Rada
Unii Europejskiej

Bruksela, 18 listopada 2022 r.
(OR. en)

14477/22

Międzyinstytucjonalny numer referencyjny:
2022/0272(COD)

LIMITE

CYBER 353
JAI 1430
DATAPROTECT 303
MI 799
CSC 505
CSCI 163
CODEC 1686
IA 179

NOTA

Od:	Sekretariat Generalny Rady
Do:	Komitet Stałych Przedstawicieli / Rada
Nr poprz. dok.:	14680/22, 12429/22 + ADD 1-6
Dotyczy:	Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów w cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/102 – Sprawozdanie z postępu prac

Prezydencja przygotowała sprawozdanie z postępu prac nad wnioskiem dotyczącym rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020, aby poinformować o stanie prac przeprowadzonych dotychczas przez organy przygotowawcze Rady oraz o stanie prac nad analizą wniosku.

Sprawozdanie to zostało przedstawione przez prezydencję Horyzontalnej Grupie Roboczej ds. Cyberprzestrzeni na posiedzeniu w dniu 18 listopada 2022 r.

WPROWADZENIE

1. W dniu 15 września 2022 r. Komisja przyjęła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020. Koncepcja wymogów w zakresie cyberbezpieczeństwa została wspomniana po raz pierwszy przez przewodniczącą Ursulę von der Leyen w orędziu o stanie Unii we wrześniu 2021 r., a następnie odzwierciedlona w konkluzjach Rady z dnia 23 maja 2022 r. w sprawie rozwijania pozycji Unii Europejskiej w kwestiach cyberprzestrzeni, w których wezwano Komisję do zaproponowania do końca 2022 r. wspólnych wymogów w zakresie cyberbezpieczeństwa dla urządzeń podłączonych do internetu. Przed orędziem o stanie Unii, w konkluzjach Rady w sprawie cyberbezpieczeństwa urządzeń podłączonych do internetu z dnia 2 grudnia 2020 r. podkreślono, że z myślą o uwzględnieniu wszystkich istotnych aspektów cyberbezpieczeństwa urządzeń podłączonych do internetu, takich jak dostępność, integralność i poufność, ważne jest, by ocenić potrzebę wprowadzenia horyzontalnego prawodawstwa w perspektywie długoterminowej, określając także warunki niezbędne do wprowadzenia do obrotu.

2. Celem omawianego wniosku, który opiera się na art. 114 TFUE, jest harmonizacja zasadniczych wymogów w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi we wszystkich państwach członkowskich oraz uniknięcie nakładania się wymogów wynikających z różnych aktów prawnych. Wniosek ma wypełnić luki w obowiązujących przepisach dotyczących cyberbezpieczeństwa poprzez zapewnienie, aby produkty zawierające elementy cyfrowe, na przykład produkty będące elementem internetu rzeczy, takie jak podłączone do sieci domowe kamery bezpieczeństwa, chłodziarki, telewizory, zabawki i oprogramowanie niewbudowane, stały się bezpieczne w całym łańcuchu dostaw i przez cały cykl ich życia. Wyjaśnia również powiązania z obowiązującym prawodawstwem i przyczynia się do zwiększenia jego spójności. Ponadto wniosek umożliwia również użytkownikom uwzględnianie cyberbezpieczeństwa przy wyborze produktów z elementami cyfrowymi i korzystaniu z nich.

3. W szczególności omawiany wniosek określa:

- przepisy dotyczące wprowadzania do obrotu produktów z elementami cyfrowymi w celu zapewnienia cyberbezpieczeństwa takich produktów;
- zasadnicze wymogi dotyczące projektowania, opracowywania i produkcji produktów z elementami cyfrowymi oraz obowiązki podmiotów gospodarczych w odniesieniu do tych produktów w zakresie cyberbezpieczeństwa;
- zasadnicze wymogi dotyczące procedur postępowania w przypadku wykrycia podatności wprowadzonych przez producentów w celu zapewnienia cyberbezpieczeństwa produktów z elementami cyfrowymi w całym cyklu życia oraz obowiązki podmiotów gospodarczych w odniesieniu do tych procedur; oraz
- przepisy dotyczące nadzoru rynku i egzekwowania wyżej wymienionych przepisów i wymogów.

STAN PRAC W ORGANACH PRZYGOTOWAWCZYCH RADY

4. Horyzontalna Grupa Robocza ds. Cyberprzestrzeni (HWPCI) rozpoczęła dyskusje nad wnioskiem na posiedzeniu w dniu 21 września 2022 r., kiedy to Komisja dokonała jego ogólnej prezentacji. Po tej ogólnej prezentacji HWPCI omówiła ocenę skutków na posiedzeniu w dniu 28 września 2022 r. Kilka państw członkowskich zgłosiło zastrzeżenia weryfikacji, chcąc dalej analizować ocenę skutków.

5. HWPCI przeanalizowała pełny tekst proponowanego rozporządzenia na posiedzeniach w dniach 5, 12, 19 i 26 października 2022 r. Dzięki tej analizie państwa członkowskie mogły zwrócić się do Komisji o szczegółowe wyjaśnienia dotyczące wszystkich artykułów i załączników do proponowanego rozporządzenia i uzyskać te wyjaśnienia.

6. Ponadto na posiedzeniu HWPCI w dniu 9 listopada 2022 r. Komisja przedstawiła szczegółowe wyjaśnienie przepisów dotyczących odpowiedzialności za produkt w Unii, ze szczególnym uwzględnieniem niedawno opublikowanego wniosku dotyczącego dyrektywy w sprawie odpowiedzialności za produkty wadliwe oraz interakcji między proponowanym rozporządzeniem a unijnymi przepisami dotyczącymi odpowiedzialności za produkt.

7. Na wniosek prezydencji i w związku z zainteresowaniem państw członkowskich Komisja zorganizowała w dniu 13 października 2022 r. warsztaty online na temat nowych ram prawnych w celu wyjaśnienia struktury i podstawowych elementów nowych ram prawnych unijnych przepisów dotyczących produktów, które to ramy stanowią podstawę proponowanego rozporządzenia. Ponadto Komisja przedstawiła szczegółowe informacje na temat odstępstw od nowych ram prawnych w odniesieniu do proponowanego rozporządzenia.

8. W dniu 17 października 2022 r. Rada przyjęła konkluzje w sprawie bezpieczeństwa łańcucha dostaw ICT. Wyraziła w nich zadowolenie z zaproponowanego wniosku w sprawie aktu dotyczącego cyberodporności, gdyż jest to ważny instrument ustawodawczy służący przyspieszeniu bezpiecznego rozwoju produktów z elementami cyfrowymi oraz zapewnieniu uwzględniania cyberbezpieczeństwa w całym cyklu życia takich produktów. Ponadto Rada zauważyła, że proponowane rozporządzenie może znacząco przyczynić się do wzmocnienia bezpieczeństwa łańcucha dostaw ICT, oraz zachęciła do konstruktywnych negocjacji i terminowego przyjęcia proponowanego rozporządzenia.

9. W dniu 9 listopada 2022 r. Europejski Inspektor Ochrony Danych (EIOD) wydał opinię na temat wniosku[1].

10. Na posiedzeniach HWPCI poświęconych analizie proponowanego rozporządzenia państwa członkowskie zasadniczo z zadowoleniem przyjęły to rozporządzenie jako właściwe i ogólnie poparły jego podstawowe cele. Kilka państw członkowskich podkreśliło, że horyzontalny charakter jest ważnym aspektem proponowanego rozporządzenia.

[1] Opinia EIOD nr 8/2022.

11. W trakcie dyskusji państwa członkowskie zwróciły się o dalsze wyjaśnienia dotyczące zakresu stosowania wniosku. W szczególności chodzi im o to, w jakim zakresie wniosek ma objąć oprogramowanie jako usługę, oraz na ile szerokie jest wyłączenie produktów opracowanych wyłącznie do celów bezpieczeństwa narodowego i celów wojskowych z zakresu stosowania wniosku. Ponadto państwa członkowskie wskazały, że ustalenie zakresu produktów o znaczeniu krytycznym będzie wymagało szczegółowej dyskusji. Państwa członkowskie podkreśliły również potrzebę jasności co do interakcji z innymi odpowiednimi przepisami, takimi jak dyrektywa NIS 2 lub akt o cyberbezpieczeństwie. Niektóre państwa członkowskie podkreśliły też potrzebę doprecyzowania niektórych terminów użytych w proponowanym rozporządzeniu.

12. Ponadto państwa członkowskie wezwały także do przeprowadzenia dokładnej oceny obciążenia wynikającego z obowiązków, które mają być nakładane na mocy proponowanego rozporządzenia na małe i średnie przedsiębiorstwa oraz przedsiębiorstwa typu start-up opracowujące i wytwarzające produkty z elementami cyfrowymi objęte proponowanym rozporządzeniem. Niektóre państwa członkowskie życzyłyby sobie, żeby dokładnie zbadać, czy proponowane ograniczenie zgodności jest zgodne z zasadniczymi wymogami co do oczekiwanego cyklu życia produktu lub pięciu lat po wprowadzeniu produktu na rynek wewnętrzny, w zależności od tego, który z tych terminów jest krótszy.

13. Ponadto z wymiany poglądów przeprowadzonej podczas posiedzeń poświęconych analizie wynika, że rola i zadania przewidziane dla ENISA powinny być przedmiotem dalszych dyskusji.

14. W następstwie dyskusji na forum HWPCI prezydencja zwróciła się do państw członkowskich o przedstawienie pisemnych uwag na temat zakresu stosowania proponowanego rozporządzenia i klauzuli dotyczącej swobodnego przepływu, w tym art. 2 i 4, a częściowo art. 3. Zarówno obecna prezydencja czeska, jak i nadchodząca prezydencja szwedzka uważają, że rozwiązanie kwestii zakresu stosowania i klauzuli swobodnego przepływu na pierwszych sesjach negocjacyjnych na forum HWPCI zapewni jasność co do stosowania proponowanego rozporządzenia i dobrą podstawę do dalszych negocjacji.

15. W oparciu o pisemne uwagi państw członkowskich i prace w ramach HWPCI prezydencja zamierza opracować kompromisowy tekst dotyczący zakresu stosowania i klauzuli swobodnego przepływu.

16. W sumie podczas prezydencji czeskiej HWPCI przeprowadzi łącznie 10 posiedzeń na temat wniosku dotyczącego aktu w sprawie cyberodporności.

17. Bazując na postępach poczynionych przez prezydencję czeską, nadchodząca prezydencja szwedzka planuje kontynuować prace nad tym ważnym dossier.

18. W związku z tym Komitet Stałych Przedstawicieli i Rada są proszone o odnotowanie postępów w analizie proponowanego rozporządzenia.