KOMUNIKAT KOMISJI

Wytyczne Komisji dotycz?ce stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS 2)

(2023/C 328/02)

I. WPROWADZENIE

1. Zgodnie z art. 4 ust. 3 dyrektywy 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 (dyrektywa NIS 2) ([1]) Komisja do dnia 17 lipca 2023 r. podaje wytyczne wyjaśniające stosowanie art. 4 ust. 1 i 2 tej dyrektywy.

2. Niniejsze wytyczne zawierają wyjaśnienia stosowania tych przepisów, które dotyczą związku między dyrektywą (UE) 2022/2555 a obecnymi i przyszłymi sektorowymi aktami prawnymi Unii, w których przewidziano środki zarządzania ryzykiem w cyberbezpieczeństwie lub wymogi w zakresie zgłaszania incydentów. W dodatku do niniejszych wytycznych zawarto wykaz sektorowych aktów prawnych Unii, które zdaniem Komisji wchodzą w zakres stosowania art. 4 dyrektywy (UE) 2022/2555. To, że danego aktu prawnego nie uwzględniono w wykazie zawartym w tym dodatku, niekoniecznie oznacza, że akt ten nie wchodzi w zakres stosowania tego przepisu.

3. Zgodnie z art. 4 ust. 3 zdanie trzecie dyrektywy (UE) 2022/2555 przed przyjęciem niniejszych wytycznych Komisja uwzględniła uwagi Grupy Współpracy ds. bezpieczeństwa sieci i informacji i Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

4. Niniejsze wytyczne pozostają bez uszczerbku dla wykładni prawa Unii dokonywanej przez Trybunał Sprawiedliwości Unii Europejskiej.

II. RÓWNOWAŻNOŚĆ WYMOGÓW DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA W SEKTOROWYCH AKTACH PRAWNYCH UNII

5. Jak przewidziano w art. 4 ust. 1 dyrektywy (UE) 2022/2555, w przypadku gdy na podstawie sektorowych aktów prawnych Unii wymaga się od podmiotów kluczowych lub ważnych przyjęcia środków zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania poważnych incydentów i w przypadku gdy wymogi te są co najmniej równoważne pod względem skutku obowiązkom określonym w tej dyrektywie, nie stosuje się do takich podmiotów odpowiednich przepisów dyrektywy (UE) 2022/2555, w tym przepisów dotyczących nadzoru i egzekwowania przepisów określonych w rozdziale VII tej dyrektywy. W przepisie tym przewidziano ponadto, że jeżeli sektorowe akty prawne Unii nie obejmują wszystkich podmiotów w konkretnym sektorze, objętych zakresem stosowania dyrektywy (UE) 2022/2555, odpowiednie przepisy tej dyrektywy nadal mają zastosowanie do podmiotów nieobjętych tymi sektorowymi aktami prawnymi Unii.

II.1. Wymogi dotyczące zarządzania ryzykiem w cyberbezpieczeństwie

6. Jak przewidziano w art. 4 ust. 2 lit. a) dyrektywy (UE) 2022/2555, środki zarządzania ryzykiem w cyberbezpieczeństwie, które podmioty kluczowe lub ważne są zobowiązane przyjąć na podstawie sektorowych aktów prawnych Unii, uznaje się za równoważne pod względem skutku obowiązkom określonym w dyrektywie (UE) 2022/2555, jeżeli środki te są co najmniej równoważne pod względem skutku środkom określonym w art. 21 ust. 1 i 2 tej dyrektywy. Aby ocenić, czy wymogi określone w sektorowym akcie prawnym Unii dotyczącym środków zarządzania ryzykiem w cyberbezpieczeństwie są co najmniej równoważne pod względem skutku środkom określonym w art. 21 ust. 1 i 2 dyrektywy (UE) 2022/2555, należy sprawdzić, czy wymogi określone w tym sektorowym akcie prawnym Unii co najmniej odpowiadają wymogom przedmiotowych przepisów lub mają szerszy zakres, tj. przepisy sektorowe mogą zawierać bardziej szczegółowe przepisy pod względem merytorycznym w porównaniu z odpowiednimi przepisami dyrektywy (UE) 2022/2555.

([1]) Dz.U. L 333 z 27.12.2022, s. 80.

7. Zgodnie z art. 21 ust. 1 akapit pierwszy dyrektywy (UE) 2022/2555 państwa członkowskie zapewniają, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług. Środki te powinny być oparte na analizie ryzyka oraz umożliwiać zapobieżenie wpływowi incydentów lub minimalizowanie takiego wpływu. W art. 21 ust. 1 akapit drugi dyrektywy (UE) 2022/2555 określono, jak należy oceniać proporcjonalność takich środków ([2]). Określony w art. 21 ust. 1 dyrektywy (UE) 2022/2555 obowiązek, zgodnie z którym podmioty kluczowe i ważne są zobowiązane przyjąć odpowiednie i proporcjonalne środki zarządzania ryzykiem w cyberbezpieczeństwie, odnosi się do wszystkich działalności danego podmiotu i świadczonych przez niego usług, a nie tylko do określonych zasobów technologii informacyjnej (IT) lub usług krytycznych świadczonych przez ten podmiot.

8. Oceniając równoważność sektorowego aktu prawnego Unii z odpowiednimi przepisami dotyczącymi zarządzania ryzykiem w cyberbezpieczeństwie zawartymi w dyrektywie (UE) 2022/2555, należy zwrócić szczególną uwagę na to, czy obowiązki w zakresie bezpieczeństwa przewidziane w danym akcie prawnym obejmują środki zapewniające bezpieczeństwo sieci i systemów informatycznych. Definicja „bezpieczeństwa sieci i systemów informatycznych" zawarta w art. 6 pkt 2 dyrektywy (UE) 2022/2555 odnosi się do odporności systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem. Zastosowane w tej definicji terminy „dostępność", „autentyczność", „integralność" i „poufność" odnoszą się do wszystkich czterech celów ochrony związanych z bezpieczeństwem sieci i systemów informatycznych. Termin „sieci i systemy informatyczne" zdefiniowany w art. 6 pkt 1 dyrektywy (UE) 2022/2555 obejmuje sieci łączności elektronicznej ([3]); urządzenie lub grupę wzajemnie połączonych lub powiązanych urządzeń, z których co najmniej jedno, na podstawie programu, automatycznie przetwarza dane cyfrowe; oraz dane cyfrowe przechowywane, przetwarzane, pobierane lub przekazywane przez takie sieci łączności elektronicznej lub urządzenia w celu ich eksploatacji, użycia, ochrony lub utrzymania. W związku z tym środki bezpieczeństwa, których wprowadzenia wymaga sektorowy akt prawny Unii, powinny również obejmować sprzęt, oprogramowanie układowe i oprogramowanie komputerowe wykorzystywane w działalności podmiotu.

9. Inną ważna kwestią do uwzględnienia przy ocenie równoważności sektorowego aktu prawnego Unii z wymogami art. 21 ust. 1 i 2 dyrektywy (UE) 2022/2555 jest to, że środki zarządzania ryzykiem w cyberbezpieczeństwie wymagane na podstawie tego aktu powinny opierać się na podejściu uwzględniającym wszystkie zagrożenia. Ponieważ zagrożenia dla bezpieczeństwa sieci i systemów informatycznych mogą mieć różne źródła, każdy rodzaj zdarzenia może mieć negatywny wpływ na sieci i systemy informatyczne podmiotu i potencjalnie prowadzić do incydentu. Dlatego też środki zarządzania ryzykiem w cyberbezpieczeństwie stosowane przez podmiot powinny służyć ochronie nie tylko sieci i systemów informatycznych podmiotu, ale także środowiska fizycznego tych systemów przed jakimkolwiek zdarzeniem takim jak sabotaż, kradzież, pożar, powódź, awaria telekomunikacyjna bądź awaria zasilania lub nieuprawniony dostęp fizyczny, które to zdarzenia mogłyby naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub też usług oferowanych przez sieci i systemy informatyczne lub dostępnych za pośrednictwem sieci i systemów informatycznych. W związku z powyższym środki zarządzania ryzykiem w cyberbezpieczeństwie wymagane na podstawie sektorowego aktu prawnego Unii powinny dotyczyć fizycznego i środowiskowego bezpieczeństwa sieci i systemów informatycznych jako aspektu zapewniającego ochronę przed awarią, błędem ludzkim, złośliwymi działaniami lub zjawiskami naturalnymi ([4]).

10. Zgodnie z art. 21 ust. 2 dyrektywy (UE) 2022/2555 środki zarządzania ryzykiem w cyberbezpieczeństwie muszą również obejmować szczególne wymogi w zakresie bezpieczeństwa, które wymieniono w ust. 2 lit. a)–j) tego artykułu. Wymogi te obejmują środki takie jak politykę analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługę incydentu, ciągłość działania, zarządzanie kryzysowe, bezpieczeństwo łańcucha dostaw, polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania. Zgodnie z art. 21 ust. 5 akapit drugi dyrektywy (UE) 2022/2555 Komisja jest uprawniona do przyjmowania aktów wykonawczych określających wymogi techniczne i metodykę, a w razie potrzeby również wymogi sektorowe, dotyczące środków bezpieczeństwa, o których

([2]) Zob. również motywy 78, 81 i 82 preambuły dyrektywy (UE) 2022/2555.

([3]) Art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (Dz.U. L 321 z 17.12.2018, s. 36).

([4]) Zob. motyw 79 preambuły dyrektywy (UE) 2022/2555.

mowa w art. 21 ust. 2 tej dyrektywy. Do 17 października 2024 r. Komisja przyjmuje akty wykonawcze określające wymogi techniczne i metodykę dotyczącą środków bezpieczeństwa, o których mowa w art. 21 ust. 2 dyrektywy (UE) 2022/2555, w odniesieniu do dostawców usług systemów nazw domen („DNS"), rejestrów nazw domen najwyższego poziomu („TLD"), dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform usług sieci społecznościowych i dostawców usług zaufania. Akty wykonawcze określają bardziej szczegółowo główne warunki i kryteria wykonania określone w akcie podstawowym, nie wpływając na treść tego aktu ([5]).

II.2. **Wymogi w zakresie zgłaszania incydentów**

11. Zgodnie z art. 4 ust. 2 lit. b) dyrektywy (UE) 2022/2555 wymogi dotyczące zgłaszania poważnych incydentów uznaje się za równoważne pod względem skutku obowiązkom określonym w tej dyrektywie, jeżeli sektorowy akt prawny Unii przewiduje natychmiastowy dostęp zespołów reagowania na incydenty bezpieczeństwa komputerowego („CSIRT"), właściwych organów lub pojedynczych punktów kontaktowych („SPOC") do zgłoszeń incydentów – w stosownych przypadkach automatycznie i bezpośrednio, oraz jeżeli wymogi dotyczące zgłaszania poważnych incydentów są co najmniej równoważne pod względem skutku wymogom określonym w art. 23 ust. 1–6 dyrektywy (UE) 2022/2555.

12. Ponieważ wymogi sektorowego aktu prawnego Unii dotyczące zgłaszania poważnych incydentów muszą być co najmniej równoważne pod względem skutku wymogom określonym w art. 23 ust. 1–6 dyrektywy (UE) 2022/2555, aby wymogi określone w tym akcie miały zastosowanie zamiast obowiązków w zakresie zgłaszania incydentów określonych w tej dyrektywie, wymogi określone w art. 23 ust. 1–6 dyrektywy mają szczególne znaczenie do celów oceny równoważności. W art. 23 ust. 1–6 dyrektywy (UE) 2022/2555 określono bardziej szczegółowo, jakiego rodzaju incydenty należy zgłaszać, komu należy je zgłaszać, w jakim czasie oraz jakie informacje należy zgłosić. Kwestie te wyjaśniono bardziej szczegółowo w kolejnych sekcjach.

II.2.1. *Zgłaszanie poważnych incydentów CSIRT, właściwym organom oraz odbiorcom*

13. Zgodnie z art. 23 ust. 1 akapit pierwszy zdanie pierwsze dyrektywy (UE) 2022/2555 podmioty kluczowe i ważne mają obowiązek zgłaszania bez zbędnej zwłoki swojemu właściwemu CSIRT lub, jeżeli ma to zastosowanie, swojemu właściwemu organowi każdego poważnego incydentu. Zgodnie z art. 23 ust. 1 akapit pierwszy zdanie drugie dyrektywy (UE) 2022/2555 w stosownych przypadkach podmioty kluczowe i ważne mają obowiązek powiadamiania bez zbędnej zwłoki odbiorców swoich usług o poważnych incydentach, które mogą mieć niekorzystny wpływ na świadczenie tych usług.

14. Podczas gdy w art. 6 pkt 6 dyrektywy (UE) 2022/2555 termin „incydenty" zdefiniowano bardzo szeroko jako każde zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem, w art. 23 ust. 1 tej dyrektywy obowiązkiem zgłaszania incydentów objęto jedynie poważne incydenty. Incydent jest poważny, jeżeli spowodował lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu (art. 23 ust. 3 lit. a)) lub wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe (art. 23 ust. 3 lit. b)).

([5]) Zob. rozdział D zatytułowany „Dodatkowe przepisy dotyczące wykonania aktu podstawowego", w: „Niewiążące kryteria stosowania art. 290 i 291 Traktatu o funkcjonowaniu Unii Europejskiej" – 18 czerwca 2019 r. (Dz.U. C 223 z 3.7.2019, s. 1).

15. W motywie 101 preambuły dyrektywy (UE) 2022/2555 wyjaśniono, że zgłaszanie incydentów powinno opierać się na wstępnej ocenie przeprowadzonej przez dany podmiot. W takiej ocenie wstępnej należy wziąć pod uwagę między innymi sieci i systemy informatyczne, których dotyczy incydent, a w szczególności ich znaczenie dla świadczenia usług danego podmiotu, dotkliwość i charakterystykę techniczną cyberzagrożenia oraz bazowe podatności, które są wykorzystywane, a także doświadczenia podmiotu z podobnymi incydentami. Wskaźniki takie jak zakres skutków dla funkcjonowania usługi, czas trwania incydentu lub liczba dotkniętych nim odbiorców usług mogą odegrać ważną rolę w ustaleniu, czy zakłócenie operacyjne usługi jest dotkliwe.

16. Zgodnie z art. 23 ust. 11 akapit drugi dyrektywy (UE) 2022/2555 Komisja jest uprawniona przyjmowania aktów wykonawczych doprecyzowujących przypadki, w których incydent uznaje się za poważny. Do 17 października 2024 r. Komisja przyjmuje takie akty wykonawcze w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform usług sieci społecznościowych. Akty wykonawcze określają bardziej szczegółowo główne warunki i kryteria wykonania określone w akcie podstawowym, nie wpływając na treść tego aktu ([6]).

II.2.2. *Wieloetapowe podejście do zgłaszania poważnych incydentów oraz ramy czasowe zgłaszania takich incydentów*

17. W dyrektywie (UE) 2022/2555 określono wieloetapowe podejście do zgłaszania poważnych incydentów, które obejmuje wczesne ostrzeżenie, zgłoszenie incydentu i sprawozdanie końcowe. Te trzy elementy można uzupełnić sprawozdaniem okresowym i sprawozdaniem z postępu prac.

18. Celem wieloetapowego podejścia do zgłaszania poważnych incydentów jest zapewnienie odpowiedniej równowagi między szybkim zgłaszaniem, które pomaga zahamować potencjalne rozprzestrzenianie się poważnych incydentów i pozwala podmiotom kluczowym i ważnym zwrócić się o pomoc, a szczegółowym zgłaszaniem, które umożliwia wyciągnięcie cennych wniosków z poszczególnych incydentów i z czasem poprawia cyberodporność poszczególnych podmiotów i całych sektorów ([7]).

19. Zgodnie z wieloetapowym podejściem podmioty kluczowe i ważne muszą w pierwszej kolejności przekazać wczesne ostrzeżenie właściwemu CSIRT lub właściwemu organowi bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia informacji o takim poważnym incydencie. Następnie podmioty te muszą przekazać zgłoszenie incydentu bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od powzięcia informacji o takim poważnym incydencie. Potem właściwy CSIRT lub właściwy organ może wystąpić o przedłożenie sprawozdania okresowego. Na koniec należy dostarczyć sprawozdanie końcowe właściwemu CSIRT lub właściwemu organowi nie później niż miesiąc po przekazaniu zgłoszenia incydentu, chyba że incydent nadal trwa w tym czasie, w którym to przypadku należy dostarczyć sprawozdanie z postępu prac i sprawozdanie końcowe w ciągu jednego miesiąca od obsługi incydentu.

20. W przypadku zgłoszenia incydentu, o którym mowa w art. 23 ust. 4 akapit drugi dyrektywy (UE) 2022/2555, obowiązują inne ramy czasowe w odniesieniu do dostawców usług zaufania. Dostawcy ci muszą przekazać zgłoszenie poważnych incydentów, które mają wpływ na świadczenie ich usług zaufania, bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia informacji o takim poważnym incydencie.

([6]) Zob. rozdział D zatytułowany „Dodatkowe przepisy dotyczące wykonania aktu podstawowego", w: „Niewiążące kryteria stosowania art. 290 i 291 Traktatu o funkcjonowaniu Unii Europejskiej" – 18 czerwca 2019 r. (Dz.U. C223 z 3.7.2019, s. 1).

([7]) Zob. motyw 101 preambuły dyrektywy (UE) 2022/2555.

II.2.3. *Treść obowiązkowych zgłoszeń poważnych incydentów kierowanych do CSIRT lub właściwych organów*

21. Zasadniczo zgodnie z art. 23 ust. 1 akapit pierwszy zdanie trzecie dyrektywy (UE) 2022/2555 państwa członkowskie mają obowiązek zapewnić, aby podmioty kluczowe i ważne zgłaszały m.in. informacje umożliwiające właściwemu CSIRT lub, w stosownych przypadkach, właściwemu organowi ustalenie transgranicznego wpływu incydentu. Omawiany wymóg dotyczący treści obowiązkowych zgłoszeń został doprecyzowany w art. 23 ust. 4 dyrektywy (UE) 2022/2555, w którym określono wieloetapowe podejście.

22. Zgodnie z art. 23 ust. 4 lit. a) wczesne ostrzeżenie, w stosownych przypadkach, musi wskazywać, czy istnieje podejrzenie, że poważny incydent jest spowodowany czynami niezgodnymi z prawem lub popełnionymi w złym zamiarze lub czy może on mieć wpływ transgraniczny (czy istnieje takie prawdopodobieństwo). Zgodnie z motywem 102 preambuły dyrektywy (UE) 2022/2555 wczesne ostrzeżenie powinno zawierać tylko informacje niezbędne do tego, by powiadomić właściwy CSIRT lub właściwy organ o wystąpieniu poważnego incydentu i umożliwić danemu podmiotowi zwrócenie się o pomoc w razie potrzeby.

23. Zgłoszenie incydentu musi zawierać, w stosownych przypadkach, aktualizację informacji przedłożonych w ramach wczesnego ostrzeżenia. Ponadto musi zawierać wstępną ocenę poważnego incydentu, w tym jego dotkliwości i skutków, a w stosownych przypadkach także wskaźników naruszenia integralności systemu.

24. W przypadku konieczności przedłożenia sprawozdania okresowego należy uwzględnić w nim informacje na temat odpowiednich aktualizacji statusu. Sprawozdanie końcowe musi zawierać szczegółowy opis incydentu, w tym jego dotkliwości i skutków, rodzaj zagrożenia lub pierwotną przyczynę, która prawdopodobnie była źródłem incydentu, zastosowane i wdrażane środki ograniczające ryzyko oraz, w stosownych przypadkach, transgraniczny wpływ tego incydentu.

II.2.4. *Natychmiastowy dostęp do zgłoszeń incydentów*

25. Zgodnie z art. 4 ust. 2 lit. b) dyrektywy (UE) 2022/2555, aby sektorowy akt prawny Unii miał zastosowanie do wymogów w zakresie zgłaszania incydentów zamiast tej dyrektywy, musi on zapewniać CSIRT, właściwym organom lub SPOC wyznaczonym na podstawie dyrektywy (UE) 2022/2555 natychmiastowy dostęp do zgłoszeń incydentów dokonywanych zgodnie z sektorowym aktem prawnym Unii. Zgodnie z motywem 24 preambuły dyrektywy (UE) 2022/2555 taki natychmiastowy dostęp można zapewnić w szczególności, jeżeli zgłoszenia incydentów są przekazywane bez zbędnej zwłoki CSIRT, właściwemu organowi lub SPOC.

26. Natychmiastowy dostęp można zapewnić za pomocą automatycznych i bezpośrednich środków, które państwa członkowskie powinny wdrożyć w stosownych przypadkach. Mechanizmy automatycznego i bezpośredniego zgłaszania incydentów zapewniają systematyczną i natychmiastową wymianę informacji z CSIRT, właściwymi organami lub SPOC w odniesieniu do postępowania w przypadku zgłoszeń incydentów. W celu uproszczenia zgłaszania incydentów oraz wdrożenia mechanizmu automatycznego i bezpośredniego zgłaszania incydentów państwa członkowskie mogą również korzystać z pojedynczego punktu zgłaszania incydentów, który musi być zgodny z sektorowym aktem prawnym Unii.

27. Oceniając, czy określone w sektorowym akcie prawnym Unii wymogi dotyczące zgłaszania poważnych incydentów są co najmniej równoważne pod względem skutku wymogom określonym w art. 23 ust. 1–6 dyrektywy (UE) 2022/2555, wymogi określone w tym sektorowym akcie prawnym Unii powinny co najmniej odpowiadać wymogom art. 23 ust. 1–6 lub być bardziej szczegółowe niż wymogi określone w tych przepisach. Wymogi określone w sektorowym akcie prawnym Unii powinny odnosić się do rodzaju incydentów, które podlegają zgłoszeniu zgodnie z dyrektywą (UE) 2022/2555, uwzględniając w szczególności odbiorców, treść oraz mające zastosowanie ramy prawne.

III. KONSEKWENCJE RÓWNOWAŻNOŚCI

III.1. Nadzór i egzekwowanie przepisów

28. W przypadku gdy wymogi określone w sektorowych aktach prawnych Unii są co najmniej równoważne pod względem skutku obowiązkom określonym w dyrektywie (UE) 2022/2555, nie tylko nie stosuje się odpowiednich przepisów tej dyrektywy dotyczących obowiązku przyjęcia środków zarządzania ryzykiem w cyberbezpieczeństwie i zgłaszania poważnych incydentów, ale także zastosowania nie mają przepisy dotyczące nadzoru i egzekwowania przepisów określone w rozdziale VII dyrektywy (UE) 2022/2555.

29. W motywie 25 preambuły dyrektywy (UE) 2022/2555 wyjaśniono, że sektorowe akty prawne Unii, które są co najmniej równoważne pod względem skutku, mogą przewidywać, że właściwe organy wyznaczone na podstawie takich aktów swoje uprawnienia dotyczące nadzoru i egzekwowania przepisów w odniesieniu do obowiązków w zakresie zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków w zakresie zgłaszania incydentów wykonują z pomocą właściwych organów wyznaczonych na podstawie dyrektywy (UE) 2022/2555. Odpowiednie właściwe organy mogą w tym celu przyjąć ustalenia dotyczące współpracy, w tym procedury dotyczące koordynacji działań nadzorczych procedury dochodzeń i kontroli na miejscu zgodnie z prawem krajowym, oraz mechanizm wymiany między właściwymi organami istotnych informacji na temat nadzoru i egzekwowania przepisów. Taki mechanizm wymiany istotnych informacji może obejmować dostęp do informacji związanych z cyberprzestrzenią, o które właściwe organy zwracają się na podstawie dyrektywy (UE) 2022/2555.

III.2. Krajowa strategia cyberbezpieczeństwa

30. Zgodnie z art. 7 ust. 1 dyrektywy (UE) 2022/2555 każde państwo członkowskie ma obowiązek przyjąć krajową strategię cyberbezpieczeństwa. Krajowa strategia cyberbezpieczeństwa to ustanowione przez dane państwo członkowskie spójne ramy określające strategiczne cele i priorytety w obszarze cyberbezpieczeństwa oraz środki służące ich realizacji w tym państwie członkowskim (zob. art. 6 pkt 4 dyrektywy (UE) 2022/2555). Strategia cyberbezpieczeństwa musi określać m.in. cele i priorytety obejmujące w szczególności sektory, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555. Ponadto strategia ta musi obejmować ramy zarządzania służące realizacji tych celów i priorytetów, w tym musi zawierać polityki, o których mowa w art. 7 ust. 2 dyrektywy (UE) 2022/2555.

31. Ponadto zgodnie z art. 7 ust. 1 lit. c) dyrektywy (UE) 2022/2555 krajowa strategia cyberbezpieczeństwa musi obejmować ramy zarządzania wyjaśniające role i obowiązki zainteresowanych stron na szczeblu krajowym, stanowiące podstawę współpracy i koordynacji na szczeblu krajowym między właściwymi organami, SPOC i CSIRT na gruncie dyrektywy (UE) 2022/2555, a także koordynacji i współpracy między tymi podmiotami a właściwymi organami na gruncie sektorowych aktów prawnych Unii.

32. W związku z tym wymóg przyjęcia strategii cyberbezpieczeństwa na podstawie art. 7 dyrektywy (UE) 2022/2555 nie dotyczy ani wymogów dotyczących cyberbezpieczeństwa nałożonych na podmioty kluczowe i ważne na podstawie art. 21 i 23 tej dyrektywy, ani przepisów dotyczących nadzoru i egzekwowania przepisów określonych w rozdziale VII, zgodnie z wymogiem określonym w art. 4 ust. 1 i 2 dyrektywy. Odpowiednie przepisy określone w art. 7 powinny nadal obowiązywać w przypadku sektorów, podsektorów i rodzajów podmiotów, w odniesieniu do których obowiązują sektorowe akty prawne Unii w rozumieniu art. 4 dyrektywy (UE) 2022/2555.

III.3. Wyznaczanie CSIRT

33. Zgodnie z art. 10 ust. 1 dyrektywy (UE) 2022/2555 państwa członkowskie muszą wyznaczyć lub ustanowić co najmniej jeden CSIRT, który obejmuje co najmniej sektory, podsektory i rodzaje podmiotu, o których mowa w załączniku I i II do dyrektywy, w tym sektory, podsektory i rodzaje podmiotów, w odniesieniu do których obowiązują sektorowe akty prawne Unii. Standardowo CSIRT wykonują w tym zakresie swoje zadania określone w art. 11 ust. 3 dyrektywy (UE) 2022/2555, chyba że w sektorowych aktach prawnych Unii określono ich szczególne zadania.

III.4. **Krajowe ramy zarządzania kryzysowego w cyberbezpieczeństwie i EU-CyCLONe**

34. Zgodnie z art. 9 ust. 1 dyrektywy (UE) 2022/2555 państwo członkowskie musi wyznaczyć lub ustanowić co najmniej jeden organ ds. zarządzania kryzysowego w cyberbezpieczeństwie odpowiedzialny za zarządzanie incydentami i sytuacjami kryzysowymi w cyberbezpieczeństwie na dużą skalę. Zgodnie z art. 6 pkt 7 tej dyrektywy incydent w cyberbezpieczeństwie na dużą skalę oznacza incydent, który powoduje zakłócenia na poziomie przekraczającym zdolność państwa członkowskiego do reagowania na ten incydent lub który wywiera znaczące skutki w co najmniej dwóch państwach członkowskich. W art. 9 ust. 4 dyrektywy (UE) 2022/2555 wymaga się, aby państwa członkowskie przyjęły również krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa się cele i tryb zarządzania incydentami i sytuacjami kryzysowymi w cyberbezpieczeństwie na dużą skalę. W planie tym należy określić m.in. procedury zarządzania kryzysowego w cyberprzestrzeni, w tym ich włączenie do ogólnych krajowych ram zarządzania kryzysowego, oraz kanały wymiany informacji, a także odpowiednie zainteresowane strony publiczne i prywatne oraz infrastrukturę. Takie procedury zarządzania kryzysowego w cyberprzestrzeni oraz odpowiednie zainteresowane strony publiczne i prywatne oraz infrastruktura mogą obejmować procedury sektorowe oraz zainteresowane strony z poszczególnych sektorów.

35. W art. 16 dyrektywy (UE) 2022/2555 ustanowiono Europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe), której celem jest pomaganie w skoordynowanym zarządzaniu na szczeblu operacyjnym incydentami i sytuacjami kryzysowymi w cyberbezpieczeństwie na dużą skalę oraz zapewnianie regularnej wymiany odpowiednich informacji między państwami członkowskimi a instytucjami, organami i jednostkami organizacyjnymi Unii.

36. Ponieważ art. 9 dotyczący ram zarządzania kryzysowego w cyberbezpieczeństwie oraz art. 16 dotyczący EU-CyCLONe nie są związane z wymogami dotyczącymi cyberbezpieczeństwa nakładanymi na podmioty na podstawie art. 21 i 23 dyrektywy (UE) 2022/2555 ani z przepisami dotyczącymi nadzoru i egzekwowania przepisów określonymi w rozdziale VII zgodnie z wymogiem określonym w art. 4 ust. 1 i 2 tej dyrektywy, art. 9 i 16 powinny w całości mieć zastosowanie do sektorów, nawet jeżeli istnieją sektorowe akty prawne Unii w rozumieniu art. 4. Tym samym państwo członkowskie musi wyznaczyć lub ustanowić co najmniej jeden organ ds. zarządzania kryzysowego w cyberbezpieczeństwie odpowiedzialny za zarządzanie incydentami i sytuacjami kryzysowymi w cyberbezpieczeństwie na dużą skalę w sektorach objętych zakresem stosowania sektorowych aktów prawnych Unii. Sektorów tych nie należy także pomijać przy przyjmowaniu krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę. Ponadto EU-CyCLONe powinna wykonywać swoje zadania przewidziane w art. 16 dyrektywy (UE) 2022/2555 w odniesieniu do sektorów, w których należące do nich podmioty podlegają sektorowym aktom prawnym Unii.

III.5. **Wyłączenie stosowania art. 3 ust. 3 i 4, art. 20 i art. 27 ust. 2 i 3**

37. Zgodnie z art. 3 ust. 3 dyrektywy (UE) 2022/2555 państwa członkowskie mają obowiązek ustanowić wykaz podmiotów kluczowych i ważnych, a także podmiotów świadczących usługi rejestracji nazw domen objęte zakresem stosowania dyrektywy. Zgodnie z art. 27 ust. 2 państwa członkowskie wymagają od podmiotów, o których mowa w art. 27 ust. 1 tej dyrektywy, przedłożenia właściwym organom określonych informacji. Ponieważ celem tych przepisów jest zapewnienie jasnego obrazu podmiotów objętych zakresem stosowania dyrektywy (UE) 2022/2555 w celu wsparcia nadzoru nad podmiotami kluczowymi i ważnymi objętymi zakresem tej dyrektywy, oznacza to, że przepisy te nie powinny mieć zastosowania do podmiotów, do których ma zastosowanie sektorowy akt prawny Unii w odniesieniu do wymogów w zakresie zarządzania ryzykiem w cyberbezpieczeństwie i zgłaszania incydentów. Nie uniemożliwia to państwom członkowskim włączenia takich podmiotów do wykazu.

Zgodnie z art. 20 ust. 1 dyrektywy (UE) 2022/2555 organy zarządzające podmiotów kluczowych i ważnych mają obowiązek zatwierdzić środki zarządzania ryzykiem w cyberbezpieczeństwie przyjęte przez te podmioty w celu zapewnienia zgodności z art. 21 i nadzorować ich wdrażanie, a także mogą być pociągnięte do odpowiedzialności za naruszanie przez te podmioty tego artykułu. Zgodnie z art. 20 ust. 2 tej dyrektywy państwa członkowskie zapewniają, aby członkowie organu zarządzającego podmiotów kluczowych i ważnych mieli obowiązek odbywać regularne szkolenia w celu zdobycia wystarczającej wiedzy i umiejętności pozwalających im rozpoznać ryzyko i ocenić praktyki zarządzania ryzykiem w cyberbezpieczeństwie oraz ich wpływ na usługi świadczone przez dany podmiot, a także zachęcają podmioty kluczowe i ważne do oferowania podobnych szkoleń ich pracownikom. Ponieważ obowiązki wynikające z art. 20 dyrektywy (UE) 2022/2555 są nieodłącznie związane z wymogami określonymi w art. 21 tej dyrektywy, oznacza to, że art. 20 nie powinien mieć zastosowania w przypadku sektorowych aktów prawnych Unii w rozumieniu art. 4 tej dyrektywy mających zastosowanie do wymogów w zakresie zarządzania ryzykiem w cyberbezpieczeństwie.

DODATEK

Sektorowe akty prawne Unii

Rozporządzenie (UE) 2022/2554 (rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego) ([1])

1. Art. 1 ust. 2 rozporządzenia (UE) 2022/2554 (rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego, DORA) stanowi, że w odniesieniu do podmiotów finansowych objętych zakresem stosowania dyrektywy (UE) 2022/2555 oraz odpowiednich krajowych przepisów transponujących tę dyrektywę rozporządzenie (UE) 2022/2554 uznaje się za sektorowy akt prawny Unii do celów art. 4 dyrektywy (UE) 2022/2555. Stwierdzenie to odzwierciedlono w motywie 28 preambuły dyrektywy (UE) 2022/2555, zgodnie z którym rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego należy uznać za sektorowy akt prawny Unii powiązany z dyrektywą (UE) 2022/2555 w odniesieniu do podmiotów finansowych. W związku z powyższym zamiast przepisów dyrektywy (UE) 2022/2555 zastosowanie powinny mieć przepisy rozporządzenia (UE) 2022/2554 dotyczące zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (ICT) (art. 6 i nast.), zarządzania incydentami związanymi z ICT, a w szczególności zgłaszania poważnych incydentów związanych z ICT (art. 17 i nast.), a także testowania operacyjnej odporności cyfrowej (art. 24 i nast.), mechanizmów wymiany informacji (art. 25) oraz ryzyka związanego z zewnętrznymi dostawcami ICT (art. 28 i nast.). Do podmiotów finansowych objętych rozporządzeniem (UE) 2022/2554 państwa członkowskie nie powinny zatem stosować przepisów dyrektywy (UE) 2022/2555 dotyczących zarządzania ryzykiem w cyberbezpieczeństwie i obowiązków w zakresie zgłaszania incydentów oraz nadzoru i egzekwowania przepisów.

2. W tym względzie podmioty finansowe uznaje się za podmioty, o których mowa w art. 2 ust. 1 lit. a)–t) rozporządzenia (UE) 2022/2554. Rodzaje podmiotów, które wchodzą w zakres stosowania rozporządzenia (UE) 2022/2554 jako podmioty finansowe, jak również dyrektywy (UE) 2022/2555 jako podmioty kluczowe lub ważne, obejmują instytucje kredytowe, systemy obrotu i kontrahentów centralnych. Ponieważ ważne jest utrzymanie silnych relacji i wymiany informacji z sektorem finansowym zgodnie z dyrektywą (UE) 2022/2555, rozporządzenie (UE) 2022/2554 umożliwia Europejskim Urzędom Nadzoru oraz właściwym organom wyznaczonym na podstawie tego rozporządzenia ubieganie się o udział w działaniach Grupy Współpracy ([2]) oraz wymianę informacji i współpracę z SPOC, a także z CSIRT i właściwymi organami wyznaczonymi na podstawie dyrektywy (UE) 2022/2555 ([3]). Właściwe organy wyznaczone na podstawie rozporządzenia (UE) 2022/2554 powinny także przekazywać dane na temat poważnych incydentów związanych z ICT i, w odpowiednich przypadkach, poważnych cyberzagrożeń także CSIRT, właściwym organom lub SPOC wyznaczonym na podstawie dyrektywy (UE) 2022/2555. Można to osiągnąć przez zapewnienie natychmiastowego dostępu do zgłoszeń incydentów i ich przekazywanie bezpośrednio lub za pośrednictwem pojedynczego punktu zgłaszania incydentów. CSIRT powinny mieć możliwość objęcia zakresem swoich działań sektora finansowego ([4]). Państwa członkowskie powinny w dalszym ciągu uwzględniać sektor finansowy w swoich strategiach cyberbezpieczeństwa. Przepisy dotyczące krajowych ram zarządzania kryzysowego w cyberbezpieczeństwie (art. 9 dyrektywy (UE) 2022/2555), jak również dotyczące EU-CyCLONe (art. 16 dyrektywy (UE) 2022/2555) powinny nadal mieć zastosowanie do podmiotów objętych zakresem rozporządzenia (UE) 2022/2554.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).

([2]) Art. 14 ust. 3 dyrektywy (UE) 2022/2555 i art. 47 ust. 1 rozporządzenia (UE) 2022/2554.

([3]) Zob. motyw 28 dyrektywy (UE) 2022/2555.

([4]) Tamże.