KOMISJA
EUROPEJSKA

Strasburg, dnia 20.1.2026 r.
COM(2026) 13 final

2026/0012 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

zmieniająca dyrektywę (UE) 2022/2555 w zakresie środków upraszczających i dostosowania do [wniosku dotyczącego aktu o cyberbezpieczeństwie 2]

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

(Tekst mający znaczenie dla EOG)

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Niniejszy wniosek jest częścią pakietu środków mających na celu dostosowanie unijnych ram w zakresie cyberbezpieczeństwa do potrzeb zainteresowanych stron w coraz bardziej złożonym krajobrazie cyberzagrożeń i złożonej rzeczywistości geopolitycznej. Podmioty kluczowe i ważne z sektorów krytycznych coraz częściej stają się celem cyberataków[1], a podmioty państwowe stwarzające zagrożenie wykorzystują powstające technologie, takie jak sztuczna inteligencja (AI), aby jeszcze bardziej zwiększać skalę swoich ataków i je optymalizować. W tym kontekście odporność infrastruktury krytycznej na cyberzagrożenia uznaje się za strategiczny filar naszych demokracji i bezpieczeństwa gospodarczego Unii. Zarówno europejska strategia na rzecz unii gotowości[2], jak i europejska strategia bezpieczeństwa wewnętrznego (ProtectEU)[3] sprawiły, że kwestia cyberbezpieczeństwa znalazła się w centrum unijnego programu na rzecz odporności. Podobnie w komunikacie w sprawie wzmocnienia bezpieczeństwa gospodarczego UE[4] za cele priorytetowe uznano uniemożliwienie dostępu do informacji i danych szczególnie chronionych, który mógłby zagrozić bezpieczeństwu gospodarczemu UE, a także zapobieganie zakłóceniom w funkcjonowaniu unijnej infrastruktury krytycznej mającym wpływ na gospodarkę Unii i łagodzenie tych zakłóceń; w przypadku tych celów kluczową rolę odgrywają skuteczne środki w zakresie cyberbezpieczeństwa. Ponadto w raporcie Draghiego podkreślono potrzebę zwiększenia bezpieczeństwa i zmniejszenia zależności jako jednego z głównych obszarów działania niezbędnych w Unii[5]. W komunikacie „Prostsza i szybsza Europa”[6] Komisja ogłosiła swoje zobowiązanie do realizacji ambitnego programu na rzecz promowania przyszłościowych, innowacyjnych polityk, które wzmacniają konkurencyjność Unii i zmniejszają obciążenia regulacyjne dla obywateli, przedsiębiorstw i administracji, przy jednoczesnym zachowaniu najwyższych standardów w promowaniu jej wartości.

W tym kontekście niniejszy wniosek dotyczący dyrektywy zmieniającej dyrektywę (UE) 2022/2555 w zakresie środków upraszczających i dostosowania do [wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), europejskich ram certyfikacji cyberbezpieczeństwa i bezpieczeństwa łańcucha dostaw ICT oraz uchylenia rozporządzenia (UE) 2019/881 (akt o cyberbezpieczeństwie 2)] ma na celu rozwiązanie problemu złożoności i różnorodności polityk związanych z cyberbezpieczeństwem, które to złożoność i różnorodność mają wpływ na stan cyberbezpieczeństwa w Unii, w szczególności przez wprowadzenie sprecyzowań oraz ułatwienie podmiotom objętym regulacją przestrzegania przepisów.

Cel niniejszej dyrektywy należy uznać za część nadrzędnych celów pakietu zmian aktu o cyberbezpieczeństwie, obejmującego wniosek dotyczący rozporządzenia Parlamentu

---

1 ENISA, „ENISA Threat Landscape 2025” [Sprawozdanie ENISA dotyczące krajobrazu zagrożeń z 2025 r.].
2 JOIN(2025) 130 final.
3 COM(2025) 148 final.
4 JOIN(2025) 977 final.
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 final.

Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), europejskich ram certyfikacji cyberbezpieczeństwa i bezpieczeństwa łańcucha dostaw ICT oraz uchylenia rozporządzenia (UE) 2019/881. Wniosek dotyczący tego rozporządzenia ma na celu uwzględnienie następujących problemów: (i) rozbieżność między unijnymi ramami polityki w zakresie cyberbezpieczeństwa a potrzebami zainteresowanych stron w coraz bardziej nieprzyjaznym krajobrazie zagrożeń; (ii) wstrzymanie wdrażania europejskich ram certyfikacji cyberbezpieczeństwa (ECCF); (iii) złożoność i różnorodność polityk związanych z cyberbezpieczeństwem mające wpływ na stan cyberbezpieczeństwa w Unii oraz (iv) zwiększenie ryzyka związanego z bezpieczeństwem łańcuchów dostaw ICT. Jeżeli chodzi o złożoność i różnorodność polityk związanych z cyberbezpieczeństwem mające wpływ na stan cyberbezpieczeństwa w Unii, w pakiecie zmian aktu o cyberbezpieczeństwie proponuje się – w ramach reformy europejskich ram certyfikacji cyberbezpieczeństwa – promowanie certyfikacji jako narzędzia zapewniania zgodności dla przedsiębiorstw oraz umożliwienie opracowania programu dotyczącego stanu cyberbezpieczeństwa podmiotów w celu zmniejszenia kosztów zapewnienia zgodności z przepisami ponoszonych przez podmioty podlegające dyrektywie NIS 2 i innym odpowiednim unijnym przepisom dotyczącym cyberbezpieczeństwa. Podejście to znacznie uprości obowiązki regulacyjne podmiotów podlegających wielu wymogom dotyczącym zgodności i zapewni skuteczniejsze wykorzystanie zasobów przez organy krajowe.

W uzasadnieniu wniosku dotyczącego rozporządzenia w sprawie aktu o cyberbezpieczeństwie 2 przedstawiono kluczowe kwestie leżące u podstaw wniosku, a także szczegółowe cele dotyczące ich uwzględnienia. Wniosek dotyczący dyrektywy będzie dotyczył celu szczegółowego nr 4 (CS4) oceny skutków dotyczącej zmiany aktu o cyberbezpieczeństwie, tj. ustanowienia mechanizmów i warunków ułatwiających zapewnienie zgodności z wymogami w zakresie cyberbezpieczeństwa, a tym samym zwiększenie spójności i skuteczności ich wdrażania. Ukierunkowane zmiany w dyrektywie NIS 2 mają na celu uproszczenie przestrzegania określonych aspektów ram w zakresie cyberbezpieczeństwa oraz zapewnienie ich sprawnego i spójnego wdrażania, w tym w odniesieniu do zakresu, definicji, zgłaszania ataków z użyciem oprogramowania szantażującego, a także nadzoru nad podmiotami świadczącymi usługi transgraniczne.

Wniosek dotyczący dyrektywy zmieniającej dyrektywę (UE) 2022/2555 w zakresie środków upraszczających i dostosowania do [aktu o cyberbezpieczeństwie 2] wchodzi w zakres programu sprawności i wydajności regulacyjnej (REFIT). Wraz ze zmianą aktu o cyberbezpieczeństwie w znacznym stopniu przyczynia się on do poprawy jasności, usunięcia nieefektywności i dostosowania procedur w różnych ramach prawnych. Przyczynia się on do właściwego funkcjonowania rynku wewnętrznego przy jednoczesnym zapewnieniu bezpieczeństwa i autonomii strategicznej Unii.

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Unia rozszerzyła zestaw swoich narzędzi prawnych i politycznych przez przyjęcie szeregu instrumentów prawnych i środków z zakresu polityki: (i) dyrektywa NIS 2 służy wzmocnieniu cyberbezpieczeństwa infrastruktury krytycznej; (ii) środki bezpieczeństwa fizycznego zdefiniowano w „dyrektywie siostrzanej”, tj. dyrektywie w sprawie odporności podmiotów krytycznych (dyrektywa CER); (iii) akt o cyberodporności zwiększa cyberbezpieczeństwo produktów; (iv) akt w sprawie cybersolidarności umożliwia budowanie ogólnounijnych zdolności reagowania; (v) Plan działania UE na rzecz zarządzania

cyberkryzysami[7] wspiera współpracę w zakresie zarządzania kryzysowego na szczeblu UE; (vi) unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G wspiera cyberbezpieczeństwo w sieciach 5G; (vii) europejski plan działania w sprawie cyberbezpieczeństwa szpitali i świadczeniodawców[8] przyczynia się do poprawy ich stanu cyberbezpieczeństwa oraz (viii) Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa[9] umożliwia sprostanie rosnącemu wyzwaniu, jakim jest niedobór talentów w dziedzinie cyberbezpieczeństwa.

Określone wyżej ramy prawne w zakresie cyberbezpieczeństwa uzupełniono przepisami sektorowymi, tj. aktem w sprawie operacyjnej odporności cyfrowej sektora finansowego (rozporządzenie DORA), kodeksem sieci dotyczącym zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej w podsektorze energii elektrycznej oraz przepisami dotyczącymi bezpieczeństwa informacji (część IS[10]) w podsektorze transportu lotniczego.

Niniejszy wniosek dotyczący dyrektywy, podobnie jak wniosek dotyczący rozporządzenia, któremu towarzyszy, stanowi część szerszego zestawu inicjatyw prawnych i politycznych przyjętych przez Unię w celu zwiększenia odporności podmiotów na zagrożenia bezpieczeństwa i cyberzagrożenia. Dotyczy on w szczególności ukierunkowanych zmian dyrektywy NIS 2, które mają na celu m.in. doprecyzowanie niektórych aspektów odnoszących się do zakresu stosowania, definicji i zasad dotyczących jurysdykcji, zmniejszenie obciążenia związanego z nadzorem nad podmiotami kluczowymi i ważnymi oraz ułatwienie nadzoru nad podmiotami transgranicznymi przez zwiększenie roli ENISA we wspieraniu współpracy operacyjnej. Ponadto wraz z wnioskiem dotyczącym rozporządzenia niniejszy wniosek prowadzi do osiągnięcia znacznej synergii wynikającej z opracowania certyfikacji stanu cyberbezpieczeństwa na potrzeby dyrektywy NIS 2, a także potencjalnie może ułatwiać przestrzeganie innych odpowiednich aktów prawnych Unii, takich jak ogólne rozporządzenie o ochronie danych (RODO), bez uszczerbku dla zawartych w nich szczególnych wymogów w zakresie certyfikacji. Te środki upraszczające powinny przyczynić się do uwolnienia zasobów w celu zwiększenia gotowości operacyjnej podmiotów w sektorach krytycznych Unii do reagowania w obszarze cyberbezpieczeństwa.

- **Spójność z innymi politykami Unii**

W niniejszym wniosku zaostrza się wymogi w zakresie bezpieczeństwa dla podmiotów udostępniających portfele biznesowe, jak określono we wniosku dotyczącym rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia europejskich portfeli biznesowych[11]. Ponadto Komisja zapewni spójność z przyszłymi inicjatywami, takimi jak akt w sprawie sieci cyfrowych (DNA). Niniejszy wniosek jest zgodny z wnioskiem dotyczącym rozporządzenia w sprawie uproszczenia przepisów cyfrowych (akt zbiorczy prawa cyfrowego), który zawiera m.in. zmiany w dyrektywie NIS 2 oraz w innych aktach prawnych Unii. W akcie zbiorczym prawa cyfrowego proponuje się ułatwienie przestrzegania

[7] COM(2025) 66 final.
[8] COM(2025) 10 final.
[9] COM(2023) 207 final.
[10] Rozporządzenie wykonawcze Komisji (UE) 2023/203 i rozporządzenie delegowane Komisji (UE) 2022/1645.
[11] COM(2025) 838 final.

wymogów dotyczących zgłaszania związanych z cyberbezpieczeństwem, m.in. na podstawie dyrektywy NIS 2, przez zgłaszanie za pośrednictwem pojedynczego punktu kontaktowego do celów zgłaszania incydentów, który ma być opracowany i prowadzony przez ENISA. Wniosek ten jest również zgodny z wnioskiem dotyczącym rozporządzenia Parlamentu Europejskiego i Rady w sprawie bezpieczeństwa, odporności i zrównoważonego charakteru działań kosmicznych prowadzonych w Unii[12].

Ponadto wniosek jest zgodny z raportem Draghiego na temat przyszłości europejskiej konkurencyjności, o którym mowa powyżej.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawę prawną niniejszej dyrektywy stanowi art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), którego celem jest ustanowienie i zapewnienie funkcjonowania rynku wewnętrznego przez usprawnienie środków służących zbliżeniu przepisów krajowych. Niniejszy wniosek zmienia dyrektywę (UE) 2022/2555, którą przyjęto na podstawie art. 114 TFUE.

• Pomocniczość (w przypadku kompetencji niewyłącznych)

Zasada pomocniczości wymaga oceny konieczności podjęcia działań przez Unię i ich wartości dodanej. Kwestię zgodności z zasadą pomocniczości w tej dziedzinie uznano już przy przyjmowaniu dyrektywy (UE) 2022/2555, którą zmienia niniejszy wniosek.

Niniejszy wniosek ułatwia zapewnienie zgodności z unijnymi przepisami dotyczącymi cyberbezpieczeństwa i przyczynia się do zmniejszenia kosztów zapewnienia zgodności z przepisami oraz niepewności prawa dla zainteresowanych podmiotów, a także ułatwia utrzymanie i poprawę poziomu zgodności z wymogami w zakresie cyberbezpieczeństwa. Przyczynia się on również do zbliżenia podejść do nadzoru i kontroli zgodności we wszystkich państwach członkowskich.

• Proporcjonalność

Przepisy proponowane w niniejszej dyrektywie nie wykraczają poza zakres niezbędny do osiągnięcia określonych celów w zadowalający sposób. Przewidziane dostosowanie i uproszczenie przepisów w odniesieniu do zakresu, środków bezpieczeństwa i obowiązków w zakresie zgłaszania incydentów jest związane z wnioskami państw członkowskich i przedsiębiorstw o udoskonalenie obowiązujących ram.

• Wybór instrumentu

Wniosek zmieni obowiązującą dyrektywę NIS 2 i jeszcze bardziej uprości obowiązki nałożone na przedsiębiorstwa, a tym samym zapewni wyższy poziom harmonizacji w całej Unii. Wybór instrumentu prawnego na potrzeby niniejszego wniosku jest spójny z tekstem prawnym, który ma zostać zmieniony, tj. dyrektywą NIS 2. Niniejszy wniosek opiera się na celu dyrektywy NIS 2, jakim jest zapewnienie państwom członkowskim elastyczności niezbędnej do uwzględnienia specyfiki krajowej.

[12] COM(2025) 335 final.

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- **Oceny *ex post*/oceny adekwatności obowiązującego prawodawstwa**

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

- **Konsultacje z zainteresowanymi stronami**

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

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

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

- **Ocena skutków**

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

- **Sprawność regulacyjna i uproszczenie**

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

- **Prawa podstawowe**

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

4. WPŁYW NA BUDŻET

Zob. ocena skutków finansowych regulacji zawarta we [wniosku dotyczącym aktu o cyberbezpieczeństwie 2].

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Zgodnie z art. 40 dyrektywy NIS 2 Komisja będzie dokonywać przeglądu funkcjonowania dyrektywy i co 36 miesięcy składać sprawozdanie Parlamentowi Europejskiemu i Radzie.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Wniosek ma na celu ułatwienie wypełniania obowiązków w zakresie cyberbezpieczeństwa i uwolnienie zasobów w celu zwiększenia gotowości operacyjnej podmiotów w sektorach krytycznych Unii do reagowania w obszarze cyberbezpieczeństwa.

Wnioskiem wprowadza się ukierunkowane zmiany do dyrektywy NIS 2, aby uprościć konkretne aspekty ram w zakresie cyberbezpieczeństwa, zwiększyć pewność prawa i zharmonizować wdrażanie.

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

Aby jeszcze bardziej ułatwić przestrzeganie środków zarządzania ryzykiem w cyberbezpieczeństwie przez podmioty międzynarodowe podlegające nadzorowi właściwych organów z kilku państw członkowskich, ENISA powierzono nową rolę polegającą na wspieraniu państw członkowskich w nadzorowaniu tych podmiotów,

ułatwianiu wzajemnej pomocy i tworzeniu lepszych analiz podmiotów objętych zakresem dyrektywy NIS 2.

Ponadto we wniosku przewidziano, że Komisja przyjmie wytyczne dotyczące stosowania wymogów w zakresie bezpieczeństwa łańcucha dostaw, które podmioty objęte zakresem dyrektywy NIS 2 przenoszą na swoich dostawców, aby zagwarantować pewność prawa i zapobiec nadmiernemu przenoszeniu obowiązków na podmioty nieobjęte zakresem dyrektywy NIS 2.

Inne ukierunkowane zmiany w dyrektywie NIS 2 obejmują:

- doprecyzowanie zakresu i definicji;
- usunięcie z zakresu stosowania mikro- i małych dostawców usług DNS;
- wprowadzenie maksymalnej harmonizacji aktów wykonawczych na podstawie art. 21 ust. 5 (określających środki zarządzania ryzykiem w cyberbezpieczeństwie) w celu ułatwienia podmiotom przestrzegania przepisów oraz ułatwienia organom sprawowania nadzoru;
- wprowadzenie nowej kategorii małych spółek o średniej kapitalizacji, zgodnie z zaleceniem Komisji z 2025 r. dotyczącym definicji małych spółek o średniej kapitalizacji[18]; podmioty kwalifikujące się jako małe spółki o średniej kapitalizacji mają zostać wyznaczone jako podmioty ważne, co zmniejszy ich obciążenie regulacyjne oraz obciążenie właściwych organów związane ze sprawowaniem nadzoru;
- wymóg przyjęcia przez państwa członkowskie polityki przejścia na kryptografię postkwantową w ramach ich krajowej strategii cyberbezpieczeństwa oraz
- wprowadzenie zharmonizowanego gromadzenia danych na temat ataków z użyciem oprogramowania szantażującego.

2026/0012 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

zmieniająca dyrektywę (UE) 2022/2555 w zakresie środków upraszczających i dostosowania do [wniosku dotyczącego aktu o cyberbezpieczeństwie 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) Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555[3] ustanowiono środki mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego. Od momentu wejścia w życie dyrektywy (UE) 2022/2555 poczyniono postępy w podnoszeniu poziomu cyberodporności Unii. Jednocześnie w trakcie wdrażania dyrektywy przez państwa członkowskie pojawiły się pewne wyzwania, w tym w odniesieniu do zakresu jej stosowania, wdrażania obowiązków w zakresie zarządzania ryzykiem w cyberbezpieczeństwie i obowiązku zgłaszania incydentów oraz nadzoru nad podmiotami transgranicznymi. W oparciu o [wniosek dotyczący aktu o cyberbezpieczeństwie 2] należy wprowadzić ukierunkowane zmiany w dyrektywie (UE) 2022/2555, aby sprostać tym wyzwaniom, przez uproszczenie określonych aspektów, tak aby zwiększyć pewność prawa i zapewnić jednolite wdrażanie dyrektywy (UE) 2022/2555.

(2) Aby zmniejszyć obciążenie regulacyjne podmiotów oraz obciążenie właściwych organów związane ze sprawowaniem nadzoru, w dyrektywie (UE) 2022/2555 należy wprowadzić nową kategorię małych spółek o średniej kapitalizacji, zgodnie

[1] Dz.U. C [...], [...], s. [...].
[2] Dz.U. C [...], [...], s. [...].
[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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

z zaleceniem Komisji (UE) 2025/1099[4]. Podmioty w rodzaju tych, o których mowa w załączniku I do dyrektywy (UE) 2022/2555, które kwalifikują się jako małe spółki o średniej kapitalizacji na podstawie tego zalecenia, należy co do zasady wyznaczyć jako podmioty ważne. Ponadto aby wesprzeć realizację celu Komisji, jakim jest zmniejszenie kosztów administracyjnych ogółem o 25 % oraz o 35 % w przypadku małych i średnich przedsiębiorstw, do dostawców usług systemów nazw domen należy stosować ogólną zasadę wielkościową określoną w dyrektywie (UE) 2022/2555, przewidującą, że wszystkie podmioty, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia Komisji 2003/361/WE[5] lub które przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu, powinny być objęte zakresem stosowania dyrektywy (UE) 2022/2555.

(3) Podczas wdrażania dyrektywy (UE) 2022/2555 pojawiły się wyzwania związane z interpretacją przepisów dotyczących jej zakresu stosowania. W związku z tym należy doprecyzować niektóre przepisy dotyczące zakresu stosowania odnoszące się do świadczeniodawców, producentów energii elektrycznej, przedsiębiorstw wodorowych i podmiotów w sektorze chemicznym, aby zagwarantować pewność prawa i zmniejszyć obciążenie regulacyjne zarówno dla podmiotów, jak i dla organów krajowych.

(4) Aby zapewnić proporcjonalność w odniesieniu do producentów energii elektrycznej w rozumieniu art. 2 pkt 38 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/944[6], jedynie tych producentów energii elektrycznej, których łączna moc wytwórcza przekracza 1 MW, należy uznać za podmioty kluczowe lub ważne na podstawie dyrektywy (UE) 2022/2555, pod warunkiem że spełniają oni zasadę wielkościową. Powinno to obejmować producentów energii elektrycznej, w przypadku których moc pojedynczej instalacji produkującej energię elektryczną przekracza 1 MW, a także producentów energii elektrycznej, którzy obsługują kilka instalacji wytwarzania, których łączna moc wytwórcza przekracza 1 MW. Takie podejście umożliwia zachowanie równowagi między potrzebą uwzględnienia tych podmiotów, w przypadku których ingerencja w ich sieć i system informatyczny mogłaby oznaczać utratę mocy wytwórczej, brak możliwości kontroli lub zewnętrzną kontrolę nad nią, co samo w sobie ma znaczenie dla bezpieczeństwa i stabilności sieci elektroenergetycznej, a potrzebą nienakładania nieproporcjonalnych obciążeń administracyjnych na przedsiębiorstwa na podstawie dyrektywy (UE) 2022/2555.

(5) Europejskie portfele tożsamości cyfrowej przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014[7] są zasadniczym elementem unijnej infrastruktury cyfrowej, umożliwiającym bezpieczną identyfikację i uwierzytelnianie oraz wymianę dokumentów elektronicznych, w tym elektronicznych poświadczeń

---

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

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 Parlamentu Europejskiego i Rady (UE) 2019/944 z dnia 5 czerwca 2019 r. w sprawie wspólnych zasad rynku wewnętrznego energii elektrycznej oraz 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).

atrybutów. Ze względu na ich kluczową rolę dla społeczeństwa oraz dla świadczenia usług publicznych i prywatnych każdy incydent cyberbezpieczeństwa dotyczący tych portfeli mógłby mieć znaczny wpływ. Aby zapewnić świadczenie usług, dostawcy europejskich portfeli tożsamości cyfrowej powinni być zobowiązani do wdrożenia odpowiednich środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem w cyberbezpieczeństwie, zapobiegania incydentom i reagowania na nie oraz współpracy z właściwymi organami zgodnie z dyrektywą (UE) 2022/2555. Należy ich zatem zaliczyć do podmiotów objętych tą dyrektywą, niezależnie od ich wielkości, i zaklasyfikować jako podmioty kluczowe. Europejskie portfele biznesowe oferują podobne funkcje i usługi dostosowane do potrzeb podmiotów gospodarczych i organów sektora publicznego, w oparciu o unijne ramy tożsamości cyfrowej, i mają równie kluczowe znaczenie dla bezpieczeństwa oraz 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, lecz również wszelką infrastrukturę związaną z ich eksploatacją. Taka infrastruktura obejmuje centra logistyczne i naziemne części kabla podmorskiego łączącego się z nimi, takie jak trasy lądowe od studzienek plażowych do centrum logistycznego, ośrodka przetwarzania danych lub punktu dystrybucyjnego/połączeniowego. Podmorską infrastrukturę transmisji danych eksploatują zazwyczaj podmioty już objęte dyrektywą (UE) 2022/2555, w tym dostawcy publicznych sieci i usług łączności elektronicznej lub dostawcy usług chmurowych. Podmorską infrastrukturę transmisji danych mogą jednak również eksploatować inne rodzaje podmiotów, które obecnie nie są objęte zakresem stosowania dyrektywy (UE) 2022/2555, takie jak dostawcy sieci łączności elektronicznej, które nie są publiczne, eksploatujący podmorską infrastrukturę transmisji danych, lub podmioty, które dzierżawią tę infrastrukturę w całości lub częściowo dostawcom publicznych sieci łączności elektronicznej. Biorąc pod uwagę rosnące ryzyko dla podmorskiej infrastruktury transmisji danych i wynikającą z tego jej wysoką krytyczność, należy zapewnić, aby wszystkie rodzaje operatorów podmorskiej infrastruktury transmisji danych były objęte dyrektywą (UE) 2022/2555. Inne morskie infrastruktury krytyczne, takie jak podmorskie kable elektroenergetyczne, a także gazociągi, rurociągi wodorowe i ropociągi, są już zazwyczaj objęte dyrektywą (UE) 2022/2555, ponieważ są eksploatowane przez operatorów systemów przesyłowych w podsektorach energii elektrycznej, gazu, wodoru i ropy.

(7) Aby umożliwić podmiotom świadczącym usługi w kilku państwach członkowskich korzystanie z bardziej spójnych i mniej uciążliwych podejść nadzorczych na całym rynku wewnętrznym, podmioty takie powinny mieć możliwość wykazania zgodności z określonymi lub wszystkimi obowiązkami w zakresie zarządzania ryzykiem w cyberbezpieczeństwie określonymi w dyrektywie (UE) 2022/2555 przez uzyskanie certyfikatu dotyczącego stanu cyberbezpieczeństwa w ramach europejskiego programu certyfikacji cyberbezpieczeństwa. Przy opracowywaniu takiego programu korzystne będzie przyjęcie aktów wykonawczych w sprawie wymogów technicznych,

[8] COM(2025) 838 final.

metodycznych i sektorowych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie na podstawie dyrektywy (UE) 2022/2555, które opierają się na maksymalnej harmonizacji.

(8) Biorąc pod uwagę stale rosnącą zależność naszego społeczeństwa i naszej gospodarki od technologii cyfrowych, należy wprowadzić środki ograniczające zagrożenie ze strony technologii kwantowych. Możliwość przeprowadzenia ataków typu „zbieraj teraz – odszyfruj później", które prawdopodobnie już występują, i przyszłe zagrożenia wynikające z ataków kwantowych umożliwiających podrabianie podpisów, a także planowana deprecjacja niektórych implementacji algorytmów i całkowity zakaz stosowania obecnych algorytmów kryptografii asymetrycznej zwiększają potrzebę pilnego podjęcia działań na rzecz przejścia na kryptografię postkwantową W związku z tym państwa członkowskie powinny być zobowiązane do przyjęcia polityk na rzecz przejścia na kryptografię postkwantową w ramach krajowej strategii cyberbezpieczeństwa. Takie polityki powinny ułatwiać przyspieszenie planowania strategicznego oraz tworzenie środków i narzędzi wsparcia mających na celu ocenę narażenia zasobów kryptograficznych na ryzyko stwarzane przez komputery kwantowe. Powinny one również pomóc w opracowaniu planu przejścia i testowaniu wdrażania kryptografii postkwantowej w aplikacjach i sieciach cyfrowych, a jednocześnie wspierać powstawanie i wdrażanie formalnie zweryfikowanych i ocenionych europejskich rozwiązań w zakresie kryptografii postkwantowej zgodnych z ramami zgodności w odniesieniu do produktów i usług. Polityki te powinny być zgodne z celami pośrednimi określonymi w aktach prawnych i politykach Unii, a także w dokumentach przyjętych przez grupę współpracy NIS, w szczególności w skoordynowanym planie wdrożenia dotyczącym przejścia na kryptografię postkwantową, przyjętym przez grupę współpracy NIS w czerwcu 2025 r., co pozwoli przeprowadzić migrację do kryptografii postkwantowej do 2030 r. w przypadku zastosowań krytycznych i do 2035 r. w przypadku zastosowań średniego i niskiego poziomu.

(9) Zgodnie z art. 21 ust. 2 lit. d) dyrektywy (UE) 2022/2555 podmioty kluczowe i ważne mają zapewnić odpowiedni poziom bezpieczeństwa w swoim łańcuchu dostaw. W praktyce obowiązek ten skłonił wiele podmiotów do zwrócenia się do dostawców o obszerne informacje, z wykorzystaniem przy tym różnorodnych kwestionariuszy, formatów i procesów. Chociaż takie wnioski mają na celu wspieranie należytej staranności i zarządzania ryzykiem, mogą również powodować znaczne obciążenie administracyjne dla dostawców podmiotów kluczowych i ważnych, zwłaszcza gdy podobne informacje muszą być wielokrotnie przekazywane w różnych formach. Aby zmniejszyć to obciążenie i propagować spójne, proporcjonalne i skuteczne podejście do ocen bezpieczeństwa łańcucha dostaw, Komisja powinna opracować wytyczne określające odpowiedni poziom szczegółowości, strukturę oraz format takich wniosków o udzielenie informacji. Takie wytyczne powinny ułatwiać harmonizację, ograniczać niepotrzebne powielanie działań oraz wspierać zarówno podmioty, jak i ich dostawców w skutecznym wypełnianiu obowiązków wynikających z dyrektywy (UE) 2022/2555.

(10) Ataki z użyciem oprogramowania szantażującego, w trakcie których złośliwe oprogramowanie szyfruje dane i systemy oraz żąda okupu za ich odblokowanie, pozostają jednym z głównych zagrożeń dla podmiotów kluczowych i ważnych. Harmonizacja i usprawnienie gromadzenia danych na temat ataków z użyciem oprogramowania szantażującego od podmiotów kluczowych i ważnych dostarczyłyby informacji zespołom reagowania na incydenty bezpieczeństwa komputerowego

(CSIRT) i organom krajowym i umożliwiłyby im zapewnienie, aby przyszłe interwencje w przypadku użycia oprogramowania szantażującego były odpowiednie i skuteczne, wspieranie podmiotów w zwiększaniu ich odporności i zapobieganiu przyszłym atakom oraz gromadzenie danych wywiadowczych i dowodów niezbędnych organom ścigania do zakłócania działalności i rozbijania grup przestępczych wykorzystujących oprogramowanie szantażujące oraz karania ich członków. Biorąc pod uwagę potencjalnie wrażliwy charakter informacji, które mają być udostępniane w związku z atakami z użyciem oprogramowania szantażującego, w szczególności dotyczących tego, czy dany podmiot zapłacił okup, a jeśli tak, to w jakiej kwocie i komu, takie informacje należy przekazywać wyłącznie CSIRT lub, w stosownych przypadkach, właściwym organom na ich wniosek. Do celów takiej wymiany informacji podmioty kluczowe i ważne zachęca się do wyznaczenia osoby pełniącej funkcję punktu kontaktowego oraz zapewniającej poufność i wiarygodność wymiany informacji. W kontekście Międzynarodowej inicjatywy na rzecz walki z oprogramowaniem szantażującym Unia zatwierdziła niewiążącą deklarację dotyczącą polityki międzynarodowej, zgodnie z którą odpowiednie instytucje podlegające uczestniczącym rządom krajowym nie powinny płacić okupu w związku z atakami z użyciem oprogramowania szantażującego.

(11) Wypełnienie obowiązków w zakresie zgłaszania odpowiednich informacji na temat incydentów związanych z oprogramowaniem szantażującym nie powinno skutkować nałożeniem jakichkolwiek dodatkowych obowiązków na podstawie dyrektywy (UE) 2022/2555, którym podmiot ten nie podlegałby, gdyby nie zgłosił tych informacji. W tym celu, w granicach swojego krajowego porządku prawnego, państwa członkowskie powinny uwzględnić ewentualne ryzyko wynikające ze zwiększonej odpowiedzialności związanej ze zgłaszaniem odpowiednich informacji na temat incydentów związanych z oprogramowaniem szantażującym.

(12) Biorąc pod uwagę transgraniczny wymiar wielu podmiotów kluczowych i ważnych na całym rynku wewnętrznym, jak również potrzebę zapewnienia spójności oraz propagowania konwergencji i skuteczności w odniesieniu do podejść nadzorczych, ENISA powinna wspierać państwa członkowskie w zapewnianiu wzajemnej pomocy na rzecz podmiotów kluczowych i ważnych, które świadczą usługi w więcej niż jednym państwie członkowskim lub które świadczą usługi w co najmniej jednym państwie członkowskim i ich sieci i systemy informatyczne są zlokalizowane w co najmniej jednym innym państwie członkowskim. W tym celu państwa członkowskie powinny przekazywać dodatkowe informacje do rejestru podmiotów prowadzonego przez ENISA. Na podstawie informacji zawartych w rejestrze podmiotów kluczowych i ważnych ENISA powinna przeprowadzić kompleksową analizę transgranicznego ryzyka w cyberbezpieczeństwie związanego z podmiotami kluczowymi i ważnymi. Analiza ta powinna opierać się na metodyce opracowanej wspólnie z Komisją i grupą współpracy NIS. Metodyka ta mogłaby uwzględniać stopień, w jakim podmioty kluczowe i ważne wdrażają swoje usługi na szeroką skalę w wymiarze transgranicznym, polegają na usługach transgranicznych, są narażone na ryzyko koncentracji w łańcuchu dostaw, mogą zostać zidentyfikowane jako źródło ryzyka koncentracji w łańcuchu dostaw, są narażone na incydenty, które mogłyby mieć znaczący negatywny wpływ na usługi transgraniczne, lub korzystają z sieci i systemów informatycznych w celu świadczenia usług, które to sieci i systemy znajdują się w różnych państwach członkowskich i poza Unią. Na podstawie sprawozdania z analizy ryzyka ENISA powinna zalecić odpowiednim właściwym organom utworzenie wspólnych zespołów ds. kontroli, aby wspierać nadzór nad podmiotami o wyższym stopniu ryzyka dla sprawnego funkcjonowania rynku

wewnętrznego w przypadku wystąpienia incydentów oraz wspierać właściwe organy w wykonywaniu wspólnych działań nadzorczych na ich wniosek.

(13) Ponieważ cel niniejszej dyrektywy, a mianowicie uproszczenie wdrażania środków zmierzających do osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na skutki działania możliwe jest lepsze jego osiągnięcie na poziomie Unii, Unia może podjąć działania 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) Zgodnie z art. 42 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725[9] skonsultowano się z Europejskim Inspektorem Ochrony Danych i Europejską Radą Ochrony Danych, którzy wydali wspólną opinię w dniu [data] r.,

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:

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

(i) pkt (iii) otrzymuje brzmienie:

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

(ii) dodaje się pkt (iv) i (v) w brzmieniu:

„(iv) dostawców europejskich portfeli tożsamości cyfrowej przewidzianych w rozporządzeniu (UE) nr 910/2014;

(v) dostawców 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. Niniejsza dyrektywa ma zastosowanie do podmiotów określonych jako właściciele, zarządcy i operatorzy infrastruktury strategicznej podwójnego zastosowania na podstawie rozporządzenia (UE) [...]**, niezależnie od ich wielkości.

_____

[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, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

** Rozporządzenie (UE) [...] [wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram środków ułatwiających transport sprzętu i personelu wojskowego oraz towarów wojskowych w całej Unii.].";

2) w art. 3 wprowadza się następujące zmiany:

a) w ust. 1 wprowadza się następujące zmiany:

(i) lit. a) i b) otrzymują brzmienie:

„a) podmioty w rodzaju tych, o których mowa w załączniku I, przekraczające pułapy dla małych spółek o średniej kapitalizacji;

b) kwalifikowanych dostawców usług zaufania, dostawców europejskich portfeli tożsamości cyfrowej, dostawców europejskich portfeli biznesowych i rejestry nazw domen najwyższego poziomu, niezależnie od ich wielkości;";

(ii) dodaje się lit. h) w brzmieniu:

„h) podmioty określone jako właściciele, zarządcy i operatorzy strategicznej infrastruktury podwójnego zastosowania na podstawie rozporządzenia (UE) [...] [wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram środków ułatwiających transport sprzętu i personelu wojskowego oraz towarów wojskowych w całej Unii].";

b) 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) nazwy podmiotu;

b) odpowiedniego sektora, podsektora i rodzaju podmiotu, o których mowa w załączniku I lub II, w stosownych przypadkach;

c) adresu podmiotu lub, w stosownych przypadkach, adresu głównego miejsca prowadzenia działalności podmiotu oraz jego innych prawnych miejsc prowadzenia działalności w Unii lub – jeżeli nie ma on miejsca prowadzenia działalności w Unii – przedstawiciela wyznaczonego zgodnie z art. 26 ust. 3;

d) aktualnych danych kontaktowych, w tym adresów poczty elektronicznej, numerów telefonów, niepowtarzalnego identyfikatora i adresów cyfrowych europejskiego portfela biznesowego podmiotu, w stosownych przypadkach, oraz jego przedstawiciela wyznaczonego zgodnie z art. 26 ust. 3, w stosownych przypadkach;

e) państw członkowskich, w których podmiot świadczy usługi;

f) zakresów adresów IP podmiotu.";

3) art. 5 otrzymuje brzmienie:

„*Artykuł 5*

Harmonizacja minimalna

Bez uszczerbku dla art. 21 ust. 5 akapit piąty niniejsza dyrektywa nie uniemożliwia państwom członkowskim przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie przepisy są spójne z obowiązkami państw członkowskich ustanowionymi w prawie Unii.”;

4) w art. 6:

dodaje się pkt 42 i 43 w brzmieniu:

„42) »mała spółka o średniej kapitalizacji« oznacza małą spółkę o średniej kapitalizacji zdefiniowaną w załączniku do zalecenia Komisji (UE) 2025/1099***;

43) »podmorska infrastruktura transmisji danych« oznacza kable podmorskie przesyłające dane, powiązaną infrastrukturę oraz inne obiekty lub elementy związane z transmisją danych.

_____

*** Zalecenie Komisji (UE) 2025/1099 z dnia 21 maja 2025 r. dotyczące definicji małych spółek 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) dotyczące przejścia na kryptografię postkwantową, z uwzględnieniem terminów 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 CSIRT wyznaczonych lub utworzonych zgodnie z art. 10, zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach Unii (CERT-EU) oraz ENISA.”;

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

a) akapit drugi otrzymuje brzmienie:

„Komisja może przyjąć akty wykonawcze określające wymogi techniczne i metodyczne, a w razie potrzeby również wymogi sektorowe dotyczące środków, o których mowa w ust. 2, w odniesieniu do podmiotów kluczowych i ważnych innych niż te, o których mowa w akapicie pierwszym niniejszego ustępu. Komisja regularnie ocenia, czy akty wykonawcze, o których mowa w niniejszym akapicie, należy przyjąć w odniesieniu do konkretnych 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 inkluzywny 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 akapitach pierwszym i drugim niniejszego ustępu, państwa członkowskie nie nakładają na podmioty objęte zakresem tych aktów wykonawczych żadnych dalszych wymogów technicznych, metodycznych ani sektorowych

dotyczących środków, o których mowa w art. 21 ust. 2 dyrektywy (UE) 2022/2555.”;

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

„12. Przyjmując akt wykonawczy na podstawie ust. 11 akapit pierwszy, Komisja uwzględnia wymogi dotyczące przekazywania następujących informacji w odniesieniu do ataków z użyciem oprogramowania szantażującego na podstawie ust. 1:

a) tego, czy podmiot wykrył atak z użyciem oprogramowania szantażującego;

b) wektora ataku dotyczącego ataku z użyciem oprogramowania szantażującego;

c) tego, czy wdrożono środki ograniczające ryzyko.

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

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

b) czy zapłacono okup, a jeżeli tak, to w jakiej kwocie, w jakich środkach płatniczych i na rzecz jakiego odbiorcy lub odbiorcy końcowego, w tym, w stosownych przypadkach, dostawcy kryptoaktywów lub usług w zakresie kryptoaktywów.”;

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

„4. Aby wykazać zgodność z art. 21, państwa członkowskie mogą wymagać od podmiotów kluczowych i ważnych uzyskania certyfikatu dotyczącego stanu cyberbezpieczeństwa w ramach europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego na podstawie art. 75 rozporządzenia (UE) XXX/XXX**** [wniosek dotyczący aktu o cyberbezpieczeństwie 2].

5. W przypadku gdy stan cyberbezpieczeństwa podmiotu kluczowego lub ważnego podlega certyfikacji w ramach europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego na podstawie art. 74 rozporządzenia (UE) XXX/XXX**** [wniosek dotyczący aktu o cyberbezpieczeństwie 2] i jeżeli certyfikat wykazuje zgodność z wymogami określonymi w akcie wykonawczym przyjętym na podstawie 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 na podstawie art. 32 ust. 2 lit. b) lub art. 33 ust. 2 lit. b), w stosownych przypadkach, w odniesieniu do wymogów objętych certyfikatem.

6. Certyfikacja na podstawie ust. 4 nie wpływa na odpowiedzialność podmiotu kluczowego lub ważnego za przestrzeganie niniejszej dyrektywy.

**** Rozporządzenie (UE) XXX/XXX [wniosek dotyczący aktu o cyberbezpieczeństwie 2].”;

10) w art. 26 wprowadza się następujące zmiany:

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

„d) przewoźników lotniczych, których uznaje się za podlegających jurysdykcji państwa członkowskiego, którego właściwy organ wydający koncesje przyznał koncesję danemu podmiotowi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 1008/2008*****, lub, w przypadku gdy koncesja lub jej odpowiednik nie zostały przyznane zgodnie z tym rozporządzeniem, uznaje się za podlegających jurysdykcji państwa członkowskiego, w którym mają główne miejsce prowadzenia działalności w Unii zgodnie z ust. 2.

_____

***** Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1008/2008 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) ust. 3 otrzymuje brzmienie:

„3. Jeżeli podmiot kluczowy lub ważny nie ma miejsca prowadzenia działalności w Unii, ale oferuje usługi w Unii, wyznacza przedstawiciela w Unii. Przedstawiciel musi mieć miejsce prowadzenia działalności w jednym z tych państw członkowskich, w których oferowane są usługi. Uznaje się, że taki podmiot podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel ma miejsce prowadzenia działalności. W przypadku gdy taki podmiot jest podmiotem, o którym mowa w ust. 1 lit. a), uznaje się, że podlega on jurysdykcji państwa członkowskiego, w którym świadczy usługi. W razie niewyznaczenia przedstawiciela w Unii na podstawie niniejszego artykułu państwo członkowskie, w którym dany podmiot świadczy usługi, może podjąć wobec tego podmiotu działania prawne w związku z naruszeniem niniejszej dyrektywy.”;

11) w art. 27 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. ENISA tworzy i prowadzi rejestr podmiotów kluczowych i ważnych, a także podmiotów świadczących usługi rejestracji nazw domen, na podstawie informacji otrzymanych z pojedynczych punktów kontaktowych zgodnie z ust. 4. Na wniosek ENISA zezwala właściwym organom na dostęp do przechowywanych w tym rejestrze informacji dotyczących dostawców usług DNS, rejestrów nazw TLD, podmiotów świadczących usługi rejestracji nazw domen, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz przewoźników lotniczych, zapewniając jednocześnie – w stosownych przypadkach – ochronę poufności informacji.”;

b) uchyla się ust. 2;

c) ust. 3, 4 i 5 otrzymują brzmienie:

„3. Państwa członkowskie zapewniają, aby podmioty kluczowe i ważne powiadamiały właściwy organ o zmianach w informacjach przedłożonych na podstawie art. 3 ust. 4 niezwłocznie, a w każdym razie w ciągu dwóch tygodni od dnia, w którym nastąpiła zmiana.

4. Po otrzymaniu informacji, o których mowa w art. 3 ust. 4, pojedynczy punkt kontaktowy danego państwa członkowskiego przekazuje te informacje, bez zbędnej zwłoki, ENISA.

5. W stosownych przypadkach informacje, o których mowa w art. 3 ust. 4 akapit pierwszy, przedkłada się z wykorzystaniem mechanizmu krajowego, o którym mowa w art. 3 ust. 4 akapit czwarty.”;

12) dodaje się art. 37a w brzmieniu:

„Artykuł 37a

Rola ENISA w udzielaniu wzajemnej pomocy

1. ENISA pomaga państwom członkowskim w udzielaniu wzajemnej pomocy w rozumieniu art. 37 oraz ułatwia takie procesy współpracy w odniesieniu do podmiotów kluczowych i ważnych, które świadczą usługi w więcej niż jednym państwie członkowskim lub świadczą usługi w co najmniej jednym państwie członkowskim i ich sieci i systemy informatyczne są zlokalizowane w co najmniej jednym innym państwie członkowskim.

2. Do celów określonych w ust. 1 do dnia ... [15 miesięcy po wejściu w życie niniejszego rozporządzenia] ENISA przeprowadza kompleksową analizę transgranicznego ryzyka w cyberbezpieczeństwie związanego z podmiotami kluczowymi i ważnymi, które świadczą usługi w więcej niż jednym państwie członkowskim lub świadczą usługi w co najmniej jednym państwie członkowskim i ich sieci i systemy informatyczne są zlokalizowane w co najmniej jednym innym państwie członkowskim. W analizie tej ocenia się zakres ewentualnych skutków transgranicznych oraz skutków dla rynku wewnętrznego wynikających z incydentów wpływających na takie podmioty kluczowe i ważne. Do celów tej analizy ENISA, we współpracy z Komisją i Grupą Współpracy, opracowuje metodykę. Na podstawie tej analizy ENISA sporządza kompleksowe sprawozdanie z oceny transgranicznego ryzyka w cyberbezpieczeństwie, które jest aktualizowane corocznie.

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

a) w stosownych przypadkach zaleca odpowiednim właściwym organom utworzenie wspólnych zespołów ds. kontroli w celu wsparcia nadzoru nad określonymi podmiotami;

b) opracowuje wytyczne dotyczące wspólnych działań nadzorczych;

c) na wniosek właściwych organów zainteresowanych państw członkowskich dokonuje praktycznych ustaleń dotyczących wykonywania wspólnych działań nadzorczych;

d) na wniosek właściwych organów zainteresowanych państw członkowskich, z zastrzeżeniem i proporcjonalnie do zasobów własnych, uczestniczy we wspólnych działaniach nadzorczych;

e) na wniosek właściwych organów zainteresowanych państw członkowskich pomaga w ocenie stopnia wdrożenia przez podmiot kluczowy lub ważny środków zarządzania ryzykiem w cyberbezpieczeństwie określonych w art. 21.

4. Do celów ust. 3 lit. e) niniejszego artykułu właściwe organy zainteresowanych państw członkowskich przekazują ENISA, o ile są dostępne, wykaz środków zarządzania ryzykiem w cyberbezpieczeństwie wprowadzonych przez podmiot kluczowy lub ważny zgodnie z art. 21, wykaz przeprowadzonych działań w zakresie nadzoru lub egzekwowania przepisów, a także odpowiednią dokumentację, w tym dowody wdrożenia polityki cyberbezpieczeństwa, takie jak wyniki audytów bezpieczeństwa, które to działania właściwe organy podjęły 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 takiej wzajemnej pomocy. W stosownych przypadkach pojedynczy punkt kontaktowy określa, który incydent transgraniczny, o którym mowa w art. 23 ust. 6, był związany z przypadkiem udzielenia wzajemnej pomocy.”;

13) w załącznikach I i II wprowadza się zmiany zgodnie z załącznikiem do niniejszej dyrektywy.

Artykuł 2
Transpozycja

1. Do dnia... [12 miesięcy po wejściu w życie niniejszej dyrektywy] państwa członkowskie przyjmują i publikują przepisy niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają o tym Komisję.

   Państwa członkowskie stosują te przepisy od dnia [jeden dzień od daty, o której mowa w akapicie pierwszym] r.

2. Przepisy, o których mowa w ust. 1, przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Sposób dokonywania takiego odniesienia określany jest 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 r.

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