Rada
Unii Europejskiej

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

9399/26

LIMITE

CYBER 229
JAI 606
DATAPROTECT 161
TELECOM 239
MI 489
IND 342
CADREFIN 220
FIN 697
BUDGET 19
CSC 316
CODEC 937

Międzyinstytucjonalne numery referencyjne:
2026/0011 (COD)
2026/0012 (COD)

NOTA

Od:	Sekretariat Generalny Rady
Do:	Komitet Stałych Przedstawicieli / Rada
Dotyczy:	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) Wniosek w sprawie dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę (UE) 2022/2555 w zakresie środków upraszczających i dostosowania do [wniosku dotyczącego aktu o cyberbezpieczeństwie 2] – Sprawozdanie z postępu prac

Prezydencja sporządziła sprawozdanie z postępu prac nad wnioskiem dotyczącym 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) 2019/991 (drugi akt o cyberbezpieczeństwie), aby podsumować dotychczasowe prace organów przygotowawczych Rady oraz postępy w analizie wniosku.

WPROWADZENIE

1. 20 stycznia 2026 r. Komisja zaproponowała nowy pakiet dotyczący cyberbezpieczeństwa, aby wzmocnić odporność i zdolności UE w tej dziedzinie. W skład pakietu wchodzi **rozporządzenie** w sprawie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), europejskich ram certyfikacji cyberbezpieczeństwa i bezpieczeństwa łańcucha dostaw technologii informacyjno-komunikacyjnych (ICT) oraz uchylenia rozporządzenia (UE) 2019/881 (aktu o cyberbezpieczeństwie). Uzupełnieniem tego rozporządzenia (drugiego aktu o cyberbezpieczeństwie) jest **dyrektywa** zmieniająca dyrektywę (UE) 2022/2555 (dyrektywę NIS 2) w zakresie środków upraszczających i dostosowania do [wniosku dotyczącego aktu o cyberbezpieczeństwie].

2. Zanim wniosek został przedstawiony Rada w swoich konkluzjach w sprawie ENISA z 6 grudnia 2024r.[1] zwróciła się do Komisji o przeanalizowanie i dalsze wzmocnienie roli ENISA we wspieraniu współpracy operacyjnej na szczeblu UE i między państwami członkowskimi w zakresie zwiększania cyberodporności, z uwzględnieniem kompetencji państw członkowskich w tej dziedzinie. Komisję wezwano także do zapewnienia, aby mandat ENISA w zakresie wspierania państw członkowskich był ukierunkowany i jasno określony, z wyszczególnieniem konkretnych celów strategicznych i priorytetowych zadań, obok bardziej precyzyjnego podziału zadań i kompetencji w odniesieniu do innych podmiotów. Rada wezwała także w trybie pilnym Komisję do wykorzystania możliwości, jaką stwarza ocena aktu o cyberbezpieczeństwie, aby znaleźć sposoby na przyjęcie prostszego, opartego na analizie ryzyka, a także bardziej przejrzystego i szybszego podejścia do opracowywania unijnych systemów certyfikacji cyberbezpieczeństwa. Ponadto w swoich konkluzjach z 21 maja 2024 r. w sprawie przyszłości cyberbezpieczeństwa[2] Rada podkreśliła swoje zaangażowanie na rzecz zapewnienia bezpiecznych łańcuchów dostaw ICT i zwróciła uwagę na znaczenie pozatechnicznych czynników ryzyka, w tym nadmiernego wpływu państw trzecich na dostawców i usługodawców. W konkluzjach Rady[3] z dnia 17 października 2022 r. w sprawie bezpieczeństwa łańcucha dostaw ICT podkreślono też potrzebę wzmocnienia odporności i bezpieczeństwa łańcuchów dostaw ICT, biorąc pod uwagę wpływ napięć geopolitycznych i zależności od produktów i usług ICT.

---

1 Dok. 16527/24.
2 Dok. 10133/24.
3 Dok. 13664/22.

3. Celem wniosku dotyczącego rozporządzenia, którego podstawą jest art. 114 TFUE, jest wzmocnienie unijnych ram cyberbezpieczeństwa. Wzmacnia on rolę i zadania Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) w zakresie wspierania państw członkowskich i podmiotów unijnych w osiąganiu w Unii wysokiego poziomu cyberbezpieczeństwa, odporności i zaufania. We wniosku dąży się do zwiększenia skuteczności i efektywności europejskich ram certyfikacji cyberbezpieczeństwa, aby umożliwić szybsze opracowywanie i wdrażanie systemów. Ustanawia się również unijne ramy dotyczące bezpieczeństwa zaufanego łańcucha dostaw ICT, uwzględniające pozatechniczne czynniki ryzyka i zależności mające wpływ na bezpieczeństwo krytycznej infrastruktury i krytycznych usług ICT. Wnioskowi towarzyszą ukierunkowane środki upraszczające związane z wdrażaniem dyrektywy NIS 2[4], mające na celu uproszczenie wymogów dotyczących zgodności, zmniejszenie zbędnych obciążeń administracyjnych i zwiększenie jasności prawa.

4. W planie działania „Jedna Europa, jeden rynek”[5] podpisanym przy okazji nieformalnego posiedzenia szefów państw lub rządów, które odbyło się na Cyprze 24 kwietnia 2026 r., niniejszy wniosek wskazano jako jeden z priorytetowych rezultatów.

5. W Parlamencie Europejskim na sprawozdawczynię została wyznaczona Gregorová Markéta (Verts/ALE) z przedmiotowo właściwej komisji ITRE.

6. 29 kwietnia 2026 r. Europejski Komitet Ekonomiczno-Społeczny wydał opinię w sprawie przedmiotowego wniosku[6].

---

4 Dz.U. L 333 z 27.12.2022, s. 80.
5 Dok. 8473/26.
6 Dok. 8980/26.

STAN PRAC W ORGANACH PRZYGOTOWAWCZYCH RADY

7. Pakiet dotyczący cyberbezpieczeństwa przedstawiono ogólnie na posiedzeniu Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni (HWPCI) 26 stycznia 2026 r. oraz na posiedzeniu Komitetu Stałych Przedstawicieli 28 stycznia 2026 r.

8. Omawianie wniosku na forum HWPCI rozpoczęło się 2 lutego 2026 r. od szczegółowej prezentacji przez Komisję. Podczas tej prezentacji Komisja przedstawiła również ustalenia zawarte w sprawozdaniu z oceny, ocenie skutków finansowych i ocenie skutków.

9. HWPCI rozpoczęła czytanie proponowanego rozporządzenia 23 lutego 2026 r.

10. Państwa członkowskie z zadowoleniem przyjęły wniosek i zasadniczo poparły jego ogólne cele, w szczególności zwiększenie wsparcia ENISA dla współpracy operacyjnej państw członkowskich i usprawnienie ram certyfikacji. Dyskusje pokazały jednak również, że kilka aspektów wniosku wymagałoby dalszej analizy. Delegacje zwróciły się o dalsze wyjaśnienia dotyczące zwiększonej roli operacyjnej i zadań przewidzianych dla ENISA, takich jak wczesne ostrzeganie, utworzenie punktu informacyjnego ds. oprogramowania szantażującego oraz rola ENISA w sieci CSIRT. Kilka delegacji zakwestionowało wpływ na zasoby państw członkowskich związany z proponowanym oddelegowaniem dwóch ekspertów krajowych z każdego państwa członkowskiego w celu wsparcia zadań ENISA. Dalszych dyskusji wymagają także zasady głosowania zarządu. Delegacje podkreśliły potrzebę wyjaśnienia i doprecyzowania definicji i pojęć stosowanych w całym wniosku. Dalszych wyjaśnień wymaga również struktura budżetu ENISA, w szczególności pobieranie opłat.

11. Z zadowoleniem zostały przyjęte nowe przepisy mające na celu zwiększenie skuteczności i wydajności procesu certyfikacji, chociaż stwierdzono ogólną potrzebę zwiększenia udziału państw członkowskich w całym procesie certyfikacji. Ogólnie pozytywnie odebrany został dobrowolny charakter certyfikacji. Delegacje zakwestionowały jednak niektóre terminy proponowane w odniesieniu do ram certyfikacji.

12. Dyskusje na temat ram dotyczących zaufanego łańcucha dostaw ICT uwypukliły szereg obaw wśród państw członkowskich. Delegacje zaapelowały o dalsze wyjaśnienia dotyczące metodyki i procedur identyfikacji kluczowych zasobów ICT i dostawców wysokiego ryzyka, a także zakresu i możliwych skutków proponowanych środków. Delegacje podkreśliły znaczenie zapewnienia odpowiedniego poziomu zaangażowania państw członkowskich.

13. Kilka delegacji zgłosiło zastrzeżenia weryfikacji do różnych części wniosku, w szczególności w odniesieniu do aspektów zarządzania, stosowania aktów wykonawczych i proponowanego mechanizmu identyfikacji dostawców wysokiego ryzyka, a także do bezpieczeństwa łańcucha dostaw ICT.

14. W następstwie dyskusji na forum HWPCI państwa członkowskie zostały poproszone o przedstawienie pisemnych uwag na temat przepisów związanych z tytułem I (Przepisy ogólne) i tytułem II (ENISA). Uwagi przekazały 23 państwa członkowskie. Następnie państwa członkowskie zostały również poproszone o przedstawienie pisemnych uwag na temat tytułu III (europejskie ramy certyfikacji cyberbezpieczeństwa). Z możliwości przedstawienia swojego stanowiska na piśmie skorzystało 20 państw członkowskich.

15. Na podstawie tych pisemnych uwag państw członkowskich i prac w ramach HWPCI prezydencja sporządzi kompromisowy tekst tytułów II (ENISA) i III (europejskie ramy certyfikacji cyberbezpieczeństwa), który zostanie przedstawiony na posiedzeniu HWPCI na początku czerwca 2026 r.

16. Kilka państw członkowskich zwróciło się do Służby Prawnej Rady o przeanalizowanie adekwatności podstawy prawnej.

17. Pod koniec maja 2026 r. prezydencja rozpocznie czytanie w odniesieniu do środków upraszczających przewidzianych w dyrektywie NIS 2.

18. W sumie podczas prezydencji cypryjskiej HWPCI przeprowadzi łącznie 15 posiedzeń na temat wniosku dotyczącego drugiego aktu o cyberbezpieczeństwie.

19. Bazując na postępach poczynionych przez prezydencję cypryjską, nadchodząca prezydencja irlandzka planuje kontynuować prace nad tym ważnym dossier.

20. W związku z powyższym Komitet Stałych Przedstawicieli i Rada są proszone o odnotowanie postępów w analizie wniosku dotyczącego rozporządzenia.