Svet
Evropske unije

Bruselj, 22. januar 2026
(OR. en)

Medinstitucionalni zadevi:
2026/0011 (COD)
2026/0012 (COD)

5611/26
ADD 2

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

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	21. januar 2026
Prejemnik:	Thérèse BLANCHET, generalna sekretarka Sveta Evropske unije
Št. dok. Kom.:	SWD(2026) 12 final
Zadeva:	DELOVNI DOKUMENT SLUŽB KOMISIJE POVZETEK POROČILA O OCENI UČINKA Spremni dokument k Predlogu uredbe Evropskega parlamenta in Sveta o Agenciji Evropske unije za kibernetsko varnost (ENISA), evropskem certifikacijskem okviru za kibernetsko varnost in varnosti dobavne verige IKT ter razveljavitvi Uredbe (EU) 2019/881 (Akt o kibernetski varnosti 2) in Predlogu direktive Evropskega parlamenta in Sveta o spremembi Direktive (EU) 2022/2555 glede ukrepov za poenostavitev in uskladitve s [predlogom akta o kibernetski varnosti 2]

Delegacije prejmejo priloženi dokument SWD(2026) 12 final.

Priloga: SWD(2026) 12 final

EVROPSKA
KOMISIJA

Strasbourg, 20.1.2026
SWD(2026) 12 final

DELOVNI DOKUMENT SLUŽB KOMISIJE

POVZETEK POROČILA O OCENI UČINKA

Spremni dokument

k Predlogu uredbe Evropskega parlamenta in Sveta o Agenciji Evropske unije za kibernetsko varnost (ENISA), evropskem certifikacijskem okviru za kibernetsko varnost in varnosti dobavne verige IKT ter razveljavitvi Uredbe (EU) 2019/881 (Akt o kibernetski varnosti 2)

in

Predlogu direktive Evropskega parlamenta in Sveta o spremembi Direktive (EU) 2022/2555 glede ukrepov za poenostavitev in uskladitve s [predlogom akta o kibernetski varnosti 2]

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

Povzetek ocene učinka

Cilj

Glavni cilj te ocene učinka je oceniti ustreznost veljavnih predpisov pri obravnavanju spreminjajočih se kibernetskih groženj po vsej EU. V njej se predlaga celovit sklop možnosti politike za okrepitev Agencije Evropske unije za kibernetsko varnost (v nadaljnjem besedilu: agencija ENISA), reformo evropskega certifikacijskega okvira za kibernetsko varnost in poenostavitev doseganja skladnosti z obstoječim zakonodajnim okvirom na področju kibernetske varnosti. V tej oceni je poudarjen pomen prilagajanja kibernetskega upravljanja tehnološkemu napredku in povpraševanju na trgu ob hkratnem zagotavljanju konkurenčnosti in upoštevanju vplivov na okolje.

Opis težave

Kljub obstoječim prizadevanjem se okolje kibernetske varnosti v EU zaradi vse bolj zapletenih groženj še vedno sooča z velikimi izzivi. Nezadostno usklajevanje med državami članicami in drugimi akterji na ravni EU, zastoj pri izvajanju orodij politike ter regulativne ovire in zapletenost ovirajo učinkovito upravljanje kibernetske varnosti. Ti problemi podjetjem in javnim organom povzročajo višje stroške, povečujejo tveganja kibernetskih incidentov in se kažejo v nedoslednih ravneh zaščite državljanov.

Utemeljitev ukrepanja EU

Kibernetske grožnje presegajo nacionalne meje, zato je enoten pristop ključnega pomena za odločen odziv. Posredovanje na ravni EU zagotavlja dosledno zaščito, povečuje konkurenčnost z zagotavljanjem enakih konkurenčnih pogojev ter olajšuje prosti pretok digitalnih storitev in proizvodov na enotnem trgu. Harmonizacija na ravni EU prav tako zmanjšuje upravno breme s poenostavitvijo zagotavljanja skladnosti in postopkov.

Možnosti politike in prednostna možnost

V tem poročilu so analizirana štiri področja ukrepanja, od katerih vsako vključuje sklop možnosti politike, obravnavanih glede na specifične cilje, ki jih je treba doseči: (1) mandat agencije ENISA (ki je prav tako del sedanjega akta o kibernetski varnosti); (2) evropski certifikacijski okvir za kibernetsko varnost (ki je prav tako del sedanjega akta o kibernetski varnosti) ter (3) ciljno usmerjene spremembe direktive NIS 2 z namenom poenostavitve, pri čemer je ta točka povezana tudi z mandatom agencije ENISA in evropskim certifikacijskim okvirom za kibernetsko varnost. Vsak od teh sklopov možnosti je samostojno področje ukrepanja, hkrati pa so medsebojno povezani in relevantni.

Možnosti za obravnavanje neusklajenosti okvira politike EU za kibernetsko varnost in potreb deležnikov v vse bolj sovražnem okolju

Možnost A.1: *pojasnitev mandata agencije ENISA in določitev prednostnega razvrščanja* – ta možnost bi zagotovila jasen in stabilen okvir za naloge agencije ENISA z vključitvijo nalog, določenih v drugih zakonodajnih aktih.

Možnost A.2: *reforma mandata agencije ENISA* – ta možnost bi razveljavila in nadomestila akt o kibernetski varnosti ter s tem prenovila mandat agencije.

Možnost A.3: *reforma mandata agencije ENISA z močnim poudarkom na operativni podpori* – ta možnost bi temeljila na možnosti A.2. Poleg tega bi agencija ENISA razvila zmogljivosti za neposredno podporo subjektom iz direktive NIS 2 pri odzivanju na kibernetski incident in okrevanju po njem na zahtevo države članice.

Možnosti za evropski certifikacijski okvir za kibernetsko varnost

Možnost B.1: *pojasnitev področja uporabe, elementov in ciljev evropskega certifikacijskega okvira za kibernetsko varnost ter uvedba mehanizma vzdrževanja* – ta možnost bi zagotovila nov mehanizem vzdrževanja shem, ki ga bo po njihovem sprejetju izvajala agencija ENISA.

Možnost B.2: *reforma evropskega certifikacijskega okvira za kibernetsko varnost z revizijo njegovih postopkov in razširitvijo področja uporabe, da se olajša poenostavitev doseganja skladnosti z zakonodajo* – pri tej možnosti bi se akt o kibernetski varnosti razveljavil in nadomestil z novo uredbo. Poleg možnosti B.1 vključuje revizijo postopka v zvezi z zahtevki, razvojem in sprejetjem shem, da bi se izboljšali odgovornost in učinkovitost.

Možnost B.3: *reforma evropskega certifikacijskega okvira za kibernetsko varnost, kot je predvidena v možnosti B.2, in uvedba obveznega certificiranja položaja kibernetske varnosti* – ta možnost bi temeljila na možnosti B.2, vendar je namenjena nadaljnji krepitvi učinka okvira z uvedbo obveznega certificiranja za bistvene subjekte, zajete v direktivi NIS 2, ob upoštevanju določenih scenarijev tveganja namesto zanašanja le na prostovoljno certificiranje subjektov.

Možnosti za poenostavitev

Možnost C.1: *uporaba pristopa mehkega prava in nezakonodajnih instrumentov, vključno z uporabo obstoječih pooblastil (sprejetje izvedbenih aktov v skladu s členom 21(5) in členom 23(11) direktive NIS 2)* – ta možnost predvideva sprejetje izvedbenih aktov na podlagi obstoječih pooblastil iz direktive NIS 2, da se zagotovi višja stopnja harmonizacije ukrepov za obvladovanje tveganj za kibernetsko varnost, pragov za poročanje o incidentih ter informacij, oblik in postopkov priglasitev, skupaj s sprejetjem sklopa smernic za večjo pravno varnost in bolj usklajeno izvajanje.

Možnost C.2: *usmerjena intervencija – nadaljnja poenostavitev doseganja skladnosti z zadevnim zakonodajnim okvirom Unije za kibernetsko varnost* – ta možnost vključuje omejeno intervencijo s spremembami akta o kibernetski varnosti in direktive NIS 2, katerih cilj bi bil poenostavitev določenih vidikov okvira za kibernetsko varnost, vključno s prilagoditvami področja uporabe, največjo možno harmonizacijo za izvedbene akte, dokazovanjem skladnosti s certificiranjem in sprejetjem sklopa smernic, kot je predvideno v možnosti C.1.

Možnost C.3: *harmonizacija ukrepov, povezanih s kibernetsko varnostjo, določenih v zakonodaji Unije* – ta možnost bi temeljila na možnosti C.2 in iz sektorske zakonodaje odstranila vse ukrepe za obvladovanje tveganj za kibernetsko varnost ali pooblastila v zvezi s

takimi ukrepi. Namesto tega bi se ekosistem, vzpostavljen z direktivo NIS 2, spremenil, da bi se zagotovile racionalizirane zahteve za vse vrste subjektov, s čimer bi se zagotovila večja harmonizacija.

Možnosti za varnost v dobavnih verigah IKT

Možnost D.1: *uporaba pristopa mehkega prava za obravnavanje tveganj za kibernetsko varnost v dobavnih verigah IKT* – ta možnost ne bi zagotovila regulativnega ukrepanja na ravni EU. Namesto tega bi Komisija povečala število usklajenih ocen tveganja in prostovoljnih orodij.

Možnost D.2: ad hoc *regulativni ukrep za kodifikacijo nabora orodij 5G* – ta možnost bi kodificirala ukrepe iz nabora orodij 5G. Uvedla bi obveznost držav članic, da zagotovijo, da se komponente dobaviteljev z visokim tveganjem ne uporabljajo v ključnih sredstvih omrežja.

Možnost D.3: *celovit in horizontalen okvir za obravnavanje tveganj za kibernetsko varnost v dobavnih verigah IKT* – s to možnostjo bi se vzpostavil horizontalen, tehnološko in sektorsko nevtralen regulativni okvir za obravnavanje netehničnih tveganj za kibernetsko varnost v dobavnih verigah IKT.

Prednostni sveženj politik po obsežnih analizah vključuje: možnost A.2 – reformo mandata agencije ENISA; možnost B.2 – reformo evropskega certifikacijskega okvira za kibernetsko varnost z revizijo postopka in razširitvijo področja uporabe, da se olajša poenostavitev doseganja skladnosti z zakonodajo; možnost C.2 – ciljno usmerjeno posredovanje – nadaljnjo poenostavitev doseganja skladnosti z ustreznim zakonodajnim okvirom Unije za kibernetsko varnost ter možnost D.3 – celovit in horizontalen okvir za obravnavanje tveganj za kibernetsko varnost v dobavnih verigah IKT.

Ta kombinacija zagotavlja dobro uravnotežen odziv na opredeljene izzive politike ter znatno povečuje uspešnost, učinkovitost in skladnost po vsej EU.

Glavni učinki

Analiza stroškov in koristi: Zaradi prehoda na predlagani regulativni okvir bodo nastali stroški za agencijo ENISA, ki so ocenjeni na 161,3 milijona EUR v petih letih za izpolnjevanje njenih novih nalog, in za javne organe po vsej EU, in sicer do 80 milijonov EUR v petih letih za nadzor (ob upoštevanju ustreznih prihrankov pri stroških). Kar zadeva podjetja, bi lahko postopno opuščanje določene opreme z visokim tveganjem operaterjem mobilnih omrežij v triletnem prehodnem obdobju povzročilo letne stroške v višini 3,4 do 4,3 milijarde EUR, hkrati pa bi se naložbe v zaupanja vredne dobavitelje lahko povečale za do 2 milijardi EUR letno. Poleg tega naj bi racionalizirane in zmanjšane obveznosti glede skladnosti spodbudile prihranke pri stroških za podjetja v višini do 14,6 milijarde EUR. Prav tako bi izboljšanje splošnega položaja kibernetske varnosti in večja tehnološka suverenost EU ter spodbujanje inovacij in konkurenčnosti prinesli znatne koristi za državljane, javne organe in podjetja, s čimer naj bi se začetni odhodki na dolgi rok v veliki meri izravnali.

Konkurenčnost: Prednostne možnosti z zmanjšanjem razdrobljenosti trga in uskladitvijo predpisov krepijo konkurenčno enakost po vsej EU ter podjetjem zagotavljajo jasnejše poti do skladnosti in inovacij.

Preverjanje skladnosti s podnebnimi cilji: V oceni je bil upoštevan morebitni vpliv vsake možnosti na okolje. Posebna pozornost je bila namenjena energijski učinkovitosti, emisijam, povezanim s potovanji, in konsolidaciji infrastrukture. Prednostne možnosti A.2, B.2 in C.2 imajo omejen vpliv na okolje, medtem ko se pri možnosti D.3 upošteva okoljska nevtralnost ob upoštevanju življenjskega cikla proizvodov in prehodnih obdobij za zamenjavo ključnih sredstev. To je v skladu z zavezanostjo EU k trajnostnosti.

Privzeto digitalno: Poudarek na racionaliziranih digitalnih procesih kaže zavezanost EU k pristopu „najprej digitalno“, ki zagotavlja hitrejšo in zanesljivejšo izmenjavo podatkov in odločanje. Možnost D.3 bi prav tako lahko močno vplivala na digitalizacijo, saj bi vključevala zamenjavo komponent subjektov s sedežem v tretjih državah, za katere obstajajo pomisleki glede kibernetske varnosti, ali pod nadzorom subjektov iz takih tretjih držav.

Poenostavitev in zmanjšanje bremena: Prednostne možnosti prispevajo k poenostavitvi z uvedbo pojasnil glede področja uporabe in ukrepov za racionalizacijo skladnosti in nadzora, s čimer se zmanjšujejo upravna bremena. Upošteva se načelo „za enega sprejetega se eden odpravi“, tako da se zagotovi, da se nove obveznosti izravnajo z njihovim zmanjšanjem drugje.

Zaključek

V tej oceni učinka je predstavljena celovita strategija za izboljšanje kibernetske varnosti EU, odpravo regulativnih neučinkovitosti in pripravo digitalnega okolja na prihodnje izzive. Priporoča sodelovalen in povezan pristop, ki temelji na reformah politik v obstoječih okvirih, hkrati pa se prilagaja novim tehnološkim razmeram. EU si s temi ukrepi prizadeva zagotoviti odporno, konkurenčno in trajnostno digitalno gospodarstvo.