Rada
Európskej únie

V Bruseli 22. januára 2026
(OR. en)

Medziinštitucionálne spisy:
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

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	21. januára 2026
Komu:	Thérèse BLANCHETOVÁ, generálna tajomníčka Rady Európskej únie
Č. dok. Kom.:	SWD(2026) 12 final
Predmet:	PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE ZHRNUTIE SPRÁVY O POSÚDENÍ VPLYVU Sprievodný dokument Návrh nariadenia Európskeho parlamentu a Rady o Agentúre Európskej únie pre kybernetickú bezpečnosť (ENISA), európskom rámci certifikácie kybernetickej bezpečnosti a bezpečnosti dodávateľského reťazca IKT a o zrušení nariadenia (EÚ) 2019/881 (akt o kybernetickej bezpečnosti 2) a Návrh smernice Európskeho parlamentu a Rady, ktorou sa mení smernica (EÚ) 2022/2555, pokiaľ ide o zjednodušujúce opatrenia a zosúladenie s [návrhom aktu o kybernetickej bezpečnosti 2]

Delegáciám v prílohe zasielame dokument SWD(2026) 12 final.

Príloha: SWD(2026) 12 final

EURÓPSKA
KOMISIA

V Štrasburgu 20. 1. 2026
SWD(2026) 12 final

PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE

ZHRNUTIE SPRÁVY O POSÚDENÍ VPLYVU

Sprievodný dokument

Návrh nariadenia Európskeho parlamentu a Rady o Agentúre Európskej únie pre kybernetickú bezpečnosť (ENISA), európskom rámci certifikácie kybernetickej bezpečnosti a bezpečnosti dodávateľského reťazca IKT a o zrušení nariadenia (EÚ) 2019/881 (akt o kybernetickej bezpečnosti 2)

a

Návrh smernice Európskeho parlamentu a Rady, ktorou sa mení smernica (EÚ) 2022/2555, pokiaľ ide o zjednodušujúce opatrenia a zosúladenie s [návrhom aktu o kybernetickej bezpečnosti 2]

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

Zhrnutie posúdenia vplyvu

Cieľ

Hlavným cieľom tohto posúdenia vplyvu je zhodnotiť primeranosť súčasných predpisov pri riešení vyvíjajúcich sa hrozieb v oblasti kybernetickej bezpečnosti v EÚ. Navrhuje sa v ňom integrovaný súbor politických možností zameraných na posilnenie Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA), reformu európskeho rámca certifikácie kybernetickej bezpečnosti (ECCF) a zjednodušenie dodržiavania existujúceho legislatívneho rámca v oblasti kybernetickej bezpečnosti. V tomto posúdení sa zdôrazňuje význam úpravy riadenia kybernetického priestoru tak, aby sa zosúladilo s technologickým pokrokom a požiadavkami trhu, pričom sa zabezpečí konkurencieschopnosť a zohľadnia vplyvy na životné prostredie.

Vysvetlenie problému

Napriek existujúcemu úsiliu čelí prostredie kybernetickej bezpečnosti EÚ v kontexte čoraz zložitejších hrozieb stále veľkým výzvam. Nedostatočná koordinácia medzi členskými štátmi a ďalšími aktérmi na úrovni EÚ, viaznuce vykonávanie politických nástrojov a regulačné prekážky a zložitosť bránia účinnému riadeniu kybernetickej bezpečnosti. Výsledkom týchto problémov sú zvýšené náklady pre podniky a orgány verejnej správy, zvýšené riziko kybernetických incidentov a nejednotná úroveň ochrany občanov.

Odôvodnenie pre prijatie opatrenia EÚ

Kybernetickobezpečnostné hrozby presahujú hranice štátov, na rozhodnú reakciu je preto nevyhnutný jednotný prístup. Intervenciou na úrovni EÚ sa zabezpečí konzistentná ochrana, zvýši sa konkurencieschopnosť tým, že sa poskytnú rovnaké podmienky, a uľahčí sa voľný pohyb digitálnych služieb a produktov v rámci jednotného trhu. Harmonizáciou na úrovni EÚ sa takisto zníži administratívne zaťaženie zjednodušeným dodržiavaním predpisov a zjednodušenými postupmi.

Možnosti politiky a uprednostňovaná možnosť

V tejto správe sa analyzujú štyri oblasti intervencie, pričom každá z nich obsahuje súbor politických možností, ktoré sa zvažujú vzhľadom na konkrétne ciele, ktoré sa majú dosiahnuť: 1. mandát agentúry ENISA (takisto súčasť súčasného aktu o kybernetickej bezpečnosti); 2. ECCF (takisto súčasť súčasného aktu o kybernetickej bezpečnosti) a 3. cielené zmeny smernice NIS 2 zamerané na zjednodušenie, pričom sú prepojené aj s mandátom agentúry ENISA a ECCF. Každý z týchto súborov možností je samostatnou oblasťou intervencie a zároveň sú vzájomne prepojené a relevantné.

Možnosti riešenia nesúladu politického rámca EÚ v oblasti kybernetickej bezpečnosti a potrieb zainteresovaných strán v čoraz nepriateľskejšom prostredí

Možnosť A.1: *Objasnenie mandátu agentúry ENISA a stanovenie priorít* – Touto možnosťou by sa zabezpečil jasný a stabilný rámec pre úlohy agentúry ENISA začlenením úloh stanovených v iných právnych predpisoch.

Možnosť A.2: *Reforma mandátu agentúry ENISA* – Touto možnosťou by sa zrušil a nahradil akt o kybernetickej bezpečnosti, čím by sa zabezpečila revízia mandátu agentúry.

Možnosť A.3: *Reforma mandátu agentúry ENISA so silným zameraním na operačnú podporu* – Táto možnosť by nadväzovala na možnosť A.2. Okrem toho by agentúra ENISA vyvinula kapacity na priamu podporu subjektov smernice NIS 2 na žiadosť členského štátu pri reakcii na kybernetický bezpečnostný incident a pri zotavovaní sa z neho.

Možnosti európskeho rámca certifikácie kybernetickej bezpečnosti

Možnosť B.1: *Objasnenie rozsahu pôsobnosti, prvkov a cieľov ECCF a zavedenie mechanizmu údržby* – Touto možnosťou sa zabezpečí nový mechanizmus údržby schém po ich prijatí, ktorý by zaviedla agentúra ENISA.

Možnosť B.2: *Reforma ECCF revíziou jeho postupov a rozšírením rozsahu pôsobnosti s cieľom uľahčiť zjednodušenie dodržiavania právnych predpisov – V* rámci tejto možnosti by sa zrušil akt o kybernetickej bezpečnosti a nahradil by sa novým nariadením. Okrem možnosti B.1 by sa zrevidoval postup týkajúci sa žiadostí o schémy, ich vývoja a prijímania s cieľom zlepšiť zodpovednosť a účinnosť.

Možnosť B.3: *Reforma ECCF podľa možnosti B.2 a zavedenie povinnej certifikácie úrovne kybernetickej bezpečnosti* – Táto možnosť by vychádzala z možnosti B.2, ale jej cieľom je ďalej posilniť vplyv rámca zavedením povinnej certifikácie kľúčových subjektov, na ktoré sa vzťahuje smernica NIS 2, s ohľadom na konkrétne rizikové scenáre namiesto toho, aby sa opierala len o dobrovoľnú certifikáciu subjektov.

Možnosti zjednodušenia

Možnosť C.1: *Prijatie prístupu založeného na nezáväzných právnych predpisoch a nelegislatívnych nástrojoch vrátane využitia existujúcich splnomocnení (prijímanie vykonávacích aktov podľa článku 21 ods. 5 a článku 23 ods. 11 smernice NIS 2) – V* tejto možnosti sa predpokladá prijímanie vykonávacích aktov v rámci existujúcich splnomocnení podľa smernice NIS 2 s cieľom zabezpečiť vyšší stupeň harmonizácie opatrení na riadenie rizík kybernetickej bezpečnosti, prahových hodnôt na nahlasovanie incidentov, ako aj informácií, formátov a postupov oznamovania, spolu s prijatím súboru usmernení na posilnenie právnej istoty a harmonizovaného vykonávania.

Možnosť C.2: *Cielená intervencia – ďalšie zjednodušenie dodržiavania príslušného legislatívneho rámca Únie pre kybernetickú bezpečnosť* – Táto možnosť zahŕňa obmedzenú intervenciu zmenami aktu o kybernetickej bezpečnosti a smernice NIS 2 s cieľom zjednodušiť konkrétne aspekty rámca kybernetickej bezpečnosti vrátane úprav rozsahu pôsobnosti, maximálnej harmonizácie vykonávacích aktov, preukazovania súladu prostredníctvom certifikácie a prijatia súboru usmernení, ako sa predpokladá v možnosti C.1.

Možnosť C.3: *Harmonizácia opatrení súvisiacich s kybernetickou bezpečnosťou stanovených v právnych predpisoch Únie* – Táto možnosť by nadväzovala na možnosť C.2 a v jej rámci by sa odstránili všetky opatrenia na riadenie rizík kybernetickej bezpečnosti alebo splnomocnenia v súvislosti s opatreniami zahrnutými v sektorových právnych predpisoch.

Namiesto toho by sa zmenil ekosystém smernice NIS 2, aby sa stanovili zjednodušené požiadavky pre všetky typy subjektov, čím by sa zabezpečila vyššia úroveň harmonizácie.

Možnosti týkajúce sa bezpečnosti dodávateľského reťazca IKT

Možnosť D.1: *Prístup k riešeniu rizík kybernetickej bezpečnosti pre dodávateľské reťazce IKT na základe nezáväzných právnych predpisov* – V tejto možnosti by sa nezabezpečila regulačná intervencia na úrovni EÚ. Komisia by namiesto toho zvýšila počet koordinovaných posúdení rizík a dobrovoľných súborov nástrojov.

Možnosť D.2: *Regulačná intervencia ad hoc kodifikujúca súbor nástrojov pre 5G* – Touto možnosťou by sa kodifikovali opatrenia súboru nástrojov pre 5G. Zaviedla by sa povinnosť členských štátov zabezpečiť, aby sa v kľúčových aktívach siete nepoužívali komponenty od vysokorizikových dodávateľov.

Možnosť D.3: *Komplexný a horizontálny rámec na riešenie rizík kybernetickej bezpečnosti v dodávateľských reťazcoch IKT – V* rámci tejto možnosti by sa vytvoril horizontálny, technologicky a sektorovo neutrálny regulačný rámec na riešenie netechnických kybernetickobezpečnostných rizík v dodávateľských reťazcoch IKT.

Po rozsiahlych analýzach preferovaný balík politík zahŕňa: možnosť A.2 – reformu mandátu agentúry ENISA; možnosť B.2 – reformu ECCF revíziou postupu a rozšírením rozsahu pôsobnosti s cieľom uľahčiť zjednodušenie dodržiavania právnych predpisov a možnosť C.2 – cielenú intervenciu – ďalšie zjednodušenie dodržiavania príslušného právneho rámca Únie v oblasti kybernetickej bezpečnosti a možnosť D.3 – komplexný a horizontálny rámec na riešenie rizík kybernetickej bezpečnosti dodávateľských reťazcov IKT.

Táto kombinácia ponúka vyváženú reakciu na identifikované politické výzvy a výrazne zvyšuje účinnosť, efektívnosť a súdržnosť v celej EÚ.

Hlavné vplyvy

Analýza nákladov a prínosov: Prechodom na navrhovaný regulačný rámec vzniknú agentúre ENISA náklady na plnenie jej nových úloh, ktoré sa odhadujú až na 161,3 milióna EUR za päť rokov, a orgánom verejnej správy v celej EÚ náklady na dozor vo výške až 80 miliónov EUR za päť rokov (pri zohľadnení príslušných úspor nákladov). Pokiaľ ide o podniky, počas trojročného prechodného obdobia by postupné vyraďovanie špecifických vysokorizikových zariadení mohlo viesť k ročným nákladom vo výške 3,4 až 4,3 miliardy EUR pre prevádzkovateľov mobilných sietí, zatiaľ čo investície do dôveryhodných dodávateľov by mohli súčasne vzrásť až na 2 miliardy EUR ročne. Okrem toho sa očakáva, že zjednodušenie a obmedzenie povinností týkajúcich sa dodržiavania predpisov prinesie podnikom úspory nákladov vo výške až 14,6 miliardy EUR. Zo zlepšenia celkovej úrovne kybernetickej bezpečnosti a technologickej suverenity EÚ a zo stimulácie inovácií a konkurencieschopnosti by navyše vyplynuli významné výhody pre občanov, verejné orgány a podniky, ktorými by sa mali z dlhodobého hľadiska do veľkej miery kompenzovať počiatočné výdavky.

Konkurencieschopnosť: Znížením fragmentácie trhu a harmonizáciou predpisov sa uprednostňovanými možnosťami posilňuje rovnosť v hospodárskej súťaži v celej EÚ a podnikom sa poskytujú jasnejšie cesty k dodržiavaniu predpisov a inováciám.

Kontrola súladu s cieľmi v oblasti klímy: Pri posudzovaní sa zvážil potenciálny vplyv každej možnosti na životné prostredie. Osobitná pozornosť sa venovala energetickej efektívnosti, emisiám súvisiacim s cestovaním a konsolidácii infraštruktúry. Uprednostňované možnosti A.2, B.2 a C.2 majú obmedzený vplyv na životné prostredie, zatiaľ čo v možnosti D.3 sa zohľadňuje environmentálna neutralita, pričom sa berie do úvahy životný cyklus produktu a prechodné obdobia na výmenu kľúčových aktív. Je to v súlade so záväzkom EÚ k udržateľnosti.

Digitálne služby ako štandard: Dôraz na zefektívnenie digitálnych procesov je prejavom záväzku EÚ uplatňovať prístup prednostného využívania digitálnych služieb, ktorým sa zabezpečí rýchlejšia a spoľahlivejšia výmena údajov a rozhodovanie. Možnosť D.3 by takisto mohla mať veľký vplyv na digitalizáciu, pretože by si vyžadovala nahradenie komponentov od subjektov usadených v tretích krajinách, ktoré vzbudzujú obavy z hľadiska kybernetickej bezpečnosti, alebo kontrolovaných subjektmi z takýchto tretích krajín.

Zjednodušenie a zníženie záťaže: Uprednostňované možnosti prispievajú k zjednodušeniu zavedením objasnení rozsahu pôsobnosti a opatrení na zefektívnenie dodržiavania predpisov a dozoru, čím sa znižuje administratívna záťaž. Zásada rovnováhy záťaže sa zohľadňuje tým, že sa zabezpečí, aby nové povinnosti boli vyvážené znížením v iných oblastiach.

Záver

Toto posúdenie vplyvu predstavuje komplexnú stratégiu na zlepšenie kybernetickej bezpečnosti EÚ, riešenie regulačných nedostatkov a prípravu digitálneho prostredia na budúce výzvy. Odporúča sa v ňom kooperatívny a súdržný prístup, v rámci ktorého by sa politické reformy opierali o existujúce rámce a zároveň by sa prispôsobili novej technologickej realite. Cieľom EÚ je týmito opatreniami zabezpečiť odolné, konkurencieschopné a udržateľné digitálne hospodárstvo.