Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020”

(COM(2022) 454 final – 2022/0272 (COD))

(2023/C 100/15)

Sprawozdawca: **Maurizio MENSI**

Współsprawozdawca: **Marinel Dănuț MUREȘAN**

Wniosek o wydanie opinii	Parlament Europejski, 9.11.2022
	Rada Unii Europejskiej, 28.10.2022
Podstawa prawna	art. 114 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Jednolity Rynek, Produkcja i Konsumpcja
Data przyjęcia przez sekcję	10.11.2022
Data przyjęcia na sesji plenarnej	14.12.2022
Sesja plenarna nr	574
Wynik głosowania	
(za/przeciw/wstrzymało się)	177/0/0

1. **Wnioski i zalecenia**

1.1. EKES z zadowoleniem przyjmuje wniosek Komisji w sprawie aktu dotyczącego cyberodporności (ang. „Cyber Resilience Act” – CRA), którego celem jest ustanowienie wyższych norm cyberbezpieczeństwa i tym samym stworzenie niezawodnego systemu dla podmiotów gospodarczych oraz zapewnienie obywatelkom i obywatelom UE bezpiecznego korzystania z produktów znajdujących się na rynku. Inicjatywa ta jest w rzeczywistości częścią europejskiej strategii w zakresie danych, która zwiększa bezpieczeństwo danych, również osobowych, oraz prawa podstawowe, co jest niezbędnym wymogiem w społeczeństwie cyfrowym.

1.2. EKES uważa, że zasadnicze znaczenie ma poprawienie zbiorowego reagowania na cyberataki oraz wzmocnienie procesu harmonizacji przepisów i narzędzi operacyjnych dotyczących cyberbezpieczeństwa na szczeblu krajowym, aby nie dopuścić do sytuacji, w której różne podejścia krajowe mogłyby powodować niepewność i przeszkody prawne.

1.3. EKES z zadowoleniem przyjmuje inicjatywę Komisji, która może nie tylko przyczynić się do obniżenia ponoszonych przez przedsiębiorstwa sporych kosztów cyberataków, lecz umożliwi również obywatelom/konsumentom korzystanie z lepszej ochrony takich praw podstawowych jak prywatność. Komisja pokazuje w szczególności, że przy świadczeniu usług przez podmioty certyfikujące uwzględnia się szczególne potrzeby MŚP; niemniej EKES zwraca uwagę na potrzebę doprecyzowania kryteriów zastosowania aktu dotyczącego cyberodporności.

1.4. EKES pragnie podkreślić, że choć godne uznania jest to, że akt dotyczący cyberodporności odnosi się właściwie do wszystkich produktów cyfrowych, to jego praktyczne wdrażanie może przysporzyć problemów, zważywszy na ścisłą i skomplikowaną weryfikację i kontrolę, których on wymaga. W związku z tym konieczne jest wzmocnienie narzędzi monitorowania i weryfikacji.

1.5. EKES zwraca uwagę na potrzebę dokładnego określenia zakresu przedmiotowego aktu dotyczącego cyberodporności ze szczególnym uwzględnieniem oprogramowania oraz produktów zawierających elementy cyfrowe.

1.6. EKES zaznacza, że producenci będą zobowiązani do zgłaszania Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) – z jednej strony – podatności produktów, a z drugiej – ewentualnych incydentów). W związku z tym ważne jest, aby zapewnić jej zasoby niezbędne do terminowego i skutecznego wykonywania powierzonych jej istotnych i trudnych zadań.

1.7. Aby można było uniknąć jakichkolwiek wątpliwości interpretacyjnych, EKES proponuje, by Komisja opracowała odpowiednie wytyczne dla producentów i konsumentów dotyczące obowiązujących w praktyce zasad i procedur, gdyż różnorakie produkty wchodzące w zakres stosowania wniosku podlegają również innym przepisom w dziedzinie cyberbezpieczeństwa. Dlatego też istotne byłoby również, aby zwłaszcza MŚP i MMŚP miały dostęp do wykwalifikowanego wsparcia ekspertów, którzy byliby w stanie świadczyć konkretne profesjonalne usługi.

1.8. EKES zaznacza, że związek między podmiotami certyfikującymi w rozumieniu aktu dotyczącego cyberodporności a innymi organami uprawnionymi do certyfikacji cyberbezpieczeństwa na mocy innych przepisów nie jest całkowicie jasny. Ten sam problem z koordynacją operacyjną może wystąpić również między organami nadzorczymi przewidzianymi w omawianym wniosku a organami już działającymi na mocy innych przepisów mających zastosowanie do tych samych produktów.

1.9. EKES podkreśla, że wniosek przewiduje powierzenie ogromu zadań i odpowiedzialności podmiotom certyfikującym, których praktyczną operacyjność należy zagwarantować. Nie można również dopuścić do tego, by akt dotyczący cyberodporności prowadził do zwiększenia obciążeń biurokratycznych, co postawi w gorszej sytuacji producentów zobowiązanych spełnić szereg dodatkowych wymogów certyfikacyjnych w celu dalszego prowadzenia działalności na rynku.

2. **Analiza wniosku**

2.1. Za pomocą wniosku w sprawie aktu dotyczącego cyberodporności Komisja zamierza zracjonalizować i ponownie określić w harmonijny i horyzontalny sposób obecne przepisy w zakresie cyberbezpieczeństwa, zapewniając jednocześnie ich aktualizację w świetle innowacji technologicznych.

2.2. Akt dotyczący cyberodporności ma zasadniczo cztery cele: zagwarantowanie, że na etapie projektowania i rozwoju oraz w całym cyklu życia producenci zwiększą bezpieczeństwo produktów zawierających elementy cyfrowe; zadbanie o spójne ramy prawne dotyczące cyberbezpieczeństwa, ułatwiające producentom sprzętu i oprogramowania przestrzeganie przepisów; zwiększenie przejrzystości zabezpieczeń produktów zawierających elementy cyfrowe; umożliwienie przedsiębiorstwom i konsumentom bezpiecznego korzystania z tych produktów. We wniosku wprowadza się zasadniczo oznakowanie CE w dziedzinie cyberbezpieczeństwa, nakładając wymóg zamieszczania go na wszystkich produktach, które reguluje akt dotyczący cyberodporności.

2.3. Jest to działanie horyzontalne, za pomocą którego Komisja zamierza uregulować całą dziedzinę w sposób kompleksowy, zważywszy że dotyczy ono praktycznie wszystkich produktów zawierających elementy cyfrowe. Są z niego wykluczone wyłącznie produkty o charakterze medycznym, związane z lotnictwem cywilnym i wojskowością oraz pojazdy. Wniosek nie obejmuje również oprogramowania SaaS (usług w chmurze) z wyjątkiem przypadku, gdy służy ono do opracowania produktów zawierających elementy cyfrowe.

2.4. Definicja „produktów zawierających elementy cyfrowe" jest bardzo szeroka i obejmuje wszelkie produkty w postaci oprogramowania lub sprzętu komputerowego, w tym także oprogramowanie lub sprzęt niewbudowane do produktu, lecz wprowadzane do obrotu oddzielnie.

2.5. W przepisach wprowadza się obowiązkowe wymogi odnośnie do cyberbezpieczeństwa w całym cyklu życia produktów zawierających elementy cyfrowe, lecz te przepisy nie zastępują tych już obowiązujących. Wręcz przeciwnie – produkty, które uzyskały już certyfikat zgodności z wcześniej istniejącymi normami UE, będą uznawane za prawidłowe również na mocy nowego rozporządzenia.

2.6. Zgodnie z ogólną i podstawową zasadą – w Europie wprowadza się do obrotu wyłącznie bezpieczne produkty, których producenci dbają o to, by pozostawały one bezpieczne przez cały cykl życia.

2.7. Produkt jest uważany za bezpieczny, jeżeli został zaprojektowany i wykonany w sposób zapewniający poziom bezpieczeństwa adekwatny do cyberryzyka, które wiąże się z jego użyciem, w chwili sprzedaży nie ma znanych podatności, jest bezpiecznie skonfigurowany według domyślnego standardu (ang. „default") i objęty ochroną przed nielegalnymi połączeniami, chroni gromadzone przez siebie dane i gromadzi wyłącznie dane potrzebne mu do działania.

2.8. Uznaje się, że producent może wprowadzać do obrotu swe produkty, jeżeli podaje do wiadomości wykaz różnych elementów oprogramowania produktów, stosuje szybko bezpłatne środki zaradcze w przypadku wystąpienia nowych podatności, upublicznia i szczegółowo opisuje stwierdzone podatności i im zaradza, a także regularnie sprawdza solidność produktów wprowadzanych przez siebie na rynek. Te i inne działania przewidziane w akcie dotyczącym cyberodporności powinny być podejmowane przez cały cykl życia produktu, a przynajmniej przez 5 lat od czasu jego wprowadzenia do obrotu. Producent jest zobowiązany do usunięcia podatności za pomocą okresowej aktualizacji oprogramowania.

2.9. Zgodnie z ogólną zasadą stosowaną w różnych sektorach obowiązki spoczywają również na importerach i dystrybutorach.

2.10. W akcie dotyczącym cyberodporności przewidziano makrokategorię tzw. normalnych produktów i oprogramowania, w przypadku których można zdać się na samoocenę producenta, tak jak ma to już miejsce w przypadku innych rodzajów certyfikacji oznakowania CE. Według Komisji 90 % produktów na rynku należy do tej kategorii.

2.11. Przedmiotowe produkty mogą być wprowadzane do obrotu po dokonaniu samooceny ich cyberbezpieczeństwa przez producenta, który przedstawia odpowiednią dokumentację zgodnie z wytycznymi zawartymi w przepisach. Producent jest zobowiązany do powtórzenia oceny w przypadku modyfikacji produktu.

2.12. Pozostałych 10 % produktów dzieli się na dwie inne kategorie (klasa I – mniej niebezpieczne – i klasa II – bardziej niebezpieczne), których wprowadzenie do obrotu wymaga większej uwagi. Są to tzw. produkty o krytycznym znaczeniu zawierające elementy cyfrowe, których wadliwość może prowadzić do innych niebezpiecznych i bardziej rozległych naruszeń bezpieczeństwa.

2.13. W przypadku produktów należących do tych dwóch klas podstawowe oświadczenia własne są dopuszczalne jedynie wówczas, gdy producent wykaże zgodność z konkretnymi normami rynkowymi oraz z przewidzianymi już przez UE wymogami bezpieczeństwa lub certyfikacji cyberbezpieczeństwa. W przeciwnym razie może uzyskać certyfikację produktu od akredytowanego podmiotu certyfikującego, którego poświadczenie jest obowiązkowe w przypadku produktów klasy II.

2.14. System klasyfikacji produktów według kategorii ryzyka został również zawarty we wniosku dotyczącym rozporządzenia w sprawie IA (sztucznej inteligencji). Aby uniknąć wątpliwości co do tego, które przepisy mają zastosowanie, w akcie dotyczącym cyberodporności uwzględniono produkty zawierające elementy cyfrowe, które równocześnie klasyfikuje się jako „systemy IA wysokiego ryzyka" w rozumieniu wniosku dotyczącego IA. Takie produkty będą zasadniczo musiały być zgodne z procedurą oceny zgodności określoną w rozporządzeniu w sprawie IA, z wyjątkiem produktów cyfrowych o krytycznym znaczeniu, do których – oprócz zasadniczych wymogów określonych w akcie dotyczącym cyberodporności – będą miały zastosowanie normy oceny zgodności przewidziane w tym akcie.

2.15. Aby zapewnić zgodność z aktem dotyczącym cyberodporności, przewiduje się nadzór, który każde państwo członkowskie będzie musiało powierzyć organowi krajowemu. Zgodnie z przepisami dotyczącymi bezpieczeństwa innych produktów – jeżeli organ krajowy stwierdzi, że dany produkt nie posiada zabezpieczeń cyberbezpieczeństwa, jego wprowadzenie do obrotu może w danym państwie zostać zawieszone. Agencja ENISA uprawniona do szczegółowej oceny zgłoszonego produktu, która to ocena – w wypadku stwierdzenia braku bezpieczeństwa danego produktu – może prowadzić do zawieszenia jego wprowadzenia na rynek w UE.

2.16. Akt dotyczący cyberodporności obejmuje system kar – odpowiadający powadze naruszenia – które w razie naruszenia podstawowych wymogów cyberbezpieczeństwa produktów mogą sięgnąć 15 mln EUR lub 2,5 % obrotów uzyskanych w poprzednim roku podatkowym.

3. **Uwagi**

3.1. EKES z zadowoleniem przyjmuje pomysł Komisji, by do szerszej mozaiki przepisów dotyczących cyberbezpieczeństwa dodać kluczowy element, który jest skoordynowany z dyrektywą NIS ([1]) i ją uzupełnia, a także dopełnia akt o cyberbezpieczeństwie ([2]). Wysokie standardy cyberbezpieczeństwa odgrywają bowiem zasadniczą rolę w tworzeniu solidnego unijnego systemu cyberbezpieczeństwa dla wszystkich podmiotów gospodarczych, który jest przydatny w zapewnianiu obywatelom UE bezpiecznego korzystania ze wszystkich produktów znajdujących się na rynku, a także w zwiększeniu ich zaufania do świata cyfrowego.

3.2. W rozporządzeniu poruszono zatem dwie kwestie: niski poziom cyberbezpieczeństwa wielu produktów oraz – przede wszystkim – fakt, że wielu producentów nie zapewnia aktualizacji w celu zaradzenia podatnościom. Chociaż reputacja wytwórców produktów zawierających elementy cyfrowe zostaje czasami nadszarpnięta z powodu braku bezpieczeństwa ich produktów, koszty podatności pokrywają głównie użytkownicy profesjonalni i konsumenci. Ogranicza to motywację producentów do inwestowania w projektowanie i rozwój bezpiecznych produktów oraz do zapewniania aktualizacji bezpieczeństwa. Ponadto przedsiębiorstwa i konsumenci często nie mają wystarczających i dokładnych

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

informacji na temat wyboru bezpiecznych produktów i niejednokrotnie nie wiedzą, w jaki sposób upewnić się, że nabywane produkty są skonfigurowane w bezpieczny sposób. Nowe przepisy odnoszą się do tych dwóch aspektów, gdyż poruszono w nich kwestię aktualizacji i zagadnienie dostarczania aktualnych informacji klientom. EKES uważa, że jeżeli proponowane rozporządzenie zostanie prawidłowo wdrożone, może stać się międzynarodowym punktem odniesienia i wzorcem w dziedzinie cyberbezpieczeństwa.

3.3. EKES z zadowoleniem przyjmuje propozycję wprowadzenia wymogów w zakresie cyberbezpieczeństwa odnoszących się do produktów zawierających elementy cyfrowe. Istotne będzie jednak, by nie dopuścić do nakładania się wymogów na inne obowiązujące przepisy w tym zakresie, takie jak nowa dyrektywa NIS 2 ([3]) i rozporządzenie w sprawie IA.

3.4. EKES pragnie podkreślić, że choć godne uznania jest to, że akt dotyczący cyberodporności odnosi się właściwie do wszystkich produktów cyfrowych, to jego praktyczne wdrażanie może przysporzyć problemów, zważywszy na ścisłą weryfikację i kontrolę, których on wymaga.

3.5. Zakres przedmiotowy aktu dotyczącego cyberodporności jest szeroki i obejmuje wszystkie produkty zawierające elementy cyfrowe. Zgodnie z proponowaną definicją uwzględniono wszystkie produkty w postaci oprogramowania i sprzętu, a także związane z nimi operacje przetwarzania danych. EKES proponuje, by Komisja wyjaśniła, czy w zakres stosowania wniosku dotyczącego rozporządzenia wchodzą wszystkie produkty będące oprogramowaniem.

3.6. Producenci będą zobowiązani do zgłaszania – z jednej strony – podatności, które są aktywnie wykorzystywane, a z drugiej strony – incydentów. Będą zobowiązani do informowania agencji ENISA o wszelkich aktywnie wykorzystywanych podatnościach produktu oraz (oddzielnie) o wszelkich incydentach mających wpływ na bezpieczeństwo produktu, w każdym razie w ciągu 24 godzin od uzyskania wiedzy o nich. W związku z tym EKES podkreśla, że ENISA musi dysponować odpowiednimi zasobami pod względem liczbowym i z punktu widzenia przygotowania zawodowego, by móc skutecznie wykonywać istotne i trudne zadania powierzone jej na mocy rozporządzenia.

3.7. Niepewność co do tego, które przepisy mają zastosowanie, może wiązać się z tym, że szereg produktów objętych zakresem stosowania wniosku podlega również innym przepisom dotyczącym cyberbezpieczeństwa. Chociaż akt dotyczący cyberodporności przewiduje spójność z obowiązującymi unijnymi ramami regulacyjnymi dotyczącymi produktów oraz z innymi wnioskami sporządzanymi obecnie w kontekście strategii cyfrowej UE, to jednak takie przepisy jak na przykład te dotyczące produktów sztucznej inteligencji wysokiego ryzyka pokrywają się z przepisami rozporządzenia o ochronie danych. W związku z tym EKES proponuje, by Komisja opracowała odpowiednie wytyczne w celu ukierunkowania producentów i konsumentów na prawidłowe wdrażanie wspomnianego aktu.

3.8. EKES zaznacza, że związek między podmiotami certyfikującymi w rozumieniu aktu dotyczącego cyberodporności a ewentualnymi innymi organami uprawnionymi do certyfikacji cyberbezpieczeństwa na mocy innych, w tym samym stopniu obowiązujących przepisów nie wydaje się całkowicie jasny.

3.9. Podmioty certyfikujące są poza tym w dużym stopniu obciążone pracą i odpowiedzialnością, w związku z czym trzeba zweryfikować i zagwarantować ich praktyczną operacyjność, tak by akt dotyczący cyberodporności nie prowadził do wzrostu nałożonych już na producentów obciążeń biurokratycznych, z których muszą się wywiązać, by działać na rynku. Dlatego też istotne byłoby również, aby zwłaszcza MŚP i MMŚP miały dostęp do wykwalifikowanego wsparcia ekspertów, którzy byliby w stanie świadczyć konkretne profesjonalne usługi.

3.10. Akt dotyczący cyberodporności przewiduje, że przy świadczeniu usług podmioty certyfikujące muszą uwzględniać szczególne potrzeby MŚP; niemniej EKES zwraca uwagę na potrzebę doprecyzowania kryteriów zastosowania tego aktu.

3.11. Problem z koordynacją może wystąpić ponadto między organami nadzorczymi przewidzianymi w omawianym rozporządzeniu a organami już działającymi na mocy innych przepisów mających zastosowanie do tych samych produktów. W związku z tym EKES proponuje Komisji, by wezwała państwa członkowskie do czuwania nad sytuacją i – w razie potrzeby – do podjęcia działań w celu zapobieżenia takiej ewentualności.

Bruksela, dnia 14 grudnia 2022 r.

Christa SCHWENG
Przewodnicząca
Europejskiego Komitetu Ekonomiczno-Społecznego

([3]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).