EUROPSKI
REVIZORSKI
SUD

HR

Mišljenje 02/2023

(u skladu s člankom 322. stavkom 1. UFEU-a)

o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih [Međuinstitucijski predmet 2023/0109(COD) od 18. travnja 2023.]

Sadržaj

Uvod

01 Komisija je 18. travnja 2023. objavila Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih („Akt EU-a o kibersolidarnosti”).

02 Predloženim Aktom EU-a o kibersolidarnosti utvrđuju se mjere za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih, posebice sljedeće:

- **europski kiberštit**, čija je svrha razvoj i poboljšanje zajedničkih sposobnosti za otkrivanje i informiranost o stanju;
- **mehanizam za izvanredne kibersigurnosne situacije**, čija je svrha pomoć državama članicama u pripremi za značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, odgovoru na njih i hitnom oporavku od njih;
- **mehanizam za istraživanje kibersigurnosnih incidenata**, čija je svrha istraživanje i procjena značajnih incidenata ili incidenata velikih razmjera.

03 Pravnom osnovom prijedloga Komisije propisuje se da je savjetovanje s Europskim revizorskim sudom (Sud) obvezno[1]. Europski parlament uputio je Sudu dopis tražeći njegovo stajalište 2. lipnja 2023., a Vijeće Europske unije to je učinilo 7. lipnja 2023. Ovim se mišljenjem ispunjava taj zahtjev za savjetovanje.

[1] Članak 322. stavak 1. Ugovora o funkcioniranju Europske unije.

Opća opažanja

04 Odgovornost za sprječavanje kibersigurnosnih incidenata i kriza koje iz njih proizlaze te pripravnost i odgovor na njih snose u prvom redu države članice. U skladu s člankom 4. stavkom 2. Ugovora o Europskoj uniji nacionalna sigurnost ostaje isključiva odgovornost svake države članice. Međutim, mogući učinak značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera znači da bi moglo biti potrebno zajedničko djelovanje na razini EU-a.

05 Sud pozdravlja ciljeve prijedloga u pogledu jačanja kolektivne kiberotpornosti EU-a. U ovom mišljenju iznosi posebne primjedbe o trima sastavnicama predloženog Akta o kibersolidarnosti EU-a i ističe određene rizike koje je utvrdio u vezi s izostankom procjene učinka, financijskim aspektima i načinom na koji bi se mjere utvrđene u prijedlogu mogle provesti. Konkretno, Sud ističe da bi se primjenom predložene uredbe mogla povećati složenost kibersigurnosnog okruženja EU-a i predlaže načine za ublažavanje tog rizika (vidjeti odlomke ***13***. – ***20***.).

Posebne primjedbe

Izostanak procjene učinka

06 U Komisijinim smjernicama za bolju regulativu predlaže se upotreba procjena učinka i savjetovanja s dionicima u okviru sveobuhvatne analize mogućnosti osmišljavanja i provedbe politika. Sud sveobuhvatne procjene učinka smatra ključnim instrumentom za razmatranje potrebe za djelovanjem EU-a i analizu mogućih učinaka dostupnih rješenja prije donošenja bilo kakvog prijedloga.

07 Za predloženu uredbu nije provedena procjena učinka. U odjeljku 3. popratnog obrazloženja Komisija je objasnila da je odlučila da neće provesti takvu procjenu zbog „žurnosti Prijedloga”. Navela je i da će se mjere uvedene predloženom uredbom podupirati programom Digitalna Europa (DEP) te da su u one skladu s Uredbom o programu Digitalna Europa, za koju je 2018. provedena posebna procjena učinka. Osim toga, Komisija je objasnila da su se predložene mjere temeljile na prethodnim djelovanjima koja su pripremljena u bliskoj suradnji s glavnim dionicima i državama članicama, pri čemu su objedinjena stečena iskustva.

08 Međutim, Sud napominje da procjena učinka za program Digitalna Europa ne obuhvaća nove mjere uvedene predloženom uredbom. Stoga su informacije o dostupnim opcijama u okviru politika i troškovima povezanima s prijedlogom ograničene.

Djelomične informacije o financiranju

Djelomične informacije o financiranju i potrebama za ljudskim resursima

09 Financiranje mjera utvrđenih u Aktu o kibersolidarnosti EU-a osigurat će se iz programa Digitalna Europa. Komisija je u odjeljku 4. svojeg obrazloženja navela da je za europski kiberštit iznos od 115 milijuna eura već bio izdvojen za razdoblje 2021. – 2022. u obliku pilot-projekata. Navela je i da bi se prijedlogom proračun za specifični cilj programa Digitalna Europa „kibersigurnost i povjerenje” za razdoblje 2023. – 2027., koji iznosi 743 milijuna eura, povećao za 100 milijuna eura, i to internom preraspodjelom sredstava.

10 Nakon te preraspodjele iznos financijskih sredstava EU-a dostupnih za mjere u području kibersigurnosti u razdoblju 2023. – 2027. bit će 843 milijuna eura. Sud napominje da taj iznos ne obuhvaća samo mjere utvrđene u predloženoj uredbi nego i druge mjere u području kibersigurnosti u okviru programa Digitalna Europa (kao što je potpora industrijskom sektoru ili normizaciji). U prijedlogu nije iznesena procjena ukupnih očekivanih troškova povezanih s uspostavom i provedbom predloženih mjera (europski kiberštit, mehanizam za izvanredne kibersigurnosne situacije, uključujući kibersigurnosnu pričuvu EU-a, i mehanizam za istraživanje kibersigurnosnih incidenata). Budući da prijedlog nije popraćen procjenom učinka, Sud predlaže da Komisija te procjene troškova stavi na raspolaganje radi povećanja transparentnosti.

Djelomične informacije o financijskom ustroju europskog kiberštita

11 Poglavljem II. predložene uredbe uspostavlja se „europski kiberštit”, koji se sastoji od nacionalnih centara za sigurnosne operacije (nacionalni SOC-ovi) i prekograničnih centara za sigurnosne operacije (prekogranični SOC-ovi). Predloženom uredbom predviđa se da nacionalni SOC-ovi koji ispunjavaju kriterije prihvatljivost mogu primiti financijski doprinos EU-a kojim se pokriva do 50 % njihovih troškova nabave alata i infrastruktura te do 50 % njihovih operativnih troškova. Za prekogranične SOC-ove sufinanciranjem koje provodi EU treba se pokriti do 75 % troškova nabave alata i infrastrukture te do 50 % operativnih troškova. U predloženoj uredbi ne navodi se zašto su u prekograničnim SOC-ovima potrebni dodatni alati i infrastrukture, uz višu stopu sufinanciranja, u usporedbi s alatima dostupnima nacionalnim SOC-ovima u konzorciju.

12 U predloženoj uredbi ne navodi se ni koliko će dugo EU sufinancirati operativne troškove nacionalnih i prekograničnih SOC-ova. Time se stvara rizik od toga da funkcioniranje europskog kiberštita i njegova održivost postanu ovisni o financijskim sredstvima EU-a.

Rizici povezani s europskim kiberštitom

Povećana složenost i dodatni slojevi

13 Sud je u pregledu 02/2019[2] utvrdio da je kibersigurnosno okruženje EU-a složeno i višeslojno. Uključuje brojne privatne i javne aktere u civilnoj sferi na regionalnoj i

[2] Pregled 02/2019„Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a”.

nacionalnoj razini te na razini EU-a, među ostalim tijela zadužena za izvršavanje zakonodavstva i financijsko-obavještajne jedinice. Kibersigurnost je i jedan od ključnih elemenata nacionalne sigurnosti i obrane. U ***Prilogu*** ovom mišljenju Sud iznosi plan novog kibersigurnosnog okruženja u EU-u, koje u osjenčanom okviru uključuje sve mehanizme i komponente uvedene prijedlogom. Služi kao prikaz dodatne složenosti i slojeva uvedenih Uredbom.

14 Cilj je europskog kiberštita uspostavljenog u poglavlju II. predložene uredbe razviti napredne sposobnosti EU-a za otkrivanje i analizu kiberprijetnji i kiberincidenata te obradu podataka o njima. Radit će se o međusobno povezanoj paneuropskoj infrastrukturi nacionalnih centara za sigurnosne operacije i prekograničnih centara za sigurnosne operacije.

15 Da bi sudjelovala u europskom kiberštitu, određena država članica imenuje barem jedan nacionalni SOC, koji mora biti javno tijelo. Nacionalni SOC-ovi zatim bi trebali osnovati prekogranične SOC-ove, koji će biti konzorciji sastavljeni od SOC-ova iz najmanje triju država članica koje su se obvezale surađivati i koordinirati svoje aktivnosti otkrivanja kibersigurnosnih incidenata i praćenja kiberprijetnji.

16 Posljednjih je godina EU ojačao svoj regulatorni okvir za kibersigurnost. Jedan od njegovih ključnih instrumenata čine Direktiva o sigurnosti mrežnih i informacijskih sustava („Direktiva NIS”) iz 2016. i njezina preinačena verzija iz 2022. ((Direktiva o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, tj. „Direktiva NIS 2”). U skladu s Direktivom NIS 2 države članice trebale bi na nacionalnoj razini uspostaviti jedan tim za odgovor na računalne sigurnosne incidente (CSIRT) ili više njih. Na razini EU-a Direktivom NIS 2 uspostavljena je i Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, mreža CSIRT-ova i Europska mreža organizacija za vezu za kiberkrize (EU-CyCLONe).

17 EU je 2021. osnovao Europski stručni centar za kibersigurnost. Taj centar, otvoren u svibnju 2023., podupirat će mreža od 27 nacionalnih koordinacijskih centara, po jedan za svaku državu članicu, od kojih su neki i nacionalni SOC-ovi. Centar će biti odgovoran za provedbu kibersigurnosne komponente programa Digitalna Europa, osim za kibersigurnosnu pričuvu EU-a, za čiju će provedbu biti zadužena Komisija, s tim da ENISA može biti odgovorna za njezin rad i administraciju.

18 Komisija je osnovala i Zajedničku jedinicu za kibersigurnost. Ta je jedinica najavljena u Strategiji EU-a za kibersigurnost iz 2020. i dodatno definirana u jednoj preporuci Komisije iz 2021.

19 Komisija je u travnju 2023. najavila pokretanje Akademije za vještine u području kibersigurnosti, nove inicijative usmjerene na smanjenje nedostatka talenata u području kibersigurnosti i povećanje „radne snage EU-a u području kibersigurnosti”.

20 U tom kontekstu Sud smatra da bi se primjenom predložene uredbe mogla povećati složenost cijelog kibersigurnosnog okruženja EU-a. Postoji mogućnost preklapanja između postojeće mreže CSIRT-ova i SOC-ova. Iako je Komisija u odjeljku 1. svojeg obrazloženja navela da bi prekogranične platforme SOC-ova trebale nuditi nove mogućnosti komplementarne mreži CSIRT-ova, Sud napominje da su neke zadaće i ciljevi nacionalnih SOC-ova, prekograničnih SOC-ova, CSIRT-ova i mreže CSIRT-ova slični. To uključuje otkrivanje prijetnji i odgovor na njih, obavještajne podatke o kiberprijetnjama i informiranost o stanju. Taj bi se rizik u načelu mogao ublažiti postupnom konsolidacijom uključenih struktura, posebno nacionalnih SOC-ova i CSIRT-ova te prekograničnih SOC-ova. Nadalje, u prijedlogu bi trebalo pojasniti na koji bi način te strukture trebale međudjelovati utvrđivanjem jasnih sustava upravljanja i odgovornosti kako bi se zajamčila djelotvorna koordinacija i ostvarile sinergije.

Razmjena informacija

21 Sud je u tematskom izvješću 05/2022[3] utvrdio da institucije, tijela i agencije EU-a nisu sustavno međusobno razmjenjivali ključne relevantne informacije o kibersigurnosti, čak ni kad su to bili obvezni činiti. Djelotvornu razmjenu informacija dodatno otežavaju problemi u vezi s interoperabilnošću koji narušavaju sigurnu komunikaciju. Iako su se njegova opažanja odnosila na tu relativno malu i homogenu skupinu aktera EU-a, Sud smatra da će taj izazov biti sve važniji u složenijem i raznolikijem kibersigurnosnom okruženju na razini država članica.

22 U članku 4. predložene uredbe navodi se da bi nacionalni SOC-ovi trebali djelovati kao „referentna i pristupna točka” za druge javne i privatne organizacije na nacionalnoj razini kad je riječ o prikupljanju i analizi informacija o kibersigurnosnim prijetnjama i incidentima. Međutim, na razini EU-a trenutačno ne postoje zahtjevi za izvješćivanje za javne i privatne organizacije (uključujući nacionalne CSIRT-ove, privatne SOC-ove i takozvane „ključne i važne subjekte” iz Direktive NIS 2) prema nacionalnim SOC-ovima. Stoga postoji rizik od toga da nacionalni SOC-ovi ne dobiju odgovarajuće podatke ili informacije za svoje potrebe.

---

[3] Tematsko izvješće 05/2022 „Kibersigurnost institucija, tijela i agencija EU-a: razina pripravnosti općenito nije razmjerna prijetnjama”.

23 U odjeljku 2.2.2. zakonodavnog financijskog izvještaja koji je priložen prijedlogu Komisija utvrđuje rizik od toga da države članice neće dijeliti „dovoljnu količinu” relevantnih informacija o kiberprijetnjama među prekograničnim platformama SOC-ova ili između prekograničnih platformi i drugih relevantnih subjekata na razini EU-a. Takav nedostatak razmjene informacija mogao bi ugroziti djelotvornost i dodanu vrijednost europskog kiberštita.

24 Sud stoga pozdravlja činjenicu da prijedlog sadržava posebne odredbe u člancima 4., 5. i 6. kako bi se ublažili rizici povezani s nedostatkom razmjene informacija. Prijedlogom se predviđa da će financijska sredstva EU-a nacionalnim SOC-ovima biti dostupna samo ako se obvežu da će podnijeti zahtjev za sudjelovanje u određenom prekograničnom SOC-u. Međutim, Sud napominje da ne postoji povrat financijske potpore primljene tijekom prve dvije godine ako se nacionalni SOC ne pridruži prekograničnom SOC-u. U skladu s predloženom uredbom članovi prekograničnih SOC-ova obvezni su međusobno razmjenjivati „znatne količine podataka” i uspostaviti okvir upravljanja u pisanom ugovoru o konzorciju.

25 Osim toga, u članku 7. prijedloga navodi se da prekogranični SOC-ovi moraju „bez nepotrebne odgode” mreži EU-CyCLONe-u, mreži CSIRT-ova i Komisiji dostaviti relevantne informacije o potencijalnom ili aktualnom kiberincidentu velikih razmjera. Sud naglašava važnost jamčenja odgovarajuće provedbe te odredbe.

26 U članku 6. predložene uredbe propisuje se da Komisija provedbenim aktima može utvrditi uvjete interoperabilnosti među prekograničnim SOC-ovima. U članku 8. navodi se da Komisija može donijeti i provedbene akte kojima se utvrđuju tehnički zahtjevi za države članice kako bi se zajamčila visoka razina sigurnosti podataka i fizičke sigurnosti infrastrukture. Ti uvjeti i zahtjevi trebali bi se brzo dogovoriti kako bi se izbjeglo istodobno osmišljavanje nekompatibilnih sustava i smanjili troškovi.

Rizici povezani s mehanizmom za izvanredne kibersigurnosne situacije

Upotreba kibersigurnosne pričuve EU-a

27 Sud je u tematskom izvješću 05/2022 utvrdio da CERT-EU, tim EU-a za hitne računalne intervencije koji institucijama, tijelima i agencijama EU-a pruža potporu u odgovoru, u vrijeme provedbe revizije nije djelovao 24 sata dnevno i sedam dana u tjednu.

28 U članku 14. predložene uredbe propisuje se da će zahtjeve za potporu iz kibersigurnosne pričuve EU-a ocijeniti Komisija, uz potporu ENISA-e, te da će odgovor biti poslan „bez odgode”. Budući da mogu postojati višestruki i paralelni zahtjevi zbog kojih bi se morali određivati prioriteti, predloženom uredbom utvrđuju se određeni kriteriji za donošenje odluka. U članku 13. navodi se da Komisija provedbenim aktima može pobliže utvrditi detaljne aranžmane za dodjelu usluga potpore iz pričuve.

29 Sud smatra da je od ključne važnosti da vrijeme između zahtjeva za primanje usluga potpore iz kibersigurnosne pričuve EU-a i odgovora Komisije ne bude produženo zbog trenutka u kojem je zahtjev podnesen. Međutim, u prijedlogu se ne navodi unaprijed utvrđeni rok i ne zahtijeva se poduzimanje organizacijskih koraka kako bi se taj rok poštovao.

Odstupanje od načela jedne godine

30 Jedno od temeljnih načela koje se primjenjuje u proračunu EU-a načelo je jedne godine, što znači da se odobrena sredstva unesena u proračun odobravaju za financijsku godinu koja traje do 31. prosinca. Neiskorištena odobrena sredstva za preuzete obveze i plaćanja ne prenose se automatski u sljedeću financijsku godinu. To načelo utvrđeno je u poglavlju 2. Financijske uredbe.

31 U članku 19. predložene uredbe odstupa se od tog načela kad je riječ o financiranju mjera u okviru mehanizma za izvanredne kibersigurnosne situacije. Navodi se da se neiskorištena odobrena sredstva za preuzete obveze i plaćanja za mjere povezane s pripravnošću, odgovorom i uzajamnom pomoći automatski prenose te da se za njih mogu preuzeti obveze i plaćanja do 31. prosinca sljedeće financijske godine. U odjeljku 2. obrazloženja Komisija je objasnila da je ta fleksibilnost u upravljanju proračunom bila potrebna uzimajući u obzir „nepredvidivu, iznimnu i specifičnu prirodu kibersigurnosnog okruženja i kiberprijetnji”.

32 Kad je riječ o pripravnosti, Sud smatra da bi koordinirano testiranje pripravnosti subjekata trebalo biti planirano te da stoga, općenito gledajući, nije ni nepredvidivo ni iznimno. Stajalište je Suda da za takve planirane aktivnosti nije potrebno odstupanje od temeljnog načela jedne godine.

33 Međutim, budući da će se kibersigurnosna pričuva EU-a i uzajamna pomoć upotrebljavati samo u odgovoru na nepredvidive događaje, Sud smatra da je obrazloženje za to odstupanje valjano samo u tom slučaju.

34 Radi jasnoće i u skladu s izradom drugih propisa, poput onih o Mehanizmu Unije za civilnu zaštitu ili Instrumentu za susjedstvo, razvoj i međunarodnu suradnju – Globalna Europa, Sud smatra i da bi u predloženoj uredbi trebalo navesti da bi se automatski prijenos neiskorištenih obveza trebao ograničiti na sljedeću godinu.

Rizici povezani s mehanizmom za istraživanje kibersigurnosnih incidenata

35 U članku 18. predložene uredbe navodi se da, na zahtjev Komisije, mreže EU-CyCLONe ili mreže CSIRT-ova, ENISA istražuje i procjenjuje prijetnje, ranjivosti i mjere ublažavanja s obzirom na određeni značajni kibersigurnosni incident ili kibersigurnosni incident velikih razmjera. Nakon suradnje sa svim relevantnim dionicima ENISA mora dostaviti izvješće o istraživanju incidenta koje obuhvaća glavne uzroke, ranjivosti i stečena iskustva.

36 Sud smatra da je to važan mehanizam povratnih informacija kako bi se stalno jačala sposobnost EU-a za otkrivanje kiberprijetnji i kiberincidenata te pripravnosti i odgovora na njih. Međutim, Sud predlaže da se u predmetnoj uredbi odredi maksimalan rok za dostavu izvješća ENISA-e nakon svakog incidenta kako bi se zajamčilo pravodobno dostavljanje povratnih informacija. Nadalje, u prijedlogu se navodi da bi se u izvješću prema potrebi trebale davati preporuke za poboljšanje kibersigurnosnog položaja Unije. Međutim, u prijedlogu nije navedeno na koji bi se način trebala pratiti provedba tih preporuka.

Praćenje uspješnosti i evaluacija politika

37 Člankom 19. predložene uredbe mijenja se Prilog II. Uredbi o programu Digitalna Europa tako da se uvodi novi mjerljivi pokazatelj, odnosno „broj mjera za potporu pripravnosti i odgovoru na kibersigurnosne incidente u okviru mehanizma za izvanredne kibersigurnosne situacije”. Tim se pokazateljem dopunjuju dva postojeća pokazatelja namijenjena praćenju i izvješćivanju koje se odnosi na napredak prema ostvarivanju specifičnog cilja programa Digitalna Europa „kibersigurnost i povjerenje”, tj. „količina infrastrukture i/ili alata za kibersigurnost, nabavljenih zajedničkom javnom nabavom” i „broj korisnika i zajednica korisnika s pristupom europskim kapacitetima za kibersigurnost”.

38 Sud smatra da se predloženim novim pokazateljem mjere samo ostvarenja i da će se njime pružiti slab uvid u upotrebu i rezultate europskog kiberštita i mehanizma za izvanredne kibersigurnosne situacije.

39 U skladu s člankom 20. prijedloga Komisija mora Europskom parlamentu i Vijeću podnijeti izvješće o evaluaciji i preispitivanju predmetne uredbe u roku od četiri godine od datuma njezine primjene.

40 Iako Sud smatra da bi se evaluacija trebala temeljiti na dostatnim i pouzdanim podatcima, zbog konteksta prijetnji koji se brzo mijenja potrebne su stalne prilagodbe i inovacije EU-a i njegovih država članica. Sud stoga smatra da bi se provedba evaluacije kako je trenutačno predložena mogla dogoditi prekasno za novo programsko razdoblje. Osim toga, kad je riječ o cijelom iznosu koji je predviđen proračunom za specifični cilj programa Digitalna Europa „kibersigurnost i povjerenje”, obveze će biti preuzete do kraja 2027.

Zaključne napomene

41 Predloženim Aktom EU-a o kibersolidarnosti utvrđuju se mjere za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih. Sud pozdravlja ciljeve prijedloga u pogledu jačanja kolektivne kiberotpornosti EU-a.

42 U mišljenju Suda ističu se određeni rizici koje je utvrdio i način na koji bi se mjere utvrđene u prijedlogu mogle provesti. Konkretno, Sud ističe rizike od toga da funkcioniranje europskog kiberštita i njegova održivost postanu ovisni o financijskim sredstvima EU-a, da funkcioniranje europskog kiberštita bude otežano zbog nedostatka razmjene informacija i da se mjerama uvedenim prijedlogom cijelo kibersigurnosno okruženje EU-a učini složenijim.

43 Sud na temelju pregleda zakonodavnog prijedloga predlaže da **Komisija i zakonodavci razmotre sljedeće**:

— stavljanje na raspolaganje procjena troškova povezanih s uvođenjem i provedbom predloženih mjera radi povećanja transparentnosti (vidjeti odlomak ***10***.);

— pojašnjavanje načina na koji bi nacionalni SOC-ovi, prekogranični SOC-ovi i mreža CSIRT-ova trebali međudjelovati utvrđivanjem jasnih sustava upravljanja i odgovornosti kako bi se zajamčila djelotvorna koordinacija i ostvarile sinergije (odlomak ***20***.);

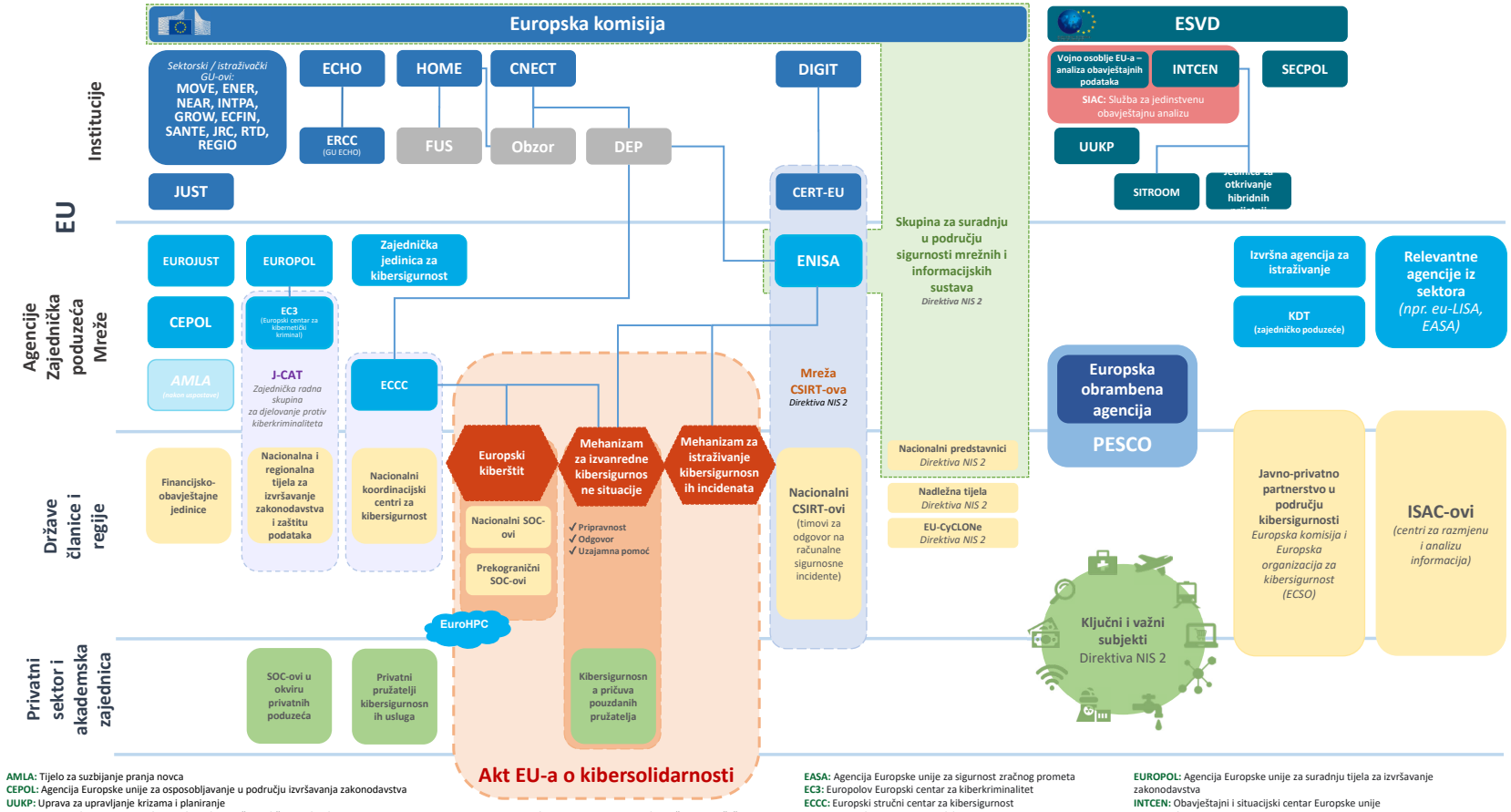
— jamčenje toga da vrijeme između zahtjeva za primanje usluga potpore iz kibersigurnosne pričuve EU-a i odgovora Komisije ne bude produženo zbog trenutka u kojem je zahtjev podnesen (odlomak ***29***.);

— ograničavanje odstupanja od načela jedne godine za mjere odgovora i uzajamnu pomoć te pojašnjenje da bi automatski prijenos neiskorištenih obveza trebao biti ograničen na sljedeću godinu (odlomci ***32***. – ***34***.);

— određivanje maksimalnog roka za dostavu izvješća ENISA-e nakon svakog incidenta kako bi se zajamčilo pravodobno dostavljanje povratnih informacija (odlomak ***36***.);

— pomicanje unaprijed rokova za izvješća koja Komisija podnosi o evaluaciji i preispitivanju Uredbe (odlomak ***40***.).

Prilog – Europsko kibersigurnosno okruženje



AMLA: Tijelo za suzbijanje pranja novca
CEPOL: Agencija Europske unije za osposobljavanje u području izvršavanja zakonodavstva
UUKP: Uprava za upravljanje krizama i planiranje
GU CONNECT: Glavna uprava za komunikacijske mreže, sadržaje i tehnologije
GU ECFIN: Glavna uprava za gospodarske i financijske poslove
GU ECHO: Glavna uprava za europsku civilnu zaštitu i europske operacije humanitarne pomoći
GU ENER: Glavna uprava za energetiku
GU GROW: Glavna uprava za unutarnje tržište, industriju, poduzetništvo te male i srednje poduzetnike
GU HOME: Glavna uprava za migracije i unutarnje poslove
GU INTPA: Glavna uprava za međunarodna partnerstva

GU JUST: Glavna uprava za pravosuđe i zaštitu potrošača
GU MOVE: Glavna uprava za mobilnost i promet
GU NEAR: Glavna uprava za susjedsku politiku i pregovore o proširenju
GU REGIO: Glavna uprava za regionalnu i urbanu politiku
GU RTD: Glavna uprava za istraživanje i inovacije
GU SANTE: Glavna uprava za zdravlje i sigurnost hrane
DIGIT: Glavna uprava za informatiku

EASA: Agencija Europske unije za sigurnost zračnog prometa
EC3: Europolov Europski centar za kiberkriminalitet
ECCC: Europski stručni centar za kibersigurnost
ECSO: Europska organizacija za kibersigurnost
EDA: Europska obrambena agencija
ESVD: Europska služba za vanjsko djelovanje
ERCC: Koordinacijski centar za odgovor na hitne situacije
EU-CyCLONe: Europska mreža organizacija za vezu za kiberkrize
EuroHPC: Europsko računalstvo visokih performansi
EUROJUST: Agencija Europske unije za suradnju u kaznenom pravosuđu

EUROPOL: Agencija Europske unije za suradnju tijela za izvršavanje zakonodavstva
INTCEN: Obavještajni i situacijski centar Europske unije
FUS: Fond za unutarnju sigurnost
JRC: Zajednički istraživački centar
KDT: Zajedničko poduzeće za ključne digitalne tehnologije
Direktiva NIS: Direktiva o sigurnosti mrežnih i informacijskih sustava
PESCO: okvir za stalnu strukturiranu suradnju
SECPOL: Uprava za sigurnosnu politiku i sprečavanje sukoba
SITROOM: soba za krizne situacije
SOC: centar za sigurnosne operacije

Izvor: Sud.

Ovo mišljenje donijelo je III. revizijsko vijeće, kojim predsjeda članica Revizorskog suda Bettina Jakobsen, na sastanku održanom u Luxembourgu 26. rujna 2023.

za Revizorski sud

Tony Murphy

predsjednik

AUTORSKA PRAVA