



Briuselis, 2018 09 12  
COM(2018) 630 final

2018/0328 (COD)

Pasiūlymas

## **EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS**

**kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas**

*Europos Komisijos įnašas Zalcburgo vadovų susitikime 2018 m. rugsėjo 19–20 d.*

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

## AIŠKINAMASIS MEMORANDUMAS

### 1. PASIŪLYMO APLINKYBĖS

#### • Pasiūlymo pagrindimas ir tikslai

Kasdienis mūsų gyvenimas ir ekonomika vis labiau priklauso nuo skaitmeninių technologijų, todėl piliečiams vis dažniau grėsmę kelia rimti kibernetiniai incidentai. Kad ateityje būtume saugūs, turime stiprinti savo gebėjimą saugoti Sąjungą nuo kibernetinių grėsmių – tiek civilinė infrastruktūra, tiek karinis pajėgumas priklauso nuo saugių skaitmeninių sistemų.

Kad išspręstų kylančias problemas, Sąjunga, remdamasi 2013 m. Kibernetinio saugumo strategija<sup>1</sup> ir jos tikslais bei principais, nuolat plečia savo veiklą šioje srityje, siekdama kurti patikimą, saugią ir atvirą kibernetinę ekosistemą. 2016 m. Sąjunga priėmė pirmąsias kibernetinio saugumo priemones, išdėstytas Europos Parlamento ir Tarybos direktyvoje (ES) 2016/1148<sup>2</sup> dėl tinklų ir informacinių sistemų saugumo.

Atsižvelgdama į spartų grėsmių kibernetiniam saugumui kitimą, 2017 m. rugsėjo mėn. Komisija ir Sąjungos vyriausioji įgaliotinė užsienio reikalams ir saugumo politikai pristatė Bendrą komunikatą<sup>3</sup> „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“, kad būtų toliau stiprinamas Sąjungos atsparumas kibernetiniams išpuoliams, ir užtikrinta, kad nuo jų būtų atgrasoma labiau ir į juos reaguojama tinkamiau. Remiantis ir ankstesnėmis iniciatyvomis, Bendrame komunikate išvardyti siūlomi veiksmai, be kita ko, stiprinti Europos Sąjungos tinklų ir informacijos apsaugos agentūrą (ENISA), kurti savanorišką Sąjungos lygmens kibernetinio saugumo sertifikavimo sistemą, siekiant padidinti skaitmeninio pasaulio produktų ir paslaugų kibernetinį saugumą, taip pat spartaus ir koordinuoto reagavimo į didelio masto kibernetinius incidentus ir kritines situacijas projektą.

Bendrame komunikate pripažinta, kad Sąjungai yra strategiškai svarbu išlaikyti ir plėtoti esminius kibernetinio saugumo technologinius pajėgumus, būtinus siekiant užtikrinti bendrosios skaitmeninės rinkos saugumą, apsaugoti ypatingos svarbos tinklus ir informacines sistemas ir teikti pagrindines kibernetinio saugumo paslaugas. Sąjunga turi turėti galimybę savarankiškai apsaugoti savo skaitmeninį turtą ir konkuruoti pasaulinėje kibernetinio saugumo rinkoje.

Šiuo metu Sąjunga importuoja kibernetinio saugumo produktus ir sprendimus ir daugiausia priklauso nuo ne Europos paslaugų teikėjų<sup>4</sup>. Pasaulinė kibernetinio saugumo rinka yra 600 mlrd. EUR vertės rinka. Numatoma, kad per ateinančius penkerius metus ji vidutiniškai augs apie 17 % (pagal pardavimų apimtį, įmonių ir darbo vietų skaičių). Tačiau tarp 20 rinkos požiūriu pažangiausių kibernetinio saugumo šalių yra vos 6 valstybės narės<sup>5</sup>.

Kita vertus, Sąjungoje sukaupta daug specialiųjų žinių ir patirties kibernetinio saugumo srityje – daugiau nei 660 organizacijų iš visos ES įtrauktos į naujausią Komisijos atliktą kibernetinio

<sup>1</sup> BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“, JOIN(2013) 1 *final*.

<sup>2</sup> 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).

<sup>3</sup> BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“, JOIN(2017) 450 *final*.

<sup>4</sup> Galutinės 2018 m. kibernetinio saugumo rinkos tyrimo ataskaitos projektas.

<sup>5</sup> Galutinės 2018 m. kibernetinio saugumo rinkos tyrimo ataskaitos projektas.

saugumo kompetencijos centrų padėties analizę<sup>6</sup>. Pavertus šias specialiąsias žinias tinkamais parduoti produktais ir sprendimais, Sąjunga galėtų dalyvauti visoje kibernetinio saugumo vertės grandinėje. Tačiau mokslinių tyrimų ir pramonės bendruomenių pastangos yra suskaidytos ir nepakankamai suderintos, trūksta bendros misijos, todėl nukenčia ES konkurencingumas šioje srityje ir ji negali tinkamai apsaugoti savo skaitmeninio turto. Dar nepakankamai remiami kibernetiniam saugumui aktualūs sektoriai (pvz., energetika, kosmosas, gynyba, transportas)<sup>7</sup> bei posričiai. Europoje taip pat nėra visiškai išnaudojama civilinio ir gynybos sektorių sinergija kibernetinio saugumo srityje.

2016 m. Sąjungoje įsteigta viešojo ir privačiojo sektorių partnerystė kibernetinio saugumo srityje buvo svarbus pirmasis žingsnis, vienijantis mokslinių tyrimų, pramonės ir viešojo sektoriaus bendruomenių pastangas palengvinti kibernetinio saugumo mokslinius tyrimus ir inovacijas, o vykdant 2014–2020 m. finansinę programą turėtų būti prisidėta prie geresnių ir tikslingesnių mokslinių tyrimų ir inovacijų rezultatų. Įsteigus viešojo ir privačiojo sektorių partnerystę, pramonės partneriai galėjo prisiimti įsipareigojimus dėl individualių išlaidų srityse, apibrėžtose partnerystės strateginėje mokslinių tyrimų ir inovacijų darbotvarkėje.

Tačiau Sąjunga gali siekti daug platesnio masto investicijų ir jai reikalingas veiksmingesnis mechanizmas, kuris sudarytų sąlygas sukurti ilgalaikius pajėgumus, sutelkti pastangas, kompetencijas ir skatinti naujoviškų sprendimų kūrimą, reaguojant į kibernetinio saugumo pramonės problemas naujų daugiafunkčių technologijų (pvz., dirbtinio intelekto, kvantinės kompiuterijos, blokų grandinių ir saugių skaitmeninių tapatybių) srityje bei ypatingos svarbos (pvz., transporto, energetikos, sveikatos apsaugos, finansų, vyriausybės, telekomunikacijų, gamybos, gynybos, kosmoso) sektoriuose.

Bendrame komunikate apsvairstyta galimybė stiprinti Sąjungos pajėgumą užtikrinti kibernetinį saugumą sukuriant kibernetinio saugumo kompetencijos centrų tinklą, kurio branduolys būtų Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centras. Taip būtų siekiama prisidėti prie pastangų stiprinti šios srities pajėgumus Sąjungos ir nacionaliniu lygmenimis. Bendrame komunikate paminėtas Komisijos ketinimas 2018 m. atlikti poveikio vertinimą siekiant išnagrinėti turimas galimybes sukurti struktūrą. Siekdama žengti pirmąjį žingsnį ir surinkti informacijos, kuria būtų galima remtis ateityje, Komisija pagal programą „Horizontas 2020“ pradėjo bandomąjį etapą, kuris padėtų sujungti nacionalinius centrus į tinklą siekiant suteikti naują postūmį kibernetinio saugumo kompetencijos ugdymui ir kibernetinio saugumo technologijų plėtrai.

2017 m. rugsėjo mėn. surengtame Talino aukščiausiojo lygio susitikime skaitmeniniais klausimais valstybių ir vyriausybių vadovai paragino Sąjungą tapti „pasauline lydere kibernetinio saugumo srityje iki 2025 m., siekiant užtikrinti mūsų piliečių, vartotojų ir įmonių pasitikėjimą ir apsaugą internete ir sudaryti sąlygas naudotis laisvu ir teisės aktais reglamentuojamu internetu“.

2017 m. lapkričio mėn. priimtose Tarybos išvadose<sup>8</sup> Komisija raginama skubiai atlikti galimybių poveikio vertinimą ir iki 2018 m. vidurio pateikti pasiūlymą dėl teisinės priemonės, pagal kurią būtų įgyvendinama iniciatyva.

<sup>6</sup> JRC techninė ataskaita: Europos kibernetinio saugumo kompetencijos centrai, 2018 m.

<sup>7</sup> JRC techninė ataskaita: Padėties analizės rezultatai (žr. 4 ir 5 priedą).

<sup>8</sup> Tarybos išvados dėl Bendro komunikato Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“, priimtose Bendrųjų reikalų tarybos 2017 m. lapkričio 20 d.

Skaitmeninės Europos programa<sup>9</sup>, kurią Komisija pasiūlė 2018 m. birželio mėn., siekiama padidinti ir išplėsti skaitmeninės transformacijos naudą visiems Europos piliečiams ir įmonėms visose svarbiose ES politikos srityse stiprinant politiką ir remiant bendrosios skaitmeninės rinkos plataus užmojo planus. Programoje siūlomas darnus ir visapusiškas požiūris, siekiant geriausio pažangių technologijų panaudojimo ir tinkamo techninių pajėgumų derinimo su žmonių kompetencija skaitmeninei transformacijai užtikrinti ne tik kibernetinio saugumo srityje, bet ir išmaniųjų duomenų infrastruktūros, dirbtinio intelekto, aukšto lygio įgūdžių, pramonės ir viešojo intereso taikomųjų programų srityse. Šie elementai yra vienas nuo kito priklausomi, vienas kitą sustiprinantys, o vienu metu puoselėjami jie padės pasiekti mastą, leisiantį duomenų ekonomikai klestėti<sup>10</sup>. Kibernetinis saugumas taip pat yra vienas iš kitos ES bendrosios MTI programos – „Europos horizontas“<sup>11</sup> – prioritetų.

Todėl šiuo reglamentu siūloma įsteigti Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą ir nacionalinių koordinavimo centrų tinklą. Šis tikslingai sukurtas bendradarbiavimo modelis turėtų veikti toliau aprašytu būdu, siekiant paskatinti kurti Europos kibernetinio saugumo technologijų ir pramonės ekosistemą: Kompetencijos centras palengvins ir padės koordinuoti Tinklo darbą, puoselės kibernetinio saugumo kompetencijos bendruomenę, vykdys kibernetinio saugumo technologinių klausimų darbotvarkę ir sudarys palankesnes sąlygas naudotis sukaupta praktine patirtimi. Tai visų pirma bus vykdoma įgyvendinant atitinkamas Skaitmeninės Europos programos ir programos „Europos horizontas“ dalis skiriant dotacijas ir vykdant viešuosius pirkimus. Atsižvelgiant į kitose pasaulio vietose skiriamas dideles investicijas kibernetinio saugumo sričiai ir į poreikį koordinuoti ir sutelkti išteklius Europoje, siūloma Kompetencijos centrą įsteigti kaip Europos partnerystę<sup>12</sup> ir taip sudaryti palankesnes sąlygas Sąjungos, valstybių narių ir (arba) pramonės bendroms investicijoms. Todėl pasiūlyme reikalaujama, kad valstybės narės proporcingai prisidėtų remiant Kompetencijos centro ir Tinklo veiklą. Pagrindinis sprendimus priimančias organas yra Valdyba, kurioje dalyvauja visos valstybės narės, tačiau balsavimo teises turi tik tos valstybės narės, kurios prisideda finansiškai. Valdybos balsavimo mechanizmas pagrįstas dvigubos daugumos principu – reikalinga 75 % finansinio įnašo ir 75 % balsų dauguma. Atsižvelgiant į Komisijos atsakomybę už Sąjungos biudžetą, ji turi 50 % balsų. Dirbdama Valdyboje, Komisija prireikus pasinaudos Europos išorės veiksmų tarnybos praktine patirtimi. Siekiant palaikyti nuolatinį dialogą su privačiuoju sektoriumi, vartotojų organizacijomis ir kitomis atitinkamomis suinteresuotosiomis šalimis, Valdybai padeda Pramonės ir mokslo patariamoji taryba.

Glaudžiai bendradarbiaudamas su Nacionalinių koordinavimo centrų tinklu ir kibernetinio saugumo kompetencijos bendruomene (apimančia didelę ir įvairią kuriant kibernetinio saugumo technologijas dalyvaujančių subjektų grupę, pvz., mokslinių tyrimų organizacijas, pasiūlos ir paklausos sričių pramonės įmones ir viešąjį sektorių), Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras bus pagrindinė

<sup>9</sup> COM(2018) 434 Europos Parlamento ir Tarybos reglamento dėl 2021–2027 m. Skaitmeninės Europos programos sudarymo pasiūlymas.

<sup>10</sup> Žr. SWD(2018) 305.

<sup>11</sup> COM(2018) 435 Europos Parlamento ir Tarybos reglamento dėl bendrosios mokslinių tyrimų ir inovacijų programos „Europos horizontas“ ir su ja susijusių dalyvavimo ir sklaidos taisyklių pasiūlymas.

<sup>12</sup> Kaip apibrėžta COM(2018) 435 Europos Parlamento ir Tarybos reglamento dėl bendrosios mokslinių tyrimų ir inovacijų programos „Europos horizontas“ ir su ja susijusių dalyvavimo ir sklaidos taisyklių pasiūlyme; ir nurodyta COM(2018) 434 Europos Parlamento ir Tarybos reglamento dėl 2021–2027 m. Skaitmeninės Europos programos sudarymo pasiūlyme.

pagal siūlomą *Skaitmeninės Europos programą ir programą „Europos horizontas“* skirtų ES finansinių išteklių įgyvendinimo institucija.

Toks visapusiškas požiūris sudarytų sąlygas remti kibernetinį saugumą visoje vertės grandinėje – nuo mokslinių tyrimų iki pagrindinių technologijų diegimo ir naudojimo. Valstybių narių finansinis dalyvavimas turėtų būti proporcingas ES finansiniam įnašui į šią iniciatyvą ir yra būtinas jos sėkmės elementas.

Atsižvelgiant į Europos kibernetinio saugumo organizacijos, kuri pagal programą „Horizontas 2020“ yra Komisijos partnerė viešojo ir privačiojo sektorių partnerystėje kibernetinio saugumo klausimais, ypatingą praktinę patirtį ir platų bei reikšmingą suinteresuotųjų šalių atstovavimą, ji turėtų būti pakviesta prisidėti prie Centro ir Tinklo veiklos.

Be to, Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras taip pat turėtų siekti padidinti kibernetinio saugumo civilinių ir gynybos aspektų sinergiją. Jis turėtų teikti paramą valstybėms narėms ir kitiems susijusiems subjektams, konsultuodamas, dalydamasis praktine patirtimi ir palengvindamas bendradarbiavimą įgyvendinant projektus ir veiksmus. Valstybėms narėms paprašius, jis taip pat galėtų būti projektų valdytojas, ypač, kai tai susiję su Europos gynybos fondu. Šia iniciatyva siekiama padėti spręsti toliau išvardytas problemas:

- **Nepakankamas kibernetinio saugumo paklausos ir pasiūlos sričių pramonės įmonių bendradarbiavimas.** Europos įmonės susiduria su problema bandydamos tiek pačios išlikti saugios, tiek siūlyti savo klientams saugius produktus ir paslaugas. Tačiau dažnai jos negali tinkamai apsaugoti savo esamų produktų, paslaugų ir turto arba kurti saugių novatoriškų produktų ir paslaugų. Pavieniams rinkos dalyviams, kurių pagrindinė verslo veikla nėra susijusi su kibernetiniu saugumu, dažnai per brangu kurti ir taikyti pagrindines kibernetinio saugumo priemones. Kartu kibernetinio saugumo rinkos paklausos ir pasiūlos sričių subjektų ryšiai nėra pakankamai gerai išvystyti, todėl nepakankamai optimaliai tiekiami Europos produktai ir sprendimai, pritaikyti skirtingų sektorių poreikiams, taip pat nepakankamas rinkos dalyvių tarpusavio pasitikėjimo lygis.
- **Nėra veiksmingo valstybių narių bendradarbiavimo mechanizmo, reikalingo pramonės pajėgumams stiprinti.** Šiuo metu taip pat nėra veiksmingo bendradarbiavimo mechanizmo, pagal kurį valstybės narės galėtų bendradarbiauti stiprindamos reikiamus pajėgumus, reikalingus kibernetinio saugumo inovacijoms remti visuose pramonės sektoriuose ir pažangiausiems Europos kibernetinio saugumo sprendimams diegti. Pagal Direktyvą (ES) Nr. 2016/1148 veikiančiuose valstybių narių bendradarbiavimo kibernetinio saugumo srityje mechanizmuose tokia veikla nenumatyta pagal joms suteiktus įgaliojimus.
- **Nepakankamas bendradarbiavimas mokslinių tyrimų ir pramonės bendruomenėse ir tarp jų.** Nepaisant teorinio Europos gebėjimo dalyvauti visoje kibernetinio saugumo vertės grandinėje, esama svarbių kibernetinio saugumo sektorių (pvz., energetika, kosmosas, gynyba, transportas) ir posričių, kuriuos šiuo metu per mažai remia mokslinių tyrimų bendruomenė arba kuriuos remia vos keletas centrų (pvz., postkvantinė ir kvantinė kriptografija, dirbtinio intelekto patikimumas ir kibernetinis saugumas). Nors šis bendradarbiavimas akivaizdžiai vyksta, labai dažnai jis tėra trumpalaikis susitarimas dėl konsultacijų, kuris nesuteikia teisės dalyvauti ilgalaikiuose mokslinių tyrimų planuose, siekiant išspręsti pramonės problemas, susijusias su kibernetiniu saugumu.
- **Nepakankamas bendradarbiavimas tarp kibernetinio saugumo mokslinių tyrimų ir inovacijų civilinių ir gynybos bendruomenių.** Nepakankamo bendradarbiavimo

problema taip pat yra susijusi su civilinėmis ir gynybos bendruomenėmis. Esama sinergija nėra visiškai išnaudota, kadangi trūksta veiksmingų mechanizmų, suteikiančių šioms bendruomenėms galimybę veiksmingai bendradarbiauti ir didinti pasitikėjimą, kuris labiau nei kitose srityse yra būtina sėkmingo bendradarbiavimo sąlyga. Problemos nepadedą spręsti ir tai, kad ES kibernetinio saugumo rinkos finansinis pajėgumas ribotas, įskaitant nepakankamas lėšas naujovėms remti.

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

Kibernetinio saugumo kompetencijos centrų tinklas ir Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras užtikrins papildomą paramą esamoms kibernetinio saugumo politikos nuostatoms ir joje dalyvaujantiems subjektams. Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro įgaliojimai papildys ENISA pastangas, tačiau jų paskirtis kita ir reikalingi kitokie įgūdžiai. Nors ENISA įgaliojimuose numatytas konsultavimo ES kibernetinio saugumo mokslinių tyrimų ir inovacijų klausimais vaidmuo, siūlomi įgaliojimai daugiausia susiję su kitais uždaviniais, kurie yra svarbūs didinant kibernetinio saugumo atsparumą ES. Be to, ENISA įgaliojimuose nenumatyta veiklos rūšių, kurios būtų pagrindinės Centro ir tinklo užduotys, t. y. skatinti kurti ir diegti kibernetinio saugumo technologijas ir prisidėti prie pastangų stiprinti šios srities pajėgumus ES ir nacionaliniu lygmenimis.

Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Kibernetinio saugumo kompetencijos centrų tinklas taip pat remis mokslinius tyrimus, siekdami palengvinti ir pagreitinti standartizacijos ir sertifikavimo procesus, ypač susijusius su kibernetinio saugumo sertifikavimo sistemomis, siūlomomis Kibernetinio saugumo akte<sup>1314</sup>.

Šia iniciatyva *de facto* sustiprinama viešojo ir privačiojo sektorių partnerystė kibernetinio saugumo srityje, kuri buvo pirmasis bandymas ES mastu sujungti kibernetinio saugumo pramonę, paklauskos srities subjektus (kibernetinio saugumo produktų ir sprendimų pirkėjus, įskaitant viešojo administravimo įstaigas ir ypatingos svarbos sektorius, pvz., transporto, sveikatos apsaugos, energetikos, finansų) ir mokslinių tyrimų bendruomenę, siekiant sukurti tvaraus dialogo platformą ir sudaryti sąlygas savanoriškai bendrai investuoti. 2016 m. įsteigta viešojo ir privačiojo sektorių partnerystė iki 2020 m. pritrauks iki 1,8 mlrd. EUR investicijų. Tačiau kitose pasaulio šalyse daromų investicijų mastas (pvz., vien 2017 m. JAV į kibernetinį saugumą investavo 19 mlrd. USD) rodo, kad ES turi daugiau nuveikti, kad pasiektų kritinę investicijų masę ir išspręstų pajėgumų išsibarstymo po visą ES problemą.

- **Suderinamumas su kitomis Sąjungos politikos sritimis**

Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras veiks kaip pagrindinė įvairių Sąjungos programų, remiančių kibernetinį saugumą (Skaitmeninės Europos programa ir programa „Europos horizontas“), įgyvendinimo įstaiga ir stiprins jų suderinamumą bei sinergiją.

<sup>13</sup> EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO dėl ES kibernetinio saugumo agentūros ENISA ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas, COM(2017) 477 *final/3*), pasiūlymas.

<sup>14</sup> Taip nepažeidžiami sertifikavimo mechanizmai pagal Bendrąjį duomenų apsaugos reglamentą, pagal kurį duomenų apsaugos institucijos atlieka tam tikrą vaidmenį, kaip numatyta 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 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).

Šia iniciatyva taip pat bus sudarytos sąlygos papildyti valstybių narių pastangas ir tinkamai padėti švietimo politikos formuotojams, kad jie galėtų gerinti kibernetinio saugumo įgūdžius (pvz., sukurti civilinėms ir karinėms švietimo sistemoms skirtas su kibernetiniu saugumu susijusias mokymo programas) ir sukurti kvalifikuotą ES kibernetinio saugumo specialistų bazę – pagrindinę priemonę, skirtą kibernetinio saugumo įmonėms ir kitoms pramonės įmonėms, turinčioms interesų kibernetinio saugumo srityje. Kalbant apie švietimą ir mokymą kibernetinės gynybos klausimais, ši iniciatyva bus suderinama su Europos saugumo ir gynybos koledžo įsteigtos su kibernetine gynyba susijusios švietimo, mokymo ir pratybų platformos vykdomu darbu.

Ši iniciatyva papildys ir parems skaitmeninių inovacijų centrų pastangas pagal Skaitmeninės Europos programą. Skaitmeninių inovacijų centrai – tai ne pelno organizacijos, padedančios bendrovėms, ypač startuoliams, MVĮ ir vidutinės kapitalizacijos įmonėms, didinti konkurencingumą gerinant verslo / gamybos procesus bei produktus ir paslaugas pasitelkus išmaniąsias inovacijas, sukurtas naudojant skaitmenines technologijas. Skaitmeninių inovacijų centrai teikia į verslą orientuotas novatoriškas paslaugas, pvz., rinkos tyrimus, finansavimo konsultacijas, galimybę naudotis atitinkama bandymų ir eksperimentų infrastruktūra, mokymą ir įgūdžių tobulinimą, kad padėtų naujiems produktams ar paslaugoms sėkmingai įsitvirtinti rinkoje arba pristatytų geresnius gamybos procesus. Kai kurie skaitmeninių inovacijų centrai, turintys konkrečios kibernetinio saugumo praktinės patirties, galėtų tiesiogiai dalyvauti pagal šią iniciatyvą įsteigtos kibernetinio saugumo kompetencijos bendruomenės veikloje. Tačiau daugeliu atvejų skaitmeninių inovacijų centrai, neturintys konkretaus kibernetinio saugumo profilio, palengvintų savo klientams galimybę naudotis kibernetinio saugumo bendruomenės praktine patirtimi, žiniomis ir pajėgumais glaudžiai bendradarbiaudami su Nacionalinių koordinavimo centrų tinklu ir Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centru. Skaitmeninių inovacijų centrai taip pat paremtų novatoriškų kibernetinio saugumo produktų ir sprendimų, tenkinančių bendrovių ir kitų galutinių naudotojų poreikius, diegimą. Paskutinis, bet ne mažiau svarbus dalykas – konkrečiam sektoriui priskirtini skaitmeninių inovacijų centrai galėtų dalytis žiniomis apie realius sektoriaus poreikius su Tinklu ir Centru ir papildyti mokslinių tyrimų ir inovacijų darbotvarkę, atitinkančią pramonės poreikius.

Bus siekiama sinergijos su atitinkamomis Europos inovacijos ir technologijos instituto (EIT) žinių ir inovacijos bendrijomis, ypač su „EIT Digital“.

## **2. TEISINIS PAGRINDAS, SUBSIDIARUMO IR PROPORCINGUMO PRINCIPAI**

### **• Teisinis pagrindas**

Dėl savo pobūdžio ir konkrečių tikslų Kompetencijos centras turėtų būti įsteigtas remiantis dvigubu teisiniu pagrindu. SESV 187 straipsniu, kuriuo leidžiama kurti struktūras, reikalingas Sąjungos mokslinių tyrimų, technologijų plėtros ir demonstravimo programoms veiksmingai vykdyti, Kompetencijos centrui sudaromos sąlygos kurti sinergijas ir telkti išteklius, siekiant investuoti į būtinus pajėgumus valstybių narių lygmeniu ir kaupti bendrą Europos turtą (pvz., bendrai įsigyti reikalingą kibernetinio saugumo bandymų ir eksperimentų infrastruktūrą). 188 straipsnio pirmojoje pastraipoje numatytas tokių priemonių priėmimas. Nepaisant to, 188 straipsnio pirmoji pastraipa, kaip vienintelis teisinis pagrindas, nesuteiktų teisės vykdyti veiklą, nesusijusią su moksliniais tyrimais ir technologine plėtra siekiant įgyvendinti visus šiame reglamente nustatytus Kompetencijos centro tikslus – remti kibernetinio saugumo produktų ir sprendimų diegimą rinkoje, siekti stiprinti Europos kibernetinio saugumo pramonės konkurencingumą, didinti savo rinkos dalį ir prisidėti prie nacionalinių pastangų

sprendžiant kibernetinio saugumo įgūdžių trūkumo problemą. Todėl, siekiant minėtųjų tikslų, kaip teisinį pagrindą reikia nurodyti ir 173 straipsnio 3 dalį, pagal kurią Sąjungai leidžiama numatyti priemones, remiančias pramonės konkurencingumą.

- **Pasiūlymo pagrindimas subsidiarumo ir proporcingumo principų požiūriu**

Kaip nurodyta pirmiau minėtose Tarybos išvadose, kibernetinis saugumas yra Sąjungos bendros svarbos klausimas. Tokių incidentų kaip „WannaCry“ ar „NonPetya“ mastas ir tarpvalstybinis pobūdis yra geriausias pavyzdys. Atsižvelgdama į kibernetinio saugumo technologinių uždavinių pobūdį ir mastą bei nepakankamą pastangų koordinavimą pramonės sektoriuose, viešajame sektoriuje ir mokslinių tyrimų bendruomenėse ir tarp jų, ES turi toliau remti koordinavimo pastangas, kad būtų sutelkta kritinė išteklių masė ir užtikrintas geresnis žinių ir turto valdymas. Šie veiksmai reikalingi atsižvelgiant į išteklių poreikius, susijusius su tam tikrais kibernetinio saugumo mokslinių tyrimų, technologinės plėtros ir diegimo pajėgumais; poreikį suteikti galimybę naudotis tarpdisciplinine kibernetinio saugumo praktine patirtimi skirtingose disciplinose (kuri dažnai tik iš dalies prieinama nacionaliniu lygmeniu); pasaulinį pramonės vertės grandinės pobūdį, taip pat visose rinkose veikiančių pasaulinių konkurentų veiklą.

Tam reikia tokio masto išteklių ir praktinės patirties, kuriuos vargu ar galima pasiekti bet kurios valstybės narės pavieniais veiksmais. Pavyzdžiui, visos Europos kvantinės komunikacijos tinklui gali prireikti apie 900 mln. EUR ES investicijų, priklausomai nuo valstybių narių investicijų (kurios turi būti tarpusavyje susijusios / papildyti viena kitą) ir to, kiek technologija leis pakartotinai panaudoti esamas infrastruktūras. Inicijatyva bus sudarytos sąlygos sutelkti finansavimą ir įgyvendinti tokios rūšies investicijas Sąjungoje.

Pavienės valstybės narės negali visiškai pasiekti šios iniciatyvos tikslų. Kaip anksčiau minėta, jų geriau siekti Sąjungos lygmeniu, sutelkiant pastangas ir išvengiant nereikalingo dubliavimo, padedant pasiekti kritinę investicijų masę ir užtikrinant optimalų viešojo finansavimo panaudojimą. Kartu pagal proporcingumo principą šiuo reglamentu neviršijama to, kas būtina nurodytam tikslui pasiekti. Todėl ES veiksmai yra pagrįsti pagal subsidiarumo ir proporcingumo principus.

Pagal šią priemonę nenumatoma jokių naujų reglamentavimo įsipareigojimų įmonėms. Be to, greičiausiai sumažės įmonių, ypač MVI išlaidos, susijusios su jų pastangomis kurti novatoriškus kibernetinio saugumo produktus, nes iniciatyva sudaromos sąlygos telkti išteklius, siekiant investuoti į būtinus gebėjimus valstybių narių lygmeniu ir kaupti bendrą Europos turtą (pvz., bendrai įsigyti reikalingą kibernetinio saugumo bandymų ir eksperimentų infrastruktūrą). Šį turtą įvairiuose sektoriuose galėtų naudoti pramonės įmonės ir MVI, siekdamas užtikrinti, kad jų produktai būtų saugūs kibernetiniu požiūriu ir kad kibernetinis saugumas taptų jų konkurenciniu pranašumu.

- **Priemonės pasirinkimas**

Pagal siūlomą priemonę bus įsteigta įstaiga, vykdydianti kibernetinio saugumo veiksmus pagal Skaitmeninės Europos programą ir programą „Europos Horizontas“. Joje išdėstomi įstaigos įgaliojimai, užduotys ir valdymo struktūra. Norint įsteigti tokią Sąjungos įstaigą, reikia priimti reglamentą.



### 3. KONSULTACIJOS SU SUINTERESUOTOSIOMIS ŠALIMIS IR POVEIKIO VERTINIMAS

Pasiūlymas sukurti Kibernetinio saugumo kompetencijos centrų tinklą ir Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą yra nauja iniciatyva. Ji yra 2016 m. įsteigtos sutartimi pagrįstos viešojo ir privačiojo sektorių partnerystės kibernetinio saugumo srityje tąsa ir išplėtimas.

#### • Konsultacijos su suinteresuotosiomis šalimis

Kibernetinis saugumas yra platus tarpsektorinis klausimas. Komisija naudojo skirtingus konsultavimosi metodus siekdama įsitikinti, kad šioje iniciatyvoje būtų tinkamai atspindėtas Sąjungos bendras viešasis interesas, o ne konkretūs pavienių suinteresuotųjų šalių grupių interesai. Toks metodas užtikrina Komisijos darbo skaidrumą ir atskaitingumą. Nors dėl tikslinės auditorijos (pramonės ir mokslinių tyrimų bendruomenė ir valstybės narės) dėl šios iniciatyvos nebuvo vykdomos atviros viešos konsultacijos su tiksline auditorija, ši tema jau buvo įtraukta į kelias kitas atviras viešas konsultacijas:

- 2018 m. vykdytos bendros atviros viešos konsultacijos investicijų, mokslinių tyrimų ir inovacijų, MVĮ ir bendrosios rinkos tema;
- 2017 m. pradėtos 12 savaičių trukmės internetinės viešos konsultacijos, siekiant išsiaiškinti platesnės visuomenės (maždaug 90 respondentų) požiūrį į ENISA veiklos vertinimą ir peržiūrą;
- Įsteigus sutartimis grindžiamą viešojo ir privačiojo sektorių partnerystę kibernetinio saugumo srityje, 2016 m. vykdytos 12 savaičių trukmės internetinės viešos konsultacijos (maždaug 240 respondentų).

Komisija taip pat surengė tikslines konsultacijas dėl šios iniciatyvos, įskaitant praktinius seminarus, susitikimus ir tikslinius prašymus pateikti informaciją (skirtus ENISA ir Europos gynybos agentūrai). Konsultacijų laikotarpis truko ilgiau kaip 6 mėnesius, nuo 2017 m. lapkričio mėn. iki 2018 m. kovo mėn. Komisija taip pat atliko kompetencijos centrų padėties analizę ir gavo informaciją iš 665 kibernetinio saugumo kompetencijos centrų apie jų praktinę patirtį, veiklą, darbo sritis ir tarptautinį bendradarbiavimą. Tyrimas buvo pradėtas sausio mėn. ir atliekant ataskaitos analizę buvo atsižvelgta į atsakymus, pateiktus iki 2018 m. kovo 8 d.

Pramonės ir mokslinių tyrimų bendruomenių suinteresuotosios šalys teigė, kad Kompetencijos centras ir Tinklas galėtų prisidėti prie dabartinių pastangų nacionaliniu lygmeniu ir padėti sukurti visos Europos kibernetinio saugumo ekosistemą, kuri sudarytų veiksmingesnio mokslinių tyrimų ir pramonės bendruomenių bendradarbiavimo sąlygas. Jų nuomone, taip pat būtina, kad ES ir valstybės narės taikytų iniciatyvų, ilgalaikį ir strateginį požiūrį į kibernetinio saugumo pramonės politiką, apimančią ne tik mokslinius tyrimus ir inovacijas. Suinteresuotosios šalys pareiškė, kad reikia turėti galimybę naudotis pagrindiniais pajėgumais, pvz., bandymų ir eksperimentų infrastruktūra, ir ryžtingiau spręsti kibernetinio saugumo įgūdžių trūkumo problemą, pvz., įgyvendinant didelio masto Europos projektus, pritraukiančius geriausius talentus. Visi pirmiau išdėstyti argumentai buvo laikomi būtiniais, kad Sąjunga visame pasaulyje būtų pripažįstama kibernetinio saugumo srities lydere.

Atsižvelgdamos į konsultacijas, vykusias nuo praėjusių metų rugsėjo mėn.<sup>15</sup>, taip pat į specialiąsias Tarybos išvadas<sup>16</sup>, valstybės narės palankiai įvertino ketinimą sukurti

<sup>15</sup> Pvz., Aukšto lygio apskritojo stalo susitikimas su valstybėmis narėmis, Pirmininko pavaduotojas A. Ansipas, Komisijos narė M. Gabriel, 2017 m. gruodžio 5 d.

Kibernetinio saugumo kompetencijos centrų tinklą, skirtą kibernetinio saugumo technologijų plėtrai ir diegimui skatinti, pabrėždamos būtinybę įtraukti visas valstybes nares ir jų veikiančius kompetencijos centrus bei ypač daug dėmesio skirti papildomumui. Konkrečiai dėl būsimo Kompetencijos centro valstybės narės pabrėžė, kad, jo kaip koordinatoriaus vaidmuo itin svarbus remiant tinklą. Kalbant apie kibernetinės gynybos srities nacionalinius veiksmus ir poreikius, valstybių narių kibernetinės gynybos poreikių analizė, kurią 2018 m. kovo mėn. atliko Europos išorės veiksnių tarnyba, parodė, kad dauguma valstybių narių pridėtinę vertę sieja su ES parama mokymui ir švietimui kibernetinio saugumo klausimais bei parama pramonei vykdant mokslinius tyrimus ir technologinę plėtrą<sup>17</sup>. Ši iniciatyva iš tiesų būtų įgyvendinama kartu su valstybėmis narėmis ar jų remiamais subjektais. Bendradarbiavimas tarp pramonės, mokslinių tyrimų ir (arba) viešojo sektoriaus bendruomenių susietų ir sustiprintų esamus subjektus ir jų pastangas, bet neskatintų naujų subjektų steigimo. Valstybės narės taip pat dalyvautų apibrėžiant konkrečius veiksmus, skirtus viešajam sektoriui, tiesiogiai naudojančiam kibernetinio saugumo technologijas ir praktinę patirtį.

#### • **Poveikio vertinimas**

2017 m. balandžio 11 d. poveikio vertinimas, kuriuo grindžiama ši iniciatyva, pateiktas Reglamentavimo patikros valdybai ir ji pateikė teigiamą nuomonę su išlygomis. Atsižvelgiant į Valdybos pastabas, poveikio vertinimas buvo peržiūrėtas. Valdybos nuomonė ir priedas, kuriame paaiškinama, kaip buvo atsižvelgta į Valdybos pastabas, skelbiami kartu su šiuo pasiūlymu.

Poveikio vertinime apsvaistytos įvairios tiek teisėkūros, tiek ne teisėkūros pobūdžio politikos galimybės. Toliau pateiktos galimybės buvo pasirinktos išsamiam vertinimui:

- bendradarbiavimo varianto atskaitos scenarijuje perimtas dabartinis požiūris į kibernetinio saugumo pramonės ir technologinių pajėgumų stiprinimą ES, remiant mokslinius tyrimus ir inovacijas bei susijusius bendradarbiavimo mechanizmus pagal FP9;
- 1 galimybė. Kibernetinio saugumo kompetencijos centrų tinklui ir Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrui suteikiami dvigubi įgaliojimai įgyvendinti priemonės, kuriomis remiamos pramonės technologijos, taip pat priemonės mokslinių tyrimų ir inovacijų srityje;
- 2 galimybė. Kibernetinio saugumo kompetencijos centrų tinklo ir Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centro veikla sutelkta į mokslinius tyrimus ir inovacijas.

Ankstyvuosiuose etapuose atmetos galimybės: 1) galimybė nesiiimti jokių veiksmų, 2) galimybė kurti tik kibernetinio saugumo kompetencijos centrų tinklą, 3) galimybė kurti tik centralizuotą struktūrą ir 4) galimybė naudotis jau veikiančia agentūra (Europos Sąjungos tinklą ir informacijos apsaugos agentūra (ENISA), Mokslinių tyrimų vykdomąja įstaiga (REA) arba Inovacijų ir tinklų programų vykdomąja įstaiga (INEA)).

Atlikus analizę buvo padaryta išvada, kad 1 galimybė geriausiai tinka iniciatyvos tikslams pasiekti, užtikrinant aukščiausią ekonominį, socialinį ir aplinkosauginį poveikį bei apsaugant

<sup>16</sup> Bendrųjų reikalų taryba: Tarybos išvados dėl Bendro komunikato Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“ (2017 m. lapkričio 20 d.).

<sup>17</sup> EIVT, 2018 m. kovo mėn.

Sąjungos interesus. Pagrindiniai šio pasirinkimo argumentai: galimybė kurti tikrą kibernetinio saugumo pramonės politiką remiant veiklą, susijusią ne tik su moksliniais tyrimais ir technologine plėtra, bet ir su diegimu rinkoje; lankstumas sudarant sąlygas plėtoti skirtingus bendradarbiavimo su kompetencijos centrų tinklu modelius, siekiant optimizuoti esamų žinių ir išteklių naudojimą; gebėjimas struktūrizuoti bendradarbiavimą ir bendrus viešojo ir privačiojo sektorių suinteresuotųjų šalių, atstovaujančių visiems susijusiems sektoriams, įskaitant gynybą, įsipareigojimus. Galiausiai, pasirinkus 1 galimybę galima padidinti sinergiją ir įgalinti dviejų skirtingų ES kibernetinio saugumo finansavimo srautų įgyvendinimo mechanizmą pagal kitą daugiametę finansinę programą (Skaitmeninės Europos programą, programą „Europos horizontas“).

- **Pagrindinės teisės**

Šia iniciatyva visų valstybių narių valdžios institucijoms ir pramonės įmonėms bus suteikta galimybė veiksmingiau užkirsti kelią kibernetinėms grėsmėms ir į jas reaguoti, siūlant saugesnius produktus ir sprendimus ir jais aprūpinant. Tai ypač svarbu siekiant užtikrinti galimybę naudotis pagrindinėmis paslaugomis (pvz., transporto, sveikatos apsaugos, bankų ir finansinėmis paslaugomis).

Padidėjęs Europos Sąjungos pajėgumas savarankiškai saugoti savo produktus ir paslaugas taip pat gali padėti piliečiams pasinaudoti savo demokratinėmis teisėmis ir vertybėmis (pvz., geriau apsaugoti Pagrindinių teisių chartijoje įtvirtintas su informacija susijusias teises, ypač teisę į asmens duomenų apsaugą ir privatų gyvenimą) ir taip padidinti jų pasitikėjimą skaitmenine visuomene ir ekonomika.

#### **4. POVEIKIS BIUDŽETUI**

Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras, bendradarbiaudamas su kibernetinio saugumo kompetencijos centrų tinklu, bus pagrindinė pagal Skaitmeninės Europos programą ir programą „Europos horizontas“ skirtų ES finansinių išteklių įgyvendinimo institucija.

Poveikis biudžetui, susijęs su Skaitmeninės Europos programos įdiegimu, yra išsamiai išdėstytas šio pasiūlymo priede pateiktoje finansinėje teisės akto pažymoje. Komisija per teisėkūros procedūrą ir bet koku atveju prieš pasiekiant politinį susitarimą pasiūlys įnašą iš programos „Europos horizontas“ II veiklos srities „Pasauliniai uždaviniai ir pramonės konkurencingumas“ veiksmų grupės „Įtrauki ir saugi visuomenė“ finansinio paketo (bendra paketo suma – 2 800 000 000 EUR), nurodytą 21 straipsnio 1 dalies b punkte Pasiūlymas bus pagrįstas strateginio planavimo proceso rezultatais, kaip apibrėžta Reglamento XXX 6 straipsnio 6 dalyje [bendroji programa „Europos horizontas“].

#### **5. KITI ELEMENTAI**

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

Pasiūlyme numatyta išsamaus vertinimo išlyga (38 straipsnis), kuria remdamasi Komisija atliks nepriklausomą vertinimą. Tada Komisija pateiks atlikto vertinimo ataskaitą Europos Parlamentui ir Tarybai ir, jei reikės, pasiūlymą peržiūrėti teisinę priemonę, kad būtų galima įvertinti priemonės ir jos pridėtinės vertės poveikį. Bus taikoma Komisijos geresnio reglamentavimo vertinimo metodika.

Vykdomasis direktorius kas dvejus metus, kaip nustatyta šio pasiūlymo 17 straipsnyje, Valdybai turėtų pateikti Europos kibernetinio saugumo pramonės, technologijų ir mokslinių

tyrimų kompetencijos centro ir Tinklo veiklos *ex post* vertinimą. Vykdomasis direktorius taip pat turėtų parengti tolesnių veiksmų planą dėl retrospektyvių įvertinimų išvadų ir kas dvejus metus teikti Komisijai padarytos pažangos ataskaitą. Valdyba turėtų būti atsakinga už tinkamų tolesnių veiksmų, susijusių su tokiomis išvadomis, stebėseną, kaip nustatyta šio pasiūlymo 16 straipsnyje.

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

## Pasiūlymas

**EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS****kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas**

*Europos Komisijos įnašas Zalcburgo vadovų susitikime 2018 m. rugsėjo 19–20 d.*

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 173 straipsnio 3 dalį ir 188 straipsnio pirmą pastraipą,

atsižvelgdami į Europos Komisijos pasiūlymą,

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę<sup>18</sup>,

atsižvelgdami į Regionų komiteto nuomonę<sup>19</sup>,

laikydami įprastos teisėkūros procedūros,

kadangi:

- (1) kasdienis mūsų gyvenimas ir ekonomika vis labiau priklauso nuo skaitmeninių technologijų, todėl piliečiams vis dažniau grėsmę kelia rimti kibernetiniai incidentai. Kad ateityje būtume saugūs, be kita ko, turime stiprinti savo technologinį ir pramoninį gebėjimą saugoti Sąjungą nuo kibernetinių grėsmių – tiek civilinė infrastruktūra, tiek karinis pajėgumas priklauso nuo saugių skaitmeninių sistemų;
- (2) kad išspręstų kylančias kibernetinio saugumo problemas, Sąjunga, remdamasi 2013 m. Kibernetinio saugumo strategija<sup>20</sup>, kuria siekiama kurti patikimą, saugią ir atvirą kibernetinę ekosistemą, nuolat plečia savo veiklą šioje srityje. 2016 m. Sąjunga priėmė pirmąsias kibernetinio saugumo priemones, išdėstytas Europos Parlamento ir Tarybos direktyvoje (ES) 2016/1148<sup>21</sup> dėl tinklų ir informacinių sistemų saugumo;
- (3) 2017 m. rugsėjo mėn. Komisija ir Sąjungos vyriausioji įgaliotinė užsienio reikalams ir saugumo politikai pristatė Bendrą komunikatą<sup>22</sup> „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“, kad būtų toliau stiprinamas Sąjungos atsparumas

<sup>18</sup> OL C [...], [...], p. [...].

<sup>19</sup> OL C [...], [...], p. [...].

<sup>20</sup> Bendras komunikatas Europos Parlamentui ir Tarybai Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“, JOIN(2013) 1 *final*.

<sup>21</sup> 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).

<sup>22</sup> Bendras komunikatas Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“, JOIN(2017) 450 *final*.

kibernetiniams išpuoliams, ir užtikrinta, kad nuo jų būtų atgrasoma labiau ir į juos reaguojama tinkamiau;

- (4) 2017 m. rugsėjo mėn. surengtame Talino aukščiausiojo lygio susitikime skaitmeniniais klausimais valstybių ir vyriausybių vadovai paragino Sąjungą tapti „pasauline lydere kibernetinio saugumo srityje iki 2025 m., siekiant užtikrinti mūsų piliečių, vartotojų ir įmonių pasitikėjimą ir apsaugą internete ir sudaryti sąlygas naudotis laisvu ir teisės aktais reglamentuojamu internetu“;
- (5) didelis tinklų ir informacinių sistemų sutrikimas gali paveikti atskiras valstybes nares ir visą Sąjungą. Todėl tinklų ir informacinių sistemų saugumas yra būtinas, kad vidaus rinka veiktų sklandžiai. Šiuo metu Sąjunga priklauso nuo ne Europos kibernetinio saugumo paslaugų teikėjų. Tačiau Sąjungai yra strategiškai svarbu išlaikyti ir plėtoti esminius kibernetinio saugumo technologinius pajėgumus, būtinus siekiant užtikrinti bendrosios skaitmeninės rinkos saugumą, apsaugoti ypatingos svarbos tinklus ir informacines sistemas ir teikti pagrindines kibernetinio saugumo paslaugas;
- (6) Sąjungoje sukaupta daug specialiųjų žinių ir patirties kibernetinio saugumo mokslinių tyrimų, technologijų ir pramonės srityje, tačiau pramonės ir mokslinių tyrimų bendruomenių pastangos yra suskaidytos ir nepakankamai suderintos, trūksta bendros misijos, todėl nukenčia konkurencingumas šioje srityje. Šios pastangos ir praktinė patirtis turi būti sutelktos, sujungtos tinkle ir naudojamos veiksmingai, siekiant sustiprinti ir papildyti esamus mokslinių tyrimų, technologinius ir pramonės pajėgumus Sąjungos ir nacionaliniu lygmenimis;
- (7) 2017 m. lapkričio mėn. priimtose Tarybos išvadose Komisija raginama skubiai atlikti poveikio vertinimą, kad išnagrinėtų kibernetinio saugumo kompetencijos centrų tinklo ir Europos mokslinių tyrimų ir kompetencijos centro kūrimo galimybes, ir iki 2018 m. vidurio pateikti pasiūlymą dėl atitinkamos teisinės priemonės;
- (8) Kompetencijos centras turėtų būti pagrindinė Sąjungos priemonė investicijoms į kibernetinio saugumo mokslinius tyrimus, technologijų ir pramonės plėtrą sutelkti, taip pat atitinkamiems projektams ir iniciatyvoms įgyvendinti kartu su Kibernetinio saugumo kompetencijos centrų tinklu. Jis turėtų užtikrinti finansinę paramą kibernetiniam saugumui iš programos „Europos horizontas“ ir Skaitmeninės Europos programos lėšų, o prireikus ir iš Europos regioninės plėtros fondo ir kitų programų. Toks požiūris turėtų padėti sukurti sinergiją ir koordinuoti finansinę paramą, susijusią su kibernetinio saugumo moksliniais tyrimais, inovacijomis, technologijomis ir pramonės plėtra, ir išvengti dubliavimosi;
- (9) atsižvelgiant į tai, kad šios iniciatyvos tikslų bus galima geriausiai pasiekti, jei dalyvaus visos valstybės narės arba kuo daugiau valstybių narių, valstybės narės skatinamos dalyvauti balsavimo teises suteikiant tik toms, kurios finansiškai prisideda padengiant Kompetencijos centro administracines ir veiklos išlaidas;
- (10) dalyvaujančiųjų valstybių narių finansinis indėlis turėtų būti proporcingas Sąjungos finansiniam įnašui į šią iniciatyvą;
- (11) Kompetencijos centras turėtų palengvinti Kibernetinio saugumo kompetencijos centrų tinklo (toliau – Tinklas), kurį sudaro kiekvienos valstybės narės nacionaliniai koordinavimo centrai, darbą ir padėti jį koordinuoti. Nacionaliniai koordinavimo centrai turėtų gauti tiesioginę Sąjungos finansinę paramą, įskaitant dotacijas, skirtas be kvietimo teikti pasiūlymus, kad galėtų vykdyti su šiuo reglamentu susijusią veiklą;
- (12) valstybės narės turėtų pasirinkti nacionalinius koordinavimo centrus. Be reikalingų administracinių pajėgumų, centrai turėtų turėti arba gauti galimybę tiesiogiai naudotis

kibernetinio saugumo technologinėmis žiniomis, ypač tokiose srityse kaip kriptografija, IRT saugumo paslaugos, įsibrovimų aptikimas, sistemos saugumas, tinklo saugumas, programinės įrangos ir programų saugumas arba žmogiškieji ir visuomeniniai saugumo ir privatumo aspektai. Jie taip pat turėtų turėti pakankamai pajėgumų, kad galėtų veiksmingai dalyvauti ir koordinuoti veiksmus su pramone, viešuoju sektoriumi, įskaitant institucijas, paskirtas pagal Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148<sup>23</sup>, ir mokslinių tyrimų bendruomenę;

- (13) kai nacionaliniams koordinavimo centrams teikiama finansinė parama, kad nacionaliniu lygmeniu būtų remiamos trečiosios šalys, ji perduodama atitinkamoms suinteresuotosioms šalims taikant pakopinius dotacijų susitarimus;
- (14) naujos technologijos, kaip dirbtinis intelektas, daiktų internetas, itin našus skaičiavimas (HPC) ir kvantinė kompiuterija, blokų grandinės ir tokios sąvokos kaip saugios skaitmeninės tapatybės tuo pat metu sukuria naujų kibernetinio saugumo uždavinių ir padeda rasti sprendimų. Norint įvertinti ir patvirtinti esamų ar būsimų IRT sistemų patikimumą, reikės išbandyti saugumo sprendimus, susijusius su išpuoliais, nukreiptais prieš HPC ir kvantinius skaičiavimus atliekančias mašinas. Kompetencijos centras, Tinklas ir kibernetinio saugumo kompetencijos bendruomenė turėtų padėti tobulinti ir skleisti naujausius kibernetinio saugumo sprendimus. Kartu Kompetencijos centras ir Tinklas turėtų tarnauti kūrėjams ir operatoriams, veikiantiems ypatingos svarbos sektoriuose, pavyzdžiui, transporto, energetikos, sveikatos apsaugos, finansų, valdžios, telekomunikacijų, gamybos, gynybos ir kosmoso, siekiant padėti jiems spręsti kibernetinio saugumo problemas;
- (15) Kompetencijos centrui turi būti priskirtos kelios pagrindinės funkcijos. Pirmą, Kompetencijos centras turėtų palengvinti Europos kibernetinio saugumo kompetencijos centrų tinklo darbą ir padėti jį koordinuoti ir puoselėti kibernetinio saugumo kompetencijos bendruomenę. Centras turėtų vykdyti kibernetinio saugumo technologinių klausimų darbotvarkę ir sudaryti palankesnes sąlygas naudotis Tinklo ir kibernetinio saugumo kompetencijos bendruomenės sukauptą praktinę patirtimi. Antra, jis turėtų įgyvendinti atitinkamas Skaitmeninės Europos programos ir programos „Europos horizontas“ dalis, skirdamas dotacijas, paprastai po konkurencija pagrįsto kvietimo teikti pasiūlymus. Trečia, Kompetencijos centras turėtų sudaryti palankesnes sąlygas bendroms Sąjungos, valstybių narių ir (arba) pramonės investicijoms;
- (16) Kompetencijos centras turėtų skatinti ir remti kibernetinio saugumo kompetencijos bendruomenės, kuri apimtų didelę, atvirą ir įvairią kuriant kibernetinio saugumo technologijas dalyvaujančių subjektų grupę, bendradarbiavimą ir jos veiklos koordinavimą. Ši bendruomenė visų pirma turėtų apimti mokslinių tyrimų subjektus, pasiūlos ir paklausos sričių pramonės įmones ir viešąjį sektorių. Kibernetinio saugumo kompetencijos bendruomenė turėtų prisidėti prie Kompetencijos centro veiklos ir darbo plano, jai taip pat turėtų būti naudinga Kompetencijos centro ir Tinklo bendruomenės stiprinimo veikla, tačiau ji neturėtų gauti jokių privilegijų, kai kalbama apie kvietimus teikti pasiūlymus arba kvietimus dalyvauti konkurse;
- (17) siekiant patenkinti ir paklausos, ir pasiūlos sričių pramonės įmonių poreikius, Kompetencijos centro užduotis teikti pramonės įmonėms su kibernetiniu saugumu

---

<sup>23</sup> 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).

susijusias žinias ir techninę pagalbą turėtų būti susijusi tiek su IRT produktais ir paslaugomis, tiek su visais kitais pramonės ir technologijų produktais ir sprendimais, kurių kibernetinis saugumas turi būti užtikrintas;

- (18) kadangi Kompetencijos centras ir Tinklas turėtų siekti kibernetinio saugumo civilinių ir gynybos aspektų sinergijos, pagal programą „Europos horizontas“ finansuojami projektai bus įgyvendinami vadovaujantis Reglamentu Nr. XXX [Programos „Europos horizontas“ reglamentu], kuriame numatyta, kad vykdant mokslinių tyrimų ir inovacijų veiklą pagal programą „Europos horizontas“ daugiausia dėmesio bus skiriama civilinėms reikmėms;
- (19) siekiant užtikrinti struktūrinį ir tvarų bendradarbiavimą, Kompetencijos centro ir nacionalinių koordinavimo centrų santykiai turėtų būti grindžiami sutartimis;
- (20) reikėtų nustatyti tinkamas Kompetencijos centro atsakomybę ir veiklos skaidrumą užtikrinančias nuostatas;
- (21) atsižvelgiant į jų atitinkamą praktinę patirtį kibernetinio saugumo srityje, Komisijos Jungtinis tyrimų centras ir Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA) turėtų aktyviai dalyvauti kibernetinio saugumo kompetencijos bendruomenės ir Pramonės ir mokslo patariamąsios tarybos veikloje;
- (22) gavę finansinį įnašą iš Sąjungos bendrojo biudžeto, nacionaliniai koordinavimo centrai ir subjektai, priklausantys kibernetinio saugumo kompetencijos bendruomenei, turėtų pavišinti informaciją, kad atitinkama veikla vykdoma pagal šią iniciatyvą;
- (23) Sąjungos įnašas į Kompetencijos centrą turėtų padengti pusę Kompetencijos centro įsteigimo, administravimo ir koordinavimo veiklos išlaidų. Siekiant išvengti dvigubo finansavimo, ši veikla neturėtų būti kartu finansuojama pagal kitas Sąjungos programas;
- (24) Kompetencijos centro valdyba, sudaryta iš valstybių narių ir Komisijos atstovų, turėtų apibrėžti bendrąją Kompetencijos centro veiklos kryptį ir užtikrinti, kad savo užduotis jis vykdytų pagal šį reglamentą. Valdybai turėtų būti suteikti įgaliojimai, būtini sudaryti biudžetą, tikrinti, kaip jis vykdomas, priimti reikiamas finansines taisykles, sukurti skaidrias Kompetencijos centro sprendimų priėmimo procedūras, priimti Kompetencijos centro darbo planą ir daugiametį strateginį planą, į kurį įtraukiami prioritetine tvarka išdėstyti Kompetencijos centro tikslai ir uždaviniai, nustatyti savo darbo tvarkos taisykles, paskirti vykdomąjį direktorių ir nuspręsti dėl vykdomojo direktoriaus kadencijos pratęsimo bei jos nutraukimo;
- (25) kad Kompetencijos centras veiktų tinkamai ir veiksmingai, Komisija ir valstybės narės turėtų užtikrinti, kad į Valdybą būtų skiriami tinkamos profesinės patirties ir patirties funkcinėse srityse turintys asmenys. Komisija ir valstybės narės taip pat turėtų stengtis riboti savo atstovų Valdyboje kaitą, kad būtų užtikrintas jos veiklos tęstinumas;
- (26) kad Kompetencijos centras veiktų sklandžiai, jo vykdomasis direktorius turi būti skiriamas atsižvelgiant į privalumus ir į dokumentais pagrįstus administracinio ir vadovaujamojo darbo įgūdžius, kompetenciją bei patirtį kibernetinio saugumo srityje, o vykdomojo direktoriaus pareigos turi būti atliekamos visiškai nepriklausomai;
- (27) siekiant palaikyti nuolatinį dialogą su privačiuoju sektoriumi, vartotojų organizacijomis ir kitomis atitinkamomis suinteresuotosiomis šalimis Kompetencijos centre turėtų būti įsteigta Pramonės ir mokslo patariamoji taryba, veikianti kaip patariamasis organas. Pramonės ir mokslo patariamoji taryba turėtų spręsti suinteresuotosioms šalims svarbias problemas ir pateikti jas svarstyti Kompetencijos



centro valdybai. Pramonės ir mokslo patariamiosios tarybos sudėtis ir jai paskirtos užduotys, pvz., konsultavimas darbo plano klausimais, turi būti suformuotos taip, kad būtų užtikrintas pakankamas suinteresuotųjų šalių atstovavimas Kompetencijos centro veikloje;

- (28) Pramonės ir mokslo patariamoji taryba turi sudaryti sąlygas Kompetencijos centrui pasinaudoti specialia praktine patirtimi ir plačiu bei atitinkamu suinteresuotųjų šalių atstovavimu, vykdamas viešojo ir privačiojo sektorių partnerystę kibernetinio saugumo srityje programos „Horizontas 2020“ vykdymo laikotarpiu;
- (29) Kompetencijos centras turėtų priimti interesų konfliktų prevencijos ir valdymo taisykles. Kompetencijos centras taip pat turėtų taikyti atitinkamas Sąjungos nuostatas dėl galimybės visuomenei susipažinti su dokumentais, kaip nustatyta Europos Parlamento ir Tarybos reglamente (EB) Nr. 1049/2001<sup>24</sup>. Kompetencijos centro vykdomam asmens duomenų tvarkymui taikomas Europos Parlamento ir Tarybos reglamentas (ES) Nr. XXX/2018. Kompetencijos centras turėtų laikytis Sąjungos institucijoms taikytinų nuostatų ir nacionalinės teisės aktų dėl informacijos, visų pirma neskelbtinos neįslaptintos ir ES įslaptintos informacija tvarkymo;
- (30) Sąjungos ir valstybių narių finansiniai interesai turėtų būti apsaugoti taikant proporcingas priemones viso išlaidų ciklo metu, įskaitant skirtas pažeidimų prevencijai, nustatymui ir tyrimui, prarastų, nepagrįstai išmokėtų ar netinkamai panaudotų lėšų susigrąžinimui ir, prireikus, administracinių ir finansinių sankcijų taikymui pagal Europos Parlamento ir Tarybos reglamentą Nr. XXX (ES, Euratomas)<sup>25</sup> [Finansinis reglamentas];
- (31) Kompetencijos centras turėtų veikti atvirai ir skaidriai, laiku teikti visą reikalingą informaciją, taip pat propaguoti savo veiklą, be kita ko, vykdyti platesnei visuomenei skirtą informavimo ir sklaidos veiklą. Kompetencijos centro organų darbo tvarkos taisyklės turėtų būti skelbiamos viešai;
- (32) Kompetencijos centro atžvilgiu Komisijos vidaus auditorius turėtų turėti tuos pačius įgaliojimus, kaip ir Komisijos atžvilgiu;
- (33) Komisijai, Kompetencijos centrui, Audito Rūmams ir Europos kovos su sukčiavimu tarnybai turėtų būti užtikrinta galimybė susipažinti su visa reikalinga informacija ir galimybė patekti į patalpas, kad jie galėtų atlikti Kompetencijos centro pasirašytų dotacijų, sutarčių ir susitarimų auditą ir tyrimą;
- (34) kadangi dėl išsklaidytų turimų ribotų išteklių ir dėl reikalingų investicijų masto valstybės narės negali deramai pasiekti šio reglamento tikslų, t. y. išsaugoti ir plėtoti Sąjungos kibernetinio saugumo technologinius ir pramonės pajėgumus, didinti Sąjungos kibernetinio saugumo pramonės konkurencingumą ir paversti kibernetinį saugumą konkurenciniu kitų Sąjungos pramonės įmonių pranašumu, o minėtus tikslus geriau galima pasiekti Sąjungos lygmeniu, išvengiant nereikalingo pastangų dubliavimo, padedant pasiekti kritinę investicijų masę ir užtikrinant, kad viešasis finansavimas būtų naudojamas optimaliai, remdamasi subsidiarumo principu, nustatytu Europos Sąjungos sutarties 5 straipsnyje, Sąjunga gali patvirtinti atitinkamas

---

<sup>24</sup> 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).

<sup>25</sup> [įrašyti pavadinimą ir OL nuorodą].

priemonės. Pagal tame straipsnyje nustatytą proporcingumo principą šiuo reglamentu neviršijama to, kas būtina nurodytam tikslui pasiekti,

PRIĖMĖ ŠĮ REGLAMENTĄ:

## I SKYRIUS

# KOMPETENCIJOS CENTRO IR TINKLO BENDROSIOS NUOSTATOS IR PRINCIPAI

### *1 straipsnis*

#### **Dalykas**

1. Šiuo reglamentu įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras (toliau – Kompetencijos centras), taip pat Nacionalinių koordinavimo centrų tinklas, ir nustatomos nacionalinių koordinavimo centrų paskyrimo ir kibernetinio saugumo kompetencijos bendruomenės kūrimo taisyklės.
2. Kompetencijos centras prisideda prie Skaitmeninės Europos programos, įsteigtos Reglamentu Nr. XXX, kibernetinio saugumo dalies įgyvendinimo, visų pirma veiksmų, numatytų Reglamento (ES) Nr. XXX [Skaitmeninės Europos programa] 6 straipsnyje, ir prie programos „Europos horizontas“, įsteigtos Reglamentu Nr. XXX, kibernetinio saugumo dalies įgyvendinimo, visų pirma Sprendimo Nr. XXX dėl specialiosios programos, kuria įgyvendinama bendroji mokslinių tyrimų ir inovacijų programa „Europos horizontas“ [Specialiosios programos nuorodos numeris] I priedo II veiksmų srities 2.2.6 punkto.
3. Kompetencijos centro buveinė yra [Briuselis, Belgija.]
4. Kompetencijos centras turi juridinio asmens statusą. Kiekvienoje valstybėje narėje jis naudojasi plačiausiu teisumu, suteikiamu juridiniams asmenims pagal tos valstybės narės įstatymus. Visų pirma jis gali įsigyti kilnojamojo ir nekilnojamojo turto ar juo disponuoti ir būti teismo proceso šalis.

### *2 straipsnis*

#### **Apibrėžtys**

Šiame reglamente vartojamų sąvokų apibrėžtys:

- (1) kibernetinis saugumas – tinklų ir informacinių sistemų, jų naudotojų ir kitų asmenų apsauga nuo kibernetinių grėsmių;
- (2) kibernetinio saugumo produktai ir sprendimai – IRT produktai, paslaugos ar procesai, kurių speciali paskirtis apsaugoti tinklų ir informacines sistemas, jų naudotojus ir susijusius asmenis nuo kibernetinių grėsmių;
- (3) valdžios institucija – nacionalinio, regioninio ar vietos lygmens valstybinė ar kita viešojo administravimo institucija, įskaitant viešąsias patariamąsias įstaigas, arba fizinis ar juridinis asmuo, vykdamas viešojo administravimo funkcijas pagal nacionalinę teisę, įskaitant konkrečias pareigas;
- (4) dalyvaujančioji valstybė narė – valstybė narė, kuri savanoriškai finansiškai prisideda padengiant Kompetencijos centro administracines ir veiklos išlaidas.

### 3 straipsnis

#### Centro ir Tinklo misija

1. Kompetencijos centras ir Tinklas padeda Sąjungai:
  - (a) išsaugoti ir plėtoti kibernetinio saugumo technologinius ir pramonės pajėgumus, reikalingus jos bendrajai skaitmeninei rinkai apsaugoti;
  - (b) didinti Sąjungos kibernetinio saugumo pramonės konkurencingumą ir paversti kibernetinį saugumą kitų Sąjungos pramonės įmonių konkurenciniu pranašumu.
2. Prireikus, Kompetencijos centras savo užduotis vykdo bendradarbiaudamas su Nacionalinių koordinavimo centrų tinklu ir kibernetinio saugumo kompetencijos bendruomene.

### 4 straipsnis

#### Centro tikslai ir uždaviniai

Kompetencijos centrui keliami šie tikslai ir susijusios užduotys:

1. palengvinti ir padėti koordinuoti 6 straipsnyje nurodyto Nacionalinių koordinavimo centrų tinklo (toliau – Tinklo) ir 8 straipsnyje nurodytos kibernetinio saugumo kompetencijos bendruomenės veiklą;
2. prisidėti prie Skaitmeninės Europos programos, įsteigtos Reglamentu Nr. XXX<sup>26</sup>, kibernetinio saugumo dalies įgyvendinimo, visų pirma veiksmų, numatytų Reglamento (ES) Nr. XXX [Skaitmeninės Europos programa] 6 straipsnyje, ir prie programos „Europos horizontas“, įsteigtos Reglamentu Nr. XXX<sup>27</sup>, kibernetinio saugumo dalies įgyvendinimo, visų pirma Sprendimo Nr. XXX dėl specialiosios programos, kuria įgyvendinama bendroji mokslinių tyrimų ir inovacijų programa „Europos horizontas“ [Specialiosios programos nuorodos numeris] I priedo II veiksmų srities 2.2.6 punkto, bei prie kitų Sąjungos programų įgyvendinimo, jei tai numatyta Sąjungos teisės aktuose;
3. stiprinti kibernetinio saugumo pajėgumus, žinias ir infrastruktūrą, kuriais naudojasi pramonės įmonės, viešasis sektorius ir mokslinių tyrimų bendruomenės, vykdant šias užduotis:
  - (a) atsižvelgiant į pažangiausią kibernetinio saugumo pramonės ir mokslinių tyrimų infrastruktūrą ir susijusias paslaugas, įsigyti, atnaujinti ir eksploatuoti tokią infrastruktūrą ir sudaryti sąlygas ja naudotis ir teikti susijusias paslaugas įvairiems naudotojams iš pramonės sektoriaus visoje Sąjungoje, įskaitant MVI, viešąjį sektorių ir mokslinių tyrimų bei mokslo bendruomenę;
  - (b) atsižvelgiant į pažangiausią kibernetinio saugumo pramonės ir mokslinių tyrimų infrastruktūrą ir susijusias paslaugas, teikti paramą (ir finansinę) kitiems subjektams įsigyjant, atnaujinant ir eksploatuojant tokią infrastruktūrą ir sudarant sąlygas ja naudotis ir teikiant susijusias paslaugas įvairiems naudotojams iš pramonės sektoriaus visoje

<sup>26</sup> [įrašyti visą pavadinimą ir OL nuorodą].

<sup>27</sup> [įrašyti visą pavadinimą ir OL nuorodą].

- Sąjungoje, įskaitant MVI, viešąjį sektorių ir mokslinių tyrimų ir mokslo bendruomenę;
- (c) perduoti kibernetinio saugumo žinias ir teikti techninę pagalbą pramonei ir valdžios institucijoms, visų pirma remiant veiksmus, kuriais siekiama palengvinti galimybę naudotis Tinklo ir kibernetinio saugumo kompetencijos bendruomenės sukaupta praktine patirtimi;
4. prisidėti prie plataus masto pažangiausių kibernetinio saugumo produktų ir sprendimų įdiegimo visoje ekonomikoje, vykdant šias užduotis:
- (a) skatinti valdžios institucijas ir naudotojų pramonės įmones vykdyti kibernetinio saugumo mokslinius tyrimus, kurti ir naudoti Sąjungos kibernetinio saugumo produktus ir sprendimus;
  - (b) padėti valdžios institucijoms, paklausos srities pramonės įmonėms ir kitiems naudotojams diegti ir integruoti naujausius kibernetinio saugumo sprendimus;
  - (c) padėti visų pirma valdžios institucijoms organizuoti viešuosius pirkimus arba jų vardu įsigyti pažangiausius kibernetinio saugumo produktus ir sprendimus;
  - (d) teikti finansinę paramą ir techninę pagalbą kibernetinio saugumo srityje veikiantiems startuoliams ir MVI, šiems prisijungiant prie potencialių rinkų ir pritraukiant investicijas;
5. pagerinti supratimą apie kibernetinį saugumą ir prisidėti prie kibernetinio saugumo įgūdžių trūkumo mažinimo Sąjungoje, vykdant šias užduotis:
- (a) remti tolesnį kibernetinio saugumo įgūdžių tobulinimą, prireikus bendradarbiaujant su atitinkamomis ES agentūromis ir įstaigomis, įskaitant ENISA;
6. prisidėti prie kibernetinio saugumo mokslinių tyrimų ir technologinės plėtros Sąjungoje stiprinimo:
- (a) finansuojant kibernetinio saugumo mokslinius tyrimus, pagrįstus bendra, nuolat vertinama ir patobulinta daugiamete strategine, pramonės, technologijų ir mokslinių tyrimų darbotvarke;
  - (b) remiant plataus masto mokslinių tyrimų ir demonstravimo projektus naujos kartos kibernetinio saugumo technologinių pajėgumų srityje, bendradarbiaujant su pramone ir Tinklu;
  - (c) remiant mokslinius tyrimus ir inovacijas, skirtas kibernetinio saugumo technologijoms standartizuoti;
7. skatinti civilinio ir gynybos sektorių bendradarbiavimą dvejopo panaudojimo technologijų ir taikomųjų programų kibernetinio saugumo srityje vykdant šias užduotis:
- (a) remti valstybes nares ir pramonės bei mokslinių tyrimų suinteresuotąsias šalis mokslinių tyrimų, technologinės plėtros ir diegimo srityse;
  - (b) prisidėti prie valstybių narių bendradarbiavimo, remiant švietimą, mokymą ir pratybas;
  - (c) sutelkti suinteresuotąsias šalis, kad būtų skatinama civilinio ir gynybos kibernetinio saugumo mokslinių tyrimų ir rinkų sinergija;

8. didinti kibernetinio saugumo civilinių ir gynybos aspektų sinergiją, susijusią su Europos gynybos fondu, vykdant šias užduotis:
- (a) konsultuoti, dalytis praktine patirtimi ir palengvinti atitinkamų suinteresuotųjų šalių bendradarbiavimą;
  - (b) valdyti tarptautinius kibernetinės gynybos projektus, kai to reikalauja valstybės narės, ir vykdyti projektų valdytojo pareigas, kaip apibrėžta Reglamente Nr. XXX [Reglamentas dėl Europos gynybos fondo įsteigimo].

#### *5 straipsnis*

#### **Investicijos į infrastruktūrą, pajėgumus, produktus ar sprendimus ir jų naudojimas**

1. Jei Kompetencijos centras finansuoja infrastruktūrą, pajėgumus, produktus ar sprendimus pagal 4 straipsnio 3 ir 4 dalis dotacijos ar apdovanojimo forma, Kompetencijos centro darbo plane gali būti nurodytos:
  - (a) taisyklės, kuriomis reglamentuojamas infrastruktūros ar pajėgumų eksploatavimas, įskaitant (jei taikoma) pavedimą jį vykdyti prieglobos paslaugą teikiančiam subjektui remiantis kriterijais, kuriuos nustato Kompetencijos centras;
  - (b) taisyklės, kuriomis reglamentuojama prieiga prie infrastruktūros ar pajėgumų ir jų naudojimas.
2. Kompetencijos centras gali būti atsakingas už bendrų viešųjų pirkimų veiksmų, įskaitant ikiprekybinius viešuosius pirkimus, vykdymą Tinklo narių, kibernetinio saugumo kompetencijos bendruomenės narių ar kitų trečiųjų šalių, atstovaujančių kibernetinio saugumo produktų ir sprendimų naudotojams, vardu. Tuo tikslu Kompetencijos centrai gali padėti vienas ar keli nacionaliniai koordinavimo centrai arba kibernetinio saugumo kompetencijos bendruomenės nariai.

#### *6 straipsnis*

#### **Nacionalinių koordinavimo centrų paskyrimas**

1. Iki [data] kiekviena valstybė narė paskiria subjektą, kuris šio reglamento tikslais vykdys nacionalinio koordinavimo centro funkcijas, ir praneša apie jį Komisijai.
2. Remdamasi šio subjekto atitikties 4 dalyje nustatytiems kriterijams įvertinimu, Komisija priima sprendimą per šešis mėnesius nuo paskyrimo, apie kurį pranešė valstybė narė, ir nurodo akredituoti subjektą kaip nacionalinį koordinavimo centrą arba atmesti kandidatūrą. Nacionalinių koordinavimo centrų sąrašą skelbia Komisija.
3. Šio reglamento tikslais valstybės narės bet kada gali paskirti naują subjektą vykdyti nacionalinio koordinavimo centro funkcijas. Paskiriant naują subjektą taikomos 1 ir 2 dalys.
4. Paskirtasis nacionalinis koordinavimo centras turi galėti padėti Kompetencijos centrai ir Tinklui vykdyti jų misiją, išdėstytą šio reglamento 3 straipsnyje. Jie turi turėti arba gauti galimybę tiesiogiai naudotis technologinėmis žiniomis kibernetinio saugumo srityje bei turėti galimybę veiksmingai bendrauti ir koordinuoti veiksmus su pramonės, viešojo sektoriaus ir mokslinių tyrimų bendruomenės atstovais.

5. Kompetencijos centro ir nacionalinių koordinavimo centrų santykiai grindžiami Kompetencijos centro ir kiekvieno nacionalinio koordinavimo centro pasirašytomis sutartimis. Sutartyse numatomos taisyklės, kuriomis reglamentuojami santykiai ir užduočių pasidalijimas tarp Kompetencijos centro ir kiekvieno nacionalinio koordinavimo centro.
6. Nacionalinių koordinavimo centrų tinklą sudaro visi valstybių narių paskirti nacionaliniai koordinavimo centrai.

### *7 straipsnis*

#### **Nacionalinių koordinavimo centrų užduotys**

1. Nacionalinių koordinavimo centrų užduotys yra šios:
  - (a) remti Kompetencijos centrą šiam siekiant savo tikslų, visų pirma koordinuojant kibernetinio saugumo kompetencijos bendruomenės veiklą;
  - (b) palengvinti pramonės ir kitų subjektų dalyvavimą tarpvalstybiniuose projektuose valstybių narių lygmeniu;
  - (c) kartu su Kompetencijos centru prisidėti prie konkrečiam sektoriui būdingų kibernetinio saugumo pramonės problemų nustatymo ir sprendimo;
  - (d) būti nacionalinio lygmens ryšių palaikymo centru kibernetinio saugumo kompetencijos bendruomenei ir Kompetencijos centrui;
  - (e) siekti sukurti sinergiją su atitinkama nacionaliniu ir regioniniu lygmenimis vykdoma veikla;
  - (f) įgyvendinti konkrečius veiksmus, kuriems Kompetencijos centras skyrė dotacijas, taip pat teikiant finansinę paramą trečiosioms šalims pagal Reglamento Nr. XXX [naujas Finansinis reglamentas] 204 straipsnį, laikantis atitinkamuose dotacijų susitarimuose nurodytų sąlygų;
  - (g) propaguoti ir skleisti atitinkamus Tinklo, kibernetinio saugumo kompetencijos bendruomenės ir Kompetencijos centro darbo rezultatus nacionaliniu arba regioniniu lygmeniu;
  - (h) vertinti toje pačioje valstybėje narėje, kaip koordinavimo centras, įsteigtų subjektų prašymus tapti kibernetinio saugumo kompetencijos bendruomenės dalimi.
2. Taikant f punktą finansinė parama trečiosioms šalims gali būti teikiama visomis formomis, nurodytomis Reglamento Nr. XXX [naujas Finansinis reglamentas] 125 straipsnyje, įskaitant vienkartinės išmokas.
3. Nacionaliniai koordinavimo centrai gali gauti Sąjungos dotaciją pagal Reglamento Nr. XXX [naujas Finansinis reglamentas] 195 straipsnio d punktą šiame straipsnyje nustatytoms užduotims vykdyti.
4. Prireikus, nacionaliniai koordinavimo centrai bendradarbiauja Tinklo lygmeniu, kad galėtų vykdyti 1 dalies a, b, c, e ir g punktuose nurodytas užduotis.

### *8 straipsnis*

#### **Kibernetinio saugumo kompetencijos bendruomenė**

1. Kibernetinio saugumo kompetencijos bendruomenė turi prisidėti prie Kompetencijos centro misijos, išdėstytos 3 straipsnyje, ir stiprinti bei skleisti kibernetinio saugumo praktinę patirtį Sąjungoje.
2. Kibernetinio saugumo kompetencijos bendruomenę sudaro pramonės, akademinės ir ne pelno mokslinių tyrimų organizacijos ir asociacijos bei valdžios institucijos ir kiti subjektai, sprendžiantys veiklos ir techninius klausimus. Ji sutelkia pagrindines suinteresuotąsias šalis, susijusias su Sąjungos kibernetinio saugumo technologiniais ir pramonės pajėgumais. Jos veikloje dalyvauja nacionaliniai koordinavimo centrai, taip pat reikiamos praktinės patirties turinčios Sąjungos institucijos ir įstaigos.
3. Tik Sąjungoje įsteigti subjektai gali būti akredituoti kaip kibernetinio saugumo kompetencijos bendruomenės nariai. Jie turi įrodyti, kad yra kompetentingi kibernetinio saugumo klausimais bent vienoje iš toliau išvardytų sričių:
  - (a) mokslinių tyrimų,
  - (b) pramonės plėtros,
  - (c) mokymo ir švietimo.
4. Kompetencijos centras akredituoja pagal nacionalinę teisę įsteigtus subjektus kaip kibernetinio saugumo kompetencijos bendruomenės narius, valstybės narės, kurioje įsteigtas subjektas, nacionaliniam koordinavimo centrui atlikus įvertinimą ir įsitikinęs, kad minėtasis subjektas atitinka 3 dalyje nustatytus kriterijus. Akreditacijos galiojimo laikas nėra ribotas, tačiau Kompetencijos centras gali ją bet kuriuo metu atšaukti, jei jis arba atitinkamas nacionalinis koordinavimo centras mano, kad subjektas neatitinka 3 dalyje išdėstytų kriterijų arba jam taikomos atitinkamos nuostatos, išdėstytos Reglamento Nr. XXX [naujas Finansinis reglamentas] 136 straipsnyje.
5. Atlikęs įvertinimą ir įsitikinęs, kad minėtasis subjektas atitinka 3 dalyje nustatytus kriterijus, Kompetencijos centras akredituoja atitinkamas Sąjungos įstaigas, agentūras ir biurus kaip kibernetinio saugumo kompetencijos bendruomenės narius. Akreditacijos galiojimo laikas nėra ribotas, tačiau Kompetencijos centras gali ją bet kuriuo metu atšaukti, jei jis mano, kad subjektas neatitinka 3 dalyje išdėstytų kriterijų arba jam taikomos atitinkamos nuostatos, išdėstytos Reglamento Nr. XXX [naujas Finansinis reglamentas] 136 straipsnyje.
6. Bendruomenės veikloje gali dalyvauti Komisijos atstovai.

#### *9 straipsnis*

#### **Kibernetinio saugumo kompetencijos bendruomenės narių užduotys**

Kibernetinio saugumo kompetencijos bendruomenės nariai turi:

- (1) padėti Kompetencijos centrui įgyvendinti 3 ir 4 straipsniuose apibrėžtą misiją ir tikslus, ir šiuo tikslu glaudžiai bendradarbiauti su Kompetencijos centru ir atitinkamais nacionaliniais koordinavimo centrais;
- (2) dalyvauti Kompetencijos centro ir nacionalinių koordinavimo centrų remiamoje veikloje;
- (3) prireikus dalyvauti Kompetencijos centro valdybos įsteigtose darbo grupėse konkrečiai veiklai atlikti, kaip numatyta Kompetencijos centro darbo plane;

- (4) prireikus padėti Kompetencijos centrui ir nacionaliniams koordinavimo centrams propaguoti konkrečius projektus;
- (5) propaguoti ir skleisti svarbius bendruomenės vykdomos veiklos ir projektų rezultatus.

#### *10 straipsnis*

### **Kompetencijos centro bendradarbiavimas su Sąjungos institucijomis, įstaigomis, biurais ir agentūromis**

1. Kompetencijos centras bendradarbiauja su atitinkamomis Sąjungos institucijomis, įstaigomis, biurais ir agentūromis, įskaitant Europos Sąjungos tinklą ir informacijos apsaugos agentūrą, Kompiuterinių incidentų tyrimo tarnybą (CERT-EU), Europos išorės veiksmų tarnybą, Komisijos Jungtinių tyrimų centrą, Mokslinių tyrimų vykdomąją įstaigą, Inovacijų ir tinklų programų vykdomąją įstaigą, Europolo Europos kovos su elektroniniu nusikalstamumu centrą ir Europos gynybos agentūrą.
2. Toks bendradarbiavimas grindžiamas darbiniais susitarimais, kurie pateikiami išankstiniam Komisijos pritarimui gauti.

## **II SKYRIUS**

### **KOMPETENCIJOS CENTRO ORGANIZACIJA**

#### *11 straipsnis*

#### **Narystė ir struktūra**

1. Kompetencijos centro nariai yra Sąjunga, kuriai atstovauja Komisija, ir valstybės narės.
2. Kompetencijos centro struktūrą sudaro:
  - (a) Valdyba, atliekanti 13 straipsnyje nustatytas užduotis,
  - (b) vykdomasis direktorius, atliekantis 16 straipsnyje nustatytas užduotis,
  - (c) Pramonės ir mokslo patariamoji taryba, atliekanti 20 straipsnyje nustatytas funkcijas.

#### **I SKIRSNIS**

#### **VALDYBA**

#### *12 straipsnis*

#### **Valdybos sudėtis**

1. Valdybą sudaro po vieną kiekvienos valstybės narės atstovą ir penki Komisijos atstovai, veikiantys Sąjungos vardu.
2. Kiekvienas Valdybos narys turi pakaitinį narį, kuris atstovauja nariui šiam nedalyvaujant.
3. Valdybos nariai ir jų pakaitiniai nariai skiriami atsižvelgiant į jų žinias technologijų srityje, taip pat į valdymo, administracinio darbo ir biudžeto valdymo įgūdžius. Komisija ir valstybės narės deda pastangas apriboti savo atstovų Valdyboje kaitą,



siekiant užtikrinti jos veiklos tęstinumą. Komisija ir valstybės narės siekia užtikrinti vyrų ir moterų atstovavimo pusiausvyrą Valdyboje.

4. Valdybos narių ir jų pakaitinių narių kadencija – ketveri metai. Ta kadencija gali būti pratęsta.
5. Valdybos nariai nepriklausomai ir skaidriai vykdo veiklą vadovaudamiesi Kompetencijos centro interesais, gindami jo tikslus ir misiją, tapatybę, savarankiškumą ir darną.
6. Komisija gali pakviesti stebėtojus, įskaitant atitinkamų Sąjungos įstaigų, biurų ir agentūrų atstovus, prireikus dalyvauti Valdybos posėdžiuose.
7. Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA) Valdyboje turi nuolatinio stebėtojo statusą.

### *13 straipsnis*

#### **Valdybos užduotys**

1. Valdyba bendrai atsako už Kompetencijos centro strateginę kryptį bei operacijas ir prižiūri jo veiklos įgyvendinimą.
2. Valdyba priima savo darbo tvarkos taisykles. Tos taisyklės apima konkrečias interesų konfliktų nustatymo ir prevencijos, taip pat neskelbtinos informacijos konfidencialumo užtikrinimo procedūras.
3. Valdyba priima reikiamus strateginius sprendimus, visų pirma:
  - (a) tvirtina daugiametį strateginį planą, kuriame išdėstomi svarbiausi Kompetencijos centro prioritetai ir planuojamos iniciatyvos, įskaitant finansavimo poreikių ir šaltinių įvertinimą;
  - (b) remdamasi vykdomojo direktoriaus siūlymu, tvirtina Kompetencijos centro darbo planą, metines finansines ataskaitas ir balansą bei metinę veiklos ataskaitą;
  - (c) priima konkrečias finansines Kompetencijos centro taisykles pagal [Finansinio reglamento 70 straipsnį];
  - (d) priima vykdomojo direktoriaus skyrimo tvarką;
  - (e) priima kriterijus ir procedūras subjektams vertinti ir akredituoti kaip kibernetinio saugumo kompetencijos bendruomenės narius;
  - (f) skiria ir atleidžia vykdomąjį direktorių, pratęsia jo kadenciją, teikia jam konsultacijas, stebi vykdomojo direktoriaus veiklos rezultatus ir skiria apskaitos pareigūną;
  - (g) tvirtina Kompetencijos centro metinį biudžetą, įskaitant atitinkamą personalo etatų planą, kuriame nurodomas laikinų etatų pagal pareigų grupes ir lygį skaičius, taip pat sutartininkų ir deleguotųjų nacionalinių ekspertų skaičius, išreikštas etato ekvivalentu;
  - (h) priima interesų konfliktų taisykles;
  - (i) su kibernetinio saugumo kompetencijos bendruomenės nariais steigia darbo grupes;
  - (j) skiria Pramonės ir mokslo patarimosios tarybos narius;

- (k) įkuria vidaus audito padalinį pagal Komisijos deleguotąjį reglamentą (EB) Nr. 1271/2013<sup>28</sup>;
- (l) propaguoja Kompetencijos centrą visame pasaulyje, kad padidintų jo patrauklumą ir jis taptų pasaulinio lygio aukščiausios kompetencijos įstaiga kibernetinio saugumo srityje;
- (m) pagal vykdomojo direktoriaus rekomendaciją rengia Kompetencijos centro komunikacijos politiką;
- (n) yra atsakinga už tinkamų tolesnių veiksmų, susijusių su retrospektyvių vertinimų išvadomis, stebėseną;
- (o) prireikus pagal 31 straipsnio 3 dalį rengia Tarnybos nuostatų ir Įdarbinimo sąlygų įgyvendinimo taisykles;
- (p) prireikus nustato taisykles dėl nacionalinių ekspertų komandiravimo į Kompetencijos centrą ir stažuotojų pasitelkimą pagal 32 straipsnio 2 dalį;
- (q) tvirtina Kompetencijos centro saugumo taisykles;
- (r) atsižvelgdama į įgyvendintinių priemonių ekonominės naudos analizę, priima kovos su sukčiavimu strategiją, kuri proporcingai atitinka sukčiavimo riziką;
- (s) tvirtina valstybių narių finansinio įnašo apskaičiavimo metodiką;
- (t) yra atsakinga už visas užduotis, kurių Kompetencijos centras nėra konkrečiai paskyręs vykdyti vienam iš savo organų; ji gali skirti tokias užduotis bet kuriam Kompetencijos centro atstovui.

#### 14 straipsnis

#### **Valdybos pirmininkas ir susirinkimai**

1. Valdyba iš savo balso teisę turinčių narių renka pirmininką ir pirmininko pavaduotoją dvejų metų laikotarpiui. Valdybos sprendimu pirmininko ir pirmininko pavaduotojo kadencija gali būti pratęsiama tik vieną kartą. Tačiau jei bet kuriuo kadencijos metu jie netenka Valdybos nario statuso, tą pačią dieną automatiškai baigiasi ir jų kadencija. Pirmininko pavaduotojas *ex officio* pakeičia pirmininką, jei šis negali vykdyti savo pareigų. Pirmininkas balsuoja.
2. Valdyba rengia eilinius posėdžius bent tris kartus per metus. Komisijos, trečdalis visų jos narių, pirmininko arba vykdomojo direktoriaus, šiam vykdamas savo užduotis, prašymu ji gali surengti neeilinius posėdžius.
3. Vykdomasis direktorius dalyvauja svarstymuose, išskyrus atvejus, kai Valdyba nusprendžia kitaip, tačiau neturi balsavimo teisės. Kiekvienu konkrečiu atveju Valdyba į savo posėdžius dalyvauti stebėtojų teisėmis gali pakviesti kitų asmenų.
4. Pirmininko kvietimu Valdybos posėdžiuose Pramonės ir mokslo patariamąsios tarybos nariai gali dalyvauti be balsavimo teisės.
5. Pagal darbo tvarkos taisykles Valdybos nariams ir jų pakaitiniams nariams posėdžiuose gali padėti patarėjai arba ekspertai.

---

<sup>28</sup> 2013 m. rugsėjo 30 d. Komisijos deleguotasis reglamentas (ES) Nr. 1271/2013 dėl finansinio pagrindų reglamento, taikomo įstaigoms, nurodytoms Europos Parlamento ir Tarybos reglamento (ES, Euratomas) Nr. 966/2012 208 straipsnyje (OL L 328, 2013 12 7, p. 42).

6. Kompetencijos centras vykdo Valdybos sekretoriato funkciją.

*15 straipsnis*

**Valdybos balsavimo taisyklės**

1. Sąjungai priklauso 50 % balsavimo teisių. Sąjungos balsavimo teisės yra nedalomos.
2. Kiekviena dalyvaujančioji valstybė narė turi vieną balsą.
3. Valdyba priima sprendimus ne mažiau kaip 75 % visų balsų, įskaitant nedalyvaujančių narių balsus, dauguma, kuri sudaro ne mažiau kaip 75 % visų finansinių įnašų į Kompetencijos centrą. Finansinis įnašas apskaičiuojamas remiantis 17 straipsnio 2 dalies c punkte nurodytomis valstybių narių pasiūlytomis išlaidomis ir remiantis 22 straipsnio 5 dalyje nurodytų dalyvaujančiųjų valstybių narių įnašų vertės ataskaita.
4. Balsavimo teisės priklauso tik Komisijos atstovams ir dalyvaujančiųjų valstybių narių atstovams.
5. Pirmininkas balsuoja.

**II SKIRSNIS**

**VYKDOMASIS DIREKTORIUS**

*16 straipsnis*

**Vykdomojo direktoriaus skyrimas, atleidimas ar kadencijos pratęsimas**

1. Vykdomasis direktorius yra asmuo, turintis patirties ir gerą reputaciją Kompetencijos centro veiklos srityse.
2. Remiantis Kitų tarnautojų įdarbinimo sąlygų 2 straipsnio a punktu, vykdomasis direktorius įdarbinamas kaip Kompetencijos centro laikinai priimtas tarnautojas.
3. Vykdomąjį direktorių skiria Valdyba iš Komisijos pasiūlytų kandidatų sąrašo po atviros ir skaidrios atrankos procedūros.
4. Sudarant sutartį su vykdomuoju direktoriumi Kompetencijos centrui atstovauja Valdybos pirmininkas.
5. Vykdomojo direktoriaus kadencija – ketveri metai. To laikotarpio pabaigoje Komisija atlieka vertinimą, kuriame atsižvelgiama į vykdomojo direktoriaus veiklos rezultatų vertinimą ir būsimas Kompetencijos centro užduotis ir iššūkius.
6. Remdamasi Komisijos pasiūlymu, kuriame atsižvelgiama į 5 dalyje nurodytą vertinimą, Valdyba gali vieną kartą pratęsti vykdomojo direktoriaus kadenciją ne daugiau kaip ketveriems metams.
7. Vykdomasis direktorius, kurio kadencija buvo pratęsta, negali dalyvauti kitoje atrankos į tą pačią pareigybę procedūroje.
8. Vykdomasis direktorius pašalinamas iš pareigų tik Valdybos, kuri remiasi Komisijos siūlymu, sprendimu.

*17 straipsnis*

**Vykdomojo direktoriaus užduotys**

1. Vykdomasis direktorius atsako už kasdienį Kompetencijos centro valdymą bei jo operacijas ir yra jo teisėtas atstovas. Vykdomasis direktorius yra atskaitingas Valdybai ir vykdo savo pareigas visiškai nepriklausomai, neviršydamas jam suteiktų įgaliojimų.
2. Vykdomasis direktorius visų pirma nepriklausomai atlieka šias užduotis:
  - (a) įgyvendina Valdybos priimtus sprendimus;
  - (b) padeda Valdybai atlikti savo darbą, užtikrina sekretoriato paslaugas per jos posėdžius ir teikia visą jos pareigoms atlikti būtiną informaciją;
  - (c) pasikonsultavęs su Valdyba ir Komisija, parengia ir pateikia Valdybai patvirtinti daugiamečio strateginio plano projektą ir Kompetencijos centro metinio darbo plano projektą, įskaitant kvietimų teikti pasiūlymus, kvietimų pareikšti susidomėjimą ir kvietimų dalyvauti konkurse apimtį, reikalingą darbo planui įgyvendinti, ir atitinkamas valstybių narių ir Komisijos pasiūlytas išlaidų sąmatas;
  - (d) rengia ir teikia Valdybai tvirtinti metinio biudžeto projektą, įskaitant atitinkamą personalo etatų planą, kuriame nurodomas laikinų etatų pagal kiekvieną lygį ir pareigų grupę skaičius, taip pat sutartininkų ir deleguotųjų nacionalinių ekspertų skaičius, išreikštas etato ekvivalentu;
  - (e) įgyvendina darbo planą ir praneša apie tai Valdybai;
  - (f) rengia Kompetencijos centro metinės veiklos ataskaitos projektą, įskaitant informaciją apie atitinkamas išlaidas;
  - (g) užtikrina, kad būtų įgyvendintos veiksmingos stebėsenos ir vertinimo procedūros, susijusios su Kompetencijos centro veiklos rezultatais;
  - (h) rengia tolesnių veiksmų planą atsižvelgiant į retrospektyvių įvertinimų išvadas ir kas dvejus metus teikia Komisijai padarytos pažangos ataskaitą;
  - (i) rengia, veda derybas ir sudaro susitarimus su nacionaliniais koordinavimo centrais;
  - (j) yra atsakingas už administracinius, finansinius ir personalo klausimus, įskaitant Kompetencijos centro biudžeto įgyvendinimą, deramai atsižvelgdamas į vidaus audito padalinio rekomendacijas, neviršydamas Valdybos suteiktų įgaliojimų;
  - (k) tvirtina ir tvarko kvietimų teikti pasiūlymus paskelbimą pagal darbo planą ir administruoja dotacijų susitarimus ir sprendimus;
  - (l) tvirtina pagal nepriklausomų ekspertų grupės parengtą eilės sąrašą finansuoti atrinktų veiksmų sąrašą;
  - (m) tvirtina ir tvarko kvietimų dalyvauti konkurse paskelbimą pagal darbo planą ir administruoja sutartis;
  - (n) tvirtina finansuoti atrinktus konkurso tvarka gautus pasiūlymus;
  - (o) teikia metinės finansinės atskaitomybės ir balanso projektą vidaus audito padaliniui, o vėliau – Valdybai;
  - (p) užtikrina, kad būtų atliekamas rizikos vertinimas ir rizikos valdymas;
  - (q) pasirašo konkrečius dotacijų susitarimus, sprendimus ir sutartis;
  - (r) pasirašo viešojo pirkimo sutartis;

- (s) rengia veiksmų planą, kuriuo atsižvelgiama į vidaus ar išorės audito ataskaitų išvadas, taip pat į Europos kovos su sukčiavimu tarnybos (OLAF) atliktus tyrimus, ir teikia padarytos pažangos ataskaitas du kartus per metus – Komisijai ir reguliariai – Valdybai;
- (t) rengia Kompetencijos centro taikytinų finansinių taisyklių projektą;
- (u) nustato efektyvią ir veiksmingą vidaus kontrolės sistemą, užtikrina jos veikimą ir Valdybai praneša apie visus reikšmingus jos pakeitimus;
- (v) užtikrina veiksmingus ryšius su Sąjungos institucijomis;
- (w) imasi bet kokių kitų priemonių, reikalingų Kompetencijos centro pažangai, padarytai siekiant jo misijos ir tikslų, nustatytų šio reglamento 3 ir 4 straipsniuose, įvertinti;
- (x) atlieka visas kitas Valdybos jam patikėtas ar skirtas užduotis.

### **III SKIRSNIS**

#### **PRAMONĖS IR MOKSLO PATARIAMOJI TARYBA**

##### *18 straipsnis*

##### **Pramonės ir mokslo patariamąsios tarybos sudėtis**

1. Pramonės ir mokslo patariamąją tarybą sudaro ne daugiau kaip 16 narių. Narius iš kibernetinio saugumo kompetencijos bendruomenės subjektų atstovų skiria Valdyba.
2. Pramonės ir mokslo patariamąsios tarybos nariai turi būti kompetentingi kibernetinio saugumo tyrimų, pramonės plėtros, profesinių paslaugų ar jų diegimo srityse. Šios praktinės patirties reikalavimus papildomai nurodo Valdyba.
3. Patariamąsios tarybos narių paskyrimo Valdybos sprendimu ir Patariamąsios tarybos veiklos procedūros nustatomos Kompetencijos centro darbo tvarkos taisyklėse ir viešai skelbiamos.
4. Pramonės ir mokslo patariamąsios tarybos nariai skiriami trejiems metams. Ta kadencija gali būti pratęsta.
5. Komisijos ir Europos tinklų ir informacijos apsaugos agentūros atstovai gali dalyvauti Pramonės ir mokslo patariamąsios tarybos veikloje ir ją remti.

##### *19 straipsnis*

##### **Pramonės ir mokslo patariamąsios tarybos veikla**

1. Pramonės ir mokslo patariamąoji taryba susitinka bent du kartus per metus.
2. Pramonės ir mokslo patariamąoji taryba gali patarti Valdybai dėl specialiųjų darbo grupių, susijusių su Kompetencijos centro veikla, sudarymo, ir prireikus, tokių darbo grupių veiklą koordinuoja vienas ar kelis Pramonės ir mokslo patariamąsios tarybos nariai.
3. Pramonės ir mokslo patariamąoji taryba renka savo pirmininką.
4. Pramonės ir mokslo patariamąoji taryba tvirtina savo darbo tvarkos taisyklės, kuriose nurodo savo atstovus, paskirtus pagal poreikį atstovauti Patariamąjai tarybai, ir jų kadencijos trukmę.

### **Pramonės ir mokslo patariamąsios tarybos užduotys**

Pramonės ir mokslo patariamąoji taryba konsultuoja Kompetencijos centrą jo veiklos vykdymo klausimais ir:

- (1) teikia vykdomajam direktoriui ir Valdybai strategines konsultacijas bei prisideda rengiant darbo planą ir daugiametį strateginį planą Valdybos nustatytais terminais;
- (2) organizuoja viešas konsultacijas, skirtas visoms viešojo ir privačiojo sektorių suinteresuotosioms šalims, turinčioms interesą kibernetinio saugumo srityje, siekdama surinkti informaciją, reikalingą 1 dalyje nurodytoms strateginėms konsultacijoms vykdyti;
- (3) propaguoja Kompetencijos centro darbo planą ir daugiametį strateginį planą ir renka atsiliepimus apie juos.

## **III SKYRIUS FINANSINĖS NUOSTATOS**

### **Sąjungos finansinis įnašas**

1. Sąjungos įnašas Kompetencijos centro administracinėms ir veiklos išlaidoms padengti yra toks:
  - (a) 1 981 668 000 EUR iš Skaitmeninės Europos programos, įskaitant iki 23 746 000 EUR administracinėms išlaidoms padengti;
  - (b) pagal programą „Europos horizontas“ skiriama suma, įskaitant administracinėms išlaidoms padengti, nustatoma atsižvelgiant į strateginio planavimo procesą, kuris turi būti vykdomas pagal Reglamento Nr. XXX [Programos „Europos horizontas“ reglamentas] 6 straipsnio 6 dalį.
2. Didžiausias Sąjungos įnašas mokamas iš Sąjungos bendrojo biudžeto asignavimų, skirtų [Skaitmeninės Europos programai] ir specialiajai programai, kuria įgyvendinama programa „Europos horizontas“, įsteigta Sprendimu Nr. XXX.
3. Kompetencijos centras turi įgyvendinti [Skaitmeninės Europos programos] ir [programos „Europos horizontas“] kibernetinio saugumo veiksmus pagal Reglamento Nr. XXX (ES, Euratomas) [Finansinis reglamentas]<sup>29</sup> 62 straipsnio c punkto iv papunktį.
4. Sąjungos finansiniu įnašu nefinansuojamos 4 straipsnio 8 dalies b punkte minimos užduotys.

---

<sup>29</sup> [įrašyti visą pavadinimą ir OL nuorodą].

## 22 straipsnis

### Dalyvaujančiųjų valstybių narių įnašai

1. Dalyvaujančiosios valstybės narės bendrai padengia Kompetencijos centro veiklos ir administracines išlaidas bent tokiomis pačiomis sumomis, kaip nurodyta reglamento 21 straipsnio 1 dalyje.
2. Siekiant įvertinti 23 straipsnio 1 dalyje ir 3 dalies b punkto ii papunktyje nurodytus įnašus, išlaidos nustatomos pagal atitinkamų valstybių narių įprastą išlaidų apskaitos praktiką, pagal toje valstybėje narėje, kurioje įsisteigęs subjektas, taikomus apskaitos standartus ir pagal taikomus tarptautinius apskaitos standartus bei tarptautinius finansinės atskaitomybės standartus. Išlaidas patvirtina nepriklausomas išorės auditorius, kurį paskiria atitinkama valstybė narė. Jei kyla neaiškumų dėl išlaidų patvirtinimo, vertinimo metodą gali patikrinti Kompetencijos centras.
3. Jeigu kuri nors dalyvaujančioji valstybė narė nevykdo įsipareigojimų dėl savo finansinio įnašo, vykdomasis direktorius tai pažymi raštu ir nustato pagrįstą laikotarpį, per kurį mokėjimo įsipareigojimai turi būti įvykdyti. Jeigu per nustatytą laikotarpį mokėjimo įsipareigojimai neįvykdomi, vykdomasis direktorius sušaukia Valdybos posėdį, kuriame sprendžiama, ar mokėjimo įsipareigojimų nevykdančios dalyvaujančiosios valstybės narės balsavimo teisė turėtų būti panaikinta, ar reikėtų imtis kokių nors kitų priemonių, kol ji įvykdys įsipareigojimus. Mokėjimo įsipareigojimų nevykdančios valstybės narės balsavimo teisės sustabdomos, kol ji įvykdys savo mokėjimo įsipareigojimus.
4. Komisija gali nutraukti, proporcingai sumažinti arba sustabdyti Sąjungos finansinį įnašą į Kompetencijos centrą, jei dalyvaujančiosios valstybės narės nesumoka, prisideda tik iš dalies arba vėluoja sumokėti 1 dalyje nurodytus įnašus.
5. Dalyvaujančiosios valstybės narės kiekvienais metais iki sausio 31 d. pateikia Valdybai 1 dalyje nurodytų įnašų, sumokėtų kiekvienais ankstesniais finansiniais metais, vertės ataskaitą.

## 23 straipsnis

### Kompetencijos centro išlaidos ir ištekliai

1. Kompetencijos centrą bendrai finansuoja Sąjunga ir valstybės narės, dalimis mokėdamos finansinius įnašus ir įnašus, susidedančius iš nacionalinių koordinavimo centrų ir paramos gavėjų patirtų išlaidų įgyvendinant veiksmus, kurių nekompensuoja Kompetencijos centras.
2. Kompetencijos centro administracinės išlaidos neviršija [skaičius] EUR; jos padengiamos finansiniais įnašais, kurie kasmet lygiai padalijami tarp Sąjungos ir dalyvaujančiųjų valstybių narių. Jei dalis įnašo administracinėms išlaidoms padengti nepanaudojama, ji gali būti panaudota Kompetencijos centro veiklos išlaidoms padengti.
3. Kompetencijos centro veiklos išlaidos padengiamos:
  - (a) Sąjungos finansiniu įnašu;
  - (b) dalyvaujančiųjų valstybių narių įnašais, kaip:
    - i) finansiniais įnašais ir

- ii) jei taikoma, dalyvaujančiųjų valstybių narių įnašais natūra, susidedančiais iš nacionalinių koordinavimo centrų ir paramos gavėjų patirtų išlaidų įgyvendinant netiesioginius veiksmus, atėmus Kompetencijos centro įnašą ir bet koki kitą Sąjungos įnašą šioms išlaidoms padengti.
4. Į Kompetencijos centro biudžetą įtraukiamus išteklius sudaro tokie įnašai:
    - (a) dalyvaujančiųjų valstybių narių finansiniai įnašai administracinėms išlaidoms padengti,
    - (b) dalyvaujančiųjų valstybių narių finansiniai įnašai veiklos išlaidoms padengti,
    - (c) visos Kompetencijos centro gautos pajamos,
    - (d) visi kiti finansiniai įnašai, ištekliai ir pajamos.
  5. Visos palūkanos, gautos iš įnašų, kurias dalyvaujančiosios valstybės narės moka Kompetencijos centrui, laikomos jo pajamomis.
  6. Visi Kompetencijos centro ištekliai ir jo veikla turi būti skirti 4 straipsnyje nustatytiems tikslams pasiekti.
  7. Kompetencijos centras nuosavybės teise valdo visą turtą, kurį jis sukaupe arba kuris jam buvo perduotas jo tikslams pasiekti.
  8. Kai pajamos viršija išlaidas, perviršis dalyvaujantiems Kompetencijos centro nariams neišmokamas, išskyrus Kompetencijos centro likvidavimo atveju.

#### *24 straipsnis*

#### **Finansiniai įsipareigojimai**

Kompetencijos centro finansiniai įsipareigojimai neviršija finansinių išteklių, kuriuos jo biudžetui skyrė ar įsipareigojo skirti jos nariai, sumos.

#### *25 straipsnis*

#### **Finansiniai metai**

Finansiniai metai prasideda sausio 1 d. ir baigiasi gruodžio 31 d.

#### *26 straipsnis*

#### **Biudžeto sudarymas**

1. Kasmet vykdomasis direktorius parengia Kompetencijos centro ateinančių finansinių metų pajamų ir išlaidų sąmatos projektą ir perduoda jį Valdybai kartu su etatų plano projektu. Pajamos ir išlaidos turi būti subalansuotos. Kompetencijos centro išlaidas sudaro personalo, administracinės, infrastruktūros ir veiklos išlaidos. Administracinės išlaidos turi būti minimalios.
2. Valdyba, vadovaudamasi 1 dalyje nurodytu pajamų ir išlaidų sąmatos projektu, kasmet parengia Kompetencijos centro ateinančių finansinių metų pajamų ir išlaidų sąmatą.
3. 2 dalyje nurodytą sąmatą, kuri taip pat įtraukiama į bendrojo programavimo dokumento projektą, Valdyba iki kiekvienų metų sausio 31 d. nusiunčia Komisijai.



4. Pagal tą sąmatą Komisija į Sąjungos biudžeto projektą įtraukia, jos manymu, etatų planui būtinų lėšų sąmatas ir įnašo į bendrąjį biudžetą, kurį ji pagal SESV 313 ir 314 straipsnius pateikia Europos Parlamentui ir Tarybai, sumą.
5. Europos Parlamentas ir Taryba patvirtina Kompetencijos centro skiriamo įnašo asignavimus.
6. Europos Parlamentas ir Taryba tvirtina Kompetencijos centro etatų planą.
7. Valdyba Centro biudžetą priima kartu su darbo planu. Jis tampa galutiniu galutinai priėmus Sąjungos bendrąjį biudžetą. Prireikus Valdyba tikslina Kompetencijos centro biudžetą ir darbo planą pagal Sąjungos bendrąjį biudžetą.

#### *27 straipsnis*

#### **Kompetencijos centro ataskaitų pateikimas ir biudžeto įvykdymo patvirtinimas**

Kompetencijos centro preliminarių ir galutinių ataskaitų pateikimas ir biudžeto įvykdymo patvirtinimas turi atitikti Finansinio reglamento ir jo finansinių taisyklių, priimtų pagal 29 straipsnį, taisykles ir tvarkaraštį.

#### *28 straipsnis*

#### **Veiklos ir finansinių ataskaitų teikimas**

1. Vykdomasis direktorius kasmet teikia Valdybai savo pareigų vykdymo ataskaitą pagal Kompetencijos centro finansines taisykles.
2. Per du mėnesius nuo kiekvienų finansinių metų pabaigos vykdomasis direktorius pateikia Valdybai tvirtinti metinę veiklos ataskaitą apie praėjusiais kalendoriniais metais Kompetencijos centro padarytą pažangą, visų pirma pagal tų metų darbo planą. Toje ataskaitoje, *inter alia*, pateikiama informacija apie:
  - (a) atliktus operatyvinius veiksmus ir atitinkamas išlaidas;
  - (b) pateiktus veiksmus, atskirai nurodant dalyvių rūšis, įskaitant MVI, ir valstybes nares;
  - (c) finansuoti atrinktus veiksmus, atskirai nurodant dalyvių rūšis, įskaitant MVI, ir valstybes nares, taip pat nurodant Kompetencijos centro įnašą atskiriems dalyviams ir veiksmams;
  - (d) pažangą, padarytą siekiant 4 straipsnyje nustatytų tikslų, ir pasiūlymus dėl tolesnio šiems tikslams pasiekti būtino darbo.
3. Valdybos patvirtinta metinė veiklos ataskaita paskelbiama viešai.

#### *29 straipsnis*

#### **Finansinės taisyklės**

Kompetencijos centras savo konkrečias finansines taisykles priima pagal Reglamento Nr. XXX [naujas Finansinis reglamentas] 70 straipsnio nuostatas.

#### *30 straipsnis*

#### **Finansinių interesų apsauga**

1. Kompetencijos centras tinkamomis priemonėmis užtikrina, kad įgyvendinant pagal šį reglamentą finansuojamus veiksmus Sąjungos finansiniai interesai būtų saugomi taikant kovos su sukčiavimu, korupcija ir kita neteisėta veikla priemones, atliekant veiksmingas patikrinimus ir, jei nustatoma pažeidimų, susigražinant nepagrįstai išmokėtas sumas ir prireikus taikant veiksmingas, proporcingas ir atgrasomas administracines sankcijas.
2. Kompetencijos centras suteikia Komisijos darbuotojams bei kitiems Komisijos įgaliotiems asmenims ir Audito Rūmams galimybę patekti į savo objektus ir patalpas ir susipažinti su visa informacija, įskaitant informaciją elektroniniu formatu, kurios jiems reikia auditui atlikti.
3. Europos kovos su sukčiavimu tarnyba (OLAF) gali, laikydamasi Tarybos reglamente (Euratomas, EB) Nr. 2185/96<sup>30</sup> ir Europos Parlamento ir Tarybos reglamente (ES, Euratomas) Nr. 883/2013<sup>31</sup> nustatytų nuostatų ir procedūrų, atlikti tyrimus, įskaitant patikras ir inspektavimus vietoje, siekdama nustatyti, ar vykdant pagal šį reglamentą tiesiogiai arba netiesiogiai finansuojamą dotacijos susitarimą ar sutartį nebūta sukčiavimo, korupcijos ar kitos neteisėtos veiklos atvejų, darančių poveikį Sąjungos finansiniams interesams.
4. Nedarant poveikio šio straipsnio 1, 2 ir 3 dalių taikymui, į sutartis ir dotacijų susitarimus sudaromus įgyvendinant šį reglamentą, įtraukiamos nuostatos, kuriomis Komisijai, Kompetencijos centrui, Audito Rūmams ir OLAF aiškiai suteikiami įgaliojimai atlikti tokius auditus ir tyrimus pagal jų atitinkamą kompetenciją. Tais atvejais, kai visą veiksmą ar jo dalį pavesta įgyvendinti išorės paslaugų teikėjui arba perįgaliotam subjektui arba kai norint įgyvendinti veiksmą reikia sudaryti viešojo pirkimo sutartį su trečiaja šalimi arba trečiajai šaliai skirti finansinę paramą, sutartyje arba dotacijos susitarime nurodoma rangovo arba paramos gavėjo pareiga nustatyti reikalavimą kiekvienai dalyvaujančiai trečiajai šaliai aiškiai sutikti su tais Komisijos, Kompetencijos centro, Audito Rūmų ir OLAF įgaliojimais.

## IV SKYRIUS

### KOMPETENCIJOS CENTRO PERSONALAS

#### *31 straipsnis*

##### **Personalas**

1. Kompetencijos centro personalui taikomi Europos Sąjungos pareigūnų tarnybos nuostatai ir Kitų tarnautojų įdarbinimo sąlygos, išdėstyti Tarybos reglamente (EEB, Euratomas, EAPB) Nr. 259/68<sup>32</sup> (toliau – Tarnybos nuostatai ir Įdarbinimo sąlygos),

---

<sup>30</sup> 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).

<sup>31</sup> 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).

<sup>32</sup> 1968 m. vasario 29 d. Tarybos reglamentas (EEB, Euratomas, EAPB) Nr. 259/68, nustatantis Europos Bendrijų pareigūnų tarnybos nuostatus ir kitų Europos Bendrijų tarnautojų įdarbinimo sąlygas bei Komisijos pareigūnams laikinai taikomas specialias priemones (OL L 56, 1968 3 4, p. 1).

ir Sąjungos institucijų bendrai priimtos Tarnybos nuostatų ir Įdarbinimo sąlygų taikymo taisyklės.

2. Kompetencijos centro personalo atžvilgiu Valdyba naudojasi įgaliojimais, kurie Tarnybos nuostatuose suteikti paskyrimų tarnybai, o Įdarbinimo sąlygose – institucijai, įgaliotai sudaryti sutartis (toliau – paskyrimų tarnybos įgaliojimai).
3. Pagal Tarnybos nuostatų 110 straipsnį Valdyba priima sprendimą, pagrįstą Tarnybos nuostatų 2 straipsnio 1 dalimi ir Įdarbinimo sąlygų 6 straipsniu, kuriuo atitinkami paskyrimų tarnybos įgaliojimai suteikiami vykdomajam direktoriui ir nustatomos sąlygos, kuriomis tie įgaliojimai gali būti sustabdyti. Vykdomajam direktoriui leidžiama tuos įgaliojimus perduoti kitiems asmenims.
4. Išimtinėmis aplinkybėmis Valdyba gali sprendimu laikinai sustabdyti vykdomajam direktoriui suteiktus paskyrimų tarnybos įgaliojimus ir direktoriaus perduotus įgaliojimus. Tokiu atveju Valdyba pati naudojasi paskyrimų tarnybos įgaliojimais arba juos suteikia vienam iš savo narių arba Kompetencijos centro darbuotojui, kuris nėra vykdomasis direktorius.
5. Pagal Tarnybos nuostatų 110 straipsnį Valdyba priima Tarnybos nuostatų ir Įdarbinimo sąlygų įgyvendinimo taisykles.
6. Personalo išteklių nustatomi Kompetencijos centro personalo etatų plane, kuriame laikantis jos metinio biudžeto nurodomas laikinų etatų skaičius pagal pareigų grupę bei lygį ir sutartininkų skaičius, išreikštas visos darbo dienos ekvivalentais.
7. Kompetencijos centro personalą sudaro laikinieji darbuotojai ir sutartininkai.
8. Visas su personalu susijusias išlaidas padengia Kompetencijos centras.

### *32 straipsnis*

#### **Deleguotieji nacionaliniai ekspertai ir kiti darbuotojai**

1. Kompetencijos centras gali naudotis deleguotųjų nacionalinių ekspertų ar kitų darbuotojų, neįdarbintų Kompetencijos centre, paslaugomis.
2. Komisijai pritarus, Valdyba priima sprendimą, kuriuo nustato nacionalinių ekspertų delegavimo į Kompetencijos centrą taisykles.

### *33 straipsnis*

#### **Privilegijos ir imunitetai**

Kompetencijos centrui ir jo personalui taikomas Protokolas Nr. 7 dėl Europos Sąjungos privilegijų ir imunitetų, pridėtas prie Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo.

## **V SKYRIUS**

### **BENDROSIOS NUOSTATOS**

### *34 straipsnis*

#### **Saugumo taisyklės**

1. Reglamente (ES) Nr. XXX [Skaitmeninės Europos programa] 12 straipsnio 7 dalis taikoma dalyvaujant visoje Kompetencijos centro finansuojamoje veikloje.

2. Pagal programą „Europos horizontas“ finansuojamai veiklai taikomos šios konkrečios saugumo taisyklės:
- (a) Reglamento (ES) Nr. XXX [Programa „Europos horizontas“] 34 straipsnio 1 dalies [Nuosavybė ir apsauga] tikslais, kai numatyta darbo plane, neišimtinių licencijų išdavimas gali būti taikomas tik trečiosioms šalims, kurios įsteigtos arba laikomos įsteigtomis valstybėse narėse ir kurias kontroliuoja valstybės narės ir (arba) valstybių narių piliečiai;
  - (b) Reglamento (ES) Nr. XXX [Programa „Europos horizontas“] 36 straipsnio 4 dalies b punkto [Perdavimas ir licencijavimas] tikslais perdavimas arba licencija juridiniam asmeniui, įsteigtam asocijuotoje šalyje arba įsteigtam Sąjungoje, tačiau kontroliuojamam iš trečiųjų šalių, taip pat yra pagrindas prieštarauti rezultatų nuosavybės perdavimui arba rezultatų išimtinės licencijos suteikimui;
  - (c) Reglamento (ES) Nr. XXX [Programa „Europos horizontas“] 37 straipsnio 3 dalies a punkto [Prieigos teisės] tikslais, kai numatyta darbo plane, prieiga prie rezultatų ir informacijos gali būti suteikiama tik juridiniam asmeniui, kuris įsteigtas arba laikomas įsteigtu valstybėse narėse ir kurį kontroliuoja valstybės narės ir (arba) valstybių narių piliečiai.

### *35 straipsnis*

#### **Skaidrumas**

1. Kompetencijos centras vykdo savo veiklą labai skaidriai.
2. Kompetencijos centras užtikrina, kad visuomenė ir suinteresuotosios šalys gautų tinkamą, objektyvią, patikimą ir lengvai prieinamą informaciją, ypač kai ji susijusi su Kompetencijos centro veiklos rezultatais. Jis taip pat viešai skelbia pagal 41 straipsnį pateiktas interesų deklaracijas.
3. Valdyba, vadovaudamasi vykdomojo direktoriaus siūlymu, gali leisti suinteresuotoms šalims stebėti, kaip vykdoma tam tikra Kompetencijos centro veikla.
4. Kompetencijos centras savo darbo tvarkos taisyklėse nustato praktines priemones 1 ir 2 dalyse nurodytoms skaidrumo taisyklėms įgyvendinti. Pagal programą „Europos horizontas“ finansuojamos veiklos atveju bus tinkamai atsižvelgiama į Programos „Europos horizontas“ reglamento III priedo nuostatas.

### *36 straipsnis*

#### **Saugumo taisyklės dėl įslaptintos informacijos ir neskelbtinos neįslaptintos informacijos apsaugos**

1. Nedarant poveikio 35 straipsniui, Kompetencijos centras neatskleidžia trečiosioms šalims informacijos, kurią jis tvarko arba gauna ir kurią pateiktame pagrįstame prašyme prašoma laikyti visiškai ar iš dalies konfidencialia.
2. Valdybos nariams, vykdomajam direktoriui, Pramonės ir mokslo patariamiosios tarybos nariams, *ad hoc* darbo grupėse dalyvaujantiems išorės ekspertams ir Centro personalui taikomi konfidencialumo reikalavimai pagal Sutarties dėl Europos Sąjungos veikimo 339 straipsnį, net jiems nustojus eiti savo pareigas.
3. Komisijai patvirtinus, Kompetencijos centro valdyba priima Kompetencijos centro saugumo taisykles, pagrįstas principais ir taisyklėmis, išdėstytais Komisijos saugumo

taisyklėse, skirtose Europos Sąjungos įslaptintos informacijos ir neskelbtinos neįslaptintos informacijos apsaugai užtikrinti, įskaitant, *inter alia*, tokios informacijos tvarkymo ir saugojimo nuostatas, kaip nustatyta Komisijos sprendimuose (ES, Euratomas) Nr. 2015/443<sup>33</sup> ir 2015/444<sup>34</sup>.

4. Kompetencijos centras gali imtis visų būtinų priemonių, kad palengvintų keitimąsi jo užduotims vykdyti svarbia informacija su Komisija ir valstybėmis narėmis, o tinkamais atvejais – su susijusiomis Sąjungos agentūromis ir įstaigomis. Visiems šiuo tikslu sudarytiems administraciniais susitarimams dėl dalijimosi Europos Sąjungos įslaptinta informacija arba, jei tokio susitarimo nėra, bet kuriuo išimtinu *ad hoc* pasidalijimo Europos Sąjungos įslaptinta informacija atveju reikalingas Komisijos išankstinis leidimas.

### 37 straipsnis

#### Galimybė susipažinti su dokumentais

1. Reglamentas (EB) Nr. 1049/2001 taikomas Kompetencijos centro turimiems dokumentams.
2. Valdyba per šešis mėnesius nuo Kompetencijos centro įsteigimo patvirtina Reglamento (EB) Nr. 1049/2001 įgyvendinimo priemones.
3. Sprendimai, kuriuos priima Kompetencijos centras pagal Reglamento (EB) Nr. 1049/2001 8 straipsnį, gali tapti skundo ombudsmenui pagal Sutarties dėl Europos Sąjungos veikimo 228 straipsnį ar Europos Sąjungos Teisingumo Teisme pareikšto ieškinio dalyku pagal Sutarties dėl Europos Sąjungos veikimo 263 straipsnį.

### 38 straipsnis

#### Stebėseną, vertinimas ir peržiūra

1. Kompetencijos centras užtikrina, kad jo veikla, įskaitant per nacionalinius koordinavimo centrus ir Tinklą valdomą veiklą, būtų nuolat ir sistemingai stebima ir periodiškai vertinama. Kompetencijos centras užtikrina, kad programos įgyvendinimo ir rezultatų stebėsenos duomenys būtų renkami veiksmingai, efektyviai ir laiku, o Sąjungos lėšų gavėjams ir valstybėms narėms būtų nustatyti proporcingi ataskaitų teikimo reikalavimai. Vertinimų rezultatai skelbiami viešai.
2. Kai yra pakankamai informacijos apie šio reglamento įgyvendinimą, bet ne vėliau kaip po trijų su puse metų nuo šio reglamento įgyvendinimo pradžios, Komisija atlieka tarpinį Kompetencijos centro veiklos vertinimą. Komisija parengia šio vertinimo ataskaitą ir iki 2024 m. gruodžio 31 d. pateikia ją Europos Parlamentui ir Tarybai. Kompetencijos centras ir valstybės narės pateikia Komisijai informaciją, kurios reikia šiai ataskaitai parengti.
3. 2 dalyje nurodytas vertinimas apima Kompetencijos centro pasiektų rezultatų įvertinimą, atsižvelgiant į jo tikslus, įgaliojimus ir užduotis. Jei Komisija mano, kad, atsižvelgiant į Kompetencijos centro tikslus, įgaliojimus ir užduotis, tolesnis

<sup>33</sup> 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/443 dėl saugumo Komisijoje (OL L 72, 2015 3 17, p. 41).

<sup>34</sup> 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).

Kompetencijos centro darbas pagrįstas, ji gali siūlyti pratęsti 46 straipsnyje nustatytą agentūros įgaliojimų trukmę.

4. Remdamasi 2 dalyje nurodyto tarpinio įvertinimo išvadomis Komisija gali imtis priemonių pagal 22 [straipsnio 5 dalį] arba kitų atitinkamų veiksmų.
5. Pagal programą „Europos horizontas“ finansuojamo įnašo stebėseną, vertinimas, laipsniškas jų atsisakymas ir atnaujinimas atitinka Programos „Europos horizontas“ reglamento 8, 45 ir 47 straipsnius bei Programos „Europos horizontas“ reglamento III priedą ir suderintą įgyvendinimo tvarką.
6. Pagal Skaitmeninės Europos programą finansuojamo įnašo stebėseną, ataskaitų teikimas ir vertinimas atitinka Skaitmeninės Europos programos 24, 25 straipsnių nuostatas.
7. Kompetencijos centro likvidavimo atveju Komisija atlieka galutinį Kompetencijos centro vertinimą per šešis mėnesius nuo Kompetencijos centro likvidavimo, bet ne vėliau kaip po dvejų metų nuo likvidavimo procedūros pradžios, kaip nurodyta šio reglamento 46 straipsnyje. To galutinio vertinimo rezultatai pateikiami Europos Parlamentui ir Tarybai.

### *39 straipsnis*

#### **Kompetencijos centro atsakomybė**

1. Kompetencijos centro sutartinė atsakomybė reglamentuojama aptariamam susitarimui, sprendimui ar sutarčiai taikytina teise.
2. Nesutartinės atsakomybės atveju, Kompetencijos centras, vadovaudamasis bendraisiais valstybių narių teisei būdingais principais, turi atlyginti bet kokią žalą, kurią jo personalo nariai padaro vykdydami savo pareigas.
3. Visi Kompetencijos centro mokėjimai, susiję su šio straipsnio 1 ir 2 dalyse nurodyta atsakomybe, taip pat su ja susijusios sąnaudos ir išlaidos laikomos Kompetencijos centro išlaidomis ir padengiamos iš jo lėšų.
4. Už savo pareigų vykdymą atsakingas tik pats Kompetencijos centras.

### *40 straipsnis*

#### **Europos Sąjungos Teisingumo Teismo jurisdikcija ir taikytina teisė**

1. Europos Sąjungos Teisingumo Teismas turi jurisdikciją:
  - (1) pagal bet kurią arbitražinę išlygą, įtrauktą į Kompetencijos centro sudarytus susitarimus, priimtus sprendimus ar sudarytas sutartis;
  - (2) spręsti ginčus, susijusius su žalos, kurią padarė Kompetencijos centro personalas, vykdydamas savo pareigas, atlyginimu;
  - (3) Kompetencijos centro ir jo tarnautojų ginčų atžvilgiu srityje, kuri reglamentuojama Tarnybos nuostatais.
2. Šiame reglamente ar kituose Sąjungos teisės aktuose nenumatytiems atvejams taikoma valstybės, kurioje yra Kompetencijos centro buveinė, teisė.

#### *41 straipsnis*

### **Narių atsakomybė ir draudimas**

1. Narių finansinė atsakomybė už Kompetencijos centro skolas neviršija jų jau sumokėto įnašo administracinėms išlaidoms padengti.
2. Kompetencijos centras apsidraudžia tinkamu draudimu ir užtikrina, kad draudimo apsauga nuolat galiotų.

#### *42 straipsnis*

### **Interesų konfliktai**

Kompetencijos centro valdyba priima savo nariams, organams ir personalui taikomas interesų konfliktų prevencijos ir valdymo taisykles. Šiose taisyklėse numatomos nuostatos, kuriomis siekiama išvengti Valdyboje, taip pat Pramonės ir mokslo patariamojoje taryboje dirbančių narių atstovų interesų konflikto pagal Reglamento Nr. XXX [naujas Finansinis reglamentas] nuostatas.

#### *43 straipsnis*

### **Asmens duomenų apsauga**

1. Kompetencijos centro vykdomam asmens duomenų tvarkymui taikomas Europos Parlamento ir Tarybos reglamentas (ES) Nr. XXX/2018.
2. Valdyba priima Reglamento (ES) Nr. XXX/2018 XX straipsnio 3 dalyje nurodytas įgyvendinimo priemones. Valdyba gali priimti papildomas priemones, kurių reikia, kad Kompetencijos centras taikytų Reglamentą (ES) Nr. XXX/2018.

#### *44 straipsnis*

### **Priimančiosios valstybės narės parama**

Kompetencijos centras ir valstybė narė, kurioje yra jos buveinė [Belgija], gali sudaryti administracinį susitarimą dėl privilegijų, imunitetų ir kitos paramos, kurią ta valstybė narė turi teikti Kompetencijos centrui.

## **VII SKYRIUS**

### **BAIGIAMOSIOS NUOSTATOS**

#### *45 straipsnis*

### **Pradiniai veiksmai**

1. Komisija atsako už Kompetencijos centro įsteigimą ir pradinę veiklą, kol Kompetencijos centras turės veiklos pajėgumų savo biudžetui vykdyti. Komisija, vadovaudamasi Sąjungos teise, vykdo visus reikalingus veiksmus, dalyvaujant Kompetencijos centro kompetentingiems organams.

2. Įgyvendinant 1 dalį, kol pagal 16 straipsnį Valdybos paskirtas vykdomasis direktorius ims eiti savo pareigas, Komisija gali paskirti laikinąjį vykdomąjį direktorių, kuris vykdytų vykdomajam direktoriui pavestas pareigas ir kuriam galėtų padėti tam tikras skaičius Komisijos pareigūnų, Komisija gali laikinai paskirti tam tikrą skaičių savo pareigūnų.
3. Laikinasis vykdomasis direktorius, Valdybai patvirtinus, gali leisti atlikti visus iš Kompetencijos centro metiniame biudžete numatytų asignavimų padengiamus mokėjimus, sudaryti susitarimus, priimti sprendimus ir sudaryti sutartis, įskaitant darbo sutartis, kai bus patvirtintas Kompetencijos centro personalo etatų planas.
4. Laikinasis vykdomasis direktorius bendru sutarimu su Kompetencijos centro vykdomuoju direktoriumi, gavę Valdybos pritarimą, nustato datą, nuo kurios Kompetencijos centras yra pajėgus vykdyti savo biudžetą. Nuo tos datos Komisija nebeprisiima su Kompetencijos centru veikla susijusių įsipareigojimų ir nebevykdo su ja susijusių mokėjimų.

#### *46 straipsnis*

#### **Taikymo trukmė**

1. Kompetencijos centras įsteigiamas laikotarpiui nuo 2021 m. sausio 1 d. iki 2029 m. gruodžio 31 d.
2. Pasibaigus šiam laikotarpiui, turi būti pradėta likvidavimo procedūra, nebent persvarsčius šį reglamentą būtų nuspręsta kitaip. Likvidavimo procedūra automatiškai pradama, jei Sąjunga arba visos dalyvaujančiosios valstybės narės pasitraukia iš Kompetencijos centro.
3. Kompetencijos centro likvidavimo procedūrai atlikti Valdyba paskiria vieną ar daugiau likvidatorių; jie laikosi Valdybos sprendimų.
4. Likviduojant Kompetencijos centrą, jo turtas naudojamas jo įsipareigojimams įvykdyti ir su jo likvidavimu susijusioms išlaidoms padengti. Bet koks perviršis paskirstomas Sąjungai ir dalyvaujančiosioms valstybėms narėms proporcingai jų finansiniam įnašui į Kompetencijos centrą. Sąjungai paskirtas perteklius grąžinamas į Sąjungos biudžetą.

#### *47 straipsnis*

#### **Įsigaliojimas**

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

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje

*Europos Parlamento vardu*  
*Pirmininkas*

*Tarybos vardu*  
*Pirmininkas*



## **FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA**

### **1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA**

- 1.1. Pasiūlymo (iniciatyvos) pavadinimas
- 1.2. Atitinkama (-os) politikos sritis (-ys) VGV / VGB sistemoje
- 1.3. Pasiūlymo (iniciatyvos) pobūdis
- 1.4. Tikslas (-ai)
- 1.5. Pasiūlymo (iniciatyvos) pagrindas
- 1.6. Trukmė ir finansinis poveikis
- 1.7. Numatytas (-i) valdymo būdas (-ai)

### **2. VALDYMO PRIEMONĖS**

- 2.1. Stebėsenos ir atskaitomybės taisyklės
- 2.2. Valdymo ir kontrolės sistema
- 2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

### **3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS**

- 3.1. Atitinkama (-os) daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės)
- 3.2. Numatomas poveikis išlaidoms
  - 3.2.1. *Numatomo poveikio išlaidoms santrauka*
  - 3.2.2. *Numatomas poveikis veiklos asignavimams*
  - 3.2.3. *Numatomas poveikis administracinio pobūdžio asignavimams*
  - 3.2.4. *Suderinamumas su dabartine daugiamete finansine programa*
  - 3.2.5. *Trečiųjų šalių įnašai*
- 3.3. Numatomas poveikis pajamoms

## FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

### 1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

#### 1.1. Pasiūlymo (iniciatyvos) pavadinimas

Reglamentas dėl Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro įsteigimo

#### 1.2. Atitinkama (-os) politikos sritis (-ys) VGV / VGB sistemoje<sup>35</sup>

Moksliniai tyrimai ir inovacijos

Europos strateginės investicijos

#### 1.3. Pasiūlymo (iniciatyvos) pobūdis

Pasiūlymas (iniciatyva) susijęs (-usi) su  **nauja priemone**

Pasiūlymas (iniciatyva) susijęs (-usi) su  **nauja priemone, kuri bus priimta įgyvendinus bandomąjį projektą ir (arba) atlikus parengiamuosius veiksmus<sup>36</sup>**

Pasiūlymas (iniciatyva) susijęs (-usi)  **su esamos priemonės galiojimo pratęsimu.**

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

#### 1.4. Tikslas (-ai)

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

1 Sujungta bendroji skaitmeninė rinka

2 Naujas darbo vietų kūrimo, ekonomikos augimo ir investicijų postūmis

##### 1.4.2. Susijęs (-ę) konkretus (-ūs) tikslas (-ai)

###### Konkretūs tikslai

1.3. Įgyvendinant iniciatyvas, kuriomis galima visiškai išnaudoti skaitmenines ir duomenų technologijas, galima maksimali skaitmeninės ekonomikos plėtra.

2.1. Europa išlaiko pasaulio skaitmeninės ekonomikos lyderės poziciją: Europos bendrovės gali vystyti veiklą visame pasaulyje ir remdamosi stipriu skaitmeniniu verslu, ir pradėjusios verslą, o teikiant pramonės ir viešąsias paslaugas atsižvelgiama į skaitmeninę transformaciją.

2.2 Europos mokslinių tyrimų organizacijos pritraukia investavimo galimybes potencialiems technologijų laimėjimams ir siektiniams pavyzdžiams sukurti, ypač įgyvendinant programą „Horizontas 2020“ / „Europos horizontas“ bei panaudojant viešojo ir privačiojo sektorių partnerystes.

<sup>35</sup> VGV – veikla grindžiamas valdymas, VGB – veikla grindžiamas biudžeto sudarymas.

<sup>36</sup> Kaip nurodyta Finansinio reglamento 54 straipsnio 2 dalies a arba b punkte.

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

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

Kartu su Tinklu ir Bendruomene Kompetencijos centras sieks šių tikslų:

- (1) prisidėti prie Skaitmeninės Europos programos, įsteigtos Reglamentu Nr. XXX, kibernetinio saugumo dalies įgyvendinimo, visų pirma veiksmų, numatytų Reglamento (ES) Nr. XXX [Skaitmeninės Europos programa] 6 straipsnyje, ir prie programos „Europos horizontas“, įsteigtos Reglamentu Nr. XXX, kibernetinio saugumo dalies įgyvendinimo, visų pirma Sprendimo Nr. XXX dėl specialiosios programos, kuria įgyvendinama bendroji mokslinių tyrimų ir inovacijų programa „Europos horizontas“ I priedo 2.2.6 punkto, bei prie kitų Sąjungos programų įgyvendinimo, jei tai numatyta Sąjungos teisės aktuose,
- (2) stiprinti kibernetinio saugumo pajėgumus, žinias ir infrastruktūrą, kuriais naudojasi pramonės įmonės, viešasis sektorius ir mokslinių tyrimų bendruomenės,
- (3) prisidėti prie plataus masto naujausių kibernetinio saugumo produktų ir sprendimų įdiegimo visoje ekonomikoje,
- (4) pagerinti supratimą apie kibernetinį saugumą supratimą ir prisidėti prie kibernetinio saugumo įgūdžių trūkumo mažinimo Sąjungoje,
- (5) prisidėti prie kibernetinio saugumo mokslinių tyrimų ir technologinės plėtros Europos Sąjungoje stiprinimo,
- (6) skatinti civilinio ir gynybos sektorių bendradarbiavimą dvejopo panaudojimo technologijų ir taikomųjų programų srityje,
- (7) didinti kibernetinio saugumo civilinių ir gynybos aspektų sinergiją,
- (8) palengvinti ir padėti koordinuoti 10 straipsnyje nurodytų Nacionalinių koordinavimo centrų tinklo (toliau – Tinklo) ir 12 straipsnyje nurodytos kibernetinio saugumo kompetencijos bendruomenės veiklą.

### 1.4.4. *Rezultatų ir poveikio rodikliai*

*Nurodyti pasiūlymo (iniciatyvos) įgyvendinimo stebėjimo rodiklius.*

- Bendrai įsigytų kibernetinės infrastruktūros objektų / priemonių skaičius
- Europos mokslininkams ir įmonėms suteikta galimybė naudotis bandymams ir eksperimentams skirtu laiku visame Tinkle bei Centre. Kai tokios sąlygos jau yra, šioms bendruomenėms suteiktų valandų skaičiaus padidėjimas, palyginti su šiuo metu turimomis valandomis.
- Padaugėjo aptarnaujamų naudotojų bendruomenių ir mokslininkų, kurie gauna galimybę naudotis Europos kibernetinio saugumo paslaugomis, palyginti su tais, kuriems tenka ieškoti tokių išteklių už Europos ribų.
- Europos tiekėjų konkurencingumas pradeda didėti, vertinant pagal pasaulinę rinkos dalį (numatyta 25 % rinkos dalis iki 2027 m.) ir pagal pramonės įdiegtų Europos ir MTTP rezultatų dalį.
- Įnašas į kitas kibernetinio saugumo technologijas, išmatuotas pagal autorių teises, patentus, mokslinius ledinius ir komercinius produktus.
- Įvertintų ir suderintų kibernetinio saugumo įgūdžių mokymo programų skaičius, įvertintų kibernetinio saugumo profesinio sertifikavimo programų skaičius.

· Apmokytų mokslininkų, studentų, naudotojų (įmonių ir viešojo administravimo institucijų) skaičius.

## **1.5. Pasiūlymo (iniciatyvos) pagrindas**

### *1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai*

Pasiekti kritinę investicijų į kibernetinio saugumo technologijų ir pramonės plėtrą masę ir išspręsti pajėgumų išsibarstymo po visą ES problemą.

### *1.5.2. Papildoma ES dalyvavimo nauda*

Kaip nurodyta pirmiau minėtose Tarybos išvadose, kibernetinis saugumas yra Sąjungos bendros svarbos klausimas. Tokių incidentų kaip „WannaCry“ ar „NonPetya“ mastas ir tarpvalstybinis pobūdis yra geriausias pavyzdys. Atsižvelgdama į kibernetinio saugumo technologinių uždavinių pobūdį ir mastą bei nepakankamą pastangų koordinavimą pramonės sektoriuose, viešajame sektoriuje ir mokslinių tyrimų bendruomenėse ir tarp jų, ES turi toliau remti koordinavimo pastangas, kad būtų sutelkta kritinė išteklių masė ir užtikrintas geresnis žinių ir turto valdymas. Šie veiksmai reikalingi atsižvelgiant į išteklių poreikius, susijusius su tam tikrais kibernetinio saugumo mokslinių tyrimų, technologinės plėtros ir diegimo pajėgumais; poreikį suteikti galimybę naudotis tarpdisciplinine kibernetinio saugumo praktine patirtimi skirtingose disciplinose (kuri dažnai tik iš dalies prieinama nacionaliniu lygmeniu); pasaulinį pramonės vertės grandinės pobūdį, taip pat visose rinkose veikiančių pasaulinių konkurentų veiklą.

Tam reikia tokio masto išteklių ir praktinės patirties, kuriuos vargu ar galima pasiekti bet kurios valstybės narės pavieniais veiksmais. Pavyzdžiui, visos Europos kvantinės komunikacijos tinklui gali prireikti apie 900 mln. EUR ES investicijų, priklausomai nuo valstybių narių investicijų (kurios bus tarpusavyje susijusios / papildyti viena kita) ir to, kiek technologija leis pakartotinai panaudoti esamas infrastruktūras.

### *1.5.3. Panašios patirties išvados*

Tarpiniame programos „Horizontas 2020“ įvertinime buvo patvirtinta nuolatinė ES teikiamos paramos MTTP bei visuomenės uždaviniams spręsti (tarp jų – programa „Saugios visuomenės“, kuria remiami kibernetinio saugumo MTTP) svarba. Kartu vertinimu patvirtinta, kad pramonės lyderystės stiprinimas išlieka svarbus uždavinys ir kad vis dar atsiranda naujovių spragų, o ES atsilieka proveržio, rinkai reikšmingų inovacijų srityje.

Atrodo, kad Europos infrastruktūros tinklų priemonės (CEF) laikotarpio vidurio vertinimas patvirtina ES intervencijos pridėtinę vertę už MTTP ribų, nors CEF priemonės prasme kibernetinio saugumo dėmesio centras (jis buvo nukreiptas į operacinį saugumą) ir intervencijos logika šiek tiek skyrėsi. Kartu dauguma kibernetinio saugumo dotacijų pagal CEF priemonę gavėjų – nacionalinių reagavimo į kompiuterių saugumo incidentus tarnybų – išreiškė pageidavimą kitoje daugiametėje finansinėje programoje numatyti specialią paramos programą.

2016 m. ES įsteigta viešojo ir privačiojo sektorių partnerystė kibernetinio saugumo srityje buvo svarbus pirmasis žingsnis, vienijantis mokslinių tyrimų, pramonės ir viešojo sektoriaus bendruomenių pastangas siekiant palengvinti kibernetinio saugumo mokslinius tyrimus ir inovacijas, o pagal 2014–2020 m. finansinę programą juo turėtų būti prisidėta prie geresnių ir tikslingesnių mokslinių tyrimų ir inovacijų rezultatų. Įsteigus viešojo ir privačiojo sektorių partnerystę, pramonės partneriai

galėjo prisiimti įsipareigojimus dėl individualių išlaidų srityse, apibrėžtose partnerystės strateginėje mokslinių tyrimų ir inovacijų darbotvarkėje.

1.5.4. *Suderinamumas ir galima sąveika su kitomis atitinkamomis priemonėmis*

Kibernetinio saugumo kompetencijos centrų tinklas ir Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras užtikrins papildomą paramą esamoms kibernetinio saugumo politikos nuostatomis ir joje dalyvaujantiems subjektams. Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro įgaliojimai papildys ENISA pastangas, tačiau jų paskirtis kita ir reikalingi kitokie įgūdžiai. Nors ENISA įgaliojimuose numatytas konsultavimo vaidmuo ES kibernetinio saugumo mokslinių tyrimų ir inovacijų srityje, siūlomi Centro įgaliojimai daugiausia nukreipti į kitus uždavinius, kurie yra svarbūs stiprinant kibernetinio saugumo atsparumą ES. Šis Centras turėtų skatinti kurti ir diegti kibernetinio saugumo technologijas ir turėtų prisidėti prie pastangų stiprinti šios srities pajėgumus ES ir nacionaliniu lygmenimis.

Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Kibernetinio saugumo kompetencijos centrų tinklas taip pat rems mokslinius tyrimus, siekdami palengvinti ir pagreitinti standartizacijos ir sertifikavimo procesus, ypač susijusius su Kibernetinio saugumo akte apibrėžtomis kibernetinio saugumo sertifikavimo sistemomis.

Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras veiks kaip pagrindinis dviejų Europos programų, remiančių kibernetinį saugumą (Skaitmeninės Europos programa ir programa „Europos horizontas“), įgyvendinimo mechanizmas ir stiprins jų suderinamumą bei sinergiją.

Šia iniciatyva bus sudarytos sąlygos papildyti valstybių narių pastangas ir tinkamai padėti švietimo politikos formuotojams, kad jie galėtų pagerinti su kibernetiniu saugumu susijusį švietimą (pvz., sukurti civilinėms ir karinėms švietimo sistemoms skirtas kibernetinio saugumo mokymo programas ir pagrindinio ugdymo kibernetinio saugumo klausimais sistema). Ji taip pat leistų remti profesionalių kibernetinio saugumo sertifikavimo programų suderinimą ir tolesnį vertinimą – visą būtiną veiklą, padedančią išspręsti kibernetinio saugumo įgūdžių trūkumo problemą ir palengvinti pramonės įmonių ir kitų bendruomenių galimybę naudotis kibernetinio saugumo specialistų žiniomis. Suderinus švietimą ir įgūdžius bus galima sukurti kvalifikuotų ES kibernetinio saugumo specialistų bazę – pagrindinę priemonę, skirtą kibernetinio saugumo įmonėms ir kitoms pramonės įmonėms, turinčioms interesų kibernetinio saugumo srityje.

## 1.6. Trukmė ir finansinis poveikis

### Pasiūlymo (iniciatyvos) **trukmė ribota**

- Pasiūlymas (iniciatyva) galioja nuo 2021 01 01 iki 2029 12 31
- įsipareigojimų asignavimų finansinis poveikis nuo 2021 iki 2027 m., o mokėjimų asignavimų – nuo 2021 iki 2031 m.

### Pasiūlymo (iniciatyvos) **trukmė neribota**

- Įgyvendinimo pradinis laikotarpis – nuo MMMM iki MMMM,
- vėliau – visuotinis taikymas.

## 1.7. Numatytas (-i) valdymo būdas (-ai)<sup>37</sup>

### **Tiesioginis valdymas**, vykdomas Komisijos,

- padalinių, įskaitant Sąjungos delegacijų darbuotojus;
- vykdomųjų įstaigų

### **Pasidalijamasis valdymas** kartu su valstybėmis narėmis

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

- trečiosioms šalims arba jų paskirtoms įstaigoms;
- tarptautinėms organizacijoms ir jų agentūroms (nurodyti);
- EIB ir Europos investicijų fondui;
- įstaigoms, nurodytoms Finansinio reglamento 70 ir 71 straipsnyje;
- viešosios teisės įstaigoms;
- įstaigoms, kurių veiklą reglamentuoja privatinė teisė, veikiančioms viešųjų paslaugų srityje, jeigu jos pateikia pakankamų finansinių garantijų;
- įstaigoms, kurių veiklą reglamentuoja valstybės narės privatinė teisė, kurioms pavesta įgyvendinti viešojo ir privačiojo sektorių partnerystę ir kurios pateikia pakankamų finansinių garantijų;
- asmenims, kuriems pavestas konkrečių BUSP veiksmų vykdymas pagal ES sutarties V antraštinę dalį ir kurie nurodyti atitinkamame pagrindiniame teisės akte
- *Jei nurodomas daugiau kaip vienas valdymo būdas, išsamią informaciją pateikti šio punkto pastabų skiltyje.*

<sup>37</sup>

Informacija apie valdymo būdus ir nuorodos į Finansinį reglamentą pateikiamos svetainėje „BudgWeb“ adresu [http://www.cc.cec/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html).

## 2. VALDYMO PRIEMONĖS

### 2.1. Stebėsenos ir atskaitomybės taisyklės

*Nurodyti dažnumą ir sąlygas.*

28 straipsnyje numatytos išsamios stebėsenos ir atskaitomybės nuostatos.

### 2.2. Valdymo ir kontrolės sistema

#### 2.2.1. Nustatyta rizika

Siekdama sušvelninti riziką, susijusią su Kompetencijos centro veikimu po jo įsteigimo ir vėlavimais, Komisija šiame etape parems Kompetencijos centrą, siekdama užtikrinti greitą pagrindinio personalo įdarbinimą ir veiksmingos vidaus kontrolės sistemos bei patikimų procedūrų sukūrimą.

#### 2.2.2. Informacija apie įdiegtą vidaus kontrolės sistemą

Vykdomasis direktorius atsako už kasdienį Kompetencijos centro valdymą bei jo operacijas ir yra jo teisėtas atstovas. Jis atskaitingas Valdybai ir nuolat jai teikia ataskaitas apie Kompetencijos centro veiklos vykdymą.

Valdyba bendrai atsako už Kompetencijos centro strateginę kryptį bei operacijas ir prižiūri jo veiklos įgyvendinimą.

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

Kompetencijos centro atžvilgiu Komisijos vidaus auditorius turi vykdyti tuos pačius įgaliojimus, kaip ir Komisijos atžvilgiu. Audito Rūmai turi įgaliojimus atlikti visų dotacijų gavėjų, rangovų ir subrangovų, kurie iš Kompetencijos centro yra gavę Sąjungos lėšų, auditą remdamiesi dokumentais ir auditą vietoje.

#### 2.2.3. Kontrolės sąnaudų ir naudos apskaičiavimas ir numatomo klaidų rizikos lygio vertinimas

##### **Kontrolės sąnaudos ir nauda**

Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro kontrolės sąnaudos padalijamos iš priežiūros lygio Komisijos lygmeniu ir operacinės kontrolės sąnaudų įgyvendinančios institucijos lygmeniu.

Apskaičiuotos kontrolės sąnaudos Kompetencijos centro lygmeniu yra maždaug 1,19 % veiklos mokėjimų asignavimų, įgyvendintų Kompetencijos centro lygmeniu.

Numatytos priežiūros išlaidos Komisijos lygmeniu sudaro 1,20 % veiklos mokėjimų asignavimų, kurie bus įgyvendinami Kompetencijos centro lygmeniu.

Remiantis prielaida, kad Komisija visiškai valdys veiklą be įgyvendinančios institucijos paramos, kontrolės sąnaudos būtų daug didesnės ir galėtų siekti apie 7,7 % mokėjimų asignavimų.

Numatytomis kontrolės priemonėmis siekiama užtikrinti sklandžią ir veiksmingą Komisijos atliekamą vykdomųjų subjektų priežiūrą ir reikiamą patikimumo lygį Komisijos lygmeniu.

Kontrolės priemonių nauda yra ši:

- išvengiama silpnų arba netinkamų pasiūlymų pasirinkimo;
- optimizuojamas planavimas ir ES lėšų naudojimas siekiant išsaugoti ES pridėtinę vertę;
- užtikrinama dotacijos susitarimų kokybė, išvengiama klaidų nustatant teisinius subjektus, užtikrinamas tinkamas ES įnašų apskaičiavimas ir prisiimamos reikiamos garantijos tinkamam dotacijų valdymui;
- mokėjimų etapu nustatomos netinkamos finansuoti išlaidos;
- audito etapu nustatomos klaidos, neigiamai veikiančios operacijų teisėtumą ir tvarkingumą.

### **Apytikris klaidų lygis**

Siekiami visos Programos likutinį klaidų lygį išlaikyti mažesnį negu 2 % riba, kartu apribojant kontrolės našta paramos gavėjams, kad būtų pasiekta tinkama teisėtumo ir tvarkingumo tikslo pusiausvyra su kitais tikslais, pvz., Programos patrauklumu, ypač MVI, ir kontrolės priemonių sąnaudomis.

### **2.3. Sukčiavimo ir pažeidimų prevencijos priemonės**

*Nurodyti dabartines arba numatytas prevencijos ir apsaugos priemones.*

OLAF gali atlikti tyrimus, įskaitant patikrinimus ir inspektavimus vietoje, laikydamosi Europos Parlamento ir Tarybos reglamento Nr. 883/2013 ir 1996 m. lapkričio 11 d. Tarybos reglamento (Euratomas, EB) Nr. 2185/9640 dėl Komisijos atliekamų patikrinimų ir inspektavimų vietoje siekiant apsaugoti Sąjungos finansinius interesus nuo sukčiavimo ir kitų pažeidimų nuostatų ir procedūrų, kad nustatytų sukčiavimo, korupcijos arba bet kurios kitos neteisėtos veiklos, susijusios su Kompetencijos centro finansuojamomis dotacijomis ar sutartimis ir turinčios neigiamą poveikį Sąjungos finansiniams interesams, atvejus.

Sutartyse, susitarimuose ir sprendimuose, sudaromuose įgyvendinant šį reglamentą, yra nuostatos, kuriomis Komisija, Kompetencijos centras, Audito Rūmai ir OLAF aiškiai įgaliojami atlikti auditą ir tyrimus pagal atitinkamas savo kompetencijos sritis.

Atlikdamas arba pavesdamas atlikti tinkamą vidaus ir išorės kontrolę Kompetencijos centras užtikrina, kad jo narių finansiniai interesai būtų tinkamai apsaugoti.

Kompetencijos centras turi prisijungti prie 1999 m. gegužės 25 d. Tarpinstitucinio susitarimo tarp Europos Parlamento, Europos Sąjungos Tarybos ir Europos Bendrijų Komisijos dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų vidaus tyrimų. Kompetencijos centras patvirtina priemones, kurios būtinos siekiant sudaryti palankesnes sąlygas OLAF atliekamiems vidaus tyrimams.

Kompetencijos centre bus priimta kovos su sukčiavimu strategija, pagrįsta sukčiavimo rizikos analize ir sąnaudų ir naudos kriterijais. Sąjungos finansiniai interesai bus apsaugoti taikant prevencines kovos su sukčiavimu, korupcija ir bet kokia kita neteisėta veikla priemones, vykdant veiksmingus patikrinimus ir, nustačius pažeidimų, susigrąžinant neteisingai išmokėtas sumas bei prireikrus taikant veiksmingas, proporcingas ir atgrasomąsias administracines ir finansines nuobaudas.





### 3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

#### 3.1. Atitinkama daugiametės finansinės programos išlaidų kategorija ir siūloma nauja biudžeto išlaidų eilutė (-ės)

- Prašomos sukurti naujos biudžeto eilutės

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

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Numeris	DA / NDA <sup>38</sup>	ELPA šalių <sup>39</sup>	šalių kandidačių <sup>40</sup>	trečiųjų šalių	pagal Finansinio reglamento [21 straipsnio 2 dalies b punktą]
I išlaidų kategorija: Bendroji rinka, inovacijos ir skaitmeninė ekonomika	01 02 XX XX Programa „Europos horizontas“, Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras – rėmimo išlaidos	DA	TAIP	TAIP (jeigu nurodyta metinėje darbo programoje)	TAIP (tačiau tik tam tikroje programos dalyje)	NE
	01 02 XX XX Programa „Europos horizontas“, Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras					
	02 06 01 XX Skaitmeninės Europos programa, Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras – rėmimo išlaidos					
	02 06 01 XX Skaitmeninės Europos programa, Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras					

<sup>38</sup> DA – diferencijuotieji asignavimai, NDA – nediferencijuotieji asignavimai.

<sup>39</sup> ELPA – Europos laisvosios prekybos asociacija.

<sup>40</sup> Šalių kandidačių ir, kai taikoma, Vakarų Balkanų potencialių šalių kandidačių.

- Įnašo į šias biudžeto eilutes laukiama iš:

mln. EUR (tūkstantųjų tikslumu)

Biudžeto eilutė	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	Iš viso
01 01 01 01 Išlaidos mokslinių tyrimų pareigūnams – laikiniejiems darbuotojams, programa „Europos horizontas“	pm	pm	pm	pm	pm	pm	pm	pm
01 01 01 02 Išorės darbuotojai, įgyvendinantys mokslinių tyrimų programas, programa „Europos horizontas“	pm	pm	pm	pm	pm	pm	pm	pm
01 01 01 03 Kitos mokslinių tyrimų valdymo išlaidos, programa „Europos horizontas“	pm	pm	pm	pm	pm	pm	pm	pm
01 02 02 Pasauliniai uždaviniai ir pramonės konkurencingumas	pm	pm	pm	pm	pm	pm	pm	pm
02 01 04 Administracinė parama, Skaitmeninės Europos programa	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
02 06 01 Kibernetinis saugumas, Skaitmeninės Europos programa	284,892	322,244	327,578	248,382	253,295	258,214	263,316	1 957,922
<b>Iš viso išlaidų</b>	<b>286,130</b>	<b>325,274</b>	<b>331,320</b>	<b>252,200</b>	<b>257,189</b>	<b>262,186</b>	<b>267,368</b>	<b>1 981,668</b>

**Komisija per teisėkūros procedūrą ir bet koku atveju prieš pasiekiant politinį susitarimą pasiūlys įnašą iš programos „Europos horizontas“ II veiklos srities „Pasauliniai uždaviniai ir pramonės konkurencingumas“ veiksmų grupės „Įtrauki ir saugi visuomenė“ finansinio paketo (bendra paketo suma – 2 800 000 000 EUR), nurodytą 21 straipsnio 1 dalies b punkte Pasiūlymas bus pagrįstas strateginio planavimo proceso rezultatais, kaip apibrėžta Reglamento XXX 6 straipsnio 6 dalyje [bendroji programa „Europos horizontas“].**

Į pirmiau nurodytas sumas neįtraukti valstybių narių įnašai į Kompetencijos centro veiklos ir administracines išlaidas, proporcingi Sąjungos finansiniam įnašui.

### 3.2. Numatomas poveikis išlaidoms

#### 3.2.1. Numatomo poveikio išlaidoms santrauka

mln. EUR (tūkstantųjų tikslumu)

<b>Daugiametės finansinės programos</b>	<b>1 išlaidų kategorija</b>	Bendroji rinka, inovacijos ir skaitmeninė ekonomika
---	-----------------------------	---

			2021 m. 41	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	Po 2027 m.	IŠ VISO
1 antraštinė dalis (Personalo išlaidos)	Įsipareigojimai = Mokėjimai	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		11,873
2 antraštinė dalis (Infrastruktūros ir veiklos išlaidos)	Įsipareigojimai = Mokėjimai	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		11,873
3 antraštinė dalis (Veiklos išlaidos)	Įsipareigojimai	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		1 957,922
	Mokėjimai	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	1 957,922
<b>IŠ VISO asignavimų programų paketui<sup>42</sup></b>	Įsipareigojimai	=1+2+ 3	<b>286,130</b>	<b>325,274</b>	<b>331,320</b>	<b>252,200</b>	<b>257,189</b>	<b>262,186</b>	<b>267,368</b>		<b>1 981,668</b>

<sup>41</sup> Personalo asignavimai numatyti tik 2021 m. pusmečiui

<sup>42</sup> Bendri numatyti asignavimai siejami tik su ES finansiniais ištekliais, skirtais kibernetiniam saugumui stiprinti pagal Skaitmeninės Europos programą. Komisija per teisėkūros procedūrą ir bet koku atveju prieš pasiekiant politinį susitarimą pasiūlys įnašą iš programos „Europos horizontas“ II veiklos srities „Pasauliniai uždaviniai ir pramonės konkurencingumas“ veiksmų grupės „Įtrauki ir saugi visuomenė“ finansinio paketo (bendra paketo suma – 2 800 000 000 EUR), nurodytą 5 straipsnio 1 dalies b punkte Pasiūlymas bus pagrįstas strateginio planavimo proceso rezultatais, kaip apibrėžta Reglamento XXX 6 straipsnio 6 dalyje [bendroji programa „Europos horizontas“].

	Mokėjimai	$\frac{=1+2+}{4}$	22,459	105,795	153,954	171,154	160,369	154,096	152,126	1 061,715	1 981,668
--	-----------	-------------------	--------	---------	---------	---------	---------	---------	---------	-----------	-----------

<b>Daugiametės finansinės programos</b>	7 išlaidų kategorija	„Administracinės išlaidos“
---	----------------------	----------------------------

mln. EUR (tūkstantųjų tikslumu)

		2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	Po 2027 m.	IŠ VISO
Žmogiškieji ištekliai		3,090	3,233	3,233	3,233	3,233	3,233	3,805		23,060
Kitos administracinės išlaidos		0,105	0,100	0,104	0,141	0,147	0,153	0,159		0,909
<b>IŠ VISO asignavimų pagal daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ</b>	(Iš viso įsipareigojimų = Iš viso mokėjimų)	<b>3,195</b>	<b>3,333</b>	<b>3,337</b>	<b>3,374</b>	<b>3,380</b>	<b>3,386</b>	<b>3,964</b>		<b>23,969</b>

mln. EUR (tūkstantųjų tikslumu)

		2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	Po 2027 m.	IŠ VISO
<b>IŠ VISO asignavimų pagal daugiametės finansinės programos IŠLAIDŲ KATEGORIJAS</b>	Įsipareigojimai	289,325	328,607	334,657	255,574	260,569	265,572	271,332		2 005,637
	Mokėjimai	25,654	109,128	157,291	174,528	163,749	157,482	156,090	1 061,715	2 005,637

### 3.2.2. Numatomo poveikio administracinio pobūdžio asignavimams santrauka

- Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimų nenaudojama
- Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

Metai	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	IŠ VISO
-------	---------	---------	---------	---------	---------	---------	---------	---------

<b>Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJA</b>								
Žmogiškieji ištekliai	3,090	3,233	3,233	3,233	3,233	3,233	3,805	23,060
Kitos administracinės išlaidos	0,105	0,100	0,104	0,141	0,147	0,153	0,159	0,909
<b>Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJOS tarpinė suma</b>	<b>3,195</b>	<b>3,333</b>	<b>3,337</b>	<b>3,374</b>	<b>3,380</b>	<b>3,386</b>	<b>3,964</b>	<b>23,969</b>

<b>Neįtraukta į daugiametės finansinės programos<sup>43</sup> 7 IŠLAIDŲ KATEGORIJA</b>								
Žmogiškieji ištekliai								
Kitos administracinio pobūdžio išlaidos	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
<b>Tarpinė suma, neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJA</b>	<b>1,238</b>	<b>3,030</b>	<b>3,743</b>	<b>3,818</b>	<b>3,894</b>	<b>3,972</b>	<b>4,051</b>	<b>23,746</b>

<b>IŠ VISO</b>	<b>4,433</b>	<b>6,363</b>	<b>7,079</b>	<b>7,192</b>	<b>7,274</b>	<b>7,358</b>	<b>8,016</b>	<b>47,715</b>
----------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	---------------

Žmogiškųjų išteklių ir kitų administracinio pobūdžio išlaidų asignavimų poreikiai bus tenkinami iš GD asignavimų, jau paskirtų priemonei valdyti ir (arba) perskirstytų generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę asignavimų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

Pirmiau nurodyti žmogiškiesiems ištekliams ir kitoms administracinio pobūdžio išlaidoms skirti asignavimai, neįtraukti į 7 išlaidų kategoriją, atitinka Sąjungos finansinio įnašo sumas pagal Skaitmeninės Europos programą.

<sup>43</sup> Techninė ir (arba) administracinė pagalba bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

Pirmiau nurodyti žmogiškiesiems ištekliams ir kitoms administracinio pobūdžio išlaidoms skirti asignavimai, neįtraukti į 7 išlaidų kategoriją, bus padidinti Sąjungos finansinio įnašo sumomis pagal programą „Europos horizontas“, Komisijai per teisėkūros procedūrą ir bet koku atveju prieš pasiekiant politinį susitarimą pasiūlius įnašą iš II veiklos srities „Pasauliniai uždaviniai ir pramonės konkurencingumas“ veiksmų grupės „Įtraukti ir saugi visuomenė“ paketo (bendra paketo suma – 2 800 000 000 EUR), nurodytą 21 straipsnio 1 dalies b punkte.

Į pirmiau nurodytus žmogiškiesiems ištekliams ir kitoms administracinio pobūdžio išlaidoms skirtus asignavimus, neįtrauktus į 7 išlaidų kategoriją, neįtraukti valstybių narių įnašai į Kompetencijos centro administracines išlaidas, proporcingi Sąjungos finansiniam įnašui.

### 3.2.2.1. Numatomi Komisijos žmogiškųjų išteklių poreikiai

- Pasiūlymui (iniciatyvai) įgyvendinti žmogiškųjų išteklių nenaudojama.
- Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

*Sąmatą surašyti etatų vienetais*

Metai	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.
<b>• Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)</b>							
Komisijos būstinė ir atstovybės	20	21	21	21	21	21	22
Delegacijos							
Moksliniai tyrimai							
<b>• Išorės darbuotojai (viso etatų ekvivalentais): AC, AL, END, INT ir JED<sup>44</sup></b>							
7 išlaidų kategorija							
Finansuojama pagal daugiamečių finansinės programos 7 IŠLAIDŲ KATEGORIJA	– būstinėje	3	3	3	3	3	3
	– delegacijose						
Finansuojama iš programos paketo lėšų <sup>45</sup>	– būstinėje						
	– delegacijose						
Moksliniai tyrimai							
Kita (nurodyti)							
<b>IŠ VISO</b>	<b>23</b>	<b>23</b>	<b>24</b>	<b>24</b>	<b>24</b>	<b>25</b>	<b>25</b>

Žmogiškųjų išteklių poreikiai bus finansuojami šiai priemonei administruoti jau skirtomis ir (arba) generaliniame direktorate (GD) persikirstytomis lėšomis, o tam tikrais atvejais – papildomomis lėšomis, kurių administruojančiam generaliniam direktoratui gali būti skirta pagal metinių asignavimų procedūrą, atsižvelgiant į biudžeto apribojimus.

Atliekamų užduočių aprašymas:

Pareigūnai ir laikinieji darbuotojai	<p>Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrui pavestų užduočių koordinavimas, stebėseną ir valdymas, įskaitant paramos iš koordinavimo išlaidas.</p> <p>Kibernetinio saugumo politikos kūrimas ir koordinavimas, susijęs su Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrui pavestomis užduotimis, pvz., mokslinių tyrimų ir pramonės politikos prioritetų nustatymas, bendras valstybių narių ir ekonominės veiklos vykdytojų bendradarbiavimas, būsimos ES kibernetinio saugumo sertifikavimo sistemos reikalavimų atitiktis, atsakomybės ir rūpestingumo pareigos nuostatos arba derinimas su HPC ir dirbtinio</p>
--------------------------------------	--

<sup>44</sup> AC – sutartininkai („Contract Agent“); AL – vietiniai darbuotojai („Local Staff“); END – deleguotieji nacionaliniai ekspertai („Seconded National Expert“); INT – per agentūrą įdarbinti darbuotojai („Agency staff“); JES – jaunesnieji delegacijos specialistai („Junior Professionals in Delegations“).

<sup>45</sup> Neviršijant ribos, nustatytos išorės darbuotojams, finansuojamiems iš veiklos asignavimų (buvusių BA eilučių).



	intelekto politika ir skaitmeniniais įgūdžiais.
Išorės darbuotojai	<p>Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrui pavestų užduočių koordinavimas, stebėseną ir valdymas, įskaitant paramos iš koordinavimo išlaidas.</p> <p>Kibernetinio saugumo politikos kūrimas ir koordinavimas, susijęs su Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrui pavestomis užduotimis, pvz., mokslinių tyrimų ir pramonės politikos prioritetų nustatymas, bendras valstybių narių ir ekonominės veiklos vykdytojų bendradarbiavimas, būsimos ES kibernetinio saugumo sertifikavimo sistemos reikalavimų atitiktis, atsakomybės ir rūpestingumo pareigos nuostatos arba derinimas su HPC ir dirbtinio intelekto politika ir skaitmeniniais įgūdžiais.</p>

### 3.2.2.2. Numatomi Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro žmogiškųjų išteklių poreikiai

	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.
Komisijos pareigūnai							
iš jų AD							
iš jų AST							
iš jų AST-SC							
Laikinieji darbuotojai							
iš jų AD	10	11	13	13	13	13	13
iš jų AST							
iš jų AST-SC							
Sutartininkai	26	32	39	39	39	39	39
Deleguotieji nacionaliniai ekspertai	1	1	1	1	1	1	1
<b>Iš viso</b>	<b>37</b>	<b>44</b>	<b>53</b>	<b>53</b>	<b>53</b>	<b>53</b>	<b>53</b>

Atliekamų užduočių aprašymas:

Pareigūnai ir laikinieji darbuotojai	Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrui pavestų užduočių įgyvendinimas pagal šio Reglamento 4 straipsnį, įskaitant paramos iš koordinavimo išlaidas.
Išorės darbuotojai	Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrui pavestų užduočių įgyvendinimas pagal šio Reglamento 4 straipsnį, įskaitant paramos iš koordinavimo išlaidas.

Pirmiau nurodyti numatomi Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro žmogiškųjų išteklių poreikiai atitinka numatytus reikalavimus įgyvendinti Sąjungos finansinį įnašą pagal Skaitmeninės Europos programą.

Pirmiau nurodyti numatomi Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro žmogiškųjų išteklių poreikiai bus padidinti Sąjungos reikalavimais įgyvendinti Sąjungos finansinį įnašą pagal programą „Europos horizontas“, Komisijai per teisėkūros procedūrą ir bet koku atveju prieš pasiekiant politinį susitarimą pasiūlius įnašą iš II veiklos srities „Pasauliniai uždaviniai ir pramonės konkurencingumas“ veiksmų grupės „Įtrauki ir saugi visuomenė“ paketo (bendra paketo suma – 2 800 000 000 EUR), nurodytą 21 straipsnio 1 dalies b punkte.

3.2.2.3. Numatomas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro etatų planas

Pareigų grupė ir lygis	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2025 m.	2025 m.
AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
Iš viso AD	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
Iš viso AST							

AST / SC 6							
AST / SC 5							
AST / SC 4							
AST / SC 3							
AST / SC 2							
AST / SC 1							
Iš viso AST / SC							
<b>BENDRA SUMA</b>	<b>10</b>	<b>11</b>	<b>13</b>	<b>13</b>	<b>13</b>	<b>13</b>	<b>13</b>

3.2.2.4. Numatytas poveikis (papildomam) personalui – Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro išorės darbuotojams

Sutartininkai	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.
IV pareigų grupė	20	22	29	29	29	29	29
III pareigų grupė	2	4	4	4	4	4	4
II pareigų grupė	4	6	6	6	6	6	6
I pareigų grupė							
<b>Iš viso</b>	<b>26</b>	<b>32</b>	<b>39</b>	<b>39</b>	<b>39</b>	<b>39</b>	<b>39</b>

Siekiant užtikrinti neutralų darbuotojų skaičių, papildomų Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro darbuotojų skaičių dalinai kompensuos atitinkamų Komisijos tarnybų pareigūnų ir išorinio personalo (t. y. dabartinio etatų plano ir išorinio personalo) mažinimas.

3.2.2.2–4 punktuose išvardytų Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro darbuotojų skaičius bus kompensuojamas taip<sup>46</sup>:

IŠ VISO	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.
Komisijos pareigūnai	5	5	6	6	6	6	6
Laikinieji darbuotojai							
<b>Sutartininkai</b>	<b>14</b>	<b>17</b>	<b>20</b>	<b>20</b>	<b>20</b>	<b>20</b>	<b>20</b>

<sup>46</sup> Pagal galutinę biudžeto, kurio įgyvendinimas bus deleguotas Kompetencijos centrui, sumą.

Deleguotieji nacionaliniai ekspertai							
Iš viso etato ekvivalentų	19	22	26	26	26	26	26
Darbuotojų skaičius	19	22	26	26	26	26	26

Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro žmogiškųjų išteklių kompensavimas bus proporcingas Sąjungos finansinio įnašo daliai, t. y. 50 %.

Pirmiau nurodytas kompensavimas siejamas su numatomais Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro žmogiškųjų išteklių poreikiais, įgyvendinant Sąjungos finansinį įnašą pagal Skaitmeninės Europos programą.

Pirmiau nurodytas kompensavimas bus padidintas Sąjungos reikalavimais įgyvendinti Sąjungos finansinį įnašą pagal programą „Europos horizontas“, Komisijai per teisėkūros procedūrą ir bet koku atveju prieš pasiekiant politinį susitarimą pasiūlius įnašą iš II veiklos srities „Pasauliniai uždaviniai ir pramonės konkurencingumas“ veiksmų grupės „Įtrauki ir saugi visuomenė“ paketo (bendra paketo suma – 2 800 000 000 EUR), nurodytą 21 straipsnio 1 dalies b punkte.

### 3.2.3. Trečiųjų šalių įnašai

Pasiūlyme (iniciatyvoje):

- nenumatyta bendro su trečiosiomis šalimis finansavimo
- numatytas trečiųjų šalių bendras finansavimas<sup>47</sup> apskaičiuojamas taip:

Asignavimai mln. EUR (tūkstantųjų tikslumu)

Metai	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	IŠ VISO
Valstybių narių įnašas į personalo išlaidas	0,619	1,515	1,871	1,909	1,947	1,986	2,026	11,873
Valstybių narių įnašas į infrastruktūros ir veiklos išlaidas	0,619	1,515	1,871	1,909	1,947	1,986	2,026	11,873
Valstybių narių įnašas į veiklos išlaidas	284,892	322,244	327,578	248,382	253,295	258,214	263,316	1 957,922
<b>IŠ VISO bendrai finansuojamų asignavimų</b>	<b>286,130</b>	<b>325,274</b>	<b>331,320</b>	<b>252,200</b>	<b>257,189</b>	<b>262,186</b>	<b>267,368</b>	<b>1 981,668</b>

Pirmiau nurodytas trečiųjų šalių dalyvavimas finansavimo veikloje susijęs tik su bendru finansavimu, proporcingu kibernetiniam saugumui skirtiems ES finansiniams ištekliams pagal Skaitmeninės Europos programą. Pirmiau nurodytas trečiųjų šalių dalyvavimas finansavimo veikloje bus padidintas Komisijai per teisėkūros procedūrą ir bet koku atveju prieš pasiekiant politinį susitarimą pasiūlius finansinį įnašą iš programos „Europos horizontas“ II veiklos srities „Pasauliniai uždaviniai ir pramonės konkurencingumas“ veiksmų grupės „Įtrauki ir saugi visuomenė“ (bendra paketo suma – 2 800 000 000 EUR), nurodytą 21 straipsnio 1 dalies b punkte. Pasiūlymas bus pagrįstas strateginio planavimo proceso rezultatais, kaip apibrėžta Reglamento XXX 6 straipsnio 6 dalyje [bendroji programa „Europos horizontas“].

### 3.3 Numatomas poveikis pajamoms

- Pasiūlymas (iniciatyva) neturi finansinio poveikio pajamoms.
- Pasiūlymas (iniciatyva) turi finansinį poveikį:
  - nuosaviems ištekliams
  - kitoms pajamoms

Nurodyti, jei pajamos priskirtos išlaidų eilutėms

mln. EUR (tūkstantųjų tikslumu)

Biudžeto pajamų eilutė	Pasiūlymo (iniciatyvos) poveikis <sup>48</sup>						
	2021 m.	2022 m.	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.
..... straipsnis							

<sup>47</sup> Numatomas valstybių narių įnašas natūra

<sup>48</sup> Tradiciniai nuosavi ištekliai (muitai, cukraus mokesčiai) turi būti nurodomi grynosiomis sumomis, t. y. iš bendros sumos atskaičius 20 % surinkimo sąnaudų.

Asignuotųjų pajamų atveju nurodyti biudžeto išlaidų eilutę (-es), kuriai (-oms) daromas poveikis.

Kitos pastabos (pvz., poveikio pajamoms apskaičiavimo metodas (formulė) arba kita informacija).