarybai dėl atlikto vertinimo, su kuriuo prireikus bus pateiktas pasiūlymas jį peržiūrėti, kad būtų galima įvertinti Reglamento ir papildomos jo vertės poveikį. Tolesni vertinimai turėtų būti atliekami kas penkerius metus. Bus taikoma Komisijos geresnio reglamentavimo metodika. Šiuos vertinimus atlikti padės tikslinės diskusijos su ekspertais, tyrimai ir plataus masto konsultacijos su suinteresuotaisiais subjektais.

ENISA vykdomasis direktorius kas dvejus metus turėtų pateikti Valdančiajai tarybai ENISA veiklos *ex post* vertinimą. Agentūra taip pat turėtų parengti tolesnių veiksmų planą dėl retrospektyvių įvertinimų išvadų ir kas dvejus metus teikti Komisijai ataskaitą apie pažangą. Valdančioji taryba turėtų būti atsakinga už tai, kad dėl tokių išvadų būtų imamasi tinkamų tolesnių veiksmų.

Dėl įtariamų netinkamo administravimo atvejų Agentūros veikloje Europos ombudsmenas gali atlikti tyrimus pagal Sutarties 228 straipsnio nuostatas.

Numatytos stebėsenos duomenų šaltiniai daugiausia bus ENISA, Europos kibernetinio saugumo sertifikavimo grupė, Bendradarbiavimo grupė, CSIRT tinklas ir valstybių narių institucijos. Be duomenų, kurie bus gaunami iš ENISA, Europos kibernetinio saugumo sertifikavimo grupės, Bendradarbiavimo grupės ir CSIRT tinklo ataskaitų (įskaitant metines veiklos ataskaitas), prireikus bus naudojamos specialios duomenų rinkimo priemonės (pavyzdžiui, nacionalinėms institucijoms skirti tyrimai, „Eurobarometro“ apklausa ir Kibernetinio mėnesio kampanijos bei visos Europos pratybų ataskaitos).

2.2. Valdymo ir kontrolės sistema

2.2.1. Nustatyta rizika

Nustatyta rizika yra ribota: Sąjungos agentūra jau egzistuoja ir bus apibrėžti jos įgaliojimai, sustiprinant tas sritis, kuriose Agentūra aiškiai įrodė savo papildomą naudą, ir įtraukiant tokias naujas sritis, kuriose reikalinga parama dėl naujų politikos prioritetų ir priemonių, ypač TIS direktyvos, ES kibernetinio saugumo strategijos peržiūros, būsimo ES kibernetinio saugumo projekto, skirto bendradarbiavimui kibernetinių krizių klausimais, ir IRT saugumo sertifikavimo.

Todėl pasiūlyme išsamiai nurodomos Agentūros funkcijos ir didesnis veiksmingumas. Didesni operatyviniai gebėjimai ir daugiau užduočių nesudaro realios rizikos, nes jie papildytų valstybių narių veiksmus ir paprašius bei atsižvelgiant į ribotas ir iš anksto nustatytas paslaugas, joms būtų teikiama parama.

Be to, siūlomu Agentūros modeliu, atitinkančiu bendrą požiūrį, užtikrinama, kad bus pakankamai kontroliuojama, kad būtų įsitikinta, jog ENISA siekia savo tikslų. Atrodo, kad siūlomų pokyčių veiklos ir finansinė rizika yra ribota.

Kartu būtina užtikrinti tinkamus finansinius išteklius, kad ENISA įvykdytų pagal naujus įgaliojimus pavestas užduotis, įskaitant sertifikavimo sritį.

2.2.2. Numatomas (-i) kontrolės metodas (-ai)

Agentūros finansinės ataskaitos bus pateiktos tvirtinti Audito Rūmams ir joms bus taikoma biudžeto įvykdymo patvirtinimo procedūra ir numatomi auditai.

Be to, Agentūros veiklą pagal Sutarties 228 straipsnio nuostatas prižiūri ombudsmenas.

Taip pat žr. ankstesnius 2.1 ir 2.2.1 punktus.

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

Nurodyti dabartines arba numatytas prevencijos ir apsaugos priemones.

ENISA prevencijos ir apsaugos priemonės visų pirma būtų taikomos taip:

- Agentūros darbuotojai tikrina prašomus mokėjimus už bet kokią paslaugą arba tyrimus prieš atlikdami tuos mokėjimus, atsižvelgdami į visus sutartinius įsipareigojimus, ekonominius principus ir gerą finansinę arba valdymo praktiką. Nuostatos dėl kovos su sukčiavimu (priežiūra, atskaitomybės reikalavimai ir kt.) bus įtrauktos į visus Agentūros ir mokėjimų gavėjų sudarytus susitarimus ir sutartis.

- Siekiant kovoti su sukčiavimu, korupcija ir kita neteisėta veikla, be apribojimų taikomos 2013 m. rugsėjo 11 d. Europos Parlamento ir Tarybos reglamento (ES, Euratomas) Nr. 883/2013 dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų tyrimų nuostatos.

- Agentūra per šešis mėnesius nuo šio reglamento įsigaliojimo dienos prisijungia prie 1999 m. gegužės 25 d. Europos Parlamento, Europos Sąjungos Tarybos ir Europos Bendrijų Komisijos tarpinstitucinio susitarimo dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų vidaus tyrimų ir nedelsdama priima atitinkamas visiems Agentūros darbuotojams taikytinas nuostatas.

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Atitinkama (-os) daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės)

- Dabartinės biudžeto eilutės

Daugiametės finansinės programos išlaidų kategorijas ir biudžeto eilutes nurodyti eilės tvarka.

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
		DA / NDA[52]	ELPA šalių[53]	šalių kandidačių[54]	trečiųjų šalių	pagal Finansinio reglamento 21 straipsnio 2 dalies b punktą
1a Konkurencingumas augimui ir užimtumui skatinti	09.0203 ENISA ir informacinių ir ryšių technologijų saugumo sertifikavimas	DA	TAIP	NE	NE	NE
5 Administracinės išlaidos	09.0101 Išlaidos Ryšių tinklų, turinio ir technologijų srityje dirbančiam personalui 09.0102 Išlaidos Ryšių tinklų, turinio ir technologijų srityje dirbančiam išorės personalui 09.010211 Kitos valdymo išlaidos	NDA	NE	NE	NE	NE

[52] DA – diferencijuotieji asignavimai, NDA – nediferencijuotieji asignavimai.

[53] ELPA – Europos laisvosios prekybos asociacija.

[54] Šalių kandidačių ir, kai taikoma, Vakarų Balkanų potencialių šalių kandidačių.

3.2. Numatomas poveikis išlaidoms

3.2.1. Numatomo poveikio išlaidoms santrauka

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos išlaidų kategorija	1a	Konkurencingumas augimui ir užimtumui skatinti

ENISA			**Atskaitos scenarijus** **2017 m. (2016 12 31)**		**2019 m.** ***(nuo 2019 07 01)***	**2020 m.**	**2021 m.**	**2022 m.**	**IŠ VISO**
1 antraštinė dalis. Personalo išlaidos *(taip pat įskaitant išlaidas, susijusias su darbuotojų įdarbinimu, mokymais, socialine ir sveikatos apsaugos infrastruktūra bei išorės paslaugomis)*	Įsipareigojimai	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Mokėjimai	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
2 antraštinė dalis. Infrastruktūra ir veiklos išlaidos	Įsipareigojimai	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Mokėjimai	(2 a)	1,770		1,957	2,232	2,461	2,565	**9,215**
3 antraštinė dalis. Veiklos išlaidos	Įsipareigojimai	(3 a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Mokėjimai	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
IŠ VISO ENISA asignavimų	Įsipareigojimai	= 1 + 1a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Mokėjimai	= 2 + 2a + 3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Daugiametės finansinės programos išlaidų kategorija	**5**	Administracinės išlaidos

mln. EUR (tūkstantųjų tikslumu)

		2019 m. *(nuo 2019 07 01)*	**2020 m.**	**2021 m.**	**2022 m.**	**IŠ VISO**
CNECT GD						
•Žmogiškieji ištekliai		0,216	0,846	0,846	0,846	**2,754**
•Kitos administracinės išlaidos		0,102	0,235	0,238	0,242	**0,817**
IŠ VISO CNECT **GD**	Asignavimai	0,318	1,081	1,084	1,088	**3,571**

Darbuotojų išlaidos apskaičiuotos pagal planuojamo įdarbinimo datą (įdarbinti numatyta nuo 2019 07 01).

Išteklių perspektyva po 2020 m. yra orientacinė ir neturi poveikio Komisijos pasiūlymams dėl daugiametės finansinės programos po 2020 m.

IŠ VISO pagal daugiametės finansinės programos 5 IŠLAIDŲ KATEGORIJĄ	(Iš viso įsipareigojimų = Iš viso mokėjimų)	0,318	1,081	1,084	1,088	**3,571**

mln. EUR (tūkstantųjų tikslumu)

		2019 m.	**2020 m.**	**2021 m.**	**2022 m.**	**IŠ VISO**
IŠ VISO asignavimų pagal daugiametės finansinės programos 1–5 IŠLAIDŲ KATEGORIJAS	Įsipareigojimai	16,868	21,727	23,332	24,11	**86,038**
	Mokėjimai	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Numatomas poveikis Agentūros asignavimams

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai nenaudojami

– ☒ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai naudojami taip:

Įsipareigojimų asignavimai mln. EUR (tūkstantųjų tikslumu)

Nurodyti tikslus ir rezultatus[55] ⇩	**2019 m.**	**2020 m.**	**2021 m.**	**2022 m.**	**IŠ VISO**
Didinti valstybių narių ir įmonių pajėgumus bei pasirengimą.	1,408	1,900	1,931	1,969	7,208
Gerinti valstybių narių ir ES institucijų, agentūrų bei įstaigų bendradarbiavimą ir koordinavimą.	0,939	1,266	1,288	1,313	4,806
Didinti ES lygmens pajėgumus, siekiant papildyti valstybių narių veiksmus, ypač tarpvalstybinių kibernetinių krizių atveju.	0,704	0,950	0,965	0,985	3,604
Didinti piliečių ir įmonių informuotumą kibernetinio saugumo klausimais.	0,704	0,950	0,965	0,985	3,604
Stiprinti pasitikėjimą bendrąja skaitmenine rinka ir skaitmeninėmis inovacijomis, didinant bendrą IRT produktų ir paslaugų kibernetinio saugumo užtikrinimo skaidrumą.	0,939	1,266	1,288	1,313	4,806
IŠ VISO IŠLAIDŲ	4.694	6,332	6,437	6,565	24,028

[55] Šioje lentelėje pateikiamos tik veiklos išlaidos pagal 3 antraštinę dalį.

3.2.3. Numatomas poveikis Agentūros žmogiškiesiems ištekliams

3.2.3.1. Santrauka

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimų nenaudojama

– ☒ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

	2019 m. 3–4 ketv.	**2020 m.**	**2021 m.**	**2022 m.**
Laikinieji pareigūnai (AD lygio)	4,242	5,695	6,381	6,709
Laikinieji pareigūnai (AST lygio)	1,601	1,998	2,217	2,217
Sutartininkai	2,041	2,041	2,041	2,041
Deleguotieji nacionaliniai ekspertai	0,306	0,447	0,656	0,796
IŠ VISO	**8,190**	**10,181**	**11,295**	**11,763**

Darbuotojų išlaidos apskaičiuotos pagal planuojamo įdarbinimo datą (visiškai įdarbinti dabartinius ENISA darbuotojus buvo numatyta nuo 2019 01 01). Naujus darbuotojus buvo numatyta laipsniškai įdarbinti nuo 2019 07 01, o visišką įdarbinimą užtikrinti 2022 m. Išteklių perspektyva po 2020 m. yra orientacinė ir neturi poveikio Komisijos pasiūlymams dėl daugiametės finansinės programos po 2020 m.

Numatomas poveikis darbuotojams (papildomi etato ekvivalentai). Etatų planas

Pareigų grupė ir lygis	2017 m. **Dabart. ENISA**	2019 m. 3–4 ketv.	2020 m.	2021 m.	2022 m.
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					
Iš viso AD	34	9	8	6	3

AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Iš viso AST	14	3	2	1	
AST / SC 6 AST / SC 5 AST / SC 4 AST / SC 3 AST / SC 2 AST / SC 1					
Iš viso AST / SC					
BENDRA SUMA	48	12	10	7	3

Užduotys papildomiems AD / AST darbuotojams, norint pasiekti priemonės tikslus, kaip aprašyta 1.4.2 skirsnyje:

Užduotys	AD	AST	SNE	Iš viso
Politikos ir pajėgumų stiprinimas	8	1		9
Operatyvinis bendradarbiavimas	8	1	7	16
Sertifikavimas (su rinka susijusios užduotys)	9	3	2	14
Žinios, informavimas ir informuotumas	1	1		2
IŠ VISO	26	6	9	41

Vykdytinų užduočių aprašymas:

Užduotys	**Reikiami papildomi ištekliai**
ES politikos formavimas ir įgyvendinimas bei pajėgumų stiprinimas	Užduotys apimtų pagalbą Bendradarbiavimo grupei, pagalbą, siekiant nuosekliai įgyvendinti TIS tarpvalstybiniu mastu, nuolatinį ataskaitų apie ES teisinės sistemos įgyvendinimo padėtį teikimą; konsultacijų teikimą ir sektoriaus kibernetinio saugumo iniciatyvų koordinavimą, įskaitant energetikos, transporto (pvz., aviacijos / kelių / jūrų / susietosios transporto priemonės), sveikatos priežiūros, finansų sritis; pagalbą įvairiuose sektoriuose kuriant keitimosi

	informacija ir jos analizės centrus (ISAC).
Operatyvinis bendradarbiavimas ir krizių valdymas	**Užduotys:** Vykdyti CSIRT tinklo sekretoriato funkciją, be kitų dalykų, užtikrinant gerą CSIRT tinklo IT infrastruktūros ir ryšių kanalų veikimą. Užtikrinti struktūrinį bendradarbiavimą su CERT-EU, EC3 ir kitomis susijusiomis ES įstaigomis. Organizuoti **Europos kibernetinio saugumo pratybas („Cyber Europe“)**[56] – užduotys susijusios su pratybų masto išplėtimu (nuo kas du metus iki kasmet organizuojamo renginio), taip pat siekiama užtikrinti, kad pratybose incidentas būtų nagrinėjamas nuo pradžios iki pabaigos. **Techninė pagalba**. Užduotys apimtų struktūrinį bendradarbiavimą su CERT-EU, siekiant teikti techninę pagalbą įvykus dideliems incidentams ir padėti jį išanalizuoti. Tai taip pat apimtų pagalbos valstybėms narėms teikimą, siekiant suvaldyti incidentus ir išanalizuoti pažeidžiamumą, artefaktus ir incidentus. Analizuojant ir kaupiant nacionalines padėties ataskaitas, remiantis informacija, kurią pateikė valstybės narės ir kiti subjektai, atskiroms valstybėms narėms būtų sudarytos palankesnės sąlygos bendradarbiauti reaguojant į incidentus. **Koordinuoto atsako į didelio masto tarpvalstybinius kibernetinio saugumo incidentus projektas**. Agentūra padės parengti koordinuotą atsaką į didelio masto tarpvalstybinius incidentus arba krizes, susijusius su kibernetiniu saugumu, atlikdama keletą užduočių, pradedant pagalba užtikrinti informuotumą apie padėtį Sąjungos ir valstybių narių lygmeniu ir baigiant bendradarbiavimo reaguojant į incidentus planų testavimu. ***Ex post* techniniai incidentų tyrimai**. Siekiant pateikti rekomendacijas ir sustiprinti pajėgumus viešųjų ataskaitų forma, kad būtų geriau užkirstas kelias būsimiems incidentams, bendradarbiaujant su CSIRT tinklu, reikia atlikti arba padėti atlikti *ex post* techninius incidentų tyrimus.

[56] „Cyber Europe“ iki šiol yra didžiausios ir visapusiškiausios ES kibernetinio saugumo pratybos, kuriose dalyvauja saugiau kaip 700 kibernetinio saugumo profesionalų iš visų 28 valstybių narių. Jos rengiamos kas antrus metus. ENISA ir 2013 m. ES kibernetinio saugumo strategijos vertinimas rodo, kad daug suinteresuotųjų subjektų pasisako už „Cyber Europe“ masto išplėtimą iki kasmet organizuojamo renginio, atsižvelgiant į greitai kintantį kibernetinių grėsmių pobūdį. Tačiau, atsižvelgiant į ribotus Agentūros išteklius, šiuo metu tai nėra įmanoma.

Su rinka susijusios užduotys (standartizavimas, sertifikavimas)	Užduotys apimtų aktyvią pagalbą vykdant veiklą pagal Sertifikavimo sistemą, įskaitant techninių ekspertinių žinių teikimą, siekiant parengti galimas Europos kibernetinio saugumo sertifikavimo schemas. Užduotys taip pat apims pagalbą formuojant ir įgyvendinant Sąjungos standartizavimo, sertifikavimo ir rinkos stebėjimo politiką – tam reikės sudaryti palankesnes sąlygas įgyvendinti elektroninių produktų, tinklų ir paslaugų rizikos valdymo standartus ir konsultuoti esminių paslaugų operatorius ir skaitmeninių paslaugų teikėjus dėl techninių saugumo reikalavimų. Užduotys taip pat apims svarbiausių kibernetinio saugumo rinkos tendencijų analizę.
Žinios ir informacija, informuotumo didinimas	Siekiant užtikrinti lengvesnę prieigą prie geresnės struktūros informacijos apie kibernetinio saugumo riziką ir galimas taisomąsias priemones, pasiūlymu Agentūrai suteikiama nauja užduotis sukurti Sąjungos informacijos centrą ir palaikyti jo veikimą. Užduotys apimtų ES institucijų, agentūrų ir įstaigų pateiktos informacijos apie tinklo ir informacinių sistemų saugumą, ypač kibernetinį saugumą, rinkimą, sutelkimą ir galimybės ta informacija specialiu portalu naudotis visuomenei užtikrinimą. Užduotys taip pat apimtų ENISA veiklos, susijusios su informuotumo didinimu, rėmimą, kad Agentūra galėtų padidinti veiksmų mastą.

3.2.3.2. Numatomi pagrindinio GD žmogiškųjų išteklių poreikiai

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškųjų išteklių nenaudojama.

– ☒ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

Sąmatą nurodyti sveikaisiais skaičiais (arba ne smulkiau nei dešimtųjų tikslumu)

		Papildomi darbuotojai			
	2017 m. atskaitos scenarijus	3–4 ketv. 2019	2020	2021	2020
• **Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)**					
09 01 01 01 (Komisijos būstinė ir atstovybės)	1	2	3		
• **Išorės darbuotojai (etatų ekvivalentais)**[57]					
09 01 02 01 (AC, END, INT finansuojami iš bendrojo biudžeto)	1	2			
IŠ VISO		**4**	**3**		

Vykdytinų užduočių aprašymas:

Pareigūnai ir laikinieji darbuotojai	Atstovauja Komisijai Agentūros Valdančiojoje taryboje. Rengia Komisijos nuomonę apie ENISA bendrąjį programavimo dokumentą ir stebi jo įgyvendinimą. Prižiūri Agentūros biudžeto rengimą ir stebi jo vykdymą. Padeda Agentūrai plėtoti savo veiklą pagal Sąjungos politikos nuostatas, be kita ko, dalyvaudami atitinkamuose posėdžiuose. Prižiūri IRT produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo schemų sistemos įgyvendinimą. Palaiko ryšius su valstybėmis narėmis ir kitais susijusiais suinteresuotaisiais subjektais sertifikavimo klausimais. Bendradarbiauja su ENISA dėl galimų schemų. Rengia galimas Europos kibernetinio saugumo schemas.
Išorės darbuotojai	Kaip nurodyta pirmiau

[57] AC = sutartininkai („Contract Staff“); AL = vietos darbuotojai („Local Staff“); END = deleguotieji nacionaliniai ekspertai („Seconded National Experts“); INT = agentūrų darbuotojai („agency staff“); JED = jaunesnieji atstovybės ekspertai („Junior Experts in Delegations“).

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

– ☐ Pasiūlymas (iniciatyva) atitinka dabartinę daugiametę finansinę programą.

– ☒ Atsižvelgiant į pasiūlymą (iniciatyvą), reikės pakeisti daugiametės finansinės programos atitinkamos išlaidų kategorijos programavimą.

Pasiūlymas apims 09 02 03 straipsnio perprogramavimą dėl ENISA įgaliojimų peržiūros, juo Agentūrai suteikiamos naujos užduotys, be kita ko, susijusios su TIS direktyvos įgyvendinimu ir Europos kibernetinio saugumo sertifikavimo sistema. Susijusios sumos:

Metai	Numatyta	Prašoma
2019	10,739	16,550
2020	10,954	20,646
2021	nėra duomenų	22,248*
2022	nėra duomenų	23,023*

* Tai yra įvertis. ES finansavimas po 2020 m. bus išnagrinėtas, kai Komisijoje bus diskutuojama dėl visų laikotarpio po 2020 m. pasiūlymų. Vadinasi, pateikusi pasiūlymą dėl kitos daugiametės finansinės programos, Komisija pateiks pataisytą finansinę teisės akto pažymą, kurioje bus atsižvelgta į poveikio vertinimo išvadas[58].

– ☐ Įgyvendinant pasiūlymą (iniciatyvą) būtina taikyti lankstumo priemonę arba patikslinti daugiametę finansinę programą[59].

3.2.5. Trečiųjų šalių įnašai

– ☐ Pasiūlyme (iniciatyvoje) nenumatyta bendro su trečiosiomis šalimis finansavimo.

– ☒ Pasiūlyme (iniciatyvoje) numatytas bendras finansavimas apskaičiuojamas taip:

	Metai **2019**	Metai **2020**	Metai **2021**	Metai **2022**
ELPA	p. m.[60]	p. m.	p. m.	p. m.

[58] Nuoroda į puslapį, kuriame pateikiamas poveikio vertinimas.

[59] Žr. Tarybos reglamento (ES, Euratomas) Nr. 1311/2013, kuriuo nustatoma 2014–2020 m. daugiametė finansinė programa, 11 ir 17 straipsnius.

[60] Tiksli vėlesniems metams skirta suma bus žinoma, kai bus nustatytas atitinkamų metų ELPA proporcingumo koeficientas.

3.3. Numatomas poveikis įplaukoms

– ☒ Pasiūlymas (iniciatyva) neturi finansinio poveikio įplaukoms.

– ☐ Pasiūlymas (iniciatyva) turi finansinį poveikį:

  – ☐ nuosaviems ištekliams

  – ☐ įvairioms įplaukoms