EVROPSKO RAČUNSKO SODIŠČE

SL

Mnenje 02/2023

(v skladu s členom 322(1) PDEU)

o predlogu uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje [medinstitucionalna zadeva 2023/0109(COD)] z dne 18. aprila 2023]

Vsebina

Uvod

01 Komisija je 18. aprila 2023 objavila predlog uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje (v nadaljnjem besedilu: akt EU o kibernetski solidarnosti).

02 V predlaganem aktu EU o kibernetski solidarnosti so določeni ukrepi za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje, zlasti z:

- **evropskim kibernetskim ščitom** za vzpostavitev in okrepitev usklajenih zmogljivosti za odkrivanje in situacijsko zavedanje,
- **mehanizmom za izredne kibernetske razmere** za podporo državam članicam pri pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in okrevanju po njih,
- **mehanizmom za pregledovanje kibernetskovarnostnih incidentov** za pregledovanje in ocenjevanje pomembnih incidentov ali incidentov velikih razsežnosti.

03 Glede na pravno podlago predloga Komisije je posvetovanje z Evropskim računskim sodiščem (v nadaljnjem besedilu: Sodišče) obvezno[1]. Evropski parlament in Svet Evropske unije sta Sodišče 2. oziroma 7. junija 2023 pisno zaprosila za mnenje. S tem mnenjem je izpolnjena zahteva po posvetovanju.

[1] Člen 322(1) Pogodbe o delovanju Evropske unije.

Splošna opažanja

04 Odgovornost za preprečevanje kibernetskovarnostnih incidentov in kriz ter pripravo in odzivanje nanje je prvenstveno naloga držav članic. V skladu s členom 4(2) Pogodbe o Evropski uniji ostaja nacionalna varnost v izključni pristojnosti vsake države članice. Vendar je zaradi morebitnega učinka pomembnih kibernetskovarnostnih incidentov in takih incidentov velikih razsežnosti morda potrebno skupno ukrepanje na ravni EU.

05 Sodišče pozdravlja cilje predloga za krepitev skupne kibernetske odpornosti EU. V tem mnenju daje specifične pripombe na tri elemente predlaganega akta EU o kibernetski solidarnosti in poudarja nekatera ugotovljena tveganja, in sicer v zvezi z neobstojem ocene učinka, finančnimi vidiki in tem, kako bi se lahko ukrepi iz predloga izvajali. Zlasti poudarja, da se s predlagano uredbo tvega, da bo celotno kibernetskovarnostno okolje EU bolj kompleksno, in predlaga načine za zmanjšanje tega tveganja (glej odstavke ***13***–***20***).

Specifične pripombe

Neobstoj ocene učinka

06 V smernicah Komisije za boljše pravno urejanje je predlagano, da se za celovito analizo možnosti zasnove in izvajanja politike uporabijo ocena učinka in posvetovanja z deležniki. Sodišče meni, da so celovite ocene učinka eno bistvenih orodij za ugotavljanje, ali je potrebno ukrepanje EU, in analizo morebitnih učinkov razpoložljivih rešitev pred sprejetjem katerega koli predloga.

07 Za ta predlog uredbe se ocena učinka ni pripravila. Komisija je v tretjem razdelku spremnega obrazložitvenega memoranduma pojasnila, da se je odločila, da take ocene ne bo izvedla zaradi „nujnosti priprave predloga”. Navedla je tudi, da se bodo ukrepi, uvedeni s predlagano uredbo, podpirali s programom Digitalna Evropa (PDE) in da so v skladu z uredbo o tem programu, za katero je bila leta 2018 pripravljena posebna ocena učinka. Poleg tega je Komisija pojasnila, da predlagani ukrepi temeljijo na prejšnjih ukrepih, pripravljenih v tesnem sodelovanju z glavnimi deležniki in državami članicami ter ob upoštevanju pridobljenih izkušenj.

08 Vendar Sodišče ugotavlja, da novi ukrepi, uvedeni s predlagano uredbo, v oceno učinka PDE niso zajeti. Zato je na voljo le malo informacij o razpoložljivih možnostih politike in stroških, povezanih s predlogom.

Delne informacije o financiranju

Delne informacije o financiranju in potrebah po človeških virih

09 Ukrepi iz akta EU o kibernetski solidarnosti bodo financirani iz PDE. Komisija je v četrtem razdelku obrazložitvenega memoranduma navedla, da je bilo za evropski kibernetski ščit že dodeljenih 115 milijonov EUR, in sicer v okviru pilotnih projektov v obdobju 2021–2022. Navedla je tudi, da se bodo s predlogom proračunska sredstva v višini 743 milijonov EUR, dodeljena specifičnemu cilju PDE, tj. kibernetska varnost in zaupanje, povečala za 100 milijonov EUR, in sicer z notranjo prerazporeditvijo sredstev v obdobju 2025–2027.

10 Po tej prerazporeditvi bodo sredstva EU za kibernetsko varnost za obdobje 2023–2027 znašala 843 milijonov EUR. Sodišče ugotavlja, da ta znesek ne zajema le ukrepov

iz predlagane uredbe, temveč tudi druge ukrepe za kibernetsko varnost PDE (npr. podpora industriji ali standardizaciji). V predlogu niso ocenjeni skupni pričakovani stroški, povezani z uvedbo in izvajanjem predlaganih ukrepov (ščit za kibernetsko varnost, mehanizem za izredne kibernetske razmere (vključno s kibernetskovarnostno rezervo EU) in mehanizem za pregledovanje kibernetskih incidentov). Ker predlogu ni priložena ocena učinka, Sodišče predlaga, naj Komisija predloži te ocene stroškov in tako poveča transparentnost.

Delne informacije o finančnem okviru za evropski kibernetski ščit

11 V poglavju II predlagane uredbe je določen „evropski kibernetski ščit", ki ga sestavljajo nacionalni centri za varnostne operacije in čezmejni centri za varnostne operacije. V predlagani uredbi je določeno, da lahko upravičeni nacionalni centri za varnostne operacije prejmejo finančni prispevek EU, s katerim se krije do 50 % stroškov nabave njihovih orodij in infrastrukture ter do 50 % njihovih operativnih stroškov. Za čezmejne centre za varnostne operacije naj bi se s sredstvi EU sofinanciralo do 75 % stroškov nabave orodij in infrastrukture ter do 50 % operativnih stroškov. V predlagani uredbi ni pojasnjeno, zakaj čezmejni centri za varnostne operacije potrebujejo dodatna orodja in infrastrukturo z višjo stopnjo sofinanciranja v primerjavi z orodji, ki so nacionalnim centrom za varnostne operacije na voljo v konzorciju.

12 V predlaganem aktu prav tako ni določeno, kako dolgo bo EU sofinancirala operativne stroške nacionalnih in čezmejnih centrov za varnostne operacije. S tem se tvega, da bosta delovanje evropskega kibernetskega ščita in njegova trajnost postala odvisna od financiranja EU.

Tveganja, povezana z evropskim kibernetskim ščitom

Večja kompleksnost in dodatne ravni

13 Sodišče je v Pregledu 02/2019[2] ugotovilo, da je kibernetskovarnostno področje EU kompleksno in večplastno. Vključuje številne zasebne in javne akterje s civilnega področja na regionalni in nacionalni ravni ter na ravni EU, tudi organe kazenskega pregona in finančnoobveščevalne enote. Kibernetska varnost je tudi eden ključnih elementov nacionalne varnosti in obrambe. Sodišče v ***Prilogi*** k temu mnenju predstavlja novo kibernetskovarnostno okolje EU, ki v okviru z imenom akt EU o

[2] Pregled 02/2019: Izzivi za uspešno politiko EU za kibernetsko varnost.

kibernetski solidarnosti vključuje vse mehanizme in njihove sestavne dele, ki naj bi bili uvedeni s predlogom. V njej so prikazani dodatna kompleksnost in ravni, do katerih naj bi prišlo po predlagani uredbi.

14 Cilj evropskega kibernetskega ščita, določenega v poglavju II predlagane uredbe, je razviti napredne zmogljivosti EU za odkrivanje, analiziranje in obdelavo podatkov o kibernetskih grožnjah in incidentih. Ščit naj bi postal medsebojno povezana vseevropska infrastruktura nacionalnih centrov za varnostne operacije in čezmejnih centrov za varnostne operacije.

15 Za sodelovanje v evropskem kibernetskem ščitu država članica imenuje vsaj en nacionalni center za varnostne operacije, ki mora biti javni organ. Nacionalni centri za varnostne operacije pa ustanovijo čezmejne centre za varnostne operacije, ki bodo delovali kot konzorciji centrov za varnostne operacije iz vsaj treh držav članic, ki so se zavezale, da bodo sodelovale pri usklajevanju svojih dejavnosti odkrivanja kibernetskih incidentov in spremljanju kibernetskih groženj.

16 EU je v zadnjih letih okrepila svoj regulativni okvir za kibernetsko varnost. Eden njegovih ključnih instrumentov sta direktiva o varnosti omrežij in informacij iz leta 2016 in njena revidirana različica iz leta 2022. V skladu z revidirano direktivo morajo države članice na nacionalni ravni ustanoviti eno ali več skupin za odzivanje na incidente na področju računalniške varnosti (CSIRT). Na ravni EU se z revidirano direktivo vzpostavlja tudi skupina za sodelovanje (na področju varnosti omrežnih in informacijskih sistemov), mreža skupin CSIRT in Evropska mreža organizacij za zvezo za kibernetske krize (mreža EU-CyCLONe).

17 EU je leta 2021 ustanovila Evropski kompetenčni center za kibernetsko varnost, ki je začel delovati maja 2023 in ga bo podpirala mreža 27 nacionalnih koordinacijskih centrov, po en iz vsake države članice, od katerih so nekateri tudi nacionalni centri za usklajevanje. Kompetenčni center bo pristojen za izvajanje kibernetskovarnostne komponente PDE, razen kibernetskovarnostne rezerve EU, ki jo bo izvajala Komisija, delovanje in upravljanje te rezerve pa se lahko zaupa agenciji ENISA.

18 Komisija je ustanovila tudi skupno kibernetsko enoto, ki jo je napovedala leta 2020 v strategiji EU za kibernetsko varnost in nadalje opredelila v priporočilu iz leta 2021.

19 Komisija je aprila 2023 napovedala ustanovitev akademije za kibernetske veščine, tj. nove pobude za zapolnitev vrzeli na področju strokovnjakov za kibernetsko varnost in povečanje števila zaposlenih v kibernetskem sektorju EU.

20 Glede na navedeno Sodišče meni, da lahko zaradi predlagane uredbe celotno kibernetskovarnostno okolje EU postane bolj kompleksno. Obstaja možnost prekrivanja med obstoječo mrežo skupin CSIRT in centri za varnostne operacije. Komisija je v prvem razdelku obrazložitvenega memoranduma sicer navedla, da bi morale čezmejne platforme centrov za varnostne operacije pomeniti novo zmogljivost, ki bi dopolnjevala mrežo skupin CSIRT. Vendar Sodišče ugotavlja, da so si nekatere naloge in cilji nacionalnih centrov za varnostne operacije, čezmejnih centrov za varnostne operacije, skupin CSIRT in mreže skupin CSIRT podobne (npr. odkrivanje groženj in odzivanje nanje, obveščevalni podatki o kibernetskih grožnjah in situacijsko zavedanje). To tveganje bi bilo načeloma mogoče ublažiti s postopno konsolidacijo zadevnih struktur, zlasti nacionalnih centrov za varnostne operacije in skupin CSIRT ter čezmejnih centrov za varnostne operacije. Poleg tega bi bilo treba v predlogu pojasniti, kako naj te strukture medsebojno sodelujejo, in sicer z določitvijo jasnih ureditev upravljanja in odgovornosti, da se zagotovi uspešno usklajevanje in dosežejo sinergije.

Izmenjava informacij

21 Sodišče je v Posebnem poročilu 05/2022[3] ugotovilo, da si institucije, organi in agencije EU med seboj niso sistematično izmenjevali ključnih relevantnih informacij o kibernetski varnosti, niti v primerih, ko so bili k temu zavezani. Dodaten problem za uspešno izmenjavo informacij so bile težave z interoperabilnostjo, zaradi katerih je ovirana varna komunikacija. Ugotovitve iz poročila so se sicer nanašale na to razmeroma majhno in homogeno skupino akterjev EU, vendar Sodišče meni, da bo ta izziv v bolj kompleksnem in raznolikem kibernetskovarnostnem okolju na ravni držav članic vse pomembnejši.

22 V členu 4 predlagane uredbe je določeno, da bi morali nacionalni centri za varnostne operacije delovati kot „referenčna točka in točka dostopa” do drugih javnih in zasebnih organizacij na nacionalni ravni za zbiranje in analiziranje informacij o kibernetskovarnostnih grožnjah in incidentih. Vendar trenutno ni zahtev glede poročanja na ravni EU za javne in zasebne organizacije (vključno z nacionalnimi skupinami CSIRT, zasebnimi centri za varnostne operacije ter tako imenovanimi „bistvenimi in pomembnimi subjekti” iz revidirane direktive o varnosti omrežij in informacij) nacionalnim centrom za varnostne operacije. Zato obstaja tveganje, da

[3] Posebno poročilo 05/2022 –Kibernetska varnost institucij, organov in agencij EU: raven pripravljenosti na splošno ni sorazmerna z grožnjami.

nacionalni centri za varnostne operacije ne bodo prejeli potrebnih podatkov ali informacij.

23 Komisija je v razdelku 2.2.2 ocene finančnih posledic zakonodajnega predloga, priložene predlogu, opredelila tveganje, da si države članice morda na platformah čezmejnih centrov za varnostne operacije ali med čezmejnimi platformami in drugimi ustreznimi subjekti na ravni EU morda ne bodo izmenjevale zadostne količine ustreznih informacij o kibernetskih grožnjah. Zaradi te nezadostne izmenjave informacij bi lahko bila ogrožena uspešnost in dodana vrednost evropskega kibernetskega ščita.

24 Sodišče zato pozdravlja, da predlog v členih 4, 5 in 6 vsebuje posebne določbe za zmanjšanje tveganj, povezanih z nezadostno izmenjavo informacij. V predlogu je določeno, da bodo sredstva EU nacionalnim centrom za varnostne operacije na voljo le, če se zavežejo, da bodo sodelovali v čezmejnem centru za varnostne operacije. Vendar Sodišče ugotavlja, da lahko nacionalni centri za varnostne operacije v primeru, če v čezmejnem centru ne sodelujejo, finančno podporo, ki so jo prejeli v prvih dveh letih, obdržijo. Poleg tega je v predlagani uredbi določeno, da se člani čezmejnih centrov za varnostne operacije zavežejo soupoabi „znatne količine podatkov” in da v pisni konzorcijski pogodbi vzpostavijo okvir upravljanja.

25 Poleg tega je v členu 7 predloga določeno, da morajo čezmejni centri za varnostne operacije relevantne informacije v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti „nemudoma” zagotoviti mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji. Sodišče poudarja, da je treba zagotoviti ustrezno izvrševanje te določbe.

26 V skladu s členom 6 predlagane uredbe lahko Komisija z izvedbenimi akti določi pogoje za interoperabilnost med čezmejnimi centri za varnostne operacije. V členu 8 je določeno, da lahko Komisija sprejme tudi izvedbene akte, s katerimi določi tehnične zahteve za države članice, v skladu s katerimi morajo te zagotavljati visoko raven varnosti podatkov in fizično varnost infrastrukture. O teh pogojih in zahtevah bi se bilo treba hitro dogovoriti, da ne bi prišlo do vzporednega razvoja sistemov, ki niso združljivi, in da se znižajo stroški.

Tveganja, povezana z mehanizmom za izredne kibernetske razmere

Vzpostavitev kibernetskovarnostne rezerve EU

27 Sodišče je v Posebnem poročilu 05/2022 ugotovilo, da CERT-EU, skupina EU za odzivanje na računalniške grožnje, ki institucijam, organom in agencijam EU zagotavlja podporo pri odzivanju, v času revizije ni delovala 24 ur na dan, 7 dni v tednu.

28 V členu 14 predlagane uredbe je določeno, da bo Komisija ob podpori agencije ENISA ocenila zahtevke za podporo iz kibernetskovarnostne rezerve EU in da bo odgovor poslan „nemudoma". V predlagani uredbi je v primeru več hkratnih zahtevkov za njihovo prednostno razvrstitev določenih nekaj meril. V skladu s členom 13 lahko Komisija z izvedbenimi akti natančneje določi podrobne ureditve za zagotavljanje podpore iz rezerve.

29 Za Sodišče je ključnega pomena, da pri odzivu Komisije ne pride do zamud zaradi vrstnega reda, v katerem je bila vložena prošnja za storitve podpore iz kibernetskovarnostne rezerve EU. Vendar v predlogu ni vnaprej določenega roka in zahteve, da se sprejmejo organizacijski ukrepi za njegovo dosego.

Odstopanje od načela enoletnosti

30 Eno od temeljnih načel proračuna EU je njegova enoletnost, kar pomeni, da se odobritve, knjižene v proračun, odobrijo za proračunsko leto, ki traja do 31. decembra. Neporabljene odobritve za prevzem obveznosti in odobritve plačil se v naslednje proračunsko leto ne prenesejo samodejno. To načelo je določeno v poglavju 2 finančne uredbe.

31 Predlagana uredba v členu 19 odstopa od tega načela, in sicer v zvezi s financiranjem ukrepov v okviru mehanizma za izredne kibernetske razmere. V zadevnem členu je določeno, da se neporabljene odobritve za prevzem obveznosti in odobritve plačil za ukrepe, povezane s pripravljenostjo, odzivanjem in medsebojno pomočjo, samodejno prenesejo ter se lahko prevzamejo in izplačajo do 31. decembra naslednjega proračunskega leta. Komisija je v drugem delu obrazložitvenega memoranduma pojasnila, da je ta prožnost v zvezi z upravljanjem proračuna potrebna zaradi „nepredvidljive, izjemne in posebne narave kibernetskovarnostne krajine in kibernetskih groženj".

32 Kar zadeva pripravljenost, bi bilo po mnenju Sodišča treba usklajeno preskušanje pripravljenosti subjektov šteti med načrtovane dejavnosti, zaradi česar v splošnem meni, da to preskušanje ni niti nepredvidljivo niti izjemno. Sodišče meni, da pri takšnih načrtovanih dejavnosti ni treba odstopati od osnovnega načela enoletnosti.

33 Ker pa se bosta kibernetskovarnostna rezerva EU in medsebojna pomoč uporabljali le v odziv na nepredvidljive dogodke, Sodišče meni, da je utemeljitev za to odstopanje lahko upravičena le v tem primeru.

34 Zaradi jasnosti in v skladu s pripravo drugih uredb, kot sta mehanizem Unije na področju civilne zaščite ali Instrument za sosedstvo ter razvojno in mednarodno sodelovanje – Globalna Evropa, bi moralo biti v predlagani uredbi po mnenju Sodišča določeno, da je samodejni prenos neporabljenih odobritev omejen na naslednje leto.

Tveganja, povezana z mehanizmom za pregledovanje kibernetskih incidentov

35 V skladu s členom 18 predlagane uredbe mora agencija ENISA na zahtevo Komisije, mreže EU-CyCLONe ali mreže skupin CSIRT pregledati in oceniti grožnje, ranljivosti in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskovarnostnim incidentom ali takim incidentom velikih razsežnosti. Agencija sodeluje z vsemi ustreznimi deležniki in pripravi poročilo o pregledu incidenta, v katerem navede glavne vzroke, ranljivosti in pridobljena spoznanja.

36 Sodišče meni, da je to pomemben mehanizem povratnih informacij, s katerim bo lahko EU nenehno krepila svoje zmogljivosti za odkrivanje kibernetskih groženj in incidentov ter pripravljenost in odzivanje nanje. Vendar predlaga, da se v predlagani uredbi določi najdaljši rok, v katerem agencija ENISA po vsakem incidentu predloži poročilo, da se zagotovijo pravočasne povratne informacije. Poleg tega je v predlogu navedeno, da bi moralo poročilo po potrebi vključevati priporočila za izboljšanje kibernetske drže EU. Vendar ni določeno, kako naj bi se izvajanje priporočil spremljalo.

Spremljanje smotrnosti in ocena politike

37 S členom 19 predlagane uredbe naj bi se spremenila Priloga II k uredbi PDE z uvedbo novega merljivega kazalnika, in sicer „število ukrepov za podporo pripravljenosti in odzivanju na kibernetskovarnostne incidente v okviru mehanizma za izredne kibernetske razmere”. Ta kazalnik dopolnjuje dva obstoječa kazalnika,

namenjena spremljanju napredka pri doseganju specifičnega cilja PDE na področju kibernetske varnosti in zaupanja in pri poročanju o njem, tj. „[š]tevilo skupno naročenih infrastruktur ali orodij za kibernetsko varnost ali obojega” ter „[š]tevilo uporabnikov in uporabniških skupnosti, ki imajo dostop do evropskih zmogljivosti za kibernetsko varnost”.

38 Po mnenju Sodišča se bodo s predlaganim novim kazalnikom merili le izložki in zagotavljal omejen vpogleda v uporabo in rezultate evropskega kibernetskega ščita in mehanizma za izredne kibernetske razmere.

39 V skladu s členom 20 bo morala Komisija najpozneje štiri leta po datumu začetka uporabe te uredbe Evropskemu parlamentu in Svetu predložiti poročilo o oceni in njenem pregledu.

40 Sodišče meni, da bi morala ocena temeljiti na zadostnih in zanesljivih podatkih, vendar se morajo EU in njene države članice zaradi hitro spreminjajočih se groženj stalno prilagajati in biti inovativne. Zato meni, da je časovni okvir ocene, kot je trenutno predlagan, morda prepozen za novo programsko obdobje. Poleg tega bodo do konca leta 2027 prevzete obveznosti za celotni znesek, predviden v proračunu za specifični cilj PDE v zvezi s kibernetsko varnostjo in zaupanjem.

Zaključne pripombe

41 V predlaganem aktu EU o kibernetski solidarnosti so določeni ukrepi za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje. Sodišče pozdravlja cilje predloga za krepitev skupne kibernetske odpornosti EU.

42 V mnenju Sodišča so poudarjena nekatera ugotovljena tveganja in to, kako bi se lahko izvajali ukrepi iz predloga. Sodišče zlasti poudarja tveganja, da bosta delovanje evropskega kibernetskega ščita in njegova trajnost postala odvisna od financiranja EU, da bo njegovo delovanje ovirano zaradi pomanjkljive izmenjave informacij ter da bo celotno kibernetskovarnostno okolje EU zaradi predlaganih ukrepov postalo bolj kompleksno.

43 Sodišče na podlagi pregleda zakonodajnega predloga predlaga, naj **Komisija in zakonodajalca**:

— dajejo na voljo ocene stroškov v zvezi z vzpostavitvijo in izvajanjem predlaganih ukrepov ter tako povečajo transparentnost (glej odstavek ***10***),

— pojasnijo, kako naj nacionalni centri za varnostne operacije, čezmejni centri za varnostne operacije, skupine CSIRT in mreža skupin CSIRT medsebojno sodelujejo, in sicer z določitvijo jasnih ureditev upravljanja in odgovornosti, da se zagotovi uspešno usklajevanje in dosežejo sinergije (odstavek ***20***),

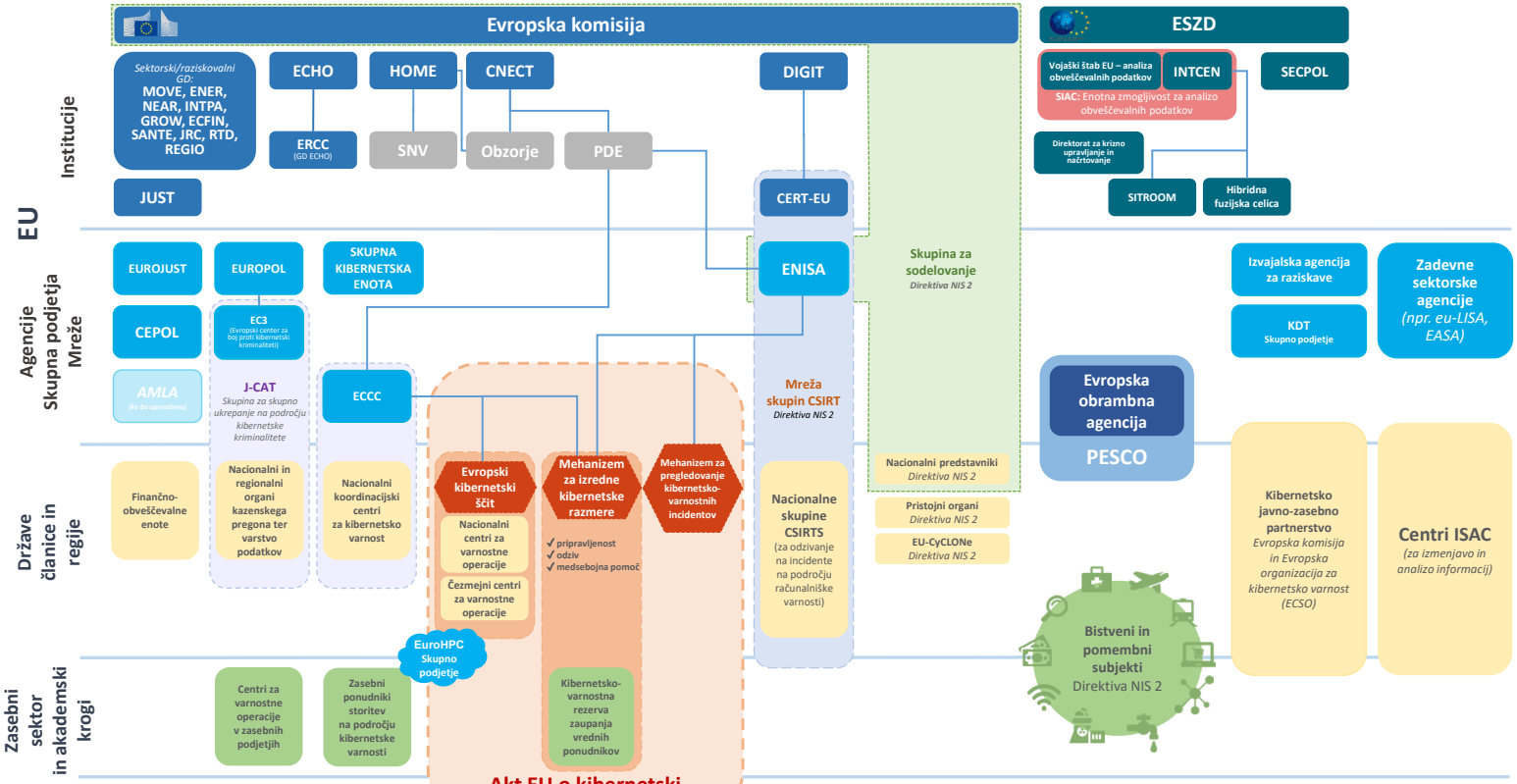
— zagotovijo, da pri odzivu Komisije na prošnje za storitve podpore iz kibernetskovarnostne rezerve EU ne pride do zamud zaradi vrstnega reda, v katerem je bila prošnja vložena (odstavek ***29***),

— omejijo odstopanje od načela enoletnosti na ukrepe odzivanja in medsebojno pomoč ter določijo, da je samodejni prenos neporabljenih odobritev omejen na naslednje leto (odstavki ***32***–***34***),

— določijo najdaljši rok, v katerem agencija ENISA po vsakem incidentu predloži poročilo, da se zagotovijo pravočasne povratne informacije (odstavek ***36***),

— časovni okvir, v katerem mora Komisija predložiti poročilo o oceni in pregledu uredbe, prestavijo na zgodnejše obdobje (odstavek ***40***).

Priloga – Evropsko kibernetskovarnostno okolje



AMLA: Organ za preprečevanje pranja denarja
CEPOL: Agencija Evropske unije za usposabljanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj
CMPD: Direktorat za krizno upravljanje in načrtovanje
GD CONNECT: Generalni direktorat za komunikacijska omrežja, vsebine in tehnologijo
GD ECFIN: Generalni direktorat za ekonomske in finančne zadeve
GD ECHO: Generalni direktorat za Evropsko civilno zaščito in evropske operacije humanitarne pomoči
GD ENER: Generalni direktorat za energetiko
GD GROW: Generalni direktorat za notranji trg, industrijo, podjetništvo ter mala in srednja podjetja
GD HOME: Generalni direktorat za migracije in notranje zadeve
GD INTPA: Generalni direktorat za mednarodna partnerstva

GD JUST: Generalni direktorat za pravosodje in potrošnike
GD MOVE: Generalni direktorat za mobilnost in promet
GD NEAR: Generalni direktorat za sosedstvo in širitvena pogajanja
GD REGIO: Generalni direktorat za regionalno in mestno politiko
GD RTD: Generalni direktorat za raziskave in inovacije
GD SANTE: Generalni direktorat za zdravje in varnost hrane
GD DIGIT: Generalni direktorat za informatiko

EASA: Agencija Evropske unije za varnost v letalstvu
EC3: Europolov Evropski center za boj proti kibernetski kriminaliteti
ECCC: Evropski kompetenčni center za kibernetsko varnost
ECSO: Evropska organizacija za kibernetsko varnost
EDA: Evropska obrambna agencija
ESZD: Evropska služba za zunanje delovanje
ERCC: Center za usklajevanje nujnega odziva
EU-CyCLONe: Evropska organizacijska mreža za povezovanje v kibernetski krizi
EuroHPC: Evropsko visokozmogljivostno računalništvo
EUROJUST: Agencija Evropske unije za pravosodno sodelovanje v kazenskih zadevah

EUROPOL: Agencija Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj
INTCEN: Obveščevalni in situacijski center Evropske unije
SNV: Sklad za notranjo varnost
JRC: Skupno raziskovalno središče
KDT: Ključne digitalne tehnologije
Direktiva NIS: direktiva o varnosti omrežij in informacij
PESCO: Stalno strukturno sodelovanje
SECPOL: Varnostna politika in preprečevanje konfliktov
SITROOM: situacijska soba

Vir: Evropsko računsko sodišče

To poročilo je sprejel senat III, ki ga vodi članica Evropskega računskega sodišča Bettina Jakobsen, v Luxembourgu na zasedanju 26. septembra 2023.

Za Evropsko računsko sodišče

Tony Murphy
predsednik

AVTORSKE PRAVICE

Politika Evropskega računskega sodišča (Sodišča) glede ponovne uporabe je določena v njegovem sklepu o politiki odprtih podatkov in ponovni uporabi dokumentov *ECA Decision No 6-2019*.

Če ni drugače navedeno (npr. v posameznih obvestilih o avtorskih pravicah), so vsebine Sodišča, ki so v lasti EU, pod licenco *Creative Commons Attribution 4.0 International (CC BY 4.0)*. Praviloma je zato ponovna uporaba dovoljena, če se ustrezno navede vir in označijo morebitne spremembe. Kdor ponovno uporabi vsebine Sodišča, ne sme potvoriti prvotnega pomena ali sporočila. Sodišče ni odgovorno za morebitne posledice ponovne uporabe.

Če so na gradivu prikazane določljive fizične osebe, npr. na fotografijah uslužbencev Sodišča, ali če gradivo vsebuje dela tretjih oseb, je treba pridobiti dodatne pravice.

Kadar je pridobljeno tako dovoljenje, se z njim razveljavi in nadomesti zgoraj omenjeno splošno dovoljenje, zato morajo biti v njem jasno navedene morebitne omejitve glede uporabe.

Za uporabo in prikazovanje vsebin, katerih lastnica ni EU, je morda treba pridobiti dovoljenje neposredno od imetnikov avtorskih pravic.

Programska oprema ali dokumenti, za katere veljajo pravice industrijske lastnine, kot so patenti, blagovne znamke, registrirani modeli, logotipi in imena, niso vključeni v politiko Sodišča glede ponovne uporabe.

Na spletiščih institucij Evropske unije znotraj domene europa.eu so povezave do spletišč tretjih oseb. Ker Sodišče na ta spletišča ne more vplivati, vas poziva, da preberete njihove dokumente o politiki glede varstva osebnih podatkov in avtorskih pravic.

Uporaba logotipa Sodišča

Logotip Sodišča se ne sme uporabljati brez predhodnega soglasja Sodišča.