D.E.U. br. 19/023

HRVATSKI SABOR
Odbor za europske poslove

Klasa: 022-03/19-03/54
Urbroj: 6521-31-19-01
Zagreb, 10. travnja 2019.

ODBOR ZA OBRANU
Predsjednik Igor Dragovan

ODBOR ZA INFORMIRANJE, INFORMATIZACIJU I MEDIJE
Predsjednica Sunčana Glavak

Poštovani predsjednici odbora,

Odbor za europske poslove na temelju članka 154. stavka 1. Poslovnika Hrvatskoga sabora prosljeđuje Odboru za obranu i Odboru za informiranje, informatizaciju i medije stajalište o dokumentu Europske unije iz Radnog programa za razmatranje stajališta Republike Hrvatske za 2019. godinu:

Stajalište Republike Hrvatske o
Prijedlogu uredbe Europskog parlamenta i Vijeća o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara
COM (2018) 630

koje je Koordinacija za vanjsku i europsku politiku i ljudska prava Vlade Republike Hrvatske usvojila Zaključkom: Klasa: 022-03/19-07/148, Urbroj: 50301-23/22-19-3 na sjednici održanoj 26. ožujka 2019. godine.

Predmetni Prijedlog uredbe Komisija je dostavila Hrvatskom saboru 12. rujna 2018., te je u tijeku njegovo donošenje u Europskom parlamentu i Vijeću Europske unije.

U skladu s člankom 154. stavkom 2. Poslovnika Hrvatskoga sabora, molim vas da Odboru za europske poslove dostavite mišljenje o Stajalištu Republike Hrvatske najkasnije do 10. svibnja 2019. godine.

S poštovanjem,

PREDSJEDNIK ODBORA
Domagoj Ivan Milošević

U prilogu:
- Stajalište Republike Hrvatske o COM (2018) 630
- COM (2018) 630

Na znanje:
- INFODOK služba

PRIJEDLOG STAJALIŠTA RH

Naziv dokumenta (na hrvatskom i engleskom):

Prijedlog uredbe Europskog parlamenta i Vijeća o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara

Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres[1]

Brojčana oznaka dokumenta: **7583/19; Međuinstitucijski predmet: 2018/0328 (COD)**

Nadležno TDU za izradu prijedloga stajališta (nositelj izrade stajališta), ustrojstvena jedinica i službenik/ica:

Nadležno državno tijelo: Središnji državni ured za razvoj digitalnog društva (ured@rdd.hr)

Nadležni službenik: Marin Ante Pivčević (marin.ante.pivcevic@rdd.hr)

Zamjena: Ana Jovičić (ana.jovicic@rdd.hr)

Druga TDU, agencije i javne ustanove uključene u izradu Prijedloga stajališta:

Ministarstvo mora, prometa i infrastrukture; Ministarstvo gospodarstva, poduzetništva i obrta; Ministarstvo znanosti i obrazovanja; Ured Vijeća za nacionalnu sigurnost; Zavod za sigurnost informacijskih sustava

Nadležna službenica u MVEP (Sektor za COREPER I):

Ana Đukić (ana.dukic@mvep.hr) 01/4569-816

Nadležna radna skupina Vijeća EU i nadležna službenica u SP RH pri EU:

Horizontalna radna skupina za kibernetička pitanja; Tamara Tafra (Tamara.Tafra@mvep.hr)

Osnovne sadržajne odredbe prijedloga EU:

Prijedlogom uredbe Europskog parlamenta i Vijeća o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara (dalje u tekstu: Prijedlog) predlaže se osnivanje Europskog industrijskog, tehnološkog i istraživačkog središta za kibernetičku sigurnost (dalje u tekstu: Centar kompetencija) te Mreže nacionalnih koordinacijskih središta (dalje u tekstu: Mreža kompetencija). Kako bi ovaj namjenski model suradnje potaknuo europski tehnološki i industrijski ekosustav, trebao bi djelovati na sljedeći

[1] Ime prijedloga akta, službeno objavljenog od strane EK kako je navedeno u ovoj kategoriji, u daljnjim raspravama je izmijenjeno na način da se izostavlja riječ „*competence*" iz naziva: Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research ~~Competence~~ Centre and the Network of National Coordination Centres

način: Centar kompetencija olakšavat će i potpomagati koordinaciju rada Mreže kompetencija, poticati Zajednicu stručnjaka za kibernetičku sigurnost (eng. *Cybersecurity Competence Community*) i provedbu programa tehnološkog razvoja te olakšavati pristup tako prikupljenom znanju. Zamišljeno je da Centar kompetencija djeluje na razini Europske unije (dalje u tekstu EU), Mreža kompetencija na nacionalnoj razini, a Zajednica stručnjaka za kibernetičku sigurnost sveobuhvatno, na razini zainteresiranih strana (eng. *stakeholder level*).

Centar kompetencija bi ponajprije trebao provoditi relevantne dijelove programa Digitalna Europa i Obzor Europa, dodjelom nepovratnih sredstava i obavljanjem nabave. S obzirom na znatna ulaganja u kibernetičku sigurnost drugdje u svijetu te potrebu za koordinacijom i udruživanjem financijskih sredstava u Europi, predlaže se da Centar kompetencija ima oblik europskog partnerstva kako bi se olakšala zajednička ulaganja EU-a, država članica i/ili industrije. Stoga se ovim Prijedlogom uredbe zahtijeva od država članica da djelovanju Mreže kompetencija i Centra kompetencija pridonesu odgovarajućim novčanim sredstvima, ovisno o projektima. Tijela Centra kompetencija bi trebala biti Upravni odbor, izvršni direktor te Savjetodavni industrijski i znanstveni odbor. Glavno tijelo za donošenje odluka bi bio Upravni odbor, u kojem sudjeluju sve države članice i predstavnici Europske komisije (dalje u tekstu EK) koji imaju 50% glasačkih prava u proračunskim pitanjima *(kompromisni prijedlog nakon dosta osporavanja)*. U slučaju združenih projekata nekih država članica i EK, glasačka prava bi bila proporcionalna svačijem doprinosu tom projektu *(kompromisni prijedlog)*. Za potrebe svojega rada u Upravnom odboru EK bi, kad god to bude moguće, tražila stručno mišljenje Europske službe za vanjsko djelovanje *(EEAS)*. Upravnom odboru bi pomagao Industrijski i znanstveni savjetodavni odbor kako bi se osigurao redoviti dijalog s privatnim sektorom, organizacijama potrošača i drugim interesnim skupinama.

U bliskoj suradnji s Mrežom kompetencija i Zajednicom stručnjaka za kibernetičku sigurnost (u kojoj sudjeluje velika i raznolika skupina dionika koji su uključeni u razvoj tehnologije kibernetičke sigurnosti, kao što su istraživački subjekti, industrije na strani ponude, industrije na strani potražnje i javni sektor), koji se osnivaju ovom Uredbom, Centar kompetencija bio bi glavno usmjerivačko tijelo za financijska sredstva EU-a namijenjena za kibernetičku sigurnost u okviru predloženog programa Digitalna Europa i programa Obzor Europa. Takvim sveobuhvatnim pristupom omogućilo bi se poticanje kibernetičke sigurnosti u cijelom vrijednosnom lancu, od istraživanja do podupiranja primjene i prihvaćanja ključnih tehnologija. Financijski doprinosi država članica (kroz projekte) trebali bi biti razmjerni financijskom doprinosu EU-a ovoj inicijativi i nužan su element njezina uspjeha.

Nadalje, Centar kompetencija trebao bi nastojati povećati prožimanje civilne i obrambene dimenzije kibernetičke sigurnosti, trebao bi podupirati države članice i druge relevantne zainteresirane strane davanjem savjeta, razmjenom stručnosti i olakšavanjem suradnje na projektima i mjerama. Na zahtjev država članica Centar kompetencija trebao bi djelovati i u svojstvu voditelja projekta, osobito u pogledu Europskog fonda za obranu. Također, Centar kompetencija i Mreža kompetencija trebali bi podupirati i istraživanja usmjerena na olakšavanje i ubrzavanje postupaka standardizacije i certifikacije, posebno onih povezanih s programima kibernetičke sigurnosne certifikacije u smislu predloženog „Akta o kibernetičkoj sigurnosti“ *(u završnoj fazi donošenja)*.

Razlozi za donošenje i pozadina dokumenta:

Budući da naš svakodnevni život i gospodarstvo sve više ovise o digitalnim tehnologijama, građani postaju sve izloženiji ozbiljnim kibernetičkim incidentima. Buduća sigurnost ovisi o jačanju sposobnosti za zaštitu EU-a od kibernetičkih prijetnji, jer se civilna infrastruktura i vojni kapaciteti oslanjaju na sigurne digitalne sustave.

Kako bi se mogla suočiti sa sve većim izazovima, EU je postupno povećavala svoje aktivnosti u tom području na temelju Strategije za kibernetičku sigurnost iz 2013. godine i njezinih ciljeva i načela poticanja pouzdanog, sigurnog i otvorenog kibernetičkog ekosustava. EU je 2016. godine donio prve mjere u području kibernetičke sigurnosti, donošenjem Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća o sigurnosti mrežnih i informacijskih sustava (skraćeno NIS Direktiva).

Budući da se područje kibernetičke sigurnosti brzo razvija, EK i Visoki predstavnik EU-a za vanjske poslove i sigurnosnu politiku predstavili su u rujnu 2017. godine Zajedničku komunikaciju "Otpornost, odvraćanje i obrana: jačanje kibernetičke sigurnosti EU-a", u cilju daljnjeg jačanja otpornosti EU-a, odvraćanja i odgovora na kibernetičke napade. U Zajedničkoj komunikaciji, koja se temelji i na prethodnim inicijativama, naveden je skup predloženih mjera, uključujući, uz ostalo, jačanje Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA), uspostavu dobrovoljnog okvira EU-a za kibernetičku sigurnosnu certifikaciju u cijelom EU-u sa ciljem povećanja kibernetičke sigurnosti proizvoda i usluga u digitalnom svijetu, te plan za brzi, koordinirani odgovor na opsežne kibernetičke incidente i krize.

U Zajedničkoj komunikaciji istaknuto je da je u strateškom interesu EU-a osigurati da zadrži i razvije bitne tehnološke sposobnosti za kibernetičku sigurnost, u cilju zaštite svojega jedinstvenoga digitalnog tržišta, a posebno u cilju zaštite ključnih mrežnih i informacijskih sustava i pružanja ključnih kibernetičkih sigurnosnih usluga. EU mora moći neovisno zaštititi svoju digitalnu imovinu i natjecati se na globalnom tržištu kibernetičke sigurnosti.

Programom Digitalna Europa, koji je EK predložila u lipnju 2018. godine, nastoji se povećati i što više iskoristiti digitalnu transformaciju za europske građane i poduzeća u svim relevantnim područjima politika EU-a, ojačati politike i poduprijeti ambicije jedinstvenoga digitalnog tržišta. Programom se predlaže dosljedan i sveobuhvatan pristup osiguravanju najbolje uporabe naprednih tehnologija i odgovarajuće kombinacije tehničkih kapaciteta i ljudskih sposobnosti za digitalnu transformaciju, ne samo u području kibernetičke sigurnosti, već i u pogledu infrastrukture pametnih podataka, umjetne inteligencije, naprednih vještina i primjena u industriji i područjima od javnog interesa. Ti elementi su međuovisni, uzajamno se podupiru i, uz istodobno poticanje, mogu se razviti do mjere koja je nužna za uspješno podatkovno gospodarstvo. Kibernetička sigurnost obuhvaćena je i prioritetima programa Obzor Europa, odnosno sljedećeg okvirnog programa EU-a za istraživanje i razvoj.

Status dokumenta:

Prijedlog je objavljen 12. rujna 2018. godine te je provedena rasprava u Horizontalnoj radnoj skupini za kibernetička pitanja. U prosincu 2018. godine TTE Vijeće je usvojilo izvješće o napretku

austrijskog Predsjedništva. 13. ožujka 2019. godine rumunjsko je Predsjedništvo na sastanku COREPER-a I potraživalo mandat za pregovore temeljem revidirane verzije teksta prijedloga Uredbe te je isti i odobren, a trijalog se održao 20. ožujka godine. Novi revidirani mandat za trijalog 28. ožujka 2019. godine rumunjsko će Predsjedništvo tražiti na sastanku COREPER-a I 27. ožujka 2019. godine.

Stajalište RH:

Republika Hrvatska (dalje u tekstu: RH) podržava do sada predložene promjene i ističe zadovoljstvo uloženim trudom i kvalitetnim prijedlozima i članica i Predsjedništva. Osobito se podržavaju paragrafi recitala (8), (8a), (11), (12), (13), (17) i (21) u njihovom sadašnjem izričaju, a (15), (18a), (18b) i (28) u njihovom smislu. Glede odredbenih članaka osobito se podržava sadašnji izričaj: čl. 2.1.(3), čl. 6.4., čl. 7.3., čl. 8.4., čl. 8.5., čl. 12.3., čl. 15.3., čl.15.3a., čl.15.1., čl. 18.2a., čl. 21.1., čl. 36.2., čl. 36.3. i čl. 42., a čl. 4. i čl. 4a. u njihovom smislu. Glede recitala (7a), ako ne može formalno biti u predloženom obliku, RH podržava izravno određivanje sjedišta u čl. 1.3, s tim da se navede geografsko načelo kao ključno. U cjelini je Prijedlog uredbe prihvatljiv i može se pristupiti izradi završnog kompromisnog teksta.

Stajališta DČ, EK i Predsjedništva EU:

Sve države članice su s entuzijazmom pristupile radu na ovome Prijedlogu, shvaćajući njegov značaj za povećanje kompetitivnosti EU. Brojnim primjedbama je početni tekst poboljšan, otvorena pitanja koja su uključivala model financiranja, sjedište, svrhu, ciljeve, uloge dionika te preklapanje s drugim tijelima/institucijama su pred konačnim usklađivanjem, a dvojbe i rezerve oko statusa su u fazi usuglašavanja.

Sporna/otvorena pitanja za DČ, EK i Predsjedništvo EU:

Otvoreno pitanje se odnosi na status Centra kompetencija, kojem većina nikako ne želi dodijeliti status (još jedne) agencije, a time se otvara i dvojba oko sjedišta Centra, te financiranja. Većina se slaže da financiranje administrativnih troškova pokriva EK (nikako pak na nacionalnoj razini), a traži se i temelj za primjenu geografskog kriterija.

Stav RH o spornim/otvorenim pitanjima:

RH ne vidi zapreke da se izravno u dokumentu ne razriješe statusna pitanja i podržava sve prijedloge koji na takav način uređuju stvar. RH se slaže da se Centar osnuje zajednički između EK i država članica (ne kao agencija EU-a), da se administrativne potrebe financiraju iz proračuna EU-a (ne one na nacionalnoj razini) te da se pri određivanju sjedišta donese politička odluka, odnosno primjene geografski kriteriji (RH nema ni jednu, pa makar i hibridnu organizaciju na svom teritoriju, te je zainteresirana strana). Glede ostalih dvojbi, RH načelno podržava one prijedloge koji sprječavaju majorizaciju.

Postojeće zakonodavstvo RH i potreba njegove izmjene slijedom usvajanja dokumenta:

Po usvajanju dokumenta, biti će nužno pristupiti formiranju Nacionalnog koordinacijskog središta ili pak nominirati neko postojeće tijelo za tu ulogu, što pak, zbog specifičnih uvjeta i ograničenja,

podliježe postupku formalnog odobravanja od strane Centra kompetencija. U slučaju regulacije ove problematike Uredbom Vlade, ne predviđa se utjecaj na zakonodavstvo.

Utjecaj provedbe dokumenta na proračun RH:

Za sada nije moguće procijeniti utjecaj provedbe dokumenta na proračun RH jer je predviđeno hibridno financiranje nacionalnih središta, pa proračunsko opterećenje može jako varirati, ovisno o programu. Administrativne troškove prve godine rada nacionalnog središta će se najvjerojatnije morati pokriti iz proračuna RH, dok bi se ubuduće ti troškovi u potpunosti pokrivali putem projekata iz programa Digitalna Europa i Obzor Europa te putem nacionalnih projekata dionika: gospodarstva, akademske zajednice i javnog sektora.

EUROPSKA
KOMISIJA

Bruxelles, 12.9.2018.
COM(2018) 630 final

2018/0328 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara

Doprinos Europske Komisije za sastanak čelnika u Salzburgu 19.–20. rujna 2018.

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

OBRAZLOŽENJE

1. KONTEKST PRIJEDLOGA

• Razlozi i ciljevi prijedloga

Budući da naš svakodnevni život i naše gospodarstvo sve više ovise o digitalnim tehnologijama, građani postaju sve izloženiji ozbiljnim kiberincidentima. Buduća sigurnost ovisi o jačanju sposobnosti za zaštitu Unije od kiberprijetnji jer se civilna infrastruktura i vojni kapaciteti oslanjaju na sigurne digitalne sustave.

Da bi se mogla suočiti sa sve većim izazovima, Unija je postupno povećavala svoje aktivnosti u tom području na temelju Strategije za kibersigurnost iz 2013.[1] i njezinih ciljeva i načela poticanja pouzdanog, sigurnog i otvorenog kiberekosustava. Unija je 2016. donijela svoje prve mjere u području kibersigurnosti donošenjem Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća[2] o sigurnosti mrežnih i informacijskih sustava.

Budući da se područje kibersigurnosti brzo razvija, Komisija i Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku predstavili su u rujnu 2017. Zajedničku komunikaciju[3] „Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a" u cilju daljnjeg jačanja otpornosti Unije, odvraćanja od i njezina odgovora na kibernapade. U Zajedničkoj komunikaciji, koja se temelji i na prethodnim inicijativama, naveden je skup predloženih mjera, uključujući, među ostalim, jačanje Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA), uspostavu dobrovoljnog okvira EU-a za kibersigurnosnu certifikaciju u cijelom EU-u u cilju povećanja kibersigurnosti proizvoda i usluga u digitalnom svijetu te plan za brz, koordinirani odgovor na opsežne kiberincidente i krize.

U zajedničkoj komunikaciji istaknuto je da je u strateškom interesu Unije osigurati da zadrži i razvije bitne tehnološke sposobnosti za kibersigurnost u cilju zaštite svojeg jedinstvenog digitalnog tržišta, a posebno u cilju zaštite ključnih mrežnih i informacijskih sustava i pružanja ključnih kibersigurnosnih usluga. Unija mora moći neovisno zaštititi svoju digitalnu imovinu i natjecati se na globalnom tržištu kibersigurnosti.

Ona je trenutačno neto uvoznik proizvoda i rješenja za kibersigurnost i u velikoj mjeri ovisi o pružateljima izvan Europe[4]. Tržište kibersigurnosti globalno je tržište vrijednosti 600 milijardi EUR za koje se očekuje da će se u sljedećih pet godina u prosjeku povećati za približno 17 % u pogledu prodaje, broja trgovačkih društava i zapošljavanja. Međutim, među vodećih 20 zemalja na tržištu kibersigurnosti nalazi se samo 6 država članica[5].

U Uniji istodobno postoji veliki broj stručnjaka i bogato iskustvo u području kibersigurnosti – više od 660 organizacija iz cijelog EU-a registriralo se za nedavno izrađeni pregled centara za

---

1 ZAJEDNIČKA KOMUNIKACIJA EUROPSKOM PARLAMENTU I VIJEĆU: Strategija Europske unije za kibersigurnost: otvoren, siguran i zaštićen kibernetički prostor, JOIN(2013) 1 final.

2 Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

3 ZAJEDNIČKA KOMUNIKACIJA EUROPSKOM PARLAMENTU I VIJEĆU Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a, JOIN(2017) 450 final

4 Nacrt Konačnog izvješća o istraživanju tržišta kibersigurnosti, 2018.

5 Nacrt Konačnog izvješća o istraživanju tržišta kibersigurnosti, 2018.

stručnost u području kibersigurnosti koje je provela Komisija[6]. Kada bi se to stručno znanje pretvorilo u proizvode i rješenja koji se mogu stavljati na tržište, Unija bi mogla pokriti čitavi vrijednosni lanac kibersigurnosti. Međutim, istraživanje i industrijske zajednice fragmentirani su, neusklađeni i nemaju zajedničku misiju, što otežava razvoj konkurentnosti EU-a u tom području i njegovu sposobnost da zaštiti svoju digitalnu imovinu. Relevantni sektori kibersigurnosti (npr. energetika, svemir, obrana, promet) i poddomene danas ne primaju dostatnu potporu[7]. U Europi se potpuno ne iskorištava ni sinergija između sektora civilne i obrambene kibersigurnosti.

Osnivanje javno-privatnog partnerstva za kibersigurnost („JPP za kibersigurnost”) u Uniji 2016. bilo je prvi čvrst korak prema okupljanju istraživačke zajednice, industrije i javnog sektora kako bi se olakšalo istraživanje i inovacije u području kibersigurnosti i to bi, unutar ograničenja financijskog okvira za razdoblje 2014.–2020., trebalo dovesti do dobrih, usmjerenijih rezultata u području istraživanja i inovacija. JPP za kibersigurnost omogućio je partnerima u industriji da se obvežu na pojedinačnu potrošnju u područjima definiranima u strateškom programu istraživanja i inovacija tog partnerstva.

Međutim, Unija može ulagati više i potreban joj je djelotvorniji mehanizam za izgradnju trajnih kapaciteta, objedinjavanje napora, sposobnosti i poticanje razvoja inovativnih rješenja koja su u skladu s industrijskim izazovima kibersigurnosti u području novih višenamjenskih tehnologija (npr. umjetna inteligencija, kvantno računalstvo, ulančani blokovi i sigurni digitalni identiteti) i u ključnim sektorima (npr. promet, energetika, zdravstvo, financije, uprava, telekomunikacije, proizvodnja, obrana, svemir).

U Zajedničkoj komunikaciji razmatrala se mogućnost jačanja sposobnosti Unije u području kibersigurnosti uspostavom mreže centara za stručnost u području kibersigurnosti koja će u središtu imati Europski centar za stručnost u području kibersigurnosti. Time bi se nastojali dopuniti postojeći napori jačanja kapaciteta u tom području na razini Unije i nacionalnoj razini. U Zajedničkoj komunikaciji spominje se namjera Komisije da 2018. pokrene procjenu učinka kako bi razmotrila dostupne mogućnosti u cilju uspostave strukture. Komisija je kao prvi korak i osnovu za daljnje promišljanje pokrenula pilot-fazu u okviru programa Obzor 2020. kako bi se olakšalo povezivanje nacionalnih centara u mrežu radi novog poticaja razvoju sposobnosti i tehnologije u području kibersigurnosti.

Šefovi država i vlada pozvali su Uniju na sastanku na vrhu o digitalnoj budućnosti u Tallinnu u rujnu 2017. da postane „globalna predvodnica u području kibersigurnosti do 2025. kako bismo osigurali povjerenje i zaštitu naših građana, potrošača i poduzeća na internetu te ostvarili slobodan i zakonom uređen internet.”

U Zaključcima Vijeća[8] iz studenoga 2017. Komisija je pozvana da brzo provede procjenu učinka dostupnih mogućnosti i do sredine 2018. predloži relevantni pravni instrument za provedbu inicijative.

Programom Digitalna Europa koji je Komisija predložila u lipnju 2018.[9] nastoje se povećati i što više iskoristiti digitalnu transformaciju za europske građane i poduzeća u svim

---

6 Tehnička izvješća Zajedničkog istraživačkog centra (JRC): Europski centri za stručnost u području kibersigurnosti, 2018.

7 Tehničko izvješće JRC-a: Rezultati mapiranja (detaljnije navedeni u prilozima 4. i 5.).

8 Zaključci Vijeća o Zajedničkoj komunikaciji Europskom parlamentu i Vijeću: Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a, koje je donijelo Vijeće za opće poslove 20. studenoga 2017.

relevantnim područjima politika EU-a, ojačati politike i poduprijeti ambicije jedinstvenog digitalnog tržišta. Programom se predlaže dosljedan i sveobuhvatan pristup osiguravanju najbolje uporabe naprednih tehnologija i odgovarajuće kombinacije tehničkih kapaciteta i ljudskih sposobnosti za digitalnu transformaciju, ne samo u području kibersigurnosti već i u pogledu infrastrukture pametnih podataka, umjetne inteligencije, naprednih vještina i primjena u industriji i područjima od javnog interesa. Ti elementi su međuovisni, uzajamno se podupiru i, uz istodobno poticanje, mogu se razviti do mjere koja je nužna za uspješno podatkovno gospodarstvo[10]. Kibersigurnost je obuhvaćena i prioritetima programa Obzor Europa[11], odnosno sljedeći okvirni program EU-a za istraživanje i razvoj.

U tom se kontekstu ovom Uredbom predlaže osnivanje europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja s Mrežom nacionalnih koordinacijskih centara. Da bi taj namjenski model suradnje potaknuo europski tehnološki i industrijski ekosustav, trebao bi djelovati na sljedeći način: Centar za stručnost olakšavat će i potpomagati koordinaciju rada Mreže, poticati Zajednicu stručnjaka za kibersigurnost i provedbu programa tehnološkog razvoja te olakšavati pristup tako prikupljenom znanju. Centar za stručnost će to prije svega činiti provedbom relevantnih dijelova programa Digitalna Europa i Obzor Europa dodjelom bespovratnih sredstava i obavljanjem nabave. S obzirom na znatna ulaganja u kibersigurnost drugdje u svijetu i potrebe za koordinacijom i udruživanjem financijskih sredstava u Europi, predlaže se da Centar za stručnost ima oblik europskog partnerstva[12] jer će se time olakšati zajednička ulaganja Unije, država članica i/ili industrije. Stoga se prijedlogom zahtijeva od država članica da djelovanju Mreže i Centra za stručnost pridonesu odgovarajućim iznosom. Glavno tijelo za donošenje odluka jest Upravni odbor, u kojem sudjeluju sve države članice, ali samo one države članice koje doprinose financijski imaju pravo glasa. Sustav glasovanja u Upravnom odboru u skladu je s načelom dvostruke većine kojim se zahtijeva 75 % financijskog doprinosa i 75 % glasova. S obzirom na njezinu odgovornost za proračun Unije, Komisija ima 50 % glasova. Za potrebe svojeg rada u Upravnom odboru Komisija će, kad god to bude moguće, tražiti stručno mišljenje Europske službe za vanjsko djelovanje. Upravnom odboru pomaže Industrijski i znanstveni savjetodavni odbor kako bi se osigurao redoviti dijalog s privatnim sektorom, organizacijama potrošača i drugim interesnim skupinama.

U bliskoj suradnji s Mrežom nacionalnih koordinacijskih centara i Zajednicom stručnjaka za kibersigurnost (u kojoj sudjeluje velika i raznolika grupa dionika koji su uključeni u razvoj tehnologije kibersigurnosti kao što su istraživački subjekti, industrije na strani ponude, industrije na strani potražnje i javni sektor) koji se osnivaju ovom Uredbom, Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja bio bi glavno provedbeno tijelo za financijska sredstva EU-a namijenjena za kibersigurnost u okviru predloženog programa Digitalna Europa i programa Obzor Europa.

Takvim sveobuhvatnim pristupom omogućilo bi se poticanje kibersigurnosti u cijelom vrijednosnom lancu, od istraživanja do podupiranja primjene i prihvaćanja ključnih

---

9 Prijedlog Uredbe Europskog parlamenta i Vijeća o uspostavi programa Digitalna Europa za razdoblje 2021.–2027., COM(2018) 434.

10 Vidjeti SWD(2018) 305.

11 Prijedlog Uredbe Europskog parlamenta i Vijeća o uspostavi Obzora Europa – Okvirnog programa za istraživanja i inovacije te o utvrđivanju pravila za sudjelovanje i širenje rezultata, COM(2018) 435.

12 Kako je definirano u Prijedlogu Uredbe Europskog parlamenta i Vijeća o uspostavi Obzora Europa – Okvirnog programa za istraživanja i inovacije te o utvrđivanju pravila za sudjelovanje i širenje rezultata, COM(2018) 435. kako je navedeno u Prijedlogu Uredbe Europskog parlamenta i Vijeća o uspostavi programa Digitalna Europa za razdoblje 2021.–2027., COM(2018) 434.

tehnologija. Financijski doprinosi država članica trebali bi biti razmjerni financijskom doprinosu EU-a ovoj inicijativi i neophodan su element njezina uspjeha.

Europsku organizaciju za kibersigurnost, koja je partner Komisije u ugovornom javno-privatnom partnerstvu za kibersigurnost u okviru programa Obzor 2020., trebalo bi, zbog njezina posebnog iskustva i široke i relevantne zastupljenosti dionika, pozvati da pridonese radu Centra i Mreže.

Nadalje, Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja trebao bi nastojati povećati sinergiju između civilne i obrambene dimenzije kibersigurnosti. On bi trebao podupirati države članice i druge relevantne zainteresirane strane davanjem savjeta, razmjenom stručnosti i olakšavanjem suradnje na projektima i mjerama. Na zahtjev država članica on bi trebao djelovati i u svojstvu voditelja projekta posebno u pogledu Europskog fonda za obranu. Ovom inicijativom želi se pridonijeti rješavanju sljedećih problema:

- **neučinkovite suradnje između industrija ponude i potražnje u području kibersigurnosti:** europska poduzeća suočavaju se s izazovom očuvanja svoje sigurnosti i potrebom da svojim klijentima ponude sigurne proizvode i usluge. Ona često ne mogu prikladno zaštititi svoje postojeće proizvode, usluge i imovinu ili osmisliti sigurne inovativne proizvode i usluge. Ključnu imovinu za kibersigurnost često je skupo razviti te je uspostavljaju pojedinačni sudionici na tržištu čija osnovna poslovna djelatnost nije povezana s kibersigurnošću. Istodobno nisu dostatno razvijene veze između ponude i potražnje na tržištu kibersigurnosti, što dovodi do nedostatne ponude europskih proizvoda i rješenja prilagođenih potrebama različitih sektora i do nepovjerenja među sudionicima na tržištu,
- **nepostojanja učinkovitog mehanizma suradnje među državama članicama za jačanje kapaciteta u industriji:** trenutačno ne postoji učinkovit mehanizam suradnje među državama članicama kako bi mogle zajedno raditi na jačanju potrebnih kapaciteta za podupiranje inovacija u području kibersigurnosti u različitim industrijskim sektorima i za primjenu najsuvremenijih rješenja za kibersigurnost u Europi. U okviru postojećih mehanizama suradnje među državama članicama u području kibersigurnosti u skladu s Direktivom (EU) 2016/1148 nisu predviđene takve aktivnosti,
- **nedostatne suradnje unutar istraživačke i industrijske zajednice te između njih:** unatoč teoretskoj sposobnosti Europe da pokrije cijeli vrijednosni lanac kibersigurnosti, istraživačka zajednica danas slabo podupire relevantne sektore kibersigurnosti (npr. energetika, svemir, obrana, promet) i njihove poddomene ili ih podupire samo ograničen broj centara (npr. postkvantna i kvantna kriptografija, povjerenje i kibersigurnost u umjetnoj inteligenciji). Iako ta suradnja nedvojbeno postoji, često su to kratkoročni aranžmani koji se temelje na savjetodavnim uslugama i ne omogućuju dugoročno planiranje istraživanja za rješavanje industrijskih izazova u području kibersigurnosti,
- **nedostatne suradnje između civilnih i obrambenih zajednica za istraživanje i inovacije u području kibersigurnosti:** problem nedostatne suradnje odnosi se i na civilne i obrambene zajednice. Postojeća sinergija ne iskorištava se u potpunosti jer ne postoje učinkoviti mehanizmi koji bi omogućili učinkovitu suradnju tih zajednica i izgradnju povjerenja, što je, čak i više nego u drugim područjima, preduvjet za uspješnu suradnju. To pogoršavaju ograničene financijske sposobnosti na tržištu kibersigurnosti EU-a, uključujući nedostatna sredstva za podupiranje inovacija.
- **Dosljednost s postojećim odredbama politike u određenom području**

Mreža centara za stručnost u području kibersigurnosti i Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja dodatno će podupirati postojeće odredbe politike kibersigurnosti i zainteresirane strane u tom području. Mandat Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja dopunjavat će napore ENISA-e, ali ima drugačije usmjerenje i zahtijeva različiti skup vještina. Dok mandat ENISA-e predviđa savjetodavnu ulogu u okviru istraživanja i inovacija u području kibersigurnosti u EU-u, njezin predloženi mandat usredotočen je u prvom redu na druge zadaće koje su od ključne važnosti za jačanje kiberotpornosti u EU-u. Nadalje, mandat ENISA-e ne predviđa vrste aktivnosti koje bi bile osnovne zadaće Centra i Mreže, odnosno poticanje razvoja i primjene tehnologije kibersigurnosti i dopunjavanje napora jačanja kapaciteta u tom području na razini EU-a i nacionalnoj razini.

Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreža centara za stručnost u području kibersigurnosti podupirat će i istraživanja usmjerena na olakšavanje i ubrzavanje postupaka standardizacije i certifikacije, posebno onih povezanih s programima kibersigurnosne certifikacije u smislu predloženog Akta o kibersigurnosti[13][14].

Ovom inicijativom zapravo se nadograđuje javno-privatno partnerstvo za kibersigurnost (JPP za kibersigurnost), koje je bilo prvi pokušaj povezivanja industrije kibersigurnosti u cijelom EU-u, strane ponude (kupci proizvoda i rješenja za kibersigurnost, uključujući javnu upravu i ključne sektore kao što su promet, zdravstvo, energetika, financijske usluge) i istraživačke zajednice u cilju izgradnje platforme održivog dijaloga i stvaranja uvjeta za dobrovoljna zajednička ulaganja. JPP za kibersigurnost stvoren je 2016. i potaknuo je približno 1,8 milijardi EUR ulaganja do 2020. Međutim, količina ulaganja u drugim dijelovima svijeta (npr. SAD je samo 2017. uložio 19 milijardi dolara u kibersigurnost) pokazuje da EU mora više raditi kako bi postigao kritičnu masu ulaganja i prevladao fragmentiranost sposobnosti raširenih po cijelom EU-u.

- **Dosljednost u odnosu na druge politike Unije**

Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja djelovat će kao jedinstveno provedbeno tijelo za različite programe Unije kojima se podupire kibersigurnost (program Digitalna Europa i Obzor Europa) te će jačati dosljednosti i sinergije među njima.

Ovom inicijativom nadopunit će se rad država članica pružanjem odgovarajućeg doprinosa donositeljima politika u cilju jačanja vještina za kibersigurnost (npr. razvijanjem kurikuluma za kibersigurnost u civilnim i vojnim obrazovnim sustavima) kako bi se pridonijelo razvoju kvalificirane radne snage EU-a za kibersigurnost – ključne vrijednosti za trgovačka društva specijalizirana za kibersigurnost i druge industrije kojima je kibersigurnost važna. Kad je riječ o obrazovanju i osposobljavanju u području kibersigurnosti, ova će inicijativa biti dosljedna s dosadašnjim radom platforme za obrazovanje, osposobljavanje, osposobljavanje i vježbe osnovane u okviru Europske akademije za sigurnost i obranu.

---

13 Prijedlog Uredbe Europskog parlamenta i Vijeća o ENISA-i (agenciji EU-a za kibersigurnost) i stavljanju izvan snage Uredbe (EU) 526/2013 te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije („Akt o kibersigurnosti”, COM(2017) 477 final/3).

14 Ovime se ne dovode u pitanje certifikacijski mehanizmi u okviru Opće uredbe o zaštiti podataka u kojoj sudjeluju tijela za zaštitu podataka, u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ („Opća uredba o zaštiti podataka”).

Ovom inicijativom dopunjivat će se i podupirati napori digitalnoinovacijskih centara u okviru programa Digitalna Europa. Digitalnoinovacijski centri neprofitne su organizacije koje pomažu trgovačkim društvima, posebno novoosnovanim poduzećima, MSP-ovima i poduzećima srednje tržišne kapitalizacije, poboljšanjem njihovih postupaka poslovanja/proizvodnje te proizvoda i usluga pametnom inovacijom koju omogućuje digitalna tehnologija. Digitalnoinovacijski centri pružaju poslovno-inovacijske usluge, kao što su tržišna inteligencija, financijski savjeti, pristup relevantnim objektima za testiranje i eksperimentiranje, osposobljavanje i razvoj vještina, u cilju uspješnog uvođenja novih proizvoda ili usluga na tržište ili uvođenja boljih proizvodnih postupaka. Neki digitalnoinovacijski centri, koji su posebno stručni za kibersigurnost, mogli bi neposredno sudjelovati u Zajednici stručnjaka za kibersigurnost koja se osniva ovom inicijativom. Međutim, u većini slučajeva digitalnoinovacijski centri, koji nemaju posebni kibersigurnosni profil, olakšali bi svojim članovima pristup stručnom znanju o kibersigurnosti i znanju i sposobnostima dostupnima u Zajednici stručnjaka za kibersigurnost bliskom suradnjom s mrežom nacionalnih koordinacijskih centara i Europskim centrom za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja. Digitalnoinovacijski centri podupirali bi i uvođenje inovativnih proizvoda i rješenja za kibersigurnost u skladu s potrebama poduzeća i drugih krajnjih korisnika kojima pružaju usluge. I konačno, sektorski specifični digitalnoinovacijski centri mogli bi dijeliti svoje znanje o stvarnim potrebama u sektoru s Mrežom i Centrom kako bi pridonijeli razmišljanjima o programu istraživanja i inovacija koji odgovara industrijskim zahtjevima.

Tražit će se sinergija s relevantnim zajednicama znanja i inovacija Europskog instituta za inovacije i tehnologiju te posebno s centrima EIT Digital.

2. PRAVNA OSNOVA, SUPSIDIJARNOST I PROPORCIONALNOST

• Pravna osnova

Centar za stručnost trebalo bi osnovati na temelju dvostruke pravne osnove zbog njegove prirode i posebnih ciljeva. Člankom 187. UFEU-a, kojim se uspostavljaju strukture potrebne za učinkovitu provedbu istraživačkih, tehnološko-razvojnih i demonstracijskih programa Unije, dopušta se Centru za stručnost da stvara sinergije i udružuje sredstva za ulaganje u nužne kapacitete na razini država članica te da razvija zajedničku europsku imovinu (npr. zajedničkom nabavom potrebne infrastrukture za testiranje i eksperimentiranje u području kibersigurnosti) U članku 188. stavku 1. predviđeno je donošenje takvih mjera. Međutim, ako bi se kao isključiva pravna osnova uzeo članak 188. prvi podstavak, ne bi bile moguće aktivnosti izvan istraživanja i razvoja koje su potrebne za ostvarenje ciljeva Centra za stručnost utvrđenih u ovoj Uredbi kojima se podupire uvođenje na tržište proizvoda i rješenja za kibersigurnost, pomaže europskoj industriji kibersigurnosti da postane konkurentnija i poveća tržišni udio i dodaje vrijednost nacionalnim naporima za uklanjanje manjka vještina u području kibersigurnosti. Stoga je, da bi se mogli postići ti ciljevi, nužno kao pravnu osnovu dodati članak 173. stavak 3. kojim se Uniji dopušta da predvidi mjere za podupiranje konkurentnosti industrije.

• Opravdanje prijedloga u odnosu na načela supsidijarnosti i proporcionalnosti

Kibersigurnost je pitanje od zajedničkog interesa za Uniju, što je potvrđeno u prethodno navedenim Zaključcima Vijeća. To je pokazao opseg i prekogranični karakter incidenata kao što su *WannaCry* ili *NonPetya*. Zbog prirode i opsega kibersigurnosnih tehnoloških izazova i nedostatne koordinacije napora unutar industrije i među industrijama, javni sektor i istraživačke zajednice traže od EU-a da dodatno podupire koordinacijske napore u cilju

udruživanja kritične mase sredstava i osiguranja boljeg znanja i upravljanja imovinom. To je potrebno zbog zahtjeva za sredstvima povezanima s određenim sposobnostima za istraživanje, razvoj i primjenu u području kibersigurnosti, potrebe za pružanjem pristupa interdisciplinarnom znanju i iskustvu o kibersigurnosti u različitim disciplinama (koje je često samo djelomično dostupno na nacionalnoj razini), globalne prirode industrijskih vrijednosnih lanaca i aktivnosti globalnih konkurenata koji djeluju na različitim tržištima.

Za to su potrebna sredstva i stručno znanje koji se ne mogu ostvariti pojedinačnim djelovanjem pojedinih država članica. Na primjer, za paneuropsku kvantnu komunikacijsku mrežu mogla bi biti potrebna ulaganja EU-a od približno 900 milijuna EUR, ovisno o ulaganjima država članica (koje treba međusobno povezati/dopuniti) te o mjeri u kojoj će tehnologija omogućiti ponovnu uporabu postojećih infrastruktura. Inicijativa će biti od ključne važnosti za udruživanje financijskih sredstava i omogućivanje takve vrste ulaganja u Uniji.

Države članice ne mogu samostalno ostvariti ciljeve ove inicijative. Kako je prethodno navedeno, oni se mogu bolje ostvariti na razini Unije zajedničkim naporima i izbjegavanjem nepotrebnog ponavljanja, pomaganjem u postizanju kritične mase ulaganja i osiguravanjem optimalne uporabe javnih sredstava. Istodobno, u skladu s načelom proporcionalnosti, ova Uredba ne prelazi ono što je potrebno za postizanje to cilja. Djelovanje EU-a stoga je opravdano na temelju supsidijarnosti i proporcionalnosti.

Ovim instrumentom ne predviđaju se nove regulatorne obveze za poduzeća. Istodobno, vjerojatno će se smanjiti troškovi poduzeća i MSP-ova koje ulažu u osmišljavanje inovativnih kibersigurnih proizvoda jer se inicijativom omogućuje udruživanje sredstava za ulaganja u potrebne kapacitete na razini država članica ili za razvoj zajedničke europske imovine (npr. zajedničkom nabavom potrebne infrastrukture za testiranje i eksperimentiranje u području kibersigurnosti). Tu imovinu mogle bi upotrebljavati industrije i MSP-ovi u različitim sektorima kako bi se osiguralo da su njihovi proizvodi kibersigurni i kako bi kibersigurnost pretvorili u svoju konkurentnu prednost.

- **Odabir instrumenta**

Predloženim instrumentom osniva se tijelo za provedbu mjera kibersigurnosti u okviru Programa Digitalna Europa i programa Obzor Europa. U njemu se opisuju njegov mandat, zadaće i upravljačka struktura. Da bi Unija mogla osnovati takvo tijelo, mora se donijeti Uredba.

3. SAVJETOVANJA S DIONICIMA I PROCJENE UČINAKA

Prijedlog o stvaranju Mreže za stručnost u području kibersigurnosti s Europskim centrom za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja nova je inicijativa. Ona je nastavak i nadogradnja ugovornog javno-privatnog partnerstva o kibersigurnosti uspostavljenog 2016.

- **Savjetovanja s dionicima**

Kibersigurnost je široka, međusektorska tema. Komisija je upotrebljavala različite načine savjetovanja kako bi osigurala da se u ovoj inicijativi uzme u obzir opći javni interes Unije umjesto posebnih interesa malog broja skupina dionika. Na taj način osigurava se transparentnost i odgovornost u radu Komisije. Iako zbog ciljne publike (industrijska i istraživačka zajednica i države članice) nije organizirano posebno javno savjetovanje za ovu inicijativu, tema je već bila pokrivena u nekoliko drugih otvorenih javnih savjetovanja:

- općem otvorenom javnom savjetovanju koje je provedeno 2018. na temu ulaganja, istraživanja i inovacija, MSP-ova i jedinstvenog tržišta,
- dvanaestotjednom javnom savjetovanju na internetu koje je pokrenuto 2017. radi prikupljanja stajališta šire publike (približno 90 sudionika) o evaluaciji i preispitivanju ENISA-e,
- dvanaestotjednom javnom savjetovanju koje je provedeno 2016. povodom pokretanja ugovornog javno-privatnog partnerstva o kibersigurnosti (približno 240 sudionika).

Komisija je organizirala i ciljna savjetovanja o ovoj inicijativi, uključujući radionice, sastanke i ciljane zahtjeve za doprinose (od ENISA-e i Europske obrambene agencije). Razdoblje savjetovanja trajalo je više od 6 mjeseci od studenoga 2017. do ožujka 2018. Komisija je izradila i pregled centara stručnosti i na temelju toga prikupila doprinose 665 centara stručnosti u području kibersigurnosti o njihovu znanju i iskustvu, aktivnostima, područjima rada i međunarodnoj suradnji. Anketa je pokrenuta u siječnju i u analizi u izvješću uzeti su u obzir odgovori dostavljeni do 8. ožujka 2018.

Dionici iz industrijske i istraživačke zajednice smatrali su da bi Centar za stručnost i Mreža mogli dodati vrijednost trenutačnim naporima na nacionalnoj razini jer bi pomogli u stvaranju europskog ekosustava kibersigurnosti koji bi omogućio bolju suradnju između istraživačke i industrijske zajednice. Smatrali su nužnim i da EU i države članice prihvate proaktivnu, dugoročniju i stratešku perspektivu industrijske politike o kibersigurnosti koja ne uključuje samo istraživanje i inovacije. Dionici su izrazili potrebu za ostvarenjem pristupa ključnim kapacitetima kao što su objekti za testiranje i eksperimentiranje i za ambicioznijim radom na zatvaranju manjka vještina u području kibersigurnosti, primjerice opsežnim europskim projektima za prikupljanje najboljih kandidata. Sve prethodno navedeno smatralo se nužnim da bi se Unija mogla smatrati globalnom predvodnicom u području kibersigurnosti.

Države članice u okviru aktivnosti savjetovanja koje se provode od prošlog rujna[15] i u Zaključcima Vijeća[16] pozdravile su namjeru osnivanja Mreže za stručnost u području kibersigurnosti u cilju poticanja razvoja i primjene tehnologija kibersigurnosti, ističući potrebu za uključivanjem svih država članica i njihovih postojećih centara izvrsnosti i stručnosti te za posvećivanjem posebne pozornosti komplementarnosti. Države članice su, posebno u pogledu budućeg Centra za stručnost, istaknule važnost njegove koordinacijske uloge u podupiranju rada Mreže. Kad je riječ o nacionalnim aktivnostima i potrebama u kiberobrani, mapiranje potreba država članica u području kiberobrane koje je Europska služba za vanjsko djelovanje provela u ožujku 2018. pokazalo je da većina država članica uočava dodanu vrijednost potpore EU-a obrazovanju i osposobljavanju u području kibernetike te u pružanju potpore industriji u okviru istraživanja i razvoja[17]. Inicijativa bi se provodila zajedno s državama članicama ili subjektima koje one podupiru. Suradnjom između industrijske i istraživačke zajednice i/ili zajednica javnog sektora približili bi se i ojačali postojeći subjekti i pojačali napori da se ne stvaraju novi. Države članice sudjelovale bi i u oblikovanju posebnih mjera za javni sektor kao izravni korisnik tehnologije kibersigurnosti i znanja i iskustva u tome području.

---

15 Npr. okrugli stol na visokoj razini s državama članicama, potpredsjednik Ansip, povjerenica Gabriel, 5. prosinca 2017.

16 Vijeće za opće poslove: Zaključci Vijeća o Zajedničkoj komunikaciji Europskom parlamentu i Vijeću: Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a od 20. studenoga 2017.

17 ESVD, ožujak 2018.

- **Procjena učinka**

Procjena učinka kojom se podupire ova inicijativa podnesena je Oboru za nadzor regulative 11. travnja 2017. i dobila je pozitivno mišljenje sa zadrškama. Procjena učinka potom je revidirana u skladu s primjedbama Odbora. S ovim se prijedlogom objavljuju mišljenje Odbora i Prilog, u kojem se objašnjava kako se razmatraju komentari Odbora.

U Procjeni učinka razmatrale su se različite mogućnosti politike, zakonodavne i nezakonodavne. Sljedeće mogućnosti zadržane su radi podrobnije procjene:

- osnovni scenarij – suradnička mogućnost – pretpostavlja nastavak trenutačnog pristupa izgradnji industrijskih i tehnoloških kapaciteta u području kibersigurnosti u EU-u podupiranjem istraživanja i inovacija i povezanih mehanizama suradnje u okviru Devetog okvirnog programa,
- prva mogućnost: Mreža za stručnost u području kibersigurnosti s Europskim centrom za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja koji imaju dvostruki mandat provedbe mjera za podupiranje industrijskih tehnologija i u području istraživanja i inovacija,
- druga mogućnost: Mreža za stručnost u području kibersigurnosti s Europskim centrom za istraživanje i stručnost u području kibersigurnosti usmjereni na aktivnosti istraživanja i inovacija.

U ranoj fazi odbačene su sljedeće mogućnosti: 1. nedjelovanje, 2. mogućnost stvaranja samo mreže za stručnost u području kibersigurnosti, 3. mogućnost stvaranja samo centralizirane strukture i 4. mogućnost uporabe postojeće agencije (Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA), Izvršne agencije za istraživanje (REA) ili Izvršne agencije za inovacije i mreže (INEA).

Nakon provedene analize donesen je zaključak da je prva mogućnost najprikladnija za ostvarenje ciljeva inicijative te da se njome istodobno ostvaruje najveći gospodarski, društveni i okolišni učinak i zaštita interesa Unije. Glavni argumenti u korist te mogućnosti uključivali su mogućnost stvaranja stvarne industrijske politike kibersigurnosti podupiranjem aktivnosti koje nisu povezane samo s istraživanjem i razvojem već i s razvojem tržišta, fleksibilnost omogućivanja različitih modela suradnje s mrežom centara za stručnost kako bi se najbolje moglo iskoristiti postojeće znanje i sredstva, mogućnost strukturiranja suradnje i zajedničkih obveza javnih i privatnih dionika iz svih relevantnih sektora, među ostalim obrane. Naposljetku, prva mogućnost omogućuje i povećanje sinergija i može djelovati kao provedbeni mehanizam za dva različita izvora financiranja kibersigurnosti u EU-u u okviru sljedećeg višegodišnjeg financijskog okvira (program Digitalna Europa i Obzor Europa).

- **Temeljna prava**

Ovom inicijativom omogućit će se tijelima javne vlasti i industrijama u svim državama članicama da učinkovitije sprečavaju kiberprijetnje i odgovaraju na njih tako da mogu ponuditi više sigurnih proizvoda i rješenja te se opremiti takvim proizvodima i rješenjima. To je posebno važno za zaštitu pristupa osnovnim uslugama (npr. promet, zdravstvo, bankarstvo i financijske usluge).

Veća sposobnost Europske unije da neovisno osigura svoje proizvode i usluge također će vjerojatno pomoći građanima da uživaju svoja demokratska prava i vrijednosti (npr. da bolje zaštite svoja prava povezana s informacijama utjelovljena u Povelji o temeljnim pravima,

posebno pravo na zaštitu osobnih podataka i privatni život) te da posljedično povećaju svoje povjerenje u digitalno društvo i gospodarstvo.

4. UTJECAJ NA PRORAČUN

Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja, u suradnji s Mrežom centara za stručnost u području kibersigurnosti, bit će glavno provedbeno tijelo za financijska sredstva EU-a namijenjena za kibersigurnost u okviru programa Digitalna Europa i Obzor Europa.

Utjecaj na proračun provedbe programa Digitalna Europa detaljno je opisan u Zakonodavnom financijskom izvještaju koji je priložen ovom prijedlogu. Doprinos iz financijske omotnice za klaster „Uključivo i sigurno društvo" stupa II. „Globalni izazovi i industrijska konkurentnost" programa Obzor Europa (ukupna omotnica od 2 800 000 000 EUR) iz članka 21. stavka 1. točke (b) predložit će Komisija tijekom zakonodavnog postupka, a u svakom slučaju prije postizanja političkog dogovora. Prijedlog će se temeljiti na rezultatima postupka strateškog planiranja kako je definirano u članku 6. stavku 6. Uredbe XXX [okvirni program Obzor Europa].

5. OSTALI DIJELOVI

- **Planovi provedbe i mehanizmi praćenja, evaluacije i izvješćivanja**

U ovom prijedlogu predviđena je izričita odredba o evaluaciji na temelju koje će Komisija provesti neovisnu evaluaciju (članak 38.). Komisija će Europskom parlamentu i Vijeću dostaviti izvješće o svojoj evaluaciji prema potrebi popraćeno prijedlogom za reviziju, u cilju mjerenja učinka Uredbe i njezine dodane vrijednosti. Komisija će tijekom evaluacije primjenjivati svoju metodologiju bolje regulative.

Izvršni direktor trebao bi Upravnom odboru svake dvije godine dostaviti *ex post* evaluaciju rada Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže kako je utvrđeno u članku 17. ovog prijedloga. Izvršni direktor trebao bi izraditi i akcijski plan na temelju zaključaka naknadnih evaluacija i svake dvije godine Komisiju izvješćivati o napretku. Upravni odbor trebao bi biti odgovoran za praćenje provedbe daljnjih mjera na temelju tih zaključaka, kako je navedeno u članku 16. ovog prijedloga.

Navodne nepravilnosti u radu pravne osobe može istraživati Europski ombudsman u skladu s odredbama članka 228. Ugovora.

2018/0328 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara

Doprinos Europske Komisije za sastanak čelnika u Salzburgu 19.–20. rujna 2018.

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 173. stavak 3. i prvi stavak članka 188.,

uzimajući u obzir prijedlog Europske komisije,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora[18],

uzimajući u obzir mišljenje Odbora regija[19],

u skladu s redovnim zakonodavnim postupkom,

budući da:

(1) Naš svakodnevni život i naša gospodarstva sve više ovise o digitalnim tehnologijama zbog čega su građani sve izloženiji ozbiljnim kiberincidentima. Naša sigurnost u budućnosti ovisi, među ostalim, o jačanju tehnološke i industrijske sposobnosti za zaštitu Unije od kiberprijetnji jer se civilna infrastruktura i vojni kapaciteti oslanjaju na sigurne digitalne sustave.

(2) Unija je nakon donošenja Strategije za kibersigurnost iz 2013.[20] stalno povećavala svoje aktivnosti suočavanja sa sve većim izazovima u području kibersigurnosti u cilju poticanja pouzdanog, sigurnog i otvorenog kiberekosustava. Unija je 2016. donijela prve mjere u području kibersigurnosti donošenjem Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća[21] o sigurnosti mrežnih i informacijskih sustava.

(3) U rujnu 2017. Komisija i Visoka predstavnica Unije za vanjske poslove i sigurnosnu politiku predstavili su Zajedničku komunikaciju[22] „Otpornost, odvraćanje i obrana:

---

18 SL C , str. .

19 SL C , , str...

20 Zajednička Komunikacija Europskom parlamentu i Vijeću: Strategija Europske unije za kibersigurnost: otvoren, siguran i zaštićen kibernetički prostor, JOIN(2013) 1 final.

21 Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

22 Zajednička komunikacija Europskom parlamentu i Vijeću: Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a, JOIN(2017) 450 final.

jačanje kibersigurnosti EU-a” u cilju daljnjeg jačanja otpornosti Unije, odvraćanja od i njezina odgovora na kibernapade.

(4) Šefovi država i vlada pozvali su Uniju na sastanku na vrhu o digitalnoj budućnosti u Tallinnu u rujnu 2017. da postane „globalna predvodnica u području kibersigurnosti do 2025. kako bismo osigurali povjerenje i zaštitu naših građana, potrošača i poduzeća na internetu te ostvarili slobodan i zakonom uređen internet.”

(5) Znatan poremećaj u radu mrežnih i informacijskih sustava može utjecati na pojedine države članice i cijelu Uniju. Stoga je sigurnost mrežnih i informacijskih sustava ključna za neometano funkcioniranje unutarnjeg tržišta. Unija trenutačno ovisi o pružanjima usluga kibersigurnosti izvan Europe. Međutim, u strateškom je interesu Unije osigurati da zadrži i razvije bitne tehnološke sposobnosti u području kibersigurnosti u cilju zaštite svojeg jedinstvenog digitalnog tržišta, a posebno kako bi zaštitila ključne mrežne i informacijske sustave i pružila ključne kibersigurnosne usluge.

(6) U Uniji postoji bogato stručno znanje i iskustvo u području istraživanja, tehnologije i industrijskog razvoja u području kibersigurnosti, ali istraživačke zajednice su fragmentirane, neusklađene i nedostaje im zajednička misija, što sprečava razvoj konkurentnosti u tom području. Potrebno je udružiti i umrežiti te napore i stručno znanje te ih učinkovito upotrijebiti za jačanje i nadopunu postojećih sposobnosti u području istraživanja, tehnologije i industrije na razini Unije i na nacionalnim razinama.

(7) U Zaključcima Vijeća koji su doneseni u studenome 2017. Komisija je pozvana da brzo provede procjenu učinka dostupnih mogućnosti za stvaranje mreže centara za stručnost u području kibersigurnosti i Europskog centra za istraživanje i stručnost te da do sredine 2018. predloži relevantni pravni instrument.

(8) Centar za stručnost trebao bi biti glavni instrument Unije za udruživanje ulaganja u istraživanje, tehnologiju i industrijski razvoj u području kibersigurnosti i za provedbu relevantnih projekata i inicijativa zajedno s Mrežom centara za stručnost u području kibersigurnosti. Oni bi trebao ostvarivati financijsku potporu za kibersigurnost iz programa Obzor Europa i Digitalna Europa i prema potrebi bi trebao biti otvoren prema Europskom fondu za regionalni razvoj i drugim programima. Ovaj pristup trebao bi pridonijeti stvaranju sinergija i koordiniranju financijske potpore za istraživanje, inovacije, tehnologiju i industrijski razvoj u području kibersigurnosti i izbjegavanju dvostrukog financiranja.

(9) Budući da se ciljevi ove inicijative najbolje mogu postići sudjelovanjem svih država članica ili njihova što većeg broja, te kako bi se države članice potaknule na sudjelovanje, pravo glasa trebale bi imati samo države članice koje financijski pridonose administrativnim troškovima i troškovima poslovanja Centra za stručnost.

(10) Financijski doprinos država članica sudionica trebao bi biti razmjeran financijskom doprinosu Unije ovoj inicijativi.

(11) Centar za stručnost trebao bi olakšati rad Mreže centara za stručnost u području kibersigurnosti („Mreža”), koja je sastavljena od nacionalnih koordinacijskih centara svake države članice, i pridonijeti njezinu radu. Nacionalni koordinacijski centri trebali bi primati izravnu financijsku potporu Unije, uključujući bespovratna sredstva koja se dodjeljuju bez poziva na podnošenje prijedloga, u cilju obavljanja aktivnosti povezanih s ovom Uredbom.

(12) Nacionalne koordinacijske centre trebale bi odabrati države članice. Povrh potrebne administrativne sposobnosti Centri bi trebali imati tehnološke stručnjake za područje kibersigurnosti ili imati pristup takvim stručnjacima, posebno u područjima šifriranja, sigurnosnih usluga IKT-a, otkrivanja neovlaštenih pristupa, sigurnosti sustava, mrežne sigurnosti, sigurnosti softvera i aplikacija ili ljudskih i društvenih aspekata sigurnosti i privatnosti. Trebali bi biti sposobni djelotvorno surađivati i koordinirati aktivnosti s industrijom, javnim sektorom, uključujući tijela određena na temelju Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća[23], te istraživačkom zajednicom.

(13) Ako se nacionalnim koordinacijskim centrima pruža financijska potpora za podupiranje trećih strana na nacionalnoj razini, ona se prenosi na relevantne dionike na temelju kaskadnih ugovora o dodjeli bespovratnih sredstava.

(14) Nove tehnologije, kao što su umjetna inteligencija, internet stvari, računalstvo visokih performansi (HPC) i kvantno računalstvo, ulančani blokovi i pojmovi kao što su sigurni digitalni identiteti istodobno donose nove izazove i rješenja za kibersigurnost. Kako bi se mogla ocijeniti i provjeriti pouzdanost postojećih ili budućih sustava IKT-a, bit će potrebna rješenja za testiranje sigurnosti protiv napada na HPC i kvantne strojeve. Centar za stručnost, Mreža i Zajednica stručnjaka za kibersigurnost trebali bi pomoći u razvoju i širenju najnovijih rješenja za kibersigurnost. Centar za stručnost i Mreža trebali bi istodobno biti na raspolaganju developerima i operaterima u ključnim sektorima kao što su promet, energija, zdravstvo, financije, uprava, telekomunikacije, proizvodnja, obrana i svemir kako bi im pomogli u rješavanju problema u području kibersigurnosti.

(15) Centar za stručnost trebao bi imati nekoliko ključnih zadaća. Prvo, Centar za stručnost trebao bi olakšavati rad Europske mreže centara za stručnost u području kibersigurnosti i koordinirati ga te njegovati Zajednicu stručnjaka za kibersigurnost. Centar bi trebao poticati provedbu programa tehnološkog razvoja u području sigurnosti i olakšavati pristup stručnjacima okupljenima u Mreži i Zajednici stručnjaka za kibersigurnost. Drugo, trebao bi provoditi relevantne dijelove programa Digitalna Europa i Obzor Europa dodjelom bespovratnih sredstava, u načelu nakon natječajnog postupka na temelju poziva na podnošenje prijedloga. Treće, Centar za stručnost trebao bi olakšavati zajednička ulaganja Unije, država članica i/ili industrije.

(16) Centar za stručnost trebao bi poticati i podupirati suradnju i koordinaciju aktivnosti Zajednice stručnjaka za kibersigurnost, koja bi uključivala veliku, otvorenu i raznoliku skupinu dionika u području kibersigurnosne tehnologije. Ta Zajednica posebno bi trebala uključivati istraživačka tijela, industrije na strani ponude, industrije na strani potražnje i javni sektor. Zajednica stručnjaka za kibersigurnost trebala bi pridonijeti aktivnostima i planu rada Centra za stručnost i sudjelovati u aktivnostima jačanja zajedništva Centra za stručnost i Mreže, ali inače ne bi trebala imati prednost kod poziva na podnošenje prijedloga ili natječaja.

(17) Kako bi se mogle zadovoljiti potrebe industrija na strani ponude i potražnje, zadaća Centra za stručnost koja se odnosi na pružanje industrijama znanja i tehničke pomoći u području kibersigurnosti trebala bi se odnositi na proizvode i usluge IKT-a i sve druge industrijske i tehnološke proizvode i rješenja u koja treba ugraditi kibersigurnost.

[23] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

(18) Budući da bi Centar za stručnost i Mreža trebali nastojati postići sinergije između kibersigurnosti u civilnom i obrambenom sektoru, projekti koji se financiraju iz programa Obzor Europa provodit će se u skladu s Uredbom XXX [Uredba o Obzoru Europa], u kojoj je predviđeno da su aktivnosti istraživanja i inovacija koje se provode u okviru Obzora Europa usmjerene su na primjenu u civilnom području.

(19) Kako bi se osigurala strukturirana i održiva suradnja, odnos između Centra za stručnost i nacionalnih koordinacijskih centara trebao bi se zasnivati na ugovoru.

(20) Odgovarajućim odredbama trebalo bi jamčiti odgovornost i transparentnost Centra za stručnost.

(21) Uzimajući u obzir njihovu stručnost u području kibersigurnosti, Zajednički istraživački centar Komisije i Europska agencija za mrežnu i informacijsku sigurnost (ENISA) trebali bi imati aktivnu ulogu u Zajednici stručnjaka za kibersigurnost i u Industrijskom i znanstvenom savjetodavnom odboru.

(22) Ako dobiju financijski doprinos iz općeg proračuna Unije, nacionalni koordinacijski centri i subjekti koji su dio Zajednice stručnjaka za kibersigurnost trebali bi objaviti činjenicu da se predmetne aktivnosti provode u kontekstu ove inicijative.

(23) Doprinosom Unije Centru za stručnost trebalo bi se financirati pola troškova osnivanja i administrativnih i koordinacijskih aktivnosti Centra za stručnost. Kako bi se izbjeglo dvostruko financiranje, te aktivnosti ne bi se trebale istodobno financirati iz drugih programa Unije.

(24) Upravni odbor Centra za stručnost sastavljen od država članica i Komisije trebao bi definirati opće usmjerenje rada Centra za stručnost i osigurati da on obavlja svoje zadaće u skladu s ovom Uredbom. Upravnom odboru trebalo bi povjeriti ovlasti potrebne za izradu proračuna, provjeru njegova izvršenja, donošenje odgovarajućih financijskih pravila, uspostavu transparentnih radnih postupaka za donošenje odluka Centra za stručnost, donošenje plana rada Centra i višegodišnjeg strateškog plana u skladu s prioritetima u postizanju ciljeva i izvršavanju zadaća Centra za stručnost, donošenje poslovnika, imenovanje izvršnog direktora i odlučivanje o produljenju ili prestanku mandata izvršnog direktora.

(25) Kako bi Centar za stručnost mogao pravilno i djelotvorno funkcionirati, Komisija i države članice trebale bi osigurati da osobe koje će imenovati u Upravni odbor imaju odgovarajuća stručna znanja i iskustvo u područjima njegova djelovanja. Komisija i države članice također bi trebale ograničiti učestalost izmjena njihovih predstavnika u Upravnom odboru kako bi se osigurao kontinuitet njihova rada.

(26) Kako bi se osiguralo nesmetano funkcioniranje Centra za stručnost, njegov izvršni direktor imenuje se na temelju zasluga i dokazanih administrativnih i rukovoditeljskih sposobnosti, kao i sposobnosti i iskustava relevantnih za kibersigurnost, a svoje dužnosti obavlja potpuno neovisno.

(27) Centar za stručnost trebao bi imati Industrijski i znanstveni savjetodavni odbor kao savjetodavno tijelo kako bi se osigurao redoviti dijalog s privatnim sektorom, organizacijama potrošača i drugim interesnim skupinama. Industrijski i znanstveni savjetodavni odbor trebao bi se usredotočiti na pitanja koja su važna za dionike i s njima upoznati Upravni odbor Centra za stručnost. Sastavom Industrijskog i znanstvenog savjetodavnog odbora i njegovim zadaćama, kao što je savjetovanje o planu rada, trebalo bi osigurati dostatnu zastupljenost dionika u radu Centra za stručnost.

(28) Centar za stručnost trebao bi u okviru svojeg Industrijskog i znanstvenog savjetodavnog odbora iskoristiti posebno stručno znanje i široku i relevantnu zastupljenost dionika stvorenu ugovornim javno-privatnim partnerstvom za kibersigurnost tijekom trajanja Obzora 2020.

(29) Centar za stručnost trebao bi uspostaviti pravila o sprečavanju sukoba interesa i upravljanju njime. Centar za stručnost trebao bi primjenjivati mjerodavne odredbe Unije o javnom pristupu dokumentima u skladu s Uredbom (EZ) br. 1049/2001 Europskog parlamenta i Vijeća[24]. Centar za stručnost obrađuje osobne podatke u skladu s Uredbom (EU) br. XXX/2018 Europskog parlamenta i Vijeća. Centar za stručnost trebao bi se pridržavati odredaba primjenljivih na institucije Unije i nacionalnog zakonodavstva u vezi s postupanjem s osjetljivim dokumentima, posebno s osjetljivim neklasificiranim podacima i klasificiranim podacima EU-a.

(30) Financijske interese Unije i država članica tijekom cijelog ciklusa potrošnje trebalo bi zaštititi proporcionalnim mjerama, uključujući mjerama za sprečavanje, otkrivanje i ispitivanje nepravilnosti, povrat izgubljenih, nepravilno plaćenih ili nepravilno upotrijebljenih sredstava te prema potrebi primjenom administrativnih i financijskih sankcija u skladu s Uredbom XXX (EU, Euratom) Europskog parlamenta i Vijeća[25] [Financijska uredba].

(31) Centar za stručnost trebao bi djelovati otvoreno i transparentno tako da pravodobno dostavlja sve relevantne informacije i da promiče svoje aktivnosti, uključujući aktivnosti informiranja i obavješćivanja šire javnosti. Poslovnici tijela Centra za stručnost trebali bi biti javno dostupni.

(32) Unutarnji revizor Komisije trebao bi u pogledu Centra za stručnost imati jednake ovlasti kakve ima u pogledu Komisije.

(33) Komisija, Centar za stručnost, Revizorski sud i Europski ured za borbu protiv prijevara trebali bi imati pristup svim potrebnim informacijama i prostorijama za provođenje revizija i istraga bespovratnih sredstava, ugovora i sporazuma koje je potpisao Centar za stručnost.

(34) Budući da ciljeve ove Uredbe, odnosno zadržavanje i razvoj tehnoloških i industrijskih sposobnosti Unije u području kibersigurnosti, povećanje konkurentnosti Unijine industrije kibersigurnosti i pretvaranje kibersigurnosti u konkurentnu prednost drugih industrija Unije, ne mogu dostatno ostvariti države članice budući da su postojeća, ograničena sredstva raširena te zbog opsega potrebnih ulaganja, već se oni bolje mogu ostvariti na razini Unije kako bi se izbjeglo nepotrebno udvostručavanje napora, lakše postigla kritična masa ulaganja i osigurala najbolja uporaba javnog financiranja, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. Ugovora o Europskoj uniji. U skladu s načelom proporcionalnosti utvrđenim u tom članku, ova Uredba ne prelazi se ono što je potrebno za ostvarenje tog cilja,

---

[24] Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije (SL L 145, 31.5.2001., str. 43.).

[25] [dodati naslov i upućivanje na SL]

DONIJELI SU OVU UREDBU:

POGLAVLJE I.

OPĆE ODREDBE I NAČELA CENTRA ZA STRUČNOST I MREŽE

Članak 1.

Predmet

1. Ovom Uredbom osnivaju se Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja („Centar za stručnost”) i Mreža nacionalnih koordinacijskih centara te se utvrđuju pravila za imenovanje nacionalnih koordinacijskih centara i za uspostavu Zajednice stručnjaka za kibersigurnost.

2. Centar za stručnost pridonosi provedbi programa Digitalna Europa uspostavljenog Uredbom br. XXX u dijelu koji se odnosi na kibersigurnost, a posebno mjera povezanih s člankom 6. Uredbe (EU) br. XXX [Program Digitalna Europa], programa Obzor Europa uspostavljenog Uredbom br. XXX, a posebno odjeljka 2.2.6. stupa II. Priloga I. Odluci br. XXX o uspostavi posebnog programa za provedbu Obzora Europa – Okvirnog programa za istraživanje i inovacije [referentni broj posebnog programa].

3. Sjedište Centra za stručnost nalazi se u [Bruxellesu, u Belgiji].

4. Centar za stručnost ima pravnu osobnost. U svakoj državi članici on ima najširu pravnu sposobnost koja se pravnim subjektima priznaje u skladu sa zakonodavstvom te države članice. On osobito može stjecati pokretnine i nekretnine ili njima raspolagati te biti stranka u sudskom postupku.

Članak 2.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

(1) „kibersigurnost” znači zaštita mrežnih i informacijskih sustava, njihovih korisnika i drugih osoba od kiberprijetnji;

(2) „proizvodi i rješenja za kibersigurnost” znači proizvodi, usluge ili postupci IKT-a s posebnom svrhom zaštite od kiberprijetnji mrežnih i informacijskih sustava, njihovih korisnika i uključenih osoba;

(3) „tijelo javne vlasti” znači svaka vlast ili druga javna uprava, uključujući javna savjetodavna tijela na nacionalnoj, regionalnoj ili lokalnoj razini, ili bilo koja fizička ili pravna osoba koja obavlja javne upravne zadaće u skladu s nacionalnim pravom, uključujući posebne dužnosti;

(4) „država članica sudionica” znači država članica koja dobrovoljno financijski pridonosi administrativnim i upravnim troškovima Centra za stručnost.

Članak 3.

Misija Centra i Mreže

1. Centar za stručnost i Mreža pomažu Uniji da učini sljedeće:

   (a) zadrži i razvije tehnološke i industrijske kapacitete u području kibersigurnosti koji su nužni za zaštitu njezina jedinstvenog digitalnog tržišta;

   (b) poveća konkurentnost industrije kibersigurnosti u Uniji i pretvori kibersigurnost u konkurentnu prednost drugih industrija Unije.

2. Centar za stručnost obavlja svoje zadaće, prema potrebi, u suradnji s Mrežom nacionalnih koordinacijskih centara i Zajednicom stručnjaka za kibersigurnost.

Članak 4.

Ciljevi i zadaće Centra

Centar za stručnost ima sljedeće ciljeve i povezane zadaće:

1. olakšavati rad Mreže nacionalnih koordinacijskih centara („Mreža”) iz članka 6. i Zajednice stručnjaka za kibersigurnost iz članka 8. te pomagati u koordinaciji njihova rada;

2. pridonositi provedbi programa Digitalna Europa uspostavljenog Uredbom br. XXX[26] u dijelu koji se odnosi na kibersigurnost, a posebno mjera povezanih s člankom 6. Uredbe (EU) br. XXX [Program Digitalna Europa], programa Obzor Europa uspostavljenog Uredbom br. XXX[27], a posebno odjeljka 2.2.6. stupa II. Priloga I. Odluci br. XXX o uspostavi posebnog programa za provedbu Obzora Europa – Okvirnog programa za istraživanje i inovacije [referentni broj posebnog programa] te drugih programa Unije kada je tako predviđeno u pravnim aktima Unije;

3. unapređivati sposobnosti, znanje i infrastrukture u području kibersigurnosti u službi industrije, javnog sektora i istraživačkih zajednica obavljanjem sljedećih zadaća:

   (a) uzimajući u obzir najsuvremenije industrijske i istraživačke infrastrukture u području kibersigurnosti i povezane usluge, stjecanjem, nadogradnjom, upravljanjem radom i stavljanjem na raspolaganje takvih infrastruktura i povezanih usluga velikom broju korisnika u cijeloj Uniji od industrije, od MSP-ova, do javnog sektora i istraživačke i znanstvene zajednice;

   (b) uzimajući u obzir najsuvremenije industrijske i istraživačke infrastrukture u području kibersigurnosti i povezane usluge, pružanjem potpore drugim subjektima, uključujući financijske potpore, za stjecanje, nadogradnju, upravljanje radom i stavljanje na raspolaganje takvih infrastruktura i povezanih usluga velikom broju korisnika u cijeloj Uniji od industrije, do MSP-ova, javnog sektora i istraživačke i znanstvene zajednice;

   (c) pružanjem znanja i tehničke pomoći iz područja kibersigurnosti industriji i tijelima javne vlasti, posebno podupiranjem mjera usmjerenih na olakšavanje pristupa stručnom znanju dostupnom u Mreži i Zajednici stručnjaka za kibersigurnost;

[26] [dodati puni naslov i upućivanje na SL]
[27] [dodati puni naslov i upućivanje na SL]

4. pridonijeti raširenoj primjeni najsuvremenijih proizvoda i rješenja za kibersigurnost u cijelom gospodarstvu, obavljanjem sljedećih zadaća:

   (a) poticanjem istraživanja i razvoja u području kibersigurnosti i tijela javne vlasti te korisničkih industrija da prihvate proizvode i rješenja Unije za kibersigurnost;

   (b) pomaganjem tijelima javne vlasti, industrijama na strani potražnje i drugim korisnicima u prihvaćanju i integriranju najnovijih rješenja za kibersigurnost;

   (c) posebno podupiranjem tijela javne vlasti u organizaciji javne nabave ili obavljanju nabave najsuvremenijih proizvoda i rješenja za kibersigurnost u ime javnih tijela;

   (d) pružanjem financijske potpore i tehničke pomoći novoosnovanim poduzećima u sektoru kibersigurnosti i MSP-ovima kako bi se mogli povezati s mogućim tržištima i privući ulaganja;

5. poboljšavati razumijevanje kibersigurnosti i pridonositi smanjenju nedostatka vještina u Uniji u području kibersigurnosti obavljanjem sljedećih zadaća:

   (a) podupiranjem daljnjeg razvoja vještina u području kibersigurnosti, prema potrebi zajedno s relevantnim agencijama i tijelima EU-a, uključujući s ENISA-om;

6. pridonositi jačanju istraživanja i razvoja u području kibersigurnosti u Uniji na sljedeće načine:

   (a) pružanjem financijske potpore za istraživanje u području kibersigurnosti na temelju zajedničkog višegodišnjeg strateškog programa za industriju, tehnologiju i istraživanje koji se stalno ocjenjuje i unaprjeđuje;

   (b) podupiranjem opsežnih istraživačkih i demonstracijskih projekata posvećenih tehnološkim sposobnostima sljedeće generacije u području kibersigurnosti, u suradnji s industrijom i mrežom;

   (c) podupiranjem istraživanja i inovacija za standardizaciju u tehnologiji kibersigurnosti;

7. jačati suradnju između civilnog i obrambenog sektora u pogledu tehnologija za dvojnu uporabu i primjenu u kibersigurnosti, obavljanjem sljedećih zadaća:

   (a) pružanjem potpore državama članicama i dionicima u području industrije i istraživanja u istraživanju, razvoju i primjeni;

   (b) pridonošenjem suradnji među državama članicama podupiranjem obrazovanja, osposobljavanja i vježbi;

   (c) okupljanjem dionika, poticanjem sinergije između civilnog i obrambenog istraživanja i tržišta u području kibersigurnosti;

8. jačati sinergiju između civilne i obrambene dimenzije kibersigurnosti u pogledu Europskog fonda za obranu obavljanjem sljedećih zadaća:

   (a) davanjem savjeta, razmjenom iskustva i olakšavanjem suradnje među relevantnim dionicima;

(b) upravljanjem multinacionalnim projektima u području kiberobrane na zahtjev država članica i djelovanjem u svojstvu voditelja projekta u smislu Uredbe XXX [Uredba o osnivanju Europskog fonda za obranu].

Članak 5.

Ulaganje u infrastrukture, sposobnosti, proizvode ili rješenja i njihova uporaba

1. Ako Centar za stručnost pruža financijska sredstva za infrastrukture, sposobnosti, proizvode ili rješenja u skladu s člankom 4. stavcima 3. i 4. u obliku bespovratnih sredstava ili nagrade, u planu rada Centra za stručnost može se posebno navesti sljedeće:

   (a) pravila za rad infrastrukture ili sposobnosti, uključujući, prema potrebi, povjeravanje upravljanja subjektu domaćinu na temelju kriterija koje utvrđuje Centar za stručnost;

   (b) pravila kojima se uređuje pristup infrastrukturi ili sposobnosti i njihova uporaba.

2. Centar za stručnost može biti odgovoran za opće izvršenje relevantnih aktivnosti zajedničke nabave, uključujući pretkomercijalne nabave u ime članova Mreže, članova Zajednice stručnjaka za kibersigurnost ili trećih strana koje predstavljaju korisnike proizvoda i rješenja za kibersigurnost. U tu svrhu, Centru za stručnost može pomagati jedan ili više nacionalnih koordinacijskih centara ili članova Zajednice stručnjaka za kibersigurnost.

Članak 6.

Imenovanje nacionalnih koordinacijskih centara

1. Do [datum] svaka država članica imenuje subjekt koji će djelovati kao nacionalni koordinacijski centar za potrebe ove Uredbe i o tome obavješćuje Komisiju.

2. Na temelju procjene ispunjava li taj subjekt kriterije iz stavka 4., Komisija u roku od 6 mjeseci od imenovanja koje joj je dostavila država članica donosi odluku o akreditaciji subjekta kao nacionalnog koordinacijskog centra ili o odbijanju imenovanja. Komisija objavljuje popis nacionalnih koordinacijskih centara.

3. Države članice mogu za potrebe ove Uredbe u bilo kojem trenutku nacionalnim koordinacijskim centrom imenovati novi subjekt. Na imenovanje novog subjekta primjenjuju se stavci 1. i 2.

4. Imenovani nacionalni koordinacijski centar ima sposobnost podupirati Centar za stručnost i Mrežu u izvršavanju njihove misije utvrđene u članku 3. ove Uredbe. Oni posjeduju tehnološko stručno znanje u području kibersigurnosti ili imaju pristup tom znanju te mogu djelotvorno surađivati i koordinirati aktivnosti s industrijom, javnim sektorom i istraživačkom zajednicom.

5. Odnos između Centra za stručnost i nacionalnih koordinacijskih centara temelji se na sporazumu potpisanom između Centra za stručnost i svakog od nacionalnih koordinacijskih centara. U sporazumu su predviđena pravila kojima se uređuje odnos između Centra za stručnost i svakog nacionalnog koordinacijskog centra te podjela zadaća.

6. Mreža nacionalnih koordinacijskih centara sastoji se od svih nacionalnih koordinacijskih centara koje su imenovale države članice.

Članak 7.

Zadaće nacionalnih koordinacijskih centara

1. Nacionalni koordinacijski centri imaju sljedeće zadaće:

   (a) podupirati Centar za stručnost u ostvarivanju ciljeva, a posebno u koordiniranju Zajednice stručnjaka za kibersigurnost;

   (b) olakšavati sudjelovanje industrije i drugih zainteresiranih strana na razini države članice u prekograničnim projektima;

   (c) pridonositi, zajedno s Centrom za stručnost, prepoznavanju i uklanjanju kibersigurnosnih izazova u industriji u pojedinim sektorima;

   (d) djelovati kao kontaktna točka na nacionalnoj razini za Zajednicu stručnjaka za kibersigurnost i Centar za stručnost;

   (e) nastojati uspostaviti sinergiju s relevantnim aktivnostima na nacionalnoj i regionalnoj razini;

   (f) provoditi posebne mjere za koje je Centar za stručnost dodijelio bespovratna sredstva, među ostalim pružanjem financijske potpore trećim stranama u skladu s člankom 204. Uredbe XXX [nova Financijska uredba] pod uvjetima navedenima u predmetnim sporazumima o dodjeli bespovratnih sredstava;

   (g) promovirati i širiti relevantne rezultate rada Mreže, Zajednice stručnjaka za kibersigurnost i Centra za stručnost na nacionalnoj ili regionalnoj razini;

   (h) ocjenjivati zahtjeve za članstvo u Zajednici stručnjaka za kibersigurnost subjekata koji su u istoj državi članici osnovani kao koordinacijski centar:

2. Za potrebe točke (f), financijska potpora trećim stranama može se pružati u bilo kojem obliku iz članka 125. Uredbe XXX [nova Financijska uredba], među ostalim u obliku jednokratnih iznosa.

3. Nacionalni koordinacijski centri mogu primiti bespovratna sredstva od Unije u skladu s člankom 195. točkom (d) Uredbe XXX [nova Financijska uredba] za obavljanje zadaća iz ovog članka.

4. Nacionalni koordinacijski centri, prema potrebi, surađuju posredstvom Mreže za potrebe provedbe zadaća iz stavka 1. točaka (a), (b), (c), (e) i (g).

Članak 8.

Zajednica stručnjaka za kibersigurnost

1. Zajednica stručnjaka za kibersigurnost pridonosi misiji Centra za stručnost utvrđenoj u članku 3. te jača i širi stručno znanje u području kibersigurnosti u cijeloj Uniji.

2. Zajednica stručnjaka za kibersigurnost sastoji se od industrije, akademskih i neprofitnih istraživačkih organizacija i udruga te od javnih tijela i drugih subjekata koji se bave operativnim i tehničkim pitanjima. Ona okuplja glavne dionike u području tehnoloških i industrijskih kapaciteta za kibersigurnost u Uniji. U njoj sudjeluju nacionalni koordinacijski centri i institucije te tijela Unije s odgovarajućim stručnim znanjem.

3. Samo subjekti s poslovnim nastanom u Uniji mogu biti akreditirani članovi Zajednice stručnjaka za kibersigurnost. Oni dokazuju da imaju stručno znanje u području kibersigurnosti iz barem jednog od sljedećih područja:

(a) istraživanje;

(b) industrijski razvoj;

(c) osposobljavanje i obrazovanje.

4. Centar za stručnost akreditira subjekte osnovane u skladu s nacionalnim pravom kao članove Zajednice stručnjaka za kibersigurnost nakon procjene ispunjava li subjekt kriterije iz stavka 3. koju obavlja nacionalni koordinacijski centar države članice u kojoj subjekt ima poslovni nastan. Akreditacija nije ograničenog trajanja, ali je Centar za stručnost može u bilo kojem trenutku opozvati ako on ili nacionalni koordinacijski centar smatraju da subjekt ne ispunjava kriterije iz stavka 3. ili ako se na njega primjenjuju mjerodavne odredbe iz članka 136. Uredbe XXX [nova Financijska uredba].

5. Centar za stručnost akreditira relevantna tijela, agencije i urede Unije kao članove Zajednice stručnjaka za kibersigurnost nakon procjene ispunjava li subjekt kriterije iz stavka 3. Akreditacija nije ograničenog trajanja, ali je Centar za stručnost može u bilo kojem trenutku opozvati ako smatra da subjekt ne ispunjava kriterije iz stavka 3. ili ako se na njega primjenjuju mjerodavne odredbe iz članka 136. Uredbe XXX [nova Financijska uredba].

6. U radu Zajednice mogu sudjelovati predstavnici Komisije.

Članak 9.

Zadaće članova Zajednice stručnjaka za kibersigurnost

Članovi Zajednice stručnjaka za kibersigurnost obavljaju sljedeće:

(1) podupiru Centar za stručnost u ostvarivanju misije i ciljeva iz članaka 3. i 4. i u tu svrhu blisko surađuju s Centrom za stručnost i relevantnim nacionalnim koordinacijskim centrima;

(2) sudjeluju u aktivnostima koje promiču Centar za stručnost i nacionalni koordinacijski centri;

(3) prema potrebi, sudjeluju u radnim skupinama koje je osnovao Upravni odbor Centra za stručnost za obavljanje posebnih aktivnosti, kako je predviđeno u planu rada Centra za stručnost;

(4) prema potrebi, podupiru Centar za stručnost i nacionalne koordinacijske centre u promicanju posebnih projekata;

(5) promiču i objavljuju relevantne rezultate aktivnosti i projekata koji se provode unutar Zajednice.

Članak 10.

Suradnja Centra za stručnost s institucijama, tijelima, uredima i agencijama Unije

1. Centar za stručnost surađuje s relevantnim institucijama, tijelima, uredima i agencijama Unije, uključujući s Agencijom Europske unije za mrežnu i informacijsku sigurnost, timom za hitne računalne intervencije (CERT-EU), Zajedničkom službom za vanjsko djelovanje, Zajedničkim istraživačkim centrom Komisije, Izvršnom agencijom za istraživanje, Izvršnom agencijom za inovacije i mreže, Europskim centrom za kiberkriminal pri Europolu i Europskom obrambenom agencijom.

2. Ta suradnja odvija se u okviru radnih aranžmana. Ti aranžmani podnose se Komisiji na prethodno odobrenje.

POGLAVLJE II.

USTROJSTVO CENTRA ZA STRUČNOST

Članak 11.

Članstvo i struktura

1. Članovi Centra za stručnost jesu Unija, koju zastupa Komisija, i države članice.
2. Struktura Centra za stručnost sastoji se od sljedećeg:
   (a) Upravnog odbora koji obavlja zadaće utvrđene u članku 13.;
   (b) izvršnog direktora koji obavlja zadaće utvrđene u članku 16.;
   (c) Industrijskog i znanstvenog savjetodavnog odbora koji obavlja zadaće utvrđene u članku 20.

ODJELJAK I.

UPRAVNI ODBOR

Članak 12.

Sastav Upravnog odbora

1. Upravni odbor sastoji se od jednog predstavnika svake države članice i pet predstavnika Komisije, u ime Unije.
2. Svaki član Upravnog odbora ima zamjenika koji ga predstavlja u slučaju njegove odsutnosti.
3. Članovi Upravnog odbora i njihovi zamjenici imenuju se uzimajući u obzir njihovo znanje u području tehnologije te relevantne upravljačke i administrativne vještine i vještine upravljanja proračunom. Komisija i države članice nastoje ograničiti fluktuaciju svojih predstavnika u Upravnom odboru kako bi se osigurao kontinuitet njegova rada. Komisija i države članice imaju za cilj postići uravnoteženu zastupljenost muškaraca i žena u Upravnom odboru.
4. Mandat članova Upravnog odbora i njihovih zamjenika traje četiri godine. Taj mandat može se produljiti.
5. Članovi Upravnog odbora djeluju u interesu Centra za stručnost, zauzimajući se na neovisan i transparentan način za njegove ciljeve, misiju, identitet, autonomnost i usklađenost.
6. Prema potrebi Komisija može pozvati promatrače, među ostalim zastupnike odgovarajućih tijela, ureda i agencija Unije, da sudjeluju na sastancima Upravnog odbora.
7. Europska agencija za mrežnu i informacijsku sigurnost (ENISA) stalni je promatrač u Upravnom odboru.

Članak 13.

Zadaće Upravnog odbora

1. Upravni odbor u cijelosti je odgovoran za strateško usmjeravanje i djelovanje Centra za stručnost te nadzire provedbu njegovih aktivnosti.

2. Upravni odbor donosi svoj poslovnik. Taj poslovnik uključuje posebne postupke kojima se prepoznaju i izbjegavaju sukobi interesa te osigurava povjerljivost mogućih osjetljivih informacija.

3. Upravni odbor donosi potrebne strateške odluke, a posebno:

   (a) donosi višegodišnji strateški plan u kojem su navedeni glavni prioriteti i planirane inicijative Centra za stručnost, uključujući procjenu potreba za financiranjem i izvora financiranja;

   (b) donosi plan rada Centra za stručnost, godišnje financijske izvještaje i bilancu te godišnje izvješće o radu, na temelju prijedloga izvršnog direktora;

   (c) donosi posebna financijska pravila Centra za stručnost u skladu s [člankom 70. Financijske uredbe];

   (d) donosi postupak za imenovanje izvršnog direktora;

   (e) donosi kriterije i postupke za ocjenjivanje i akreditiranje subjekata kao članova Zajednice stručnjaka za kibersigurnost;

   (f) imenuje i razrješava izvršnog direktora, produljuje njegov mandat, daje mu smjernice i prati njegov rad te imenuje računovodstvenog službenika;

   (g) donosi godišnji proračun Centra za stručnost, uključujući odgovarajući plan radnih mjesta u kojem se navodi broj privremenih radnih mjesta prema funkcijskoj skupini i razredu kao i broj ugovornog osoblja te upućenih nacionalnih stručnjaka iskazan u ekvivalentu punog radnog vremena;

   (h) donosi pravila o sukobu interesa;

   (i) osniva radne skupine s članovima Zajednice stručnjaka za kibersigurnost;

   (j) imenuje članove Industrijskog i znanstvenog savjetodavnog odbora;

   (k) uspostavlja Funkciju unutarnje revizije u skladu s Delegiranom uredbom Komisije (EU) br. 1271/2013[28];

   (l) promiče Centar za stručnost na globalnoj razini kako bi povećao njegovu privlačnost i pretvorio ga u vrhunsko tijelo izvrsnosti u području kibersigurnosti;

   (m) utvrđuje komunikacijsku politiku Centra za stručnost na preporuku izvršnog direktora;

   (n) odgovoran je za provođenje odgovarajućih daljnjih mjera na temelju zaključaka naknadnih evaluacija;

   (o) prema potrebi utvrđuje provedbena pravila za Pravilnik o osoblju i Uvjete zapošljavanja u skladu s člankom 31. stavkom 3.;

[28] Delegirana uredba Komisije (EU) br. 1271/2013 od 30. rujna 2013. o Okvirnoj financijskoj uredbi za tijela iz članka 208. Uredbe (EU, Euratom) br. 966/2012 Europskog parlamenta i Vijeća (SL L 328, 7.12.2013., str. 42.).

(p) prema potrebi, utvrđuje pravila o upućivanju nacionalnih stručnjaka u Centar za stručnost i o uporabi vježbenika u skladu s člankom 32. stavkom 2.;

(q) donosi sigurnosna pravila za Centar za stručnost;

(r) donosi strategiju za suzbijanje prijevara koja je razmjerna rizicima od prijevare, uzimajući u obzir analizu troškova i koristi mjera koje će se provoditi;

(s) donosi metodologiju za izračun financijskog doprinosa država članica;

(t) odgovoran je za sve zadaće koje nisu posebno dodijeljene određenom tijelu Centra za stručnost; može dodijeliti takve zadaće bilo kome u Centru za stručnost.

Članak 14.

Predsjednik i sastanci Upravnog odbora

1. Upravni odbor među svojim članovima s pravom glasa bira predsjednika i zamjenika predsjednika, na razdoblje od dvije godine. Mandat predsjednika i zamjenika predsjednika može se produljiti jednom na temelju odluke Upravnog odbora. Međutim, ako im članstvo u Upravnom odboru prestane u bilo kojem trenutku tijekom njihova mandata, mandat im automatski prestaje na taj datum. Zamjenik predsjednika po službenoj dužnosti zamjenjuje predsjednika ako predsjednik nije u mogućnosti obavljati svoje zadaće. Predsjednik sudjeluje u glasovanju.
2. Upravni odbor održava redovite sastanke najmanje tri puta godišnje. On pri izvršavanju svojih zadaća može održavati izvanredne sastanke na zahtjev Komisije, na zahtjev jedne trećine svojih članova, na zahtjev predsjednika ili na zahtjev izvršnog direktora.
3. Izvršni direktor sudjeluje u raspravama, osim ako Upravni odbor odluči drukčije, ali nema pravo glasa. Upravni odbor može, ovisno o slučaju, pozvati druge osobe da prisustvuju njegovim sastancima u svojstvu promatrača.
4. Članovi Industrijskog i znanstvenog savjetodavnog odbora mogu, na poziv predsjednika, sudjelovati u sastancima Upravnog odbora, bez prava glasa.
5. Članovima Upravnog odbora i njihovim zamjenicima na sastancima mogu, u skladu s njegovim poslovnikom, pomagati savjetnici ili stručnjaci.
6. Centar za stručnost Upravnom odboru pruža usluge tajništva.

Članak 15.

Pravila Upravnog odbora o glasovanju

1. Unija ima 50 % glasačkih prava. Glasačka prava Unije nedjeljiva su.
2. Svaka država članica sudionica ima jedan glas.
3. Upravni odbor donosi odluke većinom od barem 75 % svih glasova, uključujući glasove odsutnih članova, koji čine barem 75 % ukupnih financijskih doprinosa Centru za stručnost. Financijski doprinos izračunava se na temelju procijenjenih rashoda koje predlažu države članice iz članka 17. stavka 2. točke (c) i temelji se na izvješću o vrijednosti doprinosa država članica sudionica iz članka 22. stavka 5.

4. Pravo glasa imaju samo predstavnici Komisije i predstavnici država članica sudionica.

5. Predsjednik sudjeluje u glasovanju.

ODJELJAK II.

IZVRŠNI DIREKTOR

Članak 16.

Imenovanje i razrješenje izvršnog direktora ili produljenje njegova mandata

1. Izvršni direktor stručna je i ugledna osoba u područjima djelovanja Centra za stručnost.

2. Izvršni direktor zapošljava se kao član privremenog osoblja Centra za stručnost u skladu s člankom 2. točkom (a) Uvjeta zaposlenja ostalih službenika.

3. Izvršnog direktora imenuje Upravni odbor s popisa kandidata koji predlaže Komisija, nakon otvorenog i transparentnog postupka odabira.

4. Centar za stručnost pri sklapanju ugovora s izvršnim direktorom zastupa predsjednik Upravnog odbora.

5. Mandat izvršnoga direktora traje četiri godine. Do kraja tog razdoblja Komisija provodi procjenu u kojoj se uzimaju u obzir ocjena uspješnosti izvršnog direktora te budući izazovi i zadaće Centra za stručnost.

6. Upravni odbor na prijedlog Komisije, kojim se uzima u obzir procjena iz stavka 5., može jedanput produljiti mandat izvršnog direktora za razdoblje od najdulje četiri godine.

7. Izvršni direktor čiji je mandat produljen ne može sudjelovati u još jednom postupku odabira za isto radno mjesto.

8. Izvršni direktor može biti razriješen dužnosti samo na temelju odluke Upravnog odbora koji djeluje na prijedlog Komisije.

Članak 17.

Zadaće izvršnog direktora

1. Izvršni direktor odgovoran je za rad Centra za stručnost i svakodnevno upravljanje njime te je njegov zakonski zastupnik. Izvršni direktor odgovara Upravnom odboru i obavlja svoje dužnosti potpuno samostalno u okviru ovlasti koje su mu dodijeljene.

2. Izvršni direktor neovisno obavlja prvenstveno sljedeće zadaće:

   (a) provodi odluke koje je donio Upravni odbor;

   (b) pomaže Upravnom odboru u radu, pruža usluge tajništva za njegove sastanke i pruža sve informacije koje su nužne za obavljanje njegovih dužnosti;

   (c) nakon savjetovanja s Upravnim odborom i Komisijom, izrađuje i podnosi Upravnom odboru na donošenje nacrt višegodišnjeg strateškog plana i nacrt godišnjeg plana rada Centra za stručnost, uključujući područje primjene poziva na podnošenje prijedloga, poziva na iskaz interesa i poziva na podnošenje ponuda koji su potrebni za provođenje plana rada i odgovarajuće procjene troškova kako su predložile države članice i Komisija;

(d) izrađuje i podnosi Upravnom odboru na donošenje nacrt godišnjeg proračuna, uključujući odgovarajući plan radnih mjesta u kojem se navodi broj privremenih radnih mjesta prema svakom platnom razredu i funkcijskoj grupi te broj ugovornog osoblja i upućenih nacionalnih stručnjaka iskazan u ekvivalentima punog radnog vremena;

(e) provodi plan rada i o tome izvješćuje Upravni odbor;

(f) izrađuje nacrt godišnjeg izvješća o radu Centra za stručnost, koji uključuje informacije o odgovarajućim rashodima;

(g) osigurava provedbu djelotvornih postupaka praćenja i evaluacije rada Centra za stručnost;

(h) izrađuje akcijski plan na temelju zaključaka naknadnih evaluacija i svake dvije godine izvješćuje Komisiju o napretku;

(i) sastavlja sporazume s nacionalnim koordinacijskim centrom, pregovara o njima i sklapa ih;

(j) odgovoran je za administrativna i financijska pitanja te pitanja povezana s osobljem, uključujući za izvršenje proračuna Centra za stručnost, uzimajući u obzir savjete zaprimljene od Funkcije unutarnje revizije, unutar ograničenja delegiranih ovlasti koje mu je dodijelio Upravni odbor;

(k) odobrava pokretanje poziva na podnošenje prijedloga i upravlja njihovim pokretanjem, u skladu s planom rada, te upravlja sporazumima i odlukama o bespovratnim sredstvima;

(l) odobrava popis mjera odabranih za financiranje na temelju rang-liste koju je izradila skupina neovisnih stručnjaka;

(m) odobrava pokretanje poziva na podnošenje ponuda i upravlja njihovim pokretanjem, u skladu s planom rada, te upravlja ugovorima;

(n) odobrava ponude odabrane za financiranje;

(o) podnosi nacrte godišnjih izvještaja i bilance Funkciji unutarnje revizije i nakon toga Upravnom odboru;

(p) osigurava provedbu procjene rizika i upravljanja rizikom;

(q) potpisuje pojedinačne sporazume, odluke i ugovore o dodjeli bespovratnih sredstava;

(r) potpisuje ugovore o nabavi;

(s) izrađuje akcijski plan na temelju zaključaka iz izvješća o unutarnjoj ili vanjskoj reviziji i istraga Europskog ureda za borbu protiv prijevara (OLAF) i izvješćuje Komisiju o napretku dva puta godišnje te redovito izvješćuje Upravni odbor;

(t) izrađuje nacrt financijskih pravila koja se primjenjuju na Centar za stručnost;

(u) uspostavlja djelotvorni i učinkovit sustav unutarnje kontrole i osigurava njegovo funkcioniranje te izvješćuje Upravni odbor o svakoj bitnoj promjeni u njemu;

(v) osigurava učinkovitu komunikaciju s institucijama Unije;

(w) poduzima druge mjere koje su potrebne za ocjenjivanje napretka Centra za stručnost ka ostvarenju njegove misije i ciljeva utvrđenih u člancima 3. i 4. Uredbe;

(x) izvršava sve ostale zadaće koje mu povjeri ili za koje ga ovlasti Upravni odbor.

ODJELJAK III.

INDUSTRIJSKI I ZNANSTVENI SAVJETODAVNI ODBOR

Članak 18.

Sastav Industrijskog i znanstvenog savjetodavnog odbora

1. Industrijski i znanstveni savjetodavni odbor ima najviše 16 članova. Članove imenuje Upravni odbor među predstavnicima subjekata Zajednice stručnjaka za kibersigurnost.
2. Članovi Industrijskog i znanstvenog savjetodavnog odbora stručnjaci su za istraživanje, industrijski razvoj i profesionalne usluge u području kibersigurnosti ili za njihovu primjenu. Zahtjeve u pogledu tog stručnog znanja dodatno utvrđuje Upravni odbor.
3. Postupci imenovanja članova Upravnog odbora i postupci za rad Industrijskog i znanstvenog savjetodavnog odbora navedeni su u poslovniku Centra za stručnost i objavljuju se.
4. Mandat članova Industrijskog i znanstvenog savjetodavnog odbora traje tri godine. Taj se mandat može produljiti.
5. Predstavnici Komisije i Europske agencije za mrežnu i informacijsku sigurnost mogu sudjelovati u radu Industrijskog i znanstvenog savjetodavnog odbora i podupirati njegov rad.

Članak 19.

Funkcioniranje Industrijskog i znanstvenog savjetodavnog odbora

1. Industrijski i znanstveni savjetodavni odbor sastaje se barem dvaput godišnje.
2. Industrijski i znanstveni savjetodavni odbor može savjetovati Upravni odbor o osnivanju radnih skupina o posebnim pitanjima koja su važna za rad Centra za stručnost, prema potrebi, čiji rad koordiniraju jedan ili više članova Industrijskog i znanstvenog savjetodavnog odbora.
3. Industrijski i znanstveni savjetodavni odbor bira svojeg predsjednika.
4. Industrijski i znanstveni savjetodavni odbor donosi svoj poslovnik, uključujući pravila o imenovanju zastupnika koji, prema potrebi, zastupaju Industrijski i znanstveni savjetodavni odbor i o trajanju njihova imenovanja.

Članak 20.

Zadaće Industrijskog i znanstvenog savjetodavnog odbora

Industrijski i znanstveni savjetodavni odbor savjetuje se s Centrom za stručnost o obavljanju svojih aktivnosti te obavlja sljedeće zadaće:

(1) pruža izvršnom direktoru i Upravnom odboru strateške savjete i informacije za izradu plana rada i višegodišnjeg strateškog plana unutar rokova koje je utvrdio Upravni odbor;

(2) organizira javna savjetovanja koja su otvorena za javnost i privatne dionike s interesom u području kibersigurnosti u cilju prikupljanja informacija za strateške savjete iz stavka 1.;

(3) promiče i prikuplja povratne informacije o planu rada i višegodišnjem strateškom planu Centra za stručnost.

POGLAVLJE III.

FINANCIJSKE ODREDBE

Članak 21.

Financijski doprinos Unije

1. Doprinos Unije Centru za stručnost za pokrivanje administrativnih troškova i troškova poslovanja obuhvaća sljedeće:

   (a) 1 981 668 000 EUR iz programa Digitalna Europa, uključujući do 23 746 000 EUR za administrativne troškove;

   (b) iznos iz programa Obzor Europa, uključujući za administrativne troškove, koji se utvrđuje uzimajući u obzir postupak strateškog planiranja koji se obavlja u skladu s člankom 6. stavkom 6. Uredbe XXX [Uredba o Obzoru Europa].

2. Najveći doprinos Unije plaća se iz odobrenih sredstava u općem proračunu Unije dodijeljenih [programu Digitalna Europa] i posebnom programu za provedbu programa Obzor Europa, koji je uspostavljen Odlukom XXX.

3. Centar za stručnost provodi aktivnosti kibersigurnosti iz [programa Digitalna Europa] i [programa Obzor Europa] u skladu s člankom 62. točkom (c) podtočkom iv. Uredbe (EU, Euratom) XXX[29] [Financijska uredba].

4. Financijski doprinos Unije ne obuhvaća zadaće iz članka 4. stavka 8. točke (b).

Članak 22.

Doprinosi država članica sudionica

1. Države članice sudionice daju ukupni doprinos troškovima poslovanja i administrativnim troškovima Centra za stručnost u barem jednakim iznosima kao što su oni iz članka 21. stavka 1. ove Uredbe.

2. U svrhu procjene doprinosa iz stavka 1. i članka 23. stavka 3. točke (b) podtočke ii., troškovi se utvrđuju u skladu s uobičajenom praksom troškovnog računovodstva predmetnih država članica, mjerodavnim računovodstvenim standardima države članice i primjenjivim međunarodnim računovodstvenim standardima i međunarodnim standardima financijskog izvještavanja. Troškove ovjerava neovisni vanjski revizor kojeg imenuje predmetna država članica. U slučaju bilo kakve nejasnoće u pogledu certificiranja, Centar za stručnost može provjeriti metodu procjene.

[29] [dodati puni naslov i upućivanje na SL]

3. Ako bilo koja država članica sudionica ne ispuni svoje obveze u pogledu svojeg financijskog doprinosa, izvršni direktor o tome sastavlja izvješće i određuje razuman rok za ispravljanje tog propusta. Ako propust ne bude ispravljen u danom roku, izvršni direktor saziva sastanak Upravnog odbora kako bi se odlučilo treba li opozvati pravo glasa države članice sudionice koja nije ispunila obveze ili poduzeti druge mjere dok ona ne ispuni svoje obveze. Pravo glasa države članice koja nije ispunila svoje obveze obustavlja se dok ona ne ispuni svoje obveze.

4. Komisija može ukinuti, razmjerno smanjiti ili obustaviti financijski doprinos Unije Centru za stručnost ako države članice sudionice ne plaćaju, plaćaju samo djelomično ili kasno plaćaju svoje doprinose iz stavka 1.

5. Države članice sudionice svake godine izvješćuju Upravni odbor do 31. siječnja o vrijednosti doprinosa iz stavka 1. koji su plaćeni svake prethodne financijske godine.

Članak 23.

Troškovi i sredstva Centra za stručnost

1. Centar za stručnost zajednički financiraju Unija i države članice u obliku financijskih doprinosa koji se plaćaju u obrocima i doprinosa koji se sastoje od troškova nastalih nacionalnim koordinacijskim centrima i korisnicima pri provođenju mjera koje Centar za stručnost ne nadoknađuje.

2. Administrativni troškovi Centra za stručnost ne prekoračuju [broj] EUR i financiraju se financijskim doprinosima koji se na godišnjoj osnovi ravnomjerno dijele između Unije i država članica sudionica. Ako se dio doprinosa za administrativne troškove ne iskoristi, može se namijeniti za financiranje troškova poslovanja Centra za stručnost.

3. Troškovi poslovanja Centra za stručnost pokrivaju se sljedećim:

   (a) financijskim doprinosom Unije;

   (b) doprinosima država članica sudionica u obliku sljedećeg:

      i. financijskih doprinosa i

      ii. prema potrebi, doprinosa u naravi država članica sudionica za pokrivanje troškova nacionalnih koordinacijskih centara i korisnika nastalih provedbom neizravnih mjera umanjenih za doprinos Centra za stručnost i bilo koji drugi doprinos Unije za pokrivanje tih troškova;

4. Sredstva Centra za stručnost uključena u njegov proračun sastoje se od sljedećih doprinosa:

   (a) financijskih doprinosa država članica sudionica administrativnim troškovima;

   (b) financijskih doprinosa država članica sudionica troškovima poslovanja;

   (c) svih prihoda Centra za stručnost;

   (d) svih drugih financijskih doprinosa, sredstava i prihoda.

5. Sve kamate obračunane na temelju doprinosa koje su Centru za stručnost uplatile države članice sudionice smatraju se njegovim prihodom.

6. Sredstvima Centra za stručnost i njegovim aktivnostima nastoje se ostvariti ciljevi iz članka 4.

7. Centar za stručnost vlasnik je sve imovine koju je samo stvorilo ili koja mu je prenesena radi ostvarivanja njegovih ciljeva.

8. Osim u slučaju likvidacije Centra za stručnost, članovima Centra za stručnost ne isplaćuje se višak prihoda nad rashodima.

Članak 24.

Financijske obveze

Financijske obveze Centra za stručnost ne prekoračuju iznos raspoloživih financijskih sredstava ili financijskih sredstava koje članovi uplaćuju u njegov proračun.

Članak 25.

Financijska godina

Financijska godina traje od 1. siječnja do 31. prosinca.

Članak 26.

Utvrđivanje proračuna

1. Izvršni direktor svake godine izrađuje nacrt računa procijenjenih prihoda i i rashoda Centra za stručnost za sljedeću financijsku godinu te ga prosljeđuje Upravnom odboru zajedno s nacrtom plana radnih mjesta. Prihodi i rashodi moraju biti u ravnoteži. Rashodi Centra za stručnost uključuju rashode za osoblje, administrativne i infrastrukturne rashode te rashode za poslovanje. Administrativni rashodi moraju se svesti na najmanju moguću mjeru.

2. Svake godine Upravni odbor, na temelju nacrta računa procijenjenih prihoda i rashoda iz stavka 1., izrađuje račun procijenjenih prihoda i rashoda Centra za stručnost za sljedeću financijsku godinu.

3. Upravni odbor svake godine do 31. siječnja Komisiji šalje račun procijenjenih prihoda i rashoda iz stavka 2., koji je dio nacrta jedinstvenog programskog dokumenta.

4. Na temelju tog računa Komisija one procijenjene iznose koje smatra potrebnima za plan radnih mjesta i iznos doprinosa na teret općeg proračuna unosi u nacrt proračuna Unije, koji podnosi Europskom parlamentu i Vijeću u skladu s člancima 313. i 314. UFEU-a.

5. Europski parlament i Vijeće odobravaju dodjelu sredstava za doprinos Centru za stručnost.

6. Europski parlament i Vijeće donose plan radnih mjesta Centra za stručnost.

7. Upravni odbor zajedno s planom rada donosi i proračun Centra za stručnost. Proračun postaje konačan nakon konačnog donošenja općeg proračuna Unije. Upravni odbor, prema potrebi, prilagođava proračun i plan rada Centra za stručnost u skladu s općim proračunom Unije.

Članak 27.

Podnošenje financijskih izvještaja Centra za stručnost i razrješnica

Centar za stručnost podnosi privremene i konačne financijske izvještaje i razrješnicu u skladu s pravilima i rasporedom iz Financijske uredbe i u skladu sa svojim financijskim pravilima donesenima u skladu s člankom 29.

Članak 28.

Operativno i financijsko izvješćivanje

1. Izvršni direktor Upravnom odboru podnosi godišnje izvješće o izvršavanju svojih dužnosti u skladu s financijskim pravilima Centra za stručnost.

2. Izvršni direktor u roku od dva mjeseca nakon zaključenja svake financijske godine podnosi Upravnom odboru na odobrenje godišnje izvješće o radu u kojem izvješćuje o napretku koji je Centar za stručnost ostvario u prethodnoj kalendarskoj godini, osobito u vezi s planom rada za tu godinu. Izvješće među ostalim obuhvaća informacije o sljedećim pitanjima:

   (a) provedenim operativnim mjerama i odgovarajućim rashodima;

   (b) podnesenim mjerama, uključujući pregled prema vrsti sudionika, uključujući MSP-ove, i prema zemlji;

   (c) odabranim mjerama za financiranje, uključujući pregled prema vrsti sudionika, uključujući MSP-ove, te prema zemlji, kao i doprinos Centra za stručnost pojedinačnim sudionicima i mjerama;

   (d) napretku u postizanju ciljeva utvrđenih člankom 4. i prijedlozima o daljnjim aktivnostima potrebnima za njihovo ostvarenje.

3. Nakon što Upravni odbor odobri godišnje izvješće o radu, ono se objavljuje.

Članak 29.

Financijska pravila

Centar za stručnost donosi svoja posebna financijska pravila u skladu s člankom 70. Uredbe XXX [nova Financijska uredba].

Članak 30.

Zaštita financijskih interesa

1. Centar za stručnost poduzima odgovarajuće mjere kojima osigurava da su, dok se provode mjere koje se financiraju u okviru ove Uredbe, financijski interesi Unije zaštićeni primjenom preventivnih mjera protiv prijevare, korupcije i svih drugih nezakonitih aktivnosti, učinkovitim provjerama i, ako se utvrde nepravilnosti, osiguravanjem povrata pogrešno plaćenih iznosa te, prema potrebi, učinkovitim, proporcionalnim i odvraćajućim administrativnim sankcijama.

2. Centar za stručnost omogućava osoblju Komisije i drugim osobama koje Komisija ovlasti te Revizorskom sudu pristup svojim lokacijama i prostorijama te svim informacijama koje su im potrebne za obavljanje revizija, uključujući informacije u elektroničkom obliku.

3. Europski ured za borbu protiv prijevara (OLAF) može provoditi istrage, uključujući provjere i inspekcije na terenu, u skladu s odredbama i postupcima utvrđenima u Uredbi Vijeća (Euratom, EZ) br. 2185/96[30] Europskog parlamenta i Vijeća i Uredbi (EU, Euratom) br. 833/2013 Europskog parlamenta i Vijeća[31], kako bi se utvrdilo je li došlo do prijevare, korupcije ili bilo koje druge nezakonite aktivnosti koja utječe na financijske interese Unije u vezi s ugovorom o dodjeli bespovratnih sredstava ili ugovorom koji se, izravno ili neizravno, financira u skladu s ovom Uredbom.

4. Ne dovodeći u pitanje stavke 1., 2. i 3. ovog članka., ugovori i sporazumi o dodjeli bespovratnih sredstava koji proizlaze iz provedbe ove Uredbe sadržavaju odredbe kojima se Komisija, Centar za stručnost, Revizorski sud i OLAF izričito ovlašćuju za provođenje takvih revizija i istraga u skladu sa svojim mjerodavnim nadležnostima. Ako se provedba mjere izdvaja ili dalje delegira, u cijelosti ili djelomično, ili ako to zahtijeva sklapanje ugovora o javnoj nabavi ili dodjelu financijske potpore trećoj strani, u ugovoru ili sporazumu o dodjeli bespovratnih sredstava navodi se obveza ugovaratelja ili korisnika da od bilo koje uključene treće strane zahtijeva izričito prihvaćanje tih ovlasti Komisije, Centra za stručnost, Revizorskog suda i OLAF-a.

POGLAVLJE IV.

OSOBLJE CENTRA ZA STRUČNOST

Članak 31.

Osoblje

1. Na osoblje Centra za stručnost primjenjuju se Pravilnik o osoblju za dužnosnike i Uvjeti zaposlenja ostalih službenika Europskih zajednica utvrđeni Uredbom Vijeća (EEZ, Euratom, EZUČ) br. 259/68[32] („Pravilnik o osoblju” i „Uvjeti zaposlenja”) i pravila koja su zajednički donijele institucije Unije radi primjene Pravilnika o osoblju i Uvjeta zaposlenja.

2. Upravni odbor izvršava u odnosu na osoblje Centra za stručnost ovlasti koje su Pravilnikom o osoblju dodijeljene tijelu za imenovanje te ovlasti koje su Uvjetima zapošljavanja dodijeljene tijelu nadležnom za sklapanje ugovora o radu („ovlasti tijela za imenovanja”).

3. Upravni odbor u skladu s člankom 110. Pravilnika o osoblju donosi odluku, na temelju članka 2. stavka 1. Pravilnika o osoblju i članka 6. Uvjeta zaposlenja, kojom se odgovarajuće ovlasti tijela za imenovanja delegiraju izvršnom direktoru i kojom se utvrđuju uvjeti pod kojima se to delegiranje ovlasti može suspendirati. Izvršni direktor ovlašten je dalje prenijeti te ovlasti.

---

30 Uredba Vijeća (Euratom, EZ) br. 2185/96 od 11. studenoga 1996. o provjerama i inspekcijama na terenu koje provodi Komisija s ciljem zaštite financijskih interesa Europskih zajednica od prijevara i ostalih nepravilnosti (SL L 292, 15.11.1996., str. 2.).

31 Uredba (EU, Euratom) br. 883/2013 Europskog parlamenta i Vijeća od 11. rujna 2013. o istragama koje provodi Europski ured za borbu protiv prijevara (OLAF) i stavljanju izvan snage Uredbe (EZ) br. 1073/1999 Europskog parlamenta i Vijeća te Uredbe Vijeća (Euratom) br. 1074/1999 (SL L 248, 18.9.2013., str. 1.).

32 Uredba (EEZ, Euratom, EZUČ) br. 259/68 Vijeća od 29. veljače 1968. kojom se utvrđuje Pravilnik o osoblju za dužnosnike i Uvjeti zaposlenja ostalih službenika Europskih zajednica i kojom se uvode posebne mjere koje se privremeno primjenjuju na dužnosnike Komisije (SL L 56, 4.3.1968., str. 1.).

4. U izvanrednim okolnostima Upravni odbor može donijeti odluku o privremenoj obustavi delegiranja ovlasti tijela za imenovanja izvršnom direktoru i bilo kakvog daljnjeg delegiranja tih ovlasti od strane izvršnog direktora. U takvim slučajevima Upravni odbor samostalno izvršava ovlasti tijela za imenovanja ili ih delegira jednom od svojih članova ili članu osoblja Centra za stručnost koji nije izvršni direktor.

5. Upravni odbor donosi provedbena pravila za Pravilnik o osoblju i Uvjete zaposlenja, u skladu s člankom 110. Pravilnika o osoblju.

6. Broj zaposlenika utvrđuje se u planu radnih mjesta Centra za stručnost, u kojem se navodi broj privremenih radnih mjesta po funkcijskoj grupi i platnom razredu te broj ugovornog osoblja iskazan ekvivalentima punog radnog vremena u skladu s njegovim godišnjim proračunom.

7. Osoblje Centra za stručnost sastoji se od privremenih i ugovornih djelatnika.

8. Sve troškove povezane s osobljem snosi Centar za stručnost.

Članak 32.

Upućeni nacionalni stručnjaci i drugo osoblje

1. Centar za stručnost može angažirati upućene nacionalne stručnjake i drugo osoblje koje nije zaposleno u Centru za stručnost.

2. Upravni odbor u dogovoru s Komisijom donosi odluku kojom utvrđuje pravila o upućivanju nacionalnih stručnjaka u Centar za stručnost.

Članak 33.

Povlastice i imuniteti

Protokol br.7 o povlasticama i imunitetima Europske unije priložen Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije primjenjuje se na Centar za stručnost i njegovo osoblje.

POGLAVLJE V.
ZAJEDNIČKE ODREDBE

Članak 34.

Sigurnosna pravila

1. Na sudjelovanje u svim mjerama koje financira Centar za stručnost primjenjuje se članak 12. stavak 7. Uredbe (EU) br. XXX [program Digitalna Europa].

2. Sljedeća posebna sigurnosna pravila primjenjuju se na mjere koje se financiraju iz programa Obzor Europa:

   (a) za potrebe članka 34. stavka 1. [Vlasništvo i zaštita] Uredbe (EU) br. XXX [Obzor Europa], kada je to predviđeno u planu rada, dodjela neisključivih licencija može biti ograničena na treće strane koje imaju poslovni nastan ili za koje se smatra da imaju poslovni nastan u državama članicama i koje su pod kontrolom država članica i/ili državljana država članica;

   (b) za potrebe članka 36. stavka 4. točke (b) [Prijenos i licenciranje] Uredbe (EU) br. XXX [Obzor Europa], prijenos licencije na pravnu osobu s poslovnim

nastanom u pridruženoj zemlji ili u Uniji, ali pod kontrolom trećih zemalja, također je osnova za prigovor na prijenos vlasništva nad rezultatima ili na dodjelu isključive licencije u pogledu rezultata;

(c) za potrebe članka 37. stavka 3. točke (a) [Prava pristupa] Uredbe (EU) br. XXX [Obzor Europa], kada je to predviđeno u planu rada, odobravanje pristupa rezultatima i postojećem znanju može biti ograničena samo na pravnu osobu koja ima poslovni nastan ili za koju se smatra da ima poslovni nastan u državama članicama i koja je pod kontrolom država članica i/ili državljana država članica.

Članak 35.

Transparentnost

1. Centar za stručnost obavlja svoje zadaće uz visok stupanj transparentnosti.
2. Centar za stručnost osigurava da javnost i sve zainteresirane strane dobiju odgovarajuće, objektivne, pouzdane i lako dostupne informacije, posebno u pogledu rezultata njegova rada. Centar objavljuje i izjave o interesima dane u skladu s člankom 41.
3. Upravni odbor može na prijedlog izvršnog direktora zainteresiranim stranama odobriti da u svojstvu promatrača sudjeluju u određenim aktivnostima Centra za stručnost.
4. Centar za stručnost utvrđuje u svojem poslovniku praktična rješenja za provedbu pravila o transparentnosti iz stavaka 1. i 2. U pogledu mjera koje se financiraju iz Obzora Europa uzet će se u obzir odredbe iz Priloga III. Uredbe o Obzoru Europa.

Članak 36.

Sigurnosna pravila za zaštitu klasificiranih i osjetljivih neklasificiranih podataka

1. Ne dovodeći u pitanje članak 35., Centar za stručnost trećim stranama ne otkriva informacije koje obrađuje ili prima, a za koje je podnesen opravdan zahtjev da s njima djelomično ili u cijelosti postupa kao s povjerljivim informacijama.
2. Članovi Upravnog odbora, izvršni direktor, članovi Industrijskog i znanstvenog savjetodavnog odbora, vanjski stručnjaci koji sudjeluju u radu *ad hoc* radnih skupina i članovi osoblja Centra, poštuju zahtjeve u pogledu povjerljivosti iz članka 339. Ugovora o funkcioniranju Europske unije, čak i nakon što prestanu obavljati svoje dužnosti.
3. Upravni odbor Centra za stručnost donosi sigurnosna pravila Centra za stručnost, nakon odobrenja Komisije, na temelju načela i pravila utvrđenih u sigurnosnim pravilima Komisije za zaštitu klasificiranih podataka Europske unije (EUCI) i osjetljivih neklasificiranih podataka, uključujući, među ostalim, odredbe za obradu i pohranu takvih podataka kako je utvrđeno u Odlukama Komisije (EU, Euratom) 2015/443[33] i 2015/444[34].

[33] Odluka Komisije (EU, Euratom) 2015/443 od 13. ožujka 2015. o sigurnosti u Komisiji (SL L 72, 17.3.2015., str. 41.).

[34] Odluka Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 72, 17.3.2015., str. 53.).

4. Centar za stručnost može poduzeti sve potrebne mjere kako bi olakšao razmjenu informacija relevantnih za njezine zadaće s Komisijom i državama članicama te prema potrebi s relevantnim agencijama i tijelima Unije. Za svaki administrativni sporazum sklopljen u tu svrhu o razmjeni EUCI-ja ili, ako nema takvog sporazuma, za svako iznimno *ad hoc* objavljivanje EUCI-ja potrebno je prethodno odobrenje Komisije.

Članak 37.

Pristup dokumentima

1. Na dokumente koje čuva Centar za stručnost primjenjuje se Uredba (EZ) br. 1049/2001.
2. Upravni odbor donosi pravila za provedbu Uredbe (EZ) br. 1049/2001 u roku od šest mjeseci od osnivanja Centra za stručnost.
3. Protiv odluka koje Centar za stručnost donosi u skladu s člankom 8. Uredbe (EZ) br. 1049/2001 može se podnijeti pritužba Europskom ombudsmanu u skladu s člankom 228. Ugovora o funkcioniranju Europske unije ili tužba Sudu Europske unije u skladu s člankom 263. Ugovora o funkcioniranju Europske unije.

Članak 38.

Praćenje, evaluacija i preispitivanje

1. Centar za stručnost osigurava trajno i sustavno praćenje i povremenu evaluaciju svojeg rada, uključujući aktivnosti kojima upravljaju nacionalni koordinacijski centri i Mreža. Centar za stručnost osigurava učinkovito, djelotvorno i pravodobno prikupljanje podataka za praćenje provedbe programa i rezultata te se primateljima sredstava Unije i državama članicama određuju razmjerni zahtjevi za izvješćivanje. Rezultati evaluacije objavljuju se.
2. Kada su dostupne dostatne informacije o provedbi ove Uredbe, ali najkasnije tri i pol godine nakon početka provedbe ove Uredbe, Komisija provodi privremenu evaluaciju Centra za stručnost. Komisija izrađuje izvješće o toj evaluaciji i podnosi ga Europskom parlamentu i Vijeću do 31. prosinca 2024. Centar za stručnost i države članice dostavljaju Komisiji sve potrebne informacije za izradu tog izvješća.
3. Evaluacija iz stavka 2. uključuje ocjenu rezultata koje je ostvario Centar za stručnost, uzimajući u obzir njegove ciljeve, mandat i zadaće. Ako Komisija smatra da je daljnje djelovanje Centra za stručnost opravdano s obzirom na dodijeljene ciljeve, mandat i zadaće, ona može predložiti produljenje trajanja mandata Centra za stručnost utvrđenog u članku 46.
4. Na temelju zaključaka privremene evaluacije iz stavka 2. Komisija može djelovati u skladu s [člankom 22. stavkom 5.] ili poduzeti druge prikladne mjere.
5. Praćenje, evaluacija, postupno smanjivanje i obnova doprinosa iz Obzora Europa provodit će se u skladu s odredbama članaka 8., 45. i 47. Priloga III. Uredbi o Obzoru Europa i s dogovorenim načinima provedbe.
6. Praćenje, izvješćivanje i evaluacija doprinosa iz programa Digitalna Europa provodit će se u skladu s odredbama članaka 24. i 25. programa Digitalna Europa.
7. U slučaju likvidacije Centra za stručnost, Komisija provodi njegovu završnu evaluaciju u roku od šest mjeseci od likvidacije, a najkasnije dvije godine nakon

pokretanja likvidacijskog postupka iz članka 46. ove Uredbe. Rezultati te završne evaluacije dostavljaju se Europskom parlamentu i Vijeću.

Članak 39.

Odgovornost Centra za stručnost

1. Ugovorna odgovornost Centra za stručnost uređena je pravom koje se primjenjuje na predmetni sporazum, odluku ili ugovor.
2. U slučaju izvanugovorne odgovornosti, Centar za stručnost, u skladu s općim načelima koja su zajednička zakonima država članica, nadoknađuje svu štetu koju uzrokuje njegovo osoblje pri obavljanju svojih dužnosti.
3. Sva plaćanja Centra za stručnost u vezi s odgovornostima iz stavaka 1. i 2. te s time povezani troškovi i izdaci smatraju se rashodima Centra za stručnost i pokrivaju se iz njegovih sredstava.
4. Centar za stručnost isključivo je odgovoran za ispunjavanje svojih obveza.

Članak 40.

Nadležnost Suda Europske unije i mjerodavno pravo

1. Sud Europske unije nadležan je:
   (1) u skladu s odredbom o arbitraži sadržanom u sporazumima, odlukama ili ugovorima koje je sklopio Centar za stručnost;
   (2) za sporove povezane s nadoknadama za štete koje je osoblje Centra za stručnost uzrokovalo pri obavljanju svojih dužnosti;
   (3) u svim sporovima između Centra za stručnost i njegova osoblja u okvirima i uz uvjete utvrđene u Pravilniku o osoblju.
2. Na sva pitanja koja nisu obuhvaćena ovom Uredbom ili drugim pravnim aktima Unije primjenjuje se pravo države članice kojoj se nalazi sjedište Centra za stručnost.

Članak 41.

Odgovornost članova i osiguranje

1. Financijska odgovornost članova za dugove Centra za stručnost ograničava se na njihove već dane doprinose za pokrivanje administrativnih troškova.
2. Centar za stručnost ugovara i održava odgovarajuće osiguranje.

Članak 42.

Sukob interesa

Upravni odbor Centra za stručnost donosi pravila za sprečavanje sukoba interesa svojih članova, tijela i zaposlenika te za postupanje u slučajevima sukoba interesa. Ta pravila sadržavaju odredbe kojima se nastoji spriječiti sukob interesa u pogledu predstavnika članova

koji sudjeluju u Upravnom odboru te u Industrijskom i znanstvenom savjetodavnom odboru u skladu s Uredbom XXX [nova Financijska uredba].

Članak 43.

Zaštita osobnih podataka

1. Centar za stručnost obrađuje osobne podatke u skladu s Uredbom (EU) br. XXX/2018 Europskog parlamenta i Vijeća.
2. Upravni odbor donosi provedbene mjere iz članka xx. stavka 3. Uredbe (EZ) br. XXX/2018. Upravni odbor može donijeti dodatne mjere koje su potrebne kako bi Centar za stručnost primjenjivao Uredbu (EZ) br. 45/2018.

Članak 44.

Potpora države članice domaćina

Može se sklopiti administrativni sporazum između Centra za stručnost i države članice [Belgija] u kojoj se nalazi njegovo sjedište o povlasticama i imunitetima i drugim oblicima potpore koju ta država članica osigurava Centru za stručnost.

POGLAVLJE VII.

ZAVRŠNE ODREDBE

Članak 45.

Početne aktivnosti

1. Komisija je odgovorna za osnivanje i početno djelovanje Centra za stručnost dok on stekne operativnu sposobnost za provedbu svojeg proračuna. U skladu s pravom Unije Komisija provodi sve nužne radnje uz pomoć nadležnih tijela Centra za stručnost.
2. Za potrebe stavka 1., Komisija može imenovati privremenog izvršnog direktora i obavljati dužnosti dodijeljene izvršnom direktoru uz pomoć određenog broja dužnosnika Komisije, sve dok izvršni direktor ne preuzme svoje dužnosti nakon što ga Upravni odbor imenuje u skladu s člankom 16. Komisija može privremeno premjestiti određeni broj svojih službenika.
3. Privremeni izvršni direktor može, nakon odobrenja Upravnog odbora, odobravati sva plaćanja koja su obuhvaćena odobrenim sredstvima iz godišnjeg proračuna Centra za stručnost te sklapati sporazume, odluke i ugovore, uključujući ugovore s osobljem nakon što Centar za stručnost donese plan radnih mjesta.
4. Privremeni izvršni direktor određuje, u dogovoru s izvršnim direktorom Centra za stručnost i uz suglasnost Upravnog odbora, datum od kojeg će Centar za stručnost imati sposobnost za provedbu vlastitog proračuna. Od tog datuma nadalje Komisija više ne preuzima obveze i ne izvršava plaćanja za aktivnosti Centra za stručnost.

Članak 46.

Trajanje

1. Centar za stručnost osniva se na razdoblje od 1. siječnja 2021. do 31. prosinca 2029.
2. Na kraju tog razdoblja, osim ako se nakon revizije ove Uredbe donese drugačija odluka, pokreće se likvidacijski postupak. Likvidacijski postupak pokreće se automatski ako se Unija ili sve države članice sudionice povuku iz Centra za stručnost.
3. Za potrebe provedbe postupka likvidacije Centra za stručnost, Upravni odbor imenuje jednog ili više likvidatora koji poštuju odluke Upravnog odbora.
4. Pri likvidaciji Centra za stručnost njegova se imovina koristi za podmirivanje njegovih obveza i rashoda povezanih s likvidacijom. Sav višak raspodjeljuje se između Unije i država članica sudionica razmjerno njihovom financijskom doprinosu Centru za stručnost. Svaki višak koji se dodijeli Uniji vraća se u proračun Unije.

Članak 47.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu,

Za Europski parlament	*Za Vijeće*
Predsjednik	*Predsjednik*

ZAKONODAVNI FINANCIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

1.2. Odgovarajuća područja politike u strukturi ABM/ABB

1.3. Vrsta prijedloga/inicijative

1.4. Cilj/ciljevi

1.5. Osnova prijedloga/inicijative

1.6. Trajanje i financijski učinak

1.7. Predviđene metode upravljanja

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

2.2. Sustav upravljanja i kontrole

2.3. Mjere za sprečavanje prijevara i nepravilnosti

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunskih linija rashoda na koje se prijedlog/inicijativa odnosi

3.2. Procijenjeni učinak na rashode

3.2.1. Sažetak procijenjenog učinka na rashode

3.2.2 Procijenjeni učinak na odobrena sredstva za poslovanje

3.2.3. Procijenjeni utjecaj na odobrena administrativna sredstva

3.2.4. Usklađenost s važećim višegodišnjim financijskim okvirom

3.2.5. Doprinosi trećih strana

3.3. Procijenjeni utjecaj na prihode

ZAKONODAVNI FINANCIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

Uredba o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije

1.2. Odgovarajuća područja politike u strukturi ABM/ABB[35]

Istraživanje i inovacije

Europska strateška ulaganja

1.3. Vrsta prijedloga/inicijative

☒ Prijedlog/inicijativa odnosi se na **novo djelovanje**

☐ Prijedlog/inicijativa odnosi se na **novo djelovanje nakon pilot-projekta/pripremnog djelovanja**[36]

☐ Prijedlog/inicijativa odnosi se na **produženje postojećeg djelovanja**

☐ Prijedlog/inicijativa odnosi se na **djelovanje koje je preusmjereno na novo djelovanje**

1.4. Cilj/ciljevi

1.4.1. Višegodišnji strateški ciljevi Komisije na koje se odnosi prijedlog/inicijativa

1. Povezano jedinstveno digitalno tržište

2. Novi poticaj za zapošljavanje, rast i ulaganja

1.4.2. Posebni cilj/ciljevi

Posebni ciljevi

1.3. Digitalno gospodarstvo može se potpuno razviti uz potporu inicijativa kojima se potiče potpuni rast digitalnih i podatkovnih tehnologija.

2.1. Europa zadržava svoj položaj svjetskog predvodnika u digitalnom gospodarstvu ako se europska poduzeća mogu širiti na globalnoj razini na temelju snažnog digitalnog poduzetništva i uspješnih novoosnovanih poduzeća i ako industrija i javne usluge uspješno provedu digitalnu transformaciju.

2.2. Europsko istraživanje pronalazi prilike za ulaganja za mogući tehnološki napredak i nova rješenja, posebno u okviru programa Obzor 2020./Obzor Europa i uporabom javno-privatnih partnerstava.

[35] ABM: upravljanje po djelatnostima; ABB: priprema proračuna na temelju aktivnosti.

[36] Kako je navedeno u članku 54. stavku 2. točkama (a) ili (b) Financijske uredbe.

1.4.3. Očekivani rezultat/rezultati i utjecaj

Navesti učinke koje bi prijedlog/inicijativa trebali imati na ciljane korisnike/skupine.

Centar za stručnost nastojat će, zajedno s Mrežom i Zajednicom, ostvariti sljedeće ciljeve:

(1) pridonijeti provedbi programa Digitalna Europa uspostavljenog Uredbom br. XXX u dijelu koji se odnosi na kibersigurnost, a posebno mjera povezanih s člankom 6. Uredbe (EU) br. XXX [Program Digitalna Europa], programa Obzor Europa uspostavljenog Uredbom br. XXX, a posebno odjeljka 2.2.6. Priloga I. Odluci br. XXX o uspostavi posebnog programa za provedbu Obzora Europa – Okvirnog programa za istraživanje i inovacije [referentni broj posebnog programa] te drugih programa Unije kada je tako predviđeno u pravnim aktima Unije;

(2) jačati sposobnosti, znanje i infrastrukture u području kibersigurnosti u službi industrija, javnog sektora i istraživačkih zajednica;

(3) pridonijeti uporabi najnovijih proizvoda i rješenja za kibersigurnost u cijelom gospodarstvu;

(4) poboljšati razumijevanje kibersigurnosti i pridonijeti smanjenju manjka vještina u Uniji u području kibersigurnosti;

(5) pridonijeti jačanju istraživanja i razvoja u području kibersigurnosti u Uniji;

(6) jačati suradnju između civilnog i obrambenog sektora u pogledu tehnologija za dvojnu uporabu i primjenu;

(7) jačati sinergiju između civilne i obrambene dimenzije kibersigurnosti;

(8) pomagati u koordinaciji i olakšavanju rada Mreže nacionalnih koordinacijskih centara („Mreža”) iz članka 10. i Zajednice stručnjaka za kibersigurnost iz članka 12.

1.4.4. Pokazatelji rezultata i utjecaja

Navesti pokazatelje koji omogućuju praćenje provedbe prijedloga/inicijative.

· broj infrastruktura/alata za kibersigurnost nabavljenih zajedničkom javnom nabavom,

· pristup vremenu za testiranje i eksperimentiranje omogućen europskim istraživačima i industriji u cijeloj Mreži i unutar Centra. Kada objekti već postoje, veći broj sati dostupan tim zajednicama u odnosu na trenutačno dostupan broj sati,

· broj zajednica korisnika kojima se pružaju usluge i broj istraživača koji su dobili pristup europskim instrumentima za kibersigurnost u odnosu na broj onih koji moraju takve resurse tražiti izvan Europe,

· povećava se konkurentnost europskih dobavljača mjerena na temelju globalnog tržišnog udjela (ciljni tržišni udio od 25 % do 2027.) i na temelju udjela rezultata europskih istraživanja i razvoja koje je preuzela industrija,

· doprinos sljedećim tehnologijama u području kibersigurnosti koji se mjeri brojem autorskih prava, patenata, znanstvenih publikacija i komercijalnih proizvoda,

· broj kurikuluma vještina za kibersigurnost koji su ocijenjeni i usklađeni, broj ocijenjenih profesionalnih programa za kibersigurnosnu certifikaciju,

· broj osposobljenih znanstvenika, studenata, korisnika (industrijskih i javnih uprava).

1.5. Osnova prijedloga/inicijative

1.5.1. Zahtjev/zahtjevi koje je potrebno kratkoročno ili dugoročno ispuniti

Ostvariti kritičnu masu ulaganja u tehnološki i industrijski razvoj u području kibersigurnosti i u prevladavanje fragmentiranosti relevantnih sposobnosti raširenih diljem EU-a.

1.5.2. Dodana vrijednost sudjelovanja EU-a

Kibersigurnost je pitanje od zajedničkog interesa za Uniju, što je potvrđeno u prethodno navedenim Zaključcima Vijeća. To je pokazao opseg i prekogranični karakter incidenata kao što su *WannaCry* ili *NonPetya*. Zbog prirode i opsega kibersigurnosnih tehnoloških izazova i nedostatne koordinacije napora unutar industrije i među industrijama, javni sektor i istraživačke zajednice traže od EU-a da dodatno podupire koordinacijske napore u cilju udruživanja kritične mase sredstava i osiguranja boljeg znanja i upravljanja imovinom. To je potrebno zbog zahtjeva za sredstvima povezanima s određenim sposobnostima za istraživanje, razvoj i primjenu u području kibersigurnosti, potrebe za pružanjem pristupa interdisciplinarnom znanju i iskustvu o kibersigurnosti u različitim disciplinama (koje je često samo djelomično dostupno na nacionalnoj razini), globalne prirode industrijskih vrijednosnih lanaca i aktivnosti globalnih konkurenata koji djeluju na različitim tržištima.

Za to su potrebna sredstva i stručno znanje koji se ne mogu ostvariti pojedinačnim djelovanjem pojedinih država članica. Na primjer, za paneuropsku kvantnu komunikacijsku mrežu mogla bi biti potrebna ulaganja EU-a od približno 900 milijuna EUR, ovisno o ulaganjima država članica (koje treba međusobno povezati/dopuniti) te o tome u kojoj će mjeri tehnologija omogućiti ponovnu uporabu postojećih infrastruktura.

1.5.3. Pouke iz prijašnjih sličnih iskustava

Evaluacija programa Obzor 2020. na sredini programskog razdoblja potvrdila je, među ostalim, trajnu relevantnost potpore EU-a istraživanju i razvoju i društvenim izazovima (uključujući „Sigurna društva” iz kojeg se podupire istraživanje i razvoj u području kibersigurnosti). Evaluacijom je istodobno potvrđeno da je i dalje teško jačati vodstvo u industriji te da i dalje postoji jaz inovacija i EU zaostaje prema ključnim inovacijama kojima se stvaraju tržišta.

Čini se da je evaluacija na sredini provedbenog razdoblja Instrumenta za povezivanje Europe (CEF) potvrdila dodanu vrijednost intervencije EU-a koja ne uključuje samo istraživanje i razvoj, iako je kibersigurnost u okviru CEF-a imala drugačije usmjerenje (na operativnu sigurnost) i intervencijsku logiku. Istodobno je većina primatelja bespovratnih sredstava CEF-a za kibersigurnost – zajednica nacionalnih CSIRT-ova – izrazila želju za ugovorenim programom potpore u okviru sljedećeg VFO-a.

Osnivanje javno-privatnog partnerstva za kibersigurnost („JPP za kibersigurnost”) u Uniji 2016. bilo je prvi čvrst korak prema okupljanju istraživačke zajednice, industrije i javnog sektora u cilju olakšavanja istraživanja i inovacija u području kibersigurnosti te bi, unutar ograničenja financijskog okvira za razdoblje 2014.–2020., trebalo dovesti do dobrih, usmjerenijih rezultata u području istraživanja i inovacija. JPP za kibersigurnost omogućio je partnerima u industriji da se obvežu na pojedinačnu potrošnju u područjima definiranima u strateškom programu istraživanja i inovacija tog partnerstva.

1.5.4. Usklađenost i moguća sinergija s drugim odgovarajućim instrumentima

Mreža centara za stručnost u području kibersigurnosti i Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja dodatno će podupirati postojeće odredbe politike kibersigurnosti i zainteresirane strane u tom području. Mandat Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja dopunjavat će napore ENISA-e, ali ima drugačije usmjerenje i zahtijeva različiti skup vještina. Dok ENISA sudjeluje u pružanju savjeta u okviru istraživanja i inovacija u području kibersigurnosti u EU-u, njezin predloženi mandat usredotočen je u prvom redu na druge zadaće koje su od ključne važnosti za jačanje kiberotpornosti u EU-u. Centar bi trebao poticati razvoj i primjenu tehnologije u području kibersigurnosti i dopunjavati napore jačanja kapaciteta u tom području na razini EU-a i nacionalnoj razini.

Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreža centara za stručnost u području kibersigurnosti podupirat će i istraživanja usmjerena na olakšavanje i ubrzavanje postupaka standardizacije i certifikacije, posebno onih povezanih s programima kibersigurnosne certifikacije u smislu Akta o kibersigurnosti.

Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja djelovat će kao jedinstveni provedbeni mehanizam za dva europska programa kojima se podupire kibersigurnost (program Digitalna Europa i Obzor Europa) te će jačati dosljednosti i sinergiju među njima.

Ova inicijativa omogućuje dopunu napora država članica pružanjem odgovarajućih informacija stvarateljima obrazovne politike u cilju jačanja obrazovanja iz kibersigurnosti (npr. razvojem kurikuluma za kibersigurnost u civilnim i vojnim obrambenim sustavima, ali i ulazne informacije za osnovno obrazovanje iz kibersigurnosti). Ona bi omogućila i podupiranje usklađivanja i trajnog ocjenjivanja profesionalnih programa za kibersigurnosnu certifikaciju – sve aktivnosti koje su potrebne kako bi se omogućilo zatvaranje jaza u vještinama kibersigurnosti i olakšao pristup industrija i drugih zajednica stručnjacima za kibersigurnost. Usklađivanjem obrazovanja i vještina pomoći će se u razvoju kvalificirane radne snage za kibersigurnost u EU-u – ključnog čimbenika za trgovačka društva u području kibersigurnosti i druge industrije s interesom za kibersigurnost.

1.6. Trajanje i financijski učinak

☒ Prijedlog/inicijativa **ograničenog trajanja**

– ☒ Prijedlog/inicijativa na snazi od 1.1.2021. do 31.12.2029.

– ☒ Financijski učinak od 2021. do 2027. za odobrena sredstva za preuzete obveze i od 2021. do 2031. za odobrena sredstva za plaćanje.

☐ Prijedlog/inicijativa **neograničenog trajanja**

– provedba s početnim razdobljem od GGGG. do GGGG.,

– nakon čega slijedi redovna provedba.

1.7. Predviđeni načini upravljanja[37]

☐ **Izravno upravljanje** koje provodi Komisija

– ☐ putem svojih službi, uključujući osoblje u delegacijama Unije;

– ☐ putem izvršnih agencija

☐ **Podijeljeno upravljanje** s državama članicama

☒

Neizravno upravljanje povjeravanjem zadaća izvršenja proračuna

– ☐ trećim zemljama ili tijelima koja su one odredile;

– ☐ međunarodnim organizacijama i njihovim agencijama (navesti);

– ☐ EIB-u i Europskom investicijskom fondu;

– ☒ tijelima iz članaka 70. i 71. Financijske uredbe;

– ☐ tijelima javnog prava;

– ☐ tijelima uređenima privatnim pravom koja pružaju javne usluge u mjeri u kojoj daju odgovarajuća financijska jamstva;

– ☐ tijelima uređenima privatnim pravom države članice kojima je povjerena provedba javno-privatnog partnerstva i koja daju odgovarajuća financijska jamstva;

– ☐ osobama kojima je povjerena provedba određenih djelovanja u području ZVSP-a u skladu s glavom V. UEU-a i koje su navedene u odgovarajućem temeljnom aktu.

– *Ako je označeno više načina upravljanja, pojedinosti navesti u odjeljku „Napomene”.*

[37] Informacije o načinima upravljanja i upućivanja na Financijsku uredbu dostupni su na internetskim stranicama BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

Navesti učestalost i uvjete.

Članak 28. sadržava detaljne odredbe o praćenju i izvješćivanju.

2.2. Sustav upravljanja i kontrole

2.2.1. Utvrđeni rizik/rizici

Kako bi ublažila rizike povezane s radom Centra za stručnost nakon njegove uspostave i kašnjenja, Komisija će tijekom te faze podupirati Centar za stručnost kako bi osigurala brzo zapošljavanje ključnog osoblja i uspostavu učinkovitog sustava unutarnje kontrole i pouzdanih postupaka.

2.2.2. Informacije o uspostavljenom sustavu unutarnje kontrole

Izvršni direktor odgovoran je za rad Centra za stručnost i svakodnevno upravljanje njime i njegov je zakonski zastupnik. Direktor je odgovoran Upravnom odboru i kontinuirano ga izvješćuje o razvoju aktivnosti Centra za stručnost.

Upravni odbor u cijelosti je odgovoran za strateško usmjerenje i rad Centra za stručnost te nadzire provedbu njegovih aktivnosti.

Financijska pravila koja se primjenjuju na Centar za stručnost donosi Upravni odbor nakon savjetovanja s Komisijom. Ona ne odstupaju od Uredbe (EU) br. 1271/2013, osim ako je to odstupanje posebno potrebno za rad Centra za stručnost i ako je Komisija prethodno dala suglasnost.

Unutarnji revizor Komisije ima jednake ovlasti nad Centrom za stručnost kao što ih ima u odnosu na Komisiju. Revizorski sud ima ovlasti provoditi reviziju, na temelju dokumenata i na terenu, svih korisnika bespovratnih sredstava, ugovaratelja i podugovaratelja koji su primili sredstva Unije od Centra za stručnost.

2.2.3. Procjena troškova i koristi kontrola i ocjena očekivane razine rizika od pogreške

Troškovi i koristi kontrola

Troškovi kontrole Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja podijeljeni su između troška nadzora na razini Komisije i troška operativnih kontrola na razini provedbenog tijela.

Procjenjuje se da trošak kontrola na razini Centra za stručnost iznosi otprilike 1,19 % operativnih odobrenih sredstava za plaćanje provedenih na razini Centra za stručnost.

Procjenjuje se da trošak nadzora na razini Komisije iznosi otprilike 1,20 % operativnih odobrenih sredstava za plaćanje provedenih na razini Centra za stručnost.

Pod pretpostavkom da bi aktivnostima u potpunosti upravljala Komisija bez pomoći provedbenog tijela, trošak kontrole bio bi znatno veći i mogao bi iznositi približno 7,7 % odobrenih sredstava za plaćanje.

Predviđene kontrole imaju za cilj osigurati Komisijin neometan i učinkovit nadzor provedbenih tijela te osigurati potreban stupanj jamstva na razini Komisije.

Koristi kontrola jesu sljedeće:

— izbjegavanje odabira lošijih ili neodgovarajućih prijedloga,

— optimiziranje planiranja i uporabe sredstava EU-a kako bi se sačuvala dodana vrijednost EU-a,

— osiguravanje kvalitete sporazumâ o dodjeli bespovratnih sredstava, izbjegavanje pogrešaka pri utvrđivanju pravnih subjekata, osiguravanje ispravnog izračuna doprinosa EU-a i prihvaćanja potrebnih jamstava za ispravne operacije bespovratnih sredstava,

— otkrivanje neprihvatljivih troškova u fazi plaćanja.

— otkrivanje pogrešaka koje utječu na zakonitost i pravilnost operacija u fazi revizije.

Procijenjena stopa pogreške

Cilj je zadržati stopu preostale pogreške ispod praga od 2 % za cijeli program te istodobno ograničiti opterećenje u pogledu kontrole za korisnike kako bi se postigla prava ravnoteža između cilja zakonitosti i pravilnosti i drugih ciljeva kao što su privlačnost programa osobito za MSP-ove i troškova kontrola.

2.3. Mjere za sprečavanje prijevara i nepravilnosti

Navesti postojeće ili predviđene mjere za sprečavanje i zaštitu.

OLAF može provoditi istrage, među ostalim provjere i inspekcije na terenu, u skladu s odredbama i postupcima propisanima Uredbom br. 883/2013 Europskog parlamenta i Vijeća i Uredbom Vijeća (Euratom, EZ) br. 2185/9640 od 11. studenoga 1996. o provjerama i inspekcijama na terenu koje provodi Komisija s ciljem zaštite financijskih interesa Europskih zajednica od prijevara i ostalih nepravilnosti kako bi utvrdio je li došlo do prijevare, korupcije ili bilo koje druge nezakonite aktivnosti koja utječe na financijske interese Unije u vezi s bespovratnim sredstvima ili ugovorom koji financira Agencija.

Sporazumi, odluke i ugovori koji proizlaze iz provedbe ove Uredbe sadržavaju odredbe kojima se Komisija, Centar za stručnost, Revizorski sud i OLAF izričito ovlašćuju za obavljanje revizija i provedbu istraga u skladu sa svojim mjerodavnim nadležnostima.

Centar za stručnost osigurava odgovarajuću zaštitu financijskih interesa svojih članova provedbom ili naručivanjem provedbe odgovarajućih unutarnjih i vanjskih kontrola.

Centar za stručnost pristupa Međuinstitucijskom sporazumu od 25. svibnja 1999. između Europskog parlamenta, Vijeća Europske unije i Komisije Europskih zajednica u pogledu unutarnjih istraga Europskog ureda za borbu protiv prijevara (OLAF). Centar za stručnost donosi mjere potrebne za lakšu provedbu unutarnjih istraga koje provodi OLAF.

Centar za stručnost donosi strategiju za borbu protiv prijevara na temelju analize rizika od prijevara i razmatranja troškova i koristi. On štiti financijske interese Unije primjenom preventivnih mjera za borbu protiv prijevara, korupcije i drugih nezakonitih aktivnosti, izvršavanjem djelotvornih provjera i, ako se otkriju

nepravilnosti, povratom nepropisno isplaćenih iznosa i, prema potrebi, izricanjem djelotvornih, razmjernih i odvraćajućih administrativnih i novčanih kazni.

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslov višegodišnjeg financijskog okvira i predložene nove proračunske linije rashoda

- Zatražene nove proračunske linije

  Prema redoslijedu naslova višegodišnjeg financijskog okvira i proračunskih linija:

Naslov višegodišnjeg financijskog okvira:	Proračunska linija	Vrsta rashoda	Doprinos			
	Broj	Diff./Nedif.[38].	zemalja EFTA-e[39]	zemalja kandidatkinja[40]	trećih zemalja	u smislu članka [21. stavka 2. točke (b) Financijske uredbe
Naslov 1.: Jedinstveno tržište, inovacije i digitalno gospodarstvo	01 02 XX XX Obzor Europa Centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja – potpora rashodima 01 02 XX XX Obzor Europa Centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja 02 06 01 XX program Digitalna Europa Centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja – potpora rashodima 02 06 01 XX program Digitalna Europa Centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja	Dif.	DA	DA (ako je navedeno u godišnjem programu rada)	DA (ograničeno na određeni dio programa)	NE

[38] Dif. = diferencirana odobrena sredstva; Nedif. = nediferencirana odobrena sredstva.

[39] EFTA: Europsko udruženje slobodne trgovine.

[40] Zemlje kandidatkinje i, ako je primjenjivo, potencijalni kandidati sa zapadnog Balkana.

- Očekuje se da će se doprinos za ovu proračunsku liniju osigurati iz:

u milijunima EUR (do tri decimalna mjesta)

Proračunska linija	Godina 2021.	Godina 2022.	Godina 2023.	Godina 2024.	Godina 2025.	Godina 2026.	Godina 2027.	**Ukupno**
01 01 01 01 Rashodi povezani sa službenicima za istraživanje, privremenim djelatnicima – Obzor Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Vanjsko osoblje koje provodi istraživačke programe – Obzor Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Ostali rashodi upravljanja za istraživanje – Obzor Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Globalni izazovi i industrijska konkurentnost	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Administrativna potpora – program Digitalna Europa	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Kibersigurnost – program Digitalna Europa	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Ukupni rashodi	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Doprinos iz financijske omotnice za klaster „Uključivo i sigurno društvo” stupa II. „Globalni izazovi i industrijska konkurentnost” programa Obzor Europa (ukupna omotnica od 2 800 000 000 EUR) iz članka 21. stavka 1. točke (b) predložit će Komisija tijekom zakonodavnog postupka, a u svakom slučaju prije postizanja političkog dogovora. Prijedlog će se temeljiti na rezultatima postupka strateškog planiranja kako je definirano u članku 6. stavku 6. Uredbe XXX [okvirni program Obzor Europa].

Navedeni iznosi ne uključuju doprinos država članica operativnim i administrativnim troškovima Centra za stručnost koji su razmjeni financijskom doprinosu Unije.

3.2. Procijenjeni učinak na rashode

3.2.1. Sažetak procijenjenog učinka na rashode

u milijunima EUR (do tri decimalna mjesta)

Naslov višegodišnjeg financijskog okvira	**1**	Jedinstveno tržište, inovacije i digitalno gospodarstvo

			2021.[41]	**2022.**	**2023.**	**2024.**	**2025.**	**2026.**	**2027.**	***Nakon 2027.***	**UKUPNO**
Naslov 1. (Rashodi za osoblje)	Obveze = plaćanja	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Naslov 2. (Rashodi za infrastrukturu i poslovanje)	Obveze = plaćanja	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Naslov 3. (Troškovi poslovanja)	Obveze	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Plaćanja	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
UKUPNA odobrena sredstva za omotnicu programa[42]	Obveze	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**
	Plaćanja	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

41 Odobrena sredstva za osoblje obračunavaju se samo za pola godine 2021.

42 Navedena ukupna odobrena sredstva odnose se samo na financijska sredstva EU-a izdvojena za kibersigurnost u okviru programa Digitalna Europa. Doprinos iz financijske omotnice za klaster „Uključivo i sigurno društvo” stupa II. „Globalni izazovi i industrijska konkurentnost” programa Obzor Europa (ukupna omotnica od 2 800 000 000 EUR) iz članka 5. stavka 1. točke (b) predložit će Komisija tijekom zakonodavnog postupka, a u svakom slučaju prije postizanja političkog dogovora. Prijedlog će se temeljiti na rezultatima postupka strateškog planiranja kako je definirano u članku 6. stavku 6. Uredbe XXX [okvirni program Obzor Europa].

Naslov višegodišnjeg financijskog okvira	7	„Administrativni rashodi”

u milijunima EUR (do tri decimalna mjesta)

		2021.	**2022.**	**2023.**	**2024.**	**2025.**	**2026.**	**2027.**	***Nakon 2027.***	**UKUPNO**
Ljudski resursi		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Ostali administrativni rashodi		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
UKUPNA odobrena sredstva iz NASLOVA 7. višegodišnjeg financijskog okvira	(Ukupne obveze = ukupna plaćanja)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

u milijunima EUR (do tri decimalna mjesta)

		2021.	**2022.**	**2023.**	**2024.**	**2025.**	**2026.**	**2027.**	***Nakon 2027.***	**UKUPNO**
UKUPNA odobrena sredstva prema NASLOVIMA višegodišnjeg financijskog okvira	Obveze	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Plaćanja	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1.²061,715**	**2 005,637**

3.2.2. Sažetak procijenjenog učinka na administrativna odobrena sredstva

– ☐ Za prijedlog/inicijativu nisu potrebna administrativna odobrena sredstva.

– ☒ Za prijedlog/inicijativu potrebna su sljedeća administrativna odobrena sredstva:

u milijunima EUR (do tri decimalna mjesta)

Godine	2021.	2022.	2023.	2024.	2025.	2026.	2027.	UKUPNO
NASLOV 7. višegodišnjeg financijskog okvira								
Ljudski resursi	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Ostali administrativni rashodi	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Međuzbroj za NASLOV 7. višegodišnjeg financijskog okvira	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**

Izvan NASLOVA 7.[43] višegodišnjeg financijskog okvira								
Ljudski resursi								
Ostali administrativni rashodi	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Međuzbroj izvan NASLOVA 7. višegodišnjeg financijskog okvira	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**

UKUPNO	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

Potrebna odobrena sredstva za ljudske potencijale i ostale administrativne rashode pokrit će se odobrenim sredstvima glavne uprave koja su već dodijeljena za upravljanje djelovanjem i/ili su preraspodijeljena unutar glavne uprave te, prema potrebi, bilo kojim dodatnim sredstvima koja se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

Prethodno navedena potrebna odobrena sredstva za ljudske potencijale i ostale administrativne rashode izvan Naslova 7. odgovaraju iznosima pokrivenima financijskim doprinosom Unije iz programa Digitalna Europa.

Odobrena sredstva potrebna za ljudske potencijale i ostale administrativne rashode iz Naslova 7. povećat će se za iznose pokrivene financijskim doprinosom Unije iz programa Obzor Europa kad Komisija tijekom zakonodavnog postupka predloži doprinos iz financijske omotnice za klaster „Uključivo i sigurno društvo" stupa II. „Globalni izazovi i industrijska konkurentnost" programa Obzor Europa (ukupna omotnica od 2 800 000 000 EUR) iz članka 21. stavka 1. točke (b), a u svakom slučaju prije postizanja političkog dogovora.

[43] Tehnička i/ili administrativna pomoć i rashodi za potporu provedbi programa i/ili djelovanja EU-a (prijašnje linije „BA"), neizravno istraživanje, izravno istraživanje.

Prethodno navedena potrebna odobrena sredstva za ljudske potencijale i ostale administrativne rashode izvan Naslova 7. ne uključuju doprinos država članica za administrativne troškove Centra za stručnost koji je razmjeran financijskom doprinosu Unije.

3.2.2.1. Procjena potrebnih ljudskih resursa za Komisiju

– ☐ Za prijedlog/inicijativu nisu potrebni ljudski resursi.

– ■ Za prijedlog/inicijativu potrebni su sljedeći ljudski resursi:

Procjenu navesti u ekvivalentu punog radnog vremena

Godine		**2021.**	**2022.**	**2023.**	**2024.**	**2025.**	**2026.**	**2027.**
• Radna mjesta prema planu radnih mjesta (dužnosnici i privremeno osoblje)								
Sjedište i predstavništva Komisije		20	21	21	21	21	21	22
Delegacije								
Istraživanje								
• Vanjsko osoblje (u ekvivalentu punog radnog vremena: EPRV) – UO, LO, UNS, UsO i MSD [44] Naslov 7.								
Financirano iz NASLOVA 7. višegodišnjeg financijskog okvira	– u sjedištima	3	3	3	3	3	3	3
	– u delegacijama							
Financirano iz omotnice programa [45]	– u sjedištima							
	– u delegacijama							
Istraživanje								
Ostalo (navesti)								
UKUPNO		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Potrebe za ljudskim resursima pokrit će se osobljem glavne uprave kojemu je već povjereno upravljanje provedbom mjere i/ili koje je preraspoređeno unutar glavne uprave te, prema potrebi, resursima koji se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

Opis zadaća koje treba obaviti:

Dužnosnici i privremeno osoblje	Koordinacija, praćenje i usmjeravanje zadaća povjerenih Europskom centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja, uključujući troškove potpore i koordinacije. Razvoj politike i koordinacija u području kibersigurnosti u pogledu zadaća povjerenih Europskom centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja, primjerice u pogledu utvrđivanja prioriteta za istraživanje i industrijsku politiku, opće suradnje između država članica i gospodarskih subjekata, dosljednosti s budućim okvirom EU-a za kibersigurnosnu certifikaciju, rada na odgovornosti i dužna pažnja ili koordinacije s politikama o računalstvu visokih performansi, umjetnoj inteligenciji i digitalnim vještinama. .
Vanjsko osoblje	Koordinacija, praćenje i usmjeravanje zadaća povjerenih Europskom centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja, uključujući troškove potpore i koordinacije. Razvoj politike i koordinacija u području kibersigurnosti u pogledu zadaća povjerenih Europskom centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja, primjerice u pogledu utvrđivanja prioriteta za istraživanje i industrijsku

[44] UO = ugovorno osoblje; LO = lokalno osoblje; UNS = upućeni nacionalni stručnjaci; UsO = ustupljeno osoblje; MSD = mladi stručnjaci u delegacijama.

[45] U okviru gornje granice za vanjsko osoblje iz odobrenih sredstava za poslovanje (prijašnje linije „BA”).

	politiku, opće suradnje između država članica i gospodarskih subjekata, dosljednosti s budućim okvirom EU-a za kibersigurnosnu certifikaciju, rada na odgovornosti i dužnosti skrbi ili koordinacije s politikama o računalstvu visokih performansi, umjetnoj inteligenciji i digitalnim vještinama. .

3.2.2.2. Procijenjeni zahtjevi za ljudske potencijale u Centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja

	2021.	2022.	2023.	2024.	2025.	2026.	2027.
Službenici Komisije							
od čega AD							
od čega AST							
od čega AST-SC							
Privremeno osoblje							
od čega AD	10	11	13	13	13	13	13
od čega AST							
od čega AST-SC							
Ugovorno osoblje	26	32	39	39	39	39	39
UNS-ovi	1	1	1	1	1	1	1
Ukupno	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Opis zadaća:

Dužnosnici i privremeno osoblje	Operativna provedba zadaća povjerenih Europskom centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja, u skladu s člankom 4. ove Uredbe, uključujući troškove potpore i koordinacije.
Vanjsko osoblje	Operativna provedba zadaća povjerenih Europskom centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja, u skladu s člankom 4. ove Uredbe, uključujući troškove potpore i koordinacije.

Prethodno navedeni zahtjevi za ljudske potencijale u Centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja odgovaraju procijenjenim zahtjevima za provedbu financijskog doprinosa Unije u okviru programa Digitalna Europa.

Prethodno navedeni zahtjevi za ljudske potencijale u Centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja povećat će se za procijenjene zahtjeve za provedbu financijskog doprinosa Unije u okviru programa Obzor Europa kada Komisija tijekom zakonodavnog postupka predloži doprinos iz financijske omotnice za klaster „Uključivo i sigurno društvo” stupa II. „Globalni izazovi i industrijska konkurentnost” programa Obzor Europa (ukupna omotnica od 2 800 000 000 EUR) iz članka 21. stavka 1. točke (b), a u svakom slučaju prije postizanja političkog dogovora.

3.2.2.3. Plan radnih mjesta Centra za stručnost u području kibersigurnosti, industrije, tehnologije

Funkcijska skupina i platni razred	2021.	2022.	2023.	2024.	2025.	2025.	2025.
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
AD ukupno	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							
AST ukupno							
AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							

AST/SC ukupno							
SVEUKUPNO	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Procijenjeni učinak na osoblje (dodatni) – vanjsko osoblje Centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja

Ugovorno osoblje	2021.	2022.	2023.	2024.	2025.	2026.	2027.
Funkcijska skupina IV.	20	22	29	29	29	29	29
Funkcijska skupina III.	2	4	4	4	4	4	4
Funkcijska skupina II.	4	6	6	6	6	6	6
Funkcijska skupina I.							
Ukupno	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Kako bi se osigurala neutralnost broja osoblja, dodatno osoblje za Centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja djelomično će se poravnati smanjenjem broja službenika i vanjskog osoblja (tj. plan radnih mjesta i trenutačno vanjsko osoblje) u relevantnim službama Komisije.
Broj osoblja Centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja iz točaka 3.2.2.2.–4. nadoknadit će se kako slijedi[46]:

UKUPNO	2021.	2022.	2023.	2024.	2025.	2026.	2027.
Službenici Komisije	5	5	6	6	6	6	6
Privremeni djelatnici							
Ugovorno osoblje	14	17	20	20	20	20	20
UNS-ovi							
Ukupno EPRV	19	22	26	26	26	26	26
Ukupni broj	19	22	26	26	26	26	26

Nadoknada ljudskih potencijala u Centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja bit će razmjerna udjelu financijskog doprinosa Unije, odnosno 50 %.

Prethodno navedena naknada odnosi se na procijenjene zahtjeve za ljudske potencijale u Centru za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja za provedbu financijskog doprinosa Unije iz programa Digitalna Europa.

[46] Podložno konačnom iznosu proračuna čija će se provedba delegirati Centru za stručnost.

Prethodno navedena naknada povećat će se za procijenjene zahtjeve za provedbu financijskog doprinosa Unije iz programa Obzor Europa kada Komisija tijekom zakonodavnog postupka predloži doprinos iz financijske omotnice za klaster „Uključivo i sigurno društvo” stupa II. „Globalni izazovi i industrijska konkurentnost” programa Obzor Europa (ukupna omotnica od 2 800 000 000 EUR) iz članka 21. stavka 1. točke (b), a u svakom slučaju prije postizanja političkog dogovora.

3.2.3. Doprinosi trećih strana

U prijedlogu/inicijativi:

– ☐ ne predviđa se sudjelovanje trećih strana u sufinanciranju

– ☒ predviđa se sudjelovanje trećih strana u sufinanciranju[47] procijenjeno u nastavku:

Odobrena sredstva u milijunima EUR (do tri decimalna mjesta)

Godine	2021.	2022.	2023.	2024.	2025.	2026.	2027.	UKUPNO
Države članice – doprinos za troškove osoblja	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Države članice – doprinos za infrastrukturne troškove i troškove poslovanja	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Države članice – doprinos za troškove poslovanja	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
UKUPNO sufinancirana odobrena sredstva	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Prethodno navedeni doprinos treće strane odnosi se samo na sufinanciranje razmjerno financijskim sredstvima EU-a izdvojenima za kibersigurnost u okviru programa Digitalna Europa. Prethodno navedeni doprinos treće strane povećat će se kada Komisija tijekom zakonodavnog postupka predloži financijski doprinos iz klastera „Uključivo i sigurno društvo" stupa II. „Globalni izazovi i industrijska konkurentnost" programa Obzor Europa (ukupna omotnica od 2 800 000 000 EUR) iz članka 21. stavka 1. točke (b), a u svakom slučaju prije postizanja političkog dogovora. Prijedlog će se temeljiti na rezultatima postupka strateškog planiranja kako je definirano u članku 6. stavku 6. Uredbe XXX [okvirni program Obzor Europa].

3.3. Procijenjeni učinak na prihode

– ☒ Prijedlog/inicijativa nema financijski učinak na prihode.

– ☐ Prijedlog/inicijativa ima sljedeći financijski učinak:

☐ na vlastita sredstva

☐ na ostale prihode

navesti ako su prihodi dodijeljeni proračunskim linijama rashoda ☐

u milijunima EUR (do tri decimalna mjesta)

Proračunska linija prihoda:	Učinak prijedloga/inicijative[48]						
	2021.	2022.	2023.	2024.	2025.	2026.	2027.
Članak …….							

Za namjenske prihode navesti odgovarajuće proračunske linije rashoda.

Ostale napomene (npr. metoda/formula za izračun učinka na prihode ili druge informacije).

[47] Doprinosi u naravi od država članica

[48] Kad je riječ o tradicionalnim vlastitim sredstvima (carine, pristojbe na šećer) navedeni iznosi moraju biti neto iznosi, to jest bruto iznosi umanjeni za 20 % na ime troškova naplate.