Vijeće
Europske unije

Bruxelles, 22. siječnja 2026.
(OR. en)

5611/26
ADD 2

Međuinstitucijski predmeti:
2026/0011 (COD)
2026/0012 (COD)

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

POPRATNA BILJEŠKA

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	21. siječnja 2026.
Za:	Thérèse BLANCHET, glavna tajnica Vijeća Europske unije
Br. dok. Kom.:	SWD(2026) 12 final
Predmet:	RADNI DOKUMENT SLUŽBI KOMISIJE SAŽETAK IZVJEŠĆA O PROCJENI UČINKA priložen dokumentima Prijedlog uredbe Europskog parlamenta i Vijeća o Agenciji Europske unije za kibernetičku sigurnost (ENISA), Europskom okviru za kibernetičkosigurnosnu certifikaciju i sigurnosti lanca opskrbe IKT-om te o stavljanju izvan snage Uredbe (EU) 2019/881 (Akt o kibernetičkoj sigurnosti 2) i Prijedlog direktive Europskog parlamenta i Vijeća o izmjeni Direktive (EU) 2022/2555 radi uvođenja mjera pojednostavnjenja i usklađivanja s [Prijedlogom Akta o kibernetičkoj sigurnosti 2]

Za delegacije se u prilogu nalazi dokument SWD(2026) 12 final.

Priloženo: SWD(2026) 12 final

EUROPSKA
KOMISIJA

Strasbourg, 20.1.2026.
SWD(2026) 12 final

RADNI DOKUMENT SLUŽBI KOMISIJE

SAŽETAK IZVJEŠĆA O PROCJENI UČINKA

priložen dokumentima

Prijedlog uredbe Europskog parlamenta i Vijeća o Agenciji Europske unije za kibernetičku sigurnost (ENISA), Europskom okviru za kibernetičkosigurnosnu certifikaciju i sigurnosti lanca opskrbe IKT-om te o stavljanju izvan snage Uredbe (EU) 2019/881 (Akt o kibernetičkoj sigurnosti 2)

i

Prijedlog direktive Europskog parlamenta i Vijeća o izmjeni Direktive (EU) 2022/2555 radi uvođenja mjera pojednostavnjenja i usklađivanja s [Prijedlogom Akta o kibernetičkoj sigurnosti 2]

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Sažetak procjene učinka

Cilj

Glavni je cilj ove procjene učinka ocijeniti u kolikoj su mjeri postojeći propisi primjereni za odgovor na sve veće kibernetičkosigurnosne prijetnje u cijelom EU-u. U njoj se predlaže integrirani skup opcija politike kojima je cilj ojačati Agenciju Europske unije za kibernetičku sigurnost (ENISA), reformirati Europski okvir za kibernetičkosigurnosnu certifikaciju (ECCF) i olakšati poštovanje postojećeg zakonodavnog okvira za kibernetičku sigurnost. Naglašava se da je važno prilagoditi pravila o kibernetičkoj sigurnosti kako bi držala korak s tehnološkim napretkom i potražnjom na tržištu, a da se pritom očuva konkurentnost i vodi računa o učincima na okoliš.

Izjava o problemu

Unatoč postojećim mjerama situacija u kibernetičkosigurnosnom okruženju EU-a i dalje je zahtjevna jer su prijetnje sve složenije. Nedovoljna koordinacija među državama članicama i drugim akterima na razini EU-a, spora implementacija političkih rješenja te regulatorne prepreke i kompleksna pravila otežavaju učinkovito upravljanje kibernetičkom sigurnošću. Ti problemi uzrokuju veće troškove za poduzeća i javna tijela, porast rizika od kibernetičkih incidenata i nedosljednu zaštitu građana.

Opravdanje za djelovanje EU-a

Kibernetičkosigurnosne prijetnje nadilaze nacionalne granice i zato je za snažan odgovor potrebno primijeniti jedinstven pristup. Intervencijom na razini EU-a osigurava se dosljedna zaštita, povećava konkurentnost zahvaljujući jednakim uvjetima i olakšava slobodno kretanje digitalnih usluga i proizvoda na jedinstvenom tržištu. Usklađivanjem na razini EU-a također se smanjuje administrativno opterećenje jer se olakšava poštovanje pravila i pojednostavnjuju postupci.

Opcije politike i najpoželjnije opcije

U ovom se izvješću analiziraju četiri područja intervencije, a za svako od njih razmatra se niz opcija politike s obzirom na specifične ciljeve koje treba ostvariti: 1. mandat ENISA-e (obuhvaćen i postojećim Aktom o kibersigurnosti); 2. europski okvir za kibernetičkosigurnosnu certifikaciju (obuhvaćen i postojećim Aktom o kibersigurnosti) i 3. ciljane izmjene Direktive NIS 2 radi pojednostavnjenja te povezivanja s mandatom ENISA-e i europskim okvirom za kibernetičkosigurnosnu certifikaciju. Svaki od tih skupova opcija zasebno je područje intervencije, ali ti su skupovi međusobno povezani i relevantni jedni za druge.

Opcije za rješavanje problema neusklađenosti okvira politike EU-a za kibernetičku sigurnost i potreba dionika u sve neprijateljskijem okruženju

Opcija A.1: *Razjašnjenje mandata ENISA-e i utvrđivanje prioriteta* – Tom bi se opcijom uspostavio jasan i stabilan okvir za zadaće ENISA-e tako što bi se obuhvatile zadaće utvrđene u drugim zakonodavnim aktima.

Opcija A.2: *Reforma mandata ENISA-e* – Tom bi se opcijom stavio izvan snage i zamijenio Akt o kibersigurnosti te bi se na taj način reformirao mandat Agencije.

Opcija A.3: *Reforma mandata ENISA-e s težištem na operativnoj potpori* – Ta bi se opcija temeljila na opciji A.2. Uz to, ENISA bi razvila kapacitete zahvaljujući kojima bi na zahtjev pojedine države članice mogla subjektima iz Direktive NIS 2 pružati izravnu potporu u odgovoru na kibernetičkosigurnosne incidente i oporavku od njih.

Opcije za Europski okvir za kibernetičkosigurnosnu certifikaciju (ECCF)

Opcija B.1: *Razjašnjenje područja primjene, elemenata i ciljeva ECCF-a te uvođenje mehanizma održavanja* – Tom bi se opcijom uveo novi mehanizam održavanja programa nakon njihova donošenja, za što bi bila zadužena ENISA.

Opcija B.2: *Reforma ECCF-a revizijom njegovih postupaka i proširenjem područja primjene radi lakšeg pojednostavnjenja poštovanja propisa* – Tom bi se opcijom Akt o kibersigurnosti stavio izvan snage i zamijenio novom uredbom. Povrh opcije B.1 revidirao bi se postupak za podnošenje zahtjeva, izradu i donošenje programa kako bi se povećale odgovornost i učinkovitost.

Opcija B.3: *Reforma ECCF-a kao u opciji B.2 i uvođenje obveznog certificiranja stanja kibernetičke sigurnosti* – Ta bi se opcija temeljila na opciji B.2, ali imala bi za cilj dodatno pojačati učinak okvira jer bi se umjesto oslanjanja isključivo na dobrovoljno certificiranje subjekata za ključne subjekte obuhvaćene Direktivom NIS 2 uvelo obvezno certificiranje s obzirom na specifične scenarije rizika.

Opcije pojednostavnjenja

Opcija C.1: *Primjena pristupa neobvezujućeg prava i nezakonodavnih instrumenata, uključujući upotrebu postojećih ovlasti (donošenje provedbenih akata na temelju članka 21. stavka 5. i članka 23. stavka 11. Direktive NIS 2)* – Tom se opcijom predviđa donošenje provedbenih akata na temelju postojećih ovlasti iz Direktive NIS 2 kako bi se postigla veća usklađenost mjera upravljanja kibernetičkosigurnosnim rizicima, pragova za izvješćivanje o incidentima te informacija, formata i postupaka obavješćivanja, kao i donošenje niza smjernica radi poboljšanja pravne sigurnosti i usklađivanja provedbe.

Opcija C.2: *Ciljana intervencija – daljnje pojednostavnjenje sukladnosti s relevantnim zakonodavnim okvirom Unije za kibernetičku sigurnost* – Ta opcija uključuje ograničenu intervenciju u obliku izmjena Akta o kibersigurnosti i Direktive NIS 2 kako bi se pojednostavnili određeni aspekti okvira za kibernetičku sigurnost, što obuhvaća prilagodbu područja primjene, maksimalno usklađivanje provedbenih akata, dokazivanje sukladnosti putem certifikacije i donošenje skupa smjernica kako je predviđeno u opciji C.1.

Opcija C.3: *Usklađivanje mjera za kibernetičku sigurnost utvrđenih u propisima Unije* – Ta bi se opcija temeljila na opciji C.2 i njome bi se iz sektorskih propisa uklonile sve mjere

upravljanja kibernetičkosigurnosnim rizicima ili ovlasti povezane s takvim mjerama. Umjesto njih bi se izmjenama ekosustava Direktive NIS 2 uveli pojednostavnjeni zahtjevi za sve vrste subjekata i tako postigla bolja usklađenost.

Opcije za sigurnost lanca opskrbe IKT-om

Opcija D.1: *Primjena neobvezujućeg pravnog pristupa za uklanjanje kibernetičkosigurnosnih rizika za lance opskrbe IKT-om* – Ta opcija ne bi obuhvaćala regulatornu intervenciju na razini EU-a, već bi Komisija povećala broj koordiniranih procjena rizika i dobrovoljnih paketa instrumenata.

Opcija D.2: Ad hoc *regulatorna intervencija za kodifikaciju paketa instrumenata za 5G tehnologije* – U okviru te opcije kodificirale bi se mjere iz paketa instrumenata za 5G tehnologije i uvela bi se obveza za države članice da osiguraju da se u ključnoj mrežnoj imovini ne upotrebljavaju komponente visokorizičnih dobavljača.

Opcija D.3: *Sveobuhvatni i horizontalni okvir za uklanjanje kibernetičkosigurnosnih rizika u lancima opskrbe IKT-om* – Tom bi se opcijom uspostavio horizontalni, tehnološki i sektorski neutralan regulatorni okvir za uklanjanje netehničkih kibernetičkosigurnosnih rizika u lancima opskrbe IKT-om.

Opsežnim analizama utvrđeno je da najpoželjniji paket politika čine: opcija A.2 – reforma mandata ENISA-e; opcija B.2 – reforma ECCF-a revizijom postupaka i proširenjem područja primjene kako bi se olakšalo pojednostavnjenje regulatorne sukladnosti; opcija C.2 – ciljana intervencija – daljnje pojednostavnjenje sukladnosti s relevantnim zakonodavnim okvirom Unije za kibernetičku sigurnost i opcija D.3 – sveobuhvatni i horizontalni okvir za uklanjanje kibernetičkosigurnosnih rizika u lancima opskrbe IKT-om.

Ta kombinacija uravnotežen je odgovor na identificirane nedostatke politika i znatno pridonosi djelotvornosti, učinkovitosti i usklađenosti u cijelom EU-u.

Glavni učinci

Analiza troškova i koristi: Procjenjuje se da će zbog prelaska na predloženi regulatorni okvir ENISA u razdoblju od pet godina na obavljanje svojih novih zadaća utrošiti do 161,3 milijuna EUR, a javna tijela u cijelom EU-a u tom istom razdoblju do 80 milijuna EUR za nadzor (uzimajući u obzir relevantne uštede troškova). Kad je riječ o poduzećima, u prijelaznom bi trogodišnjem razdoblju operatorima pokretnih mreža postupno stavljanje određene visokorizične opreme izvan upotrebe moglo prouzročiti godišnje troškove od 3,4 do 4,3 milijarde EUR, a ulaganja u pouzdane dobavljače mogla bi istodobno doseći i do 2 milijarde EUR godišnje. Nadalje, očekuje se da će pojednostavnjene i smanjene obveze usklađivanja potaknuti uštede za poduzeća u iznosu do 14,6 milijardi EUR. Uz to, građani, javna tijela i poduzeća imali bi znatne koristi zahvaljujući boljem ukupnom stanju kibernetičke sigurnosti i tehnološke suverenosti EU-a te poticanju inovacija i konkurentnosti, za koje se očekuje da će dugoročno u velikoj mjeri nadoknaditi početne rashode.

Tržišno natjecanje: Zahvaljujući najpoželjnijim opcijama tržišno natjecanje u EU-u bit će ravnopravnije jer se smanjuje rascjepkanost i usklađuju propisi, a poduzeća dobivaju jasnije smjernice za postizanje sukladnosti i uvođenje inovacija.

Provjera usklađenosti s klimatskom politikom: U procjeni je razmotren mogući utjecaj svake opcije na okoliš. Posebna pozornost posvećena je energetskoj učinkovitosti, emisijama povezanima s putovanjima i konsolidaciji infrastrukture. Najpoželjnije opcije A.2., B.2. i C.2. imaju ograničen utjecaj na okoliš, dok se u opciji D.3. u obzir uzima okolišna neutralnost jer se vodi računa o životnom ciklusu proizvoda i prijelaznim razdobljima za zamjenu ključne imovine. To je u skladu s EU-ovim promicanjem održivosti.

Digitalno kao standard: Naglasak na pojednostavnjenim digitalnim procesima pokazuje predanost EU-a pristupu „digitalizacija na prvom mjestu", koji omogućuje bržu i pouzdaniju razmjenu podataka i donošenje odluka. Opcija D.3 mogla bi također imati velik učinak na digitalizaciju jer bi podrazumijevala zamjenu komponenata koje dobavljaju subjekti iz trećih zemalja ili pod kontrolom subjekata iz trećih zemalja s dvojbenom kibernetičkom sigurnošću.

Pojednostavnjenje i smanjenje opterećenja: Najpoželjnije opcije pridonose pojednostavnjenju jer se njima pojašnjava područje primjene i uvode mjere za pojednostavnjenje sukladnosti i nadzora te tako smanjuje administrativno opterećenje. Načelo „jedan za jedan" uvaženo je tako što se vodilo računa da se nove obveze kompenziraju smanjenjem opterećenja drugdje.

Zaključak

U ovoj procjeni učinka predstavljena je sveobuhvatna strategija za poboljšanje kibernetičke sigurnosti EU-a, uklanjanje regulatornih neučinkovitosti i pripremu digitalnog okruženja za buduće izazove. U njoj se preporučuje suradnički i kohezivni pristup prema kojem se reforme politika temelje na postojećim okvirima i istodobno prilagođavaju novim tehnološkim okolnostima. Tim mjerama EU želi izgraditi otporno, konkurentno i održivo digitalno gospodarstvo.