KOMISJA EUROPEJSKA

Strasburg, 20.1.2026
COM(2026) 13 wersja

ostateczna 2026/0012 (COD)

Wniosek dotyczący

DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY

zmieniającej dyrektywę (UE) 2022/2555 w odniesieniu do środków upraszczających i dostosowania do [wniosku dotyczącego aktu w sprawie cyberbezpieczeństwa 2]

{SWD(2026) 11-12 final} – {SEC(2026) 11 final}

(Tekst mający znaczenie dla EOG)

UZASADNIENIE

1. KONTEKST WNIOSKU

- **Uzasadnienie i cele wniosku**

Niniejszy wniosek stanowi część pakietu środków mających na celu dostosowanie unijnych ram w zakresie cyberbezpieczeństwa do potrzeb zainteresowanych stron w obliczu coraz bardziej wyrafinowanych zagrożeń cybernetycznych i złożonej sytuacji geopolitycznej. Istotne i ważne podmioty z sektorów krytycznych są coraz częściej celem cyberataków[1] a państwowe podmioty stanowiące zagrożenie wykorzystują nowe technologie, takie jak sztuczna inteligencja (AI), do dalszego zwiększania skali i optymalizacji swoich ataków. W tym kontekście odporność infrastruktury krytycznej na cyberzagrożenia uznaje się za strategiczny filar naszych demokracji i bezpieczeństwa gospodarczego Unii. Zarówno europejska strategia gotowości Unii[2], jak i europejska strategia bezpieczeństwa wewnętrznego (ProtectEU)[3] umieściły cyberbezpieczeństwo w centrum programu Unii na rzecz odporności. Podobnie w komunikacie w sprawie wzmocnienia bezpieczeństwa gospodarczego UE[4] jako priorytetowe cele wskazano zapobieganie dostępowi do informacji i danych wrażliwych, które mogłyby zagrozić bezpieczeństwu gospodarczemu Unii, oraz zapobieganie zakłóceniom w funkcjonowaniu infrastruktury krytycznej Unii mającym wpływ na gospodarkę Unii i łagodzenie takich zakłóceń, w czym kluczową rolę odgrywają skuteczne środki w zakresie cyberbezpieczeństwa. Ponadto w raporcie Draghiego podkreślono potrzebę zwiększenia bezpieczeństwa i zmniejszenia zależności jako jeden z głównych obszarów działania niezbędnych w Unii[5]. W komunikacie w sprawie prostszej i szybszej Europy[6]Komisja ogłosiła swoje zaangażowanie w ambitny program promowania przyszłościowych, innowacyjnych polityk, które wzmacniają konkurencyjność Unii i zmniejszają obciążenia regulacyjne dla obywateli, przedsiębiorstw i administracji, przy jednoczesnym utrzymaniu najwyższych standardów w promowaniu jej wartości.

W tym kontekście niniejszy wniosek dotyczący dyrektywy zmieniającej dyrektywę (UE) 2022/2555 w odniesieniu do środków upraszczających i dostosowania do [wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), europejskich ram certyfikacji cyberbezpieczeństwa oraz bezpieczeństwa łańcucha dostaw technologii informacyjno-komunikacyjnych oraz uchylającego rozporządzenie (UE) 2019/881 (ustawa o cyberbezpieczeństwie 2)] ma na celu rozwiązanie problemu złożoności i różnorodności polityk związanych z cyberbezpieczeństwem, które mają wpływ na pozycję Unii w zakresie cyberbezpieczeństwa, w szczególności poprzez wprowadzenie wyjaśnień i ułatwienie podmiotom podlegającym regulacjom przestrzegania przepisów.

Cel niniejszej dyrektywy należy rozpatrywać w kontekście nadrzędnych celów pakietu zmian do ustawy o cyberbezpieczeństwie, obejmującego wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), europejskich ram certyfikacji cyberbezpieczeństwa oraz bezpieczeństwa łańcucha dostaw technologii informacyjno-komunikacyjnych, a także uchylającego rozporządzenie (UE) 2019/881. Wniosek dotyczący tego rozporządzenia ma na celu rozwiązanie następujących problemów: (i) rozbieżność między ramami polityki Unii w zakresie cyberbezpieczeństwa a potrzebami zainteresowanych stron w coraz bardziej nieprzyjaznym środowisku zagrożeń; (ii) opóźnienia we wdrażaniu europejskich ram certyfikacji w zakresie cyberbezpieczeństwa (ECCF); (iii) złożoność i różnorodność

---

1 ENISA, ENISA Threat Landscape 2025.
2 JOIN/2025/130 wersja ostateczna.
3 COM/2025/148 wersja ostateczna.
4 JOIN(2025) 977 wersja ostateczna.
5 Komisja Europejska, Przyszłość europejskiej konkurencyjności, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.
6 COM(2025) 47 wersja ostateczna.

polityki związane z cyberbezpieczeństwem mające wpływ na pozycję cybernetyczną Unii; oraz (iv) rosnące zagrożenia dla bezpieczeństwa łańcuchów dostaw ICT. W odniesieniu do złożoności i różnorodności polityk związanych z cyberbezpieczeństwem, które mają wpływ na cyberposturę Unii, w pakiecie zmian do aktu o cyberbezpieczeństwie proponuje się – w ramach reformy europejskich ram certyfikacji cyberbezpieczeństwa – promowanie certyfikacji jako narzędzia zapewniania zgodności dla przedsiębiorstw oraz umożliwienie opracowania systemu dotyczącego cyberpostury podmiotów w celu zmniejszenia kosztów zapewnienia zgodności dla podmiotów podlegających dyrektywie NIS 2 i innym odpowiednim przepisom Unii w zakresie cyberbezpieczeństwa. Podejście to znacznie uprości obowiązki regulacyjne podmiotów podlegających wielu wymogom w zakresie zgodności i zapewni bardziej efektywne wykorzystanie zasobów przez organy krajowe.

W uzasadnieniu wniosku dotyczącego rozporządzenia w sprawie ustawy o cyberbezpieczeństwie 2 przedstawiono kluczowe kwestie leżące u podstaw wniosku, a także konkretne cele, które mają je rozwiązać. Wniosek dotyczący dyrektywy będzie dotyczył konkretnego celu 4 (SPO4) oceny skutków zmiany CSA, tj. ustanowienia mechanizmów i warunków ułatwiających zgodność z wymogami w zakresie cyberbezpieczeństwa, a tym samym zapewnienia bardziej spójnego i skutecznego wdrażania tych wymogów. Ukierunkowane zmiany do dyrektywy NIS 2 mają na celu uproszczenie zgodności z ramami cyberbezpieczeństwa oraz zapewnienie usprawnionego i spójnego wdrażania określonych aspektów tych ram, w tym w odniesieniu do zakresu, definicji, zgłaszania przypadków ransomware oraz nadzoru nad podmiotami świadczącymi usługi transgraniczne.

Wniosek dotyczący dyrektywy zmieniającej dyrektywę (UE) 2022/2555 w sprawie środków upraszczających i dostosowania do [ustawy o cyberbezpieczeństwie 2] wchodzi w zakres programu dostosowania i skuteczności regulacji (REFIT). Wraz z przeglądem ustawy o cyberbezpieczeństwie przyczynia się on w znacznym stopniu do poprawy przejrzystości, usunięcia nieefektywności i ujednolicenia procedur w różnych ramach prawnych. Przyczynia się on do prawidłowego funkcjonowania rynku wewnętrznego, zapewniając jednocześnie bezpieczeństwo i autonomię strategiczną Unii.

- **Spójność z istniejącymi przepisami w danej dziedzinie polityki**

Unia rozszerzyła swoje narzędzia prawne i polityczne poprzez przyjęcie szeregu instrumentów prawnych i środków politycznych: (i) dyrektywa NIS 2 służy wzmocnieniu cyberbezpieczeństwa infrastruktury krytycznej; (ii) środki bezpieczeństwa fizycznego są określone w jej „dyrektywie siostrzanej", dyrektywie w sprawie odporności podmiotów krytycznych (CER); (iii) ustawa o cyberodporności (CRA) zwiększa cyberbezpieczeństwo produktów; (iv) ustawa o cyber solidarności (CSoA) buduje zdolności reagowania w całej UE; (v) plan działania UE w zakresie cyberbezpieczeństwa[7] wspiera współpracę na szczeblu UE w zakresie zarządzania kryzysowego; (vi) zestaw narzędzi dotyczących cyberbezpieczeństwa 5G (5G Toolbox) wspiera cyberbezpieczeństwo w sieciach 5G; (vii) europejski plan działania w zakresie cyberbezpieczeństwa szpitali i podmiotów świadczących usługi opieki zdrowotnej[8] pomaga poprawić ich cyberbezpieczeństwo; oraz (viii) Akademia Umiejętności w zakresie Cyberbezpieczeństwa[9] zajmuje się rosnącym wyzwaniem, jakim jest niedobór talentów w dziedzinie cyberbezpieczeństwa.

Wyżej wymienione ramy prawne dotyczące cyberbezpieczeństwa zostały uzupełnione przepisami sektorowymi, tj. rozporządzeniem w sprawie odporności operacyjnej w sektorze cyfrowym (rozporządzenie DORA) dla sektora finansowego, kodeksem sieciowym dotyczącym przepisów sektorowych w zakresie cyberbezpieczeństwa w ruchu transgranicznym

[7] COM/2025/66 wersja ostateczna.
[8] COM(2025) 10 final.
[9] COM(2023) 207 wersja ostateczna.

przepływy energii elektrycznej (NCCS) dla podsektora energii elektrycznej, zasady bezpieczeństwa informacji (część IS[10]) dla podsektora transportu lotniczego.

Niniejszy wniosek dotyczący dyrektywy, podobnie jak towarzyszący mu wniosek dotyczący rozporządzenia, stanowi część szerszego zestawu inicjatyw prawnych i politycznych przyjętych przez Unię w celu poprawy odporności podmiotów na zagrożenia bezpieczeństwa i cyberzagrożenia. Skupia się on na ukierunkowanych zmianach w dyrektywie NIS 2, które mają na celu między innymi wyjaśnienie niektórych aspektów dotyczących zakresu, definicji i zasad jurysdykcji, zmniejszenie obciążenia związanego z nadzorem nad podmiotami o znaczeniu istotnym i ważnym oraz ułatwienie nadzoru nad podmiotami transgranicznymi poprzez wzmocnienie roli ENISA we wspieraniu współpracy operacyjnej. Ponadto, wraz z wnioskiem dotyczącym rozporządzenia, niniejszy wniosek tworzy silną synergię wynikającą z opracowania certyfikacji cyberbezpieczeństwa dla dyrektywy NIS 2, a także potencjalnie ułatwia zgodność z innymi odpowiednimi aktami prawnymi Unii, takimi jak ogólne rozporządzenie o ochronie danych (RODO), bez uszczerbku dla ich szczególnych wymogów certyfikacyjnych. Środki upraszczające powinny uwolnić zasoby w celu wzmocnienia operacyjnej gotowości podmiotów w sektorach krytycznych Unii w zakresie cyberbezpieczeństwa.

- **Spójność z innymi politykami Unii**

Niniejszy wniosek zaostrza wymogi bezpieczeństwa dla podmiotów świadczących usługi w zakresie portfeli biznesowych, określone we wniosku dotyczącym rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia europejskich portfeli biznesowych[11] . Ponadto Komisja zapewni spójność z przyszłymi inicjatywami, takimi jak ustawa o sieciach cyfrowych (DNA). Niniejszy wniosek jest zgodny z wnioskiem dotyczącym rozporządzenia w sprawie uproszczenia przepisów dotyczących cyfryzacji (Digital Omnibus), który zawiera między innymi zmiany do dyrektywy NIS 2 oraz innych aktów prawnych Unii. W Digital Omnibus proponuje się ułatwienie przestrzegania wymogów dotyczących zgłaszania incydentów związanych z cyberbezpieczeństwem, między innymi na mocy dyrektywy NIS 2, poprzez zgłaszanie za pośrednictwem jednego punktu kontaktowego do zgłaszania incydentów, który ma zostać opracowany i utrzymywany przez ENISA. Ponadto niniejszy wniosek jest zgodny z wnioskiem dotyczącym rozporządzenia Parlamentu Europejskiego i Rady w sprawie bezpieczeństwa, odporności i zrównoważonego rozwoju działań w przestrzeni kosmicznej w Unii[12] .

Ponadto wniosek jest zgodny z raportem Mario Draghiego „Przyszłość europejskiej konkurencyjności”, o którym mowa powyżej.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

Podstawą prawną niniejszej dyrektywy jest art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), którego celem jest ustanowienie i zapewnienie funkcjonowania rynku wewnętrznego poprzez wzmocnienie środków służących zbliżeniu przepisów krajowych. Niniejszy wniosek zmienia dyrektywę (UE) 2022/2555, która została przyjęta na podstawie art. 114 TFUE.

[10] Rozporządzenie wykonawcze Komisji (UE) 2023/203 i rozporządzenie delegowane Komisji (UE) 2022/1645.
[11] COM/2025/838 wersja ostateczna.
[12] COM/2025/335 wersja ostateczna.

- **Pomocniczość (w przypadku kompetencji niewyłącznych)**

Zasada pomocniczości wymaga oceny konieczności i wartości dodanej działania Unii. Zgodność z zasadą pomocniczości w tej dziedzinie została już uznana przy przyjmowaniu dyrektywy (UE) 2022/2555, którą zmienia niniejszy wniosek.

Niniejszy wniosek ułatwia przestrzeganie unijnych przepisów dotyczących cyberbezpieczeństwa, zmniejszając koszty związane z zapewnieniem zgodności i niepewność prawną dla zainteresowanych podmiotów oraz ułatwiając i poprawiając poziom zgodności z wymogami w zakresie cyberbezpieczeństwa. Przyczynia się on również do wyrównania szans w zakresie podejść do nadzoru i kontroli zgodności w państwach członkowskich.

- **Proporcjonalność**

Przepisy proponowane w niniejszej dyrektywie nie wykraczają poza to, co jest konieczne do osiągnięcia określonych celów w sposób zadowalający. Przewidywane ujednolicenie i usprawnienie zakresu, środków bezpieczeństwa i obowiązków sprawozdawczych wynika z wniosków państw członkowskich i przedsiębiorstw o poprawę obecnych ram.

- **Wybór instrumentu**

Wniosek zmieni obowiązującą dyrektywę NIS 2 i jeszcze bardziej uprości obowiązki nakładane na przedsiębiorstwa, zapewniając w ten sposób wyższy poziom harmonizacji w całej Unii. Wybór instrumentu prawnego dla niniejszego wniosku jest zgodny z wyborem instrumentu prawnego, który zmienia, tj. dyrektywą NIS 2. Niniejszy wniosek opiera się na celu dyrektywy NIS 2, jakim jest zapewnienie państwom członkowskim elastyczności niezbędnej do uwzględnienia specyfiki krajowej.

3. WYNIKI WYNIKÓW OCEN OCEN, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCENACH SKUTKÓW

- **Oceny ex post/kontrole adekwatności istniejących przepisów**

Zob. uzasadnienie [wniosku dotyczącego ustawy o cyberbezpieczeństwie 2].

- **Konsultacje z zainteresowanymi stronami**

Zob. uzasadnienie [wniosku dotyczącego ustawy o cyberbezpieczeństwie 2].

- **Gromadzenie i wykorzystanie wiedzy specjalistycznej**

Zob. uzasadnienie [wniosku dotyczącego ustawy o cyberbezpieczeństwie 2].

- **Ocena skutków**

Zob. uzasadnienie oraz sprawozdanie z oceny skutków towarzyszące [wnioskowi dotyczącemu ustawy o cyberbezpieczeństwie 2].

- **Adekwatność i uproszczenie regulacji**

Zob. uzasadnienie [wniosku dotyczącego ustawy o cyberbezpieczeństwie 2].

- **Prawa podstawowe**

Zob. uzasadnienie [wniosku dotyczącego ustawy o cyberbezpieczeństwie 2].

4. SKUTKI BUDŻETOWE

Proszę zapoznać się z oceną skutków regulacji i skutków finansowych zawartą w [wniosku dotyczącym ustawy o cyberbezpieczeństwie 2].

5. INNE ELEMENTY

- **Plany wdrożeniowe oraz ustalenia dotyczące monitorowania, oceny i sprawozdawczości**

Zgodnie z art. 40 dyrektywy NIS 2 Komisja dokona przeglądu funkcjonowania dyrektywy i co 36 miesięcy przedstawi sprawozdanie Parlamentowi Europejskiemu i Radzie.

- **Szczegółowe wyjaśnienie poszczególnych przepisów wniosku**

Wniosek ma na celu ułatwienie wypełniania obowiązków w zakresie cyberbezpieczeństwa oraz uwolnienie zasobów w celu wzmocnienia gotowości operacyjnej podmiotów w sektorach krytycznych Unii w zakresie cyberbezpieczeństwa.

Wniosek wprowadza ukierunkowane zmiany do dyrektywy NIS 2 w celu uproszczenia określonych aspektów ram cyberbezpieczeństwa, zwiększenia pewności prawnej i harmonizacji wdrażania.

Aby ułatwić podmiotom i dostawcom wykazanie zgodności z dyrektywą NIS 2, zgodnie z wnioskiem dotyczącym rozporządzenia, któremu towarzyszy niniejszy wniosek, podmioty podlegające dyrektywie NIS 2 będą mogły uzyskać certyfikaty w ramach systemów certyfikacji cyberbezpieczeństwa organizacji opracowanych w ramach ECCF.

Aby jeszcze bardziej ułatwić przestrzeganie środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa przez podmioty wielonarodowe podlegające nadzorowi właściwych organów z kilku państw członkowskich, ENISA otrzymała nowe zadanie wspierania państw członkowskich w nadzorowaniu tych podmiotów, ułatwianiu wzajemnej pomocy i tworzeniu lepszego przeglądu podmiotów objętych dyrektywą NIS 2.

Ponadto wniosek przewiduje, że Komisja przyjmie wytyczne dotyczące stosowania wymogów w zakresie bezpieczeństwa łańcucha dostaw, które podmioty objęte zakresem dyrektywy NIS 2 przekazują swoim dostawcom, aby zapewnić pewność prawną i zapobiec nieuzasadnionemu przenoszeniu obowiązków na podmioty nieobjęte zakresem dyrektywy NIS 2.

Inne ukierunkowane zmiany w dyrektywie NIS 2 obejmują:

- wyjaśnienia dotyczące zakresu stosowania i definicji;
- wyłączenie mikro- i małych dostawców usług DNS z zakresu stosowania;
- wprowadzenie maksymalnej harmonizacji aktów wykonawczych na mocy art. 21 ust. 5 (określających środki zarządzania ryzykiem w zakresie cyberbezpieczeństwa) w celu ułatwienia podmiotom przestrzegania przepisów, a organom nadzoru – sprawowania nadzoru;
- wprowadzenie nowej kategorii małych przedsiębiorstw o średniej kapitalizacji, zgodnie z zaleceniem Komisji z 2025 r. w sprawie definicji małych przedsiębiorstw o średniej kapitalizacji[18] ; podmioty kwalifikujące się jako małe przedsiębiorstwa o średniej kapitalizacji mają być wyznaczane jako podmioty ważne, co zmniejszy obciążenia związane z przestrzeganiem przepisów i nadzorem dla właściwych organów;
- wymóg przyjęcia przez państwa członkowskie polityki migracji do kryptografii postkwantowej (PQC) w ramach krajowej strategii w zakresie cyberbezpieczeństwa; oraz
- wprowadzenie zharmonizowanego gromadzenia danych dotyczących ataków ransomware.

2026/0012 (COD)

Wniosek dotyczący

DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY

zmieniająca dyrektywę (UE) 2022/2555 w odniesieniu do środków upraszczających i dostosowania do [wniosku dotyczącego aktu prawnego w sprawie cyberbezpieczeństwa 2]

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[1] ,

uwzględniając opinię Komitetu Regionów[2] ,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, a także mając na

uwadze, co następuje:

(1) W dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555[3] określono środki mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, z myślą o poprawie funkcjonowania rynku wewnętrznego. Od momentu wejścia w życie dyrektywy (UE) 2022/2555 poczyniono postępy w zwiększaniu poziomu cyberodporności Unii. Jednocześnie podczas wdrażania dyrektywy przez państwa członkowskie pojawiły się pewne wyzwania, m.in. w odniesieniu do zakresu dyrektywy, wdrażania obowiązków w zakresie zarządzania ryzykiem cyberbezpieczeństwa i zgłaszania incydentów oraz nadzoru nad podmiotami transgranicznymi. W oparciu o [wniosek dotyczący aktu w sprawie cyberbezpieczeństwa 2] należy wprowadzić ukierunkowane zmiany do dyrektywy (UE) 2022/2555, aby sprostać tym wyzwaniom, upraszczając określone aspekty w celu zwiększenia pewności prawnej i zapewnienia jednolitego wdrożenia dyrektywy (UE) 2022/2555.

(2) Aby zmniejszyć obciążenia związane z przestrzeganiem przepisów dla podmiotów i nadzorem dla właściwych organów, w dyrektywie (UE) 2022/2555 należy wprowadzić nową kategorię małych przedsiębiorstw o średniej kapitalizacji, zgodnie z zaleceniem Komisji (UE) 2025/1099[4]. Podmioty, o których mowa w załączniku I do dyrektywy (UE) 2022/2555,

---

1 Dz.U. C [...], [...], s. [...]

2 Dz.U. C [...], [...], s. [...]

3 Dyrektywa (UE) 2022/2555 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

4 Zalecenie Komisji (UE) 2025/1099 z dnia 21 maja 2025 r. w sprawie definicji małych przedsiębiorstw o średniej kapitalizacji (Dz.U. L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

które kwalifikują się jako małe przedsiębiorstwa o średniej kapitalizacji zgodnie z tym zaleceniem, powinny co do zasady być uznawane za podmioty istotne. Ponadto, aby wesprzeć cel Komisji polegający na obniżeniu kosztów administracyjnych o 25 % ogółem i o 35 % w przypadku małych i średnich przedsiębiorstw, należy stosować ogólną zasadę dotyczącą wielkości przedsiębiorstwa określoną w dyrektywie (UE) 2022/2555, zgodnie z którą wszystkie podmioty kwalifikujące się jako średnie przedsiębiorstwa zgodnie z art. 2 załącznika do zalecenia Komisji 2003/361/WE[5] lub przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu, wchodzą w zakres stosowania dyrektywy (UE) 2022/2555, powinna mieć zastosowanie do dostawców usług systemu nazw domenowych.

(3) Podczas wdrażania dyrektywy (UE) 2022/2555 pojawiły się trudności w interpretacji przepisów dotyczących jej zakresu. W związku z tym należy doprecyzować niektóre przepisy dotyczące zakresu stosowania odnoszące się do podmiotów świadczących usługi opieki zdrowotnej, producentów energii elektrycznej, przedsiębiorstw zajmujących się wodorem oraz podmiotów z sektora chemicznego, aby zapewnić pewność prawną i zmniejszyć obciążenia związane z przestrzeganiem przepisów zarówno dla podmiotów, jak i organów krajowych.

(4) W celu zapewnienia proporcjonalności w odniesieniu do producentów energii elektrycznej w rozumieniu art. 2 pkt 38 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/944[6] za podmioty istotne lub ważne w rozumieniu dyrektywy (UE) 2022/2555 należy uznawać wyłącznie tych producentów energii elektrycznej, których łączna moc wytwórcza przekracza 1 MW, pod warunkiem że spełniają oni wymóg dotyczący ograniczenia wielkości. Powinno to obejmować producentów energii elektrycznej, których pojedyncza elektrownia ma moc przekraczającą 1 MW, a także producentów energii elektrycznej, którzy eksploatują kilka elektrowni, których łączna moc wytwórcza przekracza 1 MW. Takie podejście pozwala na osiągnięcie równowagi między potrzebą uwzględnienia podmiotów, w przypadku których zakłócenie funkcjonowania ich sieci i systemu informatycznego mogłoby oznaczać utratę, brak kontroli lub zewnętrzną kontrolę mocy wytwórczej, co samo w sobie ma znaczenie dla bezpieczeństwa i stabilności sieci elektroenergetycznej, a potrzebą uniknięcia nakładania nieproporcjonalnych obciążeń administracyjnych na przedsiębiorstwa na mocy dyrektywy (UE) 2022/2555.

(5) Europejskie portfele tożsamości cyfrowej, przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014[7],stanowią istotny element infrastruktury cyfrowej Unii, umożliwiając bezpieczną identyfikację i uwierzytelnianie oraz wymianę dokumentów elektronicznych, w tym elektronicznych poświadczeń atrybutów. Biorąc pod uwagę ich kluczową rolę dla społeczeństwa oraz świadczenia usług publicznych i prywatnych, każdy incydent związany z cyberbezpieczeństwem mający wpływ na te portfele może mieć szerokie skutki. Aby zapewnić świadczenie swoich usług, dostawcy europejskich portfeli tożsamości cyfrowej powinni być zobowiązani do wdrożenia odpowiednich środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem związanym z cyberbezpieczeństwem, zapobiegania incydentom i reagowania na nie oraz współpracy z właściwymi organami zgodnie z dyrektywą (UE) 2022/2555. Powinni oni zatem zostać uwzględnieni wśród podmiotów objętych tą dyrektywą, niezależnie od ich wielkości, i zostać sklasyfikowani jako podmioty o znaczeniu krytycznym. Europejskie

---

5 Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

6 Dyrektywa (UE) 2019/944 z dnia 5 czerwca 2019 r. w sprawie wspólnych zasad rynku wewnętrznego energii elektrycznej i zmieniająca dyrektywę 2012/27/UE (Dz.U. L 158 z 14.6.2019, s. 125; ELI: http://data.europa.eu/eli/dir/2019/944/oj).

7 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

Portfele biznesowe oferują podobne funkcje i usługi dostosowane do potrzeb podmiotów gospodarczych i organów sektora publicznego, opierając się na unijnych ramach tożsamości cyfrowej, i mają równie kluczowe znaczenie dla bezpieczeństwa i integralności gospodarki cyfrowej. W związku z tym dostawcy europejskich portfeli biznesowych ustanowionych zgodnie z [wnioskiem dotyczącym rozporządzenia w sprawie ustanowienia europejskich portfeli biznesowych][8] powinni podlegać tym samym wymogom i obowiązkom w zakresie cyberbezpieczeństwa, co dostawcy europejskich portfeli tożsamości cyfrowej, aby zapewnić spójny i wysoki poziom bezpieczeństwa w całym ekosystemie tożsamości cyfrowej.

(6) Podmorska infrastruktura transmisji danych obejmuje nie tylko kable, ale także wszelką infrastrukturę związaną z ich eksploatacją. Infrastruktura ta obejmuje stacje lądowe i naziemne części kabli podmorskich łączących się z nimi, takie jak trasy lądowe od studzienki brzegowej do stacji lądowej, centrum danych lub punktu obecności. Podmorska infrastruktura transmisji danych jest zazwyczaj eksploatowana przez podmioty już objęte dyrektywą (UE) 2022/2555, w tym dostawców publicznych sieci i usług łączności elektronicznej lub dostawców usług przetwarzania w chmurze. Infrastruktura podmorska do transmisji danych może być jednak również eksploatowana przez inne rodzaje podmiotów, które obecnie nie są objęte zakresem dyrektywy (UE) 2022/2555, takie jak infrastruktura podmorska do transmisji danych eksploatowana przez dostawców sieci łączności elektronicznej, które nie są publiczne, lub przez podmioty, które wynajmują eksploatację infrastruktury podmorskiej do transmisji danych w całości lub w części dostawcom publicznych sieci łączności elektronicznej. Biorąc pod uwagę rosnące zagrożenia dla podmorskiej infrastruktury transmisji danych i wynikającą z nich wysoką krytyczność, konieczne jest zapewnienie, aby dyrektywa (UE) 2022/2555 obejmowała wszystkie rodzaje operatorów podmorskiej infrastruktury transmisji danych. Inne infrastruktury krytyczne o znaczeniu morskim, takie jak podmorskie kable elektryczne oraz gazociągi, rurociągi wodorowe i naftowe, są zazwyczaj już objęte dyrektywą (UE) 2022/2555, ponieważ są eksploatowane przez operatorów systemów przesyłowych w podsektorach energii elektrycznej, gazu, wodoru i ropy naftowej.

(7) Aby umożliwić podmiotom świadczącym usługi w kilku państwach członkowskich korzystanie z bardziej spójnych i mniej uciążliwych podejść nadzorczych na całym rynku wewnętrznym, podmioty te powinny mieć możliwość wykazania zgodności z określonymi lub wszystkimi obowiązkami w zakresie zarządzania ryzykiem cyberbezpieczeństwa określonymi w dyrektywie (UE) 2022/2555 poprzez uzyskanie certyfikatu dotyczącego stanu cyberbezpieczeństwa w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa. Opracowanie takiego systemu będzie korzystne dzięki przyjęciu aktów wykonawczych dotyczących wymagań technicznych i metodologicznych, a także sektorowych, odnoszących się do środków zarządzania ryzykiem cyberbezpieczeństwa na mocy dyrektywy (UE) 2022/2555, które opierają się na maksymalnej harmonizacji.

(8) Biorąc pod uwagę stale rosnącą zależność naszego społeczeństwa i gospodarki od technologii cyfrowych, konieczne jest podjęcie działań łagodzących zagrożenie kwantowe. Możliwość przeprowadzenia ataków typu „zbierz teraz – odszyfruj później”, które prawdopodobnie mają już miejsce, oraz przyszłe ryzyko związane z atakami kwantowymi na fałszowanie podpisów, a także planowane wycofanie niektórych implementacji algorytmów i całkowite zakazanie stosowania obecnych algorytmów kryptograficznych opartych na kluczu publicznym zwiększają pilność podjęcia działań na rzecz przejścia na kryptografię postkwantową (PQC). W związku z tym państwa członkowskie powinny być zobowiązane do przyjęcia polityki migracji do PQC w ramach krajowej strategii cyberbezpieczeństwa. Polityka ta powinna ułatwić przyspieszenie planowania strategicznego oraz stworzenie środków wsparcia i narzędzi służących do oceny narażenia

[8] COM(2025) 838 final

zasobów kryptograficznych na ryzyko związane z komputerami kwantowymi. Ponadto powinny one pomóc w opracowaniu planu migracji i przetestowaniu wdrożenia PQC w aplikacjach cyfrowych i sieciach, jednocześnie wspierając pojawienie się i upowszechnienie formalnie zweryfikowanych i ocenionych europejskich rozwiązań PQC zgodnych z ramami zgodności w produktach i usługach. Polityki te powinny być zgodne z kamieniami milowymi określonymi w aktach prawnych Unii i politykach Unii, a także w dokumentach przyjętych przez grupę ds. współpracy w zakresie bezpieczeństwa sieci i informacji, w szczególności w skoordynowanym planie działania dotyczącym przejścia na PQC, przyjętym przez grupę ds. współpracy w zakresie bezpieczeństwa sieci i informacji w czerwcu 2025 r., umożliwiając w ten sposób migrację do PQC do 2030 r. w przypadku krytycznych zastosowań oraz do 2035 r. w przypadku zastosowań średniego i niskiego poziomu.

(9) Zgodnie z art. 21 ust. 2 lit. d) dyrektywy (UE) 2022/2555 podmioty o znaczeniu kluczowym i istotnym mają obowiązek zapewnić odpowiedni poziom bezpieczeństwa w swoim łańcuchu dostaw. W praktyce obowiązek ten skłonił wiele podmiotów do żądania od swoich dostawców obszernych informacji za pomocą niejednolitych kwestionariuszy, formatów i procesów. Chociaż żądania takie mają na celu wspieranie należytej staranności i zarządzania ryzykiem, mogą one również stanowić znaczne obciążenie administracyjne dla dostawców podmiotów istotnych i ważnych, zwłaszcza gdy podobne informacje muszą być wielokrotnie dostarczane w różnych formach. Aby złagodzić to obciążenie i promować spójne, proporcjonalne i skuteczne podejście do oceny bezpieczeństwa łańcucha dostaw, Komisja powinna opracować wytyczne zalecające odpowiedni poziom szczegółowości, strukturę i format takich wniosków o udzielenie informacji. Wytyczne takie powinny ułatwić harmonizację, ograniczyć niepotrzebne powielanie działań oraz wspierać zarówno podmioty, jak i ich dostawców w skutecznym wypełnianiu obowiązków wynikających z dyrektywy (UE) 2022/2555.

(10) Ataki ransomware, w których złośliwe oprogramowanie szyfruje dane i systemy oraz żąda okupu za ich odblokowanie, pozostają jednym z głównych zagrożeń dla kluczowych i ważnych podmiotów. Harmonizacja i usprawnienie gromadzenia danych dotyczących ataków ransomware od poszkodowanych kluczowych i ważnych podmiotów zapewniłaby zespołom reagowania na incydenty związane z bezpieczeństwem komputerowym (CSIRT) i organom krajowym informacje umożliwiające im zapewnienie odpowiednich i skutecznych interwencji w przypadku przyszłych ataków ransomware, wspieranie podmiotów w zwiększaniu ich odporności i zapobieganiu przyszłym atakom oraz gromadzenie informacji wywiadowczych i dowodów potrzebnych organom ścigania do rozbicia i likwidacji gangów ransomware oraz ukarania ich członków. Ze względu na potencjalnie wrażliwy charakter informacji, które mają być udostępniane w odniesieniu do ataków ransomware, w szczególności dotyczących tego, czy podmiot zapłacił okup, a jeśli tak, to w jakiej wysokości i komu, informacje takie powinny być przekazywane wyłącznie zespołom CSIRT lub, w stosownych przypadkach, właściwym organom na ich wniosek. W celu wymiany takich informacji zachęca się podmioty o znaczeniu krytycznym i istotnym do wyznaczenia osoby pełniącej funkcję punktu kontaktowego i zapewniającej poufność i wiarygodność wymiany informacji. W kontekście międzynarodowej inicjatywy przeciwko oprogramowaniu ransomware Unia poparła niewiążące międzynarodowe oświadczenie polityczne, zgodnie z którym odpowiednie instytucje podlegające władzom uczestniczących rządów krajowych nie powinny płacić okupu za oprogramowanie ransomware.

(11) Wypełnienie obowiązku zgłaszania istotnych informacji o incydentach związanych z oprogramowaniem ransomware nie powinno skutkować nałożeniem dodatkowych obowiązków wynikających z dyrektywy (UE) 2022/2555, którym podmiot nie podlegałby, gdyby nie zgłosił tych informacji. W tym celu państwa członkowskie powinny, w granicach swojego krajowego porządku prawnego, zająć się ewentualnym ryzykiem wynikającym ze zwiększonej odpowiedzialności związanej ze zgłaszaniem istotnych informacji o incydentach związanych z oprogramowaniem ransomware.

(12) Biorąc pod uwagę transgraniczny wymiar wielu istotnych i ważnych podmiotów na rynku wewnętrznym oraz potrzebę zapewnienia spójności i promowania konwergencji i efektywności w odniesieniu do podejść nadzorczych, ENISA powinna wspierać państwa członkowskie w udzielaniu wzajemnej pomocy istotnym i ważnym podmiotom, które świadczą usługi w więcej niż jednym państwie członkowskim lub które świadczą usługi w jednym lub kilku państwach członkowskich, a ich sieci i systemy informatyczne znajdują się w jednym lub kilku innych państwach członkowskich. W tym celu państwa członkowskie powinny przedkładać dodatkowe informacje do rejestru podmiotów prowadzonego przez ENISA. Na podstawie informacji zawartych w rejestrze podmiotów o znaczeniu kluczowym i istotnym ENISA powinna przeprowadzić kompleksową analizę transgranicznych zagrożeń dla cyberbezpieczeństwa związanych z podmiotami o znaczeniu kluczowym i istotnym. Analiza ta powinna opierać się na metodologii opracowanej wspólnie z Komisją i grupą ds. współpracy w zakresie bezpieczeństwa sieci i informacji. Metodologia ta mogłaby uwzględniać stopień, w jakim podmioty istotne i ważne świadczą swoje usługi na szeroką skalę transgraniczną, polegają na usługach transgranicznych, są narażone na ryzyko koncentracji łańcucha dostaw, mogą być identyfikowane jako źródło ryzyka koncentracji łańcucha dostaw, są narażone na incydenty, które mogą mieć znaczący wpływ na zakłócenie usług transgranicznych, lub polegają na systemach sieciowych i informatycznych do świadczenia swoich usług, które znajdują się w różnych państwach członkowskich i poza Unią. Na podstawie sprawozdania z analizy ryzyka ENISA powinna zalecić właściwym organom powołanie wspólnych zespołów kontrolnych w celu wsparcia nadzoru nad podmiotami o wyższym stopniu ryzyka dla sprawnego funkcjonowania rynku wewnętrznego w przypadku incydentów oraz pomocy właściwym organom w wykonywaniu wspólnych działań nadzorczych na ich wniosek.

(13) Ponieważ cel niniejszej dyrektywy, a mianowicie uproszczenie wdrażania środków zapewniających wysoki wspólny poziom cyberbezpieczeństwa w całej Unii, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, ale ze względu na skutki działania może zostać lepiej osiągnięty na poziomie Unii, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(14) Skonsultowano się z Europejskim Inspektorem Ochrony Danych i Europejską Radą Ochrony Danych zgodnie z art. 42 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725[9] , które wydały wspólną opinię w dniu [data],

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

Artykuł 1
Zmiany w dyrektywie (UE) 2022/2555

W dyrektywie (UE) 2022/2555 wprowadza się następujące zmiany:

(1) W art. 2 wprowadza się następujące zmiany:

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy unijne, w związku z swobodnym przepływem takich danych oraz uchylające rozporządzenie (WE) nr 45/2001 oraz Decyzja nr 1247/2002/WE (Dz.U. L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(a) w ust. 2 lit. a) wprowadza się następujące zmiany:

(i) pkt (iii) otrzymuje brzmienie:

„(iii) „rejestry nazw domen najwyższego poziomu;”;

(ii) dodaje się lit. (iv) i (v) w brzmieniu:

„(iv) dostawcy europejskich portfeli tożsamości cyfrowej zgodnie z rozporządzeniem (UE) nr 910/2014;

(v) dostawcy europejskich portfeli biznesowych ustanowionych zgodnie z rozporządzeniem (UE) […]*.

_____

* „rozporządzenie (UE) […] [wniosek dotyczący rozporządzenia w sprawie ustanowienia europejskich portfeli biznesowych]”.

(b) dodaje się ust. 3a w brzmieniu:

„3a. Niezależnie od ich wielkości, niniejsza dyrektywa ma zastosowanie do podmiotów określonych jako właściciele, zarządcy i operatorzy strategicznej infrastruktury podwójnego zastosowania zgodnie z rozporządzeniem (UE) […]**.

_____

** „Rozporządzenie (UE) […] [Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram środków ułatwiających transport sprzętu wojskowego, towarów i personelu w całej Unii].”;

(2) W art. 3 wprowadza się następujące zmiany:

(a) ustęp 1 otrzymuje brzmienie:

(i) lit. a) i b) otrzymują brzmienie:

„a) podmioty typu określonego w załączniku I, które przekraczają pułapy dla małych przedsiębiorstw o średniej kapitalizacji;

„b) kwalifikowani dostawcy usług zaufania, dostawcy europejskich portfeli tożsamości cyfrowej, dostawcy europejskich portfeli biznesowych oraz rejestry nazw domen najwyższego poziomu, niezależnie od ich wielkości;”;

(ii) dodaje się lit. h) w brzmieniu:

„h) podmioty zidentyfikowane jako właściciele, zarządcy i operatorzy strategicznej infrastruktury podwójnego zastosowania zgodnie z rozporządzeniem (UE) […] [wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram środków ułatwiających transport sprzętu wojskowego, towarów i personelu w całej Unii];”.

(b) w ust. 4 akapit pierwszy otrzymuje brzmienie:

„W celu ustanowienia wykazu, o którym mowa w ust. 3, państwa członkowskie wymagają od podmiotów, o których mowa w tym ustępie, przedłożenia właściwym organom co najmniej następujących informacji:

(a) nazwę podmiotu;

(b) odpowiedni sektor, podsektor i rodzaj podmiotu, o których mowa w załączniku I lub II, w stosownych przypadkach;

(c) adres podmiotu lub, w stosownych przypadkach, adres głównego zakładu podmiotu i jego innych zakładów prawnych w Unii lub, jeżeli podmiot nie ma siedziby w Unii, adres przedstawiciela wyznaczonego zgodnie z art. 26 ust. 3;

(d) aktualne dane kontaktowe, w tym adresy e-mail, numery telefonów, niepowtarzalny identyfikator i adresy cyfrowe europejskiego portfela biznesowego podmiotu, w stosownych przypadkach, oraz jego przedstawiciela wyznaczonego zgodnie z art. 26 ust. 3, w stosownych przypadkach;

(e) państwa członkowskie, w których podmiot świadczy usługi;

(f) zakresy adresów IP podmiotu.

(3) Artykuł 5 otrzymuje brzmienie:

„Artykuł 5

Minimalna harmonizacja

Bez uszczerbku dla art. 21 ust. 5 akapit piąty, niniejsza dyrektywa nie wyklucza przyjęcia lub utrzymania przez państwa członkowskie przepisów zapewniających wyższy poziom cyberbezpieczeństwa, pod warunkiem że przepisy te są zgodne z obowiązkami państw członkowskich określonymi w prawie Unii.”;

(4) w art. 6

dodaje się pkt 42 i 43 w brzmieniu:

„(42) »małe przedsiębiorstwo o średniej kapitalizacji« oznacza małe przedsiębiorstwo o średniej kapitalizacji zgodnie z definicją zawartą w załączniku do zalecenia Komisji (UE) 2025/1099***;

(43) „podmorska infrastruktura transmisji danych” oznacza podmorskie kable służące do transmisji danych, powiązaną infrastrukturę oraz inne urządzenia lub elementy związane z transmisją danych.

*** Zalecenie Komisji (UE) 2025/1099 z dnia 21 maja 2025 r. w sprawie definicji małych przedsiębiorstw o średniej kapitalizacji (Dz.U. L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj)”.

(5) w art. 7 ust. 2 dodaje się lit. k) w brzmieniu:

„k) w odniesieniu do przejścia na kryptografię postkwantową, z uwzględnieniem harmonogramu przejścia i odpowiednich wymogów określonych w mających zastosowanie aktach prawnych i politykach Unii”.

(6) w art. 15 ust. 2 zdanie pierwsze otrzymuje brzmienie:

„Sieć CSIRT składa się z przedstawicieli zespołów CSIRT wyznaczonych lub ustanowionych zgodnie z art. 10, zespołu reagowania na incydenty komputerowe dla instytucji, organów i agencji Unii (CERT-EU) oraz ENISA.”;

(7) W art. 21 ust. 5 wprowadza się następujące zmiany:

(a) akapit drugi otrzymuje brzmienie:

„Komisja może przyjmować akty wykonawcze określające wymogi techniczne i metodologiczne, a także wymogi sektorowe, w razie potrzeby, dotyczące środków, o których mowa w ust. 2, w odniesieniu do istotnych i ważnych podmiotów innych niż te, o których mowa w akapicie pierwszym

niniejszego ustępu. Komisja regularnie ocenia, czy akty wykonawcze, o których mowa w niniejszym akapicie, powinny zostać przyjęte dla określonych sektorów lub rodzajów podmiotów w celu poprawy funkcjonowania rynku wewnętrznego. Przygotowując takie oceny, Komisja koncentruje się w szczególności na transgranicznym charakterze sektorów lub rodzajów podmiotów i przeprowadza otwarty, przejrzysty i integracyjny proces konsultacji z odpowiednimi zainteresowanymi stronami i państwami członkowskimi.”;

(b) dodaje się akapit piąty w brzmieniu:

„W przypadku gdy Komisja przyjmuje akty wykonawcze, o których mowa w akapicie pierwszym i drugim niniejszego ustępu, państwa członkowskie nie nakładają żadnych dodatkowych wymogów technicznych, metodologicznych lub sektorowych dotyczących środków, o których mowa w art. 21 ust. 2 dyrektywy (UE) 2022/2555, na podmioty objęte zakresem tych aktów wykonawczych.”;

(8) w art. 23 dodaje się ust. 12 i 13 w brzmieniu:

„12. Przyjmując akt wykonawczy zgodnie z ust. 11 akapit pierwszy, Komisja uwzględnia wymogi dotyczące przedkładania następujących informacji dotyczących ataków z użyciem oprogramowania ransomware zgodnie z ust. 1:

(a) czy podmiot wykrył atak ransomware;

(b) wektor ataku ransomware;

(c) czy wdrożono środki łagodzące.

13. Państwa członkowskie zapewniają, aby w przypadku znaczącego incydentu spowodowanego atakiem z użyciem oprogramowania ransomware zainteresowane podmioty informowały, na wniosek CSIRT lub, w stosownych przypadkach, właściwego organu, za pośrednictwem kanału komunikacyjnego zapewnionego przez CSIRT lub, w stosownych przypadkach, właściwy organ:

(a) czy podmiot otrzymał żądanie okupu i, w stosownych przypadkach, od kogo;

(b) czy okup został zapłacony, a jeśli tak, to w jakiej wysokości, za pomocą jakich środków płatniczych i na rzecz jakiego odbiorcy lub adresata, w tym dostawcy kryptowalut i usług związanych z kryptowalutami, w stosownych przypadkach.

(9) W art. 24 dodaje się ust. 4, 5 i 6 w brzmieniu:

„4. W celu wykazania zgodności z art. 21 państwa członkowskie mogą wymagać od podmiotów o znaczeniu kluczowym i istotnym uzyskania certyfikatu dotyczącego stanu cyberbezpieczeństwa w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa przyjętego zgodnie z art. 75 rozporządzenia (UE) XXX/XXX **** [wniosek dotyczący CSA2].

5. W przypadku gdy cyberbezpieczeństwo podmiotu istotnego lub ważnego jest certyfikowane w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa przyjętego zgodnie z art. 74 rozporządzenia (UE) XXX/XXX**** [wniosek dotyczący CSA2], a certyfikat wykazuje zgodność z wymogami określonymi w akcie wykonawczym przyjętym zgodnie z art. 21 ust. 5 niniejszej dyrektywy lub w prawie krajowym transponującym art. 21 ust. 1 i 2 niniejszej dyrektywy, właściwe organy nie nakładają na podmiot dodatkowych środków zgodnie z art. 32 ust. 2 lit. b) lub art. 33 ust. 2 lit. b), stosownie do wymogów objętych certyfikatem.

6. Certyfikacja zgodnie z ust. 4 nie ma wpływu na obowiązek przestrzegania niniejszej dyrektywy przez podmiot o znaczeniu zasadniczym lub istotnym.

**** Rozporządzenie (UE) XXX/XXX [Wniosek dotyczący CSA2]";

(10) W art. 26 wprowadza się następujące zmiany:

(a) w ust. 1 dodaje się lit. d) w brzmieniu:

„d) przewoźnicy lotniczy, którzy są uznawani za podlegających jurysdykcji państwa członkowskiego, którego właściwy organ wydający koncesje udzielił podmiotowi koncesji zgodnie z rozporządzeniem (WE) nr 1008/2008 Parlamentu Europejskiego i Rady*****, lub, jeżeli koncesja lub jej odpowiednik nie zostały udzielone zgodnie z tym rozporządzeniem, uznaje się je za podlegające jurysdykcji państwa członkowskiego, w którym mają swoją główną siedzibę w Unii zgodnie z ust. 2.

***** Rozporządzenie (WE) nr 1008/2008 Parlamentu Europejskiego i Rady z dnia 24 września 2008 r. w sprawie wspólnych zasad wykonywania przewozów lotniczych na terenie Wspólnoty (wersja przekształcona) (Dz.U. L 293 z 31.10.2008, s. 3, ELI: http://data.europa.eu/eli/reg/2008/1008/oj)".

(b) ustęp 3 otrzymuje brzmienie:

„3. Jeżeli podmiot o zasadniczym lub istotnym znaczeniu nie ma siedziby w Unii, ale świadczy usługi na jej terytorium, wyznacza on przedstawiciela w Unii. Przedstawiciel ma siedzibę w jednym z państw członkowskich, w których świadczone są usługi. Uznaje się, że taki podmiot podlega jurysdykcji państwa członkowskiego, w którym ma siedzibę przedstawiciel. Jeżeli podmiot taki jest podmiotem, o którym mowa w ust. 1 lit. a), uznaje się go za podlegający jurysdykcji państwa członkowskiego, w którym świadczy swoje usługi. W przypadku braku przedstawiciela w Unii wyznaczonego zgodnie z niniejszym ustępem każde państwo członkowskie, w którym podmiot świadczy usługi, może podjąć działania prawne przeciwko temu podmiotowi z tytułu naruszenia niniejszej dyrektywy".

(11) W art. 27 wprowadza się następujące zmiany:

(a) ustęp 1 otrzymuje brzmienie:

„1. ENISA tworzy i prowadzi rejestr podmiotów o znaczeniu podstawowym i istotnym, a także podmiotów świadczących usługi rejestracji nazw domen, na podstawie informacji otrzymanych od pojedynczych punktów kontaktowych zgodnie z ust. 4. Na wniosek ENISA umożliwia właściwym organom dostęp do informacji dotyczących dostawców usług DNS, rejestrów nazw TLD, podmiotów świadczących usługi rejestracji nazw domen, dostawców usług przetwarzania w chmurze, dostawców usług centrów danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, a także dostawców platform handlu internetowego, wyszukiwarek internetowych i platform usług społecznościowych oraz przewoźników lotniczych, przechowywanych w tym rejestrze, zapewniając jednocześnie ochronę poufności informacji, w stosownych przypadkach".

(b) ustęp 2 skreśla się;

(c) ustępy 3, 4 i 5 otrzymują brzmienie:

„3. Państwa członkowskie zapewniają, aby podmioty o znaczeniu istotnym i ważnym niezwłocznie, a w każdym razie w ciągu dwóch tygodni od daty zmiany, powiadamiały właściwy organ o wszelkich zmianach w informacjach przekazanych zgodnie z art. 3 ust. 4.

4. Po otrzymaniu informacji, o których mowa w art. 3 ust. 4, pojedynczy punkt kontaktowy zainteresowanego państwa członkowskiego niezwłocznie przekazuje je ENISA.

5. W stosownych przypadkach informacje, o których mowa w art. 3 ust. 4 akapit pierwszy, przekazuje się za pośrednictwem krajowego mechanizmu, o którym mowa w art. 3 ust. 4 akapit czwarty.

(12) dodaje się art. 37a w brzmieniu:

„Artykuł 37a

Rola ENISA w zakresie wzajemnej pomocy

1. ENISA wspiera państwa członkowskie w udzielaniu wzajemnej pomocy w rozumieniu art. 37 oraz pomaga w ułatwianiu takich procesów współpracy w odniesieniu do istotnych i ważnych podmiotów, które świadczą usługi w więcej niż jednym państwie członkowskim lub które świadczą usługi w jednym lub kilku państwach członkowskich, a ich sieci i systemy informatyczne znajdują się w jednym lub kilku innych państwach członkowskich.

2. Do celów określonych w ust. 1, do dnia … [15 miesięcy po wejściu w życie niniejszego rozporządzenia] ENISA przeprowadza kompleksową analizę transgranicznych zagrożeń dla cyberbezpieczeństwa związanych z istotnymi i ważnymi podmiotami, które świadczą usługi w więcej niż jednym państwie członkowskim lub które świadczą usługi w jednym lub kilku państwach członkowskich, a ich sieci i systemy informatyczne znajdują się w jednym lub kilku innych państwach członkowskich. W analizie tej ocenia się zakres możliwych skutków transgranicznych i skutków dla rynku wewnętrznego incydentów mających wpływ na takie istotne i ważne podmioty. Do celów tej analizy ENISA we współpracy z Komisją i grupą ds. współpracy opracowuje metodologię. Na podstawie tej analizy ENISA sporządza kompleksowe sprawozdanie z oceny transgranicznego ryzyka w zakresie cyberbezpieczeństwa, które jest aktualizowane co roku.

3. Na podstawie kompleksowego sprawozdania z oceny transgranicznego ryzyka w zakresie cyberbezpieczeństwa ENISA:

(a) w stosownych przypadkach zaleca właściwym organom powołanie wspólnych zespołów kontrolnych w celu wsparcia nadzoru nad określonymi podmiotami;

(b) opracowuje wytyczne dotyczące wspólnych działań nadzorczych;

(c) na wniosek właściwych organów zainteresowanych państw członkowskich ustanowi praktyczne ustalenia dotyczące wykonywania wspólnych działań nadzorczych;

(d) na wniosek właściwych organów zainteresowanych państw członkowskich oraz w zależności od dostępnych zasobów i proporcjonalnie do tych zasobów, uczestniczy we wspólnych działaniach nadzorczych;

(e) na wniosek właściwych organów zainteresowanych państw członkowskich pomagać w ocenie poziomu wdrożenia przez podmioty o znaczeniu istotnym lub ważnym środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa określonych w art. 21.

4. Do celów ust. 3 lit. e) niniejszego artykułu właściwe organy zainteresowanych państw członkowskich przekazują ENISA, o ile są one dostępne, wykaz środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa podjętych przez podmiot o znaczeniu kluczowym lub istotnym zgodnie z art. 21, wykaz podjętych działań nadzorczych lub egzekucyjnych, a także odpowiednią dokumentację, w tym dowody wdrożenia polityki w zakresie cyberbezpieczeństwa, takie jak wyniki audytów bezpieczeństwa, które właściwe organy przeprowadziły zgodnie z art. 32 i 33 w odniesieniu do tego podmiotu.

5. W przypadku gdy państwo członkowskie otrzymuje wzajemną pomoc, o której mowa w art. 37 ust. 1 akapit pierwszy lit. c), pojedynczy punkt kontaktowy informuje ENISA o udzieleniu wzajemnej pomocy. W stosownych przypadkach pojedynczy punkt kontaktowy podaje, który transgraniczny incydent, o którym mowa w art. 23 ust. 6, był związany ze sprawą wzajemnej pomocy.

(13) Załączniki I i II zmienia się zgodnie z załącznikiem do niniejszej dyrektywy.

Artykuł 2
Transpozycja

1. Do dnia … [12 miesięcy od wejścia w życie niniejszej dyrektywy] państwa członkowskie przyjmują i publikują środki niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie informują o tym Komisję.

   Państwa członkowskie stosują te środki od dnia … [dzień po dacie, o której mowa w akapicie pierwszym].

2. Środki przyjęte przez państwa członkowskie zgodnie z ust. 1 zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.

Artykuł 3
Wejście w życie

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 4
Adresaci

Niniejsza dyrektywa skierowana jest do państw

członkowskich. Sporządzono w Strasburgu, dnia

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*
[...]	*[...]*