Rada
Unii Europejskiej

Bruksela, 22 stycznia 2026 r.
(OR. en)

5611/26
ADD 2

Międzyinstytucjonalne numery referencyjne:
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

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	21 stycznia 2026 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	SWD(2026) 12 final
Dotyczy:	DOKUMENT ROBOCZY SŁUŻB KOMISJI STRESZCZENIE SPRAWOZDANIA Z OCENY SKUTKÓW […] Towarzyszący dokumentom wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), europejskich ram certyfikacji cyberbezpieczeństwa i bezpieczeństwa łańcucha dostaw ICT oraz uchylenia rozporządzenia (UE) 2019/881 (drugi akt o cyberbezpieczeństwie) oraz wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę (UE) 2022/2555 w zakresie środków upraszczających i dostosowania do [wniosku dotyczącego aktu o cyberbezpieczeństwie 2]

Delegacje otrzymują w załączeniu dokument SWD(2026) 12 final.

Zał.: SWD(2026) 12 final

KOMISJA
EUROPEJSKA

Strasburg, dnia 20.1.2026 r.
SWD(2026) 12 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE SPRAWOZDANIA Z OCENY SKUTKÓW

[…]

Towarzyszący dokumentom

wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), europejskich ram certyfikacji cyberbezpieczeństwa i bezpieczeństwa łańcucha dostaw ICT oraz uchylenia rozporządzenia (UE) 2019/881 (drugi akt o cyberbezpieczeństwie)

oraz
wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę (UE) 2022/2555 w zakresie środków upraszczających i dostosowania do [wniosku dotyczącego aktu o cyberbezpieczeństwie 2]

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

Streszczenie oceny skutków

Cel

Głównym celem niniejszej oceny skutków jest ocena adekwatności obecnych przepisów w odniesieniu do zmieniających się zagrożeń cyberbezpieczeństwa w całej UE. Zaproponowano w niej zintegrowany zestaw wariantów strategicznych mających na celu wzmocnienie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), reformę europejskich ram certyfikacji cyberbezpieczeństwa (ECCF) i uproszczenie przestrzegania obowiązujących ram prawnych dotyczących cyberbezpieczeństwa. W niniejszej ocenie podkreślono znaczenie dostosowania cyberzarządzania w celu zharmonizowania go z postępem technologicznym i wymaganiami rynku przy jednoczesnym zapewnieniu konkurencyjności i uwzględnieniu wpływu na środowisko.

Opis problemu

Pomimo dotychczasowych starań cyberbezpieczeństwo w UE nadal stoi przed poważnymi wyzwaniami w kontekście coraz bardziej złożonych zagrożeń. Niewystarczająca koordynacja między państwami członkowskimi i innymi podmiotami na szczeblu unijnym, powolne wdrażanie narzędzi politycznych oraz przeszkody regulacyjne i złożoność utrudniają skuteczne zarządzanie cyberbezpieczeństwem. Powyższe kwestie prowadzą do wzrostu kosztów dla przedsiębiorstw i organów publicznych, zwiększenia ryzyka cyberincydentów oraz niejednolitych poziomów ochrony obywateli.

Uzasadnienie działania UE

Zagrożenia cyberbezpieczeństwa wykraczają poza granice państw, w związku z tym jednolite podejście ma zasadnicze znaczenie dla skutecznego reagowania. Interwencja na szczeblu UE zapewnia spójną ochronę, wzmacnia konkurencyjność poprzez zapewnienie równych warunków działania oraz ułatwia swobodny przepływ usług i produktów cyfrowych na jednolitym rynku. Harmonizacja na szczeblu UE zmniejsza również obciążenia administracyjne dzięki uproszczeniu procedur przestrzegania przepisów i usprawnieniu procedur.

Warianty strategiczne i preferowany wariant

W niniejszej ocenie przeanalizowano cztery obszary interwencji, z których każdy obejmuje zestaw wariantów strategicznych rozważanych w świetle celów szczegółowych, które mają zostać osiągnięte: 1) mandat ENISA (również część obecnego aktu o cyberbezpieczeństwie); 2) europejskie ramy certyfikacji cyberbezpieczeństwa (ECCF) (również część obecnego aktu o cyberbezpieczeństwie); oraz 3) ukierunkowane zmiany dyrektywy NIS 2 służące uproszczeniu, a jednocześnie powiązane z mandatem ENISA i ECCF. Każdy z tych zestawów wariantów jest sam w sobie obszarem interwencji, a jednocześnie jest wzajemnie powiązany i istotny dla innych obszarów.

Warianty odnoszące się do kwestii niedostosowania ram polityki UE w zakresie cyberbezpieczeństwa do potrzeb zainteresowanych stron w coraz bardziej nieprzyjaznym środowisku

Wariant A.1: *Doprecyzowanie mandatu ENISA i ustalenie priorytetów* – wariant ten zapewniłby jasne i stabilne ramy dla zadań ENISA poprzez włączenie zadań określonych w innych aktach prawnych.

Wariant A.2: *Reforma mandatu ENISA* – w wariancie tym nastąpiłoby uchylenie i zastąpienie aktu o cyberbezpieczeństwie, co zapewni aktualizację mandatu Agencji.

Wariant A.3: *Reforma mandatu ENISA z silnym naciskiem na wsparcie operacyjne* – podstawę tego wariantu stanowiłby wariant A.2. ENISA rozwinęłaby ponadto zdolności do bezpośredniego wspierania podmiotów objętych dyrektywą NIS 2 w ramach odpowiedzi na incydent w cyberbezpieczeństwie i usuwania jego skutków na żądanie państwa członkowskiego.

Warianty odnoszące się do europejskich ram certyfikacji cyberbezpieczeństwa

Wariant B.1: *Doprecyzowanie zakresu, elementów i celów ECCF oraz wprowadzenie mechanizmu utrzymania* – w tym wariancie przewidziano nowy mechanizm utrzymania systemów po ich przyjęciu, ma to być zadanie w gestii ENISA.

Wariant B.2: *Reforma ECCF w drodze zmiany procedur i rozszerzenia zakresu w celu wspierania uproszczenia przestrzegania przepisów* – w tym wariancie przewiduje się uchylenie aktu o cyberbezpieczeństwie i zastąpienie go nowym rozporządzeniem. W uzupełnieniu wariantu B.1 dokonano by przeglądu procedur związanych ze składaniem wniosków, opracowywaniem i przyjmowaniem programów w celu poprawy rozliczalności i skuteczności.

Wariant B.3: *Reforma ECCF przewidziana w wariancie B.2 i wprowadzenie obowiązkowej certyfikacji w odniesieniu do stanu cyberbezpieczeństwa* – wariant ten opiera się na wariancie B.2, ale ma na celu dodatkowe wzmocnienie wpływu ram poprzez wprowadzenie obowiązkowej certyfikacji podmiotów kluczowych objętych dyrektywą NIS 2, z uwzględnieniem konkretnych scenariuszy ryzyka, zamiast polegania wyłącznie na dobrowolnej certyfikacji podmiotów.

Warianty dotyczące uproszczenia

Wariant C.1: *Przyjęcie podejścia opartego na prawie miękkim i instrumentach o charakterze nieustawodawczym, w tym wykorzystanie istniejących uprawnień (przyjęcie aktów wykonawczych na podstawie art. 21 ust. 5 i art. 23 ust. 11 dyrektywy NIS 2)* – wariant ten przewiduje przyjęcie aktów wykonawczych na podstawie istniejących uprawnień na mocy dyrektywy NIS 2 w celu zapewnienia wyższego stopnia harmonizacji środków zarządzania ryzykiem w cyberprzestrzeni, progów zgłaszania incydentów, a także informacji, formatów i procedur notyfikowania wraz z przyjęciem zestawu wytycznych zmierzających do zwiększenia pewności prawa i zharmonizowanego wdrożenia.

Wariant C.2: *Ukierunkowana interwencja – dalsze uproszczenie w zakresie zgodności z odpowiednimi unijnymi ramami prawnymi dotyczącymi cyberbezpieczeństwa* – wariant ten obejmuje ograniczoną interwencję poprzez zmiany w akcie o cyberbezpieczeństwie i dyrektywie NIS 2 w celu uproszczenia konkretnych aspektów ram cyberbezpieczeństwa, w tym dostosowania zakresu, maksymalnej harmonizacji aktów wykonawczych, dowodu zgodności w drodze certyfikacji oraz przyjęcia zestawu wytycznych przewidzianych w wariancie C1.

Wariant C.3: *Harmonizacja środków związanych z cyberbezpieczeństwem określonych w przepisach Unii* – wariant ten opierałby się na wariancie C.2 i przyczyniłby się do usunięcia w przepisach sektorowych wszystkich środków zarządzania ryzykiem w cyberprzestrzeni oraz uprawnień w odniesieniu do takich środków. Zamiast tego ekosystem objęty dyrektywą NIS 2 zostałby zmieniony, aby zapewnić uproszczone wymogi dla wszystkich rodzajów podmiotów, gwarantując w ten sposób wyższy stopień harmonizacji.

Warianty dotyczące bezpieczeństwa łańcucha dostaw ICT

Wariant D.1: *Przyjęcie podejścia opartego na prawie miękkim w celu przeciwdziałania ryzyku w cyberprzestrzeni związanemu z łańcuchami dostaw ICT* – wariant ten nie przewidywałby interwencji regulacyjnej na szczeblu UE. Zamiast tego Komisja zwiększyłaby liczbę skoordynowanych ocen ryzyka oraz dobrowolnych zestawów narzędzi.

Wariant D.2: *Interwencja regulacyjna ad hoc kodyfikująca unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G* – wariant ten kodyfikowałby środki w ramach unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G. Na państwa członkowskie nałożono by obowiązek zagwarantowania, że komponenty pochodzące od dostawców wysokiego ryzyka nie będą wykorzystywane w kluczowych zasobach sieci.

Wariant D.3: *Kompleksowe i horyzontalne ramy przeciwdziałania ryzyku w cyberprzestrzeni związanemu z łańcuchami dostaw ICT* – W ramach tego wariantu ustanowiono by horyzontalne, neutralne pod względem technologicznym i sektorowym ramy regulacyjne mające na celu przeciwdziałanie pozatechnicznemu ryzyku w cyberprzestrzeni związanemu z łańcuchami dostaw ICT.

Po przeprowadzeniu szeroko zakrojonych analiz preferowany pakiet strategiczny obejmuje: wariant A.2 – reforma mandatu ENISA; wariant B.2 – reforma ECCF w drodze zmiany procedur i rozszerzenia zakresu w celu wspierania uproszczenia przestrzegania przepisów, wariant C.2 – ukierunkowana interwencja – dalsze uproszczenie zgodności z odpowiednimi unijnymi ramami prawnymi dotyczącymi cyberbezpieczeństwa, oraz wariant D.3 – kompleksowe i horyzontalne ramy przeciwdziałania ryzyku w cyberprzestrzeni związanemu z łańcuchami dostaw ICT.

Taki zestaw zapewnia wyważoną reakcję na zidentyfikowane wyzwania w zakresie polityki, znacznie zwiększając skuteczność, efektywność i spójność w całej UE.

Główne skutki

Analiza kosztów i korzyści: Przejście na proponowane ramy regulacyjne pociągnie za sobą koszty zarówno dla ENISA (szacowane na maksymalnie 161,3 mln EUR w ciągu pięciu lat na realizację nowych zadań), jak i dla organów publicznych w całej UE w wysokości do 80 mln EUR w ciągu pięciu lat na nadzór (z uwzględnieniem odpowiednich oszczędności kosztów). Jeżeli chodzi o przedsiębiorstwa, w okresie przejściowym trwającym trzy lata stopniowe wycofywanie określonych urządzeń wysokiego ryzyka mogłoby generować roczne koszty w wysokości 3,4–4,3 mld EUR dla operatorów sieci ruchomych, natomiast inwestycje w zaufanych dostawców mogłyby jednocześnie wzrosnąć do 2 mld EUR rocznie. Ponadto oczekuje się, że uproszczone i ograniczone obowiązki w zakresie przestrzegania przepisów przyczynią się do oszczędności kosztów dla przedsiębiorstw w wysokości do 14,6 mld EUR. Ponadto znaczne korzyści dla obywateli, organów publicznych i przedsiębiorstw wynikałyby z poprawy ogólnego stanu cyberbezpieczeństwa i suwerenności technologicznej w UE oraz ze stymulowania innowacji i konkurencyjności, przy czym oczekuje się, że w perspektywie długoterminowej w dużej mierze zrównoważą one początkowe wydatki.

Konkurencyjność: Dzięki zmniejszeniu fragmentacji rynku i harmonizacji przepisów preferowane warianty stwarzają bardziej równe warunki konkurencji w całej UE, zapewniając przedsiębiorstwom jaśniejsze ścieżki zagwarantowania zgodności z przepisami i innowacji.

Ocena spójności z celem neutralności klimatycznej: W ocenie uwzględniono potencjalny wpływ każdego wariantu na środowisko. Szczególną uwagę zwrócono na efektywność energetyczną, emisje związane z podróżami i konsolidację infrastruktury. Preferowane warianty A.2, B.2 i C.2 mają ograniczony wpływ na środowisko, natomiast wariant D.3 uwzględnia neutralność środowiskową, biorąc pod uwagę cykl życia produktu i okresy przejściowe na wymianę kluczowych aktywów. Jest to zgodne ze zobowiązaniem UE do zrównoważonego rozwoju.

Domyślna cyfrowość: Nacisk na usprawnione procesy cyfrowe świadczy o zaangażowaniu UE na rzecz podejścia „kontakt w pierwszej kolejności cyfrowy”, zapewniającego szybsze i bardziej wiarygodne procesy wymiany danych i podejmowania decyzji. Wariant D.3 mógłby również mieć duży wpływ na cyfryzację, ponieważ wiązałby się z wymianą komponentów pochodzących od podmiotów mających siedzibę w państwach trzecich stwarzających obawy dotyczące cyberbezpieczeństwa lub kontrolowanych przez podmioty z takich państw.

Uproszczenie i zmniejszenie obciążeń: Preferowane warianty przyczyniają się do uproszczenia poprzez doprecyzowanie zakresu i wprowadzenie środków mających na celu usprawnienie przestrzegania przepisów i nadzoru oraz zmniejszenie obciążeń administracyjnych. Zasada „jedno więcej – jedno mniej” jest uwzględniana dzięki zapewnieniu kompensowania nowych obowiązków redukcją obowiązków w innych obszarach.

Wnioski

W niniejszej ocenie skutków przedstawiono kompleksową strategię mającą na celu zwiększenie cyberbezpieczeństwa UE, rozwiązanie problemu niewydolności regulacyjnej i przygotowanie otoczenia cyfrowego na przyszłe wyzwania. Zaleca się w nim podejście

oparte na współpracy i spójności, osadzające reformy polityczne w istniejących ramach, przy jednoczesnym dostosowaniu się do nowych realiów technologicznych. Za pomocą tych środków UE dąży do zapewnienia odpornej, konkurencyjnej i zrównoważonej gospodarki cyfrowej.