EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (ES) 2019/881

2019 m. balandžio 17 d.

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

(Tekstas svarbus EEE)

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

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

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

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

atsižvelgdami į Regionų komiteto nuomonę ([2]),

laikydamiesi įprastos teisėkūros procedūros ([3]),

kadangi:

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

(2) piliečiai, organizacijos ir verslo įmonės visoje Sąjungoje dabar labai plačiai naudoja tinklų ir informacines sistemas. Vis daugiau produktų ir paslaugų yra grindžiami skaitmeninimu ir susietumu, ir numatoma, kad, įsitvirtinus daiktų internetui, per ateinantį dešimtmetį Sąjungoje bus įdiegtas ypatingai didelis skaičius susietųjų skaitmeninių įrenginių. Nors prie interneto prijungiama vis daugiau įrenginių, jų projektavimo etape nepakankamai atsižvelgiama į saugumą ir atsparumą, dėl to jų kibernetinis saugumas yra nepakankamas. Tomis aplinkybėmis dėl riboto sertifikavimo naudojimo pavieniai naudotojai, organizacijos ir verslo įmonės negauna pakankamai informacijos apie IRT produktų, paslaugų ir procesų kibernetinio saugumo savybes, o tai mažina pasitikėjimą skaitmeniniais sprendimais. Tinklų ir informacinės sistemos gali mums talkinti visose mūsų gyvenimo srityse ir skatinti Sąjungos ekonomikos augimą. Jos yra skaitmeninės bendrosios rinkos kūrimo pagrindas;

(3) dėl išaugusio skaitmeninimo ir susietumo padidėjo kibernetiniam saugumui kylanti rizika, todėl visa visuomenė gali labiau nukentėti nuo kibernetinių grėsmių ir didėja gyventojams, įskaitant pažeidžiamus asmenis, pvz., vaikus, kylantys pavojai. Siekiant sumažinti šiuos pavojus, būtina imtis visų reikiamų veiksmų Sąjungoje padidinti kibernetinį saugumą, kad nuo kibernetinių grėsmių būtų geriau apsaugotos tinklų ir informacinės sistemos, ryšių tinklai, skaitmeniniai produktai, paslaugos ir įrenginiai, kuriais naudojasi piliečiai, organizacijos ir verslo įmonės – nuo mažųjų ir vidutinių įmonių (MVĮ), kaip apibrėžta Komisijos rekomendacijoje Nr. 2003/361/EB ([4]), iki ypatingos svarbos infrastruktūros objektų operatorių;

([1]) OL C 227, 2018 6 28, p. 86.
([2]) OL C 176, 2018 5 23, p. 29.
([3]) 2019 m. kovo 12 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2019 m. balandžio 9 d. Tarybos sprendimas.
([4]) 2003 m. gegužės 6 d. Komisijos rekomendacija dėl labai mažų, mažų ir vidutinių įmonių (MVĮ) apibrėžties (OL L 124, 2003 5 20, p. 36).

(4) sudarydama visuomenei sąlygas susipažinti su atitinkama informacija, Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA), įsteigta Europos Parlamento ir Tarybos reglamentu (ES) Nr. 526/2013 ([5]), prisideda prie kibernetinio saugumo pramonės Sąjungoje vystymo, visų pirma prie MVĮ ir startuolių plėtros. ENISA turėtų siekti glaudžiau bendradarbiauti su universitetais ir mokslinių tyrimų centrais, kad būtų prisidedama prie priklausomybės nuo kibernetinio saugumo produktų ir paslaugų, kurie nėra iš Sąjungos, sumažinimo ir tiekimo grandinių Sąjungos viduje stiprinimo;

(5) kibernetinių išpuolių daugėja, todėl susietajai ekonomikai ir visuomenei, kuri gali labiau nukentėti nuo 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 incidentai gali sutrikdyti esminių paslaugų visoje Sąjungoje teikimą. Todėl būtinas veiksmingas ir koordinuotas Sąjungos lygmens atsakas ir krizių valdymas, paremtas tiksline politika ir bendresnio pobūdžio Europos solidarumo ir savitarpio pagalbos priemonėmis. Be to, politikos formuotojams, verslo 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, iššūkiai ir grėsmės;

(6) 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. Tie tikslai apima tolesnį valstybių narių ir įmonių pajėgumų bei parengties gerinimą, taip pat valstybių narių ir Sąjungos institucijų, įstaigų, organų ir agentūrų bendradarbiavimo, dalijimosi informacija ir veiksmų koordinavimo gerinimą. Be to, dėl tarpvalstybinio kibernetinių grėsmių pobūdžio būtina didinti Sąjungos lygmens pajėgumus, kurie galėtų papildyti valstybių narių veiksmus, visų pirma didelių tarpvalstybinių incidentų ir krizių atveju, kartu atsižvelgiant į nacionalinių reagavimo į bet kokio masto kibernetines grėsmes pajėgumų palaikymo ir tolesnio plėtojimo svarbą;

(7) taip pat reikia dėti daugiau pastangų siekiant didinti piliečių, organizacijų ir verslo įmonių informuotumą apie kibernetinio saugumo klausimus. Be to, atsižvelgiant į tai, kad incidentai mažina pasitikėjimą skaitmeninių paslaugų teikėjais ir pačia skaitmenine bendrąja rinka, ypač tarp vartotojų, reikėtų toliau stiprinti pasitikėjimą skaidriai teikiant informaciją apie IRT produktų, paslaugų ir procesų saugumo lygį, pabrėžiant, kad net ir aukštas kibernetinio saugumo sertifikavimo lygis negali garantuoti IRT produkto, paslaugos ar proceso visiško saugumo. Padidinti pasitikėjimą galėtų pagerinti Sąjungos masto sertifikavimas, numatant bendrus kibernetinio saugumo reikalavimus ir vertinimo kriterijus visose nacionalinėse rinkose ir sektoriuose;

(8) kibernetinis saugumas nėra vien su technologijomis susijęs klausimas, vienodai svarbus yra žmonių elgesys. Todėl reikėtų aktyviai propaguoti „kibernetinę higieną“ – nesudėtingas įprastines priemones, kurias įgyvendinę ir reguliariai taikydami piliečiai, organizacijos ir įmonės kiek įmanoma labiau sumažina kibernetinių grėsmių jiems keliamą riziką;

(9) siekiant stiprinti Sąjungos kibernetinio saugumo struktūras, svarbu palaikyti ir plėtoti valstybių narių pajėgumus visapusiškai reaguoti į kibernetines grėsmes, įskaitant tarpvalstybinius incidentus;

(10) įmonės ir individualūs vartotojai turėtų turėti tikslią informaciją apie tai, koks yra sertifikavimu patvirtintas jų IRT produktų, paslaugų ir procesų saugumo užtikrinimo lygis. Tuo pačiu metu joks IRT produktas ar paslauga nėra visiškai saugus kibernetiniu požiūriu, ir reikia propaguoti elementarias kibernetinės higienos taisykles ir teikti joms pirmenybę. Atsižvelgiant į tai, kad daugėja daiktų interneto įrenginių, esama daug įvairių savanoriškų priemonių, kurių gali imtis privatusis sektorius, kad sustiprintų pasitikėjimą IRT produktų, paslaugų ir procesų saugumu;

(11) šiuolaikiniai IRT produktai ir sistemos dažnai turi integruotas vieną ar kelias trečiųjų šalių technologijas ir komponentus ir jais remiasi, pavyzdžiui, programinės įrangos modulius, bibliotekas ar taikomųjų programų sąsajas. Dėl šio rėmimosi, vadinamo „priklausomybe“, galėtų kilti papildoma rizika kibernetiniam saugumui, nes trečiųjų šalių komponentuose aptiktos pažeidžiamumo spragos taip pat galėtų pakenkti IRT produktų, paslaugų ir procesų saugumui. Daugeliu atveju tokios priklausomybės identifikavimas ir dokumentavimas sudaro galimybę galutiniams IRT produktų, paslaugų ir procesų naudotojams pagerinti savo rizikos kibernetiniam saugumui valdymo veiklą patobulinant, pavyzdžiui, naudotojų kibernetinio saugumo pažeidžiamumo spragų valdymo ir ištaisymo procedūras;

([5]) 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).

(12) IRT produktų, paslaugų arba procesų projektavime ir plėtojime dalyvaujančios organizacijos, gamintojai ar tiekėjai turėtų būti skatinami ankstyviausiuose projektavimo ir plėtojimo etapuose diegti tokias priemones, kad tie produktai, paslaugos ir procesai būtų kiek įmanoma geriau apsaugomi, kad būtų daroma prielaida, jog kibernetinių išpuolių pasitaikys, ir būtų numatomas bei iki minimumo sumažinamas šių išpuolių poveikis (integruotasis saugumas). Saugumas turėtų būti užtikrinamas per visą IRT produkto, paslaugos ar proceso gyvavimo laikotarpį, o projektavimo ir plėtojimo procesai turėtų būti nuolat tobulinami siekiant sumažinti piktybinių veiksmų žalą;

(13) įmonės, organizacijos ir viešasis sektorius turėtų taip konfigūruoti jų kuriamus IRT produktus, paslaugas ar procesus, kad būtų užtikrintas aukštesnis saugumo lygis, tokiu būdu pirmajam naudotojui sudarant galimybes gauti pačių saugiausių įmanomų nustatymų integruotąją konfigūraciją („integruotasis saugumas“), ir taip būtų sumažinta naudotojams tenkanti IRT produkto, paslaugos ar proceso tinkamo konfigūravimo našta. Jeigu integruotasis saugumas yra įdiegtas, jis turėtų tiesiog lengvai ir patikimai veikti – jo veikimui užtikrinti neturėtų reikėti atlikti išsamių nustatymų, arba kad naudotojas turėtų specialių techninių žinių ar atliktų kitokius, nei savaime suprantami, veiksmus. Jei konkrečiu atveju remiantis rizikos ir tinkamumo naudoti analize galima daryti išvadą, kad toks numatytasis nustatymas neįmanomas, naudotojai turėtų būti paraginti pasirinkti saugiausią nustatymą;

(14) Europos Parlamento ir Tarybos reglamentu (EB) Nr. 460/2004 ([6]) įsteigta ENISA, siekiant prisidėti prie šių tikslų įgyvendinimo: užtikrinti aukštą Sąjungos tinklų ir informacijos saugumo lygį ir piliečių, vartotojų, įmonių ir viešojo administravimo institucijų labui formuoti tinklų ir informacijos saugumo kultūrą. Europos Parlamento ir Tarybos reglamentu (EB) Nr. 1007/2008 ([7]) ENISA įgaliojimai pratęsti iki 2012 m. kovo mėn. Europos Parlamento ir Tarybos reglamentu (ES) Nr. 580/2011 ([8]) ENISA įgaliojimai buvo dar pratęsti iki 2013 m. rugsėjo 13 d. Reglamentu (ES) Nr. 526/2013 ENISA įgaliojimai buvo pratęsti iki 2020 m. birželio 19 d.;

(15) Sąjunga jau ėmėsi svarbių veiksmų siekdama užtikrinti kibernetinį saugumą ir padidinti pasitikėjimą skaitmeninėmis technologijomis. 2013 m. buvo priimta Europos Sąjungos kibernetinio saugumo strategija siekiant nubrėžti Sąjungos politikos atsako į kibernetines grėsmes ir riziką gaires. Kad piliečiai būtų geriau apsaugoti internete, 2016 m. priimtas pirmasis Sąjungos kibernetinio saugumo srities teisės procedūra priimamas aktas – Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 ([9]). Direktyva (ES) 2016/1148 buvo nustatyti reikalavimai, susiję su kibernetinio saugumo srities nacionaliniais pajėgumais, sukurti pirmieji mechanizmai, kuriais siekiama stiprinti strateginį ir operatyvinį valstybių narių bendradarbiavimą, ir nustatytos pareigos, susijusios su saugumo priemonėmis ir pranešimais apie incidentus sektoriuose, kurie yra itin svarbūs ekonomikai ir visuomenei, pvz., energetikos, transporto, geriamo vandens tiekimo ir paskirstymo, bankininkystės, finansų rinkų infrastruktūros, sveikatos priežiūros, skaitmeninės infrastruktūros, taip pat pagrindinių skaitmeninių paslaugų teikėjų (paieškos sistemų, debesijos kompiuterijos paslaugų ir elektroninių prekyviečių).

Vienas iš pagrindinių vaidmenų remiant tos direktyvos įgyvendinimą buvo priskirtas ENISA. Be to, veiksminga kova su kibernetiniais nusikaltimais yra svarbus Europos saugumo darbotvarkės prioritetas, prisidedantis prie bendro tikslo užtikrinti aukštą kibernetinio saugumo lygį. Prie aukšto kibernetinio saugumo lygio bendrojoje skaitmeninėje rinkoje prisideda ir kiti teisės aktai, pavyzdžiui, Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 ([10]), Europos Parlamento ir Tarybos direktyvos 2002/58/EB ([11]) ir (ES) 2018/1972 ([12]).

([6]) 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).

([7]) 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).

([8]) 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).

([9]) 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1).

([10]) 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).

([11]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

([12]) 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (nauja redakcija) (OL L 321, 2018 12 17, p. 36).

(16) nuo tada, kai 2013 m. buvo priimta Europos Sąjungos kibernetinio saugumo strategija ir buvo atlikta paskiausia ENISA įgaliojimų peržiūra, įvyko didelių bendrų politinių aplinkybių pokyčių, susijusių su mažiau nuspėjama ir mažiau saugia pasauline aplinka. Šiomis aplinkybėmis ir atsižvelgiant į pozityvią ENISA vaidmens kaip informacinio centro, kuris teikia rekomendacijas ir ekspertines žinias, taip pat padeda bendradarbiauti ir stiprinti pajėgumus, raidą, taip pat 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 iššūkius, kylančius dėl radikaliai pasikeitusios kibernetinių grėsmių padėties, o šiam tikslui pasiekti, kaip pripažinta ENISA vertinime, esamų įgaliojimų nepakanka;

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

(18) Sprendimu 2004/97/EB, Euratomas, kurį bendru susitarimu priėmė valstybių narių atstovai, posėdžiavę valstybės arba Vyriausybės vadovų lygiu ([13]), valstybių narių atstovai nusprendė, kad ENISA būstinė bus viename iš Graikijos miestų, dėl kurio nuspręs Graikijos Vyriausybė. ENISA priimančioji valstybė narė turėtų užtikrinti kuo geresnes jos sklandžios ir veiksmingos veiklos sąlygas. Kad ENISA tinkamai ir veiksmingai vykdytų savo užduotis, samdytų ir išsaugotų darbuotojus bei veiksmingiau vykdytų tinklaveiką, yra būtina ENISA įkurdinti tinkamoje vietovėje, be kita ko, užtikrinant tinkamas transporto jungtis ir infrastruktūrą su ENISA darbuotojais atvykstantiems sutuoktiniams ir vaikams. ENISA ir priimančiosios valstybės narės susitarime, sudarytame gavus ENISA Valdančiosios tarybos pritarimą, turėtų būti nustatytos reikiamos nuostatos;

(19) atsižvelgiant į didėjančią kibernetiniam saugumui kylančią riziką ir iššūkius, su kuriais susiduria Sąjunga, reikėtų padidinti ENISA skiriamus finansinius ir žmogiškuosius išteklius, kad būtų atsižvelgta į išaugusį jos vaidmenį ir uždavinius, taip pat labai svarbų jos vaidmenį Sąjungos skaitmeninę ekosistemą ginančių organizacijų ekosistemoje, kad ENISA galėtų veiksmingai atlikti jai pagal šį Reglamentą pavestas užduotis;

(20) ENISA 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 rekomendacijas ir skleisdama kokybišką informaciją, užtikrindama savo procedūrų ir veiklos būdų skaidrumą bei uoliai vykdydama savo užduotis. Vykdydama savo užduotis ENISA turėtų aktyviai remti nacionalinius veiksmus ir iniciatyviai prisidėti prie Sąjungos veiksmų, visapusiškai bendradarbiaudama su Sąjungos institucijomis, įstaigomis, organais ir agentūromis bei valstybėmis narėmis, vengdama darbo dubliavimo ir propaguodama sinergiją. Be to, ENISA turėtų remtis privačiojo sektoriaus ir kitų atitinkamų suinteresuotųjų subjektų indėliu ir bendradarbiavimu su jais. Užduočių sąraše turėtų būti nurodyta, kaip ENISA turi siekti savo tikslų, tačiau jos veiklos sąlygos turėtų būti lanksčios;

(21) kad galėtų valstybėms narėms teikti tinkamą paramą operatyvinio bendradarbiavimo srityje, ENISA turėtų toliau stiprinti savo techninius ir žmogiškuosius pajėgumus ir įgūdžius. ENISA turėtų plėsti savo praktinę patirtį ir pajėgumus. ENISA ir valstybės narės savanorišku pagrindu galėtų plėtoti nacionalinių ekspertų komandiravimo į ENISA programas, telkiant ekspertus ir vykdant darbuotojų mainus;

(22) ENISA turėtų padėti Komisijai teikdama rekomendacijas, nuomones ir analizę visais Sąjungos klausimais, susijusiais su politikos ir teisės kūrimu, atnaujinimais ir peržiūromis kibernetinio saugumo srityje, ir jų specifiniais sektorių aspektais, siekiant padidinti kibernetinio saugumo aspektą apimančios Sąjungos politikos ir teisės aktualumą ir sudaryti galimybę tą politiką ir teisę nuosekliai įgyvendinti nacionaliniu lygmeniu. Rengiant Sąjungos sektorinę politiką ir teisės aktų iniciatyvas kibernetinio saugumo klausimais ENISA turėtų veikti kaip informacinis centras, teikdama rekomendacijas ir ekspertines žinias. ENISA turėtų reguliariai teikti informaciją Europos Parlamentui apie savo veiklą;

([13]) 2003 m. gruodžio 13 d. Sprendimas 2004/97/EB, Euratomas, kurį bendru susitarimu priėmė valstybių narių atstovai, posėdžiavę valstybės arba vyriausybės vadovų lygiu dėl tam tikrų Europos Sąjungos įstaigų ir agentūrų būstinių vietos (OL L 29, 2004 2 3, p. 15).

(23) atvirojo interneto viešasis pagrindas, kitaip tariant – interneto pagrindiniai protokolai ir infrastruktūra, kurie yra pasaulinės viešosios gėrybės, užtikrina esmines viso interneto funkcines galimybes ir nuo jų priklauso jo įprastas veikimas. ENISA turėtų remti atvirojo interneto viešojo pagrindo funkcionavimo saugumą ir stabilumą, įskaitant pagrindinius protokolus (visų pirma DNS, BGP ir IPv6), domeno vardų sistemos veikimą (kaip antai visų aukščiausio lygio domenų vardų veikimą) ir šakninės zonos veikimą, bet ne tik tai;

(24) pagrindinė ENISA užduotis yra skatinti nuosekliai įgyvendinti atitinkamus teisės aktus, visų pirma veiksmingai įgyvendinti Direktyvą (ES) 2016/1148 ir kitus susijusius teisinius dokumentus, į kuriuos įtrauktos kibernetinio saugumo srities nuostatos, nes tai itin svarbu siekiant padidinti kibernetinį atsparumą. Turint omenyje sparčiai kintančią kibernetinių grėsmių padėtį, akivaizdu, kad valstybėms narėms būtina padėti pasiūlant platesnį, įvairias politikos sritis apimantį požiūrį į kibernetinio atsparumo didinimą;

(25) ENISA turėtų padėti valstybėms narėms ir Sąjungos institucijoms, įstaigoms, organams ir agentūroms joms dedant pastangas plėtoti ir stiprinti pajėgumą ir parengtį užkirsti kelią tinklų ir informacinių sistemų saugumui kylančioms kibernetinėms grėsmėms ir incidentams, juos nustatyti ir į juos reaguoti. Visų pirma ENISA turėtų padėti plėtoti ir stiprinti nacionalines ir Sąjungos reagavimo į kompiuterių saugumo incidentus tarnybas (toliau – CSIRT), nurodytas Direktyvoje (ES) 2016/1148, kad Sąjungoje būtų užtikrintas vienodas aukštas jų kompetencijos lygis. ENISA vykdoma veikla, susijusi su valstybių narių operaciniais pajėgumais, turėtų aktyviai remti veiksmus, kurių imasi pačios valstybės narės siekdamos vykdyti savo pareigas pagal Direktyvą (ES) 2016/1148, ir todėl neturėtų jų pakeisti;

(26) ENISA taip pat turėtų padėti rengti ir atnaujinti tinklų ir informacinių sistemų saugumo, visų pirma kibernetinio saugumo, strategijas Sąjungos lygmeniu ir, gavusi prašymą, valstybių narių lygmeniu, skatinti tokių strategijų sklaidą ir stebėti jų įgyvendinimo pažangą. Taip pat ENISA turėtų prisidėti patenkinant mokymų rengimo ir mokomosios medžiagos teikimo poreikius, įskaitant viešųjų įstaigų poreikius, ir, kai tinkama, plačiu mastu rengti instruktorius, remiantis Piliečiams skirta Europos skaitmeninės kompetencijos programa siekiant padėti valstybėms narėms ir Sąjungos institucijoms, įstaigoms, organams ir agentūroms plėtoti savo mokymo pajėgumus;

(27) ENISA turėtų remti valstybių narių veiklą informuotumo didinimo ir švietimo kibernetinio saugumo klausimais srityje, palengvindama jų glaudesnį bendradarbiavimą ir keitimąsi geriausios praktikos pavyzdžiais. Tokią paramą galėtų sudaryti nacionalinių švietimo informacinių centrų tinklo ir mokymo kibernetinio saugumo srityje platformos sukūrimas. Nacionalinių švietimo informacinių centrų tinklas galėtų būti nacionalinių ryšių palaikymo pareigūnų tinklo dalis ir sudaryti pradines sąlygas būsimam koordinavimui valstybėse narėse;

(28) ENISA turėtų padėti pagal Direktyvą (ES) 2016/1148 sukurtai Bendradarbiavimo grupei vykdyti jos užduotis, visų pirma susijusias su valstybių narių esminių paslaugų teikėjų nustatymu, be kita ko, klausimais, susijusiais su tarpvalstybine priklausomybe, rizika ir incidentais, teikdama ekspertines žinias bei rekomendacijas ir sudaryti palankesnes sąlygas keistis geriausia praktika;

(29) siekiant skatinti viešojo ir privačiojo sektorių bendradarbiavimą ir bendradarbiavimą privačiajame sektoriuje, visų pirma stiprinti paramą ypatingos svarbos infrastruktūros apsaugai, ENISA turėtų remti dalijimąsi informacija sektoriuose ir tarp sektorių, visų pirma Direktyvos (ES) 2016/1148 II priede išvardytuose sektoriuose, dalydamasi geriausios praktikos pavyzdžiais ir teikdama rekomendacijas dėl esamų priemonių ir procedūrų, taip pat rekomendacijas, kaip spręsti su dalijimusi informacija susijusius reguliavimo klausimus, pavyzdžiui, padėdama steigti sektorių keitimosi informacija ir jos analizės centrus;

(30) kadangi potencialus IRT produktų, paslaugų ir procesų pažeidžiamumo spragų neigiamas poveikis nuolat didėja, aptikti ir pašalinti tokias pažeidžiamumo spragas labai svarbu mažinant bendrą kibernetiniam saugumui kylančią riziką. Patirtis rodo, kad organizacijų, pažeidžiamų IRT produktų, paslaugų ir procesų gamintojų ar teikėjų ir kibernetinio saugumo tyrimų bendruomenės narių bei Vyriausybių, kurios aptinka pažeidžiamumo spragas, bendradarbiavimas žymiai padidina IRT produktų, paslaugų ir procesų pažeidžiamumo spragų aptikimo ir pašalinimo lygį. Suderintas pažeidžiamumo spragų atskleidimas yra struktūrinis bendradarbiavimo procesas, per kurį informacinės sistemos savininkui pranešama apie pažeidžiamumo spragas, suteikiant tai organizacijai galimybę problemą diagnozuoti ir išspręsti prieš atskleidžiant išsamią informaciją apie pažeidžiamumo spragą trečiosioms šalims arba visuomenei. Taip pat procese numatytas problemą aptikusio subjekto ir organizacijos veiksmų koordinavimas, susijęs su tų pažeidžiamumo spragų viešu paskelbimu. Suderinto pažeidžiamumo spragų atskleidimo politika gali atlikti svarbų vaidmenį valstybių narių pastangų stiprinti kibernetinį saugumą kontekste;

(31) Agentūra turėtų apibendrinti ir analizuoti savanoriškai pasidalintas nacionalines CSIRT ir Europos institucijų, įstaigų, organų ir agentūrų Kompiuterinių incidentų tyrimo tarnybos, įsteigtos Europos Parlamento, Europos Vadovų Tarybos, Europos Sąjungos Tarybos, Europos Komisijos, Europos Sąjungos Teisingumo Teismo, Europos Centrinio Banko, Europos Audito Rūmų, Europos išorės veiksmų tarnybos, Europos ekonomikos ir socialinių reikalų komiteto, Europos regionų komiteto ir Europos investicijų banko susitarimu dėl Sąjungos institucijų, įstaigų, organų ir agentūrų Kompiuterinių incidentų tyrimo tarnybos (CERT-EU) darbo organizavimo ir veiklos ([14]), ataskaitas, siekdama prisidėti prie bendrų keitimosi informacija procedūrų, kalbos ir terminijos kūrimo. Remdamasi Direktyva (ES) 2016/1148, kuria padėtas pamatas savanoriškiems techninės informacijos mainams ta direktyva įkurtos reagavimo į kompiuterių saugumo incidentus tarnybos tinkle (toliau – CSIRT tinklas) operatyviniu lygmeniu, ENISA taip pat turėtų įtraukti privatųjį sektorių;

(32) ENISA turėtų padėti Sąjungos lygmeniu reaguoti į didelio masto tarpvalstybinius su kibernetiniu saugumu susijusius incidentus ir krizes. Ta veikla turėtų būti vykdoma laikantis ENISA įgaliojimų pagal šį reglamentą ir požiūrio, dėl kurio turi susitarti valstybės narės pagal Komisijos rekomendaciją (ES) 2017/1584 ([15]) ir 2018 m. birželio 26 d. Tarybos išvadas dėl ES koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes. Vykdydama šią veiklą ENISA galėtų rinkti svarbią informaciją ir prisiimti tarpininkės tarp CSIRT tinklo, techninės bendruomenės ir už krizių valdymą atsakingų sprendimus priimančių asmenų vaidmenį. Be to, ENISA turėtų remti operatyvinį valstybių narių bendradarbiavimą, jei to paprašo viena arba daugiau valstybių narių, padėti valdyti incidentus techniniu požiūriu, sudarydama palankesnes sąlygas valstybėms narėms keistis tinkamais techniniais sprendimais ir prisidėdama prie viešųjų ryšių. ENISA turėtų remti šį procesą, per reguliarias kibernetinio saugumo pratybas išbandydama tokio bendradarbiavimo būdus;

(33) remdama operatyvinį bendradarbiavimą, ENISA turėtų naudotis esamomis CERT-EU techninėmis ir operatyvinėmis ekspertinėmis žiniomis pasinaudodama struktūriniu bendradarbiavimu. Toks struktūrinis bendradarbiavimas galėtų sustiprinti ENISA ekspertines žinias. Kai tikslinga, turėtų būti sudaryti specialūs šių dviejų organizacijų susitarimai, siekiant nustatyti, kaip toks bendradarbiavimas bus įgyvendinamas praktiškai ir išvengti veiklos dubliavimo;

(34) vykdydama savo užduotis, kuriomis remiamas operatyvinis bendradarbiavimas CSIRT tinkle, ENISA turėtų galėti valstybėms narėms paprašius teikti joms paramą, pavyzdžiui, teikdama rekomendacijas, kaip pagerinti jų pajėgumus užkirsti kelią incidentams, juos aptikti ir į juos reaguoti, palengvindama didelį arba esminį poveikį turinčių incidentų techninį valdymą arba užtikrindama kibernetinių grėsmių ir incidentų analizę. ENISA turėtų palengvinti didelį arba esminį poveikį turinčių incidentų techninį valdymą, visų pirma teikdama paramą savanoriškam valstybių narių dalijimuisi techniniais sprendimais arba rengdama bendrą techninę informaciją, kuri galėtų apimti, pavyzdžiui, valstybių narių savanoriškai pasidalytus techninius sprendimus. Rekomendacijoje (ES) 2017/1584 rekomenduojama, kad valstybės narės geranoriškai bendradarbiautų ir nedelsdamos dalytųsi tarpusavyje bei su ENISA informacija apie didelio masto su kibernetiniu saugumu susijusius incidentus ir krizes. Tokia informacija dar labiau padėtų ENISA vykdyti savo operatyvinio bendradarbiavimo rėmimo užduotis;

(35) reguliaraus techninio bendradarbiavimo, padedančio būti geriau informuotiems apie padėtį Sąjungoje, dalis turėtų būti ENISA reguliariai, glaudžiai bendradarbiaujant su valstybėmis narėmis, rengiamos išsamios ES kibernetinio saugumo techninės padėties ataskaitos, kuriose apžvelgiami incidentai ir kibernetinės grėsmės ir kurios grindžiamos viešai prieinama informacija, pačios Agentūros atliekama analize ir ataskaitomis, kurias Agentūrai pateikė valstybių narių CSIRT arba Direktyvoje (ES) 2016/1148 nurodyti nacionaliniai bendrieji tinklų ir informacinių sistemų saugumo informaciniai centrai (toliau – bendrasis informacinis centras) (tiek vieni, tiek kiti – savanoriškai), Europolo Europos kovos su elektroniniu nusikalstamumu centras (EC3), CERT-EU ir, kai tikslinga, Europos išorės veiksmų tarnybai priklausantis Europos Sąjungos žvalgybos analizės centras (EU INTCEN). Ta ataskaita turėtų būti pateikta Tarybai, Komisijai, Sąjungos vyriausiajam įgaliotiniui užsienio reikalams ir saugumo politikai ir CSIRT tinklui;

(36) ENISA susijusių valstybių narių prašymu remiant didelį arba esminį poveikį turinčių incidentų *ex post* techninius tyrimus, daugiausia dėmesio turėtų būti skiriama incidentų prevencijai ateityje. Susijusios valstybės narės turėtų teikti būtiną informaciją ir pagalbą, kad ENISA galėtų veiksmingai prisidėti prie *ex-post* techninio tyrimo;

([14]) OL C 12, 2018 1 13, p. 1.
([15]) 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (OL L 239, 2017 9 19, p. 36).

(37) valstybės narės gali paraginti nuo incidento nukentėjusias įmones bendradarbiauti, suteikiant būtiną informaciją ir pagalbą ENISA, nepažeidžiant jų teisės apsaugoti neskelbtiną komercinę informaciją ir su visuomenės saugumu susijusią informaciją;

(38) siekdama geriau suprasti kibernetinio saugumo srities problemas ir teikti strategines ilgalaikes rekomendacijas valstybėms narėms ir Sąjungos institucijoms, įstaigoms, organams ir agentūroms, ENISA turi analizuoti esamą ir naujausią kibernetinio saugumo riziką. Šiuo tikslu ENISA, bendradarbiaudama su valstybėmis narėmis ir prireikus su statistikos įstaigomis ir kitomis įstaigomis, turėtų rinkti reikiamą informaciją, kuri yra viešai prieinama arba savanoriškai pateikiama, ir vykdyti naujausių technologijų analizę bei teikti teminius vertinimus, susijusius su numatomu technologinių inovacijų poveikiu tinklų ir informacijos saugumui, visų pirma kibernetiniam saugumui, pasireiškiančiu visuomeniniu, teisiniu, ekonominiu ir reguliavimo aspektais. Be to, ENISA, vykdydama grėsmių, pažeidžiamumo spragų ir incidentų analizę, turėtų padėti valstybėms narėms ir Sąjungos institucijoms, įstaigoms. organams ir agentūroms nustatyti naujausius kibernetinės rizikos veiksnius ir užkirsti kelią kibernetinio saugumo incidentams;

(39) kad padidintų Sąjungos atsparumą, ENISA turėtų plėtoti mokslinę kompetenciją infrastruktūros objektų, kurie užtikrina visų pirma Direktyvos (ES) 2016/1148 II priede išvardytų sektorių veiklą ir kuriuos naudoja tos direktyvos III priede išvardyti skaitmeninių paslaugų teikėjai, kibernetinio saugumo srityje, teikdama rekomendacijas, gaires ir dalydamasi geriausia praktika. Siekdama užtikrinti lengvesnę prieigą prie geriau susistemintos informacijos apie kibernetiniam saugumui kylančią riziką ir galimas jos mažinimo priemones, ENISA turėtų sukurti ir palaikyti Sąjungos informacijos centrą – vieno langelio principu veikiantį portalą, kuriame visuomenei būtų prieinama Sąjungos ir nacionalinių institucijų, įstaigų, organų ir agentūrų teikiama informacija apie kibernetinį saugumą. Paprastesnė prieiga prie geriau susistemintos informacijos apie kibernetiniam saugumui kylančią riziką ir galimas jos mažinimo priemones taip pat galėtų padėti valstybėms narėms sustiprinti savo pajėgumus ir suderinti savo praktiką, taip padidinant bendrą jų atsparumą kibernetiniams išpuoliams;

(40) ENISA turėtų padėti didinti visuomenės informuotumą, be kita ko, pasitelkiant visos ES masto informuotumo didinimo kampaniją, propaguojant švietimą apie su kibernetiniu saugumu susijusią riziką, ir piliečiams, organizacijoms bei įmonėms pateikti atskiriems naudotojams skirtas konsultacijas gerosios praktikos klausimais. ENISA taip pat turėtų padėti skatinti piliečius, organizacijas ir įmones taikyti geriausią praktiką ir sprendimus, įskaitant kibernetinę higieną ir kibernetinį raštingumą, šiuo tikslu rinkdama ir analizuodama viešai prieinamą informaciją apie didelius incidentus, taip pat rengdama ir viešai skelbdama ataskaitas ir konsultacijas piliečiams, organizacijoms ir įmonėms, kad būtų pagerintas bendras jų parengties ir atsparumo lygis. ENISA taip pat turėtų siekti suteikti vartotojams svarbią informaciją apie taikomas sertifikavimo schemas, pvz. parengdama gaires ir rekomendacijas. ENISA, laikydamasi 2018 m. sausio 17 d. Komisijos komunikate nustatyto Skaitmeninio švietimo veiksmų plano ir bendradarbiaudama su valstybėmis narėmis ir Sąjungos institucijomis, įstaigomis, organais ir agentūromis, taip pat turėtų organizuoti reguliarias galutiniams naudotojams skirtas informavimo ir visuomenės švietimo kampanijas, kuriomis būtų siekiama propaguoti saugesnį asmens elgesį internetinėje aplinkoje ir skaitmeninį raštingumą ir didinti informuotumą apie galimas kibernetines grėsmes kibernetinėje erdvėje, įskaitant nusikalstamą veiklą internete, pavyzdžiui, išpuolius siekiant vykdyti duomenų vagystes, botnetus, finansinį ir bankinį sukčiavimą, su duomenimis susijusio sukčiavimo atvejus, propaguoti bazinį daugiaveiksnį tapatumo nustatymą, bei teikti rekomendacijas pataisų, šifravimo, anoniminimo ir duomenų apsaugos srityse;

(41) ENISA turėtų atlikti pagrindinį vaidmenį spartindama galutinių naudotojų informuotumą apie įrenginių saugumą ir saugų paslaugų naudojimą, ir propaguoti Sąjungos lygmeniu integruotąjį saugumą ir integruotąją privatumo apsaugą. Siekdama to tikslo ENISA turėtų kuo optimaliau panaudoti geriausią praktiką ir patirtį, visų pirma geriausią praktiką ir patirtį, gautą iš akademinių įstaigų ir IT saugumo tyrėjų;

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

(43) ENISA turėtų prisidėti prie Sąjungos pastangų kibernetinio saugumo srityje bendradarbiauti su tarptautinėmis organizacijomis ir pagal atitinkamas tarptautinio bendradarbiavimo sistemas. Visų pirma ENISA, kai tinkama, turėtų prisidėti prie bendradarbiavimo su tokiomis organizacijomis, kaip EBPO, ESBO ir NATO. Toks bendradarbiavimas galėtų apimti bendras pratybas kibernetinio saugumo srityje ir bendro atsako į kibernetinius incidentus koordinavimą. Vykdant tą veiklą turi būti visapusiškai laikomasi įtraukumo, abipusiškumo ir Sąjungos sprendimų priėmimo autonomijos principų, nedarant poveikio valstybių narių saugumo ir gynybos politikos specifikai;

(44) siekiant užtikrinti, kad ENISA pasiektų visus savo tikslus, ji turėtų bendradarbiauti su atitinkamomis Sąjungos priežiūros institucijomis ir kitomis kompetentingomis institucijomis Sąjungoje, Sąjungos institucijomis, įstaigomis, organais ir agentūromis, be kita ko, CERT-EU, EC3, Europos gynybos agentūra (EGA), Europos pasaulinės palydovinės navigacijos sistemos agentūra (Europos GNSS agentūra), Europos elektroninių ryšių reguliuotojų institucija (BEREC), Europos Sąjungos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra (eu-LISA), Europos Centriniu Banku (ECB), Europos bankininkystės institucija (EBI), Europos duomenų apsaugos valdyba, Energetikos reguliavimo institucijų bendradarbiavimo agentūra (ACER), Europos Sąjungos aviacijos saugos agentūra (EASA) ir kitomis su kibernetiniu saugumu susijusiomis Sąjungos agentūromis. ENISA taip pat turėtų bendradarbiauti su duomenų apsaugos institucijomis siekiant keistis praktine patirtimi ir geriausios praktikos pavyzdžiais 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 ENISA patariamosios grupės veikloje. Bendradarbiaudama su teisėsaugos įstaigomis dėl tinklų ir informacijos saugumo aspektų, galinčių turėti įtakos jų darbui, ENISA turėtų naudotis esamais informacijos kanalais ir sukurtais tinklais;

(45) galėtų būti kuriamos partnerystės su akademinėmis įstaigomis, kurios yra parengusios mokslinių tyrimų iniciatyvų atitinkamose srityse, o vartotojų organizacijų ir kitų organizacijų informacija turėtų būti perduodama tinkamais kanalais ir į ją reikėtų atsižvelgti;

(46) ENISA, vykdydama CSIRT tinklo sekretoriato funkciją, turėtų remti valstybių narių CSIRT ir CERT-EU operatyvinį bendradarbiavimą, taip pat padėti vykdant visas atitinkamas CSIRT tinklo užduotis, kaip apibrėžta Direktyvoje (ES) 2016/1148. Be to, ENISA turėtų skatinti ir remti atitinkamų CSIRT bendradarbiavimą incidentų, išpuolių arba tinklo ar infrastruktūros, kurią valdo ar saugo CSIRT ir kurioje dalyvauja ar gali dalyvauti bent dvi CSIRT, sutrikimų atvejais, deramai atsižvelgdama į CSIRT tinklo standartines veiklos procedūras;

(47) kad Sąjunga būtų geriau pasirengusi reaguoti į kibernetinio saugumo incidentus, ENISA turėtų organizuoti reguliarias Sąjungos lygmens kibernetinio saugumo pratybas ir valstybių narių, Sąjungos institucijų, įstaigų, organų ir agentūrų prašymu padėti joms organizuoti pratybas. Vieną kartą per dvejus metus turėtų būti surengtos didelio masto visapusiškos pratybos, apimančios techninius, operatyvinius ir strateginius elementus. Be to, ENISA turėtų galėti reguliariai rengti ne tokias visapusiškas pratybas, siekdama to paties tikslo – didinti Sąjungos parengtį reaguoti į incidentus;

(48) kad galėtų prisidėti prie Sąjungos kibernetinio saugumo sertifikavimo politikos, ENISA turėtų toliau plėtoti ir išlaikyti savo kompetenciją šiais klausimais. ENISA turėtų pasinaudoti esama geriausia praktika ir skatinti kibernetinio saugumo sertifikavimo diegimą Sąjungoje, be kita ko, prisidėdama prie Sąjungos lygmens kibernetinio saugumo sertifikavimo sistemos (Europos kibernetinio saugumo sertifikavimo sistema) sukūrimo ir taikymo, kad būtų didinamas IRT produktų, paslaugų ir procesų kibernetinio saugumo užtikrinimo skaidrumas ir taip stiprinamas pasitikėjimas skaitmenine vidaus rinka ir jos konkurencingumas;

(49) veiksminga kibernetinio saugumo politika viešajame ir privačiajame sektoriuose turėtų būti grindžiama gerai parengtais rizikos vertinimo metodais. Rizikos vertinimo metodai taikomi įvairiais lygmenimis, nėra bendros praktikos, kaip juos veiksmingai taikyti. Geriausių rizikos vertinimo ir sąveikiųjų rizikos valdymo sprendimų populiarinimas ir plėtojimas viešojo sektoriaus ir privačiojo sektoriaus organizacijose padidins kibernetinio saugumo lygį Sąjungoje. Todėl ENISA turėtų remti suinteresuotųjų subjektų bendradarbiavimą Sąjungos lygmeniu ir palengvinti jų pastangas nustatyti Europos ir tarptautinius standartus rizikos valdymo, taip pat elektroninių produktų, sistemų, tinklų ir paslaugų, kurios kartu su programine įranga sudaro tinklų ir informacijos sistemas, išmatuojamojo saugumo srityje ir jų laikytis;

(50) ENISA turėtų skatinti valstybes nares, produktų gamintojus ir paslaugų teikėjus griežtinti savo bendruosius saugumo standartus, kad visi interneto naudotojai galėtų imtis reikiamų veiksmų savo asmeniniam kibernetiniam saugumui užtikrinti ir būtų skatinami tai daryti. Visų pirma, paslaugų teikėjai ir produktų gamintojai turėtų teikti būtinus naujinius ir atšaukti, atsiimti arba perdirbti kibernetinio saugumo standartų neatitinkančius IRT produktus, paslaugas arba IRT procesus, o importuotojai ir platintojai turėtų užtikrinti, kad IRT produktai, IRT paslaugos ir IRT procesai, kuriuos jie teikia Sąjungos rinkai, atitiktų taikomus reikalavimus ir nekeltų rizikos Sąjungos vartotojams;

(51) bendradarbiaudama su kompetentingomis institucijomis ENISA turėtų galėti skleisti informaciją apie vidaus rinkoje siūlomų IRT produktų, IRT paslaugų ir IRT procesų kibernetinio saugumo lygį ir įspėti paslaugų teikėjus bei gamintojus ir reikalauti, kad jie pagerintų savo IRT produktų, IRT paslaugų ir IRT procesų saugumą;

(52) ENISA 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 rekomendacijas Sąjungos institucijoms, įstaigoms, organams ir agentūroms, ir, kai aktualu ir joms paprašius – valstybėms narėms – dėl mokslinių tyrimų poreikių kibernetinio saugumo srityje. Kad nustatytų mokslinių tyrimų poreikius ir prioritetus, ENISA taip pat turėtų konsultuotis su atitinkamomis naudotojų grupėmis. Konkrečiau, būtų galima užmegzti bendradarbiavimą su Europos mokslinių tyrimų taryba, Europos inovacijos ir technologijos institutu ir Europos Sąjungos saugumo studijų institutu;

(53) ENISA turėtų reguliariai konsultuotis su standartizacijos organizacijomis, visų pirma Europos standartizacijos organizacijomis, kai rengiamos Europos kibernetinio saugumo sertifikavimo schemos;

(54) kibernetinės grėsmės yra pasaulinės. Būtinas glaudesnis tarptautinis bendradarbiavimas, kad būtų patobulinti kibernetinio saugumo standartai, įskaitant bendrų elgesio normų apibrėžimą ir elgesio kodeksus, tarptautinių standartų taikymą bei dalijimąsi informacija, skatinant spartesnį tarptautinį bendradarbiavimą reaguojant į tinklų ir informacijos saugumo problemas ir vadovaujantis visuotiniu požiūriu į jas. Tuo tikslu ENISA turėtų remti tolesnį Sąjungos ryšių mezgimą ir bendradarbiavimą su trečiosiomis šalimis ir tarptautinėmis organizacijomis, kai tinkama, teikdama atitinkamoms Sąjungos institucijoms, įstaigoms, organams ir agentūroms reikalingas ekspertines žinias ir analizę;

(55) ENISA turėtų būti pajėgi reaguoti į valstybių narių ir Sąjungos institucijų, įstaigų, organų ir agentūrų *ad hoc* prašymus teikti rekomendacijas ir pagalbą, susijusius su ENISA įgaliojimų tikslais;

(56) tikslinga ir rekomenduotina įgyvendinti tam tikrus ENISA valdymo principus, nustatytus bendrame pareiškime ir bendrame požiūryje, dėl kurių 2012 m. liepos mėn. susitarė Tarpinstitucinė darbo grupė ES decentralizuotų agentūrų klausimais; šiuo pareiškimu ir požiūriu siekiama racionalizuoti decentralizuotų agentūrų veiklą ir pagerinti jų darbą. Atitinkamai šiame reglamente taip pat turėtų būti atsižvelgta į rekomendacijas, pateiktas bendrame pareiškime ir bendrame požiūryje, skirtas ENISA darbo programoms, ENISA vertinimams ir ENISA ataskaitų teikimui bei administracinei veiklai;

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

(58) siekiant, kad ENISA funkcionuotų tinkamai ir veiksmingai, Komisija ir valstybės narės turėtų užtikrinti, kad į Valdančiąją tarybą būtų skiriami tinkamų profesinių žinių ir atitinkamos patirties turintys asmenys. Komisija ir valstybės narės taip pat turėtų stengtis riboti savo atstovų Valdančiojoje taryboje kaitą, kad būtų užtikrintas jos veiklos tęstinumas;

(59) kad ENISA veiktų sklandžiai, jos vykdomasis direktorius turi būti skiriamas atsižvelgiant į nuopelnus ir į dokumentais pagrįstus administracinio ir vadovaujamojo darbo įgūdžius, kibernetiniam saugumui svarbią patirtį ir kompetenciją, o vykdomojo direktoriaus pareigos turėtų būti atliekamos visiškai nepriklausomai. Pasitaręs su Komisija vykdomasis direktorius turėtų parengti ENISA metinės darbo programos pasiūlymą ir imtis visų būtinų veiksmų, kad užtikrintų tinkamą tos programos įgyvendinimą. Vykdomasis direktorius turėtų parengti Valdančiajai tarybai teikiamą metinę ataskaitą, be kita ko, apimančią Agentūros metinės darbo programos įgyvendinimą, ENISA pajamų ir išlaidų sąmatos projektą, ir vykdyti 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. Visų pirma, laikoma, kad *ad hoc* darbo grupę būtina steigti konkrečiai potencialiai Europos

kibernetinio saugumo sertifikavimo schemai (toliau – potenciali schema) parengti. Vykdomasis direktorius turėtų užtikrinti, kad *ad hoc* darbo grupės nariai būtų išrinkti pagal aukščiausius dalyko ekspertinių žinių standartus ir, atsižvelgiant į konkrečius nagrinėjamus klausimus, atitinkamai subalansuotai ir užtikrinant lyčių pusiausvyrą būtų atstovaujama valstybių narių viešojo administravimo institucijoms, Sąjungos institucijoms, įstaigoms, organams ir agentūroms bei privačiajam sektoriui, įskaitant pramonės sektorių, naudotojus ir tinklų bei informacijos saugumo akademinius ekspertus;

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

(61) siekiant užtikrinti nuolatinį dialogą su privačiuoju sektoriumi, vartotojų organizacijomis ir kitais atitinkamais suinteresuotaisiais subjektais, ENISA turėtų būti įsteigta ENISA patariamoji grupė, veikianti kaip patariamasis organas. Vykdomojo direktoriaus pasiūlymu Valdančiosios tarybos įsteigta ENISA patariamoji grupė daugiausia dėmesio turėtų skirti klausimams, kurie svarbūs suinteresuotiesiems subjektams, ir į tuos klausimus atkreipti ENISA dėmesį. Turėtų būti konsultuojamasi su ENISA patariamąja grupe visų pirma dėl ENISA metinės darbo programos projekto. ENISA patariamosios grupės sudėtis ir šiai grupei priskirtos užduotys, turėtų užtikrinti pakankamą suinteresuotųjų subjektų atstovavimą ENISA veikloje;

(62) siekiant padėti ENISA ir Komisijai sudaryti palankesnes sąlygas konsultacijoms su atitinkamais suinteresuotaisiais subjektais, turėtų būti įsteigta Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupė. Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupę turėtų sudaryti nariai, proporcingai atstovaujantys: pramonės sektoriui, tiek IRT produktų ir paslaugų paklausos, tiek pasiūlos segmentuose, įskaitant visų pirma MVĮ, skaitmeninių paslaugų teikėjams, Europos ir tarptautinėms standartizacijos įstaigoms, nacionalinėms akreditacijos įstaigoms, duomenų apsaugos priežiūros institucijoms ir atitikties vertinimo įstaigoms pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 765/2008 ([16]), akademinei bendruomenei ir vartotojų organizacijoms;

(63) ENISA turėtų priimti interesų konfliktų prevencijos ir valdymo taisykles. ENISA taip pat turėtų taikyti atitinkamas Sąjungos nuostatas dėl galimybės visuomenei susipažinti su dokumentais, kaip nustatyta Europos Parlamento ir Tarybos reglamente (EB) Nr. 1049/2001 ([17]). ENISA asmens duomenis turėtų tvarkyti laikydamasi Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([18]). ENISA turėtų laikytis Sąjungos institucijoms, įstaigoms, organams ir agentūroms taikytinų nuostatų ir nacionalinės teisės aktų dėl informacijos, visų pirma neskelbtinos neįslaptintos ir Europos Sąjungos įslaptintos informacijos (ESĮI) tvarkymo;

(64) siekiant užtikrinti visišką ENISA autonomiją ir nepriklausomumą ir suteikti jai galimybę vykdyti papildomas ir naujas užduotis, įskaitant nenumatytas užduotis kritiniais atvejais, ENISA turėtų būti skiriamas pakankamas ir nepriklausomas biudžetas, kurio pajamas iš esmės sudarytų Sąjungos įnašas ir ENISA veikloje dalyvaujančių trečiųjų šalių įnašai. Tinkamas biudžetas yra itin svarbus siekiant užtikrinti, kad ENISA turėtų pakankamai pajėgumų, kad galėtų atlikti visas savo didėjančias užduotis ir pasiekti tikslus. Dauguma ENISA darbuotojų turėtų tiesiogiai dalyvauti praktiškai vykdant ENISA įgaliojimus. Priimančiajai valstybei narei ir bet kuriai kitai valstybei narei turėtų būti leidžiama savanoriškais įnašais prisidėti prie ENISA biudžeto. Mokant subsidijas iš Sąjungos bendrojo biudžeto, turėtų būti toliau taikoma Sąjungos biudžeto procedūra. Be to, Audito Rūmai turėtų atlikti ENISA apskaitos auditą, kad būtų užtikrintas skaidrumas ir atskaitomybė;

(65) kibernetinio saugumo sertifikavimas yra labai svarbus didinant pasitikėjimą IRT produktais, paslaugomis ir procesais bei jų saugumą. Bendroji skaitmeninė rinka, ypač duomenų ekonomika ir daiktų internetas, gali klestėti tik tuo atveju, jeigu plačioji visuomenė pasitikės, jog tokie produktai, paslaugos ir procesai pasižymi tam tikro lygio kibernetiniu saugumu. Susietųjų ir automatizuotų automobilių, elektroninių medicinos priemonių, pramoninių automatizuotų valdymo sistemų ar pažangiųjų elektros energijos tinklų sektoriai yra tik keli sektorių, kuriuose sertifikavimas jau yra plačiai naudojamas arba, tikėtina, bus naudojamas artimiausioje ateityje, pavyzdžiai. Kibernetinio saugumo sertifikavimas taip pat yra itin svarbus Direktyva (ES) 2016/1148 reglamentuojamiems sektoriams;

([16]) 2008 m. liepos 9 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 765/2008 nustatantis su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinantis Reglamentą (EEB) Nr. 339/93 (OL L 218, 2008 8 13, p. 30).

([17]) 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).

([18]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

(66) 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, paslaugų ir procesų teikimas bendrojoje rinkoje geografiniu požiūriu tebėra labai susiskaidęs. Taip yra dėl to, kad kibernetinio saugumo sektorius Europoje daugiausia vystėsi priklausomai nuo nacionalinės valdžios sudaromos paklausos. Be to, kiti bendrąją kibernetinio saugumo rinką neigiamai veikiantys trūkumai yra sąveikių sprendimų (techninių standartų), metodų ir Sąjungos masto sertifikavimo mechanizmų stoka. Tai apsunkina Europos įmonių galimybes konkuruoti nacionaliniu, Sąjungos ir pasauliniu lygmenimis. Tai taip pat mažina perspektyvių ir tinkamų naudoti kibernetinio saugumo technologijų, kurios prieinamos fiziniams asmenims bei įmonėms, pasirinkimo galimybes. Be to, 2017 m. komunikate „Bendrosios skaitmeninės rinkos strategijos įgyvendinimo laikotarpio vidurio peržiūros. Sujungta bendroji skaitmeninė rinka visiems“ Komisija pabrėžė saugių susietųjų produktų ir sistemų poreikį 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;

(67) šiuo metu IRT produktų, paslaugų ir procesų kibernetinio saugumo sertifikavimas yra taikomas ribotai. Kai jie sertifikuojami, toks sertifikavimas dažniausiai vykdomas valstybių narių lygmeniu arba pagal pramonės sektoriaus inicijuojamas schemas. Vadinasi. vienos nacionalinės kibernetinio saugumo sertifikavimo institucijos išduotas sertifikatas iš esmės kitose valstybėse narėse nepripažįstamas. Todėl bendrovėms gali reikėti savo IRT produktus, paslaugas ir procesus sertifikuoti keliose valstybėse narėse, kuriose jos vykdo veiklą, pavyzdžiui, siekiant dalyvauti nacionalinėse viešųjų pirkimų procedūrose, o dėl to didėja jų išlaidos. 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 produktų aprėptimi, saugumo užtikrinimo lygiais, esminiais kriterijais ir faktiniu naudojimu, kurie trukdo abipusio pripažinimo mechanizmams Sąjungoje;

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

(69) todėl, būtina priimti bendrą požiūrį ir 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, paslaugų arba procesų Europos kibernetinio saugumo sertifikatus bei ES atitikties pareiškimus pripažinti ir taikyti visose valstybėse narėse. Atliekant šį darbą labai svarbu remtis esamomis nacionalinėmis ir tarptautinėmis schemomis, taip pat tarpusavio pripažinimo sistemomis, ypač SOG-IS, ir sudaryti sąlygas sklandžiam perėjimui nuo esamų schemų pagal tokias sistemas prie schemų pagal naująją Europos kibernetinio sertifikavimo sistemą. Europos sistema turėtų būti siekiama dvejopo tikslo: viena vertus, ji turėtų padėti didinti pasitikėjimą IRT produktais, paslaugomis ir procesais, kurie buvo sertifikuoti pagal Europos kibernetinio sertifikavimo schemas. Kita vertus, ji turėtų padėti išvengti, kad nebedidėtų viena kitai prieštaraujančių arba besidubliuojančių nacionalinių kibernetinio saugumo sertifikavimo schemų skaičius, ir taip sumažinti bendrojoje skaitmeninėje rinkoje veikiančių įmonių išlaidas. Europos kibernetinio sertifikavimo schemos turėtų būti nediskriminacinės ir pagrįstos Europos arba tarptautiniais standartais, išskyrus tuos standartus, kurie yra neveiksmingi arba netinkami siekiant įgyvendinti teisėtus šios srities Sąjungos tikslus;

(70) siekiant išvengti palankesnės ES sertifikatų išdavimo sąlygų ieškojimo praktikos, kuri taikoma dėl skirtingo reikalavimų griežtumo lygio valstybėse narėse, ši Europos kibernetinio saugumo sertifikavimo sistema turėtų būti diegiama vienodai visose valstybėse narėse;

(71) Europos kibernetinio sertifikavimo schemos turėtų būti grindžiamos tuo, kas jau veikia tarptautiniu ir nacionaliniu lygmeniu ir, jei būtina, forumų ir konsorciumų teikiamomis techninėmis specifikacijomis, mokantis iš dabartinių privalumų ir vertinant bei ištaisant trūkumus;

(72) lankstūs kibernetinio saugumo sprendimai reikalingi tam, kad pramonės sektorius būtų žingsniu priekyje kibernetinių grėsmių, todėl bet kokia sertifikavimo schema turėtų būti kuriama taip, kad būtų išvengta rizikos, kad ji greitai pasens;

(73) Komisija turėtų būti įgaliota tvirtinti konkrečioms IRT produktų, paslaugų ir procesų grupėms taikomas Europos kibernetinio saugumo sertifikavimo schemas. Tas schemas įgyvendinti ir prižiūrėti turėtų nacionalinės kibernetinio saugumo sertifikavimo institucijos, o pagal tas schemas išduoti sertifikatai turėtų galioti ir būti pripažįstami visoje Sąjungoje. Šis reglamentas neturėtų būti taikomas pramonės sektoriaus ar kitų privačių organizacijų naudojamoms sertifikavimo schemoms. Tačiau tokias schemas naudojantys subjektai turėtų galėti siūlyti Komisijai jų pagrindu patvirtinti Europos kibernetinio sertifikavimo schemą;

(74) šio reglamento nuostatomis neturėtų būti daromas poveikis Sąjungos teisės aktams, kuriais nustatomos specialios IRT produktų, paslaugų ir procesų sertifikavimo taisyklės. Visų pirma Reglamente (ES) 2016/679 išdėstytos nuostatos dėl sertifikavimo mechanizmų ir duomenų apsaugos ženklų bei žymenų nustatymo, siekiant įrodyti duomenų valdytojų ir tvarkytojų vykdomų tvarkymo operacijų atitiktį tam reglamentui. Tokie sertifikavimo mechanizmai ir duomenų apsaugos ženklai ir žymenys turėtų sudaryti sąlygas duomenų subjektams greitai įvertinti atitinkamų IRT produktų, paslaugų ir procesų duomenų apsaugos lygį. Šiuo reglamentu nedaromas poveikis duomenų tvarkymo operacijų sertifikavimui pagal Reglamentą (ES) 2016/679, taip pat tais atvejais, kai tokios operacijos pagal Bendrąjį duomenų apsaugos reglamentą integruotos į IRT produktus, paslaugas ir procesus;

(75) Europos kibernetinio saugumo sertifikavimo schemų tikslas turėtų būti užtikrinti, kad pagal tokias schemas sertifikuoti IRT produktai, paslaugos ir procesai atitiktų nustatytus reikalavimus, siekiant apsaugoti saugomų, perduodamų ar tvarkomų duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą arba tais produktais, paslaugomis ir procesais suteikiamas arba per juos prieinamas susijusias funkcijas ar paslaugas viso jų gyvavimo ciklo metu. Šiame reglamente neįmanoma išsamiai nustatyti visiems IRT produktams, paslaugoms ir procesams keliamų kibernetinio saugumo reikalavimų. IRT produktai, paslaugos ir procesai bei kibernetinio saugumo poreikiai, susiję su tais produktais, paslaugomis ir procesais, 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 turi būti pasiekti sertifikuojant konkrečius IRT produktus, paslaugas ir procesus, turėtų būti toliau išsamiai nurodyta atskiros Komisijos tvirtinamos sertifikavimo schemos lygmeniu, pavyzdžiui, nurodant standartus ar technines specifikacijas, kai tinkamų standartų nėra;

(76) Europos kibernetinio saugumo sertifikavimo schemose naudotinos techninės specifikacijos turėtų būti nustatytos laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012 ([19]) II priede išdėstytų reikalavimų. Vis dėlto tinkamai pagrįstais atvejais būtų galima laikyti, kad kai kurie nukrypimai nuo šių principų yra reikalingi, kai tos techninės specifikacijos turi būti naudojamos Europos kibernetinio saugumo sertifikavimo schemoje, patvirtinančioje aukštą saugumo užtikrinimo lygį. Tokių nukrypimų priežastys turėtų būti pateikiamos viešai;

(77) atitikties vertinimas – procedūra, kurios metu vertinama, ar buvo įvykdyti nustatyti reikalavimai, susiję su IRT produktu, paslauga arba procesu. Šią procedūrą vykdo nepriklausoma trečioji šalis, kuri nėra vertinamo IRT produkto gamintoja, IRT paslaugos teikėja ar IRT proceso vykdytoja. Po sėkmingo IRT produkto, paslaugos ar proceso įvertinimo turėtų būti išduodamas Europos kibernetinio saugumo sertifikatas. Europos kibernetinio saugumo sertifikatas turėtų būti laikomas patvirtinimu, kad įvertinimas buvo tinkamai atliktas. Priklausomai nuo saugumo užtikrinimo lygio, Europos kibernetinio saugumo sertifikavimo schemoje turėtų būti nurodyta, ar Europos kibernetinio saugumo sertifikatą išduoda privati, ar viešoji įstaiga. Pats atitikties vertinimas ir sertifikavimas negali užtikrinti, kad IRT produktai, paslaugos ir procesai kibernetiniu požiūriu yra saugūs. Tai greičiau procedūros ir techninės metodikos, kuriomis patvirtinama, kad IRT produktai, paslaugos ir procesai buvo išbandyti ir kad jie atitinka tam tikrus kitur, pavyzdžiui, techniniuose standartuose, nustatytus kibernetinio saugumo reikalavimus;

(78) Europos kibernetinio saugumo sertifikatų naudotojai, rinkdamiesi tinkamą sertifikavimą ir susijusius saugumo reikalavimus, turėtų remtis IRT produktų, paslaugų ar procesų naudojimo rizikos analize. Todėl saugumo užtikrinimo lygis turėtų atitikti rizikos, susijusios su IRT produktų, paslaugų ar procesų paskirtimi, lygį;

([19]) 2012 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1025/2012 dėl Europos standartizacijos, kuriuo iš dalies keičiamos Tarybos direktyvos 89/686/EEB ir 93/15/EEB ir Europos Parlamento ir Tarybos direktyvos 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB ir 2009/105/EB ir panaikinamas Tarybos sprendimas 87/95/EEB ir Europos Parlamento ir Tarybos sprendimas Nr. 1673/2006/EB (OL L 316, 2012 11 14, p. 12).

(79) Europos kibernetinio saugumo sertifikavimo schemoje gali būti numatyta, kad atitikties vertinimas vykdomas tik IRT produktų, paslaugų ar procesų gamintojo ar teikėjo atsakomybe (toliau – savarankiškas atitikties vertinimas). Tokiais atvejais turėtų pakakti, kad gamintojas arba teikėjas pats atliktų visus patikrinimus siekdamas užtikrinti IRT produktų, paslaugų ar procesų atitiktį Europos kibernetinio saugumo sertifikavimo schemai. Savarankiškas atitikties vertinimas turėtų būti laikomas tinkamu nesudėtingiems IRT produktams, paslaugoms ir procesais (pvz., paprastam projektavimo ir gamybos mechanizmui), dėl kurių nekyla didelė rizika viešajam interesui. Be to, savarankiškas atitikties vertinimas gali būti taikomas tik IRT produktams ir paslaugoms, atitinkantiems bazinį saugumo užtikrinimo lygį;

(80) Europos kibernetinio saugumo sertifikavimo schemose galėtų būti numatytas tiek IRT produktų, paslaugų ir procesų savarankiškas atitikties vertinimas, tiek jų sertifikavimas. Tokiu atveju schemoje turėtų būti numatytos aiškios ir suprantamos priemonės, kad vartotojai ar kiti naudotojai galėtų atskirti, kurie IRT produktai, paslaugos ir procesai yra vertinami gamintojo arba teikėjo atsakomybe, o kuriuos IRT produktus, paslaugas ir procesus sertifikuoja trečioji šalis;

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

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

(83) Europos kibernetinio saugumo sertifikavimo sistemos valdymo mechanizme atsižvelgiama į valstybių narių dalyvavimą ir į atitinkamą suinteresuotųjų subjektų dalyvavimą ir nustatomas Komisijos vaidmuo planuojant ir teikiant pasiūlymus, prašymus, rengiant, priimant ir peržiūrint Europos kibernetinio saugumo sertifikavimo schemą;

(84) Komisija turėtų, padedant Europos kibernetinio saugumo sertifikavimo grupei (toliau – EKSSG) ir Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupei ir surengusi atviras bei ir plataus masto konsultacijas, parengti tęstinę Sąjungos darbo programą, skirtą Europos kibernetinio saugumo sertifikavimo schemoms, ir ją paskelbti kaip teisiškai neprivalomą dokumentą. Tęstinė Sąjungos darbo programa turėtų būti strateginis dokumentas, sudarantis galimybę tam tikram pramonės sektoriui, nacionalinėms institucijoms ir standartizacijos įstaigoms iš anksto pasirengti visų pirma būsimoms Europos kibernetinio saugumo sertifikavimo schemoms. Tęstinėje Sąjungos darbo programoje turėtų būti pateikta daugiametė prašymų parengti potencialias schemas, kuriuos Komisija dėl konkrečių priežasčių ketina pateikti ENISA, apžvalga. Komisija turėtų atsižvelgti į šią tęstinę Sąjungos darbo programą rengdama tęstinį IRT standartizacijos planą ir Europos standartizacijos organizacijoms skirtus standartizacijos prašymus. Atsižvelgdama spartų naujų technologijų diegimą ir taikymą, į atsiradusias anksčiau nežinomas rizikos kibernetiniam saugumui rūšis arba teisės aktų bei rinkos pokyčius, Komisija arba EKSSG turėtų turėti galimybę prašyti ENISA parengti potencialias schemas, kurios nebuvo įtrauktos į tęstinę Sąjungos darbo programą. Tokiais atvejais Komisija ir EKSSG turėtų įvertinti tokio prašymo būtinumą, atsižvelgiant į bendrus šio reglamento uždavinius ir tikslus ir užtikrinant ENISA išteklių planavimo ir naudojimo tęstinumą.

Gavusi tokį prašymą, ENISA turėtų nedelsdama parengti konkretiems IRT, produktams, paslaugoms ar IRT procesams skirtas potencialias schemas. Komisija turėtų įvertinti teigiamą ir neigiamą jos prašymo poveikį konkrečiai rinkai, ypač poveikį MVĮ, inovacijoms, kliūtims patekti į tą rinką ir galutiniams naudotojams tenkančioms išlaidoms. Tada Komisija remiantis agentūros ENISA pasiūlyta potencialia schema turėtų būti įgaliota priimti įgyvendinimo aktus, kuriais būtų patvirtinta Europos kibernetinio saugumo sertifikavimo schema. 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. Tie elementai, be kita ko, turėtų apimti kibernetinio saugumo sertifikavimo taikymo sritį ir tikslą, taip pat IRT produktų, paslaugų ir procesų, kuriems taikomas sertifikavimas, kategorijas, išsamias kibernetinio saugumo reikalavimų specifikacijas, pavyzdžiui, nurodant standartus ar technines specifikacijas, konkrečius vertinimo kriterijus ir vertinimo metodus, taip pat numatomą saugumo užtikrinimo lygį, kuris gali būti bazinis, pakankamai aukštas ir (arba) aukštas, taip pat, kai taikytina, vertinimo lygius. ENISA turėtų galėti tinkamai pagrįstais atvejais atmesti Europos kibernetinio saugumo sertifikavimo grupės (EKSSG) prašymą. Tokius sprendimus turėtų priimti Valdančioji taryba ir jie turėtų būti tinkamai pagrįsti;

(85) ENISA turėtų administruoti interneto svetainę, kurioje būtų teikiama informacija apie Europos kibernetinio saugumo sertifikavimo schemas ir jų reklama, ir kurioje, be kita ko, turėtų būti pateikti prašymai parengti potencialią schemą, taip pat per parengiamąjį etapą ENISA vykdyto konsultacijų proceso metu gauta grįžtamoji informacija. Interneto svetainėje taip pat turėtų būti teikiama informacija apie pagal šį reglamentą išduotus Europos kibernetinio saugumo sertifikatus ir ES atitikties pareiškimus, taip pat informacija apie tokių Europos kibernetinio saugumo sertifikatų ir ES atitikties pareiškimų panaikinimą ir galiojimo pabaigą. Interneto svetainėje taip pat turėtų būti nurodytos nacionalinės kibernetinio saugumo sertifikavimo schemos, kurias pakeitė Europos kibernetinio saugumo sertifikavimo schema;

(86) Europos sertifikavimo schemos saugumo užtikrinimo lygis – pagrindas, kuriuo remiantis patvirtinama, kad IRT produktas, procesas ar paslauga atitinka tam tikros Europos kibernetinio saugumo sertifikavimo schemos saugumo reikalavimus. Siekiant užtikrinti Europos kibernetinio saugumo sertifikavimo sistemos nuoseklumą, Europos kibernetinio saugumo sertifikavimo schemoje turėtų būti galima apibrėžti pagal tą schemą išduodamų Europos kibernetinio saugumo sertifikatų ir ES atitikties pareiškimų saugumo užtikrinimo lygius. Kiekvienas Europos kibernetinio saugumo sertifikatas galėtų patvirtinti vieną iš saugumo užtikrinimo lygių: bazinį, pakankamai aukštą arba aukštą, o ES atitikties pareiškimas galėtų patvirtinti tik bazinį saugumo užtikrinimo lygį. Nuo saugumo užtikrinimo lygio priklausytų atitinkamas IRT produkto, paslaugos ar proceso vertinimo griežtumas ir išsamumas ir jis būtų apibūdinamas pagal tas specifikacijas, standartus ir procedūras, įskaitant technines kontrolės priemones, kurių tikslas – sušvelninti incidentus arba užkirsti jiems kelią. Kiekvienas saugumo užtikrinimo lygis turėtų būti nuoseklus įvairiose sektorių srityse, kuriose taikomas sertifikavimas;

(87) Europos kibernetinio saugumo sertifikavimo schemoje galėtų būti nustatyti keli vertinimo lygiai, priklausomai nuo taikomos vertinimo metodikos griežtumo ir išsamumo. Vertinimo lygiai turėtų atitikti vieną iš saugumo užtikrinimo lygių ir turėtų būti susieta su tinkamu saugumo užtikrinimo komponentų deriniu. Visų saugumo užtikrinimo lygių atveju IRT produktas, paslauga ar procesas turėtų turėti tam tikrų saugių funkcijų, kaip nurodyta schemoje, kurios, be kita ko, gali būti šios: saugi standartinė konfigūracija, pasirašytasis kodas, saugus naujinimas ir galimybių pasinaudoti saugumo spragomis sumažinimas ir visapusiškos dėklo arba masyvo atminties apsaugos priemonės. Šios funkcijos turėtų būti sukurtos ir palaikomos naudojant į saugumą orientuotus kūrimo metodus ir susijusias priemones, kad būtų užtikrintas patikimas veiksmingų programinės ir aparatinės įrangos mechanizmų integravimas;

(88) bazinio saugumo užtikrinimo lygio atveju atliekant vertinimą turėtų būti remiamasi bent šiais saugumo užtikrinimo komponentais: vertinimas turėtų apimti bent atitikties vertinimo įstaigos atliekamą IRT produkto, paslaugos ar proceso techninių dokumentų peržiūrą. Jei sertifikuojami IRT procesai, techninė peržiūra taip pat turėtų būti taikoma produktų ar paslaugų projektavimo, kūrimo ir palaikymo procesui. Tais atvejais, kai Europos kibernetinio saugumo sertifikavimo schemoje numatoma galimybė atlikti savarankišką atitikties vertinimą, turėtų pakakti, kad gamintojas arba paslaugų teikėjas būtų atlikęs savarankišką IRT produktų, paslaugų ar procesų atitikties sertifikavimo schemai vertinimą;

(89) vertinimas dėl pakankamai aukšto saugumo užtikrinimo lygio, be bazinio saugumo užtikrinimo lygio komponentų, turėtų būti paremtas bent patikrinimu, ar IRT produkto, paslaugos ar proceso saugumo funkcinės galimybės atitinka jų techninius dokumentus;

(90) vertinimas dėl aukšto saugumo užtikrinimo lygio, be pakankamai aukšto saugumo užtikrinimo lygio komponentų, turėtų būti paremtas bent efektyvumo bandymu, kuriuo įvertinamas IRT produkto, paslaugos ar proceso saugumo funkcinių galimybių atsparumas sudėtingų kibernetinių išpuolių, kuriuos vykdo aukšto lygio įgūdžių ir didelių išteklių turintys subjektai, rizikai;

(91) Europos kibernetinio saugumo sertifikavimas arba ES atitikties pareiškimas turėtų likti neprivalomi, išskyrus atvejus, kai Sąjungos teisę ar pagal Sąjungos teisę priimtoje valstybių narių teisėje numatyta kitaip. Jeigu nėra suderintos Sąjungos teisės, valstybės narės gali pagal Europos Parlamento ir Tarybos direktyvą (ES) 2015/1535 ([20]) priimti nacionalines technines taisykles, kuriose būtų numatytas privalomas sertifikavimas pagal Europos kibernetinio saugumo sertifikavimo schemą. Valstybės narės taip pat gali pasinaudoti Europos kibernetinio saugumo sertifikavimu viešųjų pirkimų ir Europos Parlamento ir Tarybos direktyvos 2014/24/ES ([21]) kontekste;

(92) kai kuriose srityse ateityje gali prireikti nustatyti, kad konkretūs kibernetinio saugumo reikalavimai ir sertifikavimas pagal juos būtų privalomi tam tikriems IRT produktams, paslaugoms ar procesams, siekiant padidinti kibernetinio saugumo lygį Sąjungoje. Komisija turėtų nuolat stebėti patvirtintų Europos kibernetinio saugumo sertifikavimo schemų poveikį saugių IRT produktų, paslaugų ir procesų prieinamumui vidaus rinkoje ir įvertinti, kaip plačiai sertifikavimo schemomis naudojasi gamintojai ir paslaugų teikėjai Sąjungoje. Dėl Europos kibernetinio saugumo sertifikavimo schemų efektyvumo ir poreikio konkrečias schemas padaryti privalomomis turėtų būti sprendžiama atsižvelgiant į Sąjungos teisės aktus, susijusius su kibernetiniu saugumu, visų pirma į Direktyvą (ES) 2016/1148, siekiant užtikrinti esminių paslaugų operatorių naudojamų tinklų ir informacinių sistemų saugumą;

(93) Europos kibernetinio saugumo sertifikatai ir ES atitikties pareiškimai turėtų padėti galutiniams naudotojams priimti pagrįstus sprendimus. Todėl kartu su IRT produktais, paslaugomis ir procesais, kurie buvo sertifikuoti ar kuriems buvo išduotas ES atitikties pareiškimas, turėtų būti pateikiama susisteminta informacija, pritaikyta tikėtinam techniniam numatomo naudotojo lygiui. Visa tokia informacija turėtų būti pateikiama internetu, o tam tikra informacija galėtų būti pateikiama nevirtualia, fizine forma. Galutinis naudotojas turėtų galėti gauti informaciją apie sertifikavimo schemos registracijos numerį, saugumo užtikrinimo lygį, kibernetinio saugumo rizikos, susijusios su IRT produktu, paslauga ar procesu, aprašymą, ir sertifikatą išdavusią instituciją ar įstaigą arba turėtų turėti galimybę gauti Europos kibernetinio saugumo sertifikato kopiją. Be to, galutinis naudotojas turėtų būti informuotas apie IRT produktų, paslaugų ar procesų gamintojo ar teikėjo taikomą paramos politiką kibernetinio saugumo srityje, t. y. per kiek laiko galutinis naudotojas gali tikėtis gauti kibernetinio saugumo atnaujinimus ar pataisas. Jeigu taikytina, turėtų būti teikiami patarimai dėl veiksmų ar nustatymų, kuriuos galutinis naudotojas gali atlikti siekdamas palaikyti ar padidinti IRT produkto, paslaugos ar proceso kibernetinį saugumą, ir bendrojo informacinio centro, kuriam būtų galima (papildomai prie automatinio pranešimo) pranešti apie kibernetinį išpuolį ar jo atveju gauti pagalbą, kontaktinė informacija. Ta informacija turėtų būti nuolat atnaujinama ir pateikiama informaciją apie Europos kibernetinio saugumo sertifikavimo schemas teikiančioje interneto svetainėje;

(94) tačiau, siekiant įgyvendinti šio reglamento tikslus ir išvengti vidaus rinkos susiskaidymo, nacionalinės kibernetinio saugumo sertifikavimo schemos arba procedūros, skirtos IRT produktams, paslaugoms ir procesams, kuriems taikoma Europos kibernetinio saugumo sertifikavimo schema, turėtų nustoti galioti nuo Komisijos priimtu įgyvendinimo aktu nustatytos dienos. Be to, valstybės narės neturėtų nustatyti naujų nacionalinių kibernetinio saugumo sertifikavimo schemų, skirtų IRT produktams, paslaugoms ir procesams, kuriems jau taikoma galiojanti Europos kibernetinio saugumo sertifikavimo schema. Vis dėlto valstybėms narėms neturėtų būti trukdoma priimti arba toliau taikyti nacionalines kibernetinio saugumo sertifikavimo schemas nacionalinio saugumo tikslais. Valstybės narės turėtų informuoti Komisiją ir EKSSG apie ketinimą parengti naujas nacionalines kibernetinio saugumo sertifikavimo schemas. Komisija ir EKSSG turėtų įvertinti naujų nacionalinių kibernetinio sertifikavimo schemų poveikį tinkamam vidaus rinkos veikimui ir atsižvelgiant į strateginį interesą vietoj jų pageidauti Europos kibernetinio sertifikavimo schemos;

(95) Europos kibernetinio saugumo sertifikavimo schemos yra skirtos padėti suderinti kibernetinio saugumo praktiką Sąjungoje. Jomis turi būti prisidėta prie kibernetinio saugumo lygio Sąjungoje padidinimo. Projektuojant Europos kibernetinio saugumo sertifikavimo schemas turėtų būti atsižvelgiama į inovacijas kibernetinio saugumo srityje ir sudarytos sąlygos jas kurti;

([20]) 2015 m. rugsėjo 9 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/1535, kuria nustatoma informacijos apie techninius reglamentus ir informacinės visuomenės paslaugų taisykles teikimo tvarka (OL L 241, 2015 9 17, p. 1).

([21]) 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/24/ES dėl viešųjų pirkimų, kuria panaikinama Direktyva 2004/18/EB (OL L 94, 2014 3 28, p. 65).

(96) Europos kibernetinio sertifikavimo schemose turėtų būti atsižvelgiama į esamus programinės ir aparatinės įrangos kūrimo metodus ir visų pirma į dažnų programinės ar programinės aparatinės įrangos atnaujinimų poveikį individualiems Europos kibernetinio saugumo sertifikatams. Europos kibernetinio saugumo sertifikavimo schemose turėtų būti nurodyta, kokiomis sąlygomis dėl atnaujinimo gali būti reikalaujama, kad IRT produktas, paslauga ar procesas būtų pakartotinai sertifikuojami arba kad tam tikro Europos kibernetinio saugumo sertifikato taikymo sritis būtų sumažinta atsižvelgiant, kad atnaujinimas gali daryti neigiamą poveikį atitikčiai to sertifikato saugumo reikalavimams;

(97) patvirtinus Europos kibernetinio saugumo sertifikavimo schemą IRT produktų gamintojai arba IRT paslaugų ar procesų teikėjai turėtų turėti galimybę teikti prašymą jų pasirinktai atitikties vertinimo įstaigai, įsisteigusiai bet kur Sąjungoje, sertifikuoti jų IRT produktus, paslaugas ar procesus. Atitikties vertinimo įstaigas, jeigu jos atitinka tam tikrus šiame reglamente nustatytus reikalavimus, turėtų akredituoti nacionalinė akreditacijos įstaiga. Akreditacija turėtų būti suteikiama ne ilgesniam kaip penkerių metų laikotarpiui ir turėtų būti pratęsiama tomis pačiomis sąlygomis, jei atitikties vertinimo įstaiga toliau atitinka reikalavimus. Nacionalinės akreditacijos įstaigos turėtų apriboti, laikinai sustabdyti arba panaikinti atitikties vertinimo įstaigos akreditaciją, jeigu akreditacijos sąlygos nevykdomos arba nebevykdomos arba jeigu atitikties vertinimo įstaiga pažeidžia šį reglamentą;

(98) nacionalinės teisės aktuose pateikiamos nuorodos į nacionalinius standartus, kurie nustojo galioti dėl to, kad įsigaliojo Europos kibernetinio saugumo sertifikavimo schema, gali kelti painiavą. Todėl valstybės narės turėtų Europos kibernetinio saugumo sertifikavimo schemos patvirtinimą atspindėti savo nacionalinės teisės aktuose;

(99) siekiant visoje Sąjungoje turėti lygiaverčius standartus, palengvinti Europos kibernetinio saugumo sertifikatų ir ES atitikties pareiškimų tarpusavio pripažinimą ir skatinti bendrą pasitikėjimą jais, būtina įdiegti nacionalinių kibernetinio saugumo sertifikavimo institucijų tarpusavio peržiūros sistemą. Tarpusavio peržiūra turėtų apimti procedūras, skirtas prižiūrėti IRT produktų, paslaugų ir procesų atitiktį Europos kibernetinio saugumo sertifikatams, stebėti, kaip savarankišką atitikties vertinimą atliekantys gamintojai ar teikėjai vykdo pareigas, vykdyti atitikties vertinimo įstaigų stebėseną, taip pat vertinti, ar įstaigų, išduodančių sertifikatus dėl aukšto saugumo užtikrinimo lygio, darbuotojai turi tinkamų ekspertinių žinių. Komisija turėtų priimti įgyvendinimo aktus, kuriuose nustatytų bent penkerių metų tarpusavio peržiūrų planą, taip pat išdėstytų tarpusavio peržiūros sistemos veikimo kriterijus ir metodiką;

(100) nedarant poveikio bendrajai tarpusavio peržiūros sistemai, kuri Europos kibernetinio saugumo sertifikavimo sistemos kontekste būtų įdiegta visose nacionalinėse kibernetinio saugumo sertifikavimo institucijose, tam tikrose Europos kibernetinio saugumo sertifikavimo schemose gali būti numatytas tarpusavio vertinimo mechanizmas, skirtas įstaigoms, išduodančioms IRT produktų, paslaugų ir procesų Europos kibernetinio saugumo sertifikatus dėl aukšto saugumo užtikrinimo lygio pagal tokias schemas. EKSSG turėtų remti tokių tarpusavio vertinimo mechanizmų įgyvendinimą. Atliekant tarpusavio vertinimus visų pirma turėtų būti vertinama, ar atitinkamos įstaigos suderintai vykdo savo užduotis, taip pat juose gali būti numatyti apskundimo mechanizmai. Tarpusavio vertinimų rezultatai turėtų būti skelbiami viešai. Atitinkamos įstaigos gali atitinkamai patvirtinti atitinkamas savo praktikos ir ekspertinių žinių pritaikymo priemones;

(101) valstybės narės turėtų paskirti vieną ar kelias nacionalines kibernetinio saugumo sertifikavimo institucijas, kurios prižiūrėtų, kaip vykdomos iš šio reglamento kylančios pareigos. Jeigu valstybė narė mano tai esant tikslinga, užduotys gali būti pavedamos jau veikiančioms institucijoms. Be to, valstybė narė turėtų galėti abipusiu susitarimu su kita valstybe nare nuspręsti paskirti vieną ar kelias nacionalines kibernetinio saugumo sertifikavimo institucijas tos kitos valstybės narės teritorijoje;

(102) nacionalinės kibernetinio saugumo sertifikavimo institucijos visų pirma turėtų stebėti, kaip jų atitinkamoje teritorijoje įsisteigę IRT produktų gamintojai arba IRT paslaugų ar procesų teikėjai vykdo su ES atitikties pareiškimu susijusias pareigas, ir užtikrinti jų vykdymą, padėti nacionalinėms akreditacijos įstaigoms vykdyti atitikties vertinimo įstaigų atliekamą stebėsenos ir priežiūros veiklą teikdama joms ekspertines žinias ir atitinkamą informaciją, įgalioti atitikties vertinimo įstaigas atlikti jų užduotis, kai tos įstaigos tenkina papildomus Europos kibernetinio saugumo sertifikavimo schemoje nustatytus reikalavimus, ir stebėti svarbius pokyčius kibernetinio saugumo sertifikavimo srityje. Nacionalinės kibernetinio saugumo sertifikavimo institucijos taip pat turėtų nagrinėti fizinių ar juridinių asmenų pateiktus skundus, susijusius su tų institucijų išduotais Europos kibernetinio saugumo sertifikatais arba atitikties vertinimo įstaigų išduotais Europos kibernetinio saugumo sertifikatais, patvirtinančiais aukštą saugumo užtikrinimo lygį, tinkamu mastu tirti skundo objektą ir per pagrįstą laikotarpį informuoti skundo

pateikėją apie tyrimo eigą ir rezultatus. Be to, nacionalinės kibernetinio saugumo sertifikavimo institucijos turėtų bendradarbiauti su kitomis nacionalinėmis kibernetinio saugumo sertifikavimo institucijomis ar kitomis valdžios institucijomis, be kita ko, dalydamosi informacija apie galimą IRT produktų, paslaugų ir procesų neatitiktį šio reglamento arba konkrečių Europos kibernetinio saugumo sertifikavimo schemų reikalavimams. Komisija turėtų sudaryti palankias sąlygas tokiam dalijimuisi informacija suteikdama galimybę naudotis bendrąja elektroninės informacijos teikimo sistema, pavyzdžiui, rinkos priežiūros informacine ryšių sistema (ICSMS) ir skubių pranešimų apie pavojingus ne maisto produktus sistema (RAPEX), kuriomis pagal Reglamentą (EB) Nr. 765/2008 jau naudojasi rinkos priežiūros institucijos;

(103) siekiant užtikrinti nuoseklų Europos kibernetinio saugumo sertifikavimo sistemos taikymą reikėtų įsteigti iš nacionalinių kibernetinio saugumo sertifikavimo institucijų arba kitų atitinkamų nacionalinių institucijų atstovų sudarytą EKSSG. Pagrindinės EKSSG užduotys turėtų būti konsultuoti Komisiją ir padėti jai užtikrinti nuoseklų Europos kibernetinio saugumo sertifikavimo sistemos įgyvendinimą ir taikymą, padėti ENISA ir glaudžiai su ja bendradarbiauti rengiant potencialias kibernetinio saugumo sertifikavimo schemas, tinkamai pagrįstais atvejais prašyti ENISA parengti potencialią schemą, priimti ENISA skirtas nuomones dėl potencialių schemų ir Komisijai skirtas nuomones, susijusias su esamų Europos kibernetinio saugumo sertifikavimo schemų palaikymu ir peržiūra. EKSSG turėtų sudaryti palankesnes sąlygas įvairioms nacionalinėms kibernetinio saugumo sertifikavimo institucijoms, atsakingoms už atitikties vertinimo įstaigų įgaliojimą ir Europos kibernetinio saugumo sertifikatų išdavimą, keistis gerąja praktika ir ekspertinėmis žiniomis;

(104) siekdama padidinti informuotumą ir būsimų Sąjungos kibernetinio saugumo sertifikavimo schemų priimtinumą, Komisija gali parengti bendras arba konkrečiam sektoriui skirtas kibernetinio saugumo rekomendacijas, pavyzdžiui, dėl gerosios kibernetinio saugumo praktikos, arba atsakingo saugaus elgesio kibernetinėje erdvėje, ir pabrėžti teigiamą sertifikuotų IRT produktų, paslaugų ir procesų naudojimo poveikį;

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

(106) siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011 ([22]);

(107) turėtų būti naudojama nagrinėjimo procedūra siekiant priimti įgyvendinimo aktus dėl IRT produktų, paslaugų ir procesų Europos kibernetinio saugumo sertifikavimo schemų, dėl ENISA atliekamų tyrimų tvarkos, dėl nacionalinių kibernetinio saugumo sertifikavimo institucijų tarpusavio peržiūros plano, taip pat dėl aplinkybių, formatų ir procedūrų, susijusių su nacionalinių kibernetinio saugumo sertifikavimo institucijų pranešimu Komisijai apie akredituotas atitikties vertinimo įstaigas;

(108) ENISA veikla turėtų būti vertinama reguliariai ir nepriklausomai. Turėtų būti vertinama, ar ENISA vykdo savo tikslus, jos darbo metodai ir jos užduočių aktualumas, ypač jos užduotys, susijusios su operatyviniu bendradarbiavimu Sąjungos lygmeniu. Atliekant tą vertinimą taip pat turėtų būti įvertintas Europos kibernetinio saugumo sertifikavimo sistemos poveikis, veiksmingumas ir efektyvumas. Kalbant apie peržiūrą, Komisija turėtų įvertinti, kaip galima sustiprinti ENISA, kaip informacinio centro, vaidmenį teikiant rekomendacijas ir ekspertines žinias, ir įvertinti ENISA vaidmenį padedant vertinti į Sąjungos rinką patenkančius trečiųjų valstybių IRT produktus, paslaugas ir procesus, kurie neatitinka Sąjungos taisyklių reikalavimų;

([22]) 2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 182/2011, kuriuo nustatomos valstybių narių vykdomos Komisijos naudojimosi įgyvendinimo įgaliojimais kontrolės mechanizmų taisyklės ir bendrieji principai (OL L 55, 2011 2 28, p. 13).

(109) kadangi šio reglamento tikslų valstybės narės negali deramai pasiekti, o dėl jo masto ir poveikio tų tikslų būtų geriau siekti Sąjungos lygmeniu, laikydamasi Europos Sąjungos sutarties (toliau – ES sutartis) 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šiuo reglamentu neviršijama to, kas būtina tiems tikslams pasiekti;

(110) Reglamentas (ES) Nr. 526/2013 turėtų būti panaikintas,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I ANTRAŠTINĖ DALIS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

1. Siekiant užtikrinti tinkamą vidaus rinkos veikimą ir kartu aukštą kibernetinio saugumo, kibernetinio atsparumo ir pasitikėjimo lygį Sąjungoje, šiame reglamente nustatomi:

a) ENISA (Europos Sąjungos kibernetinio saugumo agentūra) tikslai, užduotys ir organizaciniai aspektai ir

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

Sistema, nurodyta pirmos dalies b punkte, taikoma nedarant poveikio tam tikroms kitų Sąjungos teisės aktų nuostatoms dėl savanoriško arba privalomo sertifikavimo.

2. Šis reglamentas nedaro poveikio valstybių narių kompetencijai dėl veiklos, susijusios su visuomenės saugumu, gynyba, nacionaliniu saugumu, nei valstybės veiklai baudžiamosios teisės srityse.

2 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) kibernetinis saugumas– visa veikla, būtina tinklų ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems susijusiems asmenims apsaugoti nuo kibernetinių grėsmių;

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

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

4) esminių paslaugų operatorius– esminių paslaugų operatorius, kaip apibrėžta Direktyvos (ES) 2016/1148 4 straipsnio 4 punkte;

5) skaitmeninių paslaugų teikėjas– skaitmeninių paslaugų teikėjas, kaip apibrėžta Direktyvos (ES) 2016/1148 4 straipsnio 6 punkte;

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

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

8) kibernetinė grėsmė– galima aplinkybė, įvykis arba veiksmas, kuris galėtų pažeisti, sutrikdyti arba kitaip neigiamai paveikti tinklų ir informacines sistemas, tokių sistemų naudotojus ir kitus asmenis;

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

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

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

12) IRT produktas– tinklų ir informacinių sistemų elementas arba elementų grupė;

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

14) IRT procesas– veikla, vykdoma siekiant projektuoti, kurti, teikti ar palaikyti IRT produktą ar paslaugą;

15) akreditavimas– akreditavimas, kaip apibrėžta Reglamento (EB) Nr. 765/2008 2 straipsnio 10 punkte;

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

17) atitikties vertinimas– atitikties vertinimas, kaip apibrėžta Reglamento (EB) Nr. 765/2008 2 straipsnio 12 punkte;

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

19) standartas– standartas, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkte;

20) techninė specifikacija– dokumentas, kuriame nustatyti techniniai reikalavimai, kuriuos turi atitikti IRT produktas, paslauga arba procesas, arba su IRT produktu, paslauga arba procesu susijusios atitikties vertinimo procedūros;

21) saugumo užtikrinimo lygis– pagrindas pasitikėti, kad IRT produktas, paslauga arba procesas atitinka tam tikros Europos kibernetinio saugumo sertifikavimo schemos saugumo reikalavimus, nurodoma, kokiu lygiu IRT produktas, paslauga arba procesas buvo įvertinti; nustatant saugumo užtikrinimo lygį nevertinamas paties IRT produkto, paslaugos ar proceso saugumas;

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

II ANTRAŠTINĖ DALIS

ENISA (EUROPOS SĄJUNGOS KIBERNETINIO SAUGUMO AGENTŪRA)

I SKYRIUS

Įgaliojimai ir tikslai

3 straipsnis

Įgaliojimai

1. ENISA vykdo šiuo reglamentu paskirtas užduotis, kad būtų pasiektas aukštas bendras kibernetinio saugumo lygis visoje Sąjungoje, be kita ko, aktyviai padėdama valstybėms narėms ir Sąjungos institucijoms, įstaigoms, organams ir agentūroms gerinti kibernetinį saugumą. ENISA veikia kaip informacinis centras, kuris teikia rekomendacijas ir ekspertines žinias kibernetinio saugumo klausimais Sąjungos institucijoms, įstaigoms, organams ir agentūroms, taip pat kitiems atitinkamiems Sąjungos suinteresuotiesiems subjektams.

Vykdydama pagal šį reglamentą jai paskirtas užduotis, ENISA prisideda prie vidaus rinkos susiskaidymo mažinimo.

2. ENISA vykdo užduotis, kurios jai paskirtos Sąjungos teisės aktais, kuriais nustatomos valstybių narių įstatymų ir kitų teisės aktų, susijusių su kibernetiniu saugumu, suderinimo priemonės.

3. Vykdydama savo užduotis ENISA veikia nepriklausomai, kartu vengdama veiklos dubliavimo su valstybės narės veikla ir atsižvelgdama į valstybių narių jau turimas ekspertines žinias.

4. ENISA suformuoja savo išteklius, įskaitant techninius ir žmogiškuosius pajėgumus ir įgūdžius, reikalingus vykdyti šiuo reglamentu pavestas užduotis.

4 straipsnis

Tikslai

1. Būdama nepriklausoma, teikdama kokybiškas mokslines ir technines rekomendacijas, pagalbą ir informaciją, užtikrindama savo veiklos procedūrų ir veikimo metodų skaidrumą bei uoliai vykdydama savo užduotis, ENISA veikia kaip kibernetinio saugumo kompetencijos centras.

2. ENISA padeda Sąjungos institucijoms, įstaigoms, organams ir agentūroms, taip pat valstybėms narėms plėtoti ir įgyvendinti su kibernetiniu saugumu susijusią Sąjungos politiką, įskaitant sektorių politiką kibernetinio saugumo srityje.

3. ENISA visoje Sąjungoje remia pajėgumų stiprinimą ir parengtį, padėdama Sąjungos institucijoms, įstaigoms, organams ir agentūroms, taip pat valstybėms narėms ir viešojo bei privačiojo sektorių suinteresuotiesiems subjektams didinti savo tinklų ir informacinių sistemų apsaugą, plėtoti bei gerinti kibernetinį atsparumą ir reagavimo pajėgumus, taip pat plėtoti įgūdžius ir kompetencijas kibernetinio saugumo srityje.

4. ENISA skatina valstybių narių, Sąjungos institucijų, įstaigų, organų ir agentūrų bei atitinkamų privačiojo ir viešojo sektorių suinteresuotųjų subjektų bendradarbiavimą, įskaitant dalijimąsi informacija, ir veiklos koordinavimą Sąjungos lygmeniu su kibernetiniu saugumu susijusiais klausimais.

5. ENISA prisideda prie kibernetinio saugumo pajėgumų didinimo Sąjungos lygmeniu siekiant remti valstybių narių veiksmus užkertant kelią kibernetinėms grėsmėms ir reaguojant į jas, visų pirma tarpvalstybinių incidentų atveju.

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

7. ENISA skatina piliečių, organizacijų ir įmonių aukšto lygio informuotumą apie kibernetinį saugumą, įskaitant kibernetinę higieną ir kibernetinį raštingumą.

II SKYRIUS

Užduotys

5 straipsnis

Sąjungos politikos ir teisės plėtojimas ir įgyvendinimas

ENISA padeda plėtoti ir įgyvendinti Sąjungos politiką ir teisę:

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

2) padėdama valstybėms narėms nuosekliai įgyvendinti Sąjungos politiką ir teisę, susijusią su kibernetiniu saugumu, visų pirma kiek tai susiję su Direktyva (ES) 2016/1148, be kita ko, teikdama nuomones, gaires, rekomendacijas ir dalydamasi geriausia praktika tokiais klausimais, kaip rizikos valdymas, pranešimas apie incidentus ir dalijimasis informacija, taip pat šiuo tikslu palengvindama kompetentingų institucijų keitimąsi geriausia praktika;

3) padėdama valstybėms narėms ir Sąjungos institucijoms, įstaigoms, organams ir agentūroms plėtoti ir propaguoti kibernetinio saugumo politiką, susijusią su visuotinio atvirojo interneto viešosios erdvės prieinamumo arba vientisumo užtikrinimu;

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

5) remdama:

   a) Sąjungos politikos elektroninės atpažinties ir patikimumo užtikrinimo paslaugų srityje plėtojimą ir įgyvendinimą, visų pirma teikdama rekomendacijas ir technines gaires, taip pat palengvindama kompetentingų institucijų keitimąsi geriausia praktika;

   b) didesnio elektroninių ryšių saugumo propagavimą, be kita ko, teikdama ekspertines rekomendacijas ir žinias, taip pat palengvindama kompetentingų institucijų keitimąsi geriausia praktika;

   c) valstybes nares įgyvendinant konkrečius Sąjungos politikos ir teisės kibernetinio saugumo srities aspektus, susijusius su duomenų apsauga ir privatumu, įskaitant, gavus prašymą, rekomendacijų teikimą Europos duomenų apsaugos valdybai;

6) remdama nuolatinę su Sąjungos politika susijusios 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 ar vientisumo pažeidimą, kuriuos priežiūros įstaigos pateikė ENISA pagal Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 ([23]) 19 straipsnio 3 dalį;

   c) viešųjų ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjų perduotais pranešimais apie saugumo incidentus, kuriuos kompetentingos institucijos pateikė ENISA pagal Direktyvos (ES) 2018/1972 40 straipsnį.

([23]) 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 (OL L 257, 2014 8 28, p. 73).

6 straipsnis

Pajėgumų stiprinimas

1. ENISA padeda:

a) valstybėms narėms dedant pastangas siekiant gerinti kibernetinių grėsmių ir incidentų prevenciją, nustatymą, analizę ir reagavimo į juos pajėgumus, suteikdama joms reikiamų žinių ir ekspertinių žinių;

b) valstybėms narėms ir Sąjungos institucijoms, įstaigoms, organams ir agentūroms savanoriškai nustatyti bei įgyvendinti spragų atskleidimo politiką;

c) Sąjungos institucijoms, agentūroms ir įstaigoms dedant pastangas gerinti kibernetinių grėsmių ir incidentų prevenciją, nustatymą, analizę ir reagavimo į juos pajėgumus, visų pirma tinkamai remdama CERT-EU veiklą;

d) valstybėms narėms suformuoti nacionalinėms CSIRT pagal Direktyvos (ES) 2016/1148 9 straipsnio 5 dalį;

e) valstybėms narėms parengti nacionalines tinklų ir informacinių sistemų saugumo strategijas pagal Direktyvos (ES) 2016/1148 7 straipsnio 2 dalį; siekdama populiarinti geriausią praktiką, skatina tų strategijų sklaidą ir stebi jų įgyvendinimo pažangą visoje Sąjungoje;

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

g) nacionalinėms ir Sąjungos CSIRT didinti savo pajėgumus, be kita ko, skatindama dialogą ir keitimąsi informacija, kad būtų užtikrinta, jog, atsižvelgdama į naujausius technikos laimėjimus, kiekviena CSIRT turėtų būtiniausių bendrų pajėgumų ir vykdytų veiklą vadovaudamasi geriausia praktika;

h) valstybėms narėms, reguliariai ir bent kas dvejus metus Sąjungos lygmeniu organizuodama kibernetinio saugumo pratybas, nurodytas 7 straipsnio 5 dalyje, ir teikdama politines rekomendacijas, pagrįstas pratybų vertinimo procesu ir po jų padarytomis išvadomis;

i) atitinkamoms viešosioms įstaigoms, siūlydama mokymus kibernetinio saugumo srityje, kai tikslinga, bendradarbiaudama su suinteresuotaisiais subjektais;

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

2. ENISA remia dalijimąsi informacija sektoriuose ir tarp sektorių, visų pirma išvardytų Direktyvos (ES) 2016/1148 II priede, teikdama rekomendacijas ir konsultacijas apie geriausią praktiką dėl turimų priemonių ir procedūrų, taip pat dėl to, kaip spręsti su dalijimusi informacija susijusius reguliavimo klausimus.

7 straipsnis

Operatyvinis bendradarbiavimas Sąjungos lygmeniu

1. ENISA remia valstybių narių, Sąjungos institucijų, įstaigų, organų ir agentūrų, taip pat suinteresuotųjų subjektų operatyvinį bendradarbiavimą.

2. ENISA operatyviniu lygmeniu bendradarbiauja ir užtikrina sinergiją su Sąjungos institucijomis, įstaigomis, organais ir agentūromis, įskaitant CERT-EU, tarnybas, atsakingas už kovą su kibernetiniais nusikaltimais, ir priežiūros institucijas, atsakingas už privačių bei asmens duomenų apsaugą, siekdama spręsti bendrai rūpimus klausimus, be kita ko:

a) keisdamasi praktine patirtimi ir geriausia praktika;

b) teikdama rekomendacijas ir gaires su kibernetiniu saugumu susijusiais aktualiais klausimais;

c) nustatydama praktinę konkrečių užduočių atlikimo tvarką, pasikonsultavusi su Komisija.

3. ENISA teikia CSIRT tinklo sekretoriato paslaugas pagal Direktyvos (ES) 2016/1148 12 straipsnio 2 dalį ir vykdydama tą funkciją aktyviai remia šio tinklo narių dalijimąsi informacija ir bendradarbiavimą.

4. ENISA remia valstybių narių operatyvinį bendradarbiavimą CSIRT tinkle:

a) patardama, kaip gerinti jų incidentų prevencijos, nustatymo ir reagavimo į juos pajėgumus, ir vienos ar kelių valstybių narių prašymu teikdama rekomendacijas, susijusias su konkrečia kibernetine grėsme;

b) vienos ar kelių valstybių narių prašymu padėdama vertinti didelį arba esminį poveikį turinčius incidentus, teikdama ekspertines žinias ir palengvindama techninį tokių incidentų valdymą, be kita ko, pirmiausia remdama valstybių narių savanorišką dalijimąsi atitinkama informacija ir techniniais sprendimais;

c) analizuodama pažeidžiamumo spragas ir incidentus, remiantis viešai prieinama informacija arba valstybių narių tuo tikslu savanoriškai pateikta informacija;

d) vienos ar kelių valstybių narių prašymu teikdama paramą *ex post* techniniams didelį arba esminį poveikį turinčių incidentų tyrimams pagal Direktyvą (ES) 2016/1148.

Atlikdami tas užduotis ENISA ir CERT-EU vykdo struktūrinį bendradarbiavimą, kad pasinaudotų sinergija ir išvengtų veiklos dubliavimo.

5. ENISA reguliariai organizuoja kibernetinio saugumo pratybas Sąjungos lygmeniu ir padeda jas organizuoti valstybėms narėms, Sąjungos institucijoms, įstaigoms, organams ir agentūroms, kai jos to paprašo. Tokios kibernetinio saugumo pratybos Sąjungos lygmeniu gali apimti techninius, operatyvinius arba strateginius elementus. Kartą per dvejus metus ENISA organizuoja didelio masto visapusiškas pratybas.

ENISA taip pat prisideda prie sektorinių kibernetinio saugumo pratybų organizavimo kartu su atitinkamomis organizacijomis, kurios taip pat dalyvauja Sąjungos lygmens kibernetinio saugumo pratybose, ir, kai tikslinga, padeda tokias pratybas organizuoti.

6. ENISA, glaudžiai bendradarbiaudama su valstybėmis narėmis, reguliariai rengia išsamią ES kibernetinio saugumo techninės padėties ataskaitą dėl incidentų ir grėsmių, grindžiamą atvirųjų šaltinių informacija, pačios Agentūros atliekama analize ir ataskaitomis, kurias Agentūrai, be kita ko, pateikė: valstybių narių CSIRT arba pagal Direktyvą (ES) 2016/1148 įsteigti bendrieji informaciniai centrai (tiek vieni, tiek kiti – savanoriškai); EC3 prie Europolo ir CERT-EU.

7. ENISA padeda Sąjungos ir valstybių narių lygmeniu parengti bendradarbiavimu grindžiamą atsaką į didelio masto tarpvalstybinius incidentus arba krizes, susijusius su kibernetiniu saugumu, daugiausia:

a) apibendrindama ir analizuodama nacionalinių šaltinių ataskaitas, kurios yra viešojoje erdvėje arba kurios pateikiamos savanoriškai, 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) gavus paprašymą, palengvindama techninį tokių incidentų arba krizės valdymą, be kita ko, visų pirma remdama valstybių narių savanorišką dalijimąsi techniniais sprendimais;

d) remdama Sąjungos institucijų, įstaigų, organų ir agentūrų, o, valstybėms narėms paprašius, ir valstybių narių su tokiais incidentais arba krize susijusių viešųjų ryšių veiklą;

e) išbandydama bendradarbiavimo reaguojant į tokius incidentus arba krizes planus Sąjungos lygmeniu ir, gavus prašymą, padėdama valstybėms narėms išbandyti tuos planus nacionaliniu lygmeniu.

8 straipsnis

Rinka, kibernetinio saugumo sertifikavimas ir standartizavimas

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

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

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

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

d) dalyvaudama tarpusavio peržiūrose pagal 59 straipsnio 4 dalį;

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

2. ENISA teikia sekretoriato paslaugas Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupei pagal 22 straipsnio 4 dalį;

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

4. ENISA prisideda prie pakankamų pajėgumų stiprinimo, susijusio su vertinimo ir sertifikavimo procesais, rengdama ir teikdama gaires, taip pat teikdama paramą valstybėms narėms jų prašymu;

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

6. ENISA, bendradarbiaudama su valstybėmis narėmis ir verslo sektoriaus atstovais, 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;

7. ENISA reguliariai analizuoja pagrindines kibernetinio saugumo rinkos paklausos ir pasiūlos tendencijas ir skleidžia informaciją apie jas, kad būtų remiama kibernetinio saugumo rinka Sąjungoje.

9 straipsnis

Žinios ir informacija

Žinių ir informacijos srityje ENISA:

a) vykdo naujausių technologijų analizes ir teikia teminius vertinimus, susijusius su numatomu kibernetinio saugumo srities technologinių inovacijų visuomeniniu, teisiniu, ekonominiu ir reguliavimo poveikiu;

b) atlieka ilgalaikę strategines kibernetinių grėsmių ir incidentų analizes, kad galėtų nustatyti naujausias tendencijas ir padėtų užkirsti kelią incidentams;

c) bendradarbiaudama su ekspertais iš valstybių narių institucijų ir atitinkamais suinteresuotaisiais subjektais, teikia tinklų ir informacinių sistemų, visų pirma infrastruktūros, kuria remiami Direktyvos (ES) 2016/1148 II priede išvardyti sektoriai ir kuria naudojasi tos direktyvos III priede išvardyti skaitmeninių paslaugų teikėjai, saugumo užtikrinimo rekomendacijas, konsultacijas ir geriausią praktiką;

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

e) renka ir analizuoja viešai prieinamą informaciją apie didelius incidentus, taip pat rengia ataskaitas, siekdama teikti konsultacijas piliečiams, organizacijos ir įmonėms visoje Sąjungoje.

10 straipsnis

Informuotumo didinimas ir švietimas

Informuotumo didinimo ir švietimo srityje ENISA:

a) didina visuomenės informuotumą apie kibernetiniam saugumui kylančią riziką ir teikia piliečiams, organizacijoms ir įmonėms skirtas individualių naudotojų gerosios praktikos konsultacijas, be kita ko, dėl kibernetinės higienos ir kibernetinio raštingumo;

b) bendradarbiaudama su valstybėmis narėmis, Sąjungos institucijomis, įstaigomis, organams ir agentūromis ir pramonės sektoriumi, reguliariai organizuoja informavimo kampanijas, kad būtų didinamas kibernetinis saugumas bei šios problemos matomumas Sąjungoje, ir skatina plataus masto viešus debatus;

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

d) remia glaudesnį valstybių narių veiksmų tarpusavio koordinavimą ir keitimąsi geriausia praktika informuotumo ir švietimo kibernetinio saugumo klausimais srityse.

11 straipsnis

Moksliniai tyrimai ir inovacijos

Mokslinių tyrimų ir inovacijų srityje ENISA:

a) konsultuoja Sąjungos institucijas, įstaigas, organus ir agentūras, taip pat valstybes nares dėl poreikio atlikti mokslinius tyrimus kibernetinio saugumo srityje ir dėl šios srities prioritetų, siekiant sudaryti sąlygas veiksmingai reaguoti į esamą ir atsirandančią riziką bei kibernetines grėsmes, be kita ko, susijusias su naujomis ir besiformuojančiomis informacinėmis ir ryšių technologijomis, bei veiksmingai taikyti rizikos prevencijos technologijas;

b) jei Komisija yra suteikusi ENISA atitinkamus įgaliojimus, dalyvauja mokslinių tyrimų ir inovacijų finansavimo programų įgyvendinimo etape arba kaip naudos gavėja;

c) prisideda prie kibernetinio saugumo srityje vykdomos strateginės mokslinių tyrimų ir inovacijų darbotvarkės Sąjungos lygmeniu.

12 straipsnis

Tarptautinis bendradarbiavimas

ENISA remia Sąjungos pastangas bendradarbiauti su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis, be kita ko, atitinkamose tarptautinėse bendradarbiavimo sistemose, kad būtų skatinamas tarptautinis bendradarbiavimas kibernetinio saugumo klausimais:

a) kai tikslinga, dalyvaudama kaip stebėtoja organizuojant tarptautines pratybas, ir analizuodama tokių pratybų rezultatus ir teikdama Valdančiajai tarybai jų ataskaitas;

b) Komisijai paprašius, palengvindama keitimąsi geriausia praktika;

c) Komisijai paprašius, teikdama jai ekspertines žinias;

d) teikdama rekomendacijas ir paramą Komisijai klausimais, susijusiais su susitarimais dėl kibernetinio saugumo sertifikatų tarpusavio pripažinimo su trečiosiomis valstybėmis, bendradarbiaujant su pagal 62 straipsnį įsteigta Europos kibernetinio saugumo sertifikavimo grupe.

III SKYRIUS

ENISA organizacinė struktūra

13 straipsnis

Struktūra

ENISA administracinę ir valdymo struktūrą sudaro:

a) Valdančioji taryba;

b) Vykdomoji valdyba;

c) vykdomasis direktorius;

d) ENISA patariamoji grupė;

e) nacionalinių ryšių palaikymo pareigūnų tinklas.

1 skirsnis

Valdančioji taryba

14 straipsnis

Valdančiosios tarybos sudėtis

1. Valdančiąją tarybą sudaro po vieną narį, paskirtą kiekvienos valstybės narės ir jos paskirtą, ir du narius, paskirtus Komisijos. Visi nariai turi balsavimo teisę.

2. Kiekvienas Valdančiosios tarybos narys turi pakaitinį narį. Tas pakaitinis narys atstovauja nariui šiam nedalyvaujant.

3. Valdančiosios tarybos nariai ir jų pakaitiniai nariai skiriami atsižvelgiant į jų žinias kibernetinio saugumo srityje, taip pat į atitinkamus vadovavimo, 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 lyčių pusiausvyrą Valdančiojoje taryboje.

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

15 straipsnis

Valdančiosios tarybos funkcijos

1. Valdančioji taryba:

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

b) priima 24 straipsnyje nurodyto ENISA bendrojo programavimo dokumento projektą, prieš jį pateikiant Komisijai jos nuomonei gauti;

c) atsižvelgdama į Komisijos nuomonę, priima ENISA bendrąjį programavimo dokumentą;

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

e) priima ENISA metinį biudžetą ir vykdo kitas su ENISA biudžetu susijusias funkcijas pagal IV skyrių;

f) įvertina ir priima konsoliduotąją metinę ENISA veiklos ataskaitą, įskaitant finansines ataskaitas ir aprašymą, kaip ENISA pasiekė savo veiklos rezultatų rodiklius, ne vėliau kaip kitų metų liepos 1 d. pateikia metinę ataskaitą ir jos vertinimą Europos Parlamentui, Tarybai, Komisijai ir Audito Rūmams ir paskelbia metinę ataskaitą viešai;

g) vadovaudamasi 32 straipsniu priima ENISA taikytinas finansines taisykles;

h) atsižvelgdama į įgyvendintinų priemonių sąnaudų ir naudos analizę, priima kovos su sukčiavimu strategiją, kuri proporcingai atitinka sukčiavimo riziką;

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

j) 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;

k) priima savo darbo tvarkos taisykles, įskaitant konkrečių užduočių delegavimą pagal 19 straipsnio 7 dalį;

l) laikydamasi šio straipsnio 2 dalies nuostatų ENISA darbuotojų atžvilgiu naudojasi įgaliojimais, kurie pagal Pareigūnų tarnybos nuostatus (toliau – Pareigūnų tarnybos nuostatai) suteikti paskyrimų tarnybai, o pagal Kitų Europos Sąjungos tarnautojų įdarbinimo sąlygas (toliau – Kitų Europos Sąjungos tarnautojų įdarbinimo sąlygos), nustatytas Tarybos reglamente (EEB, Euratomas, EAPB) Nr. 259/68 ([24]) – tarnybai, įgaliotai sudaryti darbo sutartis (toliau – paskyrimų tarnybos įgaliojimai);

m) priima Pareigūnų tarnybos nuostatų ir kitų tarnautojų įdarbinimo sąlygų įgyvendinimo taisykles laikydamasi Pareigūnų tarnybos nuostatų 110 straipsnyje numatytos tvarkos;

n) skiria vykdomąjį direktorių ir, kai aktualu, pratęsia jo kadenciją arba atleidžia jį iš pareigų pagal 36 straipsnį;

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

p) atsižvelgdama į ENISA veiklos poreikius ir patikimą biudžeto valdymą, priima visus sprendimus dėl ENISA vidaus struktūrų sukūrimo, o kai reikia – dėl tų vidaus struktūrų keitimo;

q) atsižvelgdama į 7 straipsnį, įgalioja sudaryti darbinius susitarimus;

r) atsižvelgdama į 42 straipsnį, įgalioja sudaryti darbinius susitarimus.

2. Vadovaudamasi Pareigūnų tarnybos nuostatų 110 straipsniu, Valdančioji taryba priima Pareigūnų tarnybos nuostatų 2 straipsnio 1 dalimi ir kitų tarnautojų įdarbinimo sąlygų 6 straipsniu grindžiamą sprendimą, kuriuo atitinkami paskyrimų tarnybos įgaliojimai deleguojami vykdomajam direktoriui ir nustatomos sąlygos, kuriomis tas įgaliojimų delegavimas gali būti sustabdytas. Vykdomajam direktoriui leidžiama tuos įgaliojimus perdeleguoti.

([24]) OL L 56, 1968 3 4, p. 1.

3. Prireikus dėl išskirtinių aplinkybių Valdančioji taryba gali priimti sprendimą laikinai sustabdyti paskyrimų tarnybos įgaliojimų delegavimą vykdomajam direktoriui bei vykdomojo direktoriaus perdeleguotus įgaliojimus, ir jais naudotis pati arba deleguoti juos vienam iš savo narių arba darbuotojui, kuris nėra vykdomasis direktorius.

16 straipsnis

Valdančiosios tarybos pirmininkas

Valdančioji taryba dviejų trečdalių narių balsų dauguma iš savo narių išrenka pirmininką ir pirmininko pavaduotoją. Jie skiriami 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 pirmininkas negali vykdyti savo pareigų.

17 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. Vykdomasis direktorius dalyvauja Valdančiosios tarybos posėdžiuose, tačiau neturi teisės balsuoti.

4. ENISA patariamosios grupės nariai gali dalyvauti Valdančiosios tarybos posėdžiuose pirmininko kvietimu, tačiau neturi teisės balsuoti.

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

6. ENISA teikia Valdančiajai tarybai sekretoriato paslaugas.

18 straipsnis

Valdančiosios tarybos balsavimo taisyklės

1. Valdančioji taryba sprendimus priima savo narių balsų dauguma.

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

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

4. Valdančiosios tarybos pirmininkas dalyvauja balsavime.

5. Vykdomasis direktorius nedalyvauja balsavime.

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

19 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 20 straipsnyje nustatytoms vykdomojo direktoriaus pareigoms, padeda ir pataria vykdomajam direktoriui įgyvendinant Valdančiosios tarybos sprendimus dėl administracinių ir biudžeto klausimų.

3. Vykdomąją valdybą sudaro penki nariai. Vykdomosios valdybos nariai skiriami iš Valdančiosios tarybos narių. Vienas iš narių – Valdančiosios tarybos pirmininkas, kuris taip pat gali pirmininkauti Vykdomajai valdybai, o kitas – vienas iš Komisijos atstovų. Skiriant Vykdomosios valdybos narius siekiama joje užtikrinti lyčių pusiausvyrą. 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. Prireikus dėl skubos priežasčių Vykdomoji valdyba gali Valdančiosios tarybos vardu priimti tam tikrus laikinus sprendimus, visų pirma dėl administracinio valdymo klausimų, įskaitant sprendimą sustabdyti paskyrimų tarnybos įgaliojimų delegavimą, ir dėl biudžeto klausimų. Apie tokius laikinus sprendimus nepagrįstai nedelsiant pranešama Valdančiajai tarybai. Tada Valdančioji taryba ne vėliau kaip praėjus trims mėnesiams po sprendimo priėmimo nusprendžia, ar patvirtinti, ar atmesti laikiną sprendimą. Vykdomoji valdyba Valdančiosios valdybos vardu nepriima sprendimų, kurie turi būti priimti dviejų trečdalių Valdančiosios tarybos narių balsų dauguma.

3 skirsnis

Vykdomasis direktorius

20 straipsnis

Vykdomojo direktoriaus pareigos

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

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

3. Vykdomasis direktorius atsako už:

a) kasdienį ENISA veiklos administravimą;

b) Valdančiosios tarybos priimtų sprendimų įgyvendinimą;

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

d) bendrojo programavimo dokumento įgyvendinimą ir ataskaitų dėl jo teikimą Valdančiajai tarybai;

e) konsoliduotosios metinės ENISA veiklos ataskaitos, įskaitant ENISA metinės darbo programos įgyvendinimą, rengimą ir jos pateikimą Valdančiajai tarybai vertinti ir priimti;

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

g) tolesnių veiksmų plano atsižvelgiant į vidaus ar išorės audito ataskaitose pateiktas išvadas, taip pat į OLAF atliktus tyrimus, rengimą ir pažangos ataskaitų teikimą du kartus per metus – Komisijai ir reguliariai – Valdančiajai tarybai;

h) 32 straipsnyje nurodytų ENISA taikytinų finansinių taisyklių projekto rengimą;

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

j) Sąjungos finansinių interesų apsaugą taikant prevencines kovos su sukčiavimu, korupcija ir bet kuria kita neteisėta veikla priemones, vykdant veiksmingus patikrinimus ir, nustačius pažeidimų, susigrąžinant neteisingai išmokėtas sumas bei, kai tikslinga, taikant veiksmingas, proporcingas ir atgrasomas administracines ir finansines sankcijas;

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

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

m) reguliarų keitimąsi informacija su Sąjungos institucijomis, įstaigomis, organais ir agentūromis apie jų veiklą, susijusią su kibernetiniu saugumu, siekiant užtikrinti Sąjungos politikos plėtojimo ir įgyvendinimo nuoseklumą;

n) kitų šiuo reglamentu vykdomajam direktoriui priskirtų užduočių atlikimą.

4. Prireikus, laikydamasis ENISA tikslų ir užduočių, vykdomasis direktorius gali steigti *ad hoc* darbo grupes, sudarytas iš ekspertų, įskaitant ekspertus iš valstybių narių kompetentingų institucijų. Vykdomasis direktorius apie tai iš anksto praneša Valdančiajai tarybai. Procedūros, visų pirma susijusios su darbo grupių sudėtimi, vykdomojo direktoriaus vykdomu darbo grupių ekspertų skyrimu ir darbo grupių veikla, nustatomos ENISA vidaus darbo tvarkos taisyklėse.

5. Prireikus, siekiant veiksmingai ir efektyviai vykdyti ENISA užduotis, remdamasis atitinkama sąnaudų ir naudos analize, vykdomasis direktorius gali nuspręsti vienoje arba keliose valstybėse narėse įsteigti vieną arba kelis vietos skyrius. Prieš nuspręsdamas įsteigti vietos skyrių, vykdomasis direktorius prašo atitinkamos (-ų) valstybės (-ių) narės (-ių), įskaitant valstybę narę, kurioje yra ENISA būstinė, nuomonės ir gauna išankstinį Komisijos ir Valdančiosios tarybos pritarimą. Tais atvejais, kai vykdomojo direktoriaus ir atitinkamų valstybių narių konsultavimosi procese kyla nesutarimų, klausimas perduodamas svarstyti Tarybai. Darbuotojų skaičius visuose vietos skyriuose turi būti kuo mažesnis ir turi neviršyti 40 % bendro ENISA darbuotojų skaičiaus valstybėje narėje, kurioje yra ENISA būstinė. Darbuotojų skaičius kiekviename vietos skyriuje turi neviršyti 10 % bendro ENISA darbuotojų skaičiaus valstybėje narėje, kurioje yra ENISA būstinė.

Vietos skyriuje vykdytinos veiklos apimtis sprendime įsteigti vietos skyrių nustatoma taip, kad būtų išvengta nebūtinų išlaidų ir ENISA administracinių funkcijų dubliavimo.

4 skirsnis

ENISA patariamoji grupė, Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupė ir Nacionalinių ryšių palaikymo pareigūnų tinkas

21 straipsnis

ENISA patariamoji grupė

1. Valdančioji taryba, remdamasi vykdomojo direktoriaus pasiūlymu, skaidriai įsteigia ENISA patariamąją grupę, sudarytą iš pripažintų specialistų, atstovaujančių atitinkamiems suinteresuotiesiems subjektams, pavyzdžiui, IRT sektoriui, visuomenei prieinamų elektroninių ryšių tinklų ar paslaugų teikėjams, MVĮ, esminių paslaugų operatoriams, vartotojų grupėms, akademinės bendruomenės kibernetinio saugumo ekspertams, ir kompetentingų institucijų, apie kurias pranešta pagal Direktyvą (ES) 2018/1972, Europos standartizacijos organizacijų ir teisėsaugos bei duomenų apsaugos priežiūros institucijų atstovų. Valdančioji taryba stengiasi užtikrinti tinkamą lyčių bei geografinę pusiausvyrą, taip pat pusiausvyrą tarp įvairių suinteresuotųjų subjektų grupių.

2. ENISA patariamosios grupės procedūros, visų pirma dėl šios grupės sudėties, 1 dalyje nurodyto vykdomojo direktoriaus pasiūlymo, dydžio, jos narių skyrimo ir ENISA patariamosios grupės veiklos, nustatomos ENISA vidaus darbo tvarkos taisyklėse ir skelbiamos viešai.

3. ENISA patariamajai grupei pirmininkauja vykdomasis direktorius arba kitas vykdomojo direktoriaus kiekvienu atveju atskirai paskirtas asmuo.

4. ENISA patariamosios grupės nariai skiriami dvejų su puse metų kadencijai. Valdančiosios tarybos nariai negali būti ENISA patariamosios grupės nariais. Komisijos ir valstybių narių ekspertai turi teisę dalyvauti ENISA patariamosios grupės posėdžiuose ir jos veikloje. Kitų įstaigų, kurias vykdomasis direktorius laiko svarbiomis, atstovai, kurie nėra ENISA patariamosios grupės nariai, gali būti kviečiami dalyvauti ENISA patariamosios grupės posėdžiuose ir jos veikloje.

5. ENISA patariamoji grupė pataria ENISA jos veiklos vykdymo klausimais, išskyrus šio reglamento III antraštinės dalies taikymą. Ji visų pirma pataria vykdomajam direktoriui dėl ENISA metinės darbo programos pasiūlymo rengimo ir dėl to, kaip užtikrinti ryšius su atitinkamais suinteresuotaisiais subjektais su metine darbo programa susijusiais klausimais.

6. ENISA patariamoji grupė apie savo veiklą nuolat informuoja Valdančiąją tarybą.

22 straipsnis

Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupė

1. Įsteigiama Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupė.

2. Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupę sudaro nariai, atrinkti iš pripažintų ekspertų, atstovaujančių atitinkamiems suinteresuotiesiems subjektams. Komisija Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupės narius atrenka remdamasi ENISA pasiūlymu, surengdama skaidrų bei atvirą konkursą, užtikrindama pusiausvyrą tarp įvairių suinteresuotųjų subjektų grupių, taip pat tinkamą lyčių bei geografinę pusiausvyrą.

3. Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupės:

a) konsultuoja Komisiją strateginiais klausimais, susijusiais su Europos kibernetinio saugumo sertifikavimo sistema;

b) gavus prašymą, konsultuoja ENISA bendraisiais ir strateginiais klausimais, susijusiais su ENISA užduotimis rinkoje, kibernetinio saugumo sertifikavimu ir standartizavimu;

c) padeda Komisijai parengti tęstinę Sąjungos darbo programą, nurodytą 47 straipsnyje;

d) pateikia nuomonę dėl tęstinės Sąjungos darbo programos pagal 47 straipsnio 4 dalį ir

e) skubos atvejais teikia Komisijai ir EKSSG rekomendacijas dėl papildomų sertifikavimo sistemų, neįtrauktų į tęstinę Sąjungos darbo programą, kaip išdėstyta 47 ir 48 straipsniuose, poreikio.

4. Suinteresuotųjų subjektų kibernetinio saugumo sertifikavimo grupei bendrai pirmininkauja Komisijos ir ENISA atstovai, o sekretoriato paslaugas teikia ENISA.

23 straipsnis

Nacionalinių ryšių palaikymo pareigūnų tinklas

1. Valdančioji taryba, remdamasi vykdomojo direktoriaus pasiūlymu, įsteigia iš visų valstybių narių atstovų sudarytą nacionalinių ryšių palaikymo pareigūnų tinklą. Kiekviena valstybė narė paskiria vieną atstovą Nacionalinių ryšių palaikymo pareigūnų tinkle. Gali būti rengiami įvairių ekspertų sudėties Nacionalinių ryšių palaikymo pareigūnų tinklo susitikimai.

2. Nacionalinių ryšių palaikymo pareigūnų tinklas visų pirma sudaro palankesnes sąlygas ENISA ir valstybėms narėms keistis informacija ir remia ENISA skleidžiant informaciją apie jos veiklą, išvadas ir rekomendacijas atitinkamiems suinteresuotiesiems subjektams visoje Sąjungoje.

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

4. Nacionaliniai ryšių palaikymo pareigūnai glaudžiai bendradarbiauja su atitinkamos valstybės narės atstovais Valdančiojoje taryboje, o Nacionalinių ryšių palaikymo pareigūnų tinklas nedubliuoja nei Valdančiosios tarybos, nei kitų Sąjungos forumų darbo.

5. Nacionalinių ryšių palaikymo pareigūnų tinklo funkcijos ir procedūros nustatomos ENISA vidaus darbo tvarkos taisyklėse ir skelbiamos viešai.

5 skirsnis

Veikla

24 straipsnis

Bendrasis programavimo dokumentas

1. ENISA vykdo savo veiklą pagal bendrąjį programavimo dokumentą, į kurį įtraukiamos jos metinė bei daugiametė programos ir kuri apima visą jos planuojamą veiklą.

2. Vykdomasis direktorius kasmet parengia bendrojo programavimo dokumento projektą, kuriame, vadovaujantis Komisijos deleguotojo reglamento (ES) Nr. 1271/2013 ([25]) 32 straipsniu ir atsižvelgiant į Komisijos nustatytas gaires, nustatomos metinė ir daugiametė programos su atitinkamais žmogiškųjų ir finansinių išteklių planais.

3. Valdančioji taryba kasmet ne vėliau kaip lapkričio 30 d. priima 1 dalyje nurodytą bendrąjį programavimo dokumentą ir ne vėliau kaip kitų metų sausio 31 d. nusiunčia jį Europos Parlamentui, Tarybai ir Komisijai; ji taip pat nusiunčia jiems visas paskesnes atnaujintas to dokumento versijas.

4. Bendrasis programavimo dokumentas tampa galutiniu galutinai patvirtinus bendrąjį Sąjungos biudžetą, o prireikus atitinkamai pakoreguojamas.

([25]) 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).

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 turi būti suderinta su 7 dalyje nurodyta daugiamete darbo programa. Joje aiškiai nurodoma, kokios užduotys, palyginti su ankstesniais finansiniais metais, buvo įtrauktos, pakeistos arba išbrauktos.

6. Jei ENISA paskiriama nauja užduotis, Valdančioji taryba iš dalies keičia priimtą metinę darbo programą. Visi esminiai metinės darbo programos pakeitimai priimami laikantis tokios pačios tvarkos, kuri taikoma priimant pirminę metinę darbo programą. Valdančioji taryba gali deleguoti 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, kai tikslinga, atnaujinamas, visų pirma, kai reikia atsižvelgti į 67 straipsnyje nurodyto vertinimo rezultatus.

25 straipsnis

Interesų deklaravimas

1. Kiekvienas Valdančiosios tarybos narys, vykdomasis direktorius ir valstybių narių laikinai deleguoti pareigūnai pateikia įsipareigojimų deklaraciją ir deklaraciją, kurioje nurodoma, ar jie turi tiesioginių arba netiesioginių interesų, kurie galėtų būti laikomi trukdančiais jų nepriklausomumui. 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 darbotvarkės punktais susijusius interesus, kurie galėtų būti laikomi trukdančiais jų nepriklausomumui, ir nedalyvauja diskusijose bei balsavime dėl tokių punktų.

3. ENISA savo vidaus darbo tvarkos taisyklėse nustato praktines priemones, susijusias su taisyklėmis dėl 1 ir 2 dalyse nurodytų interesų deklaracijų.

26 straipsnis

Skaidrumas

1. ENISA vykdo savo veiklą itin skaidriai ir laikydamasi 28 straipsnio.

2. ENISA užtikrina, kad visuomenė ir visos suinteresuotosios šalys gautų tinkamą, objektyvią, patikimą ir lengvai prieinamą informaciją, ypač kiek ji susijusi su Agentūros veiklos rezultatais. Ji taip pat viešai skelbia pagal 25 straipsnį pateiktas interesų deklaracijas.

3. Valdančioji taryba, remdamasi vykdomojo direktoriaus pasiūlymu, gali leisti suinteresuotosioms šalims stebėti, kaip vykdoma tam tikra ENISA veikla.

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

27 straipsnis

Konfidencialumas

1. Nedarant poveikio 28 straipsniui, ENISA neatskleidžia trečiosioms šalims informacijos, kurią ji tvarko arba gauna ir kurią pateiktame pagrįstame prašyme paprašyta laikyti konfidencialia.

2. Valdančiosios tarybos nariai, vykdomasis direktorius, ENISA patariamosios grupės nariai, *ad hoc* darbo grupėse dalyvaujantys išorės ekspertai ir ENISA darbuotojai, įskaitant valstybių narių laikinai deleguotus pareigūnus, turi laikytis konfidencialumo reikalavimų pagal SESV 339 straipsnį, net ir nustoję eiti savo pareigas.

3. ENISA savo vidaus darbo tvarkos taisyklėse nustato praktines priemones 1 ir 2 dalyse nurodytoms konfidencialumo taisyklėms įgyvendinti.

4. Jei to reikia ENISA užduotims vykdyti, Valdančioji taryba nusprendžia leisti ENISA tvarkyti įslaptintą informaciją. Tokiu atveju E priima su Komisijos tarnybomis suderintas saugumo taisykles, kuriose taikomi Komisijos sprendimuose (ES, Euratomas) 2015/443 ([26]) ir (ES, Euratomas) 2015/444 ([27]) nustatyti saugumo principai. Tos saugumo taisyklės apima keitimosi įslaptinta informacija, jos tvarkymo ir saugojimo nuostatas.

28 straipsnis

Galimybė susipažinti su dokumentais

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

2. Valdančioji taryba ne vėliau kaip 2019 m. gruodžio 28 d. patvirtina Reglamento (EB) Nr. 1049/2001 įgyvendinimo priemones.

3. Dėl sprendimų, kuriuos priima ENISA pagal Reglamento (EB) Nr. 1049/2001 8 straipsnį, gali būti teikiamas skundas Europos ombudsmenui pagal SESV 228 straipsnį arba ieškinys Europos Sąjungos Teisingumo Teismui pagal SESV 263 straipsnį.

IV SKYRIUS

ENISA biudžeto sudarymas ir struktūra

29 straipsnis

ENISA biudžeto sudarymas

1. Vykdomasis direktorius kasmet parengia ENISA kitų finansinių metų pajamų ir išlaidų sąmatos projektą ir perduoda jį Valdančiajai tarybai kartu su etatų plano projektu. Pajamos ir išlaidos turi būti subalansuotos.

2. Kasmet Valdančioji taryba, remdamasi pajamų ir išlaidų sąmatos projektu, parengia kitų finansinių metų ENISA pajamų ir išlaidų sąmatą.

3. Valdančioji taryba kasmet ne vėliau kaip sausio 31 d. nusiunčia sąmatą, kuri įtraukiama į bendrojo programavimo dokumento projektą, Komisijai ir trečiosioms valstybėms, su kuriomis Sąjunga yra sudariusi susitarimus, kaip nurodyta 42 straipsnio 2 dalyje.

4. Remdamasi sąmata, kurią pagal SESV 314 straipsnį ji pateikia Europos Parlamentui ir Tarybai, Komisija į Sąjungos bendrojo biudžeto projektą įtraukia išlaidų, kurios, jos manymu, yra reikalingos etatų planui, sąmatas ir iš Sąjungos bendrojo biudžeto mokėtino įnašo sumą.

5. Europos Parlamentas ir Taryba patvirtina ENISA Sąjungos skiriamo įnašo asignavimus.

6. Europos Parlamentas ir Taryba patvirtina ENISA etatų planą.

([26]) 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/443 dėl saugumo Komisijoje (OL L 72, 2015 3 17, p. 41).
([27]) 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).

7. Valdančioji taryba ENISA biudžetą priima kartu su bendruoju programavimo dokumentu. ENISA biudžetas tampa galutiniu galutinai priėmus Sąjungos bendrąjį biudžetą. Kai tikslinga, Valdančioji taryba patikslina ENISA biudžetą ir bendrąjį programavimo dokumentą pagal Sąjungos bendrąjį biudžetą.

30 straipsnis

ENISA biudžeto struktūra

1. Nedarant poveikio kitiems ištekliams, ENISA pajamas sudaro:

a) įnašas iš Sąjungos bendrojo biudžeto;

b) pajamos, asignuotos konkretiems išlaidų straipsniams pagal 32 straipsnyje nurodytas jos finansines taisykles;

c) Sąjungos finansavimas, skiriamas įgaliojimo susitarimais arba skiriant *ad hoc* dotacijas pagal 32 straipsnyje nurodytas ENISA finansines taisykles ir pagal atitinkamų priemonių, kuriomis remiama Sąjungos politika, nuostatas;

d) trečiųjų valstybių, dalyvaujančių ENISA veikloje, kaip numatyta 42 straipsnyje, įnašai;

e) savanoriški valstybių narių įnašai pinigais arba natūra.

Savanoriškus įnašus pagal pirmos dalies e punktą teikiančios valstybės narės dėl to nereikalauja jokių ypatingų teisių ar paslaugų.

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

31 straipsnis

Biudžeto vykdymas

1. Už ENISA biudžeto vykdymą atsako vykdomasis direktorius.

2. Komisijos vidaus auditorius ENISA atžvilgiu naudojasi tais pačiais įgaliojimais, kaip ir Komisijos departamentų atžvilgiu.

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

4. Gavęs Audito Rūmų pastabas dėl ENISA preliminarių finansinių ataskaitų pagal Europos Parlamento ir Tarybos reglamento (ES, Euratomas) 2018/1046 ([28]) 246 straipsnį, ENISA apskaitos pareigūnas savo atsakomybe parengia Agentūros galutines finansines ataskaitas ir pateikia jas Valdančiajai tarybai, kad ši pareikštų nuomonę.

5. Valdančioji taryba pateikia nuomonę dėl ENISA finansinių ataskaitų.

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

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

([28]) 2018 m. liepos 18 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2018/1046 dėl Sąjungos bendrajam biudžetui taikomų finansinių taisyklių, kuriuo iš dalies keičiami reglamentai (ES) Nr. 1296/2013, (ES) Nr. 1301/2013, (ES) Nr. 1303/2013, (ES) Nr. 1304/2013, (ES) Nr. 1309/2013, (ES) Nr. 1316/2013, (ES) Nr. 223/2014, (ES) Nr. 283/2014 ir Sprendimas Nr. 541/2014/ES, bei panaikinamas Reglamentas (ES, Euratomas) Nr. 966/2012 (OL L 193, 2018 7 30, p. 1).

8. Tą pačią dieną, kurią apskaitos pareigūnas išsiunčia savo galutines ENISA finansines ataskaitas, jis taip pat išsiunčia vadovybės pareiškimo raštą, kuriame apžvelgiamos tos galutinės ataskaitos, Audito Rūmams, o jų kopiją – Komisijos apskaitos pareigūnui.

9. Ne vėliau kaip N + 1 metų lapkričio 15 d. vykdomasis direktorius paskelbia galutines ENISA finansines ataskaitas *Europos Sąjungos oficialiajame leidinyje*.

10. Ne vėliau kaip N + 1 metų rugsėjo 30 d. vykdomasis direktorius išsiunčia Audito Rūmams atsakymą į jų pateiktas pastabas ir taip pat išsiunčia to atsakymo kopiją Valdančiajai tarybai ir Komisijai.

11. Europos Parlamento prašymu vykdomasis direktorius jam pateikia visą informaciją, kurios reikia siekiant sklandžiai taikyti atitinkamų finansinių metų biudžeto įvykdymo patvirtinimo procedūrą, atsižvelgiant į Reglamento (ES, Euratomas) 2018/1046 261 straipsnio 3 dalį.

12. Europos Parlamentas, remdamasis Tarybos rekomendacija, anksčiau nei N + 2 metų gegužės 15 d. patvirtina, kad vykdomasis direktorius įvykdė N metų biudžetą.

32 straipsnis

Finansinės taisyklės

Pasikonsultavusi su Komisija, Valdančioji taryba priima ENISA taikytinas finansines taisykles. Jos negali nukrypti nuo Deleguotojo reglamento (ES) Nr. 1271/2013, nebent taip nukrypti aiškiai reikia dėl ENISA veiklos ir yra gautas išankstinis Komisijos sutikimas.

33 straipsnis

Kova su sukčiavimu

1. Siekiant sudaryti palankesnes sąlygas kovoti su sukčiavimu, korupcija ir kita neteisėta veikla pagal Europos Parlamento ir Tarybos reglamentą (ES, Euratomas) Nr. 883/2013 ([29]), ENISA ne vėliau kaip 2019 m. gruodžio 28 d. 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 ([30]) ir priima visiems ENISA darbuotojams taikytinas atitinkamas nuostatas naudodamasi to Susitarimo priede nustatytu modeliu.

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

3. OLAF gali atlikti tyrimus, įskaitant patikrinimus ir inspektavimus vietoje, laikydamasi Europos Parlamento ir Tarybos reglamento (ES, Euratomas) Nr. 883/2013 ir Tarybos reglamento (Euratomas, EB) Nr. 2185/96 ([31]) nuostatų ir procedūrų, kad nustatytų sukčiavimo, korupcijos arba bet kurios kitos neteisėtos veiklos, susijusios su ENISA finansuojamomis dotacijomis ar sutartimis ir kenkiančios Sąjungos finansiniams interesams, atvejus.

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

([29]) 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).

([30]) OL L 136, 1999 5 31, p. 15.

([31]) 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).

V SKYRIUS

Darbuotojai

34 straipsnis

Bendrosios nuostatos

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

35 straipsnis

Privilegijos ir imunitetas

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

36 straipsnis

Vykdomasis direktorius

1. Vykdomasis direktorius įdarbinamas kaip ENISA laikinasis darbuotojas pagal Kitų tarnautojų įdarbinimo sąlygų 2 straipsnio a punktą.

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

3. Sudarant darbo sutartį su vykdomuoju direktoriumi, ENISA atstovauja Valdančiajai tarybai pirmininkaujantis asmuo.

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 vykdomojo direktoriaus veiklos rezultatų vertinimą ir būsimas ENISA užduotis bei iššūkius.

6. Sprendimus dėl vykdomojo direktoriaus skyrimo, kadencijos pratęsimo arba atleidimo iš pareigų Valdančioji taryba priima pagal į 18 straipsnio 2 dalį.

7. Remdamasi Komisijos pasiūlymu, kuriame atsižvelgiama į 5 dalyje nurodytą vertinimą, Valdančioji taryba gali vieną kartą pratęsti vykdomojo direktoriaus kadenciją penkeriems metams.

8. Apie ketinimą pratęsti vykdomojo direktoriaus kadenciją Valdančioji taryba informuoja Europos Parlamentą. Trijų mėnesių laikotarpiu 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, nedalyvauja kitoje atrankos į tą pačią pareigybę procedūroje.

10. Vykdomasis direktorius gali būti pašalintas iš pareigų tik Valdančiosios tarybos sprendimu, priimtu remiantis Komisijos pasiūlymu.

37 straipsnis

Deleguotieji nacionaliniai ekspertai ir kiti darbuotojai

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

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

VI SKYRIUS

Bendrosios nuostatos dėl ENISA

38 straipsnis

ENISA teisinis statusas

1. ENISA yra juridinio asmens statusą turinti Sąjungos įstaiga.

2. Kiekvienoje valstybėje narėje ENISA naudojasi plačiausiu veiksnumu, suteikiamu juridiniams asmenims pagal nacionalinę teisę. Visų pirma, ji gali įsigyti kilnojamojo ir nekilnojamojo turto arba juo disponuoti, taip pat būti šalimi teismo procese, arba pasinaudoti abiem galimybėmis.

3. ENISA atstovauja jos vykdomasis direktorius.

39 straipsnis

ENISA atsakomybė

1. ENISA sutartinę atsakomybę reglamentuoja atitinkamai sutarčiai taikytina teisė.

2. Europos Sąjungos Teisingumo Teismas turi jurisdikciją priimti sprendimus pagal bet kurią ENISA sudarytos sutarties nuostatą dėl arbitražo.

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

4. Europos Sąjungos Teisingumo Teismas turi jurisdikciją spręsti ginčus dėl 3 dalyje nurodytos žalos atlyginimo.

5. Asmeninę darbuotojų atsakomybę ENISA atžvilgiu reglamentuoja atitinkamos ENISA darbuotojams taikomos nuostatos.

40 straipsnis

Nuostatos dėl kalbų

1. ENISA taikomas Tarybos reglamentas Nr. 1 ([32]). Valstybės narės ir kitos jų paskirtos įstaigos į Agentūrą gali kreiptis ir atsakymą gauti jų pasirinkta Sąjungos institucijų oficialiąja kalba.

2. ENISA veikimui būtinas vertimo raštu paslaugas teikia Europos Sąjungos įstaigų vertimo centras.

41 straipsnis

Asmens duomenų apsauga

1. ENISA vykdomam asmens duomenų tvarkymui taikomas Reglamentas (ES) 2018/1725.

2. Valdančioji taryba priima Reglamento (ES) 2018/1725 45 straipsnio 3 dalyje nurodytas įgyvendinimo taisykles. Valdančioji taryba gali priimti papildomas priemones, kurių reikia, kad ENISA taikytų Reglamentą (ES) 2018/1725.

([32]) Tarybos reglamentas Nr. 1, nustatantis kalbas, kurios turi būti vartojamos Europos ekonominėje bendrijoje (OL 17, 1958 10 6, p. 385).

42 straipsnis

Bendradarbiavimas su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

1. Tiek, kiek būtina šiame reglamente išdėstytiems tikslams pasiekti, ENISA gali bendradarbiauti su trečiųjų valstybių kompetentingomis institucijomis ir (arba) su tarptautinėmis organizacijomis. Tuo tikslu ENISA gali, gavusi Komisijos patvirtinimą, sudaryti darbinius susitarimus su tomis trečiųjų valstybių valdžios institucijomis ir tarptautinėmis organizacijomis. Tais darbiniais susitarimais nesukuriami teisinių pareigų Sąjungai ir jos valstybėms narėms.

2. ENISA veikloje gali dalyvauti trečiosios valstybės, kurios tuo tikslu yra sudariusios susitarimus su Sąjunga. Pagal atitinkamas tokių darbinių susitarimų nuostatas nustatoma tvarka, kuria apibrėžiamas, visų pirma, tų trečiųjų valstybių dalyvavimo ENISA veikloje pobūdis, mastas ir būdai, įskaitant nuostatas, susijusias su dalyvavimu ENISA vykdomose iniciatyvose, finansiniais įnašais ir darbuotojais. Tų darbinių susitarimų nuostatos dėl darbuotojų visais atvejais turi atitikti Pareigūnų tarnybos nuostatus ir Kitų Europos Sąjungos tarnautojų įdarbinimo sąlygas.

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

43 straipsnis

Saugumo taisyklės dėl neskelbtinos neįslaptintos informacijos ir įslaptintos informacijos apsaugos

Pasikonsultavusi su Komisija, ENISA priima saugumo taisykles, pagal kurias taikomi saugumo principai, išdėstyti Komisijos saugumo taisyklėse, skirtose neskelbtinos neįslaptintos informacijos ir ESĮI apsaugai užtikrinti, kaip nustatyta sprendimuose (ES, Euratomas) 2015/443 ir (ES, Euratomas) 2015/444. ENISA saugumo taisyklės apima nuostatas dėl keitimosi tokia informacija, jos tvarkymo ir saugojimo.

44 straipsnis

Susitarimas dėl būstinės ir veiklos sąlygos

1. ENISA ir valstybės narės, kurioje yra jos būstinė susitarime dėl būstinės, sudarytame gavus Valdančiosios tarybos patvirtinimą, nustatomos reikiamos nuostatos dėl ENISA įkūrimo priimančioje valstybėje narėje ir patalpų, kurias turi suteikti ta valstybė narė, taip pat toje priimančiojoje valstybėje narėje ENISA vykdomajam direktoriui, Valdančiosios tarybos nariams, darbuotojams ir jų šeimos nariams taikytinos konkrečios taisyklės.

2. ENISA priimančioji valstybė narė sudaro geriausias įmanomas sąlygas, kad būtų užtikrintas tinkamas ENISA veikimas, atsižvelgiant į vietos prieinamumą, tinkamas galimybes mokytis darbuotojų vaikams, tinkamas galimybes įsidarbinti, naudotis socialinės apsaugos ir sveikatos priežiūros paslaugomis darbuotojų vaikams ir sutuoktiniams.

45 straipsnis

Administracinė kontrolė

ENISA veiklą pagal SESV 228 straipsnį prižiūri Europos ombudsmenas.

III ANTRAŠTINĖ DALIS

KIBERNETINIO SAUGUMO SERTIFIKAVIMO SISTEMA

46 straipsnis

Europos kibernetinio saugumo sertifikavimo sistema

1. Siekiant gerinti vidaus rinkos veikimo sąlygas didinant kibernetinio saugumo lygį Sąjungoje ir sudarant sąlygas Sąjungos lygmeniu suderintai taikyti Europos kibernetinio saugumo sertifikavimo schemas, kad būtų sukurta IRT produktų, paslaugų ir procesų bendroji skaitmeninė rinka, nustatoma Europos kibernetinio saugumo sertifikavimo sistema.

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

47 straipsnis

Tęstinė Sąjungos darbo programa Europos kibernetinio saugumo sertifikavimo srityje

1. Komisija paskelbia tęstinę Sąjungos darbo programą Europos kibernetinio saugumo sertifikavimo srityje (toliau – tęstinė Sąjungos darbo programa), kurioje nustatomi būsimų Europos kibernetinio saugumo sertifikavimo schemų strateginiai prioritetai.

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

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

a) tuo, kad yra sukurtos ir plėtojamos nacionalinės kibernetinio saugumo sertifikavimo schemos, apimančios konkrečią IRT produktų, paslaugų ar procesų kategoriją, ypač kiek tai susiję su susiskaidymo rizika;

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

c) rinkos paklausa;

d) kibernetinių grėsmių raidos pokyčiais;

e) EKSSG prašymu parengti konkrečią potencialią schemą.

4. Komisija tinkamai atsižvelgia į EKSSG ir Suinteresuotųjų subjektų sertifikavimo grupės paskelbtas nuomones dėl tęstinės Sąjungos darbo programos projekto.

5. Pirmoji tęstinė Sąjungos darbo programa paskelbiama ne vėliau kaip 2020 m. birželio 28 d. Tęstinė Sąjungos darbo programa atnaujinama ne rečiau kaip kas trejus metus arba prireikus dažniau.

48 straipsnis

Prašymas parengti Europos kibernetinio saugumo sertifikavimo schemą

1. Komisija gali prašyti ENISA parengti potencialią schemą ir arba peržiūrėti esamą Europos kibernetinio saugumo sertifikavimo schemą remiantis tęstine Sąjungos darbo programa.

2. Tinkamai pagrįstais atvejais Komisija arba EKSSG gali prašyti ENISA parengti potencialią schemą arba peržiūrėti esamą Europos kibernetinio saugumo sertifikavimo schemą, kuri nėra įtraukta tęstinę Sąjungos darbo programą. Tokiu atveju tęstinė Sąjungos darbo programa atitinkamai atjauninama.

49 straipsnis

Europos kibernetinio saugumo sertifikavimo schemos rengimas, priėmimas ir peržiūra

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

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

3. Rengdama potencialias schemas ENISA konsultuojasi su visais atitinkamais suinteresuotaisiais subjektais, taikydama formalią, atvirą, skaidrią ir įtraukią konsultacijų procedūrą.

4. Kiekvienos potencialios schemos atveju ENISA pagal 20 straipsnio 4 dalį įsteigia *ad hoc* darbo grupę, kad ENISA būtų teikiamos konkrečios rekomendacijos ir ekspertinės žinios.

5. ENISA glaudžiai bendradarbiauja su EKSSG. EKSSG teikia ENISA pagalbą ir ekspertų konsultacijas, susijusias su potencialios schemos rengimu, ir priima nuomonę dėl potencialios schemos.

6. ENISA kuo labiau atsižvelgia į EKSSG nuomonę prieš pateikdama pagal 3, 4 ir 5 dalis parengtą potencialią schemą Komisijai. EKSSG nuomonė nėra ENISA privaloma, o jei ji nepateikiama, tai netrukdo ENISA perduoti potencialią schemą Komisijai.

7. Komisija, remdamasi ENISA pasiūlyta potencialia schema, gali priimti įgyvendinimo aktus, kuriuose būtų numatytos 51, 52 ir 54 straipsnių reikalavimus atitinkančios IRT produktų, IRT paslaugų ir IRT paslaugų Europos kibernetinio saugumo sertifikavimo schemos. Tie įgyvendinimo aktai priimami pagal 66 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.

8. ENISA bent kas penkerius metus įvertina kiekvieną priimtą Europos kibernetinio saugumo sertifikavimo schemą, atsižvelgdama į grįžtamąją informaciją, gautą iš suinteresuotųjų subjektų. Jei manoma, kad tai būtina, Komisija arba EKSSG gali prašyti ENISA pradėti patikslintos potencialios schemos rengimo procesą pagal 48 straipsnį ir šį straipsnį.

50 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų interneto svetainė

1. ENISA tvarko specialią interneto svetainę, kurioje pateikiama informacija apie Europos kibernetinio saugumo sertifikavimo schemas, Europos kibernetinio saugumo sertifikatus ir ES atitikties pareiškimus ir jų reklama, be kita ko, kiek tai susiję su nebegaliojančiomis Europos kibernetinio saugumo sertifikavimo schemomis, su panaikintais ir pasibaigusio galiojimo Europos kibernetinio saugumo sertifikatais ir ES atitikties pareiškimais, taip pat nuorodų į kibernetinio saugumo informaciją, teikiamą pagal 55 straipsnį, saugykla.

2. Kai taikytina, 1 dalyje nurodytoje interneto svetainėje taip pat nurodomos tos nacionalinės kibernetinio saugumo sertifikavimo schemos, kurias pakeitė Europos kibernetinio saugumo sertifikavimo schema.

51 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų saugumo tikslai

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

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

b) saugomi, perduodami ar kitaip tvarkomi duomenys būtų apsaugoti nuo atsitiktinio ar neteisėto jų sunaikinimo, praradimo ar pakeitimo arba jų neprieinamumo IRT produkto, paslaugos ar proceso viso gyvavimo ciklo metu;

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

d) būtų nustatomi ir dokumentuojami visi žinomi priklausomumo atvejai ir pažeidžiamumo spragos;

e) būtų registruojama, prie kurių duomenų, paslaugų ar funkcijų a buvo gauta prieiga, kuriais jų buvo pasinaudota ar jie buvo kitaip tvarkomi, kada ir kas tai padarė;

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

g) būtų tikrinama, kad IRT produktai, paslaugos ar procesai neturėtų žinomų pažeidžiamumo spragų;

h) įvykus fiziniam ar techniniam incidentui, būtų laiku atkuriamas duomenų, paslaugų ir funkcijų prieinamumas ir prieiga prie jų;

i) būtų užtikrintas standartizuotasis ir integruotasis IRT produktų, paslaugų ar procesų saugumas;

j) IRT produktai, paslaugos ar procesai būtų teikiami su atnaujinta programine įranga ir aparatine įranga, kuriose nėra viešai žinomų pažeidžiamumo spragų ir kurios yra aprūpintos saugaus naujinimo mechanizmais.

52 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, paslaugoms ir procesams taikomų saugumo užtikrinimo lygių: bazinis, pakankamai aukštas arba aukštas. Saugumo užtikrinimo lygis turi atitikti su IRT produkto, paslaugos arba proceso numatomu naudojimu susijusios rizikos lygį, apibrėžiamą atsižvelgiant į incidento tikimybę ir poveikį.

2. Europos kibernetinio saugumo sertifikatuose ir ES atitikties pareiškimuose nurodomas užtikrinimo lygis, numatytas Europos kibernetinio saugumo sertifikavimo sistemoje, pagal kurią išduodamas Europos kibernetinio saugumo sertifikatas arba ES atitikties pareiškimas.

3. Kiekvieną saugumo užtikrinimo lygį atitinkantys saugumo reikalavimai nustatomi atitinkamoje Europos kibernetinio saugumo sertifikavimo schemoje, įskaitant atitinkamas saugumo funkcines galimybes ir atitinkamą vertinimo, kuris turi būti atliktas IRT produktui, paslaugai ar procesui, griežtumą ir išsamumą.

4. Sertifikate arba ES atitikties pareiškime nurodomos techninės specifikacijos, standartai ir su jomis susijusios procedūros, įskaitant technines kontrolės priemones, kurių paskirtis yra sumažinti kibernetinio saugumo incidentų riziką arba jiems užkirsti kelią.

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

6. Europos kibernetinio saugumo sertifikatu, kuriame nurodytas pakankamai aukštas saugumo užtikrinimo lygis, garantuojama, kad IRT produktai, paslaugos ir procesai, dėl kurių išduotas tas sertifikatas, tenkina atitinkamus saugumo reikalavimus, įskaitant saugumo funkcines galimybes, ir kad jie buvo įvertinti tokiu lygiu, kad būtų kuo labiau sumažinta žinoma kibernetinė rizika ir kibernetinių incidentų bei kibernetinių išpuolių, kuriuos vykdo ribotų gebėjimų ir ribotų išteklių turintys subjektai, pavojus. Atliktini įvertinimo veiksmai turi apimti bent šiuos veiksmus: įvertinimą, ar nėra viešai žinomų pažeidžiamumo spragų, ir išbandoma, ar IRT produktuose, paslaugose ar procesuose tinkamai įgyvendinamos reikiamos saugumo funkcinės galimybės. Jei tokie įvertinimo veiksmai netaikytini, turi būti atlikti pakaitiniai lygiavertį poveikį turintys įvertinimo veiksmai.

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

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

53 straipsnis

Savarankiškas atitikties vertinimas

1. Europos kibernetinio saugumo sertifikavimo schemoje gali būti numatyta galimybė, kad savarankiškas atitikties vertinimas vykdomas tik IRT produktų, paslaugų ar procesų gamintojo ar teikėjo atsakomybe. Savarankiškas atitikties vertinimas taikytinas tik nedidelės rizikos IRT produktams, paslaugoms ir procesams, atitinkantiems bazinį saugumo užtikrinimo lygį.

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

3. IRT produktų gamintojas, paslaugų arba procesų teikėjas privalo atitinkamoje Europos kibernetinio saugumo sertifikavimo schemoje nurodytą laikotarpį saugoti ES atitikties pareiškimą ir visos kitos aktualios informacijos, susijusios su IRT produktų, paslaugų ar procesų atitiktimi schemai, techninę dokumentaciją, kad galėtų juos pateikti nacionalinei kibernetinio saugumo sertifikavimo institucijai, nurodytai 58 straipsnyje. ES atitikties pareiškimo kopija pateikiama nacionalinei kibernetinio saugumo sertifikavimo institucijai ir ENISA.

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

5. ES atitikties pareiškimai pripažįstami visose valstybėse narėse.

54 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų elementai

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

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

b) aiškus schemos paskirties aprašymas, taip pat aprašymas, kaip pasirinkti standartai, vertinimo metodai ir saugumo užtikrinimo lygiai atitinka numatomų schemos naudotojų poreikius;

c) nuoroda į tarptautinius, europinius ar nacionalinius standartus, kurie taikomi vertinime, arba jeigu tokių standartų nėra arba jie netinkami, į technines specifikacijas, atitinkančias Reglamento (ES) Nr. 1025/2012 II priede nustatytus reikalavimus, arba, jeigu tokių specifikacijų nėra, į technines specifikacijas arba kitus kibernetinio saugumo reikalavimus, apibrėžtus Europos kibernetinio saugumo sertifikavimo schemoje;

d) kai taikytina, vienas ar daugiau saugumo užtikrinimo lygių;

e) informacija, ar pagal schemą leidžiama atlikti savarankišką atitikties vertinimą;

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

g) naudojami specifiniai vertinimo kriterijai ir metodai, įskaitant vertinimo rūšis, siekiant įrodyti, kad yra pasiekti konkretūs 51 straipsnyje nurodyti tikslai;

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

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

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

k) kai taikytina, Europos kibernetinio saugumo sertifikatų išdavimo, išlaikymo, galiojimo pratęsimo ir atnaujinimo sąlygos, taip pat sertifikavimo taikymo srities išplėtimo arba susiaurinimo sąlygos;

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

m) taisyklės, nustatančios, kaip turi būti pranešama apie anksčiau nenustatytas IRT procesų, produktų ir paslaugų kibernetinio saugumo pažeidžiamumo spragas ir kaip jos turi būti šalinamos;

n) kai taikytina, taisyklės dėl atitikties vertinimo įstaigų įrašų laikymo;

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

p) išduodamo Europos kibernetinio saugumo sertifikato arba ES atitikties pareiškimo turinys ir forma;

q) laikotarpis, kurį turi būti prieinamas ES atitikties pareiškimas, techninė dokumentacija ir visa kita aktuali informacija, kurią IRT produktų gamintojas ar paslaugų teikėjas turi padaryti prieinamą turi galėti pateikti susipažinti ir;

r) ilgiausias pagal schemą išduotų Europos kibernetinio saugumo sertifikatų galiojimo laikotarpis;

s) suteiktų, pakeistų ar atšauktų Europos kibernetinio saugumo sertifikatų, išduotų pagal schemą, atskleidimo politika;

t) sertifikavimo schemų tarpusavio pripažinimo su trečiosiomis valstybėmis sąlygos;

u) kai taikytina, taisyklės, susijusios su visais tarpusavio vertinimo mechanizmais, nustatytais schemoje, skirtoje institucijoms ar įstaigoms, išduodančioms Europos kibernetinio saugumo sertifikatus dėl aukšto saugumo užtikrinimo lygio pagal 56 straipsnio 6 dalį. Tokiais mechanizmais nedaromas poveikis 59 straipsnyje numatytai tarpusavio peržiūrai;

v) formatas ir procedūros, kurių IRT produktų, paslaugų ar procesų gamintojai ar teikėjai turi laikytis teikdami ir atnaujindami papildomą informaciją apie kibernetinį saugumą pagal 55 straipsnį.

2. Nurodyti Europos kibernetinio saugumo sertifikavimo schemos reikalavimai turi neprieštarauti jokiems taikytiniems teisiniams reikalavimams, visų pirma suderintais Sąjungos teisės aktais nustatytiems reikalavimams.

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

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

55 straipsnis

Su sertifikuotais IRT produktais, paslaugomis ir procesais susijusi papildoma kibernetinio saugumo informacija

1. Sertifikuotų IRT produktų, paslaugų ar procesų arba IRT produktų, paslaugų ar procesų, kuriems išduotas ES atitikties pareiškimas, gamintojas arba teikėjas, viešai pateikia tokią papildomą kibernetinio saugumo informaciją:

a) konsultacijas ir rekomendacijas siekiant padėti galutiniams naudotojams IRT produktus ar paslaugas saugiai konfigūruoti, instaliuoti, įtaisyti, naudoti ir prižiūrėti;

b) laikotarpį, per kurį galutiniams naudotojams bus teikiama saugumo priežiūra, visų pirma, kalbant apie su kibernetiniu saugumu susijusių naujinių teikimą;

c) gamintojo arba teikėjo kontaktinę informaciją ir priimtinus informacijos apie pažeidžiamumo spragas gavimo iš galutinių naudotojų ir saugumo srities tyrėjų metodus;

d) nuorodą į internetines duomenų saugyklas, kuriose vardijamos viešai atskleistos pažeidžiamumo spragos, susijusios su IRT produktu, paslauga ar procesu, ir atitinkamos kibernetinio saugumo rekomendacijos.

2. Šio straipsnio 1 dalyje nurodyta informacija pateikiama elektronine forma, sudaroma galimybė ja naudotis ir ji prireikus atnaujinama bent jau iki atitinkamo Europos kibernetinio saugumo sertifikato arba ES atitikties pareiškimo galiojimo pabaigos.

56 straipsnis

Kibernetinio saugumo sertifikavimas

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

2. Kibernetinio saugumo sertifikavimas yra savanoriškas, išskyrus atvejus, kai Sąjungos ar valstybių narių teisėje nustatyta kitaip.

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

Pirmiausia Komisija daugiausia dėmesio skiria Direktyvos (ES) 2016/1148 II priede išvardytiems sektoriams, kurių atžvilgiu vertinimas turi būti atliktas ne vėliau kaip praėjus dvejiems metams po pirmos Europos kibernetinio saugumo sertifikavimo schemos priėmimo.

Rengdama vertinimą, Komisija:

a) atsižvelgia į su sąnaudomis susijusį priemonių poveikį tokių IRT produktų gamintojams ar paslaugų teikėjams ir naudotojams, taip pat numatomo didesnio saugumo visuomeninę ar ekonominę naudą tiksliniams IRT produktams, paslaugoms ir procesams;

b) atsižvelgia į atitinkamų valstybių narių ir trečiųjų šalių teisės aktų buvimą ir taikymą;

c) vykdo atvirą, skaidrų ir įtraukų konsultavimosi procesą su visais atitinkamais suinteresuotaisiais subjektais ir valstybėmis narėmis;

d) atsižvelgia į įgyvendinimo terminus, pereinamojo laikotarpio priemones ir laikotarpius, visų pirma dėl galimo priemonės poveikio IRT produktų gamintojams, paslaugų teikėjams ar procesų vykdytojams, įskaitant MVĮ;

e) siūlo greičiausią ir veiksmingiausią būdą, kaip įgyvendinti perėjimą nuo savanoriškų prie privalomų sertifikavimo schemų.

4. Europos kibernetinio saugumo sertifikatą, pagal šį straipsnį patvirtinantį bazinį arba pakankamai aukštą saugumo užtikrinimo lygį, išduoda 60 straipsnyje nurodytos atitikties vertinimo įstaigos remdamosi kriterijais, įtrauktais į Europos kibernetinio saugumo sertifikavimo schemą, Komisijos patvirtintą pagal 49 straipsnį.

5. Nukrypstant nuo 4 dalies, tinkamai pagrįstais atvejais Europos kibernetinio saugumo sertifikavimo schemoje gali būti numatyta, kad Europos kibernetinio saugumo sertifikatą pagal tą schemą gali išduoti tik viešoji įstaiga, jeigu nurodomos tokį nukrypimą pagrindžiančios priežastys. Tokia įstaiga yra viena iš šių įstaigų:

a) 58 straipsnio 1 dalyje nurodyta nacionalinė kibernetinio saugumo sertifikavimo institucija arba

b) viešoji įstaiga, kuri pagal 60 straipsnio 1 dalį yra akredituota kaip atitikties vertinimo įstaiga.

6. Kai pagal 49 straipsnį priimtoje Europos kibernetinio saugumo sertifikavimo schemoje reikalaujama aukšto saugumo užtikrinimo lygio, Europos kibernetinio saugumo sertifikatą pagal tą schemą gali išduoti tik nacionalinė kibernetinio saugumo sertifikavimo institucija arba atitikties vertinimo įstaiga šiais atvejais:

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

b) nacionalinė kibernetinio saugumo sertifikavimo institucija atitikties vertinimo įstaigai turi būti delegavusi bendrus įgaliojimus dėl tokių Europos kibernetinio saugumo sertifikatų išdavimo.

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

8. Europos kibernetinio saugumo sertifikato turėtojas informuoja 7 dalyje nurodytą instituciją arba įstaigą apie su sertifikuotu IRT produktu, paslauga arba procesu, susijusias vėliau nustatytas pažeidžiamumo spragas ar neatitikties atvejus, kurie gali daryti poveikį su sertifikavimu susijusiems reikalavimams. Ta institucija ar įstaiga nepagrįstai nedelsdama perduoda tą informaciją nacionalinei kibernetinio saugumo sertifikavimo institucijai.

9. Europos kibernetinio saugumo sertifikatai išduodami konkrečios Europos kibernetinio saugumo sertifikavimo schemos nustatytam laikotarpiui ir gali būti atnaujinami, jeigu ir toliau tenkinami susiję reikalavimai.

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

57 straipsnis

Nacionalinės kibernetinio saugumo sertifikavimo schemos ir sertifikatai

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

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

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

4. Siekiant išvengti vidaus rinkos susiskaidymo, valstybės narės apie bet kokius ketinimus parengti naujas nacionalines kibernetinio saugumo sertifikavimo schemas praneša Komisijai ir EKSSG.

58 straipsnis

Nacionalinės kibernetinio saugumo sertifikavimo institucijos

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

2. Kiekviena valstybė narė praneša Komisijai apie paskirtąsias nacionalines kibernetinio saugumo sertifikavimo institucijas. Jeigu valstybė narė paskiria daugiau nei vieną instituciją, ji taip pat informuoja Komisiją apie užduotis, pavestas kiekvienai iš tų institucijų.

3. Nedarant poveikio 56 straipsnio 5 dalies a punktui ir 56 straipsnio 6 daliai, kiekvienos nacionalinės kibernetinio saugumo sertifikavimo institucijos veiklos organizavimas, finansavimo sprendimai, teisinė struktūra ir sprendimų priėmimas nepriklauso nuo prižiūrimų subjektų.

4. Valstybės narės užtikrina, kad nacionalinės kibernetinio saugumo sertifikavimo institucijos, vykdydamos su Europos kibernetinio saugumo sertifikatų išdavimu pagal 56 straipsnio 5 dalies a punktą ir 56 straipsnio 6 dalį susijusią veiklą, laikytųsi griežto savo funkcijų ir pareigų atskyrimo nuo šiame straipsnyje nustatytos priežiūros veiklos, ir kad ta veikla būtų vykdoma tarpusavyje nepriklausomai.

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

6. Siekiant užtikrinti veiksmingą šio reglamento įgyvendinimą, tikslinga, kad nacionalinės kibernetinio saugumo sertifikavimo institucijos aktyviai, veiksmingai, efektyviai ir saugiai dalyvautų EKSSG veikloje.

7. Nacionalinės kibernetinio saugumo sertifikavimo institucijos:

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

b) stebi, kaip jų atitinkamose teritorijose įsisteigęs (-ę) ir savarankišką atitikties vertinimą atliekantis (-ys) IRT produktų, paslaugų ar procesų ar gamintojas ar teikėjas / gamintojai ir teikėjai vykdo savo pareigas, visų pirma 53 straipsnio 2 ir 3 dalyse ir atitinkamoje Europos kibernetinio saugumo sertifikavimo schemoje nustatytas tokių gamintojų ar teikėjų pareigas, ir užtikrina jų vykdymą;

c) nedarant poveikio 60 straipsnio 3 daliai, aktyviai padeda nacionalinėms akreditacijos įstaigoms vykdyti atitikties vertinimo įstaigų veiksmų stebėsenos ir priežiūros veiklą, kaip nustatyta šiame reglamente, ir jas remia;

d) stebi ir prižiūri 56 straipsnio 5 dalyje nurodytų viešųjų įstaigų veiklą;

e) kai taikytina, teikia įgaliojimus atitikties vertinimo įstaigoms pagal 60 straipsnio 3 dalį ir apriboja, sustabdo arba atšaukia suteiktus įgaliojimus tais atvejais, kai atitikties vertinimo įstaigos nesilaiko šio reglamento reikalavimų;

f) nagrinėja fizinių ar juridinių asmenų pateiktus skundus, susijusius su nacionalinių kibernetinio saugumo sertifikavimo institucijų išduotais Europos kibernetinio saugumo sertifikatais arba atitikties vertinimo įstaigų remiantis 56 straipsnio 6 dalimi išduotais Europos kibernetinio saugumo sertifikatais arba pagal 53 straipsnį padarytais ES atitikties pareiškimais, ir tinkama apimtimi tiria tokių skundų dalyką ir per pagrįstą laikotarpį informuoja skundo teikėją apie tyrimo eigą ir rezultatus;

g) ENISA ir EKSSG teikia pagal šios dalies b, c bei d punktus ar 8 dalį vykdytos veiklos metinę apibendrinamąją ataskaitą;

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

i) stebi aktualius kibernetinio saugumo sertifikavimo srities pokyčius.

8. Kiekviena nacionalinė kibernetinio saugumo sertifikavimo institucija turi bent šiuos įgaliojimus:

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

b) vykdyti tiriamąjį atitikties vertinimo įstaigų, Europos kibernetinio saugumo sertifikatų turėtojų ir ES atitikties pareiškimų išdavėjų auditą siekiant patikrinti, ar laikomasi šios antraštinės dalies;

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

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

e) laikantis nacionalinės teisės, panaikinti nacionalinių kibernetinio saugumo sertifikavimo institucijų arba pagal 56 straipsnio 6 dalį atitikties vertinimo įstaigų išduotus Europos kibernetinio saugumo sertifikatus, kurie tokie sertifikatai neatitinka šio reglamento arba Europos kibernetinio saugumo sertifikavimo schemos;

f) laikantis nacionalinės teisės, taikyti sankcijas, kaip numatyta 65 straipsnyje, ir reikalauti nedelsiant nustoti pažeidinėti šiame reglamente nustatytas pareigas.

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

59 straipsnis

Tarpusavio peržiūra

1. Siekiant visoje Sąjungoje turėti lygiaverčius standartus, susijusius su Europos kibernetinio saugumo sertifikatais ir ES atitikties pareiškimais, nacionalinėms kibernetinio saugumo sertifikavimo institucijoms taikoma tarpusavio peržiūra.

2. Tarpusavio peržiūra atliekama remiantis pagrįstais ir skaidriais vertinimo kriterijais bei procedūromis, visų pirma, kiek tai susiję su struktūriniais, žmogiškųjų išteklių ir proceso reikalavimais, konfidencialumu ir skundais.

3. Atliekant tarpusavio peržiūrą vertinama:

a) kai taikytina, ar nacionalinė kibernetinio saugumo sertifikavimo institucija, vykdydama su Europos kibernetinio saugumo sertifikatų išdavimu pagal 56 straipsnio 5 dalies a punktą ir 56 straipsnio 6 dalį susijusią veiklą, laikosi griežto savo funkcijų ir pareigų atskyrimo nuo priežiūros veiklos pagal 58 straipsnį, ir ar ta veikla vykdoma tarpusavyje nepriklausomai;

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

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

d) atitikties vertinimo įstaigų veiklos stebėsenos, įgaliojimų joms suteikimo ir jų priežiūros procedūros;

e) kai taikytina, ar institucijų arba įstaigų, išduodančių sertifikatus dėl aukšto saugumo užtikrinimo lygio pagal 56 straipsnio 6 dalį, darbuotojai turi tinkamų ekspertinių žinių.

4. Tarpusavio peržiūrą bent kartą kas penkerius metus atlieka bent dvi kitų valstybių narių nacionalinės kibernetinio saugumo sertifikavimo institucijos ir Komisija. ENISA gali dalyvauti atliekant tarpusavio peržiūrą.

5. Komisija gali priimti įgyvendinimo aktus, kuriuose nustatomas ne mažiau kaip penkerių metų laikotarpiui skirtas tarpusavio peržiūros planas, nurodomi tarpusavio peržiūros grupės sudėties kriterijai, atliekant tarpusavio peržiūrą taikoma metodika, tvarkaraštis, periodiškumas ir kitos su tarpusavio peržiūra susijusios užduotys. Priimdama šiuos įgyvendinimo aktus Komisija tinkamai atsižvelgia į EKSSG pastabas. Tie įgyvendinimo aktai priimami pagal 66 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą.

6. EKSSG išnagrinėja tarpusavio peržiūros rezultatus, parengia santraukas, kurios gali būti paskelbtos viešai, ir prireikus pateikia gaires ar rekomendacijas dėl veiksmų ar priemonių, kurių turi imtis atitinkami subjektai.

60 straipsnis

Atitikties vertinimo įstaigos

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

2. Tais atvejais, kai Europos kibernetinio saugumo sertifikatą išduoda nacionalinė kibernetinio saugumo sertifikavimo institucija pagal 56 straipsnio 5 dalies a punktą ir 56 straipsnio 6 dalį, nacionalinės kibernetinio saugumo sertifikavimo institucijos sertifikavimo įstaiga yra akredituota kaip atitikties vertinimo įstaiga pagal šio straipsnio 1 dalį.

3. Kai Europos kibernetinio saugumo sertifikavimo schemose nustatomi specialūs ar papildomi reikalavimai pagal 54 straipsnio 1 dalies f punktą, užduotis pagal tokias schemas vykdo tik tos atitikties vertinimo įstaigos, kurių atžvilgiu nacionalinės kibernetinio saugumo institucijos patvirtino, kad jos atitinka minėtus reikalavimus.

4. 1 dalyje nurodytas akreditavimas suteikiamas atitikties vertinimo įstaigoms ne ilgesniam kaip penkerių metų laikotarpiui ir gali būti pratęstas tomis pačiomis sąlygomis, jei atitikties vertinimo įstaiga toliau atitinka šiame straipsnyje nustatytus reikalavimus. Nacionalinės akreditacijos įstaigos imasi visų tinkamų priemonių per pagrįstą terminą, siekdamos apriboti, sustabdyti arba atšaukti atitikties vertinimo įstaigos akreditavimą pagal 1 dalį, jeigu netenkinamas ar nebetenkinamos akreditavimo sąlygos, arba jeigu atitikties vertinimo įstaiga pažeidžia šį reglamentą.

61 straipsnis

Notifikavimas

1. Kiekvienos Europos kibernetinio saugumo sertifikavimo schemos atveju nacionalinės kibernetinio saugumo sertifikavimo institucijos praneša Komisijai apie atitikties vertinimo įstaigas, akredituotas ir, jei taikytina, pagal 60 straipsnio 3 dalį įgaliotas išduoti 52 straipsnyje nurodytų nustatytų saugumo užtikrinimo lygių Europos kibernetinio saugumo sertifikatus. Nacionalinės kibernetinio saugumo sertifikavimo institucijos be reikalo nedelsdamos informuoja Komisiją apie visus vėlesnius jų pasikeitimus.

2. Praėjus vieniems metams po Europos kibernetinio saugumo sertifikavimo schemos įsigaliojimo Komisija *Europos Sąjungos oficialiajame leidinyje* paskelbia pagal tą schemą 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 notifikuotųjų atitikties vertinimo įstaigų sąrašo pakeitimus.

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

5. Komisija gali priimti įgyvendinimo aktus, kuriais apibrėžiamos pranešimų pagal šio straipsnio 1 dalį teikimo aplinkybės, formatai ir procedūros. Tie įgyvendinimo aktai priimami laikantis 66 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

62 straipsnis

Europos kibernetinio saugumo sertifikavimo grupė

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

2. EKSSG sudaro nacionalinių kibernetinio saugumo sertifikavimo institucijų atstovai arba kitų susijusių nacionalinių institucijų atstovai. Bet kuris EKSSG narys gali atstovauti ne daugiau kaip dviem kitoms valstybėms narėms.

3. Suinteresuotieji subjektai ir atitinkamos trečiosios šalys gali būti kviečiami dalyvauti EKSSG posėdžiuose ir jos darbe.

4. EKSSG užduotys yra šios:

a) teikti rekomendacijas ir padėti Komisijai užtikrinti nuoseklų šios antraštinės dalies įgyvendinimą ir taikymą, visų pirma susijusį su tęstine Sąjungos darbo programa, kibernetinio saugumo sertifikavimo politikos klausimais, politinių požiūrių koordinavimu ir Europos kibernetinio saugumo sertifikavimo schemų rengimu;

b) padėti, teikti rekomendacijas ENISA ir bendradarbiauti su ja rengiant potencialią schemą pagal šio 49 straipsnį;

c) priimti nuomonę dėl potencialių schemų pagal 49 straipsnį;

d) prašyti ENISA parengti potencialias schemas pagal 48 straipsnio 2 dalį;

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

f) nagrinėti aktualius kibernetinio saugumo sertifikavimo srities pokyčius ir keistis informacija ir gerąja praktika, susijusia su kibernetinio saugumo sertifikavimo schemomis;

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

h) remti tarpusavio vertinimo mechanizmų įgyvendinimą pagal taisykles, nustatytas Europos kibernetinio saugumo sertifikavimo schemoje pagal 54 straipsnio 1 dalies u punktą;

i) palengvinti Europos kibernetinio saugumo sertifikavimo schemų derinimą su tarptautiniu mastu pripažintais standartais, be kita ko, persvarstant galiojančias Europos kibernetinio saugumo sertifikavimo schemas ir, kai tinkama, teikiant rekomendacijas ENISA bendradarbiauti su atitinkamomis tarptautinėmis standartizacijos organizacijomis, siekiant šalinti esamų tarptautinių mastu pripažintų standartų trūkumus ar spragas.

5. Padedama ENISA, Komisija pirmininkauja EKSSG ir Komisija teikia EKSSG sekretoriato paslaugas, kaip numatyta 8 straipsnio 1 dalies e punkte.

63 straipsnis

Teisė pateikti skundą

1. Fiziniai ir juridiniai asmenys turi teisę pateikti skundą Europos kibernetinio saugumo sertifikato išdavėjui arba, kai skundas susijęs su Europos kibernetinio saugumo sertifikatu, kurį išdavė atitikties vertinimo įstaiga, veikdama pagal 56 straipsnio 6 dalį, – atitinkamai nacionalinei kibernetinio saugumo sertifikavimo institucijai.

2. Institucija ar įstaiga, kuriai pateiktas skundas, informuoja skundo teikėją apie skundo nagrinėjimo pažangą ir priimtą sprendimą, taip pat informuoja skundo teikėją apie teisę imtis 64 straipsnyje nurodytų veiksmingų teisminių teisių gynimo priemonių.

64 straipsnis

Teisė į veiksmingas teismines teisių gynimo priemones

1. Nedarant poveikio administracinėms ar kitoms neteisminėms teisių gynimo priemonėms, fiziniai ir juridiniai asmenys turi teisę imtis veiksmingų teisminių teisių gynimo priemonių tokiais atvejais:

a) 63 straipsnio 1 dalyje nurodytos institucijos ar įstaigos priimtų sprendimų, įskaitant, kai taikytina, susijusių su tų fizinių ir juridinių asmenų turimo Europos kibernetinio saugumo sertifikato netinkamu išdavimu, neišdavimu ar nepripažinimu, atveju;

b) 63 straipsnio 1 dalyje nurodytai institucijai arba įstaigai pateikto skundo atveju, kai nesiimama jokių veiksmų.

2. Teisminiai procesai pagal šį straipsnį pradedami valstybės narės, kurioje yra institucija arba įstaiga, prieš kurią pradedami teisminiai procesai, teismuose.

65 straipsnis

Sankcijos

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

IV ANTRAŠTINĖ DALIS

BAIGIAMOSIOS NUOSTATOS

66 straipsnis

Komiteto procedūra

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

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

67 straipsnis

Vertinimas ir peržiūra

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

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

3. Įvertinama, ar prieigai prie vidaus rinkos taikomi esminiai kibernetinio saugumo reikalavimai yra būtini siekiant užkirsti kelią IRT produktų, paslaugų ir procesų, kurie neatitinka pagrindinių kibernetinio saugumo reikalavimų, patekimui į Sąjungos rinką.

4. Ne vėliau kaip 2024 m. birželio 28 d. ir po to kas penkerius metus Komisija vertinimo ataskaitą kartu su savo išvadomis perduoda Europos Parlamentui, Tarybai ir Valdančiajai tarybai. Tos ataskaitos išvados skelbiamos viešai.

68 straipsnis

Panaikinimas ir tęstinumas

1. Reglamentas (ES) Nr. 526/2013 panaikinamas nuo 2019 m. birželio 27 d.

2. Nuorodos į Reglamentą (ES) Nr. 526/2013 ir tuo reglamentu įsteigtą ENISA laikomos nuorodomis į šį reglamentą ir ENISA, įsteigtą šiuo reglamentu.

3. ENISA, įsteigta šiuo reglamentu, perima visą Reglamentu (ES) Nr. 526/2013 įsteigtos ENISA nuosavybę, susitarimus, teisines pareigas, darbo sutartis, finansinius įsipareigojimus ir atsakomybę. Visi pagal Reglamentą (ES) Nr. 526/2013 priimti Valdančiosios tarybos ir Vykdomosios valdybos sprendimai lieka galioti, jei jie atitinka šį reglamentą.

4. ENISA įsteigiama neterminuotam laikotarpiui nuo 2019 m. birželio 27 d.

5. Pagal Reglamento (ES) Nr. 526/2013 24 straipsnio 4 dalį paskirtas vykdomasis direktorius toliau eina savo pareigas ir vykdo šio reglamento 20 straipsnyje nurodytas vykdomojo direktoriaus pareigas likusį vykdomojo direktoriaus kadencijos laiką. Kitos jo sutarties sąlygos lieka nepakeistos.

6. Pagal Reglamento (ES) Nr. 526/2013 6 straipsnį paskirti Valdančiosios tarybos nariai ir jų pakaitiniai nariai toliau eina savo pareigas ir vykdo šio reglamento 15 straipsnyje nurodytas Valdančiosios tarybos funkcijas likusį savo kadencijos laiką.

69 straipsnis

Įsigaliojimas

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

2. 58, 60, 61, 63, 64 ir 65 straipsniai taikomi nuo 2021 m. birželio 28 d.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Strasbūre 2019 m. balandžio 17 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas	*Pirmininkas*
A. TAJANI	G. CIAMBA

PRIEDAS

REIKALAVIMAI, KURIUOS TURI ATITIKTI ATITIKTIES VERTINIMO ĮSTAIGOS

Akreditacijos siekiančios atitikties vertinimo įstaigos turi atitikti šiuos reikalavimus:

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

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

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

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

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

6. Jeigu atitikties vertinimo įstaiga priklauso viešajam subjektui arba institucijai arba yra jų valdoma, užtikrinamas nacionalinės kibernetinio saugumo sertifikavimo institucijos ir atitikties vertinimo įstaigos tarpusavio nepriklausomumas ir interesų konflikto nebuvimas ir tai užfiksuojama dokumentuose.

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

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

9. Atitikties vertinimo įstaiga turi pajėgti atlikti visas atitikties vertinimo užduotis, kurios jai paskirtos pagal šį reglamentą, nepriklausomai nuo to, ar tas užduotis vykdo pati atitikties vertinimo įstaiga, ar jos vykdomos jos vardu ir jos atsakomybe. Bet kokia subranga arba konsultacijos su išorės darbuotojais turi būti tinkamai dokumentuotos, jose negali dalyvauti tarpininkai ir tuo tikslu turi būti sudaromas rašytinis susitarimas, kuriame, be kita ko, būtų nuostatos dėl konfidencialumo ir interesų konfliktų. Atitinkama atitikties vertinimo įstaiga prisiima visą atsakomybę už vykdomas užduotis.

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

    a) darbuotojus, turinčius techninių žinių ir pakankamos bei tinkamos patirties atitikties vertinimo užduotims atlikti;

    b) procedūrų, pagal kurias vertinama atitiktis, aprašymus, taip užtikrinant tų procedūrų skaidrumą ir galimybę jas pakartoti. Ji turi taikyti tinkamą politiką ir procedūras, kuriomis užtikrinamas užduočių, kurias ji atlieka kaip pagal 61 straipsnį notifikuotoji įstaiga, ir kitos veiklos atskyrimas;

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

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

12. Už atitikties vertinimo veiklos vykdymą atsakingi darbuotojai turi:

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

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

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

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

13. Užtikrinamas atitikties vertinimo įstaigų, jų vyresniosios vadovybės, už atitikties vertinimą atsakingų asmenų ir visų subrangovų nešališkumas.

14. Atitikties vertinimo įstaigos vyresniosios vadovybės ir už atitikties vertinimą atsakingų asmenų atlyginimas nepriklauso nuo atliktų atitikties vertinimų skaičiaus ar tų vertinimų rezultatų.

15. Atitikties vertinimo įstaigos apsidraudžia atsakomybės draudimu, išskyrus atvejus, kai atsakomybę pagal nacionalinę teisę prisiima valstybė narė arba kai pati valstybė narė tiesiogiai atsako už atitikties vertinimą.

16. Atitikties vertinimo įstaiga ir jos darbuotojai, jos komitetai, jos patronuojamosios bendrovės, subrangovai ir visos kitos su ja susijusios įstaigos arba jos išorės įstaigų darbuotojai laikosi konfidencialumo ir profesinio slaptumo reikalavimo, taikomo visai informacijai, kurią jie gauna atlikdami atitikties vertinimo užduotis pagal šį reglamentą arba nacionalinės teisės aktų nuostatas, kuriomis šis reglamentas įgyvendinamas, išskyrus atvejus, kai duomenis atskleisti reikalaujama pagal Sąjungos arba valstybės narės teisę, taikomą tokiems asmenims, ir išskyrus valstybių narių, kuriose vykdoma veikla, kompetentingų institucijų atvejus. Intelektinės nuosavybės teisės turi būti apsaugotos. Atitikties vertinimo įstaiga dokumentuose užfiksuoja procedūras, susijusias su šio punkto reikalavimais.

17. Išskyrus 16 punktą, šio priedo reikalavimais jokiais būdais nėra draudžiama atitikties vertinimo įstaigai ir asmeniui, prašančiam arba ketinančiam pildyti prašymą sertifikatui gauti, keistis technine informacija ir reguliavimo konsultacijomis.

18. Atitikties vertinimo įstaigos veikia vadovaudamosi nuosekliomis, sąžiningomis ir pagrįstomis nuostatomis, atsižvelgdamos į MVĮ interesus dėl mokesčių.

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

20. Atitikties vertinimo įstaigos užtikrina, kad atitikties vertinimo tikslais naudojamos bandymų laboratorijos atitiktų reikalavimus pagal susijusį standartą, kuris yra suderintas pagal Reglamentą (EB) Nr. 765/2008 bandymus atliekančių laboratorijų akreditavimo tikslais.