EUROPEAN
COMMISSION

Strasbourg, 20.1.2026
COM(2026) 11 final

2026/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)

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

(Text with EEA relevance)

NOTATKA WYJAŚNIAJĄCA

1. KONTEKST WNIOSKU

• Powody i cele wniosku

Od czasu przyjęcia ustawy o cyberbezpieczeństwie (CSA) w 2019 r. sytuacja w zakresie zagrożeń dla cyberbezpieczeństwa uległa znacznej zmianie[1] w coraz bardziej złożonej rzeczywistości geopolitycznej. Liczba cyberataków gwałtownie wzrosła, a same ataki stały się bardziej wyrafinowane, wymierzone w infrastrukturę krytyczną, przedsiębiorstwa i ogół społeczeństwa, przy czym głównym elementem tych ataków jest oprogramowanie ransomware[2] . Pojawiające się nowe technologie, takie jak sztuczna inteligencja (AI) i informatyka kwantowa, zmieniają narzędzia obrony i taktykę przeciwników. W swoim **raporcie** z 2024 r. **pt. „Przyszłość europejskiej konkurencyjności”** Mario Draghi podkreślił potrzebę zwiększenia bezpieczeństwa i zmniejszenia zależności jako jeden z głównych obszarów działania niezbędnych w Unii Europejskiej[3] . Zarówno europejska strategia gotowości[4] , jak i europejska strategia bezpieczeństwa wewnętrznego (ProtectEU)[5] umieściły cyberbezpieczeństwo w centrum programu Unii na rzecz odporności. W strategiach tych uznano, że utrzymujące się zagrożenia dla cyberbezpieczeństwa stanowią nie tylko wyzwania techniczne, ale także strategiczne zagrożenia dla naszej demokracji, gospodarki i stylu życia. Podobnie w komunikacie w sprawie wzmocnienia bezpieczeństwa gospodarczego UE[6] 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.

W tym kontekście proponowana zmiana CSA ma na celu rozwiązanie **czterech głównych 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 cyberbezpieczeństwa (ECCF); (iii) złożoność i różnorodność polityk związanych z cyberbezpieczeństwem, które mają wpływ na pozycję Unii w zakresie cyberbezpieczeństwa; oraz (iv) rosnące zagrożenia dla bezpieczeństwa łańcuchów dostaw ICT.

W oparciu o zidentyfikowane główne problemy **dwa ogólne cele** interwencji to zwiększenie zdolności i odporności w zakresie cyberbezpieczeństwa oraz zapobieganie fragmentacji jednolitego rynku poprzez:

- przyczynianie się do wzmocnienia zarządzania cyberbezpieczeństwem w Unii oraz pomoc w zapewnieniu, aby odpowiednie instytucje, organy i inne zainteresowane strony były lepiej przygotowane do zapobiegania zagrożeniom dla

---

1 ENISA, *ENISA Threat Landscape 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

2 ENISA, *ENISA Threat Landscape 2025*.

3 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.

4 JOIN/2025/130 wersja ostateczna.

5 COM/2025/148 wersja ostateczna.

6 JOIN(2025) 977 wersja ostateczna.

cyberbezpieczeństwa, ich wykrywania i reagowania na nie w sposób skoordynowany i skuteczny; oraz

- wspieranie opracowywania, wdrażania i przyjmowania wspólnych unijnych instrumentów w zakresie cyberbezpieczeństwa, takich jak systemy certyfikacji, oraz zapewnienie zharmonizowanych ram budujących zaufanie i interoperacyjność między państwami członkowskimi.

Te ogólne cele stanowią odpowiedź na kluczowe wyzwania wskazane w definicji problemu. Odzwierciedlają one nadrzędny cel polityczny, jakim jest wzmocnienie zarządzania cyberbezpieczeństwem w Unii oraz wspieranie rozwoju bezpiecznego, odpornego i konkurencyjnego jednolitego rynku cyfrowego.

Aby pomóc w osiągnięciu wyżej wymienionych celów ogólnych, niniejsza interwencja ma następujące **cele szczegółowe (SPO)**:

- rozwiązanie problemu rozbieżności między ramami polityki Unii w zakresie cyberbezpieczeństwa a potrzebami zainteresowanych stron:
  - SPO1: stworzenie zdolności do skutecznego wdrażania polityki Unii w zakresie cyberbezpieczeństwa oraz ciągłej współpracy operacyjnej umożliwiającej bardziej ustrukturyzowaną współpracę między państwami członkowskimi;
  - SPO2: opracowanie i wdrożenie środków i mechanizmów skutecznie wspierających i zaspokajających potrzeby państw członkowskich, przemysłu i innych zainteresowanych stron;
- rozwiązanie problemu ograniczonego wykorzystania i skuteczności ECCF:
  - SPO3: stworzenie warunków wstępnych dla szybszego wdrażania systemów certyfikacji w zakresie cyberbezpieczeństwa dostosowanych do potrzeb rynku poprzez rozszerzenie zakresu ECCF, zapewnienie skutecznego utrzymania i sprawnych procedur oraz zwiększenie przejrzystości;
- Aby zaradzić fragmentaryczności przepisów dotyczących zgodności oraz złożoności ram horyzontalnych i sektorowych:
  - SPO4: stworzenie mechanizmów i warunków ułatwiających zgodność z wymogami w zakresie cyberbezpieczeństwa, dzięki czemu ich wdrażanie będzie bardziej spójne i skuteczne.
- rozwiązanie problemu zagrożeń dla cyberbezpieczeństwa w łańcuchu dostaw:
  - SPO5: ograniczenie ryzyka związanego z krytycznymi łańcuchami dostaw ICT od podmiotów mających siedzibę w państwach trzecich lub kontrolowanych przez podmioty z państw trzecich budzących obawy w zakresie cyberbezpieczeństwa (dostawcy wysokiego ryzyka) oraz zmniejszenie krytycznych zależności poprzez opracowanie spójnych i skutecznych ram na szczeblu UE w celu rozwiązania problemów związanych z ryzykiem dla bezpieczeństwa łańcucha dostaw ICT.

Zmiana CSA wchodzi w zakres **programu dostosowania i skuteczności regulacji (REFIT)**. W znacznym stopniu przyczynia się ona do poprawy przejrzystości, eliminacji nieefektywności i ujednolicenia procedur w różnych ramach prawnych. Zmiana CSA przyczynia się do

prawidłowego funkcjonowania rynku wewnętrznego, zapewniając jednocześnie bezpieczeństwo i autonomię strategiczną Unii.

Konkretniej rzecz ujmując, proponuje się w niej pełną reformę mandatu Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), zapewniającą skuteczne wsparcie dla wdrażania polityki i wartość dodaną w zakresie wspierania współpracy operacyjnej między państwami członkowskimi.

Biorąc pod uwagę rosnące zagrożenia i wyzwania związane z cyberbezpieczeństwem, przed którymi stoi Unia, wniosek ma na celu zwiększenie zasobów finansowych i ludzkich ENISA, aby odzwierciedlić jej wzmocnioną rolę, zadania i kluczową pozycję w obronie ekosystemu cyfrowego Unii, umożliwiając ENISA skuteczne wykonywanie zadań powierzonych jej w niniejszym wniosku.

Zmiana ta pomoże również wyeliminować fragmentaryczne praktyki, poprawiając koordynację, a jednocześnie obniżając koszty zgodności i koszty operacyjne w perspektywie długoterminowej. Uchylając obecny CSA i oraz wprowadzając zreformowany ECCF, wniosek zapewnia skuteczniejsze i wydajniejsze narzędzie, które zarówno promuje zaufanie wśród przedsiębiorstw, ogółu społeczeństwa i organów publicznych, jak i ułatwia przestrzeganie odpowiednich przepisów unijnych. Zwiększa ono wydajność poprzez zmianę modelu zarządzania i wspieranie bardziej przewidywalnych, spójnych i elastycznych procedur certyfikacji, aby umożliwić szybsze opracowywanie i wdrażanie systemów.

Większa synergia z odpowiednimi istniejącymi ramami prawnymi Unii będzie promować certyfikację jako narzędzie zapewniania zgodności dla przedsiębiorstw i zmniejszy obciążenia administracyjne dla organów oceny zgodności działających w ramach wielu aktów prawnych dotyczących cyberbezpieczeństwa. Ponadto, poprzez rozszerzenie zakresu ECCF i umożliwienie opracowania systemu dotyczącego cyberbezpieczeństwa podmiotów, wniosek zmniejsza koszty zapewnienia zgodności dla podmiotów podlegających odpowiednim przepisom Unii w zakresie cyberbezpieczeństwa, począwszy od podmiotów objętych zakresem dyrektywy NIS 2. Podejście to znacznie uprości obowiązki regulacyjne podmiotów podlegających wielu wymogom w zakresie zgodności i zapewni bardziej efektywne wykorzystanie zasobów przez organy krajowe. Oprócz tej zmiany, wniosek dotyczący dyrektywy wprowadzającej ukierunkowane zmiany do dyrektywy NIS 2 ma na celu uproszczenie zgodności z ramami cyberbezpieczeństwa oraz zapewnienie ich usprawnionego i spójnego wdrożenia w odniesieniu do określonych aspektów, w tym zakresu, definicji, zgłaszania oprogramowania ransomware oraz nadzoru nad podmiotami świadczącymi usługi transgraniczne.

Nowe rozporządzenie tworzy również zharmonizowane ramy dotyczące przeciwdziałania ryzyku nietechnicznemu mającemu wpływ na łańcuchy dostaw ICT, zmniejszając obecne rozdrobnienie podejść w poszczególnych państwach członkowskich. Wszystkie te aspekty stanowią znaczne uproszczenie i modernizację unijnych ram prawnych w zakresie cyberbezpieczeństwa, w pełni zgodne z zasadami REFIT dotyczącymi jasności, skuteczności i gotowości cyfrowej.

- **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 NIS2 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, w ramach której Komisja i Wysoki Przedstawiciel odgrywają kluczową rolę w przygotowywaniu się do incydentów związanych z cyberbezpieczeństwem na dużą skalę i reagowaniu na nie; (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 transgranicznych przepływów energii elektrycznej ( ) dla podsektora energii elektrycznej lub przepisami dotyczącymi bezpieczeństwa informacji (część IS[10]) dla podsektora transportu lotniczego.

Zmiana CSA jest zgodna z przepisami NIS2 dotyczącymi roli ENISA we wspieraniu wdrażania NIS2, w tym w zakresie wsparcia współpracy operacyjnej, oraz wzmacnia te przepisy; jest ona również zgodna z CRA, w tym w odniesieniu do przeglądu i zarządzania podatnością na zagrożenia na rynku wewnętrznym, oraz zwiększa wartość dodaną wspólnej świadomości sytuacyjnej. W odniesieniu do ECCF zmiana CSA jest zgodna z CRA w zakresie celów bezpieczeństwa produktów i postępowania w przypadku luk w zabezpieczeniach oraz z nowymi ramami prawnymi (NLF) w zakresie akredytacji. Ponadto istnieje silna synergia wynikająca z opracowania certyfikacji cyberbezpieczeństwa dla dyrektywy NIS2, a także potencjalnie z ułatwienia zgodności z innymi odpowiednimi aktami prawnymi Unii, takimi jak ogólne rozporządzenie o ochronie danych (RODO), bez uszczerbku dla ich szczególnych wymogów certyfikacyjnych. Ponadto horyzontalne ramy dotyczące ryzyka związanego z cyberbezpieczeństwem łańcuchów dostaw ICT wspierają ogólny cel dyrektywy NIS2, jakim jest stworzenie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, i opierają się na podejściu opartym na ryzyku zawartym w dyrektywie NIS2.

Ponadto zmiana CSA w połączeniu z wnioskiem dotyczącym dyrektywy wprowadzającej ukierunkowane zmiany do dyrektywy NIS2 w celu uproszczenia zapewnia niezbędne narzędzia, aby te kompleksowe ramy były bardziej skuteczne i wydajne w osiąganiu oczekiwanych rezultatów, zapewniały silniejszy wymiar europejski i wypełniały pozostałe luki regulacyjne.

- **Spójność z innymi politykami Unii**

Zmiana CSA stanowiłaby uzupełnienie dyrektywy CER, która uwzględnia kwestie związane z łańcuchem dostaw w ramach środków zapewniających odporność podmiotów o znaczeniu

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

krytycznym. Ponadto stanowiłaby uzupełnienie przyszłych inicjatyw, takich jak: (i) ustawa o rozwoju chmury obliczeniowej i sztucznej inteligencji (CAIDA), której celem jest między innymi rozwiązanie problemu braku konkurencyjnej oferty usług przetwarzania w chmurze w Unii na skalę wystarczającą do obsługi bardzo krytycznych zastosowań lub sektorów; (ii) wniosek dotyczący ustawy o sieciach cyfrowych (DNA); (iii) przyszłą zmianę rozporządzenia (UE) 2023/1781[11] , (iv) ramy zamówień publicznych[12] , które są obecnie poddawane ocenie[13] , oraz wniosek dotyczący rozporządzenia w sprawie uproszczenia przepisów dotyczących cyfryzacji (Digital Omnibus)[14] , który nakłada na ENISA obowiązek opracowania jednego punktu kontaktowego do zgłaszania incydentów, za pośrednictwem którego podmioty mogą jednocześnie wypełniać swoje obowiązki w zakresie zgłaszania incydentów wynikające z wielu aktów prawnych. Ponadto wzmocniłoby to pozycję organów i operatorów unijnych w kontaktach z partnerami z południowego wybrzeża Morza Śródziemnego, w szczególności poprzez wspieranie wzajemnych połączeń za pomocą bezpiecznych i sprawdzonych infrastruktur cyfrowych w całym regionie Morza Śródziemnego, co stanowi podstawowy cel paktu na rzecz regionu Morza Śródziemnego.

Zmiana CSA jest również zgodna z dokumentami strategicznymi Unii, w szczególności w odniesieniu do ram bezpieczeństwa łańcucha dostaw ICT. W strategii ProtectEU Komisja stwierdziła ponadto, że zharmonizowane podejście do bezpieczeństwa łańcucha dostaw technologii informacyjno-komunikacyjnych (ICT) może rozwiązać problem obecnej fragmentacji rynku wewnętrznego spowodowanej różnymi podejściami na szczeblu krajowym, uniknąć krytycznych zależności i zmniejszyć ryzyko związane z łańcuchami dostaw ICT od dostawców wysokiego ryzyka, zapewniając w ten sposób bezpieczeństwo infrastruktury krytycznej. W strategii bezpieczeństwa gospodarczego podkreślono również potrzebę zwiększenia odporności gospodarki UE i łańcucha dostaw w celu promowania jej konkurencyjności[15] . Konieczność zajęcia się zakłóceniami w łańcuchach dostaw i cyberatakami została również podkreślona w strategii Unii na rzecz gotowości i białej księdze w sprawie europejskiej obronności[16] . Jest to również zgodne z raportem Mario Draghiego „Przyszłość europejskiej konkurencyjności”, jak podkreślono powyżej. Co więcej, przegląd CSA w obszarze bezpieczeństwa łańcucha dostaw ICT wraz z niedawno przyjętym wspólnym komunikatem do Parlamentu Europejskiego i Rady w sprawie wzmocnienia bezpieczeństwa gospodarczego UE[17] .

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawą prawną niniejszego wniosku jest art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Artykuł 114 TFUE przewiduje przyjęcie środków zapewniających ustanowienie i funkcjonowanie rynku wewnętrznego. Rozporządzenie (UE) 2019/881 w

---

11 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1781 z dnia 13 września 2023 r. ustanawiające ramy środków na rzecz wzmocnienia europejskiego ekosystemu półprzewodników i zmieniające rozporządzenie (UE) 2021/694 (ustawa o chipach), *Dz.U. L 229 z 18.9.2023, s. 1–53.*

12 W szczególności dyrektywy 2014/23/UE, 2014/24/UE i 2014/25/UE.

13 Komisja Europejska, Komisja ogłasza zaproszenie do zgłaszania dowodów i konsultacje społeczne w sprawie oceny dyrektyw dotyczących zamówień publicznych, https://single-market-economy.ec.europa.eu/news/commission-launches-call-evidence-and-public-consultation-evaluation-public-procurement-directives-2024-12-13_en.

14 COM/2025/837 wersja ostateczna

15 JOIN/2023/20 wersja ostateczna.

16 JOIN/2025/120 wersja ostateczna.

17 JOIN/2025/977 wersja ostateczna

sprawie ENISA oraz certyfikacji w zakresie cyberbezpieczeństwa technologii informacyjno-komunikacyjnych, powszechnie znane jako CSA[18] , zostało pierwotnie przyjęte na podstawie tego przepisu.

W dziedzinie cyberbezpieczeństwa łańcucha dostaw ICT fragmentacja krajowych ram regulujących nietechniczne czynniki ryzyka ma negatywny wpływ na funkcjonowanie rynku wewnętrznego, ponieważ rozbieżności w podejściach krajowych mogą ostatecznie prowadzić do większej podatności niektórych państw członkowskich na zagrożenia, co może mieć skutki uboczne w całej Unii, wpływając na ogólną odporność, a także wiarygodność.

Biorąc pod uwagę zmieniający się charakter zagrożeń dla cyberbezpieczeństwa oraz rosnącą współzależność systemów cyfrowych państw członkowskich, art. 114 TFUE pozostaje uzasadnioną podstawą prawną dla zmiany CSA. Proponowane rozporządzenie odzwierciedla najnowsze zmiany w otoczeniu prawnym w zakresie cyberbezpieczeństwa, zwłaszcza biorąc pod uwagę rosnące obowiązki ENISA oraz rozszerzający się zakres certyfikacji i zarządzania ryzykiem.

- **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 obecnej CSA.

Jak już analizowano w odniesieniu do CSA, interwencja Unii ma kluczowe znaczenie, ponieważ zagrożenia dla cyberbezpieczeństwa i związane z nimi wyzwania wykraczają poza granice poszczególnych państw członkowskich. Fragmentaryczne rozwiązania krajowe okazały się niewystarczające do osiągnięcia zaufania i koordynacji na całym rynku. Zmienione ramy prawne Unii są niezbędne do usunięcia barier, zapewnienia spójnego wdrażania oraz wspierani nego państw członkowskich w coraz bardziej złożonym środowisku regulacyjnym i zagrożeń. Cyberbezpieczeństwo jest kwestią leżącą we wspólnym interesie Unii.

Działania objęte proponowanym rozporządzeniem zapewniają wyraźną wartość dodaną poprzez wspieranie harmonizacji, jasności prawnej i skoordynowanych reakcji na wyzwania związane z cyberbezpieczeństwem.

Obecne zadania ENISA zostały rozszerzone w wyniku kolejnych aktów prawnych bez kompleksowej zmiany jej podstawowych obowiązków i zasobów. Doprowadziło to do nieefektywności i niewystarczającego priorytetowego traktowania podstawowych zadań wspierających państwa członkowskie. W związku z tym wniosek dotyczący interwencji ma na celu udoskonalenie i ustalenie priorytetów obecnych zadań w celu wzmocnienia mandatu ENISA, umożliwiając jej pełnienie funkcji jedynego punktu kontaktowego w zakresie cyberbezpieczeństwa na szczeblu unijnym. W tej kwestii nie ma istotnej różnicy pod względem pomocniczości w porównaniu z CSA. Ponadto zróżnicowane krajowe systemy certyfikacji i różne podejścia regulacyjne państw członkowskich powodują fragmentację rynku i dodatkowe obciążenia związane z zapewnieniem zgodności, co osłabia konkurencyjność.

W nowym wniosku przewidziano również nowe działania w odniesieniu do polityki dotyczącej łańcucha dostaw i wysiłków na rzecz uproszczenia na szczeblu unijnym. Wzmacnia on ponadto bezpieczeństwo łańcucha dostaw i sektor cyberbezpieczeństwa w Unii oraz zwiększa gotowość i odporność państw członkowskich i przemysłu.

[18] Rozporządzenie – 2019/881 – EN – EUR-Lex

Zależność od podmiotów mających siedzibę w państwie trzecim, stwarzających zagrożenie dla cyberbezpieczeństwa lub kontrolowanych przez takie państwo trzecie, przez podmiot mający siedzibę w takim państwie trzecim lub przez obywatela takiego państwa trzeciego (dostawcy wysokiego ryzyka) ma wpływ na podmioty w całej Unii, a poważne incydenty związane z cyberbezpieczeństwem łańcucha dostaw często mają charakter transgraniczny. Ponadto, biorąc pod uwagę transgraniczny charakter łańcuchów dostaw ICT, fragmentacja wymogów dotyczących zgodności na rynku wewnętrznym podważałaby pewność prawną podmiotów. Ponadto wnioski dotyczące wieloletnich ram finansowych (WRF) nakazują wykluczenie dostawców wysokiego ryzyka w celu ochrony integralności budżetu UE i interesów bezpieczeństwa. Ramy dotyczące łańcucha dostaw zawarte w niniejszym rozporządzeniu przewidują mechanizm identyfikacji krajów budzących obawy w zakresie cyberbezpieczeństwa, co jest działaniem, które można skutecznie przeprowadzić wyłącznie na szczeblu UE. W odniesieniu do bezpieczeństwa łańcucha dostaw ICT jedynie interwencja na szczeblu UE zapewni ten sam minimalny poziom bezpieczeństwa w całej Unii oraz niezbędną harmonizację podejść.

W niniejszej zmianie zachowano i wzmocniono cel CSA. Cel ten nie może zostać osiągnięty w wystarczającym stopniu przez państwa członkowskie, ale może zostać lepiej osiągnięty na poziomie Unii zgodnie z art. 5 Traktatu o Unii Europejskiej.

- **Proporcjonalność**

Proponowane środki nie wykraczają poza to, co jest konieczne do osiągnięcia celów politycznych wniosku. Ponadto zakres interwencji Unii nie utrudnia podejmowania dalszych działań krajowych w kwestiach bezpieczeństwa narodowego. Działanie Unii jest zatem uzasadnione zasadami pomocniczości i proporcjonalności.

Wniosek ma na celu lepsze odzwierciedlenie w przepisach prawnych mandatu ENISA oraz procesu opracowywania, przyjmowania i utrzymywania europejskich certyfikatów cyberbezpieczeństwa. Chociaż wniosek zawiera pewne nowe zadania dla ENISA, ich celem jest wspieranie państw członkowskich w obszarach, w których stwierdzono istotne luki. ENISA nie zastąpi krajowych zespołów reagowania na incydenty związane z bezpieczeństwem informatycznym (CSIRT) państw członkowskich. W odniesieniu do ECCF certyfikacja pozostaje dobrowolna i może pomóc podmiotom w wykazaniu zgodności z unijnymi wymogami w zakresie cyberbezpieczeństwa. Podejście to zapewnia przestrzeganie zasady proporcjonalności.

W odniesieniu do rozwiązań proponowanych w związku z bezpieczeństwem łańcucha dostaw ICT, ramy przewidują zebranie dowodów na to, co stanowi kluczowe aktywa oraz jakie środki byłyby proporcjonalne i niezbędne do zapewnienia ograniczenia ryzyka w krytycznych łańcuchach dostaw. Przed określeniem tych środków przeprowadzona zostanie ocena skutków gospodarczych, która obejmie między innymi wykonalność ekonomiczną, dostępne alternatywy na rynku oraz cykl życia konkretnych produktów. Ocena ta pozwoli ustalić, jakie środki oparte na ryzyku są potrzebne i najbardziej odpowiednie.

- **Wybór instrumentu**

Niniejszy wniosek stanowi przegląd rozporządzenia (UE) 2019/881, które określa obecny mandat i zadania ENISA oraz ECCF. W związku z tym zmieniony mandat ENISA i zmiany w ECCF najlepiej ustanowić w ramach tego samego instrumentu prawnego, wykorzystując instrument rozporządzenia. Proponowane przepisy obejmują również skuteczne ramy na szczeblu UE w celu przeciwdziałania zagrożeniom dla bezpieczeństwa łańcucha dostaw ICT,

w przypadku których rozporządzenie pozwoliłoby skuteczniej rozwiązać zidentyfikowane problemy i osiągnąć sformułowane cele, ponieważ tylko interwencja na szczeblu UE zapewni ten sam poziom bezpieczeństwa w całej Unii i niezbędną harmonizację podejść. Proces transpozycji w przypadku dyrektywy dotyczącej takiej interwencji mógłby pozostawić zbyt dużą swobodę decyzyjną na szczeblu krajowym, co mogłoby prowadzić do braku jednolitości niektórych podstawowych wymogów w zakresie cyberbezpieczeństwa, niepewności prawnej, dalszej fragmentacji, a nawet dyskryminujących sytuacji transgranicznych.

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

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

Zgodnie z art. 67 rozporządzenia (UE) 2019/881 Komisja Europejska oceniła znaczenie, wpływ, skuteczność, efektywność, spójność i wartość dodaną ENISA i ECCF, biorąc pod uwagę zmieniające się otoczenie technologiczne i regulacyjne. Ocena ta, zakończona w grudniu 2024 r., obejmowała okres od 2017 r. do 2023 r. i miała na celu przegląd mandatu i działalności ENISA oraz ocenę roli ECCF w promowaniu bezpiecznego środowiska cybernetycznego w całej UE. Główne ustalenia można podsumować w następujący sposób.

- **Znaczenie:** Znaczenie ENISA w dziedzinie cyberbezpieczeństwa podkreśla jej zdolność do reagowania na zmieniające się potrzeby zainteresowanych stron i dostosowywania się do zmieniającej się sytuacji. Chociaż zadowolenie zainteresowanych stron jest ogólnie pozytywne, istnieją możliwości zwiększenia wpływu ENISA. Można to osiągnąć poprzez poprawę wsparcia i widoczności dla różnych sektorów, w szczególności małych i średnich przedsiębiorstw (MŚP), które często borykają się z wymogami w zakresie cyberbezpieczeństwa. Niezbędna jest lepsza organizacja zasobów i wyraźniejsza koordynacja z organami krajowymi. Zmiana priorytetów działań i optymalizacja istniejących zasobów pozwoli ENISA lepiej dostosować się do dynamicznych potrzeb europejskiego środowiska cyberbezpieczeństwa.

  Jeśli chodzi o ECCF, pomimo obiecujących założeń, ramy te nadal są uważane za mające większy potencjał niż praktyczny wpływ, ponieważ dopiero jeden system certyfikacji został niedawno uruchomiony. Ramy te mają na celu płynną integrację z innymi aktami prawnymi Unii w celu usprawnienia procedur i ułatwienia handlu transgranicznego. Ich znaczenie jest szczególnie widoczne w obszarach wymagających wysokiego poziomu bezpieczeństwa, takich jak usługi w chmurze i infrastruktura 5G.

- **Skuteczność:** ENISA z powodzeniem wypełniła swój mandat, realizując prawie wszystkie zaplanowane zadania i wykazując się elastycznością i odpornością podczas kryzysów, takich jak pandemia COVID- 19 i agresja Rosji wobec Ukrainy. Jednakże w celu zwiększenia efektywności konieczne jest lepsze ustalanie priorytetów, jasne ukierunkowanie działań i strategiczna alokacja zasobów. Bardziej elastyczne podejście do zarządzania wewnętrznego ma zasadnicze znaczenie dla dostosowania się do zmieniających się wymagań w zakresie cyberbezpieczeństwa i minimalizacji opóźnień.

  ECCF miało na celu harmonizację certyfikacji cyberbezpieczeństwa w całej Unii, ale napotkało poważne wyzwania, w tym ograniczenia proceduralne i fragmentację, które doprowadziły do opóźnień i nieefektywności, takich jak opóźnienie w przyjęciu europejskiego systemu certyfikacji cyberbezpieczeństwa opartego na wspólnych

kryteriach (EUCC). Czynniki zewnętrzne, takie jak napięcia geopolityczne i pandemia COVID-19, dodatkowo utrudniły osiągnięcie celów ECCF, podkreślając potrzebę wprowadzenia elastycznych środków i spójnego przydzielania zasobów między zainteresowanymi stronami w celu osiągnięcia jednolitości i skuteczności certyfikacji w zakresie cyberbezpieczeństwa. Pomimo tych przeszkód osiągnięto pozytywne wyniki, zwłaszcza w zakresie podnoszenia świadomości państw członkowskich na temat znaczenia i złożoności certyfikacji w zakresie cyberbezpieczeństwa.

- **Efektywność:** ENISA działała efektywnie w ramach swojej macierzowej struktury organizacyjnej, promując współpracę i ustalanie priorytetów zadań. ENISA napotkała jednak trudności w zaspokojeniu rosnącego zapotrzebowania i obsadzeniu specjalistycznych stanowisk, co pogłębił globalny niedobór specjalistów IT, prowadząc do opóźnień i dużego obciążenia pracą. Aby rozwiązać te problemy, ENISA mogłaby zoptymalizować swoje wewnętrzne zasoby kadrowe i skutecznie realokować zasoby, czego przykładem są strategiczne dostosowania, takie jak przesunięcie zasobów w 2022 r. na rzecz działań wspierających cyberbezpieczeństwo. Ponadto poprawa zarządzania budżetem i zmniejszenie wydatków administracyjnych jeszcze bardziej poprawiłoby efektywność operacyjną agencji.

  Skuteczność ECCF była krytykowana ze względu na wydłużone terminy przyjmowania systemów certyfikacji cyberbezpieczeństwa i związane z tym złożoności, przy czym pierwszy system został przyjęty dopiero na początku 2024 r., prawie pięć lat po przyjęciu CSA. Do opóźnień przyczyniły się wyzwania polityczne i techniczne, takie jak debaty na temat suwerenności danych i trudności w przekładaniu projektów na akty prawne. Wyzwania polityczne i wymagania techniczne utrudniły postępy, co widać na przykładzie unijnego systemu certyfikacji chmury obliczeniowej (EUCS) i systemu EU5G. Pomimo tych nieefektywności ramy te przyniosły kilka pozytywnych aspektów. Nadal jednak istnieje potrzeba poprawy zaangażowania zainteresowanych stron i wewnętrznego zarządzania, aby zapewnić optymalne funkcjonowanie i wkład strategiczny.

- **Spójność:** Spójność ENISA jest wspierana przez znaczne zaangażowanie zainteresowanych stron i dostosowanie do najnowszych ram prawnych. Jednakże w celu zwiększenia spójności i poprawy alokacji zasobów konieczne jest wzmocnienie synergii z innymi organami Unii, takimi jak Europejskie Centrum Kompetencji w zakresie Przemysłu, Technologii i Badań w dziedzinie Cyberbezpieczeństwa (ECCC) oraz organami krajowymi. Ponadto należy udoskonalić komunikację wewnętrzną i zarządzanie zasobami w ramach ENISA, a także przejrzystą współpracę z prywatnymi zainteresowanymi stronami. Jasne określenie zadań ENISA, zgodne z CRA i dyrektywą NIS2, poprawi zarówno efektywność, jak i spójność regulacyjną.

  W odniesieniu do ECCF pełna spójność z innymi instrumentami prawnymi Unii, w tym z dyrektywą NIS2 i CRA, ma kluczowe znaczenie dla zapewnienia jednolitego podejścia do cyberbezpieczeństwa. Chociaż ECCF wykazuje teoretyczną zgodność z tymi środkami prawnymi, rzeczywista integracja pozostaje złożona i wymaga starannego nadzoru. Wdrożenie przyjętego systemu EUCC w ramach CRA będzie pod tym względem istotnym sprawdzianem.

- **Wartość dodana UE:** ENISA wniosła znaczący wkład w ekosystem cyberbezpieczeństwa Unii poprzez promowanie współpracy i ujednolicanie praktyk. Jej rola w ułatwianiu krajowych działań i dostarczaniu informacji na temat pojawiających się zagrożeń była niezwykle istotna. Jednak krytyka ze strony podmiotów sektora prywatnego dotycząca potrzeby bardziej dostosowanego wsparcia

wskazuje na konieczność poprawy zaangażowania zainteresowanych stron i współpracy branżowej. Strategiczna ocena zarządzania zasobami umożliwiłaby ENISA lepsze dostosowanie się do zmieniających się wyzwań w zakresie cyberbezpieczeństwa i skuteczniejsze służenie różnorodnym zainteresowanym stronom. ECCF miało na celu wprowadzenie zharmonizowanych procesów certyfikacji, ale napotkało trudności wdrożeniowe ze względu na przedłużające się terminy i fragmentację. Wartość dodana ECCF była ograniczona ze względu na niedociągnięcia w realizacji celów i brak efektywności. Pomimo tych wyzwań ECCF poprawiło harmonizację między państwami członkowskimi i stworzyło lepsze możliwości współpracy, w szczególności poprzez utworzenie forów współpracy zainteresowanych stron, takich jak Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa (ECCG).

- **Konsultacje z zainteresowanymi stronami**

W latach 2023–2025 przeprowadzono kilka konsultacji z zainteresowanymi stronami zarówno w kontekście oceny CSA, jak i przeglądu CSA, jak opisano poniżej.

– **W 2023 r.** przeprowadzono 65 wywiadów (z czego 52 dotyczyły bardziej ENISA, a 13 głównie ECCF), przeprowadzono program ankietowy, w ramach którego otrzymano 209 odpowiedzi (z czego 70 dotyczyło ECCF), zakończono konsultacje publiczne oraz zorganizowano dwa warsztaty poświęcone analizie SWOT (mocne strony, słabe strony, szanse i zagrożenia) oraz zaleceniom, w których wzięło udział odpowiednio 26 i 70 uczestników. Działania te miały na celu zebranie opinii zainteresowanych stron w celu oceny wpływu, skuteczności i efektywności ENISA. Ostateczne sprawozdanie z *badania wspierającego ocenę Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i europejskich ram certyfikacji cyberbezpieczeństwa, przeprowadzonego dla Komisji przez PwC, Intellera Consulting i PPMI (2024),* zostało ukończone w grudniu 2024 *r.*

– **W 2025 r.** Komisja ogłosiła zaproszenie do przedstawiania dowodów. W szczególności zainteresowane strony zostały zaproszone do przedłożenia pisemnych uwag, w tym dokumentów przedstawiających stanowisko, sprawozdań technicznych lub uwag dotyczących konkretnych propozycji reform. Otrzymano łącznie 184 indywidualne uwagi od szerokiego grona zainteresowanych stron, w tym stowarzyszeń branżowych, firm zajmujących się cyberbezpieczeństwem, MŚP, instytucji akademickich i organizacji pożytku publicznego.

– **W okresie od kwietnia do czerwca 2025** r. Komisja zorganizowała konsultacje społeczne w ramach przeglądu CSA i otrzymała 193 odpowiedzi. Konsultacje obejmowały 38 pytań zamkniętych i otwartych dotyczących mandatu ENISA, ECCF, bezpieczeństwa łańcucha dostaw ICT oraz uproszczenia.

– **Konsultacje ukierunkowane (wywiady):** Przeprowadzono serię częściowo ustrukturyzowanych wywiadów z wybranymi zainteresowanymi stronami. Wśród nich znaleźli się przedstawiciele ENISA, a także krajowe organy publiczne, które opracowały krajowe platformy sprawozdawcze lub zarządzają nimi. Wywiady koncentrowały się na roli i zdolnościach ENISA, funkcjonowaniu ECCF, praktycznych wyzwaniach związanych z dostosowaniem krajowych i unijnych procesów certyfikacji, obciążeniach związanych ze sprawozdawczością oraz przeszkodach we wdrażaniu. Dyskusje te dostarczyły jakościowych spostrzeżeń, które wzbogaciły interpretację wyników konsultacji społecznych i pomogły w udoskonaleniu wariantów polityki.

– **Konsultacje z przedstawicielami państw członkowskich w ramach grupy roboczej Rady ds. bezpieczeństwa cyberprzestrzeni ([19]) oraz w ramach rozmów dwustronnych,** podczas których państwa członkowskie mogły wyrazić swoje opinie na temat przeglądu CSA.

– **Konsultacje ukierunkowane (grupy ECCF – ECCG, grupa zainteresowanych stron ds. certyfikacji w zakresie cyberbezpieczeństwa (SCCG)):** Komisja, pełniąca funkcję przewodniczącego obu grup, przedstawiła stan prac nad przeglądem CSA na posiedzeniach ECCG w dniach 12 marca i 3 lipca 2025 r. oraz na posiedzeniu SCCG w dniu 17 marca 2025 r. Ponadto za pomocą kwestionariuszy zebrano dodatkowe opinie ekspertów członków ECCG.

Konsultacje koncentrowały się na pięciu kluczowych obszarach uznanych za zasadnicze dla przyszłego funkcjonowania i spójności unijnych ram w zakresie cyberbezpieczeństwa:

- **mandat i rola operacyjna ENISA**, w tym wsparcie dla państw członkowskich i wiedza specjalistyczna w zakresie nowych technologii;
- **skuteczność europejskich ram certyfikacji w zakresie cyberbezpieczeństwa**, w tym procesy zarządzania i rozwoju;
- **złożoność i fragmentacja obowiązków w zakresie cyberbezpieczeństwa**, ze szczególnym uwzględnieniem obciążeń związanych ze sprawozdawczością i możliwością uproszczenia;
- **proporcjonalność wymogów wobec MŚP** i możliwość zróżnicowanych ścieżek zgodności; oraz
- **społeczne i gospodarcze skutki** zharmonizowanych przepisów dotyczących cyberbezpieczeństwa, w tym wpływ na konsumentów, prawa, innowacje i konkurencyjność.

- **Ocena skutków**

Przegląd CSA wraz z wnioskiem dotyczącym dyrektywy wprowadzającej ukierunkowane zmiany do dyrektywy NIS2 zostały poparte oceną skutków, której streszczenie znajduje się poniżej. Rada ds. Kontroli Regulacyjnej (RSB) wydała „pozytywną opinię z zastrzeżeniami" w sprawie ponownie przedłożonego projektu sprawozdania z oceny skutków dotyczącego przeglądu CSA[20] . Ocena skutków została dostosowana w celu uwzględnienia zaleceń i uwag RSB.

Ostateczny wniosek dotyczący polityki nie odbiega od opcji ocenionych w ocenie skutków.

Komisja przeanalizowała opcje w czterech obszarach interwencji, mając na uwadze konkretne cele, które należy osiągnąć: (1) mandat ENISA (również część obecnego CSA); (2) ECCF (również część obecnego CSA); (3) ukierunkowane zmiany do dyrektywy NIS 2, mające na celu uproszczenie, ale również powiązane z mandatem ENISA i ECCF; oraz (4) bezpieczeństwo łańcucha dostaw ICT, które ma również znaczenie zarówno dla ekosystemu NIS2, jak i dla ECCF. Każdy zestaw opcji stanowi odrębny obszar interwencji, a jednocześnie jest powiązany z innymi obszarami i ma dla nich znaczenie.

[19] Horyzontalna grupa robocza ds. cyberprzestrzeni

[20] Rozporządzenie (UE) 2019/881 (http://data.europa.eu/eli/reg/2019/881/oj)

Opcje rozwiązania problemu rozbieżności między ramami polityki Unii w zakresie cyberbezpieczeństwa a potrzebami zainteresowanych stron w coraz bardziej nieprzyjaznym środowisku

Opcja A.1: *Wyjaśnienie mandatu ENISA i ustanowienie priorytetów* – opcja ta zapewniłaby jasne i stabilne ramy dla zadań ENISA poprzez włączenie zadań określonych w innych aktach prawnych.

Wariant A.2: *Reforma mandatu ENISA* – wariant ten przewiduje uchylenie i zastąpienie CSA oraz gruntowną zmianę mandatu agencji.

Wariant A.3: *Reforma mandatu ENISA z silnym naciskiem na wsparcie operacyjne* – wariant ten opierałby się na wariancie A.2. Ponadto ENISA rozwinęłaby zdolności do bezpośredniego wspierania podmiotów objętych dyrektywą NIS 2 w reagowaniu na incydenty związane z cyberbezpieczeństwem i usuwaniu ich skutków na wniosek państwa członkowskiego.

Opcje dotyczące ECCF

Wariant B.1: *Wyjaśnienie zakresu, elementów i celów ECCF oraz wprowadzenie mechanizmu utrzymania* – wariant ten przewiduje nowy mechanizm utrzymania systemów po ich przyjęciu, który miałby być wdrażany przez ENISA.

Opcja B.2: *Reforma ECCF poprzez zmianę procedur i rozszerzenie zakresu w celu ułatwienia uproszczenia zgodności z przepisami* – opcja ta uchyla CSA i zastępuje ją nowym rozporządzeniem. Oprócz opcji B.1 zmieniono by procedury związane z wnioskowaniem, opracowywaniem i przyjmowaniem systemów w celu poprawy rozliczalności i efektywności.

Opcja B.3: *Reforma ECCF zgodnie z opcją B.2 i wprowadzenie obowiązkowej certyfikacji cyberbezpieczeństwa* – opcja ta opierałaby się na opcji B.2, ale ma na celu dalsze zwiększenie wpływu ram poprzez wprowadzenie obowiązkowej certyfikacji kluczowych podmiotów z uwzględnieniem konkretnych scenariuszy ryzyka, zamiast polegania wyłącznie na dobrowolnej certyfikacji podmiotów.

Opcje uproszczenia

Wariant C.1: *Przyjęcie podejścia opartego na instrumentach prawa miękkiego i instrumentach nielegislacyjnych, w tym wykorzystanie istniejących uprawnień (przyjęcie aktów wykonawczych na podstawie art. 21 ust. 5 i art. 23 ust. 11 dyrektywy NIS 2)* – Opcja ta przewiduje przyjęcie aktów wykonawczych z wykorzystaniem istniejących uprawnień na mocy dyrektywy NIS 2 w celu zapewnienia wyższego stopnia harmonizacji środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa, progów zgłaszania incydentów, a także rodzaju informacji, formatów i procedury powiadamiania. Przewiduje ona również przyjęcie zestawu wytycznych w celu zwiększenia pewności prawnej i zharmonizowanego wdrażania.

Wariant C.2: *Ukierunkowana interwencja – dalsze uproszczenie zgodności z odpowiednimi unijnymi ramami prawnymi w zakresie cyberbezpieczeństwa* – Wariant ten obejmuje ograniczoną interwencję poprzez zmiany w CSA i dyrektywie NIS 2 w celu uproszczenia określonych aspektów ram cyberbezpieczeństwa, w tym dostosowania zakresu, maksymalnej harmonizacji aktów wykonawczych, potwierdzania zgodności poprzez certyfikację oraz przyjęcia zestawu wytycznych przewidzianych w wariancie C.1.

Wariant C.3: *Harmonizacja środków związanych z cyberbezpieczeństwem określonych w prawodawstwie unijnym* – Wariant ten opierałby się na wariancie C.2 i znosiłby wszystkie środki zarządzania ryzykiem cyberbezpieczeństwa zawarte w przepisach sektorowych oraz uprawnienia związane z takimi środkami. Zamiast tego ekosystem dyrektywy NIS 2 zostałby

zmieniony w celu zapewnienia uproszczonych wymogów dla wszystkich rodzajów podmiotów, co miałoby na celu promowanie harmonizacji.

Opcje dotyczące bezpieczeństwa łańcucha dostaw ICT

Wariant D.1: Przyjęcie *podejścia opartego na miękkim prawie w celu przeciwdziałania zagrożeniom dla cyberbezpieczeństwa łańcuchów dostaw ICT* – wariant ten nie przewiduje interwencji regulacyjnej na szczeblu UE. Zamiast tego Komisja zwiększyłaby liczbę skoordynowanych ocen ryzyka i dobrowolnych zestawów narzędzi.

Opcja D.2: *Ad hoc interwencja regulacyjna kodyfikująca zestaw narzędzi 5G* – opcja ta kodyfikowałaby środki zawarte w zestawie narzędzi 5G. Wprowadzałaby ona obowiązek zapewnienia przez państwa członkowskie, aby komponenty pochodzące od dostawców wysokiego ryzyka nie były wykorzystywane w kluczowych elementach sieci.

Wariant D.3: *Kompleksowe i horyzontalne ramy prawne dotyczące przeciwdziałania zagrożeniom dla cyberbezpieczeństwa łańcuchów dostaw ICT* – wariant ten ustanowiłby horyzontalne, neutralne pod względem technologicznym i sektorowym ramy prawne dotyczące przeciwdziałania nietechnicznym zagrożeniom dla cyberbezpieczeństwa w łańcuchach dostaw ICT.

Po przeprowadzeniu szczegółowej analizy jako preferowany pakiet polityczny wybrano następującą kombinację opcji*:* opcja A.2 (reforma mandatu ENISA); opcja B.2 (zreformowanie ECCF poprzez zmianę jego procedur i rozszerzenie zakresu działania w celu ułatwienia uproszczenia zgodności z przepisami); oraz opcja C.2 (ukierunkowana interwencja – dalsze uproszczenie zgodności z odpowiednimi unijnymi ramami prawnymi w zakresie cyberbezpieczeństwa) oraz opcja D.3 – kompleksowe i horyzontalne ramy dotyczące przeciwdziałania zagrożeniom dla cyberbezpieczeństwa w łańcuchach dostaw ICT.

Kombinacja ta stanowi dobrze wyważoną odpowiedź na zidentyfikowane wyzwania polityczne, znacznie zwiększając skuteczność, efektywność i spójność w całej Unii.

Przejście na proponowaną preferowaną opcję ram regulacyjnych będzie wiązało się z kosztami zarówno dla ENISA w związku z realizacją nowych zadań (szacowanych na maksymalnie 161,3 mln EUR w ciągu pięciu lat), jak i dla organów publicznych w całej Unii w związku z nadzorem (szacowanych na maksymalnie 80 mln EUR w ciągu pięciu lat, z uwzględnieniem odpowiednich oszczędności kosztów). W odniesieniu do przedsiębiorstw, w ciągu pięciu lat wycofanie określonego sprzętu wysokiego ryzyka może spowodować roczne koszty w wysokości od 3,4 do 4,3 mld EUR dla operatorów sieci komórkowych, podczas gdy inwestycje w zaufanych dostawców mogą wzrosnąć do 2 mld EUR rocznie.

Jednocześnie oczekuje się, że usprawnienie i ograniczenie obowiązków w zakresie zgodności przyniesie przedsiębiorstwom oszczędności w wysokości do 15,3 mld EUR w ciągu pięciu lat. Ponadto poprawa ogólnej pozycji Unii w zakresie cyberbezpieczeństwa i suwerenności technologicznej oraz stymulowanie innowacyjności i konkurencyjności przyniosłyby znaczne korzyści ogółowi społeczeństwa, organom publicznym i przedsiębiorstwom. Oczekuje się, że w perspektywie długoterminowej zrównoważy to w znacznym stopniu początkowe wydatki.

Dzięki zmniejszeniu fragmentacji rynku i harmonizacji wymogów regulacyjnych preferowane warianty zwiększają równość konkurencji w całej Unii, zapewniając przedsiębiorstwom jaśniejsze ścieżki do osiągnięcia zgodności z przepisami i wprowadzania innowacji.

Preferowane warianty przyczyniłyby się również do uproszczenia dzięki jasnym wytycznym i zintegrowanym systemom, zmniejszając obciążenia administracyjne. Warianty te są zgodne z zasadą „jedno wchodzi, jedno wychodzi”, zapewniając, że nowe obowiązki są równoważone przez ograniczenia w innych obszarach.

- **Adekwatność regulacyjna i uproszczenie**

Dzięki wybranym opcjom politycznym A.2, B.2, C.2 i D.3 zmiana CSA w znacznym stopniu przyczynia się do poprawy przejrzystości, usunięcia nieefektywności i ujednolicenia procedur w ramach ram prawnych. Mówiąc konkretniej, opcja A.2 proponuje pełną reformę mandatu ENISA, skutecznie wspierającą wdrażanie polityki i współpracę operacyjną między państwami członkowskimi. Konsolidacja ta pomoże również wyeliminować fragmentaryczne praktyki, poprawiając koordynację, a jednocześnie obniżając koszty zgodności i koszty operacyjne w perspektywie długoterminowej. Wariant B.2, który obejmuje uchylenie obecnego CSA i wprowadzenie zreformowanego ECCF, zwiększa efektywność poprzez zmianę modelu zarządzania i wspieranie bardziej przewidywalnych, spójnych i elastycznych procedur certyfikacji. Umożliwi to szybsze przyjęcie systemu i lepsze dostosowanie do przepisów przekrojowych, zmniejszając fragmentację regulacyjną i zmniejszając obciążenia zarówno dla podmiotów publicznych, jak i prywatnych ( ). Wariant C.2 zmniejsza koszty zapewnienia zgodności dla podmiotów podlegających odpowiednim przepisom Unii w zakresie cyberbezpieczeństwa poprzez zmiany zakresu oraz umożliwienie wprowadzenia organizacyjnych systemów certyfikacji cyberbezpieczeństwa dla podmiotów objętych dyrektywą NIS 2 i innymi aktami prawnymi. Podejście to znacznie uprości obowiązki regulacyjne dla podmiotów podlegających wielu wymogom i zapewni bardziej efektywne wykorzystanie zasobów przez organy krajowe. Wariant D.3 tworzy zharmonizowane ramy pozwalające przeciwdziałać ryzyku nietechnicznemu wpływającemu na łańcuchy dostaw ICT, zmniejszając obecne rozdrobnienie podejść w poszczególnych państwach członkowskich. Warianty te łącznie stanowią znaczne uproszczenie i modernizację unijnych ram prawnych w zakresie cyberbezpieczeństwa, w pełni zgodne z zasadami REFIT dotyczącymi jasności, skuteczności i gotowości cyfrowej.

Wniosek jest zgodny z „cyfrową kontrolą”, ponieważ kładzie nacisk na usprawnione procesy cyfrowe, co świadczy o zaangażowaniu Unii w podejście oparte na cyfryzacji, zapewniające szybszą i bardziej niezawodną wymianę danych oraz podejmowanie decyzji. Wariant D.3 mógłby również mieć duży wpływ na cyfryzację, ponieważ wiązałby się z wymianą komponentów pochodzących od podmiotów mających siedzibę w państwach trzecich lub kontrolowanych przez podmioty z państw trzecich budzących obawy w zakresie cyberbezpieczeństwa (dostawcy wysokiego ryzyka).

- **Prawa podstawowe**

Wniosek ustawodawczy został oceniony pod kątem jego potencjału w zakresie wzmacniania lub zagrażania prawom podstawowym oraz promowania równości i zaufania, ze szczególnym uwzględnieniem skutków społecznych i praw, w tym prywatności, ochrony danych oraz zdolności osób fizycznych do zrozumienia, wykonywania i egzekwowania swoich praw.

Rozszerzenie mandatu ENISA przyczyni się do zwiększenia cyberodporności całej gospodarki i społeczeństwa, co doprowadzi do lepszej ochrony prywatności i danych osobowych obywateli. Wniosek będzie również wspierał edukację i szkolenia w zakresie cyberbezpieczeństwa, ponieważ wyjaśnia rolę ENISA w rozwoju umiejętności pracowników zajmujących się cyberbezpieczeństwem.

Ponadto ECCF zwiększy zaufanie ogółu społeczeństwa i przedsiębiorstw w Unii do certyfikowanych rozwiązań ICT, które wspierają codzienne życie. Wprowadzenie dodatkowych systemów zwiększyłoby ten wpływ.

Wniosek przyczynia się do zwiększenia zaufania obywateli poprzez zachęcanie podmiotów w sektorach krytycznych do uzyskania certyfikatu cyberbezpieczeństwa, a tym samym publicznego wykazania wysokiego poziomu cyberbezpieczeństwa. Ponadto poprzez zapewnienie zharmonizowanego zgłaszania incydentów związanych z oprogramowaniem ransomware oraz podjęcie działań na rzecz przejścia na kryptografię postkwantową, wniosek zwiększyłby zaufanie publiczne do ochrony danych wrażliwych w sektorach krytycznych.

Przepisy dotyczące bezpieczeństwa łańcucha dostaw będą miały pewien wpływ na ochronę praw podstawowych poprzez ograniczenie ingerencji zagranicznej. Działania takie jak szpiegostwo i inwigilacja poważnie naruszają prawa podstawowe obywateli. Te horyzontalne ramy mogłyby poprawić zaufanie, bezpieczeństwo i prywatność w różnych technologiach i rozwiązaniach cyfrowych.

4. SKUTKI DLA BUDŻETU

Szacowany budżet Agencji ds. Bezpieczeństwa Sieci i Informacji UE (ENISA), która przyczyni się do znacznego zwiększenia bezpieczeństwa UE, został oszacowany na 341 mln EUR na 7 lat, co daje średni roczny budżet w wysokości 49 mln EUR (prognoza na lata 2028–2034). Stanowi to wzrost o 81,5 % w stosunku do budżetu Agencji w 2025 r. Korzyści wynikające z proponowanej inicjatywy, przeanalizowane w ocenie skutków, będą znaczące i wyniosą do 14,6 mld EUR oszczędności w zakresie ograniczania kosztów (cost-) dla przedsiębiorstw. Ponadto, chociaż skala potencjalnych oszczędności kosztów związanych z ogólną poprawą gotowości Unii na wypadek incydentów związanych z cyberbezpieczeństwem jest z natury trudna do oszacowania, szacuje się, że oszczędności kosztów związane z szybszym reagowaniem i spowolnieniem rozprzestrzeniania się incydentów związanych z cyberbezpieczeństwem mogą wynieść od 3,7 do 4,4 mld EUR w ciągu pięciu lat. W kontekście przyszłych inicjatyw politycznych Komisja przyjrzy się ogólnemu rozkładowi zasobów przeznaczonych dla europejskich instytucji, organów, agencji i urzędów w dziedzinie cyberbezpieczeństwa oraz rozkładowi tych zasobów w ramach tych instytucji, organów, agencji i urzędów, aby wykorzystać wiedzę i doświadczenie oraz zidentyfikować i rozwinąć synergie.
Dodatkowe zasoby proponowane w celu wzmocnienia Agencji przekładają się na 118 etatów w przeliczeniu na pełne etaty oraz dodatkowe koszty operacyjne, które pokryją bieżące umowy o wkładzie między ENISA a Komisją, takie jak utrzymanie jednolitej platformy sprawozdawczej; etaty związane z funkcjonowaniem i administracją rezerwy UE ds. cyberbezpieczeństwa, a także ważne inicjatywy Komisji, takie jak opracowanie jednolitego punktu kontaktowego w ramach wniosku dotyczącego pakietu „Digital Omnibus”. Inne koszty operacyjne są związane ze skoordynowanym programem ujawniania luk w zabezpieczeniach, gromadzeniem i analizą informacji o zagrożeniach dla cyberbezpieczeństwa, bezpieczną komunikacją i budowaniem dojrzałości cyberbezpieczeństwa dla ENISA. Koszty operacyjne związane z utrzymaniem europejskich systemów certyfikacji cyberbezpieczeństwa, autoryzacji umiejętności w zakresie cyberbezpieczeństwa i usług związanych z narzędziami testowymi również zostały uwzględnione w tym budżecie, jednak koszty te obejmują również mechanizmy samofinansowania poprzez opłaty.

Ważnym aspektem wniosku jest wprowadzenie mechanizmów opłat, które oprócz innych celów politycznych przyczynią się również do zrównoważonego obiegu finansowego w ramach Agencji. W zmienionym CSA przedstawiono trzy rodzaje opłat, które będą zasilać budżet ENISA, a mianowicie opłaty za wydawanie certyfikatów potwierdzających umiejętności,

opłaty za usługi związane z narzędziami testowymi oraz opłaty za wsparcie utrzymania europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa. Oczekiwane korzyści dla budżetu UE szacuje się na około 18,5 mln EUR w okresie 7 lat od 2028 r. do 2034 r.

Wniosek budżetowy Komisji przekłada się na 50 dodatkowych etatów w przeliczeniu na pełne etaty, które będą realizować ramy dotyczące łańcucha dostaw, a także zadania związane między innymi z opracowywaniem aktów wykonawczych dotyczących mechanizmów opłat, utrzymaniem systemów certyfikacji, normalizacją i wsparciem współpracy operacyjnej. Oczekuje się, że na koszty ponoszone przez Komisję w związku z wdrażaniem ram dotyczących łańcucha dostaw szczególny wpływ będzie miała liczba ocen własności i kontroli (OCA), które Komisja będzie przeprowadzać. Wyniki tego zadania przyczynią się jednak w znacznym stopniu do oszczędności dla państw członkowskich w zakresie nadzorowania wdrażania środków łagodzących i obowiązków nałożonych na podmioty NIS2 przez ramy. Państwa członkowskie będą mogły bezpośrednio wykorzystać wyniki ocen OCA, zamiast indywidualnie wydawać środki na te same potrzeby w zakresie ocen.

Więcej szczegółowych informacji można znaleźć w karcie finansowej dołączonej do pakietu cyberbezpieczeństwa.

5. INNE ELEMENTY

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

Komisja będzie monitorować stosowanie proponowanego rozporządzenia i co pięć lat przedkładać Parlamentowi Europejskiemu i Radzie sprawozdanie z jego oceny. Sprawozdania te będą podawane do wiadomości publicznej i będą zawierały szczegółowe informacje na temat skutecznego stosowania i egzekwowania proponowanego rozporządzenia.

- **Dokumenty wyjaśniające (w przypadku dyrektyw)**

Nie dotyczy, ponieważ wniosek ma charakter rozporządzenia.

- **Szczegółowe wyjaśnienie poszczególnych przepisów wniosku**

We wniosku wyjaśniono rolę ENISA i powierzono jej konkretne zadania w zakresie wspierania zainteresowanych stron, w szczególności państw członkowskich, zwłaszcza w odniesieniu do wsparcia we wdrażaniu polityki i prawodawstwa Unii, współpracy operacyjnej, budowania potencjału, certyfikacji i normalizacji w zakresie cyberbezpieczeństwa oraz poprawy jakości kadr zajmujących się cyberbezpieczeństwem i ich mobilności w całej Unii. Wniosek ma również na celu zwiększenie skuteczności i efektywności europejskich ram certyfikacji w zakresie cyberbezpieczeństwa (ECCF) w celu poprawy poziomu cyberbezpieczeństwa w Unii oraz umożliwienia klientom dokonywania świadomych wyborów przy zakupie produktów, usług, procesów i zarządzanych usług bezpieczeństwa ICT na rynku wewnętrznym. Ponadto, w połączeniu z wnioskiem dotyczącym dyrektywy wprowadzającej ukierunkowane zmiany do dyrektywy NIS 2, niniejszy 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. Wreszcie wniosek odpowiada na potrzebę zwiększenia odporności gospodarki Unii i łańcucha dostaw ICT w celu promowania jej bezpieczeństwa i konkurencyjności. Szczegóły przedstawiono poniżej.

TYTUŁ I: PRZEPISY OGÓLNE

Tytuł I proponowanego rozporządzenia zawiera przepisy ogólne: przedmiot (art. 1) i definicje (art. 2), w tym odniesienia do odpowiednich definicji zawartych w innych instrumentach unijnych, takich jak dyrektywa (UE) 2022/2555[21] (dyrektywa NIS 2), rozporządzenie (WE) nr 765/2008[22] oraz rozporządzenie (UE) nr 1025/2012[23] .

TYTUŁ II: ENISA (AGENCJA UNII EUROPEJSKIEJ DS. CYBERBEZPIECZEŃSTWA)

Tytuł II proponowanego rozporządzenia zawiera kluczowe przepisy dotyczące ENISA.

W rozdziale I określono misję (art. 3) i cele ENISA (art. 4).

W rozdziale II w trzech sekcjach określono zadania Agencji.

Sekcja 1 zawiera przepisy dotyczące zadań związanych ze wspieraniem wdrażania polityki i prawa Unii. Określa ona, które podmioty i organizacje mają otrzymać wsparcie oraz w jaki sposób powinno ono być udzielane (art. 5). W art. 6 określono obowiązki Agencji w zakresie budowania potencjału, w tym oferowania państwom członkowskim wiedzy i doświadczenia w zakresie zapobiegania cyberzagrożeniom i przeciwdziałania im, aktualizowania strategii w zakresie cyberbezpieczeństwa oraz zwiększania liczby pracowników zajmujących się cyberbezpieczeństwem. ENISA będzie również wspierać państwa członkowskie w działaniach uświadamiających (art. 7) oraz przeprowadzać analizy głównych trendów rynkowych w zakresie cyberbezpieczeństwa i rozpowszechniać porady techniczne i analizy (art. 8). ENISA będzie również przyczyniać się do współpracy międzynarodowej w zakresie cyberbezpieczeństwa i promować ją, zgodnie z opisem w art. 9.

W sekcji 2 określono zadania ENISA w zakresie współpracy operacyjnej z państwami członkowskimi, podmiotami unijnymi i CERT-EU, siecią zespołów reagowania na incydenty związane z bezpieczeństwem komputerowym (CSIRT), EU-CyCLONe i innymi zainteresowanymi stronami, w tym wydawanie wytycznych i wdrażanie bezpiecznych narzędzi komunikacyjnych (art. 10). ENISA będzie również pomagać w poprawie świadomości sytuacyjnej w zakresie cyberzagrożeń i incydentów, między innymi poprzez tworzenie jednego lub kilku repozytoriów informacji o cyberzagrożeniach, przeprowadzanie analiz i wydawanie wczesnych ostrzeżeń (art. 11). Zasady dotyczące takich wczesnych ostrzeżeń (treść, terminy, usługi) określono w art. 12. Aby pomóc podmiotom o znaczeniu istotnym i ważnym dla funkcjonowania UE ( ) w przygotowaniu się na incydenty związane z oprogramowaniem ransomware, reagowaniu na nie i usuwaniu ich skutków, ENISA będzie zarządzać rezerwą UE ds. cyberbezpieczeństwa, zgodnie z art. 13 i we współpracy z Europolem i zespołami CSIRT lub innymi właściwymi organami, stosownie do przypadku. Artykuł 14 zawiera przepisy dotyczące roli ENISA w ćwiczeniach z zakresu cyberbezpieczeństwa na poziomie Unii, w tym w opracowywaniu rocznego programu ćwiczeń z zakresu cyberbezpieczeństwa na poziomie Unii. Oprócz tych zadań ENISA powinna zapewnić narzędzia i platformy, w szczególności jednolitą platformę zgłaszania incydentów ustanowioną zgodnie z art. 16 ust. 1 rozporządzenia (UE) 2024/2847 (art. 15). Wreszcie agencja musi opracować wspólną unijną zdolność w zakresie usług zarządzania podatnością na zagrożenia i świadczyć usługi zarządzania podatnością na zagrożenia (art. 16).

W sekcji 3 dotyczącej certyfikacji i normalizacji w zakresie cyberbezpieczeństwa określono zadania Agencji w tym zakresie. W art. 17 opisano rolę ENISA w opracowywaniu i wdrażaniu

21 http://data.europa.eu/eli/dir/2022/2555/oj
22 http://data.europa.eu/eli/reg/2008/765/oj
23 http://data.europa.eu/eli/reg/2012/1025/oj

ECCF, w tym jej wiodącą rolę w przygotowywaniu systemów oraz zapewnianiu ich utrzymania i budowania potencjału, natomiast w art. 18 określono, w jaki sposób ENISA powinna angażować się w opracowywanie specyfikacji technicznych i przyczyniać się do działań normalizacyjnych na szczeblu europejskim i międzynarodowym, w tym w dziedzinie algorytmów kryptograficznych.

W sekcji 4 szczegółowo opisano zadania Agencji dotyczące wdrażania Akademii Umiejętności w zakresie Cyberbezpieczeństwa. Artykuł 19 zawiera przepisy dotyczące roli ENISA w odniesieniu do europejskich ram umiejętności w zakresie cyberbezpieczeństwa (ECSF), natomiast jej zadania dotyczące opracowywania i utrzymywania europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa określono w art. 20. Wymogi dotyczące uzyskania statusu autoryzowanego dostawcy certyfikatów określono w art. 21, a wymogi dotyczące rozpatrywania wniosków – w art. 22. ENISA musi udostępniać informacje publiczne dotyczące ECSF i indywidualnych certyfikatów umiejętności w zakresie cyberbezpieczeństwa (art. 23).

Rozdział III dotyczy organizacji ENISA. Struktura administracyjna i zarządcza Agencji obejmuje również zastępcę dyrektora wykonawczego (art. 24). Przepisy dotyczące zarządu, jego składu, przewodniczącego, posiedzeń, funkcji i zasad głosowania zawarto w sekcji 1 (art. 25–29). Rada wykonawcza musi wspierać zarząd zgodnie z art. 30 sekcji 2. Sekcja 3 zawiera zasady dotyczące mianowania, odwołania i przedłużenia kadencji dyrektora wykonawczego (art. 31) oraz zasady dotyczące zadań i obowiązków dyrektora wykonawczego (art. 32). Zarząd może podjąć decyzję o utworzeniu stanowiska zastępcy dyrektora wykonawczego, który będzie wspierał dyrektora wykonawczego (sekcja 4, art. 33 i 34). Zarząd musi powołać grupę doradczą ENISA, która ma obowiązek doradzać ENISA zgodnie z zasadami określonymi w art. 35. Sekcja 6 zawiera zasady dotyczące utworzenia i składu komisji odwoławczej (art. 36) oraz jej członków (art. 37). W art. 38 określono okoliczności, w których członkowie komisji odwoławczej muszą wstrzymać się od udziału w postępowaniu odwoławczym, oraz przedstawiono podstawy do zgłoszenia sprzeciwu wobec członka komisji. Odwołania od decyzji podjętych przez ENISA lub w przypadku zaniechania działania przez ENISA można wnosić do komisji odwoławczej (art. 39). Artykuł 40 zawiera przepisy dotyczące osób uprawnionych do wniesienia odwołania, terminu i formy odwołania. Artykuły 41–43 określają zasady dotyczące rewizji międzyinstancyjnej, rozpatrywania decyzji w sprawie odwołań oraz działań przed Trybunałem Sprawiedliwości. Wreszcie art. 44 przewiduje proces związany z jednolitym dokumentem programowym.

Rozdział IV dotyczy ustanowienia i struktury budżetu Agencji, a także zasad dotyczących jego przedstawiania i wykonania (art. 45–55). Zawiera on również przepisy ułatwiające zwalczanie nadużyć finansowych, korupcji i innych niezgodnych z prawem działań (art. 51).

Rozdział V dotyczy zatrudnienia w Agencji. Zawiera on przepisy ogólne dotyczące regulaminu pracowniczego i warunków zatrudnienia innych pracowników oraz zasady dotyczące przywilejów i immunitetów (art. 56 i 57). Wprowadza on przepisy wymagające od państw członkowskich wyznaczenia oficerów łącznikowych ds. jako oddelegowanych ekspertów krajowych do ENISA oraz określa ich rolę w Agencji (art. 58). Zawiera on również przepisy dotyczące wykorzystania oddelegowanych ekspertów krajowych i innych pracowników niebędących zatrudnionymi przez Agencję (art. 59).

Wreszcie rozdział VI zawiera przepisy ogólne dotyczące Agencji. Określa on jej status prawny (art. 60), ustanawia siedzibę (art. 61) i zawiera przepisy dotyczące umowy w sprawie siedziby Agencji i warunków jej funkcjonowania oraz kontroli administracyjnej sprawowanej przez

Rzecznika Praw Obywatelskich (art. 62 i 63). Zawiera przepisy regulujące kwestie odpowiedzialności, ustalenia językowe i ochronę danych osobowych (art. 64–66), a także zasady bezpieczeństwa dotyczące ochrony informacji szczególnie chronionych nieobjętych klauzulą tajności i informacji niejawnych (art. 67). Określa zasady współpracy z podmiotami unijnymi i organami krajowymi (art. 68) oraz innymi zainteresowanymi stronami (art. 69). Opisuje zasady regulujące współpracę Agencji z państwami trzecimi i organizacjami międzynarodowymi (art. 70).

TYTUŁ III: EUROPEJSKIE RAMY CERTYFIKACJI CYBERBEZPIECZEŃSTWA

W tytule III proponowanego rozporządzenia ustanawia się ECCF.

W rozdziale I przedstawiono cele, zakres i procedury ramowe. Cele (art. 71) obejmują wzmocnienie cyberbezpieczeństwa w całej Unii oraz ułatwienie zharmonizowanego podejścia do certyfikacji produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów. Ramy powinny również wykorzystywać certyfikację w celu uproszczenia zgodności z obowiązującym prawodawstwem unijnym poprzez domniemanie zgodności, zmniejszając tym samym obciążenia dla przedsiębiorstw (art. 78). W rozdziale I szczegółowo opisano następnie aspekty proceduralne, począwszy od konsultacji w sprawie strategicznych priorytetów europejskiej certyfikacji w zakresie cyberbezpieczeństwa i informacji publicznych związanych z opracowaniem systemu przez Komisję oraz utworzeniem nowego Europejskiego Zgromadzenia ds. Certyfikacji w zakresie Cyberbezpieczeństwa (art. 72). W odpowiedzi na szczegółowy wniosek Komisji (art. 73) ENISA ma przedstawić projekt systemu w ciągu 12 miesięcy. Artykuł 74 przewiduje dodatkowe terminy związane z przedłożeniem opinii ECCG i przedłożeniem systemu w celu jego przyjęcia przez Komisję. Artykuł 75 wprowadza jasny mechanizm utrzymania istniejących systemów, który może prowadzić do ich przeglądu (art. 76). Przegląd systemu może być dodatkowo uzupełniony okresową oceną skuteczności systemu i jego wpływu na jednolity rynek. Artykuł 77 stanowi podstawę dla ENISA do opracowania specyfikacji technicznych wspierających opracowywanie i utrzymywanie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa. Przyjmując lub dokonując przeglądu systemu, Komisja może zamieścić odniesienia do takich specyfikacji technicznych (art. 74). Różnorodne procedury zapewniają przejrzystość i jakość realizacji poprzez zaangażowanie ekspertów i ogólnych zainteresowanych stron na różnych etapach planowania, opracowywania, przyjmowania i utrzymywania systemów certyfikacji. Artykuł 79 przewiduje utworzenie specjalnej strony internetowej ENISA poświęconej europejskim systemom certyfikacji w zakresie cyberbezpieczeństwa, która powinna zawierać informacje na temat przyjętych systemów, a także europejskich certyfikatów cyberbezpieczeństwa i unijnych oświadczeń o zgodności wydanych w ramach tych systemów.

W rozdziale II określono ogólne zasady dotyczące treści europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa.

W art. 80 określono wykaz celów bezpieczeństwa, zgodnie z którymi ENISA ma opracować system, oraz zapewniono zgodność z odpowiednimi przepisami dotyczącymi cyberbezpieczeństwa. Każdy europejski system certyfikacji cyberbezpieczeństwa może przewidywać elementy określone w art. 81. Elementy te muszą być zgodne z przepisami unijnymi i mogą być zharmonizowane w ramach różnych systemów przy użyciu przepisów modelowych. Oba przepisy zapewniają niezbędną elastyczność, aby dostosować się do różnych rodzajów systemów . Dodatkowe przepisy określają zasady dotyczące poziomów zapewnienia (art. 82) i samooceny zgodności (art. 83). W rozdziale tym określono również wykaz informacji

uzupełniających (art. 84), które muszą być udostępnione przez producenta lub dostawcę produktów, usług lub procesów ICT.

Wreszcie w rozdziale III ustanawia się zasady zarządzania ECCF, podzielone na trzy sekcje.

Sekcja 1 dotyczy zasad wydawania europejskich certyfikatów cyberbezpieczeństwa, w tym certyfikatów o wysokim poziomie zapewnienia (art. 85). Ponadto określa ona zasady harmonizacji europejskich systemów certyfikacji cyberbezpieczeństwa z krajowymi systemami certyfikacji cyberbezpieczeństwa i certyfikatami cyberbezpieczeństwa (art. 86) oraz przewiduje możliwość międzynarodowego uznawania europejskich certyfikatów cyberbezpieczeństwa w oparciu o zasadę równoważności (art. 87). W sekcji tej nakreślono również rolę krajowych organów certyfikacji w zakresie cyberbezpieczeństwa i zasady mające do nich zastosowanie (art. 88) oraz określono zasady dotyczące mechanizmu wzajemnej oceny między tymi organami, zapewniającego równoważne standardy w całej Unii (art. 89), a także współpracy między tymi organami w ramach ECCG (art. 90).

Sekcja 2 zawiera: (i) zharmonizowane zasady dotyczące akredytacji i upoważniania jednostek oceniających zgodność (art. 91–92); (ii) zasady powiadamiania, w tym uprawnienia do zapewnienia dalszego dostosowania do odpowiedniego prawa Unii i NLF (art. 93); oraz (iii) procedurę odwoławczą (art. 94) zapewniającą przestrzeganie wymogów dotyczących jednostek oceniających zgodność.

Wreszcie sekcja 3 określa prawa i środki odwoławcze dotyczące decyzji związanych z certyfikacją (art. 96) oraz nakłada na państwa członkowskie obowiązek ustanowienia i egzekwowania proporcjonalnych sankcji za naruszenia przepisów.

TYTUŁ IV

W rozdziale I art. 98 określono zakres ram zaufanego łańcucha dostaw ICT. Ramy te będą dotyczyły ryzyka nietechnicznego w sektorach o wysokim znaczeniu krytycznym i innych sektorach krytycznych, o których mowa w dyrektywie (UE) 2022/2555. Mechanizm ten pozwoli zidentyfikować kluczowe zasoby ICT w krytycznych łańcuchach dostaw ICT oraz określić odpowiednie i proporcjonalne środki ograniczające ryzyko w odniesieniu do rodzajów podmiotów, o których mowa w załączniku I i załączniku II do dyrektywy (UE) 2022/2555. Ramy te będą oparte na skoordynowanych ocenach ryzyka bezpieczeństwa na poziomie Unii, o które zwróci się Komisja lub co najmniej trzy państwa członkowskie. W art. 99 szczegółowo opisano, w jaki sposób będą przeprowadzane te oceny ryzyka, oraz że powinny one również określać środki ograniczające ryzyko. Oceny ryzyka powinny zostać zakończone w ciągu sześciu miesięcy od złożenia wniosku. Na wniosek Komisji grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji może uzgodnić krótszy termin. Ramy przewidują możliwość zastosowania procedury nadzwyczajnej, jeżeli natychmiastowa interwencja jest uzasadniona w celu zachowania prawidłowego funkcjonowania rynku wewnętrznego i jeżeli Komisja ma wystarczające powody, aby uznać, że istnieje poważne zagrożenie cybernetyczne dla bezpieczeństwa Unii w odniesieniu do krytycznych łańcuchów dostaw ICT. W takim przypadku Komisja konsultuje się z państwami członkowskimi w sprawie konieczności podjęcia jednego lub kilku środków łagodzących i przeprowadza ocenę ryzyka. Artykuł 100 stanowi, że jeżeli w wyniku oceny ryzyka, o której mowa w art. 99, lub na podstawie innych źródeł, takich jak publiczne oświadczenie w imieniu Unii lub państwa członkowskiego, okaże się, że państwo trzecie stwarza poważne i strukturalne zagrożenia nietechniczne dla łańcuchów dostaw ICT, Komisja weryfikuje zagrożenie stwarzane przez to państwo, biorąc pod uwagę elementy wymienione w art. 100. W przypadku gdy Komisja stwierdzi, że pa ie stanowi

poważne i strukturalne ryzyko nietechniczne dla łańcuchów dostaw ICT, art. 100 przewiduje procedurę, zgodnie z którą Komisja może uznać takie pa ie za pa ie stwarzające zagrożenie dla cyberbezpieczeństwa łańcuchów dostaw ICT. Podmioty mające siedzibę w państwie trzecim stwarzającym zagrożenie dla cyberbezpieczeństwa, wyznaczonym zgodnie z niniejszym artykułem, lub kontrolowane przez takie państwo trzecie, przez podmiot mający siedzibę w takim państwie trzecim lub przez obywatela takiego państwa trzeciego, nie będą mogły prowadzić szeregu działań określonych w niniejszym artykule. Artykuł 101 przewiduje ogólny mechanizm dotyczący łańcucha dostaw ICT, zgodnie z którym po zakończeniu oceny ryzyka dla bezpieczeństwa przeprowadzonej przez grupę ds. współpracy w zakresie bezpieczeństwa sieci i informacji lub przez Komisję zgodnie z art. 99 Komisja może podjąć środki przewidziane w art. 102 i 103.

Komisja może określić, w drodze aktów wykonawczych, kluczowe aktywa ICT wykorzystywane do wytwarzania produktów i świadczenia usług przez rodzaje podmiotów, o których mowa w załączniku I i załączniku II do dyrektywy (UE) 2022/2555. W art. 102 szczegółowo określono elementy, które należy uwzględnić przy identyfikacji kluczowych aktywów ICT. W art. 103 ustanowiono potencjalne środki łagodzące w łańcuchu dostaw ICT. Komisja może w drodze aktów wykonawczych zdecydować, że podmioty działające w sektorach o wysokim znaczeniu krytycznym i innych sektorach krytycznych muszą podlegać szczególnym środkom ograniczającym ryzyko, które zostały szczegółowo określone w tym artykule.

Komisja, w drodze aktów wykonawczych, ustanawia wykazy dostawców wysokiego ryzyka, których dotyczą zakazy określone w aktach wykonawczych przyjętych zgodnie z art. 103 ust. 1, art. 103 ust. 7 lub zakazem, o którym mowa w art. 110 ust. 1, po przeprowadzeniu oceny siedziby, własności i kontroli. Powinna ona konsultować się z zainteresowanymi dostawcami i właściwymi organami (art. 104).

Podmiot mający siedzibę w państwie trzecim lub kontrolowany przez podmioty z państwa trzeciego budzącego obawy w zakresie cyberbezpieczeństwa, wyznaczony zgodnie z art. 100, może wystąpić z wnioskiem o zezwolenie na dostarczanie komponentów ICT do kluczowych zasobów ICT podmiotów, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, oraz o udział w zamówieniach publicznych dotyczących dostawy takich komponentów ICT. W art. 105 określono, co powinno zawierać takie wniosku oraz jaka jest procedura udzielania takiego zwolnienia. W art. 106 określono prawa do obrony przysługujące danemu podmiotowi. Komisja prowadzi publicznie dostępny rejestr decyzji dotyczących zwolnień (art. 107). W art. 108 i 109 określono zasady poufności i opłaty związane z procedurą udzielania zwolnień.

W rozdziale II przewidziano zastosowanie ram zaufanego łańcucha dostaw ICT do mobilnych, stacjonarnych i satelitarnych sieci łączności elektronicznej, zapewniając zgodność z proponowaną ustawą o sieciach cyfrowych.

Kluczowe zasoby ICT dla mobilnych, stacjonarnych i satelitarnych sieci łączności elektronicznej są określone w załączniku II. Okres przejściowy na wycofanie komponentów ICT od dostawców wysokiego ryzyka w odniesieniu do kluczowych zasobów ICT mobilnej sieci łączności elektronicznej nie może przekraczać 36 miesięcy od wejścia w życie niniejszego rozporządzenia. Okresy przejściowe dla stacjonarnych i satelitarnych sieci łączności elektronicznej określa Komisja w drodze aktów wykonawczych. Komisja jest uprawniona do przyjęcia aktu delegowanego w celu zmiany wyznaczonych kluczowych aktywów ICT i okresów przejściowych, w tym dla przyszłych generacji sieci komórkowych (art. 110). Artykuł 111 stanowi, że dostawcy sieci łączności elektronicznej, zarówno komórkowej, stacjonarnej, jak i satelitarnej, nie mogą w żadnej formie wykorzystywać, instalować ani integrować

komponentów ICT pochodzących od dostawców wysokiego ryzyka i nie mogą uzyskać ogólnego ani indywidualnego zezwolenia.

Właściwe organy, nadzór i egzekwowanie, jurysdykcja, prawo do obrony (rozdział III)

W rozdziale III określono ponadto zasady dotyczące właściwych organów, nadzoru i egzekwowania oraz jurysdykcji.

W art. 112–114 określono uprawnienia, środki i obowiązki państw członkowskich w zakresie zapewnienia wdrożenia i egzekwowania przepisów tytułu IV. Państwa członkowskie muszą wyznaczyć co najmniej jeden właściwy organ, o czym powiadamiają Komisję. W art. 113 przewidziano, że Komisja utworzy sieć współpracy między właściwymi organami państw członkowskich a Komisją w celu ułatwienia przestrzegania przepisów, natomiast w art. 114 określono środki nadzoru i egzekwowania, które właściwe organy są uprawnione do podejmowania. Kary w przypadku naruszenia przepisów tytułu IV określono w art. 115. W art. 116 wyszczególniono możliwość wzajemnej pomocy państw członkowskich w przypadku podmiotów prowadzących działalność transgraniczną lub gdy ich kluczowe zasoby ICT znajdują się w kilku państwach członkowskich. W art. 117 określono zasady dotyczące jurysdykcji i terytorialności.

TYTUŁ VI: PRZEPISY KOŃCOWE

Tytuł VI proponowanego rozporządzenia zawiera przepisy końcowe, określające zasady przyjmowania aktów wykonawczych i delegowanych, proces oceny proponowanego rozporządzenia oraz uchylenie i następstwo rozporządzenia (UE) 2019/881. Określa on również datę wejścia w życie proponowanego rozporządzenia.

2026/0011 (COD)

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 oraz uchylającego rozporządzenie (UE) 2019/881 (ustawa o cyberbezpieczeństwie 2)

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJUNION ,

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[24] ,

uwzględniając opinię Komitetu Regionów[25] ,

stępując zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Od czasu przyjęcia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881[26] sytuacja geopolityczna, technologiczna i polityczna uległa znacznym zmianom. Liczba incydentów związanych z cyberbezpieczeństwem, spowodowanych awariami systemów, błędami ludzkimi, złośliwymi działaniami lub zjawiskami naturalnymi, gwałtownie wzrosła, a cyberataki stały się bardziej wyrafinowane, dotykając kluczowe podmioty, przedsiębiorstwa i ogół społeczeństwa. Ekosystem cyberprzestępczości rozrósł się, a jego podstawą stały się działania związane z oprogramowaniem ransomware. Nasiliły się incydenty w łańcuchu dostaw, spowodowane przez przestępców w celu osiągnięcia korzyści finansowych lub przez podmioty państwowe w celu zakłócenia funkcjonowania, szpiegostwa, dezinformacji lub działań wojennych. W ramach szerszej strategii hybrydowej incydenty wynikające ze złośliwych działań cybernetycznych i awarii systemów rozprzestrzeniają się, zakłócając funkcjonowanie kluczowych usług, podważając zaufanie do instytucji i wpływając na gotowość społeczną i obronną Unii. Incydenty takie wykazały swój potencjał oddziaływania na działalność gospodarczą, stabilność finansową i życie ludzi. Jednocześnie podatność krytycznej infrastruktury cywilnej i systemów stanowi zagrożenie dla zdolności obronnych, które są od nich zależne.

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

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

[26] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa technologii informacyjno-komunikacyjnych i uchylające rozporządzenie (UE) nr 526/2013 (ustawa o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(2) Równolegle nowe technologie, takie jak sztuczna inteligencja i informatyka kwantowa, mają destrukcyjny wpływ na cyberbezpieczeństwo i cyberobronę. Zmieniają one narzędzia obronne i taktykę przeciwników, stwarzając zagrożenia dla cyberbezpieczeństwa i cyber obrony, ale jednocześnie otwierają możliwości rozwoju technologicznego. Chociaż mogą one przyczyniać się do poprawy cyberbezpieczeństwa poprzez lepsze wykrywanie zagrożeń lub zautomatyzowaną reakcję na incydenty, zwiększają one również ogólną powierzchnię ataku dla organizacji, są potencjalnymi celami manipulacji i mogą podważać długoterminową skuteczność środków bezpieczeństwa, takich jak szyfrowanie.

(3) Aby sprostać tym zmianom, Unia wzmocniła swoje narzędzia prawne i polityczne. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555[27] wzmacnia cyberbezpieczeństwo infrastruktury krytycznej, a uzupełnia ją dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557[28] dotycząca bezpieczeństwa fizycznego. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847[29] zwiększa cyberbezpieczeństwo produktów zawierających elementy cyfrowe. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38[30] buduje unijne zdolności reagowania, a zalecenie Rady z dnia 6 czerwca 2025 r. w sprawie planu UE na rzecz zarządzania kryzysowego w cyberprzestrzeni[31] („zalecenie w sprawie planu cyberbezpieczeństwa") wspiera współpracę w zakresie zarządzania kryzysowego na szczeblu unijnym. Zestaw narzędzi 5G Cybersecurity Toolbox[32] stanowi pierwszy krok w kierunku skoordynowanego podejścia na szczeblu unijnym w celu zabezpieczenia sieci 5G. Komunikat Komisji w sprawie Akademii Umiejętności w zakresie Cyberbezpieczeństwa[33] dotyczy rosnącego wyzwania, jakim jest niedobór talentów w dziedzinie cyberbezpieczeństwa. Ponadto ramy cyberbezpieczeństwa zostały wzmocnione przez przepisy sektorowe, w szczególności rozporządzenie Parlamentu

---

27 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).

28 Dyrektywa (UE) 2022/2557 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.U. L 333 z 27.12.2022, s. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

29 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymogów dotyczących cyberbezpieczeństwa produktów zawierających elementy cyfrowe oraz zmieniające rozporządzenia (UE) nr 168/2013 i (UE) 2019/1020 oraz dyrektywę (UE) 2020/1828 (ustawa o cyberodporności) (Dz.U. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

30 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z dnia 19 grudnia 2024 r. ustanawiające środki mające na celu wzmocnienie solidarności i zdolności Unii w zakresie wykrywania cyberzagrożeń i cyberincydentów, przygotowania się na nie i reagowania na nie oraz zmieniające rozporządzenie (UE) 2021/694 (ustawa o cyber solidarności) (Dz.U. L, 2025/38, 15.01.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

31 Dz.U. C, C/2025/3445 z 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3445/oj.

32 Cyberbezpieczeństwo sieci 5G – zestaw narzędzi UE służących ograniczaniu ryzyka, grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji, 1/2020, dostępny pod adresem: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

33 Komunikat Komisji do Parlamentu Europejskiego i Rady, Wypełnianie luki w zakresie talentów w dziedzinie cyberbezpieczeństwa w celu zwiększenia konkurencyjności, wzrostu gospodarczego i odporności UE („Akademia umiejętności w zakresie cyberbezpieczeństwa"), COM(2023)207 final, 18 kwietnia 2023 r.

Europejskiego i Rady (UE) 2022/2554[34] dla sektora finansowego, rozporządzenie delegowane Komisji (UE) 2024/1366[35] dla podsektora energii elektrycznej, rozporządzeniem delegowanym Komisji (UE) 2022/1645[36] oraz rozporządzeniem wykonawczym Komisji (UE) 2023/203[37] (PART-IS), a także odpowiednimi przepisami dotyczącymi bezpieczeństwa lotniczego określonymi w rozporządzeniu Komisji (UE) 2019/1583[38] dla podsektora transportu lotniczego oraz innymi dokumentami politycznymi, takimi jak komunikat Komisji w sprawie planu działania UE na rzecz cyberbezpieczeństwa szpitali i podmiotów świadczących usługi opieki zdrowotnej[39] . Podmioty unijne zostały również wzmocnione rozporządzeniem Parlamentu Europejskiego i Rady (UE, Euratom) 2023/2841[40] , które określa środki mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii. Te ulepszone ramy prawne dotyczące cyberbezpieczeństwa doprecyzowały zadania ENISA.

---

34 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie odporności operacyjnej sektora finansowego w środowisku cyfrowym oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 i (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

35 Rozporządzenie delegowane Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieciowego dotyczącego zasad sektorowych w zakresie cyberbezpieczeństwa transgranicznych przepływów energii elektrycznej (Dz.U. L, 2024/1366, 24.05.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

36 Rozporządzenie delegowane Komisji (UE) 2022/1645 z dnia 14 lipca 2022 r. ustanawiające przepisy wykonawcze do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymogów dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji, które może mieć wpływ na bezpieczeństwo lotnicze, dla organizacji objętych rozporządzeniami Komisji (UE) nr 748/2012 i (UE) nr 139/2014 oraz zmieniające rozporządzenia Komisji (UE) nr 748/2012 i (UE) nr 139/2014 (Dz.U. L 248, s. 18–31, 26.9.2022, ELI: http://data.europa.eu/eli/reg_del/2022/1645/oj).

37 Rozporządzenie wykonawcze Komisji (UE) 2023/203 z dnia 27 października 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymogów dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji, które może mieć wpływ na bezpieczeństwo lotnicze, w odniesieniu do organizacji objętych rozporządzeniami Komisji (UE) nr 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340, rozporządzeniami wykonawczymi Komisji (UE) 2017/373 i (UE) 2021/664 oraz dla właściwych organów objętych rozporządzeniami Komisji (UE) nr 748/2012, (UE) nr 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340 i (UE) nr 139/2014, rozporządzenia wykonawcze Komisji (UE) 2017/373 i (UE) 2021/664 oraz zmieniające rozporządzenia Komisji (UE) nr 1178/2011, (UE) nr 748/2012, (UE) nr 965/2012, (UE) nr 139/2014, (UE) nr 1321/2014, (UE) 2015/340 oraz rozporządzenia wykonawcze Komisji (UE) 2017/373 i (UE) 2021/664 (Dz.U. L 31 z 2.2.2023, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2023/203/oj).

38 Rozporządzenie wykonawcze Komisji (UE) 2019/1583 z dnia 25 września 2019 r. zmieniające rozporządzenie wykonawcze (UE) 2015/1998 ustanawiające szczegółowe środki w celu wdrożenia wspólnych podstawowych norm bezpieczeństwa lotniczego w odniesieniu do środków bezpieczeństwa cybernetycznego (Dz.U. L 246 z 26.9.2019, s. 15–18, ELI: http://data.europa.eu/eli/reg_impl/2019/1583/oj).

39 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejski plan działania w zakresie cyberbezpieczeństwa szpitali i podmiotów świadczących usługi opieki zdrowotnej, COM(2025) 10 final, 15 stycznia 2025 r.

40 Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2023/2841 z dnia 13 grudnia 2023 r. ustanawiające środki zapewniające wysoki wspólny poziom cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii (Dz.U. L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

(4) W tym kontekście, zgodnie z dokumentami „ProtectEU: Europejska strategia bezpieczeństwa wewnętrznego”[41] oraz „Strategia Unii w zakresie gotowości”[42] , zapewnienie gotowości, bezpieczeństwa i odporności społeczeństwa i gospodarki Unii wymaga silnej koordynacji na szczeblu europejskim, zaufania i wymiany informacji między zainteresowanymi stronami, solidnych ram zapewniających bezpieczeństwo produktów, usług, procesów i zarządzanych usług bezpieczeństwa w dziedzinie ICT, a także zwiększenia i wzmocnienia kadr zajmujących się cyberbezpieczeństwem. W komunikacie wezwano również do wzmocnienia łańcuchów dostaw ICT poprzez zapewnienie europejskiej suwerenności technologicznej w zakresie kluczowych aktywów, co zwiększyłoby odporność Unii i mogłoby przynieść korzyści w zakresie cyberobrony. Ponadto w komunikacie w sprawie wzmocnienia bezpieczeństwa gospodarczego UE[43] jako cele priorytetowe wskazano potrzebę zapobiegania dostępowi do informacji i danych wrażliwych, które mogłyby zagrozić bezpieczeństwu gospodarczemu UE, oraz zapobiegania zakłóceniom w funkcjonowaniu infrastruktury krytycznej UE mającym wpływ na gospodarkę UE i łagodzenia takich zakłóceń. W komunikacie uznano zasadniczą rolę, jaką w tym zakresie odgrywają skuteczne środki w zakresie cyberbezpieczeństwa.

(5) Incydenty związane z cyberbezpieczeństwem na dużą skalę, mające wpływ na infrastrukturę krytyczną, usługi cyfrowe lub podstawowe funkcje społeczne, mogą mieć wpływ na ludność, wymagając skoordynowanych działań w zakresie ochrony ludności i zarządzania kryzysowego na szczeblu unijnym. Zgodnie z podejściem uwzględniającym wszystkie rodzaje zagrożeń, przyjętym w europejskiej strategii gotowości i decyzji nr 1313/2013/UE w sprawie unijnego mechanizmu ochrony ludności, ustalenia dotyczące orientacji sytuacyjnej, reagowania na incydenty i ćwiczeń na mocy niniejszego rozporządzenia powinny być wykorzystywane w zarządzaniu kryzysowym Unii, w szczególności za pośrednictwem Centrum Koordynacji Reagowania Kryzysowego (ERCC).

(6) Niniejszy wniosek jest zgodny z [wnioskiem dotyczącym dyrektywy uzupełniającej [zmianę rozporządzenia (UE) 2019/881] i zmieniającej dyrektywę (UE) 2022/2555 w odniesieniu do uproszczenia wdrażania środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii] oraz z [wnioskiem dotyczącym rozporządzenia w sprawie uproszczenia przepisów dotyczących cyfryzacji (Digital Omnibus)[44] , który nakłada na ENISA obowiązek opracowania jednego punktu kontaktowego do zgłaszania incydentów, za pośrednictwem którego podmioty mogą jednocześnie wypełniać swoje obowiązki w zakresie zgłaszania incydentów wynikające z wielu aktów prawnych.

(7) Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady[45] ustanowiło ENISA w celu przyczynienia się do zapewnienia wysokiego i skutecznego poziomu

---

41 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie Protect EU: europejska strategia bezpieczeństwa wewnętrznego, COM(2025)148 final, 1 kwietnia 2025 r.

42 Wspólny komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii Unii na rzecz gotowości, JOIN(2025) 130 final.

43 Wspólny komunikat Komisji do Parlamentu Europejskiego i Rady, „Wzmocnienie bezpieczeństwa gospodarczego UE”, JOIN(2025) 977 final.

44 COM/2025/837 wersja ostateczna

45 Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (Dz.U. L 77 z 13.3.2004, s. 1, ELI: http://data.europa.eu/eli/reg/2004/460/oj).

bezpieczeństwa sieci i informacji w Unii oraz rozwoju kultury bezpieczeństwa sieci i informacji z korzyścią dla obywateli, konsumentów, przedsiębiorstw i administracji publicznej. Mandat ENISA był trzykrotnie przedłużany, zanim rozporządzeniem (UE) 2019/881 przyznano jej stały mandat. Aby lepiej zaspokajać potrzeby wynikające z ewoluującego zagrożenia i zmian technologicznych, w szczególności w odniesieniu do współpracy operacyjnej i zwiększonego zapotrzebowania na specjalistów ds. cyberbezpieczeństwa, należy dalej wzmocnić mandat ENISA. W interesie pewności prawa należy zastąpić rozporządzenie (UE) 2019/881.

(8) W zmieniającym się krajobrazie zagrożeń, w którym incydenty związane z cyberbezpieczeństwem stają się coraz bardziej znaczące, zapewnienie zaufania osób fizycznych, organów publicznych i przedsiębiorstw w zakresie codziennego korzystania z technologii jest ważniejsze niż kiedykolwiek. Wzrost zaufania można ułatwić poprzez wzmocnienie ogólnounijnego certyfikatu ECCF, który określa wspólne wymogi w zakresie cyberbezpieczeństwa i kryteria oceny na rynkach krajowych i w sektorach. Nowe ramy powinny określać główne wymogi horyzontalne dla europejskich systemów certyfikacji cyberbezpieczeństwa oraz umożliwiać uznawanie i stosowanie europejskich certyfikatów cyberbezpieczeństwa i unijnych oświadczeń o zgodności we wszystkich państwach członkowskich. W tym celu należy ustanowić procedurę i ramy zarządzania, które umożliwią terminowe i przewidywalne opracowywanie i utrzymywanie europejskich systemów certyfikacji cyberbezpieczeństwa. Europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa powinny być stosowane jednolicie we wszystkich państwach członkowskich, aby zapewnić zharmonizowane wdrażanie wymogów w zakresie cyberbezpieczeństwa, wyrównać szanse i zapobiec „certyfikacyjnemu shoppingowi" opartemu na różnych poziomach rygorystyczności w różnych państwach członkowskich. ENISA powinna odgrywać kluczową rolę w zapewnianiu rozwoju systemów poprzez specyfikacje techniczne i gwarantowaniu, że systemy te pozostają aktualne pod względem technicznym. Ponadto, aby skutecznie zaspokajać potrzeby rynku, ramy powinny przewidywać możliwość certyfikacji środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa skierowanych do podmiotów oraz ułatwiać zgodność z innymi obowiązującymi przepisami unijnymi w dziedzinie cyberbezpieczeństwa. Dostosowanie do obowiązującego prawa Unii, takiego jak rozporządzenie (UE) 2024/2847 i dyrektywa (UE) 2022/2555, ma zasadnicze znaczenie dla europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, aby przyczynić się do zmniejszenia obciążeń związanych z zapewnieniem zgodności dla przedsiębiorstw, zwiększenia ich atrakcyjności i wzmocnienia cyberodporności Unii.

(9) Misją ENISA powinno być wspieranie państw członkowskich i podmiotów unijnych w osiąganiu wysokiego poziomu cyberbezpieczeństwa, odporności i zaufania w Unii. W tym celu ENISA powinna pełnić rolę punktu odniesienia w zakresie doradztwa i wiedzy specjalistycznej w dziedzinie cyberbezpieczeństwa, a jej działania powinny koncentrować się przede wszystkim na czterech kluczowych obszarach cyberbezpieczeństwa na poziomie Unii. Po pierwsze, ENISA powinna wspierać państwa członkowskie w spójnym wdrażaniu polityki i prawodawstwa Unii w zakresie cyberbezpieczeństwa oraz pomagać państwom członkowskim poprzez działania w zakresie budowania potencjału, aby stale poprawiać ich zdolności w zakresie gotowości, odporności i reagowania. Po drugie, ENISA powinna przyczyniać się do współpracy operacyjnej na szczeblu Unii między państwami członkowskimi oraz do lepszej wspólnej świadomości sytuacji w zakresie cyberzagrożeń i incydentów wśród państw członkowskich i podmiotów unijnych. Trzecim kluczowym obszarem powinno być certyfikowanie i normalizacja w zakresie cyberbezpieczeństwa, natomiast czwartym – wdrożenie Akademii Umiejętności w zakresie Cyberbezpieczeństwa, która powinna

przyczynić się do rozwoju prężnej europejskiej kadry specjalistów ds. cyberbezpieczeństwa posiadających umiejętności, które powinny być przenośne między państwami członkowskimi.

(10) Rozporządzenie (UE, Euratom) 2023/2841 ustanawiające środki zapewniające wysoki wspólny poziom cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii oraz określające mandat CERT-EU, ustanawiające go jako służbę ds. cyberbezpieczeństwa dla instytucji, organów, urzędów i agencji Unii urzędów i agencji Unii, aby przyczyniać się do bezpieczeństwa nieklasyfikowanego środowiska ICT podmiotów unijnych poprzez doradzanie im w zakresie cyberbezpieczeństwa, wspieranie ich w zapobieganiu incydentom, ich wykrywaniu, radzeniu sobie z nimi, łagodzeniu ich skutków, reagowaniu na nie i usuwaniu ich skutków oraz pełnienie funkcji centrum wymiany informacji dotyczących cyberbezpieczeństwa i koordynacji reagowania na incydenty. Ponadto CERT-EU ma za zadanie oferować odpowiednie usługi w zakresie cyberbezpieczeństwa podmiotom unijnym. W ramach swojej misji ENISA powinna również wspierać podmioty unijne. W szczególności powinna to robić poprzez zaangażowanie się w zorganizowaną współpracę z CERT-EU w zakresie budowania potencjału, współpracy operacyjnej i długoterminowych analiz strategicznych zagrożeń cybernetycznych. W stosownych przypadkach ENISA może wykorzystać zorganizowaną współpracę z CERT-EU w celu świadczenia usług lub wsparcia ENISA w zakresie cyberbezpieczeństwa, które mogą stanowić wartość dodaną dla podmiotów unijnych, w sposób skoordynowany, aby zapewnić synergię działań CERT-EU.

(11) Jednym z podstawowych zadań ENISA powinno być wspieranie państw członkowskich w spójnym wdrażaniu polityki i prawa Unii w zakresie cyberbezpieczeństwa, w szczególności w odniesieniu do dyrektywy (UE) 2022/2555, rozporządzenia (UE) 2024/2847 i rozporządzenia (UE) 2025/38. Aby pomóc w spójnym i skutecznym wdrażaniu dorobku prawnego Unii w zakresie cyberbezpieczeństwa, ENISA powinna wydawać wytyczne techniczne i sprawozdania, udzielać porad i przedstawiać najlepsze praktyki oraz ułatwiać wymianę najlepszych praktyk między właściwymi organami w tym zakresie. Ponadto ENISA ocenia stan cyberbezpieczeństwa w Unii i przyjmuje sprawozdanie w tej sprawie zgodnie z art. 18 dyrektywy (UE) 2022/2555. ENISA powinna również być w stanie odpowiadać na wnioski państw członkowskich i, w stosownych przypadkach, podmiotów unijnych o doradztwo i pomoc w sprawach wchodzących w zakres jej kompetencji.

(12) W celu stymulowania współpracy między sektorem publicznym a sektorem prywatnym oraz w ramach sektora prywatnego, w szczególności w celu wspierania ochrony infrastruktury krytycznej, ENISA powinna wspierać wymianę informacji w ramach sektorów i między nimi, w szczególności sektorami wymienionymi w załącznikach I i II do dyrektywy (UE) 2022/2555, oraz informacji dotyczących produktów zawierających elementy cyfrowe objętych zakresem rozporządzenia (UE) 2024/2847. Wsparcie to może przybierać formę udostępniania najlepszych praktyk i wytycznych dotyczących dostępnych narzędzi i procedur, a także wytycznych dotyczących sposobu rozwiązywania kwestii regulacyjnych związanych z wymianą informacji, na przykład poprzez ułatwianie tworzenia sektorowych centrów wymiany i analizy informacji (ISAC).

(13) W celu wspierania i ułatwiania strategicznej współpracy i wymiany informacji ENISA powinna wnosić wkład w prace grupy ds. współpracy ustanowionej dyrektywą (UE) 2022/2555 („grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji”), w szczególności poprzez zapewnianie wiedzy fachowej, doradztwo i ułatwianie wymiany

najlepszych praktyk, między innymi w odniesieniu do zależności transgranicznych, dotyczących ryzyka i incydentów. ENISA powinna również wnosić wkład w prace europejskiej grupy ds. współpracy w zakresie tożsamości cyfrowej ustanowionej rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014[46] , europejskiej grupy ds. certyfikacji w zakresie cyberbezpieczeństwa oraz grupy ds. współpracy administracyjnej (ADCO) ustanowionej rozporządzeniem (UE) 2024/2847.

(14) Publiczna część otwartej sieci internetowej, a mianowicie jej główne protokoły i infrastruktura, które stanowią globalne dobro publiczne, zapewnia podstawową funkcjonalność całej sieci internetowej i stanowi podstawę jej normalnego działania. W ramach swojego mandatu ENISA powinna wspierać bezpieczeństwo i odporność publicznej części otwartej sieci internetowej oraz stabilność jej funkcjonowania, w tym między innymi bezpieczne wdrażanie i działanie kluczowych protokołów (w szczególności systemu nazw domenowych, protokołu Border Gateway Protocol i protokołu internetowego w wersji 6) oraz funkcjonowania systemu nazw domenowych (takiego jak funkcjonowanie wszystkich domen najwyższego poziomu), poprzez promowanie najlepszych praktyk, wytycznych i współpracy, zgodnie z ustalonymi globalnymi, wielostronnymi uzgodnieniami dotyczącymi zarządzania internetem oraz odpowiednimi rolami i obowiązkami właściwych międzynarodowych organów technicznych i operacyjnych.

(15) ENISA pełni rolę punktu odniesienia w zakresie doradztwa i wiedzy specjalistycznej w dziedzinie cyberbezpieczeństwa. W związku z tym, na wniosek Komisji, ENISA powinna wspierać ją, wykorzystując swoją wiedzę specjalistyczną, doradztwo techniczne, informacje, analizy, w tym studia wykonalności, opinie i prace przygotowawcze dotyczące wszelkich konkretnych kwestii w dziedzinie cyberbezpieczeństwa, w celu dostarczania Komisji informacji przydatnych w kształtowaniu polityki oraz ułatwiania Komisji monitorowania wdrażania unijnego prawodawstwa dotyczącego cyberbezpieczeństwa.

(16) Podobnie, biorąc pod uwagę swoją wiedzę specjalistyczną, ENISA powinna wspierać państwa członkowskie w ich wysiłkach na rzecz budowania i wzmacniania zdolności i gotowości do zapobiegania cyberzagrożeniom i cyberincydentom oraz reagowania na nie, a także w odniesieniu do bezpieczeństwa sieci i systemów informatycznych. W szczególności ENISA powinna wspierać rozwój i wzmacnianie zespołów reagowania na incydenty związane z bezpieczeństwem komputerowym („CSIRT”), przewidzianych w dyrektywie (UE) 2022/2555, w celu osiągnięcia wysokiego wspólnego poziomu dojrzałości CSIRT w Unii.

(17) ENISA wspierała i powinna nadal wspierać państwa członkowskie w opracowywaniu i wdrażaniu wytycznych dotyczących ich krajowych strategii w zakresie cyberbezpieczeństwa, przyczyniając się do przyjęcia i wdrożenia strategii w zakresie cyberbezpieczeństwa przez wszystkie państwa członkowskie. ENISA powinna promować rozpowszechnianie takich strategii za pośrednictwem interaktywnej mapy krajowych strategii w zakresie cyberbezpieczeństwa (NCSS) i powinna dalej śledzić postępy w ich wdrażaniu , w tym poprzez zapewnienie wsparcia w opracowywaniu kluczowych wskaźników efektywności w tym kontekście.

[46] 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).

(18) W rozporządzeniu (UE, Euratom) 2023/2841 powierzono międzyinstytucjonalnej radzie ds. cyberbezpieczeństwa zadanie wspierania podmiotów unijnych w podnoszeniu ich poziomu cyberbezpieczeństwa, a CERT-EU zadanie przyczyniania się do bezpieczeństwa nieklasyfikowanego środowiska ICT wszystkich podmiotów unijnych. ENISA, w oparciu o swoje doświadczenie w zakresie cyberbezpieczeństwa, powinna wspierać międzyinstytucjonalną radę ds. cyberbezpieczeństwa i CERT-EU w wykonywaniu ich zadań zgodnie z rozporządzeniem (UE, Euratom) 2023/2841, w tym poprzez udział w analizie cyberzagrożeń, rozpoznaniu sytuacji, ćwiczeniach z zakresu cyberbezpieczeństwa, koordynacji reagowania na incydenty oraz wymianie know-how i najlepszych praktyk.

(19) W oparciu o swoją wiedzę specjalistyczną i w celu uzupełnienia możliwości krajowych i unijnych organów publicznych ENISA powinna organizować szkolenia w oparciu o europejskie ramy umiejętności w zakresie cyberbezpieczeństwa (ECSF), w szczególności w celu wspierania skutecznego wdrażania polityki, współpracy operacyjnej i podnoszenia świadomości.

(20) Aby zapewnić synergię z Europejskim Centrum Kompetencji w zakresie Przemysłu, Technologii i Badań w dziedzinie Cyberbezpieczeństwa (ECCC) oraz siecią krajowych centrów koordynacyjnych ustanowionych na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/887[47] , ENISA powinna wspierać je poprzez wymianę informacji na temat obecnych i pojawiających się zagrożeń oraz cyberzagrożeń, w tym zagrożeń dotyczących technologii informacyjno-komunikacyjnych.

(21) W strategii gotowości podkreślono, że umiejętności cyfrowe, oparte na nabyciu podstawowych umiejętności cyfrowych, mają zasadnicze znaczenie dla wzmocnienia odporności obywateli w obliczu potencjalnych kryzysów. Jednakże, jak podkreślono w komunikacie Komisji w sprawie Unii Umiejętności[48] , prawie połowa dorosłej populacji nie posiada podstawowych umiejętności cyfrowych, mimo że ponad 90 % miejsc pracy wymaga ich posiadania. Aby zapewnić, że obecna i potencjalna przyszła siła robocza posiada umiejętności wymagane w szybko zmieniającym się środowisku cyfrowym, oraz aby przyczynić się do rozwoju europejskiej puli talentów w dziedzinie cyberbezpieczeństwa, ENISA powinna wspierać działania mające na celu podnoszenie świadomości w zakresie cyberbezpieczeństwa, które mają na celu przyciągnięcie talentów i pomoc w informowaniu o edukacji i umiejętnościach potrzebnych w dziedzinie cyberbezpieczeństwa, takie jak europejski konkurs „European Cybersecurity Challenge”. W tym zakresie ENISA powinna koordynować konkursy dotyczące cyberbezpieczeństwa, zawody typu „capture the flag” i podobne ćwiczenia praktyczne, jako środek rozwoju umiejętności w zakresie cyberbezpieczeństwa i wspierania budowania potencjału w całej Unii. Prowadząc działania uświadamiające, ENISA powinna zapewnić, aby odpowiadały one potrzebom krajowych organów publicznych i podmiotów unijnych, a także potrzebom przedsiębiorstw, w szczególności MŚP, oraz instytucji edukacyjnych i szkoleniowych, poprzez utrzymywanie praktycznych ram i szkoleń, takich jak „awareness-raising-in-a-box”. ENISA powinna dalej opracowywać praktyczne i możliwe do zastosowania wytyczne w celu wspierania wdrażania unijnej

[47] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiające Europejskie Centrum Kompetencji w zakresie Przemysłu, Technologii i Badań w dziedzinie Cyberbezpieczeństwa oraz Sieć Krajowych Centrów Koordynacyjnych (Dz.U. L 202 z 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[48] Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Unia umiejętności, COM(2025) 90 final, 5 marca 2025 r.

polityki i prawodawstwa w zakresie cyberbezpieczeństwa. ENISA powinna również dążyć do zapewnienia odpowiednich informacji na temat obowiązujących systemów certyfikacji, na przykład poprzez dostarczanie wytycznych i zaleceń.

(22) Aby wspierać przedsiębiorstwa działające w sektorze cyberbezpieczeństwa, użytkowników rozwiązań w zakresie cyberbezpieczeństwa oraz zapewnić skuteczne wdrożenie tytułu III niniejszego rozporządzenia, ENISA powinna opracować i utrzymywać „obserwatorium rynku", przeprowadzając regularne analizy i rozpowszechniając informacje na temat głównych trendów na rynku cyberbezpieczeństwa, zarówno po stronie popytu, jak i podaży. Ponadto, aby wspierać użytkowników rezerwy UE w zakresie cyberbezpieczeństwa utworzonej na mocy rozporządzenia (UE) 2025/38, ENISA powinna przygotować mapę usług potrzebnych tym użytkownikom oraz dostępności takich usług, zgodnie z tym rozporządzeniem.

(23) Zagrożenia cybernetyczne są problemem o zasięgu globalnym. W celu poprawy cyberbezpieczeństwa konieczna jest ściślejsza współpraca międzynarodowa, w tym określenie wspólnych norm postępowania i wspólnych podejść. W tym celu ENISA powinna wspierać współpracę Unii z państwami trzecimi, ze szczególnym uwzględnieniem państw kandydujących do przystąpienia do Unii, oraz z organizacjami międzynarodowymi, takimi jak NATO, poprzez zapewnienie Komisji i odpowiednim podmiotom Unii niezbędnej wiedzy fachowej i analiz, w stosownych przypadkach. Działania ENISA w obszarze międzynarodowym powinny być zawsze zgodne z priorytetami Unii.

(24) Aby pomóc w osiągnięciu wysokiego poziomu cyberbezpieczeństwa w Unii, ENISA powinna wspierać współpracę operacyjną między państwami członkowskimi, we współpracy z CERT-EU, między podmiotami Unii oraz między zainteresowanymi stronami. W tym celu należy wzmocnić rolę ENISA. ENISA powinna stać się członkiem sieci CSIRT, przyczyniając się do wymiany informacji i analiz w ramach tej sieci. ENISA powinna dalej promować i wspierać współpracę między odpowiednimi zespołami CSIRT w przypadku incydentów, ataków lub zakłóceń w funkcjonowaniu sieci lub infrastruktury zarządzanej lub chronionej przez zespoły CSIRT. Aktywne wsparcie ENISA dla prac sieci zespołów CSIRT i europejskiej sieci organizacji łącznikowych ds. cyberkryzysów (EU-CyCLONe) powinno umożliwić tym sieciom dalsze zwiększanie swojego poziomu dojrzałości. Rola ENISA we wspieraniu takiej współpracy obejmuje zwalczanie zagrożeń dla bezpieczeństwa i integralności instytucji demokratycznych, wyborów i innych procesów oraz infrastruktury krytycznej, od której są one zależne, zgodnie z europejską tarczą demokracji: wzmacnianie silnych i odpornych demokracji[49] .

(25) Aby wspierać budowanie potencjału, współpracę operacyjną i długoterminowe analizy strategiczne zagrożeń cybernetycznych, ENISA powinna wykorzystywać dostępną wiedzę techniczną i operacyjną CERT-EU poprzez ustrukturyzowaną współpracę, na przykład w ramach specjalnych porozumień.

(26) W celu wzmocnienia cyberbezpieczeństwa w całej Unii i zapewnienia szybkiej i skutecznej reakcji na cyberzagrożenia ENISA powinna wspierać państwa członkowskie na ich wniosek, w tym poprzez udzielanie porad dotyczących poprawy ich zdolności w zakresie zapobiegania incydentom, ich wykrywania, reagowania na nie i usuwania ich skutków, poprzez ułatwianie technicznego postępowania w przypadku znaczących incydentów w rozumieniu dyrektywy (UE) 2022/2555, w szczególności poprzez wspieranie dobrowolnej wymiany rozwiązań technicznych między państwami

[49] JOIN(2025) 791 final.

członkowskimi lub poprzez zapewnienie analizy cyberzagrożeń i incydentów. ENISA powinna również pomagać EU-CyCLONe w przygotowywaniu sprawozdań dla szczebla politycznego Unii i państw członkowskich.

(27) Aby ograniczyć narażenie na ingerencje zagraniczne, manipulacje w łańcuchu dostaw i strategiczne wycieki danych, ENISA powinna korzystać z bezpiecznych narzędzi komunikacyjnych w ramach sieci CSIRT i EU-CyCLONe. W oparciu o zalecenie w sprawie planu działania w dziedzinie cyberbezpieczeństwa narzędzia takie powinny być dostarczane przez podmioty prawne mające siedzibę lub uznane za mające siedzibę w Unii i kontrolowane przez państwa członkowskie lub obywateli państw członkowskich.

(28) Aby przyczynić się do gotowości i reagowania na szczeblu unijnym w przypadku incydentów i kryzysów związanych z cyberbezpieczeństwem na dużą skalę, ENISA powinna prowadzić działania w zakresie świadomości sytuacyjnej w zakresie cyberbezpieczeństwa.

(29) Dostęp do zweryfikowanych, wiarygodnych informacji o cyberzagrożeniach (CTI) w czasie rzeczywistym ma kluczowe znaczenie dla budowania wspólnej świadomości sytuacyjnej w Unii. ENISA, Komisja, CERT-EU i Europejskie Centrum ds. Cyberprzestępczości (EC3) przy Europolu opracowały już repozytoria informacji o cyberzagrożeniach dostosowane do ich konkretnych potrzeb. ENISA i inne właściwe podmioty unijne powinny dobrowolnie współpracować w celu opracowania repozytoriów sprawdzonych i wiarygodnych informacji o cyberzagrożeniach w czasie rzeczywistym oraz dążyć do osiągnięcia synergii w celu zapewnienia korzyści skali i wzmocnienia należytego zarządzania finansami. W prace te powinny być również zaangażowane sektorowe podmioty unijne, takie jak agencja UE ds. programu kosmicznego. Powinny one dzielić się wyłącznie wynikami analiz, trendami oraz taktykami, technikami i procedurami (TTP), a nie surowymi źródłami, oraz powinny szanować niezależność podmiotów w zakresie zarządzania własnym cyklem życia informacji o cyberzagrożeniach zgodnie z ich mandatami i zasadami ograniczonego dostępu do informacji.

(30) Aby przyczynić się do szybkiej i skoordynowanej reakcji, ENISA powinna mieć możliwość wydawania wczesnych ostrzeżeń o potencjalnym lub trwającym znaczącym lub zakrojonym na szeroką skalę incydencie lub cyberzagrożeniu o potencjalnym charakterze transgranicznym do zainteresowanych zespołów CSIRT lub CSIRT, a w stosownych przypadkach do sieci CSIRT i EU-CyCLONe, w szczególności w odniesieniu do podmiotów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555. Informacje zawarte w takich wczesnych ostrzeżeniach mogą obejmować publicznie znane luki w zabezpieczeniach oraz informacje o tym, czy mają one wpływ na produkty zawierające elementy cyfrowe objęte rozporządzeniem (UE) 2024/2847, a także techniki i procedury, wskaźniki naruszenia bezpieczeństwa, taktyki przeciwników, informacje dotyczące konkretnych podmiotów stanowiących zagrożenie oraz zalecenia dotyczące środków łagodzących.

(31) Aby zachować zaufanie i nie zagrażać wymianie informacji, ważne jest, aby ENISA stosowała widoczne oznaczenia wskazujące, w jakim zakresie dokument lub informacja, które sporządziła lub otrzymała, mogą być dalej udostępniane. Podobnie ENISA powinna wykorzystywać otrzymane dokumenty lub informacje do celów wykonywania swoich zadań, z zastrzeżeniem wszelkich ograniczeń dotyczących dalszego rozpowszechniania tych informacji, oznaczonych widocznym oznaczeniem.

(32) Aby pomóc w zwiększeniu świadomości na temat wskaźników cyberzagrożeń i zaleceń dotyczących środków ograniczających, ENISA powinna udostępnić usługę wczesnego

ostrzegania podmiotom działającym w sektorach wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555. Takie ogólne, dobrowolne wczesne ostrzegania powinny przynosić korzyści w szczególności MŚP i powinny być udostępniane w formacie nadającym się do odczytu maszynowego i publicznie dostępnym. W każdym przypadku taka dobrowolna usługa jest odrębna od wszelkich partnerstw publiczno-prywatnych, które ENISA może ustanowić lub już ustanowiła, i nie jest z nimi powiązana.

(33) Aby wspierać wspólną świadomość sytuacji w zakresie cyberbezpieczeństwa w Unii, ENISA, w ścisłej współpracy z państwami członkowskimi, powinna przygotowywać regularne, szczegółowe sprawozdania techniczne dotyczące sytuacji w zakresie cyberbezpieczeństwa w UE, dotyczące incydentów i cyberzagrożeń, w oparciu o informacje dostępne publicznie, własne analizy oraz sprawozdania przekazane jej przez zespoły reagowania na incydenty związane z bezpieczeństwem informatycznym (CSIRT) państw członkowskich lub krajowe pojedyncze punkty kontaktowe ds. bezpieczeństwa sieci i systemów informatycznych („pojedyncze punkty kontaktowe") przewidziane w dyrektywie (UE) 2022/2555, zarówno na zasadzie dobrowolności, jak i Europolu oraz CERT-EU. Sprawozdanie to powinno być udostępniane Radzie, Europejskiej Służbie Działań Zewnętrznych, EU-CyCLONe, sieci CSIRT, Komisji i Europolowi.

(34) W celu zwiększenia wspólnej świadomości sytuacji w zakresie cyberzagrożeń i incydentów wśród zainteresowanych stron ENISA powinna analizować trendy w zakresie cyberzagrożeń i incydentów. Powinna ona obejmować regularną analizę dotyczącą sektorów o wysokim stopniu krytyczności oraz innych sektorów krytycznych wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555, w tym sektorów opieki zdrowotnej, energii i transportu. Analiza taka powinna obejmować poziomy dojrzałości sektorów i identyfikować między innymi potencjalne wyzwania charakterystyczne dla danego sektora. W stosownych przypadkach oraz w celu zidentyfikowania skutków dla łańcucha dostaw analiza powinna wykazać cyberzagrożenia i trendy związane z kategoriami produktów objętymi rozporządzeniem (UE) 2024/2847. ENISA powinna rozwijać wiedzę specjalistyczną w dziedzinie cyberbezpieczeństwa infrastruktur i ich krytycznych zależności w łańcuchu dostaw, w szczególności w celu wspierania sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555 oraz wdrażania rozporządzenia (UE) 2024/2847. W tym celu ENISA powinna również współpracować, w stosownych przypadkach, z innymi odpowiednimi podmiotami unijnymi.

(35) Ponadto, aby lepiej zrozumieć wyzwania w dziedzinie cyberbezpieczeństwa, ENISA musi analizować obecne i powstające technologie oraz przedstawiać oceny dotyczące konkretnych zagadnień w odniesieniu do przewidywanego wpływu innowacji technologicznych na cyberbezpieczeństwo w wymiarze społecznym, prawnym, gospodarczym i regulacyjnym. Aby zapewnić społeczeństwu łatwiejszy dostęp do informacji na temat zagrożeń dla cyberbezpieczeństwa i możliwych środków zaradczych, ENISA może udostępniać odpowiednie informacje na swojej stronie internetowej w sposób przyjazny dla użytkownika i dobrze uporządkowany.

(36) Wzmocniona rola ENISA w promowaniu świadomości sytuacyjnej, analizowaniu zagrożeń i udzielaniu porad technicznych przyczyni się do wzmocnienia wspólnych wysiłków na rzecz cyberbezpieczeństwa produktów zawierających elementy cyfrowe oraz wesprze wdrożenie rozporządzenia (UE) 2024/2847. Zgodnie z rozporządzeniem (UE) 2024/2847 ENISA może proponować organom nadzoru rynku wspólne działania mające na celu sprawdzanie zgodności produktów zawierających elementy cyfrowe

oraz identyfikowanie kategorii produktów zawierających elementy cyfrowe, w odniesieniu do których można organizować kontrole. Informacje pochodzące z analizy cyberzagrożeń i wczesnych ostrzeżeń powinny wzmocnić wsparcie, jakie ENISA zapewnia tym organom, oraz przyczynić się do skutecznego egzekwowania rozporządzenia (UE) 2024/2847 w celu zapobiegania skutkom cyberataków dla łańcucha dostaw na rynku wewnętrznym oraz zwiększenia ogólnej gotowości Unii.

(37) Ataki ransomware stanowią poważne zagrożenie dla cyberbezpieczeństwa Unii. Aby wzmocnić cyberbezpieczeństwo Unii i zwalczać ransomware, ENISA powinna rozwinąć zdolności w zakresie rozpoznania sytuacji oraz wsparcia w reagowaniu na incydenty i przywracaniu sprawności. Pomagając poszczególnym podmiotom o znaczeniu kluczowym i istotnym w reagowaniu na ataki ransomware i przywracaniu sprawności po takich atakach, ENISA powinna ściśle współpracować z Europolem oraz, w stosownych przypadkach, z zespołami CSIRT lub właściwymi organami, korzystając w ten sposób z doświadczenia Europolu w zwalczaniu przestępczości związanej z ransomware. Pomoc ta powinna uzupełniać działania CSIRT wspierające reagowanie na incydenty. Aby osiągnąć synergię w swoich działaniach przeciwko oprogramowaniu ransomware, ENISA powinna utworzyć punkt pomocy technicznej i w tym celu mogłaby zgromadzić odpowiednie zdolności i usługi przeciwdziałania oprogramowaniu ransomware oraz udostępnić informacje, wytyczne i narzędzia, które mogą pomóc podmiotom istotnym i ważnym w reagowaniu na incydenty związane z oprogramowaniem ransomware i usuwaniu ich skutków.

(38) ENISA powinna zapewnić Komisji wiedzę techniczną i wsparcie w przygotowywaniu rocznego programu ćwiczeń w zakresie cyberbezpieczeństwa na szczeblu unijnym, zgodnie z zaleceniem w sprawie planu działania w zakresie cyberbezpieczeństwa, aby przygotować się na cyberkryzysy, sprawdzić poziom cyberbezpieczeństwa podmiotów uczestniczących w takich ćwiczeniach oraz zminimalizować powielanie wysiłków. ENISA powinna na przykład doradzać w sprawie odpowiednich rodzajów ćwiczeń, takich jak ćwiczenia symulacyjne, hybrydowe lub pełne ćwiczenia na żywo, a także celów, scenariuszy i udziału.

(39) Dostęp do prawidłowych i aktualnych informacji na temat luk w zabezpieczeniach oraz solidne zarządzanie tymi lukami mają zasadnicze znaczenie dla zapewnienia wysokiego poziomu cyberbezpieczeństwa na rynku wewnętrznym. Z tego powodu ENISA powinna prowadzić europejską bazę danych luk w zabezpieczeniach zgodnie z dyrektywą (UE) 2022/2555 oraz stworzyć wspólną unijną zdolność w zakresie usług zarządzania lukami w zabezpieczeniach, zapewniając odporny i zrównoważony poziom usług oraz ograniczając ryzyko zakłóceń. W tym celu ENISA powinna zbadać możliwości pogłębienia ustrukturyzowanej współpracy z programami, rejestrami lub bazami danych podobnymi do europejskiej bazy danych luk w zabezpieczeniach, aby uniknąć powielania wysiłków i dążyć do komplementarności na poziomie międzynarodowym, w stosownych przypadkach. Ponadto ENISA powinna wspierać wielostronne skoordynowane ujawnianie podatności na poziomie Unii i świadczyć usługi o wartości dodanej, takie jak ostrzeżenia o podatnościach, ocena stopnia zagrożenia i wykazy produktów, a także udostępniać ulepszony europejski katalog znanych podatności, które zostały wykorzystane, aby pomóc podmiotom w zarządzaniu podatnościami.

(40) Rola ENISA w opracowywaniu ECCF powinna być kluczowym aspektem jej mandatu. ENISA powinna zapewniać swoją wiedzę techniczną przez cały cykl życia europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa. W perspektywie przyszłego systemu ENISA powinna zidentyfikować istniejące normy lub specyfikacje techniczne, które mogą stanowić podstawę takiego systemu, a w stosownych przypadkach sama

opracować specyfikacje techniczne, do których można się odwołać w systemie. ENISA powinna być odpowiedzialna za przygotowanie projektu systemu na wniosek Komisji. W przypadku systemów już istniejących ENISA powinna być odpowiedzialna za ich utrzymanie. W ten sposób ENISA powinna przyczyniać się do budowania i rozwijania ekosystemu certyfikacji, w ramach którego zbierane są opinie państw członkowskich i prywatnych zainteresowanych stron oraz wzmacniane są ich zdolności certyfikacyjne. Powinno to również obejmować prowadzenie specjalnej strony internetowej poświęconej certyfikacji, na której odpowiednie informacje dotyczące przyjętych systemów, w tym certyfikaty i oświadczenia o zgodności, są dostępne bezpłatnie i publicznie.

(41) Aby wspierać wdrażanie odpowiednich przepisów unijnych, ENISA powinna kształtować najnowszy stan wiedzy w dziedzinie cyberbezpieczeństwa poprzez dostarczanie specyfikacji technicznych wspierających wdrażanie odpowiednich przepisów unijnych, w tym z myślą o ich potencjalnym wykorzystaniu w europejskich systemach certyfikacji cyberbezpieczeństwa. ENISA powinna również monitorować tworzenie i ewolucję norm przez odpowiednie organy normalizacyjne w celu śledzenia trendów normalizacyjnych na poziomie europejskim i globalnym oraz, w razie potrzeby, kształtować takie normy poprzez udział w działaniach organizacji normalizacyjnych, w tym poprzez opracowywanie projektów, oraz przewodzenie tym działaniom. Czyniąc to, ENISA powinna zachować bezstronność. Na przykład mogą zaistnieć sytuacje, w których ENISA powinna wycofać się z odpowiednich działań w organach normalizacyjnych, jeżeli zostanie poproszona o ocenę norm europejskich, o które zwróciła się Komisja w celu wsparcia prawodawstwa Unii. ENISA nie powinna uczestniczyć w opracowywaniu norm, za których ocenę jest odpowiedzialna.

(42) Aby wspierać wdrażanie polityk Unii i przygotowywanie potencjalnych działań normalizacyjnych, ENISA powinna przyczyniać się do opracowywania i oceny algorytmów kryptograficznych, w szczególności w dziedzinie kryptografii postkwantowej. W tym kontekście, na wniosek Komisji i z zastrzeżeniem umowy o wkładzie określonej w rozporządzeniu Parlamentu Europejskiego i Rady (UE, Euratom) 2024/2509[50] , ENISA może ustanowić proces pozyskiwania i oceny algorytmów kryptograficznych od odpowiednich zainteresowanych stron, w szczególności społeczności kryptograficznej, akademickiej i badawczej, a także producentów, zespołów CSIRT, krajowych organów certyfikacji cyberbezpieczeństwa i właściwych organów zgodnie z dyrektywą (UE) 2022/2555. W przypadku gdy ENISA przyczynia się do ustanowienia takich procesów, powinna promować współpracę między odpowiednimi zainteresowanymi stronami i wdrażać aspekty organizacyjne. Proces ten powinien być formalny, otwarty, przejrzysty i integracyjny, w tym obejmować konsultacje z odpowiednimi zainteresowanymi stronami w sprawie projektu minimalnych wymagań oraz procesu oceny i kryteriów oceny, w szczególności w odniesieniu do bezpieczeństwa i skuteczności ocen.

(43) Aby wesprzeć realizację działań w zakresie oceny zgodności w ramach europejskich systemów certyfikacji cyberbezpieczeństwa i innych odpowiednich przepisów unijnych, ENISA może udostępniać odpowiednie narzędzia do testowania technicznego, aby wspierać państwa członkowskie, przedsiębiorstwa i organy oceny zgodności w działaniach związanych z oceną. Narzędzia takie powinny mieć na celu tworzenie synergii na poziomie Unii oraz zapewnienie skutecznego funkcjonowania

[50] Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2024/2509 z dnia 23 września 2024 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii (Dz.U. L, 2024/2509, 26.09.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

procedur oceny zgodności w celu zaspokojenia potrzeb państw członkowskich i rynku. Potrzeby takie mogą pojawić się na przykład w obszarze bezpieczeństwa projektowego w celu wsparcia przedsiębiorstw, w tym małych i średnich przedsiębiorstw, w ich działaniach wdrożeniowych w kontekście rozporządzenia 2024/2847. W tym kontekście ENISA powinna pobierać opłaty na pokrycie odpowiednich kosztów związanych z ustanowieniem, projektowaniem, rozwijaniem, utrzymywaniem i aktualizowaniem niezbędnych możliwości oprogramowania i sprzętu dla takich narzędzi testowych.

(44) Aby wesprzeć państwa członkowskie w ich wysiłkach na rzecz rozwiązania problemu niedoboru specjalistów ds. cyberbezpieczeństwa oraz rosnącego zapotrzebowania na wykwalifikowaną, zróżnicowaną, w tym pod względem równowagi płci, i elastyczną siłę roboczą, a także aby umożliwić mobilność pracowników i gotowość w państwach członkowskich, ENISA powinna opierać się na zasadach i pracach zainicjowanych w ramach Akademii Umiejętności w zakresie Cyberbezpieczeństwa. W szczególności ENISA powinna ustanowić europejskie ramy umiejętności w zakresie cyberbezpieczeństwa („ECSF") jako wspólne ramy dotyczące profili zawodowych specjalistów ds. cyberbezpieczeństwa. ENISA powinna dalej wspierać państwa członkowskie w niwelowaniu dysproporcji między płciami w zawodach związanych z cyberbezpieczeństwem. Podejście to jest zgodne z wizją przedstawioną w komunikacie Komisji w sprawie Unii Umiejętności i przyczyniłoby się do realizacji jej celów. Należy dalej badać możliwość wprowadzenia znaku jakości dla europejskich indywidualnych certyfikatów umiejętności w zakresie cyberbezpieczeństwa.

(45) ECSF powinny być praktycznym i elastycznym narzędziem wykorzystywanym na zasadzie dobrowolności, zapewniającym wspólne rozumienie i terminologię odpowiednich ról oraz związanych z nimi zadań, umiejętności i wiedzy wymaganych głównie w rolach związanych z cyberbezpieczeństwem, w celu wspierania identyfikacji kluczowych zestawów umiejętności, w tym umiejętności przekrojowych, wymaganych od pracowników, oraz umożliwienia podmiotom świadczącym usługi edukacyjne, w tym przedsiębiorstwom, instytucjom szkolnictwa wyższego lub podmiotom świadczącym usługi kształcenia i szkolenia zawodowego, opracowywania programów oraz pomocy decydentom w opracowywaniu inicjatyw mających na celu wyeliminowanie luk w umiejętnościach. Ponieważ ECSF może służyć jako ramy odniesienia dla uznawania umiejętności, powinien być również interoperacyjny z europejską klasyfikacją umiejętności i zawodów (ESCO), aby pomóc działom kadr w zrozumieniu wymagań dotyczących planowania zasobów, rekrutacji i rozwoju kariery w celu zaspokojenia potrzeb w zakresie cyberbezpieczeństwa. Podczas gdy DigComp 3.0 opisuje wiedzę, umiejętności i postawy potrzebne do osiągnięcia kompetencji cyfrowych w życiu codziennym, uczestnictwie w życiu społecznym, pracy i nauce i może być stosowany zarówno przez dorosłych, jak i dzieci, ECSF oferuje proste ramy określające role w zakresie cyberbezpieczeństwa i związane z nimi zadania, wiedzę oraz umiejętności potrzebne do ich wykonywania. W tym zakresie jest on skierowany do wyspecjalizowanych odbiorców w dziedzinie cyberbezpieczeństwa, od obecnych lub potencjalnych specjalistów ds. cyberbezpieczeństwa, instytucji edukacyjnych po pracodawców. ECSF powinny również wspierać rozwój europejskich indywidualnych certyfikatów umiejętności w zakresie cyberbezpieczeństwa, stanowiąc kluczowy instrument służący do opracowywania systemów, umożliwiający pojawienie się nowych podmiotów na rynku i wspierający konkurencję rynkową w ramach wspólnych ram. ECSF powinien być regularnie oceniany i aktualizowany, aby odpowiednio odzwierciedlał potrzeby rynku pracy w zakresie cyberbezpieczeństwa , zmiany technologiczne i polityczne. ENISA powinna wspierać wdrażanie ECSF przez państwa

członkowskie i podmioty unijne oraz zapewniać odpowiednie wsparcie, gdy jest ono potrzebne.

(46) [51]Umiejętności i kwalifikacje w zakresie cyberbezpieczeństwa powinny być porównywalne, przejrzyste i godne zaufania na całym rynku wewnętrznym. W tym celu europejskie indywidualne poświadczenia umiejętności w zakresie cyberbezpieczeństwa powinny wspierać pracodawców, w tym MŚP i start-upy, w skutecznym rekrutowaniu obecnych lub potencjalnych specjalistów ds. cyberbezpieczeństwa w państwach członkowskich i między nimi, zgodnie z celami określonymi w komunikacie w sprawie Unii Umiejętności. Aby zapewnić spójne wdrażanie w państwach członkowskich, europejskie indywidualne poświadczenia umiejętności w zakresie cyberbezpieczeństwa powinny opierać się na wspólnym rozumieniu na poziomie Unii umiejętności potrzebnych do osiągnięcia tych celów i powinny być wydawane przez podmioty upoważnione przez ENISA na podstawie wspólnego zestawu kryteriów. Podejście to powinno być spójne z celami przyszłej inicjatywy na rzecz przenoszenia umiejętności i przyczyniać się do ich realizacji.

(47) Opracowanie europejskich systemów indywidualnych certyfikatów umiejętności w zakresie cyberbezpieczeństwa powinno mieć na celu uzupełnienie działań państw członkowskich poprzez umożliwienie organom publicznym i podmiotom gospodarczym korzystania z europejskiego mechanizmu certyfikacji, zgodnie z kompetencjami pomocniczymi Unii w dziedzinie kształcenia i szkolenia zawodowego, o których mowa w art. 6 lit. e) oraz art. 165 ust. 1 i art. 166 ust. 1 TFUE. Systemy te, wraz z pracami Akademii Umiejętności w zakresie Cyberbezpieczeństwa, mogą również stanowić podstawę programów szkolnictwa wyższego, takich jak sektorowe europejskie stopnie naukowe, oraz rozwoju mikrokwalifikacji. W związku z tym europejskie systemy indywidualnych certyfikatów w zakresie cyberbezpieczeństwa nie powinny mieć na celu harmonizacji przepisów prawa i regulacji w państwach członkowskich, ale raczej powinny być traktowane jako czynnik sprzyjający i szansa, z której państwa członkowskie i podmioty gospodarcze mogą chcieć skorzystać i którą mogą promować.

(48) ENISA powinna zapewnić, aby europejskie systemy certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa pozostawały zbliżone do potrzeb rynku i opierały się na doświadczeniach zarówno publicznych, jak i prywatnych podmiotów wydających certyfikaty indywidualne, w tym państw członkowskich, instytucji szkolnictwa wyższego, instytucji kształcenia i szkolenia zawodowego oraz przedsiębiorstw. ENISA powinna konsultować się z Komisją w sprawie ustalenia priorytetów europejskich systemów certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa, biorąc pod uwagę wdrożenie polityki i potrzeby rynku.

(49) Aby zapewnić spójność między ECSF a systemami, zmiana profilu roli ECSF powinna automatycznie powodować ocenę adekwatności powiązanego europejskiego systemu lub systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, co może prowadzić do ich przeglądu.

(50) Biorąc pod uwagę różnorodność profili ról w dziedzinie cyberbezpieczeństwa oraz związanych z nimi zadań, umiejętności i wiedzy, ocena osób fizycznych i metody oceny

[51] Europejskie indywidualne poświadczenia umiejętności w zakresie cyberbezpieczeństwa należy rozumieć jako podejście podobne do tego, które rynek uznaje za „certyfikaty cyberbezpieczeństwa". Aby jednak uniknąć nieporozumień w odniesieniu do europejskich ram certyfikacji cyberbezpieczeństwa, preferowane jest użycie terminu „poświadczenie", który został już zastosowany w komunikacie dotyczącym Akademii Umiejętności w zakresie Cyberbezpieczeństwa.

mogą wymagać dostosowania w każdym europejskim systemie poświadczania indywidualnych umiejętności w dziedzinie cyberbezpieczeństwa. Każdy system powinien zapewniać, aby ocena wymaganych umiejętności danej osoby pod względem efektów uczenia się, w tym, w stosownych przypadkach, ocena poziomu biegłości, była systematycznie porównywana z profilem roli ECSF lub jego podzbiorem. Metody oceny mogą obejmować takie elementy, jak sprawdzanie wiedzy teoretycznej, egzamin praktyczny, warunki wstępne i ocena rówieśnicza. Należy należycie uwzględnić doświadczenie poszczególnych osób.

(51) Aby zapewnić spójne wdrażanie europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, w szczególności w odniesieniu do oceny osób fizycznych, ENISA powinna zapewnić obowiązkowe szkolenia dla personelu odpowiedzialnego za przeprowadzanie oceny osób fizycznych. Personel ten powinien posiadać doświadczenie w dziedzinie cyberbezpieczeństwa, które można wykazać poprzez posiadanie europejskiego poświadczenia indywidualnych umiejętności w zakresie cyberbezpieczeństwa dla profilu roli, dla której przeprowadza ocenę, oraz na poziomie biegłości co najmniej równoważnym z poziomem osób, które ocenia.

(52) Rola uprawnionych podmiotów certyfikujących polega na poświadczaniu wiedzy i kompetencji osób fizycznych, aby mogły one pełnić jedną z ról ECSF, oraz na zapewnianiu pewności pracodawcom w całej Unii. Ponieważ również pracodawcy zarządzający infrastrukturą krytyczną Unii będą zwracać uwagę na zapewnienie jakości umiejętności i kompetencji osób uzyskujących europejskie indywidualne poświadczenie umiejętności w zakresie cyberbezpieczeństwa, uprawnieni dostawcy poświadczający poziom umiejętności i kompetencji powinni być godni zaufania z punktu widzenia cyberbezpieczeństwa i nie powinni podlegać niepożądanemu wpływowi państwa trzeciego, które może budzić obawy w zakresie cyberbezpieczeństwa. W związku z tym podmioty mające siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa, wyznaczone zgodnie z niniejszym rozporządzeniem lub kontrolowane przez takie państwo trzecie, przez podmiot mający siedzibę w takim państwie trzecim lub przez obywatela takiego państwa trzeciego (dostawcy wysokiego ryzyka) zgodnie z niniejszym rozporządzeniem, nie powinny kwalifikować się do uzyskania upoważnienia do wydawania europejskich certyfikatów indywidualnych umiejętności w zakresie cyberbezpieczeństwa zgodnie z tytułem II sekcja 4.

(53) Aby zapewnić osobom posiadającym europejskie poświadczenie umiejętności w zakresie cyberbezpieczeństwa możliwość łatwego korzystania z niego i dzielenia się nim oraz aby takie poświadczenie mogło być wykorzystywane we wszystkich państwach członkowskich, uprawnieni dostawcy poświadczeń powinni zapewnić, aby elektroniczne poświadczenia europejskich indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa były wydawane na wniosek osoby fizycznej do europejskiego portfela tożsamości cyfrowej (portfel EUDI) ustanowionego rozporządzeniem (UE) nr 910/2014. Upoważnieni dostawcy certyfikatów powinni być traktowani jako dostawcy usług zaufania i podlegać systemowi nadzoru i odpowiedzialności określonemu w rozporządzeniu (UE) nr 910/2014. System certyfikacji atrybutów stosowany zgodnie z rozporządzeniem wykonawczym Komisji

(UE) 2025/1569[52] powinien być zarejestrowany w katalogu systemów certyfikacji atrybutów przewidzianym w tym rozporządzeniu wykonawczym.

(54) Aby przyczynić się do rozwoju kadr w dziedzinie cyberbezpieczeństwa i przenoszenia umiejętności w całej Unii, ENISA powinna udostępnić społeczeństwu europejskie systemy poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa oraz wykaz uprawnionych podmiotów poświadczających za pośrednictwem specjalnej strony internetowej.

(55) ENISA powinna być zarządzana i prowadzona z uwzględnieniem zasad wspólnego podejścia do zdecentralizowanych agencji unijnych przyjętego w dniu 19 lipca 2012 r. przez Parlament Europejski, Radę i Komisję[53] . Zalecenia zawarte we wspólnym podejściu powinny również znaleźć odzwierciedlenie, w stosownych przypadkach, w programach prac ENISA, ocenach ENISA oraz sprawozdaniach i praktykach administracyjnych ENISA.

(56) Aby zarząd mógł skutecznie wykonywać swoje funkcje, w szczególności w zakresie wyznaczania ogólnego kierunku działań ENISA i ustalania jej priorytetów strategicznych, niezbędne jest, aby w skład zarządu wchodzili przedstawiciele wysokiego szczebla z państw członkowskich i Komisji. W tym celu każde państwo członkowskie powinno mianować członkiem zarządu szefa właściwego organu krajowego tego państwa członkowskiego odpowiedzialnego za cyberbezpieczeństwo, wyznaczonego zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555.

(57) Aby zapewnić, że zastępcy w zarządzie mogą odpowiednio wypełniać swoje role, państwa członkowskie powinny mianować zastępców posiadających odpowiednią wiedzę fachową i doświadczenie. Komisja i państwa członkowskie powinny dążyć do osiągnięcia zrównoważonej reprezentacji kobiet i mężczyzn w zarządzie oraz ograniczyć rotację członków zarządu, aby zapewnić ciągłość jego prac.

(58) Aby umożliwić ENISA skuteczne wypełnianie swojej misji, zarząd składający się z przedstawicieli państw członkowskich i Komisji powinien ustalić ogólny kierunek działań ENISA, w tym jej priorytety strategiczne, oraz zapewnić, aby ENISA wykonywała swoje zadania zgodnie z niniejszym rozporządzeniem. Zarządowi należy powierzyć uprawnienia niezbędne do ustalania i weryfikacji wykonania budżetu, przyjmowania odpowiednich przepisów finansowych, ustanawiania przejrzystych procedur roboczych dotyczących podejmowania decyzji przez ENISA, przyjmowania jednolitego dokumentu programowego ENISA, przyjmowania własnego regulaminu wewnętrznego, mianowania dyrektora wykonawczego, podejmowania decyzji w sprawie przedłużenia i zakończenia kadencji dyrektora wykonawczego oraz podejmowania decyzji w sprawie utworzenia stanowiska zastępcy dyrektora wykonawczego, a w przypadku utworzenia takiego stanowiska – w sprawie mianowania zastępcy dyrektora wykonawczego, oraz przedłużenia i zakończenia jego kadencji. Każda osoba pełniąca funkcję wykonawczą w ENISA powinna zatem być mianowana przez zarząd. Zarząd powinien być również odpowiedzialny za mianowanie lub odwoływanie członków komisji odwoławczej, a także za ustanowienie zasad zapobiegania konfliktom interesów w tym zakresie lub zarządzania nimi.

---

52 Rozporządzenie wykonawcze – UE – 2025/1569

53 Wspólne podejście, załączone do wspólnego oświadczenia Parlamentu Europejskiego, Rady UE i Komisji Europejskiej w sprawie agencji zdecentralizowanych, przyjętego w dniu 19 lipca 2012 r. i dostępnego pod adresem: https://european-union.europa.eu/document/download/d4199ff4-1e3d-45e6-af7e-90cf1a7b10bc_en?filename=joint_statement_on_decentralised_agencies_en.pdf.

(59) Aby pomóc ENISA w ustaleniu jej priorytetów strategicznych i ich aktualizacji, zarząd powinien odbywać co najmniej jedno posiedzenie w roku poświęcone priorytetom strategicznym ENISA. Aby zapewnić skuteczność i merytoryczną jakość posiedzeń zarządu, zarząd może zapraszać na swoje posiedzenia osoby, których opinia może być istotna i interesująca z punktu widzenia omawianych tematów, w celu uzyskania spostrzeżeń, wiedzy fachowej lub porad. Osoby takie będą pełnić funkcję obserwatorów *ad hoc* bez prawa głosu.

(60) Zarząd powinien podejmować decyzje bezwzględną większością głosów swoich członków posiadających prawo głosu, chyba że niniejsze rozporządzenie stanowi inaczej. Ze względu na znaczenie kwestii budżetowych i kadrowych, w szczególności kwestii dotyczących rocznego budżetu, rocznego sprawozdania z działalności, strategii zwalczania nadużyć finansowych, przepisów wykonawczych wprowadzających w życie regulamin pracowniczy, mianowania dyrektora wykonawczego, zastępcy dyrektora wykonawczego i księgowego, działań następczych w związku z ustaleniami Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych (OLAF) i Prokuratury Europejskiej (EPPO) oraz przyjęcia przepisów finansowych ENISA, zarząd powinien podejmować takie decyzje wyłącznie w przypadku, gdy przedstawiciel Komisji odda głos za. Do celów podjęcia decyzji w sprawie przyjęcia ostatecznego jednolitego dokumentu programowego po przeprowadzeniu , z uwzględnieniem opinii Komisji, pozytywny głos przedstawiciela Komisji powinien być wymagany wyłącznie w odniesieniu do elementów decyzji niezwiązanych z rocznym i wieloletnim programem prac ENISA.

(61) Zarząd wykonawczy powinien przyczyniać się do skutecznego funkcjonowania zarządu. W ramach prac przygotowawczych związanych z decyzjami zarządu zarząd wykonawczy powinien szczegółowo analizować istotne informacje, badać dostępne opcje oraz przedstawiać porady i rozwiązania w celu przygotowania decyzji zarządu. Powinien on również wspierać dyrektora wykonawczego i doradzać mu w zakresie wdrażania decyzji zarządu.

(62) Sprawne funkcjonowanie ENISA wymaga, aby dyrektor wykonawczy był mianowany na podstawie osiągnięć i udokumentowanych umiejętności administracyjnych i zarządczych, a także kompetencji i doświadczenia w zakresie cyberbezpieczeństwa. Dyrektor wykonawczy powinien wykonywać swoje obowiązki w sposób całkowicie niezależny. Zarząd powinien mianować dyrektora wykonawczego z listy kandydatów przygotowanej przez Komisję, w ramach otwartej i przejrzystej procedury, z poszanowaniem zasady równowagi płci.

(63) Dyrektor wykonawczy powinien przygotować wniosek dotyczący jednolitego dokumentu programowego ENISA, po uprzedniej konsultacji z Komisją, oraz podjąć wszelkie niezbędne kroki w celu zapewnienia właściwego wdrożenia tego jednolitego dokumentu programowego. Dyrektor wykonawczy powinien przygotować roczne sprawozdanie, które zostanie przedłożone zarządowi, obejmujące realizację rocznego programu prac ENISA, sporządzić projekt preliminarza dochodów i wydatków ENISA oraz wykonać budżet. Ponadto dyrektor wykonawczy powinien mieć możliwość powoływania grup roboczych *ad hoc* w celu rozpatrywania konkretnych spraw, w szczególności spraw o charakterze naukowym, technicznym, prawnym lub społeczno-gospodarczym. W szczególności w odniesieniu do przygotowania konkretnego europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa („system kandydujący") za konieczne uznaje się powołanie grupy roboczej *ad hoc*. Powołanie grupy roboczej *ad hoc* może być również konieczne w celu prowadzenia działań związanych z utrzymaniem konkretnych przyjętych europejskich systemów certyfikacji

w zakresie cyberbezpieczeństwa. Grupy robocze *ad hoc* powinny być również powoływane w celu opracowania i utrzymania europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa oraz wspierania Agencji w zarządzaniu, wdrażaniu i rozwijaniu ECSF. Dyrektor wykonawczy powinien zapewnić, aby członkowie grup roboczych *ad hoc* byli wybierani zgodnie z najwyższymi standardami wiedzy fachowej, dążąc do zapewnienia równowagi płci oraz odpowiedniej równowagi, w zależności od konkretnych kwestii, między administracjami publicznymi państw członkowskich, podmiotami unijnymi i sektorem prywatnym, w tym przemysłem, użytkownikami i ekspertami akademickimi w dziedzinie bezpieczeństwa sieci i informacji, a także ekspertami akademickimi w dziedzinie produktów zawierających elementy cyfrowe.

(64) Zarząd może podjąć decyzję o utworzeniu stanowiska zastępcy dyrektora wykonawczego, który będzie wspierał dyrektora wykonawczego, jeżeli zarząd uzna, że stanowisko takie jest niezbędne do zapewnienia lub utrzymania sprawnego funkcjonowania ENISA. Podejmując decyzję o utworzeniu tego stanowiska, zarząd może uwzględnić opinię dyrektora wykonawczego.

(65) ENISA powinna posiadać grupę doradczą w celu zapewnienia regularnego dialogu z sektorem prywatnym, organizacjami konsumentów i innymi zainteresowanymi stronami. Grupa doradcza ENISA, powołana przez zarząd na wniosek dyrektora wykonawczego, powinna skupiać się na kwestiach istotnych dla zainteresowanych stron i zwracać na nie uwagę ENISA. Z grupą doradczą ENISA należy konsultować się w szczególności w odniesieniu do projektu rocznego programu prac ENISA. Skład grupy doradczej ENISA i powierzone jej zadania powinny zapewniać wystarczającą reprezentację zainteresowanych stron w pracach ENISA. Przedstawiciele krajowych i unijnych organów ścigania, organów ochrony danych i organów nadzoru rynku powinni mieć prawo do reprezentacji w grupie doradczej ENISA.

(66) Osoby ubiegające się o status autoryzowanego dostawcy poświadczeń lub o przedłużenie autoryzacji powinny mieć dostęp do niezbędnych środków odwoławczych, jeżeli dotyczą ich decyzje podjęte przez ENISA. W związku z tym należy ustanowić odpowiedni mechanizm odwoławczy, tak aby związane z tym decyzje ENISA mogły być zaskarżane przed komisją odwoławczą, której decyzje mogą podlegać kontroli sądowej Trybunału Sprawiedliwości Unii Europejskiej zgodnie z traktatami. Wymóg wyczerpania procedury odwoławczej w ramach ENISA przed wniesieniem skargi do Trybunału Sprawiedliwości Unii Europejskiej ma zastosowanie wyłącznie do osób posiadających legitymację procesową przed komisją odwoławczą.

(67) Aby zagwarantować pełną autonomię i niezależność ENISA oraz umożliwić jej wykonywanie zadań, ENISA powinna otrzymać wystarczający i autonomiczny budżet finansowany głównie ze środków Unii, ale także ze środków państw trzecich uczestniczących w pracach ENISA oraz z opłat uiszczanych przez uprawnionych dostawców poświadczeń i jednostki oceniające zgodność uczestniczące w systemach i wydające europejskie certyfikaty cyberbezpieczeństwa oraz unijne deklaracje zgodności. Państwo członkowskie przyjmujące oraz każde inne państwo członkowskie powinno mieć możliwość wnoszenia dobrowolnych wkładów do budżetu ENISA. Żaden wkład, finansowy lub rzeczowy, otrzymany przez ENISA od państw członkowskich, państw trzecich lub innych podmiotów lub osób, nie powinien zagrażać jej niezależności i bezstronności. Procedura budżetowa Unii powinna mieć zastosowanie w odniesieniu do wkładu Unii i wszelkich innych dotacji pokrywanych z budżetu ogólnego Unii. Trybunał Obrachunkowy powinien przeprowadzać kontrolę rachunków ENISA w celu zapewnienia przejrzystości i rozliczalności. Aby umożliwić

agencji udział we wszystkich istotnych przyszłych projektach, należy jej zapewnić możliwość otrzymywania dotacji.

(68) Aby zapewnić zdolność ENISA do reagowania na zapotrzebowanie na prowadzone przez nią działania, w szczególności w odniesieniu do decyzji o upoważnieniu dostawców do wydawania europejskich indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa oraz w odniesieniu do utrzymania europejskich systemów certyfikacji cyberbezpieczeństwa i narzędzi testowych, ENISA powinna otrzymać uprawnienia do pobierania opłat. Opłaty związane z rozpatrywaniem wniosków o uzyskanie statusu uprawnionego dostawcy certyfikatów powinny być odpowiednio ustalone, aby w wystarczającym stopniu pokrywać szacunkowe koszty opracowania i utrzymania europejskich systemów certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa oraz oceny, czy wymogi i obowiązki związane z uzyskaniem i utrzymaniem statusu uprawnionego dostawcy certyfikatów są i nadal będą spełniane. Opłaty związane z kosztami wydawania i odnawiania upoważnień dla uprawnionych dostawców certyfikatów powinny obejmować koszty związane z ocenami przeprowadzanymi przez ENISA lub pod jej nadzorem. Opłaty związane z uczestnictwem w europejskich systemach certyfikacji w zakresie cyberbezpieczeństwa oraz z wydawaniem certyfikatów w ramach takich systemów powinny być odpowiednio ustalone, aby w wystarczającym stopniu pokrywać szacunkowe koszty utrzymania takich systemów. Uiszczanie takich opłat powinno umożliwić notyfikowanym jednostkom oceniającym zgodność oraz, w stosownych przypadkach, posiadaczom certyfikatów w ramach systemu uczestnictwo w takich działaniach, a także w odpowiednich działaniach w zakresie budowania potencjału i działaniach promocyjnych mających na celu promowanie wymiany najlepszych praktyk i wspieranie wdrażania systemów i certyfikowanych rozwiązań.

(69) Aby zapewnić proporcjonalność, przejrzystość i pewność prawną, opłaty powinny być ustalane w sposób przejrzysty i sprawiedliwy. Wszystkie wydatki ENISA związane z personelem zaangażowanym w działalność podlegającą opłatom w ramach systemu oceny zgodności ( ), w szczególności proporcjonalny wkład pracodawcy do systemu emerytalnego oraz koszty związane z komisją odwoławczą, powinny być odzwierciedlone w tych kosztach. Opłaty nie mogą prowadzić do nakładania niepotrzebnych obciążeń finansowych lub administracyjnych na wnioskodawców. Należy ustalić rozsądne terminy uiszczania opłat.

(70) Konieczne jest ustanowienie zestawu wskaźników służących do pomiaru obciążenia pracą agencji, jej skuteczności i wydajności w odniesieniu do działań finansowanych z opłat. Biorąc pod uwagę te wskaźniki, agencja powinna dostosować planowanie zatrudnienia i zarządzanie zasobami związanymi z opłatami, aby móc odpowiednio reagować na takie zapotrzebowanie i wszelkie wahania dochodów z opłat.

(71) Aby zidentyfikować i właściwie zarządzać ryzykiem rzeczywistego lub postrzeganego konfliktu interesów, ENISA powinna posiadać zasady dotyczące zapobiegania konfliktom interesów i zarządzania nimi. ENISA powinna również stosować zasady dotyczące dostępu do dokumentów określone w rozporządzeniu (WE) nr 1049/2001 Parlamentu Europejskiego i Rady[54] . Przetwarzanie danych osobowych przez ENISA powinno podlegać przepisom rozporządzenia Parlamentu Europejskiego i Rady (UE)

[54] Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43, ELI: http://data.europa.eu/eli/reg/2001/1049/oj).

2018/1725[55] . ENISA powinna przestrzegać przepisów mających zastosowanie do podmiotów unijnych oraz przepisów krajowych dotyczących postępowania z informacjami, w szczególności z informacjami wrażliwymi nieobjętymi klauzulą tajności oraz informacjami niejawnymi Unii Europejskiej (EUCI).

(72) Wykonując swoje zadania, ENISA może mieć dostęp do informacji szczególnie chronionych, takich jak informacje dotyczące cyberzagrożeń i incydentów. Dlatego też niezwykle ważne jest, aby ENISA zachowała poufność informacji, którymi dysponuje. W szczególności, zgodnie z art. 339 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), urzędnicy i inni pracownicy ENISA nie powinni ujawniać żadnych informacji objętych tajemnicą zawodową, w szczególności informacji dotyczących przedsiębiorstw, ich stosunków handlowych lub składników kosztów, nawet po zakończeniu pełnienia swoich obowiązków.

(73) Aby zapewnić pełną realizację swoich celów, ENISA powinna współpracować z odpowiednimi organami nadzorczymi Unii oraz innymi właściwymi organami w Unii, odpowiednimi podmiotami Unii, w tym CERT-EU, EC3 w Europolu, ECCC, Europejską Agencją Obrony (EDA), Agencją Unii Europejskiej ds. Programu Kosmicznego (EUSPA), Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), Europejską Agencją ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), Europejskim Bankiem Centralnym (EBC), Europejskim Urzędem Nadzoru Bankowego (EBA), Europejską Radą Ochrony Danych, Agencją ds. Współpracy Organów Regulacji Energetyki (ACER), Agencją Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA) oraz wszelkimi innymi podmiotami Unii zajmującymi się cyberbezpieczeństwem. ENISA powinna również współpracować z właściwymi organami na mocy dyrektywy (UE) 2022/2555, organami nadzoru rynku i organami zajmującymi się ochroną danych w celu wymiany wiedzy fachowej i najlepszych praktyk oraz powinna udzielać porad w kwestiach związanych z cyberbezpieczeństwem, które mogą mieć wpływ na ich pracę.

(74) Europol odgrywa ważną rolę w zapobieganiu cyberprzestępczości i jej zwalczaniu, w tym cyberprzestępczości związanej z incydentami bezpieczeństwa sieci i informacji. Aby stworzyć synergię między odpowiednimi zadaniami każdej agencji, ENISA powinna współpracować z Europolem, w szczególności poprzez wymianę informacji dotyczących trendów w zakresie technik, żądań i skutków ataków ransomware. Współpraca ta może również polegać na identyfikowaniu najczęstszych odmian ransomware atakujących podmioty wymienione w załącznikach I i II do dyrektywy (UE) 2022/2555 w celu wspierania podmiotów o znaczeniu kluczowym i istotnym w reagowaniu na incydenty i przywracaniu sprawności.

(75) Aby wspierać współpracę operacyjną i wspólną świadomość sytuacji w zakresie cyberzagrożeń i incydentów, niezbędna jest współpraca ENISA z zainteresowanymi stronami, a w szczególności z przedsiębiorstwami i organizacjami z sektora prywatnego, z którymi ENISA może nawiązać partnerstwa publiczno-prywatne.

(76) Aby skutecznie realizować cele określone w niniejszym rozporządzeniu, ENISA może współpracować w szczególności z instytucjami akademickimi prowadzącymi badania

[55] 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 i decyzję nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

w odpowiednich dziedzinach oraz opracowywać odpowiednie kanały przekazywania informacji od organizacji konsumenckich i innych organizacji.

(77) Ze względu na transgraniczny charakter cyberzagrożeń i incydentów cyberbezpieczeństwa poziom cyberbezpieczeństwa i gotowości państw trzecich może mieć wpływ na podmioty w Unii. W związku z tym ENISA powinna mieć możliwość prowadzenia działań w zakresie budowania potencjału, w tym szkoleń, budowania potencjału, działań partnerskich w państwach trzecich, a w szczególności dostosowanych do potrzeb działań w zakresie budowania potencjału dla państw kandydujących do przystąpienia do Unii lub innych państw partnerskich zgodnie z priorytetami Unii. Działania takie powinny być prowadzone na podstawie konkretnego wniosku o zapewnienie odpowiedniego wsparcia, z uwzględnieniem priorytetów Unii, i powinny być realizowane w ramach specjalnych ustaleń, w tym umów o wkładzie, o których mowa w rozporządzeniu (UE, Euratom) 2024/2509. Europejskie ramy certyfikacji w zakresie cyberbezpieczeństwa mają na celu ochronę przed zagrożeniami cybernetycznymi, takimi jak złośliwie wykorzystywane luki w cyberbezpieczeństwie lub incydenty związane z cyberbezpieczeństwem, które mają wpływ na funkcjonalność (projekt i działanie) produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów. Koncentrując się na ryzykach technicznych związanych z produktami ICT, usługami ICT, procesami ICT, zarządzanymi usługami bezpieczeństwa lub cyberbezpieczeństwem podmiotów, ECCF powinny uzupełniać ramy bezpieczeństwa łańcuchów dostaw ICT, których celem jest zapewnienie zharmonizowanego podejścia na poziomie Unii do ryzyk nietechnicznych w sektorach o wysokim znaczeniu krytycznym i innych sektorach krytycznych.

(78) Państwa członkowskie powinny mieć możliwość korzystania z europejskiej certyfikacji w zakresie cyberbezpieczeństwa w kontekście zamówień publicznych zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2014/24/UE[56] .

(79) Aby ułatwić podmiotom dostosowanie się do wymogów, ECCF powinien zapewnić im możliwość certyfikacji ich stanu cyberbezpieczeństwa. Podmioty, w szczególności te świadczące wiele rodzajów usług w kilku państwach członkowskich, mogą podlegać różnym obowiązkom w zakresie cyberbezpieczeństwa i bezpieczeństwa danych wynikającym z instrumentów horyzontalnych, takich jak rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679[57] oraz dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555[58] , a także z instrumentów sektorowych. W celu usprawnienia wdrażania ogólnych ram regulacyjnych w zakresie cyberbezpieczeństwa i ułatwienia ich przestrzegania, prawodawstwo Unii powinno przewidywać możliwość wykazania przez podmioty zgodności z wymogami w zakresie zarządzania ryzykiem cyberbezpieczeństwa poprzez europejski certyfikat cyberbezpieczeństwa. Odpowiedni system mógłby przyczynić się do usprawnienia wymogów dotyczących zgodności

---

56 Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych i uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65, ELI: http://data.europa.eu/eli/dir/2014/24/oj).

57 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych oraz uchylające dyrektywę 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

58 Dyrektywa (UE) 2022/2555 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa cybernetycznego 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).

wynikających z różnych instrumentów regulacyjnych, bez uszczerbku dla ich szczegółowych wymogów certyfikacyjnych. Takie środki upraszczające mogą potencjalnie zmniejszyć obciążenia administracyjne, uwalniając zasoby na wzmocnienie gotowości operacyjnej podmiotów w krytycznych sektorach Unii w zakresie cyberbezpieczeństwa.

(80) Europejska certyfikacja wymogów w zakresie zarządzania ryzykiem związanym z cyberbezpieczeństwem opracowana w ramach ECCF powinna umożliwić podmiotom wykazanie zgodności z odpowiednim prawodawstwem Unii, jeżeli system obejmuje odpowiednie wymogi prawne określone w takim akcie prawnym i jeżeli tak stanowi. Na tej podstawie akt prawny Unii może również przewidywać domniemanie zgodności z tymi wymogami. Systemy takie mogłyby przyczynić się do poprawy spójnego wdrażania wymogów w zakresie cyberbezpieczeństwa określonych w prawodawstwie Unii w celu wyrównania szans w państwach członkowskich i zmniejszenia obciążenia związanego z zapewnieniem zgodności.

(81) Europejskie ramy certyfikacji w zakresie cyberbezpieczeństwa powinny przewidywać możliwość certyfikacji procesów ICT, definiowanych jako zestaw działań wykonywanych w celu zaprojektowania, opracowania, dostarczenia lub utrzymania produktu lub usługi ICT. Przykładem procesu ICT jest profil ochrony określony w rozporządzeniu wykonawczym Komisji (UE) 2024/482[59] . Innym przykładem procesu ICT jest zestaw działań podejmowanych przez producenta w celu bezpiecznego projektowania i opracowywania produktu ICT, w tym fizyczne, logiczne, proceduralne, personalne i inne środki bezpieczeństwa niezbędne do ochrony poufności i integralności projektu i wdrożenia produktu ICT w jego środowisku rozwoju. Certyfikacja takich działań jest często określana jako „certyfikacja zakładu” w kontekście procesu certyfikacji zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/482.

(82) Definicja zarządzanych usług bezpieczeństwa w niniejszym rozporządzeniu powinna być spójna z definicją dostawców zarządzanych usług bezpieczeństwa zawartą w dyrektywie (UE) 2022/2555. Usługi te polegają na wykonywaniu lub świadczeniu pomocy w zakresie działań związanych z zarządzaniem ryzykiem cyberbezpieczeństwa ich klientów i zyskują coraz większe znaczenie w zapobieganiu incydentom i łagodzeniu ich skutków. W związku z tym dostawcy tych usług są uznawani za podmioty o znaczeniu krytycznym lub istotnym, należące do sektora o wysokim stopniu krytyczności zgodnie z dyrektywą (UE) 2022/2555. Dostawcy zarządzanych usług bezpieczeństwa w takich obszarach, jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo, odgrywają szczególnie ważną rolę we wspieraniu podmiotów w ich wysiłkach na rzecz zapobiegania incydentom, ich wykrywania, reagowania na nie lub usuwania ich skutków. Jednakże dostawcy zarządzanych usług bezpieczeństwa sami również stali się celem cyberataków i stanowią szczególne ryzyko ze względu na ich ścisłą integrację z działalnością swoich klientów. Konieczne jest zatem, aby podmioty o znaczeniu krytycznym i istotnym w rozumieniu dyrektywy (UE) 2022/2555 ( ) zachowywały zwiększoną staranność przy wyborze dostawców zarządzanych usług bezpieczeństwa.

(83) Europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa są istotne dla szerokiego grona zainteresowanych stron, takich jak dostawcy rozwiązań ICT, organy

[59] Rozporządzenie wykonawcze Komisji (UE) 2024/482 z dnia 31 stycznia 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do przyjęcia europejskiego systemu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC) (Dz.U. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

oceny zgodności i użytkownicy. Aby promować szerokie zaangażowanie zainteresowanych stron, co najmniej raz w roku należy organizować europejskie zgromadzenie ds. certyfikacji w zakresie cyberbezpieczeństwa („zgromadzenie") w celu wspierania współpracy między Komisją, ENISA, państwami członkowskimi i odpowiednimi zainteresowanymi stronami. Zgromadzenie to będzie odgrywać kluczową rolę w identyfikowaniu nowych wyzwań w zakresie cyberbezpieczeństwa i strategicznych priorytetów w zakresie certyfikacji oraz w reagowaniu na nie, a także w zapewnianiu, aby systemy certyfikacji ułatwiały bezpieczną integrację technologii cyfrowych i były dostosowane do potrzeb użytkowników. Zgromadzenie powinno wspierać wiodącą rolę Unii w działaniach certyfikacyjnych oraz utrzymywać zdolność ram certyfikacji do budowania zaufania przedsiębiorstw, organów publicznych i społeczeństwa.

(84) Komisja powinna prowadzić specjalną stronę internetową w celu zapewnienia przejrzystości poprzez publikowanie aktualnych informacji na temat postępów we wdrażaniu ECCF. Strona internetowa powinna zawierać informacje dotyczące przygotowywanych systemów certyfikacji, priorytetów strategicznych dla przyszłych systemów certyfikacji, wniosków skierowanych do ENISA o przygotowanie kandydackich systemów certyfikacji oraz informacje na temat przyjmowania systemów certyfikacji. Strona internetowa Komisji będzie uzupełnieniem strony internetowej ENISA poświęconej europejskim systemom certyfikacji w zakresie cyberbezpieczeństwa, która powinna zawierać wyczerpujące informacje na temat przygotowań technicznych systemów kandydujących i utrzymania systemów, ze szczególnym uwzględnieniem wydanych europejskich certyfikatów cyberbezpieczeństwa i unijnych oświadczeń o zgodności.

(85) W celu zacieśnienia dialogu między instytucjami Unii oraz przyczynienia się do formalnego, otwartego, przejrzystego i integracyjnego procesu konsultacji Komisja powinna uwzględnić elementy wynikające z opinii wyrażonych przez Parlament Europejski, Radę i Europejskie Zgromadzenie ds. Certyfikacji Cyberbezpieczeństwa podczas oceny niniejszego rozporządzenia.

(86) Studia wykonalności przeprowadzone przez ENISA powinny pomóc w przygotowaniu planowania i opracowywania systemów certyfikacji w zakresie cyberbezpieczeństwa. Badania powinny uwzględniać perspektywy odpowiednich zainteresowanych stron i dostosowywać przyszłe systemy certyfikacji do bieżących działań w zakresie badań, rozwoju i oceny technologicznej, uznając w szczególności wkład inicjatyw badawczych Unii i państw członkowskich. Badania takie mogą pomóc w identyfikacji dostępnych norm i specyfikacji technicznych. Powinny one być przeprowadzane na wniosek Komisji lub zgodnie z priorytetami strategicznymi Unii, aby zapewnić odpowiednie uwzględnienie i odzwierciedlenie zmieniającego się krajobrazu technologicznego i potrzeb w zakresie cyberbezpieczeństwa przy składaniu wniosków o ustanowienie systemów i opracowywaniu ich.

(87) Projekt systemu kandydującego oraz zakres celów i elementów bezpieczeństwa, które obejmuje, powinny być proporcjonalne do przedmiotu i zakresu certyfikacji. Na przykład system certyfikacji usług w chmurze może zatem odnosić się do celów bezpieczeństwa, które są istotne dla usług ICT i bezpieczeństwa organizacyjnego. Innym przykładem może być cel bezpieczeństwa związany z wykluczeniem znanych podatności, które można wykorzystać, który prawdopodobnie nie będzie miał znaczenia dla certyfikacji procesów ICT.

(88) Aby zapewnić harmonijne wdrażanie europejskich systemów certyfikacji cyberbezpieczeństwa we wszystkich państwach członkowskich, konieczne jest ustanowienie zasad dotyczących utrzymania tych systemów. Działania związane z utrzymaniem są również niezbędne, aby zapewnić aktualność systemów i dokumentacji uzupełniającej, zwłaszcza w dziedzinie cyberbezpieczeństwa, gdzie zagrożenia i technologie podlegają ciągłym zmianom. Systemy certyfikacji powinny zatem być projektowane i utrzymywane w sposób pozwalający uniknąć ryzyka ich szybkiego starzenia się. Działania związane z utrzymaniem powinny zazwyczaj obejmować sporządzanie i aktualizowanie dokumentacji uzupełniającej, w tym specyfikacji technicznych i wytycznych, a także identyfikowanie norm lub specyfikacji technicznych, które są istotne dla systemu. Analiza funkcjonowania systemu, jego potencjalnych niedociągnięć i koniecznych ulepszeń powinna również stanowić część działań związanych z utrzymaniem. Ponadto działania związane z utrzymaniem powinny obejmować wymianę informacji między państwami członkowskimi w odniesieniu do wdrażania systemów oraz wkład w mechanizmy wzajemnej oceny i wzajemnej weryfikacji.

(89) Ze względu na techniczny charakter działań związanych z utrzymaniem, ENISA powinna zarządzać takimi działaniami we współpracy z Komisją i przy wsparciu Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa (ECCG) oraz jej odpowiedniej podgrupy ds. utrzymania. Utworzenie podgrupy ECCG ds. utrzymania umożliwia gromadzenie wkładu technicznego i spostrzeżeń państw członkowskich w celu harmonizacji podejść.

(90) Działania związane z utrzymaniem powinny obejmować współpracę z odpowiednimi grupami zainteresowanych stron w celu zapewnienia, aby systemy pozostawały dostosowane do potrzeb rynku i aktualne, w tym poprzez wymianę i otrzymywanie wkładu technicznego. Takimi grupami zainteresowanych stron mogą być organizacje normalizacyjne, organy oceny zgodności, dostawcy, użytkownicy, organy publiczne lub stowarzyszenia branżowe. Specyfika każdego systemu, w tym odpowiadających mu forów technicznych i branż, oznacza, że powinno być możliwe gromadzenie wkładu technicznego w różny sposób w zależności od systemu. W przypadku niektórych systemów ENISA powinna mieć możliwość korzystania z pomocy doraźnej grupy roboczej, w skład której wchodzą eksperci z administracji publicznej państw członkowskich, podmiotów unijnych i sektora prywatnego. Informacje techniczne mogą również pochodzić od ISAC lub organizacji normalizacyjnych. ENISA powinna przeanalizować, jaki format jest najbardziej odpowiedni dla każdego systemu, i uwzględnić strategię utrzymania w każdym systemie kandydującym.

(91) Europejskie systemy certyfikacji cyberbezpieczeństwa powinny opierać się na normach lub specyfikacjach technicznych, w szczególności w odniesieniu do definiowania wymogów bezpieczeństwa i metodologii oceny. ENISA powinna mieć możliwość opracowywania specyfikacji technicznych w celu wsparcia przygotowania i utrzymania systemów, w szczególności w przypadku braku wyników prac organizacji normalizacyjnych lub gdy wyniki te nie są odpowiednie do realizacji celów systemu. W ramach procesu opracowywania specyfikacji ENISA powinna być wspierana przez ECCG oraz, w stosownych przypadkach, przez grupę roboczą ad hoc utworzoną dla danego systemu. ENISA powinna również zwrócić się o wkład do grup zainteresowanych stron. Ponadto ENISA powinna uwzględnić akceptację rynkową, a także normy europejskie i międzynarodowe. Biorąc pod uwagę jakość specyfikacji technicznych i cele systemu, Komisja powinna mieć możliwość odniesienia się do

specyfikacji technicznych opracowanych przez ENISA w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa.

(92) Specyfikacje techniczne opracowane przez ENISA i przywołane w systemie powinny być udostępnione na stronie internetowej ENISA poświęconej europejskim systemom certyfikacji w zakresie cyberbezpieczeństwa, tak aby wszystkie zainteresowane strony miały do nich dostęp. Jednak w niektórych szczególnych przypadkach publikacja na stronie internetowej mogłaby stanowić zagrożenie dla cyberbezpieczeństwa certyfikowanych produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów, a co za tym idzie – dla bezpieczeństwa publicznego. Na przykład specyfikacje techniczne mogą zawierać dokładne informacje na temat nowych ścieżek ataku, których publiczna dostępność umożliwiłaby wykorzystanie ich przez złośliwe podmioty. Tego rodzaju informacje powinny być rozpowszechniane w sposób ograniczony, wyłącznie wśród zainteresowanych stron, które muszą je znać, takich jak krajowe organy certyfikacji w zakresie cyberbezpieczeństwa, organy oceny zgodności i certyfikowani dostawcy. Ze względu na ograniczony zakres rozpowszechniania takie specyfikacje techniczne nie powinny być przywoływane w europejskich systemach certyfikacji w zakresie cyberbezpieczeństwa, a zatem powinny mieć charakter niewiążący.

(93) Systemy certyfikacji cyberbezpieczeństwa powinny być zaprojektowane w sposób modułowy, tak aby umożliwić wykazanie zgodności i domniemanie zgodności z odpowiednimi wymogami w zakresie cyberbezpieczeństwa określonymi w innych przepisach unijnych, jeżeli przepisy te przewidują taką możliwość. Domniemanie zgodności z wymogami tych aktów prawnych będzie zatem miało zastosowanie jako możliwy sposób wykazania zgodności tylko wtedy, gdy odpowiednie akty prawne umożliwiają takie domniemanie zgodności. Szczegóły takiego systemu, a mianowicie cel, zadania lub elementy, będą zatem prawdopodobnie różnić się od szczegółów innych systemów. W szczególności systemy certyfikacji cyberbezpieczeństwa podmiotów powinny być opracowane w taki sposób, aby umożliwić ocenę ciągłej zgodności podmiotu z przepisami unijnymi. Nie jest zatem konieczne, aby systemy certyfikacji cyberbezpieczeństwa obejmowały wszystkie elementy europejskich systemów certyfikacji cyberbezpieczeństwa, takie jak poziomy zapewnienia, co powinno znaleźć odzwierciedlenie w przepisach dotyczących tych systemów.

(94) Ramy certyfikacji cyberbezpieczeństwa w ECCF umożliwiają opracowanie systemu, który pozwala podmiotom świadczącym usługi w kilku państwach członkowskich wykazać zgodność z obowiązkami w zakresie zarządzania ryzykiem cyberbezpieczeństwa określonymi w dyrektywie Parlamentu Europejskiego i Rady 2022/2555. Na tej podstawie, dzięki możliwości wykazania zgodności, podmioty mogą korzystać z bardziej spójnych i mniej uciążliwych podejść nadzorczych na całym rynku wewnętrznym. Opracowanie takiego systemu certyfikacji powinno zostać ułatwione poprzez przyjęcie aktów wykonawczych na mocy dyrektywy (UE) 2022/2555. Dzięki profilom rozszerzenia system certyfikacji cyberbezpieczeństwa może wykazać zgodność z wymogami w przypadku, gdy państwo członkowskie przyjęło lub utrzymało przepisy zapewniające wyższy poziom cyberbezpieczeństwa zgodnie z dyrektywą (UE) 2022/2555. Na tej podstawie podmiot świadczący usługi w kilku państwach członkowskich może wykazać zgodność ze wszystkimi odpowiednimi profilami rozszerzeń za pomocą jednego europejskiego certyfikatu cyberbezpieczeństwa.

(95) Cele bezpieczeństwa i wymogi bezpieczeństwa określone w europejskich systemach certyfikacji cyberbezpieczeństwa w odniesieniu do bezpieczeństwa produktów powinny być zgodne z zasadniczymi wymogami w zakresie cyberbezpieczeństwa określonymi w

załączniku I do rozporządzenia (UE) 2024/2847. Spójność ta jest niezbędna, aby zapewnić, że producenci, których produkty wchodzą w zakres rozporządzenia (UE) 2024/2847, nie napotykają sprzecznych wymagań podczas certyfikacji swoich produktów w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa. Ponadto spójność wymogów ułatwia domniemanie zgodności na mocy art. 27 rozporządzenia (UE) 2024/2847, zgodnie z którym producenci produktów zawierających elementy cyfrowe, które zostały certyfikowane w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa, mogą pod pewnymi warunkami korzystać z domniemania zgodności z zasadniczymi wymogami w zakresie cyberbezpieczeństwa określonymi w załączniku I do tego rozporządzenia.

(96) W ramach europejskiego systemu certyfikacji cyberbezpieczeństwa powinno być możliwe określenie profilu rozszerzenia poprzez ustanowienie dodatkowych lub szczegółowych wymogów dotyczących przypadków użycia, w tym dodatkowych możliwości, takich jak ulepszone funkcje produktu, specjalistyczne oferty usług lub zasoby, zoptymalizowane procesy i zaawansowane środki bezpieczeństwa. Ponieważ profile rozszerzenia nie odpowiadają konkretnemu poziomowi zapewnienia, powinny one szczegółowo opisywać swój cel, w tym zagrożenia dla bezpieczeństwa, którym mają zaradzić. Profile rozszerzeń mają w szczególności na celu wykazanie zgodności z określonymi normami i wymogami regulacyjnymi, w tym, w stosownych przypadkach, wymogami dotyczącymi dodatkowych środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa ustanowionych przez państwo członkowskie zgodnie z zasadą minimalnej harmonizacji zgodnie z dyrektywą (UE) 2022/2555.

(97) Bez uszczerbku dla ogólnego systemu wzajemnej oceny, który ma zostać wprowadzony we wszystkich krajowych organach certyfikacji cyberbezpieczeństwa w ramach ECCF, w europejskich systemach certyfikacji cyberbezpieczeństwa powinno być możliwe uwzględnienie mechanizmu wzajemnej oceny organów wydających europejskie certyfikaty cyberbezpieczeństwa dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberpostury podmiotów, w szczególności dla organów wydających certyfikaty o wysokim poziomie zapewnienia w ramach takich systemów. Organy te powinny również obejmować organy certyfikujące krajowych organów certyfikacji w zakresie cyberbezpieczeństwa wydające certyfikaty o wysokim poziomie pewności. ECCG powinna wspierać wdrażanie takich mechanizmów wzajemnej oceny. W ramach wzajemnej oceny należy w szczególności ocenić, czy dane organy wykonują swoje zadania w sposób zharmonizowany, i można w niej uwzględnić mechanizmy odwoławcze.

(98) Kryzysy, takie jak wojny, klęski żywiołowe i pandemie, mogą mieć negatywny wpływ na działalność certyfikacyjną. W scenariuszach kryzysowych tego rodzaju zapewnienie bezpieczeństwa obiektu może być niemożliwe, na przykład z powodu zniszczenia infrastruktury, cyberataków, niedostępności personelu i braku dostępu do obiektu. Europejski system certyfikacji cyberbezpieczeństwa powinien zatem określać tymczasowe zasady dotyczące ciągłości działalności certyfikacyjnej w takich scenariuszach.

(99) Przełożenie technicznych systemów kandydujących na akty wykonawcze wymaga złożonej wiedzy technicznej i prawnej i może powodować znaczne obciążenia administracyjne. Ponadto niektóre elementy europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, takie jak zarządzanie podatnością na zagrożenia lub warunki, na jakich można stosować takie znaki lub etykiety, mają charakter międzysektorowy i mogą skorzystać z harmonizowanych przepisów odniesienia. Aby zapewnić jakość przyjętych europejskich systemów certyfikacji w zakresie

cyberbezpieczeństwa i zmniejszyć obciążenia związane z zapewnieniem zgodności dla przedsiębiorstw, Komisja powinna być uprawniona do przyjmowania przepisów wzorcowych obejmujących niektóre elementy europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa.

(100) Aby zapewnić spójność europejskich ram certyfikacji w zakresie cyberbezpieczeństwa, w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa powinno być możliwe określenie poziomów zapewnienia dla europejskich certyfikatów cyberbezpieczeństwa i unijnych oświadczeń o zgodności wydanych w ramach tego systemu. Europejski certyfikat cyberbezpieczeństwa powinien odnosić się do jednego z poziomów zapewnienia: „podstawowego", „znacznego" lub „wysokiego", natomiast unijne oświadczenie o zgodności powinno odnosić się wyłącznie do poziomu zapewnienia „podstawowego". Poziomy zapewnienia powinny zapewniać odpowiednią rygorystyczność i dogłębność oceny produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub stanu cyberbezpieczeństwa podmiotu i powinny być scharakteryzowane poprzez odniesienie do związanych z nimi specyfikacji technicznych, norm i procedur, w tym kontroli technicznych, których celem jest łagodzenie skutków incydentów lub zapobieganie im. Każdy poziom zapewnienia powinien być spójny w różnych obszarach sektorowych, w których stosuje się certyfikację.

(101) Wybór odpowiedniej certyfikacji i związanych z nią wymogów bezpieczeństwa przez użytkowników europejskich certyfikatów cyberbezpieczeństwa powinien opierać się na analizie ryzyka związanego z wykorzystaniem produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub kontekstu certyfikacji podmiotów. W związku z tym poziom zapewnienia powinien być proporcjonalny do poziomu ryzyka związanego z zamierzonym wykorzystaniem produktu ICT, usługi ICT, procesu ICT, zarządzanych usług bezpieczeństwa lub środowiska operacyjnego i charakteru podmiotu, którego cyberbezpieczeństwo podlega certyfikacji.

(102) W przypadku poziomu zapewnienia „podstawowego" ocena powinna opierać się co najmniej na następujących elementach zapewnienia: ocena powinna obejmować co najmniej przegląd dokumentacji technicznej dotyczącej produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub cyberbezpieczeństwa podmiotu przeprowadzony przez jednostkę oceniającą zgodność. W przypadku gdy certyfikacja obejmuje procesy ICT, proces stosowany do projektowania, opracowywania i utrzymywania produktu ICT, usługi ICT, zarządzanej usługi bezpieczeństwa lub cyberbezpieczeństwa podmiotu również powinien podlegać przeglądowi technicznemu. W przypadku gdy europejski system certyfikacji cyberbezpieczeństwa przewiduje samoocenę zgodności, wystarczające powinno być przeprowadzenie przez producenta lub dostawcę produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa lub przez podmiot, którego cyberbezpieczeństwo podlega certyfikacji, samooceny zgodności produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub cyberbezpieczeństwa podmiotu z systemem certyfikacji.

(103) W przypadku poziomu zapewnienia „znacznego" ocena, oprócz wymogów dotyczących poziomu zapewnienia „podstawowego", powinna opierać się co najmniej na weryfikacji zgodności funkcji bezpieczeństwa produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub stanu cyberbezpieczeństwa podmiotu z jego dokumentacją techniczną.

(104) W przypadku poziomu pewności „wysokiego" ocena, oprócz wymogów dotyczących poziomu pewności „znacznego", powinna opierać się co najmniej na testach

skuteczności, które oceniają odporność funkcji bezpieczeństwa na wyrafinowane cyberataki przeprowadzane przez osoby posiadające znaczne umiejętności i zasoby. Działania związane z oceną zgodności powinny być przeprowadzane w Europejskim Obszarze Gospodarczym w przypadku poziomu pewności „wysokiego" lub w przypadku gdy system ma na celu wykazanie zgodności i zapewnienie domniemania zgodności z innymi przepisami unijnymi. Wymóg ten jest uzasadniony faktem, że działania związane z oceną przeprowadzane poza Europejskim Obszarem Gospodarczym powodują dodatkowe zagrożenia dla cyberbezpieczeństwa, w szczególności dla własności intelektualnej ocenianych produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiotów. Na przykład kod źródłowy produktu ICT mógłby zostać poddany kontroli podczas przekraczania granicy państwa trzeciego, co stanowi zagrożenie dla własności intelektualnej. Ponadto laboratoria badawcze z siedzibą w państwach trzecich nie działają w środowisku, które podlega środkom bezpieczeństwa cybernetycznego wymaganym przez przepisy UE, takie jak dyrektywa (UE) 2022/2555 lub rozporządzenie (UE) 2024/2847. Na przykład laboratorium badawcze może korzystać z usług zewnętrznego dostawcy usług w chmurze, który nie przestrzega wymogów w zakresie cyberbezpieczeństwa określonych w dyrektywie (UE) 2022/2555. Niemniej jednak system certyfikacji powinien umożliwiać stosowanie mechanizmów odstępstw, na przykład w odniesieniu do certyfikacji obiektów lub w innych przypadkach, gdy działania związane z oceną zgodności nie mogą być w rozsądny sposób przeprowadzone w Europejskim Obszarze Gospodarczym.

(105) W niektórych przypadkach może być konieczne zastosowanie różnych podejść do osiągnięcia celów bezpieczeństwa określonego poziomu zapewnienia, aby uwzględnić specyfikę produktu ICT, usługi ICT, procesu ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów. Aby umożliwić bardziej szczegółowe podejście, w europejskim systemie certyfikacji cyberbezpieczeństwa powinno być możliwe określenie jednego lub kilku poziomów oceny odpowiadających jednemu z poziomów zapewnienia. Umożliwi to opracowanie systemów, w których wiele poziomów oceny przeznaczonych do różnych celów będzie odpowiadało poziomowi bezpieczeństwa związanemu z konkretnym poziomem zapewnienia.

(106) Europejskie systemy certyfikacji cyberbezpieczeństwa powinny umożliwiać przeprowadzanie oceny zgodności pod wyłączną odpowiedzialnością producenta lub dostawcy produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa lub podmiotu, którego cyberbezpieczeństwo jest certyfikowane („samodzielna ocena zgodności"). W takich przypadkach wystarczające powinno być, aby producent, dostawca lub podmiot, którego cyberpostura jest certyfikowana, samodzielnie przeprowadził wszystkie kontrole w celu zapewnienia zgodności produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyber y podmiotu z europejskim systemem certyfikacji cyberbezpieczeństwa. Samoocena zgodności powinna być uznana za odpowiednią w przypadku produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyber u podmiotu, które charakteryzują się niską złożonością, stanowią niewielkie zagrożenie dla społeczeństwa i mają prostą konstrukcję lub proste mechanizmy produkcji.

(107) W przypadku gdy europejski system certyfikacji w zakresie cyberbezpieczeństwa dopuszcza zarówno samoocenę zgodności, jak i certyfikację produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberxml-ph-0000@deepl.internalu podmiotów, system certyfikacji powinien zapewniać konsumentom lub innym użytkownikom jasne i zrozumiałe środki umożliwiające

rozróżnienie między produktami ICT, usługami ICT, procesami ICT, zarządzanymi usługami bezpieczeństwa lub cyberxml-ph-0000@deepl.internalem podmiotów poddanych samoocenie a produktami, usługami, procesami, usługami lub cyberxml-ph-0000@deepl.internalem poddanym certyfikacji przez stronę trzecią.

(108) Producent lub dostawca produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa lub podmioty, których cyberbezpieczeństwo zostało certyfikowane, powinni być w stanie wystawić i podpisać oświadczenie UE o zgodności w ramach procedury oceny zgodności. Oświadczenie UE o zgodności jest dokumentem stwierdzającym, że określony produkt ICT, usługa ICT, proces ICT, zarządzana usługa bezpieczeństwa lub cyberbezpieczeństwo podmiotu spełnia wymagania europejskiego systemu certyfikacji cyberbezpieczeństwa. Wydając i podpisując oświadczenie UE o zgodności, producent lub dostawca produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa lub podmiot, którego cyberbezpieczeństwo zostało certyfikowane, przyjmuje odpowiedzialność za zgodność produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub cyberbezpieczeństwa podmiotu z wymogami bezpieczeństwa europejskiego systemu certyfikacji cyberbezpieczeństwa. Kopia oświadczenia UE o zgodności powinna zostać przedłożona krajowemu organowi certyfikacji cyberbezpieczeństwa oraz ENISA.

(109) Producenci lub dostawcy produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa lub podmioty, których cyberbezpieczeństwo jest certyfikowane, powinni udostępnić właściwemu krajowemu organowi certyfikacji cyberbezpieczeństwa oświadczenie UE o zgodności, dokumentację techniczną i wszelkie inne istotne informacje dotyczące zgodności z europejskim systemem certyfikacji cyberbezpieczeństwa przez okres przewidziany w odpowiednim europejskim systemie certyfikacji cyberbezpieczeństwa i zgodnie z obowiązującym prawodawstwem Unii. Dokumentacja techniczna powinna określać wymagania mające zastosowanie w ramach systemu w zakresie istotnym dla samooceny zgodności. Dokumentacja techniczna powinna być sporządzona w taki sposób, aby umożliwić ocenę, czy produkt ICT, usługa ICT, proces ICT lub zarządzana usługa bezpieczeństwa, lub cyberbezpieczeństwo podmiotu są zgodne z wymaganiami mającymi zastosowanie w ramach systemu.

(110) Europejskie certyfikaty cyberbezpieczeństwa i unijne oświadczenia o zgodności powinny pomagać użytkownikom w dokonywaniu świadomych wyborów. W związku z tym odpowiednie informacje powinny być publikowane na stronie internetowej prowadzonej przez ENISA. Ponadto produktom ICT, usługom ICT i procesom ICT, które zostały certyfikowane lub dla których wydano unijne oświadczenie o zgodności, powinny towarzyszyć ustrukturyzowane informacje dostosowane do oczekiwanego poziomu technicznego docelowego użytkownika. Wszyscy użytkownicy powinni mieć dostęp do informacji dotyczących numeru referencyjnego systemu certyfikacji, organu lub podmiotu wydającego certyfikat oraz, w stosownych przypadkach, poziomu zapewnienia, lub powinni mieć możliwość uzyskania kopii europejskiego certyfikatu cyberbezpieczeństwa. Informacje te powinny być regularnie aktualizowane i udostępniane na specjalnej stronie internetowej poświęconej europejskim systemom certyfikacji cyberbezpieczeństwa. Ponadto, aby zapewnić ciągłą dostępność, producenci i dostawcy powinni być zobowiązani do powiadamiania odpowiedniej jednostki certyfikującej o zmianie lokalizacji informacji online lub, w stosownych przypadkach, informacji fizycznej.

(111) Ocena zgodności to procedura służąca do oceny, czy określone wymagania dotyczące produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub

podmiotu zostały spełnione. Procedura ta jest przeprowadzana przez niezależną stronę trzecią, która nie jest producentem ani dostawcą certyfikowanych produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa, ani też podmiotem, którego cyberbezpieczeństwo jest oceniane. Europejski certyfikat cyberbezpieczeństwa powinien być wydawany po pomyślnej ocenie produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub cyberbezpieczeństwa podmiotu. Europejski certyfikat cyberbezpieczeństwa należy traktować jako potwierdzenie, że ocena została przeprowadzona prawidłowo.

(112) Ścisłe rozdzielenie działań nadzorczych i certyfikacyjnych jest ważne, aby uniknąć zakłóceń i ingerencji, które mogą wystąpić w sytuacjach, gdy podmiot nadzorujący rynek konkuruje również na tym samym rynku. W związku z tym działania, w ramach których krajowe organy certyfikacji w zakresie cyberbezpieczeństwa pełnią jedynie rolę nadzorczą, np. udzielając uprzedniej zgody na wydanie certyfikatu, nie powinny wymagać dalszego wewnętrznego oddzielenia od innych działań nadzorczych. Obejmuje to na przykład sytuację, w której krajowy organ certyfikacji w zakresie cyberbezpieczeństwa aktywnie gromadzi informacje w trakcie procesu certyfikacji przeprowadzanego przez prywatne jednostki oceniające zgodność, a następnie wydaje opinię na temat wydania certyfikatu przez te jednostki („model uprzedniej zgody”).

(113) Europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa powinny określać warunki, w których produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub cyberbezpieczeństwo podmiotu mogą wymagać ponownej certyfikacji lub w których zakres konkretnego europejskiego certyfikatu cyberbezpieczeństwa może wymagać ograniczenia. Ponadto europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa powinny uwzględniać wszelkie możliwe negatywne skutki wykrytych później luk w zabezpieczeniach lub niezgodności dotyczących certyfikowanego produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub cyberpostury podmiotu w odniesieniu do zgodności z wymogami bezpieczeństwa tego certyfikatu.

(114) Harmonizacja odgrywa kluczową rolę w zapewnianiu solidnego cyberbezpieczeństwa i zwiększaniu dostępu przedsiębiorstw do rynku. Natomiast fragmentacja i brak wzajemnego uznawania certyfikatów stanowią istotne przeszkody dla płynnego przepływu danych, zwiększając tym samym koszty operacyjne dla przemysłu unijnego. Aby złagodzić te wyzwania, należy unikać fragmentacji zarówno w zakresie kontroli bezpieczeństwa, jak i metod oceny zgodności w całej Unii.

(115) Państwa członkowskie powinny poinformować Komisję i ECCG z odpowiednim wyprzedzeniem przed przyjęciem nowych krajowych systemów certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberpostury podmiotów, aby pomóc Komisji i ECCG w ocenie wpływu nowego krajowego systemu certyfikacji cyberbezpieczeństwa na prawidłowe funkcjonowanie rynku wewnętrznego oraz w świetle wszelkich strategicznych interesów związanych z wnioskiem o europejski system certyfikacji cyberbezpieczeństwa.

(116) Odniesienia w ustawodawstwie krajowym do norm krajowych, które przestały obowiązywać w związku z wejściem w życie europejskiego systemu certyfikacji cyberbezpieczeństwa, mogą być źródłem niejasności. W związku z tym państwa członkowskie powinny w stosownych przypadkach odzwierciedlić przyjęcie europejskiego systemu certyfikacji cyberbezpieczeństwa w swoim ustawodawstwie krajowym.

(117) W celu ułatwienia rozwoju niezawodnego rynku wewnętrznego, a jednocześnie nawiązania partnerstw z państwami trzecimi, proces certyfikacji ustanowiony w ramach ECCF powinien być wdrażany w sposób ułatwiający międzynarodowe uznawanie, wzajemne uznawanie i dostosowanie do norm międzynarodowych.

(118) W celu dalszego ułatwienia handlu oraz uznając międzynarodowy charakter łańcuchów dostaw ICT, Unia może zawrzeć umowy o wzajemnym uznawaniu europejskich certyfikatów cyberbezpieczeństwa zgodnie z art. 218 TFUE. Komisja powinna być uprawniona do przyjmowania aktów wykonawczych w celu jednostronnego uznawania równoważności certyfikatów państw trzecich z europejskimi certyfikatami cyberbezpieczeństwa. Powinna istnieć możliwość określenia szczegółowych warunków takiego uznawania certyfikatów państw trzecich.

(119) Aby osiągnąć równoważne wdrożenie ram w całej Unii, ułatwić wzajemne uznawanie i promować ogólną akceptację europejskich certyfikatów cyberbezpieczeństwa i unijnych oświadczeń o zgodności, konieczne jest wprowadzenie systemu wzajemnej oceny między krajowymi organami certyfikacji cyberbezpieczeństwa. Wzajemna ocena powinna obejmować procedury nadzorowania zgodności produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberbezpieczeństwa podmiotów posiadających europejskie certyfikaty cyberbezpieczeństwa, monitorowania obowiązków producentów lub dostawców produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i certyfikowanych podmiotów, które przeprowadzają samoocenę zgodności, monitorowania organów oceny zgodności, a także odpowiedniości wiedzy fachowej personelu organów wydających certyfikaty dla poziomu zapewnienia „wysokiego”. ENISA powinna uczestniczyć w wzajemnych ocenach w charakterze obserwatora i wspierać organizację mechanizmu wzajemnych ocen i samych wzajemnych ocen, w tym poprzez opracowywanie odpowiednich wytycznych i wzorów we współpracy z Komisją i ECCG. ENISA powinna również udostępniać publicznie na swojej stronie internetowej poświęconej europejskim systemom certyfikacji w zakresie cyberbezpieczeństwa informacje na temat harmonogramu wzajemnych ocen oraz wykaz krajowych organów certyfikacji w zakresie cyberbezpieczeństwa poddanych wzajemnej ocenie, które mają realizować ten harmonogram. Rozporządzenie wykonawcze Komisji (UE) 2025/2540[60] , przyjęte na mocy rozporządzenia (UE) 2019/881, ustanawia plan wzajemnych ocen, który jest wykorzystywany przez przyjęte europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa. Konieczne jest zapewnienie kontynuacji wzajemnych ocen. Niemniej jednak Komisja powinna mieć możliwość, w razie potrzeby, ustanowienia w drodze aktów wykonawczych nowego planu wzajemnych ocen na okres co najmniej pięciu lat, a także określenia kryteriów i metodologii funkcjonowania systemu wzajemnych ocen.

(120) Po przyjęciu europejskiego systemu certyfikacji cyberbezpieczeństwa producenci lub dostawcy produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmioty, których cyberbezpieczeństwo jest przedmiotem certyfikacji, powinni mieć możliwość składania wniosków o certyfikację swoich produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa do wybranej przez siebie jednostki oceniającej zgodność w dowolnym miejscu w Unii. Jednostki oceniające zgodność powinny być akredytowane

[60] Rozporządzenie wykonawcze Komisji (UE) 2025/2540 z dnia 9 grudnia 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do ustanowienia planu wzajemnej oceny (Dz.U. L 2540 z 12.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2540/oj).

przez krajową jednostkę akredytującą, jeżeli spełniają one wymogi określone w niniejszym rozporządzeniu oraz, w stosownych przypadkach, wymogi określone przez Komisję zgodnie z niniejszym rozporządzeniem. System określony w niniejszym rozporządzeniu powinien być uzupełniony systemem akredytacji przewidzianym w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 765/2008[61] .

(121) Jednostki oceniające zgodność, które zostały akredytowane lub notyfikowane na mocy obowiązujących przepisów unijnych, w szczególności rozporządzenia (UE) 2024/2847 lub rozporządzenia wykonawczego (UE) 2024/482, mogą posiadać kompetencje istotne dla nowo przyjętych europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa. Aby uniknąć niepotrzebnych obciążeń finansowych i administracyjnych, należy stworzyć synergię w zakresie akredytacji jednostek oceniających zgodność na mocy niniejszego rozporządzenia. Z tego powodu wymagania dotyczące akredytacji systemów powinny być ustanowione w taki sposób, aby były one w jak największym stopniu zgodne z wymaganiami dotyczącymi jednostek notyfikowanych określonymi w rozporządzeniu (UE) 2024/2847 oraz wymaganiami dotyczącymi akredytacji określonymi w rozporządzeniu wykonawczym (UE) 2024/482. Ponadto jednostki oceniające zgodność, które przechodzą proces akredytacji na mocy niniejszego rozporządzenia, powinny mieć możliwość oparcia się na wcześniejszych wynikach oceny ich kompetencji na mocy innych przepisów unijnych, w przypadku gdy wymogi akredytacyjne się pokrywają.

(122) W celu ułatwienia świadczenia zharmonizowanych usług oceny zgodności w całej Unii należy umożliwić określenie w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa dodatkowych lub szczególnych wymagań dla jednostek oceniających zgodność. W kontekście certyfikacji upoważnienie należy rozumieć jako decyzję krajowego organu certyfikacji w zakresie cyberbezpieczeństwa stwierdzającą, że jednostka oceniająca zgodność spełnia szczególne lub dodatkowe wymagania określone w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa, aby przeprowadzać określoną działalność w zakresie oceny zgodności.

(123) W przypadku gdy europejski system certyfikacji w zakresie cyberbezpieczeństwa określa dodatkowe lub szczególne wymagania zgodnie z niniejszym rozporządzeniem, organy oceny zgodności powinny być upoważnione przez krajowe organy certyfikacji w zakresie cyberbezpieczeństwa do wykonywania zadań w ramach takiego systemu. Aby uniknąć wielokrotnego udzielania upoważnień, zwiększyć akceptację i uznanie decyzji w sprawie upoważnień oraz zapewnić skuteczne monitorowanie upoważnionych organów oceny zgodności, organy oceny zgodności powinny wystąpić o upoważnienie do krajowego organu certyfikacji w zakresie cyberbezpieczeństwa państwa członkowskiego, w którym mają siedzibę. Niemniej jednak konieczne jest zapewnienie, aby jednostka oceniająca zgodność mogła wystąpić o upoważnienie w innym państwie członkowskim w przypadku, gdy w jej własnym państwie członkowskim nie ma krajowego organu certyfikacji w zakresie cyberbezpieczeństwa lub gdy krajowy organ certyfikacji w zakresie cyberbezpieczeństwa nie ma kompetencji do świadczenia usług w zakresie udzielania upoważnień, o które wnioskowano. W takich przypadkach należy zapewnić odpowiednią współpracę i wymianę informacji między krajowymi organami certyfikacji w zakresie cyberbezpieczeństwa. Komisja powinna być uprawniona do przyjmowania aktów wykonawczych ustanawiających

[61] Rozporządzenie (WE) nr 765/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku w odniesieniu do wprowadzania produktów do obrotu oraz uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

procedury udzielania zezwoleń, w tym dotyczące współpracy transgranicznej w zakresie udzielania zezwoleń.

(124) Aby zapewnić poziom ochrony wymagany dla produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub cyberbezpieczeństwa podmiotu, konieczne jest, aby podwykonawcy i podmioty zależne zajmujące się oceną zgodności byli zobowiązani do spełnienia tych samych wymagań, co notyfikowane jednostki oceniające zgodność w odniesieniu do wykonywania zadań związanych z oceną zgodności. W związku z tym jednostka oceniająca zgodność powinna posiadać odpowiednie kompetencje i być w stanie zweryfikować, czy jej podwykonawcy spełniają obowiązujące wymagania.

(125) Organ notyfikujący powinien odpowiednio ocenić, w jakim stopniu jednostka oceniająca zgodność zamierza polegać na podwykonawcach mających siedzibę poza Unią lub mieć dostęp do personelu lub obiektów poza państwem członkowskim notyfikacji. Organ publiczny państwa członkowskiego powinien mieć możliwość podjęcia decyzji, że nie może przyjąć całkowitej odpowiedzialności jako krajowy organ certyfikacji w zakresie cyberbezpieczeństwa za takie rozwiązanie, oraz cofnięcia lub ograniczenia zakresu notyfikacji.

(126) W celu oceny wymogów w zakresie cyberbezpieczeństwa dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberpostury podmiotów, akredytowane jednostki oceniające zgodność powinny być zgłaszane Komisji i pozostałym państwom członkowskim przez krajowe organy certyfikacji cyberbezpieczeństwa. Powiadomienie o akredytowanych i, w stosownych przypadkach, upoważnionych jednostkach oceniających zgodność wskazuje, że jednostki te są godne zaufania w zakresie wykonywania działań związanych z oceną i certyfikacją zgodnie z niniejszym rozporządzeniem i europejskim systemem certyfikacji cyberbezpieczeństwa, przyczyniając się do ogólnej reputacji europejskiej certyfikacji cyberbezpieczeństwa. Dlatego też niezbędne jest zapewnienie, aby jednostki oceniające zgodność, które zostały zgłoszone, spełniały swoje wymagania i wywiązywały się ze swoich obowiązków w czasie, a także aby wykaz zgłoszonych jednostek oceniających zgodność był aktualizowany.

(127) Rozporządzenie wykonawcze Komisji (UE) 2024/3143[62] przyjęte na mocy rozporządzenia (UE) 2019/881 określa okoliczności, formaty i procedury powiadamiania o jednostkach oceniających zgodność, które są wykorzystywane w przyjętych europejskich systemach certyfikacji w zakresie cyberbezpieczeństwa. Konieczne jest zatem zapewnienie kontynuacji działań w zakresie powiadamiania. Niemniej jednak Komisja powinna być uprawniona do przyjmowania aktów wykonawczych w celu dostosowania tych okoliczności, procedur i formatów powiadamiania organów oceny zgodności. W tym kontekście Komisja powinna wykorzystać doświadczenia zdobyte w ramach istniejących systemów i dążyć do dostosowania do innych odpowiednich przepisów i ram prawnych Unii, w szczególności do rozporządzenia (UE) 2024/2847 i nowych ram prawnych, mając na celu zmniejszenie obciążenia związanego z zapewnieniem zgodności dla organów oceny zgodności działających na podstawie różnych instrumentów prawnych.

---

[62] Rozporządzenie wykonawcze Komisji (UE) 2024/3143 z dnia 18 grudnia 2024 r. ustanawiające okoliczności, formaty i procedury powiadamiania zgodnie z art. 61 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa technologii informacyjno-komunikacyjnych (Dz.U. L 3143 z 19.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

(128) Łańcuchy dostaw technologii informacyjno-komunikacyjnych (ICT) składają się z powiązanego zestawu zasobów i procesów między podmiotami gospodarczymi. Łańcuchy dostaw ICT odgrywają kluczową rolę w utrzymaniu stabilności społecznej i stymulowaniu działalności gospodarczej w całej Unii. Odgrywają one również kluczową rolę w umożliwianiu funkcjonowania infrastruktury cyfrowej w Unii oraz stanowią podstawę funkcjonowania społeczeństwa i gospodarki Unii. Łańcuchy dostaw ICT umożliwiają wytwarzanie, produkcję, dystrybucję i utrzymanie usług ICT, systemów ICT i produktów ICT, które stanowią podstawę różnych sektorów o znaczeniu krytycznym i wysoce krytycznym, w tym opieki zdrowotnej, finansów, transportu, telekomunikacji, energii i ceł. Bezpieczeństwo łańcuchów dostaw ICT w tych krytycznych sektorach może również mieć wpływ na bezpieczeństwo infrastruktury obronnej i wojskowej, jeżeli infrastruktura ta opiera się na cywilnych sektorach krytycznych i ich łańcuchach dostaw ICT. Jednak zgodnie z raportem na temat stanu zagrożeń dla cyberbezpieczeństwa opublikowanym przez ENISA (ENISA Threat Landscape 2025)[63] ataki na łańcuchy dostaw należą do pięciu głównych zagrożeń dla cyberbezpieczeństwa , co pokazuje, że osoby atakujące aktywnie wykorzystują pośrednie ścieżki poprzez zewnętrznych dostawców i zależności. Zakłócenie łańcuchów dostaw ICT może utrudniać prowadzenie działalności gospodarczej na rynku wewnętrznym, powodować straty finansowe, podważać zaufanie użytkowników i wyrządzać poważne szkody gospodarce i społeczeństwu Unii. Gotowość i skuteczność w zakresie cyberbezpieczeństwa są zatem bardziej niż kiedykolwiek niezbędne dla prawidłowego funkcjonowania rynku wewnętrznego.

(129) Oprócz ryzyka technicznego, którym zajmuje się dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/55[64] , rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847[65] oraz europejskie ramy certyfikacji cyberbezpieczeństwa ustanowione rozporządzeniem (UE) 2019/881, łańcuchy dostaw ICT są w coraz większym stopniu narażone na ryzyko o charakterze nietechnicznym. Takie ryzyko nietechniczne może być związane, ale nie ogranicza się do jurysdykcji, której podlega dostawca niektórych komponentów, w szczególności w przypadku gdy państwo trzecie lub podmioty stanowiące zagrożenie kontrolowane z tego państwa angażują się w szpiegostwo gospodarcze, prowadzą złośliwe działania cybernetyczne lub kampanie przeciwko Unii lub jej państwom członkowskim lub angażują się w nieodpowiedzialne działania państwowe w cyberprzestrzeni. Ryzyko nietechniczne może być również związane z ukrytymi słabościami lub tylnymi furtkami lub potencjalnymi systemowymi zakłóceniami dostaw, w szczególności w przypadku uzależnienia technologicznego lub uzależnienia od dostawcy. Na przykład przełączniki awaryjne mogłyby zostać wykorzystane do wywarcia negatywnego wpływu na dostępność sieci komunikacyjnych i sieci elektroenergetycznych.

---

63 ENISA Threat Landscape 2025, październik 2025 r.

64 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. 80–152, ELI: https://eur-lex.europa.eu/eli/dir/2022/2555/oj).

65 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymogów dotyczących cyberbezpieczeństwa produktów zawierających elementy cyfrowe oraz zmieniające rozporządzenia (UE) nr 168/2013 i (UE) 2019/1020 oraz dyrektywę (UE) 2020/1828 (ustawa o cyberodporności) (Dz.U. L, 2024/2847, 20.11.2024, ELI: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng).

(130) We wspólnym komunikacie w sprawie wzmocnienia bezpieczeństwa gospodarczego UE[66] podkreślono ryzyko uzyskania przez państwa trzecie dostępu do wrażliwych informacji i danych w Unii lub jej państwach członkowskich w wyniku szpiegostwa przemysłowego, dostarczania przez nie sprzętu lub oprogramowania wykorzystywanego w niektórych produktach lub w wyniku posiadania i kontroli przez nie niektórych przedsiębiorstw dysponujących wrażliwymi informacjami i danymi. Podkreślono w nim również ryzyko zakłócenia funkcjonowania infrastruktury krytycznej Unii – w tym infrastruktury transportowej, systemów kosmicznych, energetycznej i komunikacyjnej, w szczególności tych, które uznano za strategiczne dla mobilności wojskowej – przez podmioty zagraniczne, co mogłoby wywołać efekt domina w gospodarce Unii. Zakłócenia mogą wynikać z ataków fizycznych, cyberataków lub ataków hybrydowych, w tym sabotażu całych obiektów lub ich części lub podzespołów. Mogą one również być związane z łańcuchami dostaw ICT, które stanowią podstawę krytycznych komponentów lub usług dla infrastruktury krytycznej.

(131) W odpowiedzi na wyzwania związane z bezpieczeństwem łańcucha dostaw ICT wynikające z ryzyka nietechnicznego niektóre państwa członkowskie podjęły środki regulacyjne, w tym wyznaczyły dostawców wysokiego ryzyka, a inne państwa członkowskie prawdopodobnie również to uczynią. Może to prowadzić do dalszych rozbieżności w podejściach krajowych, a ostatecznie do większej podatności niektórych państw członkowskich na zagrożenia, co może mieć skutki uboczne w całej Unii. Konieczne jest zatem zharmonizowanie niektórych aspektów związanych z nietechnicznymi zagrożeniami dla cyberbezpieczeństwa łańcucha dostaw ICT. Taka interwencja na szczeblu unijnym jest również uzasadniona ze względu na potrzebę zapewnienia wysokiego poziomu cyberbezpieczeństwa w całej Unii. Przepisy dotyczące bezpieczeństwa łańcucha dostaw ICT ( ) mają na celu wyeliminowanie tak dużych rozbieżności między państwami członkowskimi, w szczególności poprzez ustanowienie zasad dotyczących mechanizmów oceny ryzyka związanego z bezpieczeństwem łańcucha dostaw ICT na szczeblu unijnym oraz minimalnych standardów ochrony przed ryzykiem związanym z łańcuchem dostaw ICT.

(132) Aby zmniejszyć krytyczne zależności i podatność na zagrożenia, konieczne jest ustanowienie ram zaufanego łańcucha dostaw ICT, które powinny uwzględniać ryzyko nietechniczne związane z dostawcami wysokiego ryzyka i zależnościami w sektorach o wysokim znaczeniu krytycznym i innych sektorach krytycznych. W związku z tym konieczne jest zapewnienie na poziomie Unii obiektywnych, opartych na ryzyku, przyszłościowych i neutralnych technologicznie ram w celu identyfikacji kluczowych aktywów ICT i zapewnienia zestawu proporcjonalnych środków łagodzących w celu przeciwdziałania ryzyku.

(133) Ryzyko związane z cyberbezpieczeństwem, w tym ryzyko związane z zależnością od dostawców wysokiego ryzyka, można zaobserwować w kilku krytycznych łańcuchach dostaw ICT w Unii, w tym w zakresie urządzeń wykrywających, pojazdów połączonych i zautomatyzowanych, systemów dostaw energii elektrycznej i magazynowania energii elektrycznej, systemów zaopatrzenia w wodę, dronów i systemów przeciwdziałania dronom, usług przetwarzania w chmurze, urządzeń medycznych, sprzętu do nadzoru, usług kosmicznych i półprzewodników. Na przykład luki w zabezpieczeniach sprzętu do wykrywania zagrożeń bezpieczeństwa mogłyby umożliwić dostęp do systemów ICT, pozwalając złośliwym podmiotom na manipulowanie skanerami w taki sposób, aby

[66] Wspólny komunikat do Parlamentu Europejskiego i Rady, Wzmocnienie bezpieczeństwa gospodarczego UE, 3 grudnia 2025 r., JOIN(2025) 977 final.

zabronione przedmioty mogły zostać przewiezione przez punkt kontroli bezpieczeństwa bez wykrycia, co mogłoby mieć katastrofalne skutki.

(134) Niniejsze rozporządzenie nie powinno uniemożliwiać państwom członkowskim przyjmowania lub utrzymywania przepisów zapewniających wyższy poziom cyberbezpieczeństwa w odniesieniu do bezpieczeństwa łańcucha dostaw ICT, pod warunkiem że przepisy te są zgodne z obowiązkami państw członkowskich określonymi w prawie Unii. Przepisy takie mogą na przykład obejmować nakładanie bardziej rygorystycznych środków ograniczających ryzyko w odniesieniu do kluczowych aktywów ICT.

(135) W celu zidentyfikowania potencjalnych zagrożeń dla cyberbezpieczeństwa mających wpływ na określone łańcuchy dostaw ICT, grupa ds. współpracy ustanowiona na mocy art. 14 dyrektywy (UE) 2022/2555 („grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji") może oceniać określone łańcuchy dostaw ICT za pomocą skoordynowanych na poziomie Unii ocen ryzyka dla bezpieczeństwa. Skoordynowane na poziomie Unii oceny ryzyka bezpieczeństwa powinny uwzględniać między innymi głównych sprawców zagrożeń, główne zagrożenia i słabe punkty mające wpływ na kluczowe aktywa ICT. W ramach skoordynowanych na poziomie Unii ocen ryzyka bezpieczeństwa należy opracować wykaz scenariuszy ryzyka oraz wykaz środków służących ograniczeniu ryzyka. Skoordynowane na poziomie Unii oceny ryzyka bezpieczeństwa powinny zostać zakończone w ciągu sześciu miesięcy. W szczególnie pilnych przypadkach powinno być możliwe skrócenie terminów.

(136) W przypadkach, gdy Komisja ma wystarczające powody, aby sądzić, że istnieje poważne zagrożenie cybernetyczne dla bezpieczeństwa Unii związane z krytycznymi łańcuchami dostaw ICT i konieczne może być podjęcie działań w celu zachowania prawidłowego funkcjonowania rynku wewnętrznego, powinna ona bezzwłocznie skonsultować się z państwami członkowskimi w sprawie konieczności podjęcia środków ograniczających ryzyko i przeprowadzić ocenę ryzyka dla bezpieczeństwa, uwzględniając konsultacje z państwami członkowskimi.

(137) Jeżeli w wyniku oceny ryzyka dla bezpieczeństwa przeprowadzonej przez grupę ds. współpracy w zakresie bezpieczeństwa sieci i informacji lub Komisję okaże się, że określone państwo trzecie stwarza poważne i strukturalne nietechniczne zagrożenie dla cyberbezpieczeństwa łańcuchów dostaw ICT, Komisja powinna zweryfikować zagrożenie stwarzane przez to państwo. Komisja może wszcząć taką weryfikację również na podstawie innych źródeł, takich jak publiczne oświadczenie w imieniu Unii lub państw członkowskich w odpowiedzi na przypadki nieodpowiedzialnego zachowania państwa w cyberprzestrzeni, które doprowadziło do incydentu związanego z cyberbezpieczeństwem. W celu oceny poziomu zagrożenia Komisja powinna wziąć pod uwagę takie elementy, jak istnienie w państwie trzecim przepisów lub praktyk, które wymagają od podmiotów podlegających ich jurysdykcji zgłaszania organom tego państwa trzeciego informacji o lukach w oprogramowaniu lub sprzęcie komputerowym, zanim zostanie stwierdzone, że luki te zostały wykorzystane ( ). Innym istotnym elementem jest brak skutecznych środków prawnych oraz niezależnych i demokratycznych mechanizmów kontroli, które mogłyby rozwiązać problemy związane z bezpieczeństwem, w tym dotyczące istniejących praktyk, potwierdzonych informacji o incydentach związanych z podmiotami stanowiącymi zagrożenie, działającymi poza terytorium tego kraju i prowadzącymi złośliwe działania lub kampanie cybernetyczne, a także brak zdolności lub chęci państwa trzeciego do współpracy z Komisją lub państwami członkowskimi w celu przeciwdziałania ryzyku wynikającemu z działalności takich podmiotów stanowiących zagrożenie. Komisja

powinna również uwzględniać informacje pochodzące ze skoordynowanych ocen ryzyka bezpieczeństwa na szczeblu unijnym lub sprawozdań wydanych przez państwa członkowskie lub organizacje międzynarodowe, takie jak NATO.

(138) Do celów niniejszego rozporządzenia pojęcie kontroli należy rozumieć jako zdolność do wywierania decydującego wpływu na podmiot prawny bezpośrednio lub pośrednio poprzez jeden lub więcej pośrednich podmiotów prawnych. Kontrolę nad podmiotami z państwa trzeciego budzącymi obawy w zakresie cyberbezpieczeństwa należy również ustanowić w sytuacjach, gdy taki podmiot posiada struktury kierownicze w tym państwie.

(139) Unia nie powinna finansować projektów z udziałem dostawców wysokiego ryzyka, które mogłyby zagrozić bezpieczeństwu Unii oraz podważyć jej interesy i wiarygodność. Dostawcy wysokiego ryzyka zidentyfikowani na mocy niniejszego rozporządzenia nie powinni zatem mieć prawa do udziału w żadnych programach i instrumentach finansowania Unii realizowanych w ramach zarządzania bezpośredniego i pośredniego zgodnie z art. 136 rozporządzenia (UE/Euroatom) 2024/2509 i unijnych przepisów sektorowych, a także w żadnych działaniach finansowych Unii realizowanych w ramach zarządzania dzielonego, w tym w ramach kolejnych wieloletnich ram finansowych w odniesieniu do dostarczania komponentów ICT lub komponentów zawierających komponenty ICT, które mają być wykorzystywane w zidentyfikowanych kluczowych zasobach ICT. Unijni partnerzy wdrażający, tacy jak Grupa Europejskiego Banku Inwestycyjnego oraz krajowe banki i instytucje promocyjne, powinni powstrzymać się od wspierania projektów sprzecznych z powyższymi zasadami, w tym w ramach operacji na własne ryzyko.

(140) Zamówienia publiczne mogą być dla organów publicznych skutecznym narzędziem przyczyniającym się do tworzenia bardziej innowacyjnej, zrównoważonej i konkurencyjnej gospodarki oraz do strategicznego wydatkowania środków publicznych. Zamówienia publiczne związane z łańcuchami dostaw ICT nie powinny być wykorzystywane do przynoszenia korzyści dostawcom, którzy zagrażają bezpieczeństwu infrastruktury krytycznej Unii. Dostawcy wysokiego ryzyka zidentyfikowani na mocy niniejszego rozporządzenia nie powinni zatem mieć prawa do udziału w zamówieniach publicznych dotyczących dostawy komponentów ICT lub komponentów zawierających komponenty ICT, które mają być wykorzystywane w zidentyfikowanych kluczowych zasobach ICT.

(141) Certyfikacja w zakresie cyberbezpieczeństwa odgrywa rolę w wzmacnianiu ogólnego bezpieczeństwa i przeciwdziałaniu cyberzagrożeniom, służąc jako punkt odniesienia dla zaufania. Zaufanie to mogłoby ulec osłabieniu, gdyby poświadczenia umiejętności w zakresie cyberbezpieczeństwa były wydawane przez dostawców wysokiego ryzyka, którzy w związku z tym nie powinni mieć prawa ubiegać się o status autoryzowanych dostawców indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa w Unii. W podobnym duchu właściwe jest również wykluczenie dostawców wysokiego ryzyka z uzyskiwania certyfikacji w zakresie cyberbezpieczeństwa w ramach ECCF oraz uzyskiwania akredytacji jako jednostki oceniające zgodność w celu wydawania takich certyfikatów.

(142) Normy w zakresie cyberbezpieczeństwa odgrywają kluczową rolę w zapewnieniu bezpieczeństwa i wiarygodności infrastruktur cyfrowych. Konieczne jest podjęcie odpowiednich środków w celu zapewnienia standaryzacji w dziedzinie cyberbezpieczeństwa. Udział podmiotów mających siedzibę w krajach uznanych za stwarzające zagrożenie dla cyberbezpieczeństwa łańcucha dostaw ICT zgodnie z

niniejszym rozporządzeniem lub kontrolowanych z tych krajów może wpływać na normy w zakresie cyberbezpieczeństwa w sposób podważający ich bezpieczeństwo i wiarygodność.

(143) Na podstawie wyników ocen ryzyka bezpieczeństwa Komisja może określić, w drodze aktów wykonawczych, które zasoby ICT należy uznać za kluczowe ze względu na ich krytyczne znaczenie i poddać szczególnym środkom ograniczającym ryzyko. Samo istnienie możliwości połączenia danego zasobu powinno wystarczyć do uwzględnienia ryzyka związanego z jego cyberbezpieczeństwem.

(144) W razie konieczności zapewnienia wysokiego poziomu cyberbezpieczeństwa, cyberodporności i zaufania w Unii środki ograniczające ryzyko mogą być stosowane w odniesieniu do podmiotów w związku z ich łańcuchem dostaw ICT, a w szczególności w odniesieniu do zidentyfikowanych kluczowych zasobów ICT. Proponowane środki ograniczające ryzyko powinny opierać się na ocenie potencjalnych zagrożeń i zależności, w tym potencjalnego wpływu gospodarczego i społecznego takich środków na zainteresowane podmioty działające w sektorach o znaczeniu krytycznym lub innych sektorach krytycznych, a w szczególności na MŚP. Wpływ gospodarczy powinien uwzględniać koszty wdrożenia środków ograniczających, w tym czas trwania cyklu życia odpowiednich komponentów kluczowych aktywów ICT w przypadku, gdy środki obejmują wymianę dostawców. Należy również ocenić dostępność alternatywnych dostawców na rynku w celu zapewnienia ciągłości świadczenia usług.

(145) Ponieważ środki łagodzące mogą potencjalnie mieć ograniczający wpływ na międzynarodowy handel towarami i usługami, powinny one być proporcjonalne i ukierunkowane na osiągnięcie uzasadnionego celu, jakim jest zapewnienie cyberbezpieczeństwa łańcuchów dostaw ICT w odniesieniu do podmiotów typu, o którym mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, zgodnie z międzynarodowymi zobowiązaniami Unii.

(146) Wykorzystanie, instalacja lub jakikolwiek inny rodzaj integracji komponentów dostarczonych przez dostawców wysokiego ryzyka w ramach eksploatacji kluczowych aktywów ICT może wiązać się z ryzykiem późniejszego przekazania danych do państwa trzeciego. W szczególności ryzyko może wynikać z niewystarczającego poziomu ochrony danych w państwie trzecim, np. w zakresie ochrony praw podstawowych, własności intelektualnej lub tajemnic handlowych, lub z bezprawnego dostępu do tych danych i ich wykorzystania w celu ewentualnego zakłócenia łańcucha dostaw w przyszłości lub w celach szpiegowskich. Aby ograniczyć takie ryzyko, można zastosować ograniczenia dotyczące przekazywania określonych rodzajów danych do państw trzecich.

(147) Istotne słabe punkty wynikają z braku różnorodności sprzętu wykorzystywanego przez podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555. Poleganie na jednym dostawcy powoduje uzależnienie od konkretnego sprzętu lub rozwiązań. Brak różnorodności dostawców zwiększa ogólną podatność infrastruktury krytycznej na zagrożenia, w szczególności jeżeli podmioty zaopatrują się w komponenty ICT wykorzystywane w wrażliwych zasobach ICT od dostawcy stwarzającego wysokie ryzyko. Uzależnienie ma również znaczący wpływ na odporność krajową i unijną oraz stwarza pojedyncze punkty awarii. Aby ograniczyć takie ryzyko, można zastosować wymóg posiadania więcej niż jednego dostawcy określonych kluczowych zasobów ICT.

(148) Podmioty unijne mogą również korzystać z kluczowych aktywów określonych w niniejszym rozporządzeniu. W związku z tym przepisy niniejszego rozporządzenia

dotyczące bezpieczeństwa łańcucha dostaw ICT powinny mieć również zastosowanie do tych podmiotów. Aby zapewnić uwzględnienie specyfiki podmiotów unijnych, podczas przeprowadzania skoordynowanych ocen ryzyka bezpieczeństwa na szczeblu unijnym należy wziąć pod uwagę ryzyko nietechniczne wynikające z łańcuchów dostaw ICT w odniesieniu do podmiotów unijnych.

(149) W wyjątkowych okolicznościach uzasadniających natychmiastową interwencję w celu zachowania prawidłowego funkcjonowania rynku wewnętrznego i w przypadku istnienia wyraźnych dowodów dających Komisji wystarczające podstawy do uznania, że stosowanie komponentów ICT lub komponentów zawierających komponenty ICT od określonego dostawcy stanowi poważne zagrożenie dla cyberbezpieczeństwa działalności gospodarczej lub społecznej co najmniej trzech państw członkowskich , Komisja może zaproponować, w ścisłej konsultacji z państwami członkowskimi, zakaz stosowania, instalowania lub integrowania takich komponentów od tego dostawcy przez rodzaje podmiotów, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555.

(150) W celu zapewnienia proporcjonalności stosowanych środków podmioty mające siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa, wyznaczone zgodnie z niniejszym rozporządzeniem, lub kontrolowane przez takie państwo trzecie, przez podmiot mający siedzibę w takim państwie trzecim lub przez obywatela takiego państwa trzeciego mogą ubiegać się o zwolnienie z zakazu dostarczania podmiotom, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555 na potrzeby ich użytkowania, instalacji lub integracji z kluczowymi zasobami ICT tego podmiotu oraz uczestniczyć w procedurach udzielania zamówień publicznych organizowanych zgodnie z przepisami transponującymi dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE[67] oraz 2014/25/UE[68] w odniesieniu do dostarczania komponentów ICT lub komponentów zawierających komponenty ICT, które mają być wykorzystywane w określonych kluczowych zasobach ICT. W tym celu podmiot powinien wykazać w sposób jednoznaczny, że stosuje skuteczne środki ograniczające ryzyko nietechniczne i zapewniające brak jakichkolwiek niepożądanych ingerencji ze strony państw trzecich budzących obawy w zakresie cyberbezpieczeństwa.

(151) Sieci łączności elektronicznej stanowią podstawę szerokiego zakresu usług, które są niezbędne do funkcjonowania rynku wewnętrznego oraz utrzymania i działania kluczowych funkcji społecznych i gospodarczych, takich jak energia, transport, bankowość, zdrowie, obrona, a także przemysłowe systemy sterowania. Dlatego te wysoce krytyczne sieci są atrakcyjnym celem dla wszelkiego rodzaju cyberataków i zagrożeń hybrydowych, zakłóceń, szpiegostwa, gromadzenia informacji wywiadowczych, a także oszustw i przestępstw finansowych. W ocenie ryzyka przeprowadzonej przez grupę ds. współpracy w zakresie bezpieczeństwa sieci i informacji dotyczącej cyberbezpieczeństwa i odporności europejskiej infrastruktury i sieci komunikacyjnych zidentyfikowano szereg zagrożeń i ryzyk o znaczeniu strategicznym z punktu widzenia Unii, takich jak oprogramowanie typu

[67] Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych i uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65–242, ELI: https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng).

[68] Dyrektywa Parlamentu Europejskiego i Rady 2014/25/UE z dnia 26 lutego 2014 r. w sprawie zamówień udzielanych przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych oraz uchylająca dyrektywę 2004/17/WE (Dz.U. L 94 z 28.3.2014, s. 243–374, ELI: https://eur-lex.europa.eu/eli/dir/2014/25/oj?locale=fr).

wiper/ransomware, ataki, ataki na łańcuch dostaw, włamania do sieci oraz ataki typu distributed denial-of-service (DDoS).

(152) Ze względu na wzajemne powiązania i współzależność między różnymi krajowymi sieciami łączności elektronicznej konieczne jest, aby wszystkie państwa członkowskie podjęły odpowiednie środki w celu zapewnienia bezpieczeństwa swoich sieci. Z tych samych powodów istnieje potrzeba ustanowienia skutecznych ram prawnych na szczeblu Unii, które uwzględniałyby również zagrożenia nietechniczne i zapewniały kompleksowe bezpieczeństwo połączonych sieci łączności elektronicznej.

(153) W szczególności cyberbezpieczeństwo sieci 5G ma strategiczne znaczenie dla Unii, ponieważ sieci te stanowią podstawę szerokiego zakresu usług o zasadniczym znaczeniu dla funkcjonowania rynku wewnętrznego, a także mają kluczowe znaczenie dla zapewnienia naszej gotowości obronnej, w tym w odniesieniu do mobilności wojskowej. Sieci 5G są w stanie zapewnić niezawodną, ultraszybką łączność, na przykład w celu wymiany danych i informacji, wykrywania dronów i koordynacji działań na polu walki w czasie rzeczywistym.

(154) Wdrażanie sieci 5G polega przede wszystkim na tworzeniu sieci nieautonomicznych, w których tylko sieć dostępu radiowego jest modernizowana do technologii 5G, podczas gdy pozostała część sieci nadal opiera się na istniejącej sieci rdzeniowej 4G. Sieci nieautonomiczne 5G opierają się przede wszystkim na już istniejącej infrastrukturze, co oznacza, że bezpieczeństwo przyszłych sieci 5G jest w pewnym stopniu uzależnione od już zainstalowanego sprzętu sieciowego i jego konfiguracji. W związku z tym środki łagodzące powinny również obejmować sieci 4G, na których opiera się wdrożenie 5G.

(155) Aby sprostać ważnym wyzwaniom w zakresie bezpieczeństwa sieci 5G, państwa członkowskie w ramach grupy współpracy NIS wraz z Komisją i ENISA przeprowadziły skoordynowaną na szczeblu unijnym ocenę ryzyka bezpieczeństwa sieci 5G, badając zarówno ryzyko techniczne, jak i nietechniczne. W ocenie tej zidentyfikowano kilka rodzajów ryzyka, w tym potencjalne zakłócenia ze strony państw trzecich lub podmiotów z państw trzecich za pośrednictwem łańcucha dostaw, oraz sklasyfikowano aktywa według ich krytycznego znaczenia. Ocena ta powinna stanowić podstawę do określenia kluczowych aktywów ICT dla sieci łączności 5G.

(156) Aby ograniczyć ryzyko zidentyfikowane w skoordynowanej na szczeblu unijnym ocenie ryzyka bezpieczeństwa sieci 5G, grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji przyjęła unijny zestaw narzędzi dotyczących cyberbezpieczeństwa 5G, określający środki strategiczne i techniczne. Mimo że większość państw członkowskich posiada ramy prawne umożliwiające ograniczenia lub wykluczenia dostawców wysokiego ryzyka, zgodnie z zaleceniami zawartymi w zestawie narzędzi 5G, wdrożenie tych ram nie było jednolite. W rezultacie znaczna liczba lokalizacji 5G w całej Unii jest obsługiwana przez dostawców wysokiego ryzyka, o których mowa w komunikacie Komisji w sprawie wdrożenia zestawu narzędzi 5G[69] . Sytuacja ta stwarza słabe punkty, w tym strategiczną zależność i potencjalną narażoność na ingerencję państw trzecich, co może również wpłynąć na przyszłą infrastrukturę 6G opartą na istniejących sieciach 5G. Fragmentaryczne wdrażanie środków zalecanych w zestawie narzędzi 5G, w szczególności w odniesieniu do zakresu ograniczeń dotyczących dostawców wysokiego ryzyka, doprowadziło do rozbieżności między państwami członkowskimi, co skutkuje nierównymi warunkami konkurencji, które dzielą rynek wewnętrzny i osłabiają ogólne bezpieczeństwo sieci. Europejski Trybunał

[69] Komunikat Komisji w sprawie wdrożenia zestawu narzędzi dotyczących cyberbezpieczeństwa 5G, 15 czerwca 2023 r., C(2023) 4049 wersja ostateczna.

Obrachunkowy zwrócił uwagę na te rozbieżności, ostrzegając, że brak skoordynowanego podejścia podważa funkcjonowanie rynku wewnętrznego. Utrzymująca się zależność od dostawców wysokiego ryzyka stanowi poważne zagrożenie dla bezpieczeństwa infrastruktury krytycznej w Unii i może podważyć zaufanie do rynku wewnętrznego, ponieważ niespójne poziomy bezpieczeństwa mogą zniechęcać konsumentów i przedsiębiorstwa do korzystania z produktów i usług opartych na 5G w całej Unii. Dlatego też niezbędne jest wprowadzenie środków na szczeblu unijnym w celu zapewnienia zharmonizowanego podejścia do bezpieczeństwa sieci 5G.

(157) W celu ustalenia okresu wycofywania kluczowych aktywów ICT w stacjonarnych i satelitarnych sieciach łączności elektronicznej Komisja powinna przeprowadzić ocenę, uwzględniając stopień ryzyka dla bezpieczeństwa związanego z każdym konkretnym kluczowym aktywem ICT w sieciach stacjonarnych i satelitarnych, okres eksploatacji odpowiednich komponentów oraz wpływ gospodarczy, jaki wycofanie tych komponentów miałoby na zainteresowanych operatorów. Na podstawie wyników tej oceny Komisja może rozważyć ustanowienie różnych okresów wycofywania poszczególnych kluczowych aktywów ICT i ich integralnych elementów.

(158) W celu zapewnienia skutecznego nadzoru i egzekwowania obowiązków dotyczących dostawców mobilnych, stacjonarnych i satelitarnych sieci łączności elektronicznej, właściwe organy zgodnie z niniejszym rozporządzeniem powinny zapewnić ścisłą współpracę z organami właściwymi zgodnie z [wnioskiem DNA]. Na wniosek właściwego organu wyznaczonego zgodnie z niniejszym rozporządzeniem krajowe organy regulacyjne lub inne właściwe organy ds. widma radiowego, w stosownych przypadkach, powinny cofnąć prawa, o których mowa w art. 9 i art. 20 [wniosek DNA], jeżeli dostawca publicznych sieci łączności elektronicznej nie wywiązuje się z obowiązków wynikających z niniejszego rozporządzenia, w tym jeżeli dostawca nie wycofuje komponentów ICT lub komponentów zawierających komponenty ICT od dostawców wysokiego ryzyka z eksploatacji kluczowych aktywów ICT w terminie określonym zgodnie z niniejszym rozporządzeniem.

(159) Ze względu na różnice w krajowych strukturach zarządzania państwa członkowskie powinny wyznaczyć lub ustanowić jeden lub więcej właściwych organów odpowiedzialnych za środki nadzoru i egzekwowania przepisów na mocy niniejszego rozporządzenia.

(160) Właściwe organy powinny zapewnić wsparcie podmiotom, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, w wypełnianiu ich obowiązków wynikających z niniejszego rozporządzenia. W tym celu Komisja powinna ocenić, czy dostawcy, których mogą dotyczyć określone zakazy, mają siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub są kontrolowani przez takie państwo trzecie, podmiot mający siedzibę w takim państwie trzecim lub obywatela takiego państwa trzeciego. Właściwe organy powinny ściśle współpracować z Komisją i innymi właściwymi organami w ramach sieci ustanowionej na mocy niniejszego rozporządzenia. Na podstawie oceny przeprowadzonej przez Komisję właściwe organy powinny udostępniać odpowiednim podmiotom, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, istotne informacje dotyczące dostawców wysokiego ryzyka. Nie oczekuje się, aby podmioty weryfikowały, czy dostawca znajduje się pod kontrolą zagraniczną, ale mogą one w pełni polegać na informacjach otrzymanych od właściwych organów. Właściwe organy powinny zapewnić, aby na podmioty te nie nakładano zbędnych obciążeń administracyjnych.

(161) Aby zapewnić skuteczne przestrzeganie przepisów, niniejsze rozporządzenie powinno przewidywać środki nadzoru i egzekwowania, dzięki którym właściwe organy mogą nadzorować podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555. Wykonywanie przez właściwe organy zadań w zakresie nadzoru i egzekwowania przepisów w odniesieniu do tych podmiotów nie powinno wykraczać poza to, co jest konieczne, i powinno być proporcjonalne do zidentyfikowanego ryzyka.

(162) Aby egzekwowanie przepisów było skuteczne i spójne w całej Unii, konieczne jest zapewnienie właściwym organom uprawnień wykonawczych, które mogą one wykonywać w przypadku naruszenia obowiązków określonych w niniejszym rozporządzeniu. Wykonując te uprawnienia wykonawcze, właściwe organy powinny należycie uwzględniać szereg czynników, w tym charakter, wagę i czas trwania naruszenia, spowodowane szkody materialne lub niematerialne, to, czy naruszenie było umyślne czy wynikające z niedbalstwa, działania podjęte w celu zapobieżenia lub złagodzenia szkód materialnych lub niematerialnych, stopień odpowiedzialności lub wszelkie istotne wcześniejsze naruszenia, stopień współpracy z właściwym organem oraz wszelkie inne okoliczności obciążające lub łagodzące. Środki egzekucyjne, w tym kary, powinny być proporcjonalne, a ich nakładanie powinno podlegać odpowiednim gwarancjom proceduralnym zgodnie z ogólnymi zasadami prawa Unii i Kartą praw podstawowych Unii Europejskiej, w tym prawem do skutecznego środka odwoławczego i rzetelnego procesu sądowego, domniemaniem niewinności i prawem do obrony.

(163) Ważne jest również zapewnienie uprawnienia do nakładania okresowych kar pieniężnych w celu zmuszenia podmiotu, o którym mowa w załącznikach I lub II do dyrektywy (UE) 2022/2555, do zaprzestania naruszania niniejszego rozporządzenia zgodnie z uprzednią decyzją właściwego organu.

(164) Aby zapewnić skuteczne egzekwowanie obowiązków określonych w niniejszym rozporządzeniu, każdy właściwy organ powinien mieć uprawnienia do nakładania kar lub wnioskowania o ich nałożenie.

(165) Do celów nakładania kar na podmiot, o którym mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, będący przedsiębiorstwem, przedsiębiorstwo należy rozumieć zgodnie z art. 101 i 102 TFUE. W przypadku nałożenia grzywny na osobę niebędącą przedsiębiorstwem właściwy organ powinien uwzględnić ogólny poziom dochodów w państwie członkowskim, a także sytuację ekonomiczną tej osoby przy ustalaniu odpowiedniej wysokości sankcji. Do państw członkowskich powinno należeć określenie, czy i w jakim zakresie organy publiczne powinny podlegać sankcjom. Nałożenie sankcji nie powinno mieć wpływu na wykonywanie innych uprawnień właściwych organów.

(166) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze w odniesieniu do przyjmowania aktów wykonawczych ustanawiających szczegółowe zasady dotyczące opłat pobieranych przez ENISA, aktów wykonawczych przewidujących europejski system certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów, aktów wykonawczych ustanawiających wspólne zasady i przepisy odniesienia mające na celu zapewnienie elementów we wszystkich europejskich systemach certyfikacji cyberbezpieczeństwa, aktów wykonawczych określających procedury uprzedniego zatwierdzania lub ogólne modele delegowania, aktów wykonawczych w sprawie uznawania certyfikatów cyberbezpieczeństwa państw trzecich lub organizacji

międzynarodowych za równoważne z europejskimi certyfikatami cyberbezpieczeństwa, aktów wykonawczych ustanawiających plan wzajemnej oceny, aktów wykonawczych w sprawie ustanowienia procedur, w tym dotyczących współpracy transgranicznej, w sprawie upoważnienia organów oceny zgodności, akty wykonawcze ustanawiające okoliczności, formaty i procedury powiadamiania organów oceny zgodności, akty wykonawcze wyznaczające państwo trzecie jako państwo stwarzające zagrożenie dla cyberbezpieczeństwa łańcuchów dostaw ICT, akty wykonawcze określające kluczowe aktywa ICT wykorzystywane do wytwarzania produktów lub świadczenia usług przez podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, akty wykonawcze ustanawiające, że podmioty działające w sektorach o wysokim znaczeniu krytycznym i innych sektorach krytycznych podlegają szczególnym środkom łagodzącym, oraz określające terminy wycofywania komponentów ICT lub komponentów zawierających komponenty ICT dostarczane przez dostawców wysokiego ryzyka, akty wykonawcze określające warunki dotyczące zwolnienia podmiotów mających siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowanych przez takie podmioty, a także przyjęcie aktów wykonawczych ustanawiających szczegółowe zasady dotyczące opłat pobieranych przez Komisję. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011, a procedura sprawdzająca powinna być stosowana. W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy również powierzyć Komisji uprawnienia wykonawcze w odniesieniu do ustanowienia wykazu dostawców wysokiego ryzyka istotnych dla niektórych środków przewidzianych w niniejszym rozporządzeniu.

(167) Konieczne jest, aby europejskie systemy certyfikacji cyberbezpieczeństwa odzwierciedlały najnowsze osiągnięcia technologiczne, nowe powiązane zagrożenia oraz przyjęcie nowych przepisów unijnych określających wykazanie zgodności i domniemanie zgodności poprzez europejską certyfikację cyberbezpieczeństwa z odpowiednimi wymogami cyberbezpieczeństwa tych przepisów. Z tych powodów należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w celu dodania lub zmiany celów bezpieczeństwa, do których dążą europejskie systemy certyfikacji cyberbezpieczeństwa. Podobnie, w interesie wiarygodnych ram łańcucha dostaw ICT, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w celu zmiany załącznika II do niniejszego rozporządzenia, aby dostosować go do rozwoju technologicznego. Szczególnie ważne jest, aby w trakcie prac przygotowawczych Komisja prowadziła odpowiednie konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te były prowadzone zgodnie z zasadami określonymi w porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa. W szczególności, aby zapewnić równy udział w przygotowywaniu aktów delegowanych, Parlament Europejski i Rada powinny otrzymywać wszystkie dokumenty w tym samym czasie co eksperci państw członkowskich, a ich eksperci powinni mieć systematyczny dostęp do posiedzeń grup ekspertów Komisji zajmujących się przygotowywaniem aktów delegowanych.

(168) Działalność ENISA powinna podlegać regularnej i niezależnej ocenie. Ocena ta powinna uwzględniać cele ENISA oraz znaczenie jej zadań, w szczególności zadań związanych ze współpracą operacyjną na szczeblu unijnym. W przypadku przeglądu Komisja powinna ocenić, w jaki sposób można wzmocnić rolę ENISA jako punktu odniesienia w zakresie doradztwa i wiedzy fachowej.

(169) Rozporządzenie wykonawcze Komisji (UE) 2024/482 ustanawia przepisy dotyczące przyjęcia europejskiego systemu certyfikacji cyberbezpieczeństwa opartego na

wspólnych kryteriach (EUCC). EUCC jest pierwszym i jedynym europejskim systemem certyfikacji cyberbezpieczeństwa przyjętym na mocy rozporządzenia (UE) 2019/881. Dotyczy on certyfikacji produktów ICT, w tym produktów należących do dziedzin technicznych „karty inteligentne i podobne urządzenia" oraz „urządzenia sprzętowe z modułami zabezpieczającymi", a także profili ochronnych (jako procesów ICT). Konieczne jest zatem zapewnienie kontynuacji działalności certyfikacyjnej, a także działalności Agencji.

(170) Zgodnie z art. 42 ust. 2 rozporządzenia (UE) 2018/1725[70] przeprowadzono konsultacje z Europejskim Inspektorem Ochrony Danych i Europejską Radą Ochrony Danych, które wydały wspólną opinię [data].

(171) Należy uchylić rozporządzenie (UE) 2019/881.

(172) Ponieważ cele niniejszego rozporządzenia nie mogą być osiągnięte w sposób wystarczający przez państwa członkowskie, a ze względu na jego skalę i skutki mogą być lepiej osiągnięte na poziomie Unii, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej (TUE). Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

TYTUŁ I
PRZEPISY OGÓLNE

Artykuł 1
Przedmiot i zakres stosowania

1. Niniejsze rozporządzenie określa:

   a) misję, cele, zadania i kwestie organizacyjne dotyczące Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA);

   b) ramy ustanawiające europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub stanu cyberbezpieczeństwa podmiotów w Unii, a także w celu uniknięcia fragmentacji rynku wewnętrznego w odniesieniu do systemów certyfikacji w zakresie cyberbezpieczeństwa w Unii; oraz

   c) ramy zaufanego łańcucha dostaw ICT.

2. Ramy, o których mowa w ust. 1 lit. b), mają zastosowanie bez uszczerbku dla szczególnych przepisów innych aktów prawnych Unii dotyczących certyfikacji dobrowolnej lub obowiązkowej.

3 Ramy, o których mowa w akapicie pierwszym lit. c), mają zastosowanie do podmiotów publicznych lub prywatnych, o których mowa w załączniku I lub II do dyrektywy (UE) 2022/2555, które świadczą swoje usługi lub prowadzą działalność na terytorium Unii.

---

[70] 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 i decyzję nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

4. Niniejsze rozporządzenie nie narusza podstawowych funkcji państwowych państw członkowskich, w tym zapewniania integralności terytorialnej państwa, utrzymania porządku publicznego i ochrony bezpieczeństwa narodowego. W szczególności bezpieczeństwo narodowe pozostaje wyłączną odpowiedzialnością każdego państwa członkowskiego.

Artykuł 2
Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

(1) „cyberbezpieczeństwo” oznacza działania niezbędne do ochrony systemów sieciowych i informatycznych, użytkowników takich systemów oraz innych osób narażonych na cyberzagrożenia;

(2) „podmioty unijne” oznaczają podmioty unijne określone w art. 3 pkt 1 rozporządzenia (UE, Euratom) 2023/2841;

3) „upoważniony dostawca poświadczeń” oznacza podmiot publiczny lub prywatny, w odniesieniu do którego ENISA przyjęła decyzję upoważniającą ten podmiot do wydawania europejskich indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa zgodnie z europejskim systemem indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa;

(4) „europejskie indywidualne poświadczenie umiejętności w zakresie cyberbezpieczeństwa” oznacza dokument w formie cyfrowej lub fizycznej potwierdzający, że dana osoba posiada wiedzę, rozumie i jest w stanie wykonywać zadania związane z profilem stanowiska lub podzbiorem profilu stanowiska określonego w europejskich ramach umiejętności w zakresie cyberbezpieczeństwa („ECSF”), po przejściu oceny określonej w europejskim systemie indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa;

(5) „europejski system certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa” oznacza kompleksowy zestaw zasad, wymogów, norm i procedur ustanowionych przez ENISA i związanych z profilem roli ECSF lub jego podzbiorem, które mają zastosowanie do uprawnionych podmiotów certyfikujących i są przez nie stosowane;

(6) „sieć i system informatyczny” oznacza sieć i system informatyczny w rozumieniu art. 6 pkt 1 dyrektywy (UE) 2022/2555;

(7) „krajowa strategia w zakresie cyberbezpieczeństwa” oznacza krajową strategię w zakresie cyberbezpieczeństwa określoną w art. 6 pkt 4 dyrektywy (UE) 2022/2555;

(8) „incydent” oznacza incydent w rozumieniu art. 6 pkt 6 dyrektywy (UE) 2022/2555;

(9) „incydent cyberbezpieczeństwa na dużą skalę” oznacza incydent cyberbezpieczeństwa na dużą skalę w rozumieniu art. 6 pkt 7 dyrektywy (UE) 2022/2555;

(10 „reagowanie na incydent” oznacza reagowanie na incydent w rozumieniu art. 6 pkt 8 dyrektywy (UE) 2022/2555;

(11) „zagrożenie cybernetyczne” oznacza każdą potencjalną okoliczność, zdarzenie lub działanie, które mogłoby spowodować uszkodzenie, zakłócenie lub inne niekorzystne skutki dla systemów sieciowych i informatycznych, użytkowników takich systemów oraz innych osób;

(12 „europejski system certyfikacji cyberbezpieczeństwa” oznacza kompleksowy zestaw zasad, wymagań technicznych, norm i procedur ustanowionych na poziomie Unii, które mają zastosowanie do certyfikacji lub oceny zgodności określonych produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberpostury podmiotów;

(13) „krajowy system certyfikacji w zakresie cyberbezpieczeństwa” oznacza kompleksowy zestaw zasad, wymagań technicznych, norm i procedur opracowanych i przyjętych przez krajowy organ publiczny, które mają zastosowanie do certyfikacji lub oceny zgodności produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberpostury podmiotów objętych zakresem danego systemu;

(14) „europejski certyfikat cyberbezpieczeństwa” oznacza dokument wydany przez właściwy organ, poświadczający, że dany produkt ICT, usługa ICT, proces ICT lub zarządzane usługi bezpieczeństwa lub cyberbezpieczeństwo podmiotu zostały ocenione pod kątem zgodności z określonymi wymogami bezpieczeństwa określonymi w europejskim systemie certyfikacji cyberbezpieczeństwa;

(15) „oświadczenie UE o zgodności” oznacza dokument wydany przez producenta lub dostawcę produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiot, którego cyberbezpieczeństwo podlega certyfikacji, stwierdzający, że spełnienie wymagań odpowiadających poziomowi zapewnienia „podstawowemu”, określonemu w europejskim systemie certyfikacji cyberbezpieczeństwa, zostało wykazane w drodze samooceny zgodności;

(16) „produkt ICT” oznacza element lub grupę elementów sieci lub systemu informatycznego;

(17) „usługa ICT” oznacza usługę polegającą całkowicie lub głównie na przekazywaniu, przechowywaniu, odzyskiwaniu lub przetwarzaniu informacji za pomocą sieci i systemów informatycznych;

(18) „proces ICT” oznacza zbiór czynności wykonywanych w celu zaprojektowania, opracowania, dostarczenia lub utrzymania produktu ICT lub usługi ICT;

(19) „usługa zarządzania bezpieczeństwem” oznacza usługę świadczoną na rzecz osoby trzeciej, polegającą na wykonywaniu lub wspieraniu działań związanych z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa, takich jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo, w tym doradztwo eksperckie związane ze wsparciem technicznym;

(20) „akredytacja” oznacza akredytację w rozumieniu art. 2 pkt 10 rozporządzenia (WE) nr 765/2008;

(21) „krajowa jednostka akredytująca” oznacza krajową jednostkę akredytującą w rozumieniu art. 2 pkt 11 rozporządzenia (WE) nr 765/2008;

(22) „ocena zgodności” oznacza ocenę zgodności określoną w art. 2 pkt 12 rozporządzenia (WE) nr 765/2008;

(23) „jednostka oceniająca zgodność” oznacza jednostkę oceniającą zgodność w rozumieniu art. 2 pkt 13 rozporządzenia (WE) nr 765/2008;

(24 „norma” oznacza normę w rozumieniu art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012[71] ;

(25 „specyfikacja techniczna” oznacza specyfikację techniczną w rozumieniu art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012;

(26 „norma zharmonizowana” oznacza normę zharmonizowaną w rozumieniu art. 2 pkt 1 lit. c) rozporządzenia (UE) nr 1025/2012;

(27) „poziom pewności” oznacza podstawę do uzyskania pewności, że produkt ICT, usługa ICT, proces ICT, zarządzana usługa bezpieczeństwa lub cyberbezpieczeństwo podmiotu spełniają wymogi bezpieczeństwa określone w konkretnym europejskim systemie certyfikacji cyberbezpieczeństwa, oraz wskazuje poziom, na którym produkt ICT, usługa ICT, proces ICT, zarządzana usługa bezpieczeństwa lub cyberbezpieczeństwo podmiotu zostały ocenione, ale jako taki nie mierzy bezpieczeństwa produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub cyberbezpieczeństwa danego podmiotu;

(28) „samocewocena zgodności” oznacza działanie przeprowadzane przez producenta lub dostawcę produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiot, którego cyberbezpieczeństwo podlega certyfikacji, w ramach którego ocenia się, czy te produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub cyberbezpieczeństwo podmiotów spełniają wymagania określonego europejskiego systemu certyfikacji cyberbezpieczeństwa;

(29) „stan cyberbezpieczeństwa podmiotów” oznacza poziom cyberbezpieczeństwa podmiotów w odniesieniu do określonych wymogów bezpieczeństwa;

(30) „model uprzedniego zatwierdzania” oznacza model, w ramach którego jednostka oceniająca zgodność może wydać europejski certyfikat cyberbezpieczeństwa na podstawie oceny przeprowadzonej przez krajowy organ certyfikacji cyberbezpieczeństwa w kontekście określonego procesu certyfikacji w ramach odpowiedniego systemu;

(31) „model ogólnego przekazania uprawnień” oznacza model, w ramach którego jednostka oceniająca zgodność może wydać europejski certyfikat cyberbezpieczeństwa na podstawie przekazania uprawnień w zakresie certyfikacji przez krajowy organ certyfikacji cyberbezpieczeństwa;

(32) „zespół reagowania na incydenty związane z bezpieczeństwem komputerowym” lub „CSIRT” oznacza CSIRT wyznaczony lub ustanowiony zgodnie z art. 10 dyrektywy (UE) 2022/2555.

(33) „komponenty ICT” oznaczają produkty ICT, usługi ICT lub procesy ICT, które mogą być wykorzystywane w eksploatacji zasobów ICT;

(34) „zasoby ICT” oznaczają zasoby oprogramowania lub sprzętu w sieciach i systemach informatycznych wykorzystywanych przez podmiot, o którym mowa w załącznikach I i II do dyrektywy (UE) 2022/2555;

---

[71] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE Parlamentu Europejskiego i Rady oraz uchylająca decyzję Rady 87/95/EWG i decyzję nr 1673/2006/WE Parlamentu Europejskiego i Rady (Dz.U. L 316 z 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(35) „kluczowe aktywa ICT” oznaczają aktywa ICT określone zgodnie z art. 102;

(36) „sieć łączności elektronicznej” oznacza sieć łączności elektronicznej w rozumieniu art. 2 pkt 1 rozporządzenia (UE) XX/XXXX [wniosek DNA];

(37) „kontrola” oznacza zdolność do wywierania decydującego wpływu na podmiot prawny bezpośrednio lub pośrednio poprzez jeden lub więcej pośrednich podmiotów prawnych;

(38) „zakład” oznacza faktyczne prowadzenie działalności w ramach stałych ustaleń w kraju, w którym podmiot ma swoją centralną administrację lub główne miejsce prowadzenia działalności;

(39) „dostawca wysokiego ryzyka” oznacza jedną z następujących sytuacji:

a) podmiot mający siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa, wyznaczonym zgodnie z art. 100, lub kontrolowany przez takie państwo trzecie, przez podmiot mający siedzibę w takim państwie trzecim lub przez obywatela takiego państwa trzeciego;

b) podmiot wyznaczony zgodnie z art. 103 ust. 7 oraz podmioty kontrolowane przez ten podmiot;

(40) „łańcuch dostaw ICT” oznacza sumę usług ICT, produktów ICT i procesów ICT, które obejmują działania i podmioty zaangażowane na wszystkich etapach poprzedzających udostępnienie produktu lub świadczenie usługi na rynku;

(41) „państwo trzecie” oznacza państwo trzecie w rozumieniu art. 3 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2675[72] ;

(42) „ryzyko nietechniczne” oznacza prawdopodobieństwo, że dostawca zostanie poddany wpływom państwa trzeciego, które mogą spowodować utratę lub zakłócenie świadczonej usługi lub zagrozić produktowi wytwarzanemu przez podmiot lub doprowadzić do wycieku danych, w tym do celów szpiegostwa lub generowania dochodów;

(43) „istotne ryzyko nietechniczne związane z cyberbezpieczeństwem” oznacza ryzyko nietechniczne związane z cyberbezpieczeństwem, które można uznać za wysoce prawdopodobne, że spowoduje incydent mogący mieć poważne negatywne skutki, w tym spowodować znaczne straty materialne lub niematerialne lub zakłócenia;

(44) „podstawowe funkcje sieciowe mobilnych sieci łączności elektronicznej” oznaczają centralny element architektury mobilnych sieci łączności elektronicznej, łączący główne węzły sieciowe z internetem i zarządzający podstawowymi funkcjami systemu, które obejmują uwierzytelnianie urządzeń użytkowników, funkcje legalnego przechwytywania (LI), bramy bezpieczeństwa (SeGW) na obrzeżach sieci, funkcje bezpieczeństwa sygnalizacji, zarządzanie roamingiem i sesjami, transport danych użytkownika i płaszczyzny sterowania, zarządzanie polityką dostępu, rejestrację i autoryzację usług sieciowych, przechowywanie danych użytkowników końcowych i danych sieciowych, krytyczne usługi sieciowe, w tym system nazw domenowych (DNS), połączenia z sieciami komórkowymi stron trzecich, udostępnianie podstawowych funkcji sieciowych aplikacjom zewnętrznym oraz wybór i zarządzanie fragmentami sieci;

---

[72] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2675 z dnia 22 listopada 2023 r. w sprawie ochrony Unii i jej państw członkowskich przed przymusem gospodarczym ze strony państw trzecich (Dz.U. L, 2023/2675, 7.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2675/oj).

(45) „wirtualizacja funkcji sieciowych (NFV) oraz zarządzanie i koordynacja sieci (MANO) w mobilnych sieciach łączności elektronicznej” oznaczają oprogramowanie i strukturę architektoniczną zapewniającą zarządzanie cyklem życia, koordynację i automatyzację wirtualnych funkcji sieciowych (VNF), funkcji sieciowych natywnych dla chmury (CNF) oraz wybór i zarządzanie segmentami sieci w mobilnych sieciach łączności elektronicznej;

(46) „sieć dostępu radiowego (RAN) mobilnych sieci łączności elektronicznej” oznacza sieć łączącą urządzenia użytkowników mobilnych z siecią podstawową, w tym stacje bazowe (eNodeB dla 4G, gNodeB dla 5G), zdalne głowice radiowe (RRH) i jednostki pasma podstawowego (BBU), aktywne systemy antenowe (AAS) oraz, w stosownych przypadkach, rozdzielone elementy RAN, takie jak jednostki scentralizowane (CU) i jednostki rozproszone (DU), a także inteligentny kontroler RAN (RIC);

(47) „funkcje sieci rdzeniowej stacjonarnych sieci łączności elektronicznej” oznaczają inteligencję sieci szkieletowej, łączącą główne węzły i obsługującą szereg podstawowych funkcji, w tym uwierzytelnianie i autoryzację użytkowników (AAA), funkcje legalnego przechwytywania (LI), system nazw domenowych (DNS) i usługi adresowania IP (DHCP), zarządzanie polityką dostępu, przechowywanie danych użytkowników końcowych i danych sieciowych, przełączanie i routing IP oraz międzynarodowe bramy internetowe (IIG);

(48) „system zarządzania siecią stacjonarnych sieci łączności elektronicznej” oznacza wszystkie scentralizowane platformy i komponenty oprogramowania niezbędne do obsługi, administrowania, konserwacji i dostarczania (OAM&P) sieci oraz monitorowania informacji związanych z siecią;

(49) „funkcje transportowe i transmisyjne stacjonarnych sieci łączności elektronicznej” oznaczają wszystkie elementy niezbędne do przesyłu i agregacji ruchu w sieci, w tym optyczne urządzenia transportowe, łącza mikrofalowe i podmorskie systemy kablowe, które obejmują urządzenia podwodne, a także urządzenia końcowe linii podmorskich (SLTE) i fizyczne urządzenia stacji lądowej;

(50) „sieć dostępowa stacjonarnych sieci łączności elektronicznej” oznacza sieć łączącą lokal użytkownika końcowego z siecią agregacyjną lub podstawową, w tym optyczne zakończenie linii (OLT) i optyczne zakończenie sieci (ONT) w przypadku sieci światłowodowych; system zakończenia modemu kablowego (CMTS) i modemy kablowe w przypadku sieci kablowych oraz elementy stacjonarnego dostępu bezprzewodowego, jeżeli są one wykorzystywane jako zamiennik linii stacjonarnej.

TYTUŁ II
AGENCJA UNII EUROPEJSKIEJ DS. CYBERBEZPIECZEŃSTWA

Rozdział I
Misja i cele

Artykuł 3
Misja ENISA

1. Misją ENISA jest wspieranie państw członkowskich i podmiotów unijnych w osiąganiu wysokiego poziomu cyberbezpieczeństwa, cyberodporności i zaufania w Unii.

2. ENISA pełni rolę punktu odniesienia w zakresie doradztwa i wiedzy specjalistycznej w dziedzinie cyberbezpieczeństwa dla państw członkowskich, a także dla innych zainteresowanych stron w Unii.

3. ENISA przyczynia się do zmniejszenia fragmentacji rynku wewnętrznego poprzez wykonywanie zadań powierzonych jej na mocy niniejszego rozporządzenia.

4. ENISA wykonuje zadania powierzone jej na mocy aktów prawnych Unii.

5. ENISA rozwija własne zdolności, w tym zdolności i umiejętności techniczne i ludzkie, niezbędne do wykonywania zadań powierzonych jej na mocy niniejszego rozporządzenia.

Artykuł 4
Cele ENISA

1. ENISA jest centrum wiedzy specjalistycznej w zakresie cyberbezpieczeństwa dzięki swojej niezależności, jakości naukowej i technicznej udzielanych porad, wkładu i pomocy, dostarczanych informacji, przejrzystości procedur operacyjnych, metod działania oraz staranności w wykonywaniu swoich zadań.

2. ENISA wspiera państwa członkowskie oraz, w stosownych przypadkach, podmioty unijne we wdrażaniu horyzontalnych i sektorowych polityk i przepisów Unii dotyczących cyberbezpieczeństwa, w tym działań w zakresie nadzoru rynku.

3. ENISA udostępnia swoją wiedzę specjalistyczną i wspiera Komisję w opracowywaniu polityki i przepisów Unii dotyczących cyberbezpieczeństwa.

4. ENISA wspiera budowanie potencjału i gotowości w całej Unii, pomagając państwom członkowskim, podmiotom unijnym, za pośrednictwem służby ds. cyberbezpieczeństwa dla instytucji, organów i jednostek organizacyjnych Unii (CERT-EU), o której mowa w rozdziale IV rozporządzenia (UE, Euratom) 2023/2841, oraz zainteresowanym podmiotom publicznym i prywatnym w zwiększaniu ochrony ich sieci i systemów informatycznych oraz w rozwijaniu i poprawianiu cyberodporności i zdolności reagowania.

5. ENISA przyczynia się do wdrożenia Akademii Umiejętności w zakresie Cyberbezpieczeństwa i wzrostu liczby pracowników w dziedzinie cyberbezpieczeństwa w Unii poprzez wspieranie wysiłków na rzecz rozwoju przenoszalności umiejętności w całej Unii, w tym poprzez utrzymanie i wdrażanie ECSF oraz opracowanie, utrzymanie i wdrażanie europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa zgodnie z rozdziałem II sekcja 4 niniejszego tytułu, a także poprzez zapewnienie szkoleń zgodnie z art. 6 ust. 8.

6. ENISA promuje współpracę, w tym wymianę informacji i koordynację na poziomie Unii, między państwami członkowskimi, podmiotami Unii zgodnie z rozporządzeniem (UE, Euratom) 2023/2841 oraz odpowiednimi zainteresowanymi stronami z sektora prywatnego i publicznego w kwestiach związanych z cyberbezpieczeństwem.

7. ENISA przyczynia się do zwiększania zdolności w zakresie cyberbezpieczeństwa na poziomie Unii w celu wspierania działań państw członkowskich w zakresie zapobiegania cyberzagrożeniom i reagowania na nie.

8. ENISA wspiera współpracę operacyjną na poziomie Unii, w tym poprzez przyczynianie się do wspólnej świadomości sytuacyjnej w zakresie cyberzagrożeń i incydentów wśród państw członkowskich oraz, we współpracy z CERT-EU, wśród podmiotów unijnych.

9. ENISA ściśle współpracuje z Europolem, zespołami CSIRT i innymi właściwymi organami krajowymi w celu poprawy gotowości w zakresie cyberbezpieczeństwa i reagowania na incydenty związane z oprogramowaniem ransomware.

10. ENISA przyczynia się do ustanowienia i utrzymania europejskich ram certyfikacji w zakresie cyberbezpieczeństwa zgodnie z tytułem III niniejszego rozporządzenia. ENISA promuje stosowanie europejskiej certyfikacji w zakresie cyberbezpieczeństwa w celu uniknięcia fragmentacji rynku wewnętrznego.

11. ENISA przyczynia się do harmonizacji jednolitego rynku cyfrowego poprzez udział w pracach normalizacyjnych istotnych dla polityki Unii w zakresie cyberbezpieczeństwa oraz poprzez opracowywanie specyfikacji technicznych.

12. ENISA promuje wysoki poziom świadomości w zakresie cyberbezpieczeństwa wśród organizacji i przedsiębiorstw.

Rozdział II
Zadania

Sekcja 1
Wspieranie wdrażania polityki i prawa Unii

Artykuł 5
Wsparcie dla realizacji polityki i prawa Unii

1. ENISA przyczynia się do wdrażania polityki i prawa Unii poprzez:

   a) pomoc państwom członkowskim we wdrażaniu polityki i prawa Unii w zakresie cyberbezpieczeństwa w sposób spójny, w tym poprzez wydawanie wytycznych technicznych i sprawozdań, udzielanie porad i dzielenie się najlepszymi praktykami oraz ułatwianie wymiany najlepszych praktyk między właściwymi organami w tym zakresie;

   b) wspieranie wymiany informacji w ramach sektorów i pomiędzy nimi, w szczególności w odniesieniu do sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555 oraz produktów zawierających elementy cyfrowe objętych zakresem rozporządzenia (UE) 2024/2847, poprzez udostępnianie najlepszych praktyk i wytycznych dotyczących dostępnych narzędzi i procedur;

   c) na wniosek Komisji, wspieranie państw członkowskich poprzez zapewnianie wsparcia, takiego jak wytyczne techniczne, w tym dotyczące środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa, narzędzi do oceny dojrzałości cyberbezpieczeństwa oraz podręczników reagowania na incydenty, dostosowanych do sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555, lub wsparcia w zakresie wdrażania zasad bezpieczeństwa od samego początku projektowania produktów zawierających elementy cyfrowe zgodnie z rozporządzeniem (UE) 2024/2847, w celu ułatwienia poprawy

poziomów dojrzałości cyberbezpieczeństwa i zgodności z prawem Unii w zakresie cyberbezpieczeństwa;

(d) przyczynianie się do prac grupy ds. współpracy ustanowionej na mocy art. 14 ust. 1 dyrektywy (UE) 2022/2555 („grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji”); europejskiej grupy ds. współpracy w zakresie tożsamości cyfrowej ustanowionej na mocy art. 46e ust. 1 rozporządzenia (UE) nr 910/2014, europejskiej grupy ds. certyfikacji cyberbezpieczeństwa („ECCG”), o której mowa w art. 90 niniejszego rozporządzenia, oraz grupy ds. współpracy administracyjnej (ADCO) ustanowionej na mocy art. 52 ust. 15 rozporządzenia (UE) 2024/2847;

e) wspieranie państw członkowskich i odpowiednich podmiotów unijnych w opracowywaniu i promowaniu polityki w zakresie cyberbezpieczeństwa związanej z utrzymaniem ogólnej dostępności i integralności publicznej podstawowej struktury otwartego internetu;

f) zgodnie z rozporządzeniem (UE) 2024/2847, udzielanie państwom członkowskim i Komisji porad technicznych i wsparcia w kwestiach związanych z wdrażaniem tego rozporządzenia;

g) wspieranie państw członkowskich w udzielaniu wzajemnej pomocy i ułatwianiu takich procesów współpracy w odniesieniu do podmiotów o znaczeniu podstawowym i istotnym zgodnie z [art. 37a dyrektywy (UE) 2022/2555];

h) na wniosek Europejskiej Rady Ochrony Danych, udzielanie porad w zakresie wdrażania konkretnych aspektów polityki i prawa Unii dotyczących cyberbezpieczeństwa w odniesieniu do ochrony danych i prywatności.

2. ENISA przyczynia się do skoordynowanej oceny ryzyka w zakresie cyberbezpieczeństwa na poziomie Unii, w tym oceny przeprowadzanej zgodnie z art. 22 dyrektywy (UE) 2022/2555.

3. ENISA wydaje wytyczne dotyczące interoperacyjności sieci i systemów informatycznych wykorzystywanych do wymiany informacji, w tym w odniesieniu do transgranicznych centrów cyberbezpieczeństwa, o których mowa w art. 6 ust. 3 rozporządzenia (UE) 2025/38.

4. ENISA jest członkiem grupy ds. współpracy w zakresie bezpieczeństwa sieci i informacji zgodnie z art. 14 ust. 3 dyrektywy (UE) 2022/2555.

5. Na wniosek Komisji ENISA zapewnia wiedzę fachową, doradztwo techniczne, informacje lub analizy lub prowadzi prace przygotowawcze w zakresie konkretnych kwestii związanych z cyberbezpieczeństwem w celu dostarczenia Komisji informacji przydatnych w kształtowaniu polityki i monitorowaniu wdrażania prawodawstwa unijnego.

Artykuł 6
Budowanie potencjału

ENISA wspiera:

(1) państwom członkowskim w ich wysiłkach na rzecz poprawy zapobiegania cyberzagrożeniom i cyberincydentom, ich wykrywania i analizowania oraz zdolności reagowania na nie, poprzez dostarczanie im wiedzy i doświadczenia;

(2) państwom członkowskim, na ich wniosek, w ustanawianiu i wdrażaniu polityki ujawniania luk w zabezpieczeniach na zasadzie dobrowolności;

(3) zgodnie z rozporządzeniem (UE, Euratom) 2023/2841, CERT-EU i międzyinstytucjonalną radą ds. cyberbezpieczeństwa w ich działaniach na rzecz wspierania podmiotów unijnych w zakresie wzmacniania ich cyberbezpieczeństwa, poprawy zapobiegania cyberzagrożeniom i cyberincydentom oraz ich wykrywania i analizowania, a także poprawy ich zdolności reagowania na takie cyberzagrożenia i cyberincydenty;

(4) państwom członkowskim w tworzeniu krajowych zespołów reagowania na incydenty związane z bezpieczeństwem informatycznym (CSIRT), jeżeli zwrócą się one z wnioskiem zgodnie z art. 10 ust. 10 dyrektywy (UE) 2022/2555;

(5) państwa członkowskie w opracowywaniu lub aktualizowaniu krajowej strategii w zakresie cyberbezpieczeństwa i kluczowych wskaźników efektywności służących do oceny tej strategii, jeżeli jest to wymagane zgodnie z art. 7 ust. 4 dyrektywy (UE) 2022/2555, promować rozpowszechnianie tych strategii i odnotowywać postępy w ich wdrażaniu w całej Unii w celu promowania najlepszych praktyk;

(6) instytucje unijne, na ich wniosek, opracowują i dokonują przeglądu strategii Unii dotyczących cyberbezpieczeństwa, promują ich rozpowszechnianie i śledzą postępy w ich wdrażaniu;

(7) krajowe zespoły CSIRT w podnoszeniu poziomu swoich zdolności, w tym poprzez promowanie dialogu i wymiany informacji, w celu zapewnienia, aby każdy zespół CSIRT posiadał wspólny zestaw minimalnych zdolności i działał zgodnie z najlepszymi praktykami, z uwzględnieniem aktualnego stanu techniki;

(8) państwa członkowskie, podmioty unijne oraz zainteresowane strony z sektora publicznego i prywatnego w ich wysiłkach na rzecz oceny, rozwoju i wzmocnienia kadr zajmujących się cyberbezpieczeństwem, w tym poprzez opracowywanie, utrzymywanie i promowanie stosowania odpowiednich narzędzi, takich jak ECSF i europejskie systemy poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, zgodnie z sekcją 4 niniejszego rozdziału;

(9) odpowiednie organy publiczne, a także prywatne zainteresowane strony poprzez prowadzenie ukierunkowanych szkoleń, w stosownych przypadkach we współpracy z zainteresowanymi stronami;

(10) grupę ds. współpracy w zakresie bezpieczeństwa sieci i informacji (NIS) w zakresie wymiany najlepszych praktyk i informacji, w szczególności w odniesieniu do wdrażania dyrektywy (UE) 2022/2555 zgodnie z art. 14 ust. 4 lit. c) tej dyrektywy;

(11) organy nadzoru rynku wyznaczone zgodnie z rozporządzeniem (UE) 2024/2847 w ich działaniach mających na celu zapewnienie skutecznego wdrożenia tego rozporządzenia, w tym wsparcie w zakresie wytycznych i doradztwa technicznego dla podmiotów gospodarczych, wsparcie w zakresie kontroli zgodności, oceny ryzyka, wspólnych działań i kontroli wyrywkowych, zgodnie z rozporządzeniem (UE) 2024/2847;

(12) członkowie ECCG w zakresie wymiany najlepszych praktyk oraz, na wniosek poszczególnych państw członkowskich, wspierają krajowe organy certyfikacji

w zakresie cyberbezpieczeństwa w związku z wdrażaniem europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa na szczeblu krajowym;

(13) organy publiczne i prywatne podmioty w zakresie działań związanych z oceną zgodności i ewaluacją, w tym organy oceny zgodności oraz małe i średnie przedsiębiorstwa, w celu wspierania solidnego, konkurencyjnego, integracyjnego i zharmonizowanego ekosystemu oceny zgodności wspierającego wdrożenie rozporządzenia (UE) 2024/2847 i europejskich ram certyfikacji w zakresie cyberbezpieczeństwa;

(14) Europejskie Centrum Kompetencji w zakresie Przemysłu, Technologii i Badań w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych centrów koordynacyjnych ustanowionych na mocy rozporządzenia (UE) 2021/887 poprzez wymianę informacji na temat obecnych i pojawiających się zagrożeń oraz cyberzagrożeń, w tym w odniesieniu do nowych i powstających technologii informacyjno-komunikacyjnych;

(15) państwa członkowskie poprzez zapewnienie wsparcia technicznego, w tym w zakresie tworzenia i funkcjonowania piaskownic regulacyjnych w dziedzinie cyberbezpieczeństwa zgodnie z odpowiednim prawodawstwem Unii.

Artykuł 7
Podnoszenie świadomości i pula talentów

ENISA wspiera państwa członkowskie w ich wysiłkach na rzecz podnoszenia świadomości na temat polityki i prawodawstwa Unii w zakresie cyberbezpieczeństwa oraz promowania ich widoczności poprzez opracowywanie praktycznych narzędzi i wytycznych. ENISA wspiera inicjatywy mające na celu zwiększenie europejskiej puli talentów w dziedzinie cyberbezpieczeństwa, w szczególności poprzez koordynację konkursów.

Artykuł 8
Znajomość rynku i analizy

1. ENISA przeprowadza i rozpowszechnia analizy głównych trendów rynkowych na rynku cyberbezpieczeństwa, zarówno po stronie popytu, jak i podaży, w szczególności w odniesieniu do obszarów, w których istnieją lub są planowane europejskie systemy certyfikacji cyberbezpieczeństwa, sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555 oraz kategorii produktów objętych rozporządzeniem (UE) 2024/2847, w tym załącznikami III i IV do tego rozporządzenia.

2. ENISA przeprowadza i rozpowszechnia analizy trendów technologicznych w zakresie cyberbezpieczeństwa, w szczególności w odniesieniu do działań i podmiotów objętych zakresem stosowania dyrektywy (UE) 2022/2555 oraz produktów zawierających elementy cyfrowe objętych zakresem stosowania rozporządzenia (UE) 2024/2847.

3. ENISA gromadzi wiedzę oraz rozpowszechnia porady techniczne i analizy dotyczące najnowocześniejszych narzędzi, ram, standardów i najlepszych praktyk w zakresie cyberbezpieczeństwa.

Artykuł 9
Współpraca międzynarodowa

ENISA przyczynia się do wysiłków Unii na rzecz współpracy z państwami trzecimi i organizacjami międzynarodowymi, a także w ramach odpowiednich ram współpracy międzynarodowej, w celu promowania współpracy międzynarodowej w kwestiach związanych z cyberbezpieczeństwem poprzez:

a) w stosownych przypadkach, uczestnicząc w charakterze obserwatora w organizacji międzynarodowych ćwiczeń oraz analizując wyniki takich ćwiczeń i składając sprawozdania z nich zarządowi;

b) na wniosek Komisji ułatwianie wymiany najlepszych praktyk z państwami trzecimi i organizacjami międzynarodowymi;

c) na wniosek Komisji, zapewnianie jej wiedzy fachowej;

d) udzielanie Komisji fachowych porad i wsparcia w kwestiach związanych z międzynarodowym uznawaniem europejskich certyfikatów cyberbezpieczeństwa zgodnie z art. 87;

e) udzielanie Komisji fachowych porad i wsparcia w kwestiach dotyczących międzynarodowej normalizacji oraz współpracę z odpowiednimi międzynarodowymi organizacjami normalizacyjnymi, w stosownych przypadkach we współpracy z ECCG ustanowioną na mocy art. 90.

Sekcja 2

Współpraca operacyjna

Artykuł 10
Współpraca operacyjna na poziomie Unii

1. ENISA wspiera współpracę operacyjną między państwami członkowskimi, podmiotami unijnymi za pośrednictwem CERT-EU oraz między innymi zainteresowanymi stronami.

2. ENISA jest członkiem sieci krajowych zespołów CSIRT ustanowionych zgodnie z art. 15 ust. 1 dyrektywy (UE) 2022/2555 i pełni funkcję sekretariatu sieci CSIRT zgodnie z art. 15 ust. 2 dyrektywy (UE) 2022/2555.

3. ENISA pełni funkcję sekretariatu europejskiej sieci organizacji łącznikowych ds. cyberkryzysów (EU-CyCLONe) zgodnie z art. 16 ust. 2 akapit drugi dyrektywy (UE) 2022/2555.

4. ENISA wspiera współpracę techniczną i operacyjną między państwami członkowskimi, w szczególności poprzez sieć CSIRT i EU-CyCLONe. Wsparcie to obejmuje:

   a) doradztwo w zakresie poprawy zdolności do zapobiegania incydentom, ich wykrywania, reagowania na nie i usuwania ich skutków;

   b) na wniosek jednego lub kilku państw członkowskich – doradztwo i oceny w odniesieniu do konkretnego potencjalnego lub trwającego incydentu lub cyberzagrożenia, w tym poprzez zapewnienie wiedzy fachowej i ułatwianie technicznego postępowania w przypadku takich incydentów oraz poprzez

wspieranie dobrowolnej wymiany odpowiednich informacji i rozwiązań technicznych między państwami członkowskimi;

c) analizowanie słabych punktów, zagrożeń i incydentów;

d na wniosek jednego lub kilku państw członkowskich, udzielanie wsparcia w odniesieniu do technicznych dochodzeń *ex post* dotyczących znaczących incydentów w rozumieniu art. 23 ust. 3 dyrektywy (UE) 2022/2555;

e) przyczynianie się do wspierania skoordynowanego zarządzania incydentami i kryzysami w zakresie cyberbezpieczeństwa na dużą skalę na poziomie operacyjnym, w szczególności poprzez pomoc EU-CyCLONe w przygotowywaniu sprawozdań dla szczebla politycznego oraz ułatwianie terminowej wymiany informacji między siecią CSIRT a EU-CyCLONe;

5. Na wniosek państwa członkowskiego lub podmiotu unijnego we współpracy z CERT-EU ENISA wspiera spójną komunikację publiczną dotyczącą incydentu lub zagrożenia cybernetycznego.

6. ENISA wspiera współpracę między państwami członkowskimi oraz, za pośrednictwem CERT-EU, między podmiotami unijnymi w zakresie wdrażania bezpiecznych narzędzi komunikacyjnych. ENISA korzysta w ramach sieci CSIRT i EU-CyCLONe z bezpiecznych narzędzi komunikacyjnych dostarczanych przez podmioty prawne mające siedzibę lub uznane za mające siedzibę w Unii i kontrolowane przez państwa członkowskie lub obywateli państw członkowskich.

Artykuł 11
Wspólna świadomość sytuacji w zakresie cyberbezpieczeństwa

1. W celu poprawy wspólnej świadomości sytuacji w zakresie cyberzagrożeń i incydentów wśród państw członkowskich i podmiotów unijnych ENISA:

a) we współpracy z EU-CyCLONe, siecią CSIRT, Komisją, CERT-EU, Europolem i innymi odpowiednimi podmiotami Unii opracowuje repozytoria zweryfikowanych, wiarygodnych informacji wywiadowczych dotyczących cyberzagrożeń, w tym trendów w zakresie incydentów, taktyk, technik i procedur;

b) zgodnie z art. 12 wydaje wczesne ostrzeżenia o potencjalnym lub trwającym znaczącym lub zakrojonym na szeroką skalę incydencie lub cyberzagrożeniu o potencjalnym charakterze transgranicznym , w szczególności w odniesieniu do sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555;

c) dostarczać na żądanie sieci CSIRT, EU-CyCLONe lub Komisji aktualnych analiz ad hoc dotyczących pojawiających się trendów w zakresie incydentów;

d) na wniosek państw członkowskich lub Komisji dostarczać analizy lub inne informacje dotyczące rzeczywistego lub potencjalnego ryzyka lub zagrożenia dla cyberbezpieczeństwa;

e) dostarczać analizy i porady techniczne dotyczące zagrożeń dla cyberbezpieczeństwa w produktach zawierających elementy cyfrowe, w tym w celu wsparcia nadzoru rynku oraz poprzez sporządzanie co dwa lata sprawozdania technicznego na temat pojawiających się trendów zgodnie z art. 17 ust. 3 rozporządzenia (UE) 2024/2847;

f) przygotowywać regularne, szczegółowe sprawozdania techniczne UE dotyczące sytuacji w zakresie cyberbezpieczeństwa, obejmujące incydenty i zagrożenia cybernetyczne, , oraz udostępniać te sprawozdania Radzie, EU-CyCLONe, sieci CSIRT, Komisji, Europejskiej Służbie Działań Zewnętrznych i Europolowi;

g) monitorowanie trendów w zakresie technik, żądań i skutków ataków ransomware oraz przekazywanie informacji o takich trendach Komisji, sieci CSIRT, EU-CyCLONe i Europolowi.

2. W celu zwiększenia wspólnej świadomości sytuacji w zakresie cyberzagrożeń i incydentów wśród zainteresowanych stron ENISA:

a) przeprowadzać analizy cyberzagrożeń, incydentów, trendów, nowych technologii i ich skutków, w tym regularne analizy dotyczące sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555 oraz odpowiednich kategorii produktów objętych rozporządzeniem (UE) 2024/2847;

b) we współpracy z Komisją oraz, w stosownych przypadkach, z siecią CSIRT, wydaje zalecenia, wytyczne i najlepsze praktyki dotyczące bezpieczeństwa sieci i systemów informatycznych, w szczególności bezpieczeństwa infrastruktur wspierających sektory wymienione w załącznikach I i II do dyrektywy (UE) 2022/2555;

c) przeprowadzać długoterminowe analizy strategiczne zagrożeń i incydentów cybernetycznych w celu identyfikacji pojawiających się trendów i pomocy w zapobieganiu incydentom.

3. ENISA może podawać do wiadomości publicznej analizy, porady, wytyczne, najlepsze praktyki i sprawozdania, o których mowa w ust. 2, w porozumieniu z podmiotami, o których mowa w ust. 2.

4. Wykonując działania wymienione w ust. 1 lit. a)–d) i f) oraz w ust. 2, ENISA korzysta z własnych analiz oraz, w stosownych przypadkach, z informacji otrzymanych w trakcie wykonywania swoich zadań, w tym:

a) informacji pochodzących z publicznie dostępnych źródeł, w tym publicznie znanych luk w zabezpieczeniach produktów lub usług ICT dostępnych w europejskiej bazie danych dotyczących luk w zabezpieczeniach, utworzonej zgodnie z art. 12 ust. 2 dyrektywy (UE) 2022/2555;

(b) informacje udostępniane przez państwa członkowskie, podmioty unijne, CERT-EU, partnerów z sektora prywatnego lub pozarządowego oraz organizacje z państw trzecich i organizacje międzynarodowe, z zastrzeżeniem wszelkich ograniczeń dotyczących dalszego rozpowszechniania tych informacji, oznaczonych w widoczny sposób.

5. ENISA ściśle współpracuje z państwami członkowskimi przy przygotowywaniu sprawozdania UE dotyczącego sytuacji technicznej w zakresie cyberbezpieczeństwa, o którym mowa w ust. 1 lit. e). Sprawozdanie opiera się na informacjach dostępnych publicznie, własnej analizie ENISA oraz sprawozdaniach udostępnionych między innymi przez CSIRT państw członkowskich lub pojedyncze punkty kontaktowe ustanowione dyrektywą (UE) 2022/2555, zarówno na zasadzie dobrowolności, jak i przez EC3 oraz CERT-EU. W porozumieniu z podmiotami przekazującymi informacje ENISA może udostępnić publicznie zbiorczą wersję sprawozdania.

Artykuł 12
Wczesne ostrzeganie

1. Wczesne ostrzeżenia, o których mowa w art. 11 ust. 1 akapit pierwszy lit. b) niniejszego rozporządzenia, zawierają istotne informacje dotyczące potencjalnego lub trwającego znaczącego lub zakrojonego na szeroką skalę incydentu lub cyberzagrożenia o potencjalnym charakterze transgranicznym w odniesieniu do sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555. Informacje te mogą obejmować publicznie znane luki w zabezpieczeniach oraz informacje o tym, czy mają one wpływ na produkty zawierające elementy cyfrowe objęte rozporządzeniem (UE) 2024/2847, techniki i procedury, wskaźniki naruszenia bezpieczeństwa, taktyki przeciwników, informacje dotyczące konkretnych podmiotów stanowiących zagrożenie oraz zalecenia dotyczące środków łagodzących.

2. Wczesne ostrzeżenia, o których mowa w art. 11 ust. 1 akapit pierwszy lit. b), są przekazywane jak najszybciej do zainteresowanego CSIRT lub CSIRT, a w stosownych przypadkach do sieci CSIRT i EU-CyCLONe.

3. ENISA oferuje usługę wczesnego ostrzegania podmiotom działającym w sektorach wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555.

4. Usługa, o której mowa w ust. 3, jest świadczona na wniosek podmiotu w formacie nadającym się do odczytu maszynowego i udostępniana publicznie. Usługa ta obejmuje wymianę informacji na temat wskaźników zagrożeń cybernetycznych oraz zaleceń dotyczących środków łagodzących.

5. ENISA ustanawia procedurę rozpowszechniania wczesnych ostrzeżeń wśród podmiotów, o których mowa w ust. 3.

Artykuł 13
Wsparcie w reagowaniu na incydenty i przegląd

1. ENISA prowadzi i zarządza rezerwą UE w zakresie cyberbezpieczeństwa, w całości lub w części, zgodnie z rozporządzeniem (UE) 2025/38.

2 Na wniosek Komisji lub EU-CyCLONe ENISA, przy wsparciu sieci CSIRT i za zgodą zainteresowanego państwa członkowskiego, dokonuje przeglądu i oceny znaczących incydentów związanych z cyberbezpieczeństwem lub incydentów związanych z cyberbezpieczeństwem na dużą skalę zgodnie z art. 21 rozporządzenia (UE) 2025/38.

3. ENISA, we współpracy z Europolem i CSIRT lub innymi właściwymi organami, w zależności od przypadku, pomaga poszczególnym podmiotom o znaczeniu kluczowym i istotnym, wymienionym w załącznikach I i II do dyrektywy (UE) 2022/2555, w przygotowaniu się na incydent związany z oprogramowaniem ransomware, reagowaniu na niego i usuwaniu jego skutków. W tym celu ENISA ustanawia punkt pomocy technicznej, a w szczególności korzysta z ulepszonej wspólnej świadomości sytuacyjnej w zakresie cyberzagrożeń i incydentów zgodnie z art. 11 ust. 1 akapit pierwszy lit. a) i g) niniejszego rozporządzenia.

Artykuł 14
Ćwiczenia w zakresie cyberbezpieczeństwa na poziomie Unii

1. ENISA wspiera Komisję w opracowywaniu rocznego programu ćwiczeń w zakresie cyberbezpieczeństwa na poziomie Unii.

2 ENISA prowadzi rejestr wniosków wyciągniętych z ćwiczeń, o których mowa w ust. 1, oraz zaleca państwom członkowskim i, w stosownych przypadkach, podmiotom unijnym, jak skutecznie i efektywnie wdrażać wyciągnięte wnioski.

3. Na wniosek EU-CyCLONe, Komisji i ENISA organizuje lub uczestniczy w organizacji ćwiczeń w zakresie cyberbezpieczeństwa na poziomie Unii, w tym testuje gotowość do reagowania na incydenty i kryzysy związane z cyberbezpieczeństwem na dużą skalę na poziomie Unii.

4. Na wniosek państw członkowskich ENISA wspiera je w organizowaniu krajowych ćwiczeń w zakresie cyberbezpieczeństwa.

5. Na wniosek CERT-EU ENISA uczestniczy w organizacji ćwiczeń w zakresie cyberbezpieczeństwa organizowanych przez CERT-EU zgodnie z art. 13 ust. 7 rozporządzenia (UE, Euratom) 2023/2841.

Artykuł 15
Dostarczanie narzędzi i platform

1. ENISA ustanawia, zapewnia, obsługuje, utrzymuje i aktualizuje w razie potrzeby operacyjne narzędzia techniczne, w tym platformy związane z cyberbezpieczeństwem na poziomie Unii, w szczególności jednolitą platformę zgłaszania incydentów ustanowioną zgodnie z art. 16 ust. 1 rozporządzenia (UE) 2024/2847 [oraz jednolitego punktu zgłoszeniowego incydentów ustanowionego zgodnie z art. 23a dyrektywy (UE) 2022/2555], oraz narzędzia testowe wspierające wdrażanie procedur oceny zgodności zgodnie z odpowiednim prawodawstwem Unii.

2. W stosownych przypadkach do celów ust. 1 ENISA współpracuje i wymienia informacje z siecią CSIRT oraz, w stosownych przypadkach, z organami nadzoru rynku.

Artykuł 16
Usługi zarządzania podatnością na zagrożenia

ENISA rozwija wspólne unijne zdolności w zakresie usług zarządzania podatnością na zagrożenia i świadczy usługi zarządzania podatnością na zagrożenia na rzecz zainteresowanych stron poprzez:

a) prowadzenie europejskiej bazy danych podatności ustanowionej zgodnie z art. 12 ust. 2 dyrektywy (UE) 2022/2555;

b) świadczenie usług zarządzania podatnością na zagrożenia na rzecz zainteresowanych stron w oparciu o europejską bazę danych podatności na zagrożenia i z wykorzystaniem odpowiednich informacji dostępnych dla ENISA;

c) w stosownych przypadkach nawiązywanie zorganizowanej współpracy z organizacjami zapewniającymi programy, rejestry lub bazy danych podobne do europejskiej bazy danych dotyczących luk w zabezpieczeniach;

d) aktywne wspieranie zespołów CSIRT wyznaczonych jako koordynatorzy zgodnie z art. 12 ust. 1 dyrektywy (UE) 2022/2555 w zakresie zarządzania skoordynowanym ujawnianiem luk w zabezpieczeniach, które mogą mieć znaczący wpływ na podmioty w więcej niż jednym państwie członkowskim;

e) opracowywanie i utrzymywanie metodologii i mechanizmów zarządzania służących identyfikacji luk w zabezpieczeniach i skoordynowanemu ujawnianiu informacji, we

współpracy z właściwymi organami krajowymi, zespołami CSIRT, przemysłem i środowiskiem badawczym.

Sekcja 3

Certyfikacja i normalizacja w zakresie cyberbezpieczeństwa

Artykuł 17
Certyfikacja w zakresie cyberbezpieczeństwa

1. ENISA przyczynia się do opracowywania i wdrażania polityki Unii w zakresie certyfikacji w dziedzinie cyberbezpieczeństwa, określonej w tytule III niniejszego rozporządzenia, oraz promuje tę politykę. ENISA odpowiada za:

   a) przygotowywanie europejskich systemów certyfikacji cyberbezpieczeństwa będących przedmiotem wniosku („systemy będące przedmiotem wniosku") dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberbezpieczeństwa podmiotów zgodnie z art. 74 oraz, w stosownych przypadkach, opracowywanie specyfikacji technicznych zgodnie z art. 77;

   b) utrzymywanie przyjętych europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa zgodnie z art. 75, w tym z myślą o ewentualnym przeglądzie przyjętych europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa zgodnie z art. 76;

   c) promowanie stosowania przyjętych systemów oraz prowadzenie specjalnej strony internetowej zawierającej informacje na temat europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, europejskich certyfikatów cyberbezpieczeństwa i unijnych oświadczeń o zgodności oraz ich upowszechnianie zgodnie z art. 79;

   d) organizowanie działań związanych z budowaniem potencjału w zakresie procesów certyfikacji, działań oceniających, wzajemnej weryfikacji i wzajemnej oceny, w tym poprzez udzielanie wsparcia państwom członkowskim na ich wniosek zgodnie z art. 6 pkt 12.

2. ENISA wspiera Komisję w następujących działaniach:

   a) zarządzanie ECCG zgodnie z art. 90;

   b) organizowanie europejskiego zgromadzenia ds. certyfikacji cyberbezpieczeństwa zgodnie z art. 72 ust. 1;

   c) w odniesieniu do międzynarodowego uznawania europejskich certyfikatów cyberbezpieczeństwa zgodnie z art. 87;

   d) organizowanie wzajemnych ocen zgodnie z art. 89;

   e) przygotowywanie wzorcowych przepisów, do których należy się odwoływać w europejskich systemach certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberpostury podmiotów zgodnie z art. 81 ust. 5.

Artykuł 18
Normalizacja, specyfikacje techniczne i wytyczne

1. ENISA opracowuje specyfikacje techniczne i wytyczne w celu wsparcia wdrażania prawodawstwa Unii w dziedzinie cyberbezpieczeństwa. Przy opracowywaniu tych specyfikacji technicznych ENISA uwzględnia istniejące normy europejskie i międzynarodowe, jak n , a także inne odpowiednie specyfikacje techniczne. ENISA zapewnia spójność swoich specyfikacji technicznych i wytycznych.

2. ENISA monitoruje oraz, w stosownych przypadkach, uczestniczy w działaniach związanych z opracowywaniem norm na poziomie unijnym oraz, zgodnie z art. 9, na poziomie międzynarodowym, a także kieruje tymi działaniami, mając na celu wspieranie polityki Unii w zakresie cyberbezpieczeństwa.

3. ENISA wspiera opracowywanie i ocenę algorytmów kryptograficznych. W przypadku pozytywnej oceny algorytmu kryptograficznego przez ENISA, ENISA współpracuje, zgodnie z rozporządzeniem (UE) nr 1025/2012, z europejskimi organami normalizacyjnymi w celu wsparcia jego normalizacji.

4. ENISA udziela Komisji oraz, w stosownych przypadkach, państwom członkowskim doradztwa technicznego w zakresie odpowiednich norm lub specyfikacji technicznych wspierających politykę Unii w zakresie cyberbezpieczeństwa, w tym w odniesieniu do unijnych przepisów harmonizacyjnych w dziedzinie cyberbezpieczeństwa, w szczególności rozporządzenia (UE) 2024/2847, obszarów technicznych do celów art. 25 dyrektywy (UE) 2022/2555 oraz europejskich systemów certyfikacji cyberbezpieczeństwa zgodnie z art. 81 ust. 1 lit. d).

5. ENISA wspiera Komisję w ocenie projektów zharmonizowanych norm w celu wsparcia wdrażania unijnych przepisów harmonizacyjnych w dziedzinie cyberbezpieczeństwa.

6. ENISA promuje stosowanie europejskich i międzynarodowych norm w zakresie cyberbezpieczeństwa.

7. ENISA wykonuje zadania, o których mowa w ust. 1–6, w sposób uczciwy, bezstronny i poufny, w tym poprzez wycofanie się lub zawieszenie swojego udziału w określonych organach technicznych, jeżeli taki udział koliduje z innymi zadaniami lub celami.

Sekcja 4
Wdrożenie Akademii Umiejętności w zakresie Cyberbezpieczeństwa

Artykuł 19
Europejskie ramy umiejętności w zakresie cyberbezpieczeństwa

1. ENISA opracowuje i podaje do wiadomości publicznej europejskie ramy umiejętności w zakresie cyberbezpieczeństwa („ECSF”). Przed podaniem ECSF do wiadomości publicznej lub aktualizacją zgodnie z ust. 4 ENISA konsultuje się z Komisją.

2. ECSF określa profile specjalistów ds. cyberbezpieczeństwa oraz powiązania konkretnych zadań, umiejętności i wiedzy z danym profilem stanowiska. Korzystanie z ECSF jest dobrowolne dla podmiotów publicznych i prywatnych.

3. ENISA może konsultować się z zainteresowanymi stronami w zakresie opracowania i wdrożenia ECSF.

4. ENISA ocenia potrzebę regularnej aktualizacji ECSF i w stosownych przypadkach dokonuje jej.

Artykuł 20

Opracowywanie, przyjmowanie i utrzymywanie europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa

1. ENISA opracowuje, przyjmuje i utrzymuje europejskie systemy poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa. Korzystanie z europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa jest dobrowolne dla krajowych organów publicznych i podmiotów prywatnych, chyba że prawo krajowe stanowi inaczej.

2. Przed zainicjowaniem nowego europejskiego systemu poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa ENISA konsultuje się z Komisją. ENISA przyjmuje taki system wyłącznie po uzyskaniu pozytywnej opinii Komisji. Przygotowując europejski system poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, ENISA może konsultować się z odpowiednimi zainteresowanymi stronami.

3. Europejski system poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa obejmuje:

   a) przedmiot i zakres systemu certyfikacji opartego na profilach ról ECSF lub ich podzbiorach;

   b) wymogi mające zastosowanie do osób przeszkolonych do przeprowadzania ocen („oceniających”) zgodnie z art. 21, niezbędne umiejętności, wiedza i doświadczenie, a także metody szkolenia;

   c) analiza przyjęcia na rynku właściwa dla każdego systemu certyfikacji;

   d) efekty uczenia się, metody oceny i warunki, które uprawnieni dostawcy poświadczeń powinni stosować do oceny wykazania przez daną osobę wymaganych umiejętności zgodnie z art. 21;

   e) w stosownych przypadkach, jeden lub więcej poziomów biegłości;

   f) zasady dotyczące przechowywania dokumentacji przez uprawnionych dostawców poświadczeń;

   g) treść i format europejskich indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa, z należytym uwzględnieniem art. 21 ust. 5 lit. e);

   h) maksymalny okres ważności europejskiego indywidualnego poświadczenia umiejętności w zakresie cyberbezpieczeństwa wydanego w ramach systemu poświadczeń.

4. Europejski system certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa może obejmować orientacyjny koszt europejskiego certyfikatu indywidualnych umiejętności w zakresie cyberbezpieczeństwa.

5. ENISA zapewnia ścisłą współpracę z państwami członkowskimi podczas przygotowywania europejskich systemów certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa.

6. Zmiana europejskiego systemu poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa nie ma wpływu na zezwolenie udzielone zgodnie z art. 22 ust. 3 lit. a), które pozostaje ważne przez okres, na który zostało udzielone.

Artykuł 21
Upoważnieni dostawcy certyfikatów

1. Upoważnieni dostawcy certyfikatów oceniają, czy osoby fizyczne spełniają wymogi europejskiego systemu certyfikacji umiejętności w zakresie cyberbezpieczeństwa, a w przypadku spełnienia tych wymogów wydają europejskie certyfikaty umiejętności w zakresie cyberbezpieczeństwa. Dostawcy certyfikatów mogą posiadać kilka upoważnień, z których każde przyznane jest dla jednego europejskiego systemu certyfikacji umiejętności w zakresie cyberbezpieczeństwa.

2. ENISA zapewnia wytyczne dla oceniających i przeprowadza obowiązkowe szkolenia dla nich w zakresie wymogów i metod oceny zawartych w europejskim systemie poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, o którym mowa w art. 20 ust. 3 lit. b).

3. Podmioty pragnące uzyskać upoważnienie na świadczenie usług poświadczania lub odnowić swoje upoważnienie („wnioskodawcy”) składają wniosek do ENISA. Spełniają one następujące wymogi:

   a) posiadać osobowość prawną;

   b) być zdolne do wykonywania zadań określonych w niniejszym rozporządzeniu w odniesieniu do europejskich indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa, niezależnie od tego, czy ocena jest przeprowadzana przez samego uprawnionego dostawcę poświadczeń, czy w jego imieniu i na jego odpowiedzialność;

   c) posiadać środki niezbędne do wykonywania zadań technicznych i administracyjnych związanych z europejskim systemem indywidualnych certyfikatów umiejętności w zakresie cyberbezpieczeństwa w odpowiedni sposób oraz mieć dostęp do wszystkich niezbędnych urządzeń i obiektów.

   Do celów lit. b) akapitu pierwszego wszelkie podwykonawstwo lub konsultacje z personelem zewnętrznym są odpowiednio dokumentowane, nie angażują żadnych pośredników i podlegają pisemnej umowie obejmującej między innymi kwestie poufności i konfliktu interesów.

4. Wnioskodawcy nie mogą być dostawcami wysokiego ryzyka.

5. Upoważnieni dostawcy certyfikatów muszą spełniać następujące obowiązki:

   a) w odniesieniu do wdrożenia każdego europejskiego systemu certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa:

      (i) dysponować niezbędnymi oceniającymi i personelem do terminowego wykonywania swoich działań określonych w tym systemie;

      (ii) zapewnić, aby oceniający przestrzegali tajemnicy zawodowej, byli bezstronni i wykonywali swoją pracę niezależnie oraz z zachowaniem najwyższego stopnia uczciwości zawodowej;

      (iii) posiadać pisemne procedury wykonywania swoich działań w ramach systemu, do którego są uprawnione.

b) nie oceniać ani nie wydawać europejskich indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa swoim własnym oceniającym;

(c) zapewniać, w stosownych przypadkach poprzez wprowadzenie odpowiednich zabezpieczeń, aby ich oceniający mogli wykonywać swoją pracę w sposób niezależny, w szczególności w przypadku gdy osoby te należą do ich własnej struktury lub są pracownikami lub uczniami takiej struktury;

d) nie angażować się w żadną działalność, która mogłaby kolidować z niezależnością osądu lub uczciwością ich oceniających;

e) zapewnić, na wniosek danej osoby, wydawanie elektronicznych poświadczeń europejskich indywidualnych umiejętności w zakresie cyberbezpieczeństwa w formie poświadczeń elektronicznych atrybutów w formacie, który można przechowywać w europejskich portfelach tożsamości cyfrowej określonych w rozporządzeniu (UE) nr 910/2014.

6. Upoważnieni dostawcy poświadczeń niezwłocznie informują ENISA, jeżeli którekolwiek z wymogów wymienionych w ust. 3 i 4 lub obowiązków wymienionych w ust. 5 nie są już spełniane lub jeżeli pojawiają się jakiekolwiek wątpliwości co do spełnienia tych wymogów lub obowiązków, w tym dotyczące niezależności oceniających.

7. Upoważnieni wydawcy certyfikatów mogą pobierać opłaty od osób fizycznych za ocenę i wydawanie europejskich certyfikatów indywidualnych umiejętności w zakresie cyberbezpieczeństwa, biorąc pod uwagę orientacyjny koszt europejskiego certyfikatu indywidualnych umiejętności w zakresie cyberbezpieczeństwa zgodnie z art. 20 ust. 4 i podany do wiadomości publicznej na specjalnej stronie internetowej zgodnie z art. 23 lit. d).

8. Wnioskodawcy i uprawnieni dostawcy poświadczeń umożliwiają ENISA przeprowadzanie ocen w ramach procesu składania wniosków lub utrzymania upoważnienia oraz udostępniają wszystkie istotne informacje w celu zapewnienia, że wymogi określone w ust. 3 i 4 lub obowiązki określone w ust. 5 są spełnione lub nadal są spełniane zgodnie z art. 22 ust. 2.

Artykuł 22

Rozpatrywanie wniosków o uzyskanie statusu uprawnionego dostawcy poświadczeń i utrzymanie uprawnień

1. Wnioskodawcy uiszczają opłatę na rzecz ENISA za rozpatrzenie ich wniosku. Upoważnieni dostawcy poświadczeń uiszczają opłatę na rzecz ENISA za utrzymanie ich upoważnienia.

2. ENISA ocenia, czy wnioskodawcy i uprawnieni dostawcy poświadczeń spełniają lub nadal spełniają wymogi określone w art. 21 ust. 3 i 4 oraz obowiązki określone w art. 21 ust. 5.

3. Po rozpatrzeniu wniosku pod kątem wymogów określonych w art. 21 ust. 3 i 4 ENISA może wydać jedną z następujących decyzji:

a) przyznanie wnioskodawcy statusu uprawnionego dostawcy poświadczeń lub jego odnowienie;

b) odrzucenie wniosku o uzyskanie statusu upoważnionego dostawcy poświadczeń lub nieprzedłużenie tego statusu;

c) zamknięcie postępowania w sprawie wniosku z powodu braku działania wnioskodawcy po wezwaniu przez ENISA do dostarczenia dodatkowych informacji.

ENISA może zmienić, zawiesić lub uchylić takie decyzje na podstawie swojej oceny zgodnie z art. 22 ust. 2 lub w przypadku, o którym mowa w art. 21 ust. 6.

4. ENISA wydaje decyzję, o której mowa w ust. 3, w terminie trzech miesięcy od daty złożenia wniosku zgodnie z art. 21 ust. 3. W przypadku gdy ENISA zwróciła się do wnioskodawcy o dodatkowe informacje, ENISA wydaje decyzję, o której mowa w ust. 3, w terminie jednego miesiąca od otrzymania dodatkowych informacji.

5. Decyzja, o której mowa w ust. 3 lit. a), jest wydawana na okres maksymalnie trzech lat i zawiera informację o opłacie związanej z corocznym utrzymaniem zezwolenia.

6. ENISA zapewnia, aby jej działania związane z opracowywaniem i przyjmowaniem europejskich systemów potwierdzania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, określonych w art. 20, były ściśle oddzielone i prowadzone niezależnie od działań związanych z rozpatrywaniem wniosków i ocenami, o których mowa w ust. 2 i 3 niniejszego artykułu.

Artykuł 23
Informacje publiczne

ENISA prowadzi i regularnie aktualizuje specjalną stronę internetową zawierającą informacje publiczne na temat:

(a) ECSF, w tym ramy i harmonogram aktualizacji;

b) europejskie systemy certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa, postępy w ich opracowywaniu oraz harmonogramy ich rozwoju;

c) opłaty związane z każdym europejskim systemem poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa przyjętym zgodnie z art. 47 niniejszego rozporządzenia;

d) orientacyjny koszt europejskiego certyfikatu indywidualnych umiejętności w zakresie cyberbezpieczeństwa zgodnie z art. 20 ust. 4;

e) wykaz uprawnionych podmiotów certyfikujących.

Rozdział III
Organizacja ENISA

Artykuł 24
Struktura administracyjna i zarządcza ENISA

Struktura administracyjna i zarządcza ENISA obejmuje:

a) zarząd, który pełni funkcje określone w art. 28;

b) zarząd wykonawczy, który pełni funkcje określone w art. 30;

c) dyrektor wykonawczy, który wykonuje obowiązki określone w art. 32;

d) zastępca dyrektora wykonawczego, który wykonuje obowiązki określone w art. 34;

e) grupa doradcza ENISA;

f) komisję odwoławczą, która wykonuje funkcje określone w art. 39–42.

Sekcja 1
Zarząd

Artykuł 25
Skład zarządu

1. Zarząd składa się z jednego członka mianowanego przez każde państwo członkowskie oraz dwóch członków mianowanych przez Komisję. Wszyscy członkowie mają prawo głosu.

2. Każdy członek zarządu ma zastępcę. Zastępcy reprezentują członków w przypadku ich nieobecności.

3. Każde państwo członkowskie mianuje szefa właściwego organu krajowego wyznaczonego zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555 na członka zarządu. W przypadku gdy okaże się to niemożliwe, państwa członkowskie powołują wysokiego rangą przedstawiciela krajowego właściwego organu wyznaczonego zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555 na członka zarządu.

4. Członkowie mianowani przez Komisję oraz zastępcy członków zarządu są mianowani ze względu na ich wiedzę w dziedzinie cyberbezpieczeństwa, z uwzględnieniem ich odpowiednich umiejętności w zakresie zarządzania, administracji i budżetu. Komisja i państwa członkowskie, w odniesieniu do zastępców, dążą do osiągnięcia zrównoważonej reprezentacji kobiet i mężczyzn w zarządzie oraz podejmują wysiłki w celu ograniczenia ich rotacji, aby zapewnić ciągłość prac zarządu.

5. Kadencja członków mianowanych przez państwa członkowskie jest równa kadencji ich funkcji, o której mowa w ust. 3.

6. Kadencja zastępców i członków mianowanych przez Komisję trwa cztery lata. Kadencja ta może być odnawiana.

Artykuł 26
Przewodniczący zarządu

1. Zarząd wybiera przewodniczącego i wiceprzewodniczącego spośród swoich członków posiadających prawo głosu. Przewodniczący i wiceprzewodniczący są wybierani większością dwóch trzecich głosów członków zarządu posiadających prawo głosu.

2. Wiceprzewodniczący automatycznie zastępuje przewodniczącego, jeżeli przewodniczący nie może pełnić swoich obowiązków.

3. Kadencja przewodniczącego i wiceprzewodniczącego trwa cztery lata i może zostać przedłużona jeden raz. Jeżeli jednak członkostwo w zarządzie wygaśnie w dowolnym momencie kadencji, kadencja ta wygasa automatycznie z dniem wygaśnięcia członkostwa.

Artykuł 27
Posiedzenia zarządu

1. Przewodniczący zwołuje posiedzenia zarządu.

2. Dyrektor wykonawczy uczestniczy w posiedzeniach zarządu bez prawa głosu.

3. Zarząd zbiera się co najmniej dwa razy w roku na posiedzeniach zwyczajnych. Ponadto zbiera się z inicjatywy przewodniczącego, na wniosek Komisji lub na wniosek co najmniej jednej trzeciej swoich członków.

4. Przedstawiciel Europejskiego Centrum Kompetencji w zakresie Przemysłu, Technologii i Badań w dziedzinie Cyberbezpieczeństwa, ustanowionego rozporządzeniem (UE) 2021/887, jest stałym obserwatorem bez prawa głosu na posiedzeniach zarządu.

5. Zarząd może zaprosić każdą osobę, której opinia może być interesująca, do udziału w posiedzeniu lub jego części w charakterze obserwatora *ad hoc*, bez prawa głosu i z zastrzeżeniem przepisów regulaminu Zarządu.

6. Członkowie zarządu i ich zastępcy mogą być wspomagani podczas posiedzeń zarządu przez doradców lub ekspertów, z zastrzeżeniem regulaminu wewnętrznego zarządu.

Artykuł 28
Funkcje Zarządu

1. Zarząd:

a) ustala ogólny kierunek działania ENISA i zapewnia, aby ENISA działała zgodnie z zasadami i przepisami określonymi w niniejszym rozporządzeniu; zapewnia również spójność działań ENISA z działaniami prowadzonymi przez państwa członkowskie oraz na szczeblu Unii;

b) przyjmuje projekt jednolitego dokumentu programowego ENISA, o którym mowa w art. 44, przed przedłożeniem go Komisji do zaopiniowania;

c) uwzględniając opinię Komisji, przyjmuje jednolity dokument programowy ENISA zgodnie z art. 29 ust. 2 lit. a);

d) nadzoruje realizację programu wieloletniego i rocznego zawartego w jednolitym dokumencie programowym;

e) przyjmuje roczny budżet ENISA zgodnie z art. 29 ust. 2 lit. b) oraz wykonuje inne funkcje związane z budżetem ENISA zgodnie z rozdziałem IV;

f) ocenia i przyjmuje skonsolidowane roczne sprawozdanie z działalności ENISA, w tym sprawozdanie finansowe i opis realizacji wskaźników efektywności ENISA; przedkłada roczne sprawozdanie i jego ocenę do dnia 1 lipca następnego roku Parlamentowi Europejskiemu, Radzie, Komisji i Europejskiemu Trybunałowi Obrachunkowemu; podaje roczne sprawozdanie do wiadomości publicznej;

g) przyjmuje przepisy finansowe mające zastosowanie do ENISA zgodnie z art. 50;

h) przyjęcie strategii zwalczania nadużyć finansowych proporcjonalnej do ryzyka nadużyć, z uwzględnieniem analizy kosztów i korzyści środków, które mają zostać wdrożone;

i) zapewniać odpowiednie działania następcze w związku z ustaleniami i zaleceniami wynikającymi z wewnętrznych lub zewnętrznych sprawozdań z audytu i ocen oraz z dochodzeń Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych (OLAF) i Prokuratury Europejskiej (EPPO);

j) przyjąć swój regulamin wewnętrzny, w tym zasady dotyczące tymczasowych decyzji w sprawie przekazywania określonych zadań, zgodnie z art. 30 ust. 7;

k) wykonywać, zgodnie z ust. 2 niniejszego artykułu, w odniesieniu do personelu ENISA, uprawnienia przyznane na mocy regulaminu pracowniczego urzędników Unii Europejskiej („regulamin pracowniczy") oraz warunków zatrudnienia innych pracowników Unii Europejskiej („warunki zatrudnienia"), określonych w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68[73] , odpowiednio w odniesieniu do organu powołującego i organu uprawnionego do zawierania umów o pracę („uprawnienia organu powołującego");

l) przyjmuje przepisy wykonawcze wprowadzające w życie regulamin pracowniczy i warunki zatrudnienia zgodnie z art. 110 ust. 2 regulaminu pracowniczego;

m) mianowanie dyrektora wykonawczego oraz, w przypadku podjęcia decyzji o utworzeniu stanowiska zastępcy dyrektora wykonawczego, zastępcy dyrektora wykonawczego, a w stosownych przypadkach przedłużenie ich kadencji lub odwołanie ich ze stanowiska zgodnie z art. 31;

n) mianować księgowego, z zastrzeżeniem przepisów regulaminu pracowniczego i warunków zatrudnienia, który jest niezależny w wykonywaniu swoich obowiązków;

o) podejmowanie wszelkich decyzji dotyczących ustanowienia struktur wewnętrznych ENISA oraz, w razie potrzeby, zmiany tych struktur wewnętrznych, z uwzględnieniem potrzeb działalności ENISA i zasad należytego zarządzania budżetem;

p) zatwierdza zawieranie porozumień roboczych zgodnie z art. 68;

q) zatwierdzać zawieranie porozumień roboczych zgodnie z art. 70;

(r) mianować i odwoływać członków Komisji Odwoławczej zgodnie z art. 29 ust. 2 lit. d);

(s) przyjmowanie zasad dotyczących zapobiegania konfliktom interesów i zarządzania nimi w odniesieniu do członków Komisji Odwoławczej.

2. Zgodnie z art. 110 ust. 2 regulaminu pracowniczego zarząd przyjmuje decyzję na podstawie art. 2 ust. 1 regulaminu pracowniczego i art. 6 warunków zatrudnienia, przekazując dyrektorowi wykonawczemu odpowiednie uprawnienia organu powołującego i określając warunki, na jakich przekazanie tych uprawnień może zostać zawieszone. Dyrektor wykonawczy może przekazać te uprawnienia dalej.

3. W wyjątkowych okolicznościach zarząd może podjąć decyzję o tymczasowym zawieszeniu przekazania uprawnień organu powołującego dyrektorowi wykonawczemu oraz wszelkich uprawnień organu powołującego przekazanych przez dyrektora wykonawczego i zamiast tego wykonywać je samodzielnie lub przekazać je jednemu ze swoich członków lub pracownikowi innemu niż dyrektor wykonawczy.

Artykuł 29
Zasady głosowania w zarządzie

1. Zarząd podejmuje decyzje bezwzględną większością głosów swoich członków uprawnionych do głosowania, chyba że niniejsze rozporządzenie stanowi inaczej.

[73] Dz.U. L 56 z 4.3.1968, s. 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj.

2. Wymagana jest większość dwóch trzecich członków Zarządu posiadających prawo głosu w przypadku:

   a) przyjęcie jednolitego dokumentu programowego, o którym mowa w art. 28 ust. 1 lit. c);

   b) przyjęcie rocznego budżetu, o którym mowa w art. 28 ust. 1 lit. e);

   c) mianowanie, przedłużenie kadencji lub odwołanie dyrektora wykonawczego i zastępcy dyrektora wykonawczego, o których mowa w art. 31 i 33;

   d) mianowanie i odwołanie członków komisji odwoławczej, o której mowa w art. 36.

3. Decyzje dotyczące kwestii budżetowych lub zasobów ludzkich, w szczególności kwestii, o których mowa w art. 28 ust. 1 lit. c), e), f), g), h), i), k), l), m) i n), są przyjmowane wyłącznie w przypadku pozytywnego głosowania przedstawicieli Komisji. Do celów przyjęcia decyzji, o których mowa w art. 28 ust. 1 lit. c), dotyczących jednolitego dokumentu programowego ENISA, pozytywny głos przedstawiciela Komisji jest wymagany wyłącznie w odniesieniu do elementów decyzji niezwiązanych z rocznym i wieloletnim programem prac ENISA.

4. Każdy członek posiadający prawo głosu ma jeden głos. W przypadku nieobecności członka posiadającego prawo głosu jego zastępca jest uprawniony do wykonywania prawa głosu członka.

5. Przewodniczący zarządu bierze udział w głosowaniu.

6. Dyrektor wykonawczy nie bierze udziału w głosowaniu.

7. Regulamin zarządu określa bardziej szczegółowe zasady głosowania, w szczególności okoliczności, w których członek może działać w imieniu innego członka.

Sekcja 2
Zarząd

Artykuł 30
Zarząd

1. Zarządowi pomaga Rada Wykonawcza.

2. Rada Wykonawcza:

   (a) przygotowuje decyzje, które mają być przyjęte przez zarząd;

   b) wspólnie z zarządem zapewnia odpowiednie działania następcze w związku z ustaleniami i zaleceniami wynikającymi z wewnętrznych lub zewnętrznych sprawozdań z audytu i ocen, a także z dochodzeń prowadzonych przez OLAF i EPPO;

   c) bez uszczerbku dla obowiązków dyrektora wykonawczego określonych w art. 32, wspierać dyrektora wykonawczego i doradzać mu w zakresie wdrażania decyzji zarządu, mając na celu wzmocnienie nadzoru nad zarządzaniem administracyjnym i budżetowym.

3. W skład zarządu wykonawczego wchodzą: przewodniczący zarządu, jeden przedstawiciel Komisji w zarządzie oraz trzech innych członków mianowanych przez zarząd spośród jego członków posiadających prawo głosu. Przewodniczący zarządu pełni również funkcję przewodniczącego zarządu wykonawczego. Mianowanie

członków zarządu wykonawczego ma na celu zapewnienie równowagi płci w zarządzie wykonawczym. Dyrektor wykonawczy uczestniczy w posiedzeniach zarządu wykonawczego bez prawa głosu.

4. Kadencja członków Zarządu trwa cztery lata. Kadencja ta może być odnawiana. Kadencja członków Zarządu kończy się wraz z wygaśnięciem ich członkostwa w Radzie Zarządzającej.

5. Zarząd zbiera się co najmniej raz na trzy miesiące na zwyczajnym posiedzeniu. Ponadto zbiera się z inicjatywy przewodniczącego lub na wniosek członków.

6. Zarząd ustanawia regulamin wewnętrzny Rady Wykonawczej.

7. W razie konieczności ze względu na pilny charakter sprawy zarząd wykonawczy może podjąć w imieniu zarządu pewne decyzje tymczasowe, w szczególności w sprawach dotyczących zarządzania administracyjnego, w tym zawieszenia przekazania uprawnień organu powołującego oraz w sprawach budżetowych. Wszelkie takie decyzje tymczasowe są bez zbędnej zwłoki zgłaszane zarządowi. Zarząd podejmuje następnie decyzję o zatwierdzeniu lub odrzuceniu tymczasowej decyzji w terminie nieprzekraczającym trzech miesięcy od podjęcia tej decyzji. Zarząd wykonawczy nie podejmuje w imieniu zarządu decyzji, które wymagają zgody większości dwóch trzecich członków zarządu posiadających prawo głosu.

Sekcja 3
Dyrektor wykonawczy

Artykuł 31
Mianowanie, odwołanie i przedłużenie kadencji

1. Dyrektor wykonawczy jest mianowany przez zarząd na podstawie osiągnięć i umiejętności z listy kandydatów zaproponowanych przez Komisję, po przeprowadzeniu otwartej i przejrzystej procedury selekcyjnej.

2. Przed mianowaniem kandydat wybrany przez zarząd zostaje zaproszony do złożenia oświadczenia przed właściwą komisją Parlamentu Europejskiego i udzielenia odpowiedzi na pytania posłów.

3. Dyrektor wykonawczy zostaje zatrudniony jako pracownik tymczasowy ENISA na podstawie art. 2 lit. a) warunków zatrudnienia.

4. W celu zawarcia umowy z dyrektorem wykonawczym ENISA jest reprezentowana przez przewodniczącego zarządu.

5. Kadencja dyrektora wykonawczego trwa pięć lat. W odpowiednim terminie przed upływem tego okresu Komisja przeprowadza ocenę, uwzględniającą ocenę wyników pracy dyrektora wykonawczego oraz przyszłe zadania i wyzwania stojące przed ENISA.

6. Zarząd, działając na wniosek Komisji uwzględniający ocenę, o której mowa w ust. 5, może przedłużyć kadencję dyrektora wykonawczego jeden raz na okres nieprzekraczający pięciu lat.

7. Dyrektor wykonawczy, którego kadencja została przedłużona, nie może uczestniczyć w kolejnej procedurze selekcyjnej na to samo stanowisko po zakończeniu całego okresu.

8. Zarząd informuje Parlament Europejski o zamiarze przedłużenia kadencji dyrektora wykonawczego zgodnie z ust. 6. W ciągu trzech miesięcy przed takim przedłużeniem dyrektor wykonawczy, na zaproszenie, składa oświadczenie przed właściwą komisją Parlamentu Europejskiego i odpowiada na pytania posłów.

9. Dyrektor wykonawczy może zostać odwołany ze stanowiska wyłącznie na mocy decyzji zarządu podjętej na wniosek Komisji.

Artykuł 32
Zadania i obowiązki dyrektora wykonawczego

1. Dyrektor wykonawczy zarządza ENISA i odpowiada przed zarządem.

2. Dyrektor wykonawczy jest niezależny w wykonywaniu swoich zadań i nie zwraca się o instrukcje do żadnego rządu ani żadnego innego organu, ani też takich instrukcji nie przyjmuje.

3. Dyrektor wykonawczy składa sprawozdania z wykonywania swoich zadań przed Parlamentem Europejskim, gdy zostanie o to poproszony. Rada może poprosić dyrektora wykonawczego o złożenie sprawozdania z wykonywania swoich zadań.

4. Dyrektor wykonawczy jest prawnym przedstawicielem ENISA.

5. Dyrektor wykonawczy odpowiada za realizację zadań powierzonych ENISA na mocy niniejszego rozporządzenia. W szczególności dyrektor wykonawczy:

   a) zapewnia bieżące zarządzanie ENISA;

   b) wdraża decyzje przyjęte przez zarząd;

   c) zapewniać zgodność z przepisami finansowymi ENISA;

   d) przygotowywanie projektu jednolitego dokumentu programowego i przedkładanie go zarządowi do zatwierdzenia przed przekazaniem go Komisji do zaopiniowania;

   e) wdrażać jednolity dokument programowy i składać zarządowi sprawozdania z jego wdrażania;

   f) przygotowuje skonsolidowane roczne sprawozdanie z działalności ENISA, w tym z realizacji rocznego programu prac ENISA, i przedstawia je zarządowi do oceny i przyjęcia;

   g) przygotowanie planu działania będącego kontynuacją wniosków z retrospektywnych ocen ENISA, o których mowa w art. 121, oraz składanie Komisji co dwa lata sprawozdań z postępów;

   h) przygotować plan działania będący kontynuacją wniosków zawartych w sprawozdaniach z audytu wewnętrznego lub zewnętrznego oraz ocenach, a także w dochodzeniach OLAF-u i EPPO, oraz co dwa lata składać sprawozdania z postępów Komisji, a także regularnie zarządowi;

   i) przygotowywać projekt przepisów finansowych mających zastosowanie do ENISA, o których mowa w art. 50;

   j) przygotowywać projekt preliminarza dochodów i wydatków ENISA oraz wykonywać jej budżet;

   k) ochrona interesów finansowych Unii poprzez stosowanie środków zapobiegających nadużyciom finansowym, korupcji i wszelkim innym

nielegalnym działaniom, bez uszczerbku dla kompetencji dochodzeniowych OLAF-u i EPPO, poprzez skuteczne kontrole, a w przypadku wykrycia nieprawidłowości – poprzez odzyskiwanie nienależnie wypłaconych kwot oraz, w stosownych przypadkach, poprzez nakładanie skutecznych, proporcjonalnych i odstraszających sankcji administracyjnych i finansowych;

l) przygotowywanie strategii zwalczania nadużyć finansowych, strategii zwiększania wydajności i synergii, strategii współpracy z państwami trzecimi lub organizacjami międzynarodowymi oraz strategii zarządzania organizacyjnego i systemów kontroli wewnętrznej ENISA, a także przedstawianie jej zarządowi do zatwierdzenia;

m) rozwijanie i utrzymywanie kontaktów ze środowiskiem biznesowym i organizacjami konsumenckimi w celu zapewnienia regularnego dialogu z odpowiednimi zainteresowanymi stronami;

n) regularnie wymieniać poglądy i informacje z odpowiednimi podmiotami unijnymi na temat ich działań związanych z cyberbezpieczeństwem w celu zapewnienia spójności w realizacji polityki Unii w tej dziedzinie;

o) promowanie różnorodności i równowagi płci przy rekrutacji pracowników ENISA;

p) przyjmować europejskie systemy poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, o których mowa w art. 20 ust. 1;

q podejmowanie decyzji w sprawie wnioskodawców ubiegających się o status autoryzowanego dostawcy certyfikatów lub o przedłużenie ich autoryzacji, o których mowa w art. 22 ust. 3;

r wykonywać inne zadania powierzone dyrektorowi wykonawczemu na mocy niniejszego rozporządzenia.

6. W razie potrzeby i w ramach celów i zadań ENISA dyrektor wykonawczy może powołać grupy robocze ad hoc złożone z ekspertów, w tym ekspertów z właściwych organów państw członkowskich. Dyrektor wykonawczy informuje o tym z wyprzedzeniem zarząd. Procedury dotyczące w szczególności składu grup roboczych, mianowania ekspertów grup roboczych przez dyrektora wykonawczego oraz funkcjonowania grup roboczych określa się w wewnętrznych zasadach funkcjonowania ENISA.

7. W razie konieczności, w celu skutecznego i wydajnego wykonywania zadań ENISA oraz w oparciu o odpowiednią analizę kosztów i korzyści, dyrektor wykonawczy może podjąć decyzję o utworzeniu jednego lub kilku biur lokalnych w jednym lub kilku państwach członkowskich. Przed podjęciem decyzji o utworzeniu biura lokalnego dyrektor wykonawczy zasięga opinii zainteresowanych państw członkowskich, w tym państwa członkowskiego, w którym znajduje się siedziba ENISA, oraz uzyskuje uprzednią zgodę Komisji i zarządu. W przypadku braku porozumienia podczas procesu konsultacji między dyrektorem wykonawczym a zainteresowanymi państwami członkowskimi kwestia ta jest przedkładana Radzie do dyskusji. Łączna liczba pracowników we wszystkich biurach lokalnych jest ograniczona do minimum i nie przekracza 40 % całkowitej liczby pracowników ENISA zatrudnionych w państwie członkowskim, w którym znajduje się siedziba ENISA. Liczba pracowników w każdym biurze lokalnym nie przekracza 10 % całkowitej liczby pracowników ENISA zatrudnionych w państwie członkowskim, w którym znajduje się siedziba ENISA.

8. W decyzji o utworzeniu biura lokalnego określa się zakres działań, które mają być realizowane w biurze lokalnym, w sposób pozwalający uniknąć niepotrzebnych kosztów i powielania funkcji administracyjnych ENISA.

Sekcja 4
Zastępca dyrektora wykonawczego

Artykuł 33
Zastępca dyrektora wykonawczego

1. Zarząd może podjąć decyzję o utworzeniu stanowiska zastępcy dyrektora wykonawczego, który będzie wspierał dyrektora wykonawczego.
2. W przypadku podjęcia przez zarząd decyzji o utworzeniu stanowiska zastępcy dyrektora wykonawczego, do zastępcy dyrektora wykonawczego stosuje się odpowiednio przepisy art. 31.

Artykuł 34
Zadania i obowiązki zastępcy dyrektora wykonawczego

Zastępca dyrektora wykonawczego wspiera dyrektora wykonawczego w zarządzaniu ENISA i wykonywaniu zadań, o których mowa w art. 32. W przypadku nieobecności lub niezdolności do pracy dyrektora wykonawczego lub gdy stanowisko jest nieobsadzone, zastępca dyrektora wykonawczego pełni jego obowiązki w okresie nieobecności lub do czasu obsadzenia stanowiska.

Sekcja 5
Grupa doradcza ENISA

Artykuł 35
Grupa doradcza ENISA

1. Zarząd, działając na wniosek dyrektora wykonawczego, powołuje w sposób przejrzysty grupę doradczą ENISA. W skład grupy doradczej ENISA wchodzą uznani eksperci reprezentujący odpowiednie zainteresowane strony, takie jak branża cyberbezpieczeństwa, branża ICT, MŚP, podmioty działające w sektorach wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555, producenci produktów zawierających elementy cyfrowe oraz administratorzy oprogramowania open source w rozumieniu rozporządzenia (UE) 2024/2847, organów oceny zgodności notyfikowanych w ramach europejskich ram certyfikacji w zakresie cyberbezpieczeństwa, o których mowa w art. 93 i rozporządzeniu (UE) 2024/2847, podmiotów działających w obszarze środków identyfikacji elektronicznej, grup konsumentów, ekspertów akademickich w dziedzinie cyberbezpieczeństwa, europejskich organizacji normalizacyjnych, a także organów ścigania i organów nadzorujących ochronę danych. Ci uznani eksperci są obywatelami państw członkowskich. Zarząd dąży do zapewnienia odpowiedniej równowagi płci i równowagi geograficznej, a także równowagi między różnymi grupami zainteresowanych stron.
2. Procedury dotyczące grupy doradczej ENISA, w szczególności dotyczące jej składu, wniosku dyrektora wykonawczego, o którym mowa w ust. 1, liczby i mianowania jej

członków oraz funkcjonowania grupy doradczej ENISA, określa się w wewnętrznych zasadach funkcjonowania ENISA i podaje do wiadomości publicznej.

3. Grupie doradczej ENISA przewodniczy dyrektor wykonawczy lub osoba wyznaczona przez dyrektora wykonawczego w poszczególnych przypadkach.

4. Kadencja członków grupy doradczej ENISA trwa dwa i pół roku i może zostać przedłużona jeden raz. Członkowie zarządu nie mogą być członkami grupy doradczej ENISA. Eksperci z Komisji i eksperci z państw członkowskich mają prawo uczestniczyć w posiedzeniach grupy doradczej ENISA i brać udział w jej pracach. Dyrektor wykonawczy może zaprosić przedstawicieli innych organów, które nie są członkami grupy doradczej ENISA, do udziału w posiedzeniach grupy doradczej ENISA i do udziału w jej pracach.

5. Grupa doradcza ENISA doradza ENISA w zakresie wykonywania zadań ENISA, z wyjątkiem stosowania przepisów tytułów III, IV i V niniejszego rozporządzenia. W szczególności doradza dyrektorowi wykonawczemu w sprawie sporządzenia wniosku dotyczącego rocznego programu prac ENISA oraz w sprawie zapewnienia komunikacji z odpowiednimi zainteresowanymi stronami w kwestiach związanych z rocznym programem prac.

6. Grupa doradcza ENISA regularnie informuje zarząd o swoich działaniach.

7. ENISA zapewnia wsparcie logistyczne niezbędne dla grupy doradczej ENISA oraz sekretariat na potrzeby jej posiedzeń.

Sekcja 6
Komisja odwoławcza

Artykuł 36
Utworzenie i skład komisji odwoławczej

1. ENISA powołuje komisję odwoławczą na mocy decyzji zarządu.

2. Komisja Odwoławcza składa się z przewodniczącego i trzech innych członków. Każdy członek Komisji Odwoławczej ma zastępcę. Zastępca reprezentuje członka w przypadku jego nieobecności.

3. Zarząd mianuje przewodniczącego, pozostałych członków i ich zastępców z listy wykwalifikowanych kandydatów sporządzonej przez Komisję. Lista wykwalifikowanych kandydatów jest ważna przez cztery lata. Zarząd może przedłużyć ważność tej listy na kolejne czteroletnie okresy na wniosek Komisji.

4. Jeżeli Komisja Odwoławcza uzna, że wymaga tego charakter odwołania, może zwrócić się do zarządu o powołanie dwóch dodatkowych członków i ich zastępców z listy, o której mowa w ust. 3.

5. Komisja odwoławcza przyjmuje i podaje do wiadomości publicznej swój regulamin wewnętrzny.

Artykuł 37
Członkowie komisji odwoławczej

1. Kadencja członków i zastępców członków Komisji Odwoławczej trwa cztery lata. Kadencja ta może zostać przedłużona przez zarząd na kolejne cztery lata na wniosek Komisji.

2. Członkowie komisji odwoławczej są niezależni i nie pełnią żadnych innych funkcji w ENISA. Podejmując decyzje, nie zwracają się o instrukcje do żadnego rządu, innego organu ani podmiotu prywatnego ani nie przyjmują takich instrukcji.

3. Członkowie Komisji Odwoławczej nie mogą zostać odwołani ze stanowiska ani usunięci z listy wykwalifikowanych kandydatów w trakcie trwania ich kadencji, chyba że istnieją poważne powody takiego odwołania lub usunięcia, a zarząd podejmuje taką decyzję na wniosek Komisji.

Artykuł 38
Wyłączenie i sprzeciw

1. Członkowie komisji odwoławczej nie mogą brać udziału w postępowaniu odwoławczym, jeżeli mają osobisty interes w postępowaniu, jeżeli wcześniej byli zaangażowani jako przedstawiciele jednej ze stron postępowania lub jeżeli brali udział w podjęciu decyzji będącej przedmiotem odwołania.

2. Jeżeli z jednego z powodów wymienionych w ust. 1 lub z jakiegokolwiek innego powodu członek komisji odwoławczej uzna, że nie powinien brać udziału w postępowaniu odwoławczym, informuje o tym komisję odwoławczą.

3. Strona postępowania odwoławczego może zgłosić sprzeciw wobec dowolnego członka Izby Odwoławczej z dowolnej przyczyny wymienionej w ust. 1 lub w przypadku podejrzenia o stronniczość tego członka. Sprzeciw taki nie jest dopuszczalny, jeżeli strona postępowania odwoławczego, mając świadomość przyczyny sprzeciwu, podjęła czynności proceduralne. Sprzeciw nie może być oparty na narodowości członków Izby Odwoławczej.

4. Komisja Odwoławcza podejmuje decyzję w sprawie działań, które należy podjąć w przypadkach określonych w ust. 2 i 3, bez udziału danego członka. W celu podjęcia tej decyzji członek, którego dotyczy sprzeciw, zostaje zastąpiony w Komisji Odwoławczej przez swojego zastępcę.

Artykuł 39
Odwołania od decyzji i zaniechań

1. Odwołanie do komisji odwoławczej można wnieść od:

   a) decyzje przyjęte przez ENISA zgodnie z art. 22 ust. 3;

   b) niepodjęcie przez ENISA działań w terminie określonym w art. 22 ust. 4.

2. Odwołanie wniesione zgodnie z ust. 1 podlega kontroli międzyinstancyjnej zgodnie z art. 41 przed przekazaniem go do rozpatrzenia przez komisję odwoławczą.

3 Odwołanie wniesione zgodnie z ust. 1 nie ma skutku zawieszającego.

Artykuł 40
Osoby uprawnione do wniesienia odwołania, termin i forma

1. Wnioskodawcy w rozumieniu art. 21 ust. 3 mogą wnieść odwołanie od

   a) decyzji ENISA skierowanej do nich zgodnie z art. 22 ust. 3;

   b) zaniechania działania przez ENISA w odniesieniu do wniosku złożonego przez nich do ENISA w terminie określonym w art. 22 ust. 4.

2. W przypadku, o którym mowa w ust. 1 lit. a), odwołanie wraz z uzasadnieniem składa się na piśmie zgodnie z regulaminem wewnętrznym, o którym mowa w art. 36 ust. 5, w terminie dwóch miesięcy od powiadomienia zainteresowanego wnioskodawcy o decyzji lub, w przypadku braku takiego powiadomienia, od dnia, w którym wnioskodawca dowiedział się o decyzji.

3. W przypadku, o którym mowa w ust. 1 lit. b), odwołanie składa się do ENISA na piśmie zgodnie z zasadami postępowania, o których mowa w art. 36 ust. 5, w terminie dwóch miesięcy od dnia upływu terminu określonego w art. 22 ust. 4.

Artykuł 41
Kontrola międzyinstancyjna

1. Jeżeli ENISA uzna odwołanie za dopuszczalne i zasadne, koryguje decyzję lub zaniechanie działania, o których mowa w art. 40 ust. 1.

2. Jeżeli ENISA nie zmieni decyzji w ciągu miesiąca od otrzymania odwołania, niezwłocznie podejmuje decyzję o zawieszeniu wykonania swojej decyzji i przekazuje odwołanie do komisji odwoławczej.

Artykuł 42
Rozpatrywanie decyzji w sprawie odwołań

1. Komisja odwoławcza podejmuje decyzję w sprawie uwzględnienia lub odrzucenia odwołania w terminie trzech miesięcy od jego wniesienia. Rozpatrując odwołanie, komisja odwoławcza działa w terminach określonych w jej regulaminie. W razie potrzeby wzywa strony postępowania odwoławczego do przedstawienia w określonych terminach uwag dotyczących jej zawiadomień lub komunikatów innych stron postępowania odwoławczego przed Komisją Odwoławczą ds. Ochrony Środowiska ( ). Strony postępowania odwoławczego mają prawo do składania ustnych oświadczeń.

2. Jeżeli komisja odwoławcza uzna, że podstawy odwołania są uzasadnione, przekazuje sprawę do ENISA. ENISA podejmuje ostateczną decyzję zgodnie z ustaleniami komisji odwoławczej i przedstawia uzasadnienie tej decyzji. ENISA informuje o tym strony postępowania odwoławczego.

Artykuł 43
Skargi do Trybunału Sprawiedliwości Unii Europejskiej

1. Skargi o unieważnienie decyzji ENISA przyjętych zgodnie z art. 22 ust. 3 lub skargi dotyczące niewzięcia działań w odpowiednim terminie zgodnie z art. 22 ust. 4 mogą być wnoszone do Trybunału Sprawiedliwości Unii Europejskiej po wyczerpaniu procedury odwoławczej w ramach ENISA określonej w art. 39–42 lub w przypadku niewzięcia działań w odpowiednim terminie zgodnie z art. 41ust. 2.

2. ENISA podejmuje wszelkie niezbędne środki w celu wykonania wyroku Trybunału Sprawiedliwości Unii Europejskiej.

Sekcja 7
Działalność

Artykuł 44
Jednolity dokument programowy

1. ENISA działa zgodnie z jednolitym dokumentem programowym zawierającym jej roczny i wieloletni program prac, który obejmuje wszystkie planowane działania.

2. Każdego roku dyrektor wykonawczy sporządza projekt jednolitego dokumentu programowego, o którym mowa w ust. 1, wraz z odpowiednim planem zasobów finansowych i ludzkich zgodnie z art. 32 rozporządzenia delegowanego Komisji (UE) 2019/715[74] oraz z uwzględnieniem wytycznych określonych przez Komisję.

3. Do dnia 30 listopada każdego roku zarząd przyjmuje jednolity dokument programowy, o którym mowa w ust. 1, uwzględniając opinię Komisji, o której mowa w art. 32 ust. 7 rozporządzenia delegowanego (UE) 2019/715. Jeżeli zarząd postanowi nie uwzględnić niektórych elementów opinii Komisji, przedstawia szczegółowe uzasadnienie tej decyzji. Zarząd przekazuje jednolity dokument programowy Parlamentowi Europejskiemu, Radzie i Komisji do dnia 31 stycznia następnego roku, a także wszelkie późniejsze aktualizacje tego dokumentu.

4. Jednolity dokument programowy staje się ostateczny po ostatecznym przyjęciu budżetu ogólnego Unii i jest w razie potrzeby dostosowywany.

5. Roczny program prac zawiera szczegółowe cele i oczekiwane wyniki, w tym wskaźniki wykonania. Zawiera on również opis działań, które mają być finansowane, oraz wskazanie zasobów finansowych i ludzkich przydzielonych na każde działanie, zgodnie z zasadami budżetowania i zarządzania zadaniowego. Roczny program prac jest spójny z wieloletnim programem prac, o którym mowa w ust. 7. Wskazuje on wyraźnie zadania, które zostały dodane, zmienione lub usunięte w porównaniu z poprzednim rokiem budżetowym.

6. Zarząd zmienia przyjęty roczny program pracy, gdy ENISA otrzymuje nowe zadanie. Wszelkie istotne zmiany w rocznym programie pracy przyjmuje się w tej samej procedurze, co w przypadku pierwotnego rocznego programu pracy. Zarząd może przekazać dyrektorowi wykonawczemu uprawnienia do wprowadzania nieistotnych zmian w rocznym programie pracy.

7. Wieloletni program pracy określa ogólne programowanie strategiczne, w tym cele, oczekiwane wyniki i wskaźniki wykonania. Określa on również programowanie zasobów, w tym wieloletni budżet i personel.

8. Programowanie zasobów jest aktualizowane co roku. Programowanie strategiczne jest aktualizowane w stosownych przypadkach, a w szczególności wtedy, gdy jest to konieczne w celu uwzględnienia wyników oceny, o której mowa w art. 120.

---

[74] Rozporządzenie delegowane Komisji (UE) 2019/715 z dnia 18 grudnia 2018 r. w sprawie ramowego rozporządzenia finansowego dla organów utworzonych na mocy TFUE i traktatu Euratom, o których mowa w art. 70 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 (Dz.U. L 122 z 10.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj).

ROZDZIAŁ IV
Ustanowienie i struktura budżetu ENISA

Artykuł 45
Ustanowienie budżetu ENISA

1 Każdego roku dyrektor wykonawczy sporządza wstępny projekt preliminarza dochodów i wydatków ENISA na następny rok budżetowy, w tym plan zatrudnienia, i przekazuje go zarządowi.

2. Wstępny projekt preliminarza opiera się na celach i oczekiwanych wynikach rocznego programu prac oraz uwzględnia środki finansowe niezbędne do osiągnięcia tych celów i oczekiwanych wyników, zgodnie z zasadą należytego zarządzania finansami i wydajności.

3. Na podstawie wstępnego projektu preliminarza zarząd przyjmuje projekt preliminarza dochodów i wydatków ENISA na następny rok budżetowy i przesyła go Komisji do dnia 31 stycznia każdego roku.

4. Komisja przesyła projekt preliminarza władzy budżetowej wraz z projektem budżetu ogólnego Unii. Projekt preliminarza udostępnia się również ENISA.

5. Na podstawie projektu preliminarza Komisja wpisuje do projektu budżetu ogólnego Unii preliminarz, który uznaje za niezbędny dla planu zatrudnienia, oraz kwotę wkładu, który ma zostać pokryty z budżetu ogólnego Unii, i przedkłada je władzy budżetowej zgodnie z art. 313 i 314 TFUE.

6. Władza budżetowa zatwierdza środki na wkład z budżetu ogólnego Unii na rzecz ENISA.

7. Władza budżetowa przyjmuje plan zatrudnienia ENISA.

8. Zarząd przyjmuje budżet ENISA. Budżet ten staje się ostateczny po ostatecznym przyjęciu budżetu ogólnego Unii i w razie potrzeby jest odpowiednio dostosowywany.

9. W przypadku każdego projektu budowlanego, który może mieć istotny wpływ na budżet ENISA, stosuje się rozporządzenie delegowane (UE) 2019/715.

Artykuł 46
Struktura budżetu ENISA

1. Szacunki wszystkich dochodów i wydatków ENISA są przygotowywane w każdym roku budżetowym i wykazywane w budżecie ENISA. Rok budżetowy odpowiada rokowi kalendarzowemu.

2. Budżet ENISA jest zrównoważony pod względem dochodów i wydatków.

3. Bez uszczerbku dla innych zasobów, dochody ENISA składają się z:

   a) wkładu Unii wpisanego do budżetu ogólnego Unii;

   b) dochodów przeznaczonych na określone pozycje wydatków zgodnie z przepisami finansowymi, o których mowa w art. 50;

   c) finansowanie unijne w formie umów o wkładzie lub dotacji *ad hoc* zgodnie z przepisami finansowymi ENISA, o których mowa w art. 50, oraz z przepisami odpowiednich instrumentów wspierających polityki Unii;

d opłaty pobierane od wnioskodawców za działania związane z europejskimi systemami potwierdzania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, o których mowa w art. 22 ust. 1;

e) opłaty pobierane od organów oceny zgodności za udział w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa, o którym mowa w art. 47 ust. 2, oraz za wydawanie europejskich certyfikatów w zakresie cyberbezpieczeństwa w ramach tego systemu;

f) opłaty pobierane od organów publicznych lub podmiotów prywatnych za testowanie narzędzi, o których mowa w art. 47 ust. 3;

g wszelkie wkłady państw trzecich uczestniczących w pracach ENISA, zgodnie z art. 70 ust. 4;

h) wszelkie dobrowolne wkłady państw członkowskich w formie pieniężnej lub rzeczowej.

4. Państwa członkowskie, które przekazują dobrowolne wkłady, o których mowa w ust. 3 lit. g), nie mogą w związku z tym dochodzić żadnych szczególnych praw ani usług.

5 Wydatki ENISA obejmują wynagrodzenia pracowników, koszty administracyjne i infrastrukturalne oraz wydatki operacyjne.

Artykuł 47
Opłaty

1 W odniesieniu do każdego europejskiego systemu certyfikacji, o którym mowa w art. 22 ust. 1, od wnioskodawców w rozumieniu art. 21 ust. 3 lub od uprawnionych dostawców usług certyfikacyjnych pobiera się następujące opłaty w celu pokrycia pełnych kosztów działań wykonywanych przez ENISA:

a) wydawanie zezwoleń po zbadaniu wymogów określonych w art. 21 ust. 3 i 4, w tym przeprowadzanie ocen;

b) coroczne utrzymywanie zezwolenia;

(c) odnawianie upoważnień dla podmiotów wydających europejskie indywidualne certyfikaty umiejętności w zakresie cyberbezpieczeństwa, w tym przeprowadzanie ocen.

2. W odniesieniu do certyfikacji na organy oceny zgodności nakłada się następujące opłaty za utrzymanie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, w ramach których wydawane są europejskie certyfikaty cyberbezpieczeństwa, w szczególności:

a) opłata roczna za udział w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa;

b) opłata za wydawanie europejskich certyfikatów cyberbezpieczeństwa w ramach europejskich systemów certyfikacji cyberbezpieczeństwa.

Opłaty, o których mowa w lit. b), są pobierane, gdy jednostka oceniająca zgodność przedkłada europejskie certyfikaty cyberbezpieczeństwa do ENISA w celu opublikowania ich na stronie internetowej zgodnie z art. 79.

3. W odniesieniu do narzędzi testowych, o których mowa w art. 15 ust. 1, od każdego organu publicznego lub podmiotu prywatnego pobiera się opłatę za ich użytkowanie.

4. Opłaty są wyrażane i płatne w euro.

5. Komisja przyjmuje akty wykonawcze ustanawiające szczegółowe zasady dotyczące ustalania opłat pobieranych przez ENISA, określające w szczególności szacunkowe koszty związane z każdą z kwestii, za które pobierane są opłaty zgodnie z ust. 1, 2 i 3, oraz indywidualne kwoty opłat, a także sposoby i warunki uiszczania opłat. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2. Przygotowując projekty tych aktów wykonawczych, Komisja konsultuje się z ENISA.

6. Opłaty określone w aktach wykonawczych, o których mowa w ust. 5, są ustalane z wyprzedzeniem, proporcjonalnie do szacowanych kosztów przeprowadzonych działań lub świadczonych usług, określonych w sposób efektywny pod względem kosztów, i są wystarczające do pokrycia tych kosztów. Wszystkie wydatki ENISA związane z personelem zaangażowanym w działania, o których mowa w ust. 1, 2 i 3, są uwzględniane w kosztach do pokrycia. Opłaty ustala się na takim poziomie, aby uniknąć deficytu lub znacznego nagromadzenia nadwyżki w budżecie ENISA. Nadwyżki budżetowe uzyskane dzięki opłatom przenosi się na finansowanie działań ENISA, w szczególności przyszłych działań związanych z opłatami, lub kompensuje się nimi poniesione straty. Jeżeli znaczne dodatnie saldo budżetu wynikające z działań objętych opłatami staje się powtarzalne lub jeżeli świadczenie usług objętych opłatami powoduje znaczne ujemne saldo, Komisja zmienia akty wykonawcze, o których mowa w ust. 5, w celu zmiany metody obliczania opłat zgodnie z art. 118 ust. 2.

   Wysokość opłat za zadania, o których mowa w ust. 1, ustala się na takim poziomie, aby zapewnić, że dochody z tego tytułu w wystarczającym stopniu pokrywają koszty działań związanych z opracowywaniem i utrzymywaniem europejskich systemów indywidualnych poświadczeń, rozpatrywaniem wniosków oraz wydawaniem i odnawianiem zezwoleń, a także niezbędnych działań nadzorczych ENISA.

   Wysokość opłat za zadania, o których mowa w ust. 2, ustala się na takim poziomie, aby zapewnić, że dochody z tego tytułu w wystarczającym stopniu pokrywają pełne koszty działań związanych z utrzymaniem europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, określonych w art. 75.

   Wysokość opłat za zadania, o których mowa w ust. 3, ustala się na takim poziomie, aby zapewnić, że dochody z tego tytułu w wystarczającym stopniu pokrywają koszty działań związanych z udostępnianiem narzędzi testowych określonych w art. 15 ust. 1.

7. ENISA przedstawia sprawozdanie dotyczące pobranych opłat i ich wpływu na jej budżet w ramach procedury przedstawiania sprawozdań finansowych określonej w art. 50.

8. ENISA ustanawia zestaw wskaźników służących do pomiaru nakładu pracy, skuteczności i efektywności w odniesieniu do działań finansowanych z opłat. ENISA dostosowuje odpowiednio planowanie zatrudnienia i zarządzanie zasobami związanymi z opłatami, aby móc odpowiednio reagować na takie zapotrzebowanie i wszelkie wahania przychodów z opłat. ENISA przekazuje sprawozdanie Komisji, która może je wykorzystać do celów oceny, o której mowa w art. 120 ust. 1.

Artykuł 48
Wykonanie budżetu ENISA

1. Dyrektor wykonawczy jest odpowiedzialny za wykonanie budżetu ENISA i pełni funkcję urzędnika zatwierdzającego.

2. Audytor wewnętrzny Komisji wykonuje w odniesieniu do ENISA te same uprawnienia, jakie przysługują mu w odniesieniu do służb Komisji.

3. Każdego roku dyrektor wykonawczy przesyła władzy budżetowej wszystkie informacje istotne dla wyników procedur oceny.

Artykuł 49
Przedstawianie sprawozdań finansowych i udzielanie absolutorium

1. Księgowy ENISA przesyła tymczasowe sprawozdanie finansowe za dany rok budżetowy (rok N) księgowemu Komisji i Trybunałowi Obrachunkowemu do dnia 1 marca następnego roku budżetowego (rok N + 1).

2. Księgowy ENISA przekazuje również księgowemu Komisji wymagane informacje księgowe do celów konsolidacji, w sposób i formacie wymaganym przez tego ostatniego, do dnia 1 marca roku N + 1.

3. ENISA przesyła sprawozdanie z zarządzania budżetem i finansami za rok N do Parlamentu Europejskiego, Rady, Komisji i Trybunału Obrachunkowego do dnia 31 marca roku N + 1.

4. Po otrzymaniu uwag Trybunału Obrachunkowego dotyczących tymczasowego sprawozdania finansowego ENISA za rok N księgowy ENISA sporządza ostateczne sprawozdanie finansowe ENISA na własną odpowiedzialność. Dyrektor wykonawczy przedkłada je zarządowi do zaopiniowania.

5. Zarząd wydaje opinię na temat ostatecznego sprawozdania finansowego ENISA za rok N.

6. Księgowy ENISA przesyła do dnia 1 lipca roku N + 1 ostateczne sprawozdanie finansowe za rok N do Parlamentu Europejskiego, Rady, Komisji i Trybunału Obrachunkowego wraz z opinią zarządu.

7. Link do stron internetowych zawierających ostateczne sprawozdanie finansowe ENISA publikuje się w Dzienniku Urzędowym Unii Europejskiej do dnia 15 listopada roku N + 1.

8. Dyrektor wykonawczy przesyła Trybunałowi Obrachunkowemu do dnia 30 września roku N + 1 odpowiedź na uwagi zawarte w jego sprawozdaniu rocznym. Dyrektor wykonawczy przesyła tę odpowiedź również zarządowi i Komisji.

9. Dyrektor wykonawczy przedkłada Parlamentowi Europejskiemu, na jego wniosek, wszelkie informacje niezbędne do sprawnego przeprowadzenia procedury udzielania absolutorium za rok N, zgodnie z art. 267 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 2024/2509.

10. Na zalecenie Rady, stanowiącej większością kwalifikowaną, Parlament Europejski przed dniem 15 maja roku N + 2 udziela dyrektorowi wykonawczemu absolutorium z wykonania budżetu za rok N.

Artykuł 50
Przepisy finansowe

1. Przepisy finansowe mające zastosowanie do ENISA są przyjmowane przez zarząd po konsultacji z Komisją. Nie mogą one odbiegać od rozporządzenia delegowanego (UE) 2019/715, chyba że takie odstępstwo jest wyraźnie wymagane do funkcjonowania ENISA, a Komisja wyraziła na to uprzednią zgodę.

2. ENISA ustanawia i wykonuje swój budżet zgodnie ze swoimi przepisami finansowymi i rozporządzeniem (UE, Euratom) 2024/2509.

Artykuł 51
Zwalczanie nadużyć finansowych

1. W celu zwalczania nadużyć finansowych, korupcji i innych nielegalnych działań przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013[75] mają zastosowanie bez ograniczeń do działalności ENISA.

2 ENISA przystępuje do porozumienia międzyinstytucjonalnego z dnia 25 maja 1999 r. między Parlamentem Europejskim, Radą Unii Europejskiej i Komisją Wspólnot Europejskich dotyczącego dochodzeń wewnętrznych prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF)[76] w ciągu sześciu miesięcy od *[OP proszę wstawić dokładną datę, o której mowa w art. 127]* oraz przyjmuje odpowiednie przepisy mające zastosowanie do jej pracowników, korzystając z wzoru określonego w załączniku do tego porozumienia.

3. Trybunał Obrachunkowy ma prawo do kontroli, na podstawie dokumentów i kontroli na miejscu, wszystkich beneficjentów dotacji, wykonawców i podwykonawców, którzy otrzymali środki unijne od ENISA.

4. OLAF może prowadzić dochodzenia, w tym kontrole na miejscu i inspekcje, w celu ustalenia, czy doszło do nadużyć finansowych, korupcji lub jakiejkolwiek innej nielegalnej działalności mającej wpływ na interesy finansowe Unii w związku z dotacją lub umową finansowaną przez ENISA, zgodnie z przepisami i procedurami określonymi w rozporządzeniu (UE, Euratom) nr 883/2013 oraz rozporządzeniu Rady (Euratom, WE) nr 2185/96[77] .

5. Bez uszczerbku dla ust. 1–4, umowy robocze z państwami trzecimi i organizacjami międzynarodowymi, umowy, umowy o udzielenie dotacji i decyzje o udzieleniu dotacji ENISA zawierają postanowienia wyraźnie upoważniające Trybunał Obrachunkowy i OLAF do przeprowadzania takich kontroli i dochodzeń, zgodnie z ich odpowiednimi kompetencjami.

6. Zgodnie z rozporządzeniem Rady (UE) 2017/1939 EPPO może prowadzić dochodzenia i ścigać nadużycia finansowe i inne nielegalne działania naruszające

---

75 Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. w sprawie dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz uchylające rozporządzenie (WE) nr 1073/1999 Parlamentu Europejskiego i Rady oraz rozporządzenie Rady (Euratom) nr 1074/1999 (Dz.U. L 248 z 18.9.2013, s. 1, ELI: http://data.europa.eu/eli/reg/2013/883/oj).

76 Dz.U. L 136 z 31.5.1999, s. 15, ELI: http://data.europa.eu/eli/agree_interinstit/1999/531/oj.

77 Rozporządzenie Rady (Euratom, WE) nr 2185/96 z dnia 11 listopada 1996 r. w sprawie kontroli na miejscu oraz inspekcji przeprowadzanych przez Komisję w celu ochrony interesów finansowych Wspólnot Europejskich przed nadużyciami finansowymi i innymi nieprawidłowościami (Dz.U. L 292 z 15.11.1996, s. 2, ELI: http://data.europa.eu/eli/reg/1996/2185/oj).

interesy finansowe Unii, zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2017/1371[78] .

Artykuł 52
Oświadczenie o interesach

1. Członkowie zarządu, dyrektor wykonawczy, zastępca dyrektora wykonawczego oraz urzędnicy oddelegowani tymczasowo przez państwa członkowskie składają oświadczenie o zobowiązaniach oraz oświadczenie wskazujące na brak lub obecność jakichkolwiek bezpośrednich lub pośrednich interesów, które mogłyby zostać uznane za szkodliwe dla ich niezależności. Oświadczenia te są dokładne i kompletne, składane są corocznie na piśmie i aktualizowane w razie potrzeby.
2. Członkowie zarządu, dyrektor wykonawczy, zastępca dyrektora wykonawczego oraz eksperci zewnętrzni uczestniczący w pracach grup roboczych *ad hoc* składają najpóźniej na początku każdego posiedzenia dokładne i kompletne oświadczenie o wszelkich interesach, które mogłyby zostać uznane za szkodliwe dla ich niezależności w odniesieniu do punktów porządku obrad, oraz wstrzymują się od udziału w dyskusji i głosowaniu nad tymi punktami.
3. ENISA określa w swoim wewnętrznym regulaminie praktyczne zasady stosowania przepisów dotyczących oświadczeń o interesach, o których mowa w ust. 1 i 2.

Artykuł 53
Przejrzystość

1. ENISA wykonuje swoje zadania z zachowaniem wysokiego poziomu przejrzystości i zgodnie z art. 55.
2 ENISA zapewnia społeczeństwu i zainteresowanym stronom odpowiednie, obiektywne, wiarygodne i łatwo dostępne informacje, w szczególności dotyczące wyników swojej pracy. Udostępnia również publicznie oświadczenia o braku konfliktu interesów sporządzone zgodnie z art. 52.
3. Zarząd, działając na wniosek dyrektora wykonawczego, może upoważnić zainteresowane strony do obserwowania przebiegu niektórych działań ENISA.
4. ENISA określa w swoim wewnętrznym regulaminie praktyczne zasady wdrażania zasad przejrzystości, o których mowa w ust. 1 i 2.

Artykuł 54
Poufność w ramach ENISA

1. Bez uszczerbku dla art. 55 ENISA nie ujawnia osobom trzecim informacji, które przetwarza lub otrzymuje, w odniesieniu do których złożono uzasadniony wniosek o zachowanie poufności.
2. Członkowie zarządu, dyrektor wykonawczy, zastępca dyrektora wykonawczego, członkowie grupy doradczej ENISA, eksperci zewnętrzni uczestniczący w grupach roboczych *ad hoc* oraz pracownicy ENISA, w tym urzędnicy oddelegowani tymczasowo przez państwa członkowskie, są zobowiązani do przestrzegania

[78] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1371 z dnia 5 lipca 2017 r. w sprawie zwalczania nadużyć finansowych na szkodę interesów finansowych Unii za pomocą środków prawa karnego (Dz.U. L 198 z 28.7.2017, s. 29, ELI: http://data.europa.eu/eli/dir/2017/1371/oj).

wymogów dotyczących poufności określonych w art. 339 TFUE, nawet po zakończeniu pełnienia swoich funkcji.

3. ENISA określa w swoim wewnętrznym regulaminie praktyczne zasady stosowania przepisów dotyczących poufności, o których mowa w ust. 1 i 2.

Artykuł 55
Dostęp do dokumentów

1. Rozporządzenie (WE) nr 1049/2001 ma zastosowanie do dokumentów będących w posiadaniu ENISA.

2 Zarząd przyjmuje przepisy wykonawcze do rozporządzenia (WE) nr 1049/2001.

3. Od decyzji podjętych przez ENISA na podstawie art. 8 rozporządzenia (WE) nr 1049/2001 przysługuje skarga do Europejskiego Rzecznika Praw Obywatelskich na podstawie art. 228 TFUE lub skarga do Trybunału Sprawiedliwości Unii Europejskiej na podstawie art. 263 TFUE.

ROZDZIAŁ V
Pracownicy i oficerowie łącznikowi

Artykuł 56
Przepisy ogólne

1. Do personelu ENISA mają zastosowanie regulamin pracowniczy urzędników i warunki zatrudnienia innych pracowników oraz przepisy przyjęte w drodze porozumienia między instytucjami Unii w celu wykonania regulaminu pracowniczego urzędników i warunków zatrudnienia innych pracowników.

2. Pracownicy ENISA, oficerowie łącznikowi i oddelegowani do ENISA eksperci krajowi przechodzą odpowiednią procedurę sprawdzającą.

Artykuł 57
Przywileje i immunitety

Do ENISA i jej personelu stosuje się protokół nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej, załączony do TFUE.

Artykuł 58
Oficerowie łącznikowi

1. Każde państwo członkowskie wyznacza co najmniej dwóch oficerów łącznikowych z właściwego organu krajowego wyznaczonego zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555 jako oddelegowanych ekspertów krajowych do ENISA w celu pracy w jej siedzibie lub lokalnym biurze, zgodnie z art. 59 ust. 2. Komisja może również wyznaczyć oficera łącznikowego.

2 Funkcjonariusze łącznikowi przyczyniają się do wykonywania zadań ENISA, w tym poprzez ułatwianie współpracy operacyjnej i wymiany informacji, o których mowa w art. 11. Funkcjonariusze łącznikowi wspierają również ENISA w rozpowszechnianiu informacji o jej działaniach, ustaleniach i zaleceniach wśród odpowiednich zainteresowanych stron w całej Unii. Pełnią oni również rolę krajowych punktów kontaktowych w przypadku pytań pochodzących z ich państw członkowskich i

dotyczących ich państw członkowskich, odpowiadając na te pytania bezpośrednio lub współpracując z administracjami krajowymi.

3. Oficerowie łącznikowi wyznaczeni przez państwa członkowskie są uprawnieni do żądania i otrzymywania wszystkich istotnych informacji od swoich państw członkowskich, zgodnie z niniejszym rozporządzeniem, przy pełnym poszanowaniu prawa krajowego i praktyk państw członkowskich, w szczególności w odniesieniu do ochrony danych i poufności.

Artykuł 59
Oddelegowani eksperci krajowi i inni pracownicy

1. ENISA może korzystać z oddelegowanych ekspertów krajowych lub innego personelu niebędącego zatrudnionym przez ENISA we wszystkich obszarach swojej działalności. Regulamin pracowniczy i warunki zatrudnienia nie mają zastosowania do tego personelu.

2. Zarząd przyjmuje decyzję ustanawiającą zasady oddelegowywania ekspertów krajowych, w tym oficerów łącznikowych, do ENISA.

ROZDZIAŁ VI
PRZEPISY OGÓLNE DOTYCZĄCE ENISA

Artykuł 60
Status prawny ENISA

1. ENISA jest organem Unii posiadającym osobowość prawną.

2 W każdym państwie członkowskim ENISA posiada zdolność prawną w najszerszym zakresie przyznawanym osobom prawnym na mocy prawa krajowego tego państwa członkowskiego. Może ona w szczególności nabywać lub zbywać mienie ruchome i nieruchome oraz występować jako strona w postępowaniach sądowych.

3. ENISA jest reprezentowana przez dyrektora wykonawczego.

Artykuł 61
Siedziba

Siedziba ENISA znajduje się w Atenach, w Grecji.

Artykuł 62
Umowa w sprawie siedziby i warunki działalności

1. Niezbędne ustalenia dotyczące pomieszczeń, które mają zostać zapewnione ENISA w przyjmującym państwie członkowskim, oraz udogodnień, które mają zostać udostępnione przez to państwo członkowskie, wraz ze szczegółowymi zasadami mającymi zastosowanie w przyjmującym państwie członkowskim do dyrektora wykonawczego, członków zarządu, pracowników ENISA i członków ich rodzin, określa się w umowie w sprawie siedziby zawartej między ENISA a przyjmującym państwem członkowskim po uzyskaniu zgody zarządu.

2. Państwo członkowskie przyjmujące ENISA zapewnia najlepsze możliwe warunki dla prawidłowego funkcjonowania ENISA, biorąc pod uwagę dostępność lokalizacji, istnienie odpowiednich placówek edukacyjnych dla dzieci pracowników, odpowiedni

dostęp do rynku pracy, zabezpieczenie społeczne i opiekę medyczną zarówno dla dzieci, jak i małżonków pracowników.

Artykuł 63
Kontrola administracyjna

Działalność ENISA podlega nadzorowi Europejskiego Rzecznika Praw Obywatelskich zgodnie z art. 228 TFUE.

Artykuł 64
Odpowiedzialność ENISA

1. Odpowiedzialność umowna ENISA podlega prawu właściwemu dla danej umowy.
2. Trybunał Sprawiedliwości Unii Europejskiej jest właściwy do orzekania na podstawie klauzuli arbitrażowej zawartej w umowie zawartej przez ENISA.
3. W przypadku odpowiedzialności pozaumownej ENISA naprawia wszelkie szkody wyrządzone przez nią lub jej pracowników podczas wykonywania ich obowiązków, zgodnie z ogólnymi zasadami wspólnymi dla systemów prawnych państw członkowskich.
4. Trybunał Sprawiedliwości Unii Europejskiej jest właściwy do orzekania w sporach dotyczących odszkodowania za szkody, o których mowa w ust. 3.
5. Odpowiedzialność osobista pracowników ENISA wobec ENISA podlega przepisom określonym w regulaminie pracowniczym lub warunkach zatrudnienia mających do nich zastosowanie.

Artykuł 65
Ustalenia dotyczące języków

1. Do ENISA stosuje się rozporządzenie Rady nr 1[79] . Państwa członkowskie i inne organy wyznaczone przez państwa członkowskie mogą zwracać się do ENISA i otrzymywać odpowiedzi w wybranym przez siebie języku urzędowym instytucji Unii.
2. Tłumaczenia pisemne i wszelkie inne usługi językowe niezbędne do funkcjonowania ENISA, z wyjątkiem tłumaczeń ustnych, są świadczone przez Centrum Tłumaczeń dla Organów Unii Europejskiej.

Artykuł 66
Ochrona danych osobowych

1. Przetwarzanie danych osobowych przez ENISA podlega przepisom rozporządzenia (UE) 2018/1725.
2 Zarząd przyjmuje przepisy wykonawcze, o których mowa w art. 45 ust. 3 rozporządzenia (UE) 2018/1725. Zarząd może przyjąć dodatkowe środki niezbędne do stosowania rozporządzenia (UE) 2018/1725 przez ENISA.

[79] Rozporządzenie Rady nr 1 w sprawie określenia języków, które są używane przez Europejską Wspólnotę Gospodarczą (Dz.U. 17 z 6.10.1958, s. 385, ELI: http://data.europa.eu/eli/reg/1958/1(1)/oj).

Artykuł 67
Zasady bezpieczeństwa dotyczące ochrony informacji szczególnie chronionych nieobjętych klauzulą tajności oraz informacji niejawnych

W porozumieniu z Komisją ENISA przyjmuje zasady bezpieczeństwa stosujące zasady bezpieczeństwa zawarte w zasadach bezpieczeństwa Komisji dotyczących ochrony informacji niejawnych o charakterze poufnym i informacji niejawnych UE, określonych w decyzjach (UE, Euratom) 2015/443[80] i 2015/444[81] . Zasady bezpieczeństwa obejmują przepisy dotyczące wymiany, przetwarzania i przechowywania takich informacji.

Artykuł 68
Współpraca z podmiotami unijnymi i organami krajowymi

1. W celu zapewnienia spójności, tworzenia synergii i rozwiązywania problemów będących przedmiotem wspólnego zainteresowania ENISA współpracuje w sprawach związanych z cyberbezpieczeństwem z CERT-EU i odpowiednimi podmiotami Unii, w tym z Europolem, Europejskim Centrum Kompetencji w zakresie Przemysłu, Technologii i Badań w dziedzinie Cyberbezpieczeństwa ustanowionym na mocy rozporządzenia (UE) 2021/887 oraz Europejską Radą Ochrony Danych ustanowioną na mocy art. 68 ust. 1 rozporządzenia (UE) 2016/679.
2. Współpracę, o której mowa w ust. 1, można zapewnić poprzez:
   a) wymiany know-how i najlepszych praktyk;
   b) udzielania porad i wydawania wytycznych w sprawach związanych z cyberbezpieczeństwem;
   c) ustanowienie praktycznych ustaleń dotyczących wykonywania określonych zadań, po konsultacji z Komisją.
3. ENISA podejmuje zorganizowaną współpracę z CERT-EU, w szczególności w kwestiach związanych z budowaniem potencjału, współpracą operacyjną i długoterminowymi analizami strategicznymi zagrożeń cybernetycznych.
4. ENISA współpracuje i wymienia informacje z odpowiednimi organami nadzoru rynku i organami nadzorczymi wyznaczonymi na mocy przepisów unijnych w dziedzinie cyberbezpieczeństwa, w tym rozporządzenia (UE) 2024/2847.

Artykuł 69
Współpraca z zainteresowanymi stronami

1. W razie konieczności osiągnięcia celów niniejszego rozporządzenia ENISA współpracuje z odpowiednimi zainteresowanymi stronami, takimi jak sektor cyberbezpieczeństwa, sektor ICT, MŚP, podmioty działające w sektorach wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555, producenci, importerzy lub dystrybutorzy produktów zawierających elementy cyfrowe w rozumieniu rozporządzenia (UE) 2024/2847, organami oceny zgodności notyfikowanymi w ramach europejskich ram certyfikacji w zakresie cyberbezpieczeństwa i rozporządzenia (UE) 2024/2847, podmiotami działającymi w

[80] Decyzja Komisji (UE, Euratom) 2015/443 z dnia 13 marca 2015 r. w sprawie bezpieczeństwa w Komisji (Dz.U. L 72 z 17.3.2015, s. 41, ELI: http://data.europa.eu/eli/dec/2015/443/oj).

[81] Decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie zasad bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 72 z 17.3.2015, s. 53, ELI: http://data.europa.eu/eli/dec/2015/444/oj).

obszarze środków identyfikacji elektronicznej, grupami konsumentów oraz ekspertami akademickimi w dziedzinie cyberbezpieczeństwa. W tym celu ENISA może tworzyć partnerstwa publiczno-prywatne.

2. ENISA, w porozumieniu z Komisją, wspiera współpracę między notyfikowanymi organami oceny zgodności zgodnie z art. 93. W szczególności może ona utworzyć grupę notyfikowanych organów oceny zgodności w celu wymiany najlepszych praktyk, tworząc synergię z innymi odpowiednimi przepisami unijnymi, w szczególności z rozporządzeniem (UE) 2024/2847.

Artykuł 70
Współpraca z państwami trzecimi i organizacjami międzynarodowymi

1. W zakresie niezbędnym do osiągnięcia celów niniejszego rozporządzenia ENISA może współpracować z właściwymi organami państw trzecich lub organizacjami międzynarodowymi, lub z obiema tymi stronami, zgodnie z priorytetami Unii. W tym celu ENISA może ustanowić porozumienia robocze z organami państw trzecich i organizacjami międzynarodowymi, pod warunkiem uzyskania uprzedniej zgody Komisji. Porozumienia robocze nie powodują powstania zobowiązań prawnych ciążących na Unii i jej państwach członkowskich.

2. Zarząd przyjmuje strategię dotyczącą stosunków z państwami trzecimi i organizacjami międzynarodowymi w sprawach należących do kompetencji ENISA i zgodną z priorytetami, o których mowa w ust. 1. Komisja zapewnia, aby ENISA działała w ramach swojego mandatu i istniejących ram instytucjonalnych, zawierając odpowiednie porozumienia robocze z dyrektorem wykonawczym.

3. W celu wspierania współpracy z państwami trzecimi, w szczególności z państwami kandydującymi do przystąpienia do Unii, ENISA może dzielić się swoją wiedzą specjalistyczną w zakresie budowania potencjału, w szczególności w następujących obszarach:

   a) ocena poziomu dojrzałości zdolności i zasobów w zakresie cyberbezpieczeństwa;

   b) wzrost i wzmocnienie kadr zajmujących się cyberbezpieczeństwem, w tym poprzez promowanie ECSF i europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa oraz zapewnianie działań edukacyjnych i szkoleniowych;

   c) wspieranie planowania i realizacji ćwiczeń w zakresie cyberbezpieczeństwa.

4. ENISA jest otwarta na udział w swoich pracach państw trzecich, które zawarły z Unią umowy w tej sprawie. Na mocy odpowiednich postanowień umów zawartych między państwami trzecimi a Unią ustanawia się, z zastrzeżeniem uprzedniej zgody Komisji, ustalenia robocze określające w szczególności charakter, zakres i sposób udziału tych państw trzecich w pracach ENISA oraz zawierające postanowienia dotyczące udziału w inicjatywach podejmowanych przez ENISA, wkładu finansowego i personelu. W odniesieniu do spraw personalnych dotyczących pracowników ENISA ustalenia robocze są w każdym przypadku zgodne z regulaminem pracowniczym i warunkami zatrudnienia.

5. ENISA regularnie składa Radzie i Komisji sprawozdania z realizacji ustaleń roboczych, o których mowa w ust. 1 i 4.

TYTUŁ III

EUROPEJSKIE RAMY CERTYFIKACJI CYBERBEZPIECZEŃSTWA

ROZDZIAŁ I
Cele, zakres i procedury

Artykuł 71
Cele i zakres europejskich ram certyfikacji w zakresie cyberbezpieczeństwa

1. Europejskie ramy certyfikacji w zakresie cyberbezpieczeństwa ustanawia się w celu stworzenia jednolitego rynku cyfrowego dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i podmiotów. W tym celu zwiększają one poziom cyberbezpieczeństwa w Unii i umożliwiają zharmonizowane podejście do europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, a także wykorzystują certyfikację w celu ułatwienia zgodności z obowiązującym prawodawstwem Unii.

2. Europejskie ramy certyfikacji w zakresie cyberbezpieczeństwa przewidują mechanizm ustanawiania europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa oraz poświadczania następujących elementów:

   (a) że produkty ICT, usługi ICT i procesy ICT, które zostały ocenione zgodnie z takimi systemami, spełniają określone wymagania bezpieczeństwa w celu ochrony dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych lub funkcji lub usług oferowanych przez te produkty, usługi i procesy lub dostępnych za ich pośrednictwem przez cały cykl ich życia;

   (b) że zarządzane usługi bezpieczeństwa, które zostały ocenione zgodnie z takimi systemami, spełniają określone wymagania bezpieczeństwa w celu ochrony dostępności, autentyczności, integralności i poufności danych, do których uzyskuje się dostęp, które są przetwarzane, przechowywane lub przekazywane w związku ze świadczeniem tych usług, oraz że usługi te są świadczone w sposób ciągły, z zachowaniem wymaganej kompetencji, wiedzy fachowej i doświadczenia przez personel posiadający wystarczający i odpowiedni poziom odpowiedniej wiedzy technicznej i uczciwości zawodowej;

   (c) stan cyberbezpieczeństwa podmiotu, który został oceniony zgodnie z takimi systemami, jest zgodny z określonymi wymogami w zakresie cyberbezpieczeństwa.

3. Europejska certyfikacja w zakresie cyberbezpieczeństwa ma charakter dobrowolny, chyba że prawo unijne lub krajowe stanowi inaczej.

4. Europejski certyfikat cyberbezpieczeństwa i unijne oświadczenie o zgodności wydane w ramach europejskich ram certyfikacji cyberbezpieczeństwa są automatycznie uznawane we wszystkich państwach członkowskich.

Artykuł 72
Informacje publiczne i konsultacje

1. Co najmniej raz w roku Komisja organizuje, przy wsparciu ENISA, europejskie zgromadzenie ds. certyfikacji w zakresie cyberbezpieczeństwa, zapraszając członków

ECCG i innych odpowiednich ekspertów z państw członkowskich, odpowiednich ekspertów z podmiotów unijnych oraz odpowiednie zainteresowane strony w celu omówienia strategicznych priorytetów harmonizacji w dziedzinie certyfikacji w zakresie cyberbezpieczeństwa.

2 Komisja prowadzi i regularnie aktualizuje specjalną stronę internetową zawierającą informacje na temat następujących aspektów:

a) europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa, o których opracowanie wnioskowano zgodnie z art. 73;

b) strategiczne priorytety w zakresie harmonizacji produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa, cyberbezpieczeństwa podmiotów lub wymogów bezpieczeństwa określonych w przepisach unijnych, w tym potencjalne obszary, w których można by zażądać opracowania europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa.

3. Komisja podaje do wiadomości publicznej na stronie internetowej, o której mowa w ust. 2 niniejszego artykułu, informacje dotyczące jej wniosku skierowanego do ENISA o przygotowanie systemu kandydującego, o którym mowa w art. 73, oraz swojej decyzji o przyjęciu, odrzuceniu lub wycofaniu systemu kandydującego przekazanego przez ENISA zgodnie z art. 74 ust. 7.

4. Podczas przygotowywania systemu kandydującego przez ENISA zgodnie z art. 74 Parlament Europejski i Rada mogą zwrócić się do Komisji, pełniącej funkcję przewodniczącego ECCG, oraz do ENISA o przedstawienie odpowiednich informacji na temat projektu systemu kandydującego. Na wniosek Parlamentu Europejskiego lub Rady ENISA, w porozumieniu z Komisją i bez uszczerbku dla art. 54, może udostępnić Parlamentowi Europejskiemu i Radzie odpowiednie części projektu programu kandydującego w sposób odpowiedni do wymaganego poziomu poufności oraz, w stosownych przypadkach, w sposób ograniczony.

5. Parlament Europejski i Rada mogą zaprosić Komisję i ENISA do omówienia kwestii dotyczących wdrażania europejskich systemów certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów.

Artykuł 73
Wnioski o europejski system certyfikacji cyberbezpieczeństwa

1. Komisja może zwrócić się do ENISA o przygotowanie projektu europejskiego systemu certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberpostury podmiotów.

2. W należycie uzasadnionych przypadkach ECCG może zaproponować Komisji złożenie wniosku, o którym mowa w ust. 1.

3. Wniosek, o którym mowa w ust. 1, zawiera szczegółowe informacje na temat celu, zakresu i warunków realizacji odpowiednich celów i elementów bezpieczeństwa określonych w art. 80 i 81. Wniosek określa również plan rozwoju europejskiego systemu certyfikacji cyberbezpieczeństwa oraz odpowiednie specyfikacje techniczne, do których należy się odwołać lub które należy zdefiniować w systemie.

4. Przygotowując wniosek, o którym mowa w ust. 1, Komisja przeprowadza odpowiednie konsultacje z ENISA i ECCG, a także uwzględnia opinie wszystkich zainteresowanych stron i innych podmiotów unijnych, w tym, w stosownych

przypadkach, tych, które są istotne w świetle przepisów unijnych, zgodnie z którymi europejski system certyfikacji cyberbezpieczeństwa wykazuje zgodność i zapewnia domniemanie zgodności.

Artykuł 74

Przygotowanie i przyjęcie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa

1. Nie później niż 12 miesięcy po otrzymaniu wniosku od Komisji zgodnie z art. 73, o ile we wniosku nie określono inaczej, ENISA przygotowuje projekt europejskiego systemu certyfikacji cyberbezpieczeństwa, który spełnia wymogi określone w art. 80 i 81.

2 W celu przygotowania każdego projektu systemu ENISA powołuje grupę roboczą ad hoc zgodnie z art. 32 ust. 6, której zadaniem jest udzielanie ENISA fachowych porad.

3. Przygotowując projekt systemu, ENISA ściśle współpracuje z ECCG. ECCG zapewnia ENISA pomoc i fachowe doradztwo w zakresie przygotowania projektu systemu oraz, w stosownych przypadkach, wspierających specyfikacji technicznych.

4. Przygotowując projekt, w tym, w stosownych przypadkach, uzupełniające specyfikacje techniczne, ENISA konsultuje się w odpowiednim czasie z zainteresowanymi stronami w ramach formalnego, otwartego, przejrzystego i integracyjnego procesu konsultacji. ENISA współpracuje również z odpowiednimi organami publicznymi w państwach członkowskich oraz z odpowiednimi podmiotami unijnymi w celu uzyskania ich fachowych porad dotyczących przygotowania projektu oraz, w stosownych przypadkach, uzupełniających specyfikacji technicznych. Przekazując Komisji projekt planu zgodnie z ust. 6, ENISA opisuje sposób, w jaki zastosowała się do niniejszego ustępu.

5. Przed przekazaniem Komisji projektu systemu i, w stosownych przypadkach, uzupełniających specyfikacji technicznych, ENISA zwraca się do członków ECCG o przedstawienie pisemnych opinii na temat projektu systemu. Opinie należy przedstawić w terminie nieprzekraczającym 30 dni od daty złożenia wniosku. ENISA w jak największym stopniu uwzględnia opinie członków ECCG. Brak takich opinii nie stanowi przeszkody dla przekazania przez ENISA projektu systemu Komisji.

6. ENISA przekazuje Komisji projekt systemu najpóźniej w terminie 60 dni od daty złożenia wniosku, o którym mowa w ust. 5.

7. Po otrzymaniu projektu systemu Komisja ocenia, czy system ten odpowiada wnioskowi złożonemu zgodnie z art. 73. W ciągu 30 dni od daty przekazania projektu systemu Komisja podejmuje jedno z następujących działań:

   a) przyjmuje projekt programu;

   b) zwraca projekt ENISA do ponownego rozpatrzenia wraz z uzasadnieniem zwrotu i terminem nieprzekraczającym 90 dni, w którym to terminie ENISA przedstawia zmieniony projekt;

   c) zaprzestać stosowania programu kandydującego.

8. W przypadku gdy Komisja zwraca ENISA projekt do ponownego rozpatrzenia zgodnie z ust. 7 lit. b), stosuje się odpowiednio ust. 4, 5 i 7.

9. Komisja, na podstawie przyjętego programu kandydującego przygotowanego przez ENISA, jest uprawniona do przyjęcia aktów wykonawczych przewidujących europejski program certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT,

procesów ICT, zarządzanych usług bezpieczeństwa lub cyberpostury podmiotów, który spełnia wymogi określone w art. 80 i 81. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.

10. Komisja może odwoływać się do specyfikacji technicznych opracowanych przez ENISA w aktach wykonawczych, o których mowa w ust. 9 niniejszego artykułu, zgodnie z art. 18 i 77.

11. Komisja może określić warunki międzynarodowego uznawania europejskich certyfikatów cyberbezpieczeństwa w aktach wykonawczych, o których mowa w ust. 9 niniejszego artykułu, zgodnie z art. 87.

Artykuł 75

Utrzymanie europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa

1. Każdy europejski system certyfikacji w zakresie cyberbezpieczeństwa ustanawia strategię utrzymania. Strategia utrzymania określa oczekiwania dotyczące działań związanych z utrzymaniem, w szczególności tych związanych z normami lub specyfikacjami technicznymi, do których odwołuje się system, oraz z interakcją z odpowiednimi zainteresowanymi stronami.

2 ENISA, we współpracy z Komisją i przy wsparciu ECCG oraz odpowiedniej podgrupy ds. utrzymania, zapewnia utrzymanie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, w tym z uwzględnieniem ewentualnego przeglądu takich systemów przez Komisję. ENISA współpracuje i wymienia informacje z odpowiednimi podmiotami i grupami unijnymi w odniesieniu do działań związanych z utrzymaniem.

3. ENISA może zorganizować udział sektora prywatnego w utrzymaniu systemu w formie grupy roboczej ad hoc zgodnie ze strategią utrzymania, o której mowa w ust. 1.

4. Działania związane z utrzymaniem europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa obejmują:

   a) przygotowywanie, aktualizowanie i zatwierdzanie specyfikacji technicznych i wytycznych w celu wspierania zharmonizowanego i jednolitego funkcjonowania systemów;

   b) określenie norm lub specyfikacji technicznych, które są istotne dla systemu;

   c) współpraca, a w stosownych przypadkach nawiązywanie kontaktów z odpowiednimi zainteresowanymi stronami, w tym europejskimi lub międzynarodowymi organizacjami normalizacyjnymi, w tym w celu wnoszenia lub otrzymywania wkładu technicznego;

   d) wydawanie Komisji zaleceń dotyczących niezbędnych ulepszeń i aktualizacji systemów, w tym w perspektywie ewentualnego przeglądu systemów;

   e) wymianę informacji dotyczących praktycznego wdrażania systemów między państwami członkowskimi;

   (f) wkład w mechanizmy wzajemnej oceny i analizy wyników takich ocen w celu usprawnienia funkcjonowania systemów i wsparcia ich ewentualnego przeglądu.

5. ECCG może wydać opinię w sprawie utrzymania europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa.

Artykuł 76

Ocena, przegląd i wycofanie europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa

1. Co najmniej co cztery lata po wejściu w życie europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa ENISA ocenia wpływ i skuteczność tego systemu we współpracy z odpowiednią podgrupą ds. utrzymania ECCG oraz z uwzględnieniem informacji zwrotnych otrzymanych od zainteresowanych stron. ENISA przeprowadza ocenę, dokonując analizy rynku zgodnie z art. 8 ust. 1.

2 Po przeprowadzeniu oceny, o której mowa w ust. 1, Komisja może dokonać przeglądu lub wycofać akty wykonawcze ustanawiające europejski system certyfikacji w zakresie cyberbezpieczeństwa zgodnie z art. 74 ust. 9.

3. Przy przeglądzie lub wycofywaniu europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa Komisja konsultuje się z ENISA, ECCG i odpowiednią podgrupą ds. utrzymania, a także uwzględnia opinie odpowiednich zainteresowanych stron i innych podmiotów unijnych.

4. ECCG może wydać opinię w sprawie przeglądu lub wycofania europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa. Komisja należycie uwzględnia tę opinię przy dokonywaniu przeglądu lub wycofywaniu europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa.

Artykuł 77

Specyfikacje techniczne w europejskich systemach certyfikacji w zakresie cyberbezpieczeństwa

1. ENISA może opracować specyfikacje techniczne z myślą o przyszłym europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa lub w celu wsparcia utrzymania europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa.

2 Specyfikacje techniczne, o których mowa w ust. 1 niniejszego artykułu, opracowuje się w odpowiednim terminie, przy wsparciu ECCG i jej podgrup ds. utrzymania oraz, w stosownych przypadkach, odpowiedniej grupy roboczej ad hoc, o której mowa w art. 75 ust. 3. W tym celu ENISA zwraca się również o wkład do odpowiednich grup zainteresowanych stron, uwzględniając strategię utrzymania, o której mowa w art. 75 ust. 1.

3. W przypadku gdy w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa, o którym mowa w art. 74 ust. 10, znajduje się odniesienie do specyfikacji technicznych, są one udostępniane na stronie internetowej, o której mowa w art. 79.

4. W należycie uzasadnionych przypadkach, w szczególności gdy specyfikacje techniczne zawierają informacje, które mogłyby zagrozić bezpieczeństwu certyfikowanych produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów, są one udostępniane wyłącznie zainteresowanym stronom, których dotyczą wymogi systemu. W europejskim systemie certyfikacji cyberbezpieczeństwa, o którym mowa w art. 74 ust. 10, nie odwołuje się do takich specyfikacji technicznych.

Artykuł 78
Ułatwianie zgodności z prawodawstwem Unii

1. Jeżeli przewiduje to konkretny akt prawny Unii, certyfikat wydany w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa potwierdza zgodność i daje domniemanie zgodności z odpowiednimi wymogami określonymi w tym akcie prawnym.

2. Działania oceniające w ramach europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa są zgodne z odpowiednim aktem prawnym Unii określającym wykazanie zgodności i domniemanie zgodności. Jeżeli takie działania oceniające nie są określone w odpowiednim akcie prawnym Unii, określa je system. Ocena zgodności w celu certyfikacji przyznającej domniemanie zgodności z wymogami określonymi w przepisach Unii jest przeprowadzana przez jednostkę zewnętrzną.

3. W przypadku braku zharmonizowanego prawodawstwa unijnego prawo krajowe może również przewidywać, że europejski system certyfikacji w zakresie cyberbezpieczeństwa może być stosowany do wykazania zgodności i ustalenia domniemania zgodności z określonymi wymogami prawnymi określonymi w prawie krajowym.

Artykuł 79
Wdrażanie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, strona internetowa ENISA i publikacja certyfikatów

1. ENISA organizuje działania mające na celu promowanie stosowania przyjętych europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, w tym poprzez prowadzenie strony internetowej, o której mowa w ust. 2 niniejszego artykułu.

2 ENISA prowadzi i regularnie aktualizuje specjalną stronę internetową zawierającą informacje publiczne na temat:

   a) europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa;

   b) opłatach związanych z utrzymaniem każdego europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa;

   c) odpowiednie specyfikacje techniczne ENISA;

   d) europejskie certyfikaty cyberbezpieczeństwa i unijne deklaracje zgodności, w tym informacje dotyczące certyfikatów i deklaracji, które straciły ważność, zostały zawieszone, cofnięte lub wygasły;

   e) odpowiednie uzupełniające informacje dotyczące cyberbezpieczeństwa przekazane zgodnie z art. 84;

   f) podsumowania wzajemnych ocen zgodnie z art. 89 ust. 7;

   g specyfikacje techniczne, do których odwołuje się europejski system certyfikacji cyberbezpieczeństwa zgodnie z art. 74 ust. 10.

3. W stosownych przypadkach strona internetowa, o której mowa w ust. 2, wskazuje również krajowe systemy certyfikacji cyberbezpieczeństwa, które zostały zastąpione europejskim systemem certyfikacji cyberbezpieczeństwa.

ROZDZIAŁ II
Zawartość europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa

Artykuł 80

Cele bezpieczeństwa europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa

1. Europejski system certyfikacji w zakresie cyberbezpieczeństwa realizuje, w stosownych przypadkach, następujące cele w zakresie bezpieczeństwa:

   a) zapewnienie, aby produkty ICT, usługi ICT, procesy ICT i zarządzane usługi bezpieczeństwa były bezpieczne z założenia i dzięki swojej konstrukcji;

   b) ochrona danych przechowywanych, przekazywanych lub przetwarzanych w inny sposób przed przypadkowym lub nieuprawnionym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem przy użyciu odpowiednich środków technicznych, z uwzględnieniem całego cyklu życia produktów ICT, usług ICT lub procesów ICT;

   c) ochrona integralności przechowywanych, przekazywanych lub przetwarzanych w inny sposób danych osobowych lub innych danych, poleceń, programów i konfiguracji przed wszelkimi manipulacjami lub modyfikacjami nieautoryzowanymi przez użytkownika oraz zgłaszanie przypadków uszkodzeń, z uwzględnieniem całego cyklu życia produktów ICT, usług ICT lub procesów ICT;

   d) zapewnienie ochrony przed nieuprawnionym dostępem za pomocą odpowiednich mechanizmów kontroli, w tym między innymi systemów uwierzytelniania, zarządzania tożsamością lub dostępem, oraz zgłaszanie ewentualnych przypadków nieuprawnionego dostępu;

   e) identyfikowanie i dokumentowanie komponentów i słabych punktów, w tym, w stosownych przypadkach, poprzez sporządzenie wykazu komponentów oprogramowania obejmującego co najmniej zależności najwyższego poziomu;

   f) dostarczanie informacji związanych z bezpieczeństwem poprzez rejestrowanie i monitorowanie odpowiednich działań wewnętrznych, w tym dostępu do danych, usług lub funkcji lub ich modyfikacji, w stosownych przypadkach, z mechanizmem rezygnacji dla użytkownika;

   g) weryfikowanie, czy produkty, usługi i procesy ICT nie zawierają znanych podatności, które można wykorzystać;

   h) ochrona dostępności podstawowych i niezbędnych funkcji, w tym po wystąpieniu incydentu, między innymi poprzez środki zapewniające odporność i łagodzące skutki ataków typu „odmowa usługi”;

   i) minimalizowanie negatywnego wpływu na dostępność usług świadczonych przez inne sieci i urządzenia w przypadku incydentu fizycznego lub technicznego;

   j) zapewnienie regularnego testowania produktów, usług i procesów ICT oraz przeglądu ich bezpieczeństwa;

   (k) zapewnienie, aby luki w zabezpieczeniach były niezwłocznie usuwane, w tym poprzez aktualizacje zabezpieczeń, oraz aby informacje o usuniętych lukach były udostępniane i podawane do wiadomości publicznej, chyba że ryzyko związane z publikacją przewyższa korzyści dla bezpieczeństwa;

   (l) zapewnienie wprowadzenia polityki skoordynowanego ujawniania luk w zabezpieczeniach;

(m) ułatwianie wymiany informacji o potencjalnych lukach w zabezpieczeniach produktów, usług i procesów ICT;

n) zapewnienie, aby w przypadku udostępnienia aktualizacji zabezpieczeń w celu usunięcia zidentyfikowanych problemów związanych z bezpieczeństwem, aktualizacje te były bezzwłocznie rozpowszechniane;

o) zapewnienie, aby zarządzane usługi bezpieczeństwa były świadczone z zachowaniem wymaganych kompetencji, wiedzy specjalistycznej i doświadczenia, w tym aby personel odpowiedzialny za świadczenie tych usług posiadał wystarczający i odpowiedni poziom wiedzy technicznej i kompetencji w danej dziedzinie, wystarczające i odpowiednie doświadczenie oraz najwyższy stopień uczciwości zawodowej;

(p) zapewnienie, aby produkty ICT, usługi ICT i procesy ICT wykorzystywane w świadczeniu zarządzanych usług bezpieczeństwa były bezpieczne z założenia i domyślnie oraz, w stosownych przypadkach, zawierały najnowsze aktualizacje zabezpieczeń i nie zawierały publicznie znanych luk w zabezpieczeniach;

(q) zapewnienie, aby certyfikowany podmiot posiadał odpowiednie procedury wewnętrzne gwarantujące świadczenie usług na wystarczającym i odpowiednim poziomie jakości;

(r) zapewnienie, aby certyfikowany podmiot był w stanie identyfikować incydenty, chronić się przed nimi, wykrywać je, reagować na nie i usuwać ich skutki;

s) zapewnienie, aby certyfikowany podmiot był w stanie zarządzać ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez ten podmiot do prowadzenia działalności lub świadczenia usług oraz zapobiegać skutkom incydentów lub minimalizować ich wpływ na odbiorców jego usług i inne usługi;

t) zapewnienie, aby certyfikowany podmiot był w stanie budować, zapewniać i weryfikować swoją integralność operacyjną i niezawodność poprzez zapewnienie, bezpośrednio lub pośrednio poprzez korzystanie z usług świadczonych przez zewnętrznych dostawców usług ICT, że dysponuje pełnym zakresem zdolności związanych z ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez ten podmiot oraz wspierających ciągłość świadczenia usług i ich jakość, w tym w przypadku zakłóceń;

(u) zapewnienie, aby certyfikowany podmiot był w stanie wdrożyć i utrzymać system zarządzania bezpieczeństwem informacji;

(v) przeciwdziałanie wszelkim zdarzeniom, które mogą zagrozić dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez system sieci i informatyczny wykorzystywany przez podmiot lub dostępny za jego pośrednictwem, oraz zapewnienie ciągłości świadczenia usług i ich jakości, w tym w przypadku zakłóceń;

(w) zapewnienie, aby podmiot był w stanie zagwarantować bezpieczeństwo przetwarzania danych osobowych.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 119 w celu zmiany ust. 1 niniejszego artykułu poprzez dodanie lub zmianę celów bezpieczeństwa, aby zapewnić, że odzwierciedlają one najnowszy rozwój

technologiczny i nowe związane z nim zagrożenia, a także przyjęcie nowych przepisów unijnych określających wykazanie zgodności i domniemanie zgodności poprzez europejską certyfikację cyberbezpieczeństwa z odpowiednimi wymogami w zakresie cyberbezpieczeństwa zawartymi w tych przepisach.

3. Europejski system certyfikacji cyberbezpieczeństwa dotyczący produktów zawierających elementy cyfrowe, zgodnie z definicją zawartą w art. 3 pkt 1 rozporządzenia (UE) 2024/2847, należy opracować zgodnie z zasadniczymi wymogami w zakresie cyberbezpieczeństwa określonymi w załączniku I do tego rozporządzenia, z uwzględnieniem dostępnych norm zharmonizowanych.

Artykuł 81

Elementy europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa

1. Europejski system certyfikacji w zakresie cyberbezpieczeństwa obejmuje co najmniej następujące elementy:

   a) przedmiot i zakres systemu certyfikacji, w tym rodzaj lub kategorie produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa lub aktywa, usługi i funkcje podmiotu objęte zakresem certyfikacji;

   b) jasny opis celu systemu oraz, w stosownych przypadkach, wskazanie przepisów unijnych określających wymagania, których zgodność potwierdzają europejskie certyfikaty cyberbezpieczeństwa i które dają domniemanie zgodności;

   c) strategię utrzymania określającą podejście do działań związanych z utrzymaniem, o których mowa w art. 75;

   d) szczegółowe wymagania w zakresie cyberbezpieczeństwa, kryteria oceny i metody stosowane do oceny produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów oraz odniesienia do międzynarodowych, europejskich lub krajowych norm stosowanych w ocenie produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów lub, w przypadku gdy takie normy nie są dostępne lub nie są odpowiednie, do specyfikacji technicznych opracowanych przez ENISA zgodnie z art. 77 lub, jeżeli takie specyfikacje nie są dostępne, do innych specyfikacji technicznych;

   e) maksymalny okres ważności europejskich certyfikatów cyberbezpieczeństwa wydanych w ramach systemu.

2. Europejski system certyfikacji w zakresie cyberbezpieczeństwa obejmuje co najmniej zasady i warunki dotyczące:

   a) monitorowanie zgodności produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub stanu cyberbezpieczeństwa podmiotów z wymogami europejskich certyfikatów cyberbezpieczeństwa lub unijnych oświadczeń o zgodności, w tym mechanizmów wykazywania ciągłej zgodności z określonymi wymogami w zakresie cyberbezpieczeństwa;

   b) wydawanie, potwierdzanie, cofanie i odnawianie europejskich certyfikatów cyberbezpieczeństwa, rozszerzanie lub ograniczanie zakresu certyfikacji oraz ponowna certyfikacja;

   c) konsekwencje dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiotów, które uzyskały certyfikat lub dla których

wydano oświadczenie UE o zgodności, ale które nie spełniają wymogów systemu;

d) sposób zgłaszania i postępowania w przypadku wcześniej niewykrytych luk w cyberbezpieczeństwie produktów ICT, usług ICT i procesów ICT;

e) treść i format europejskich certyfikatów cyberbezpieczeństwa oraz wydawanych unijnych oświadczeń o zgodności;

f) okres dostępności unijnego oświadczenia o zgodności, dokumentacji technicznej i wszystkich innych istotnych informacji, które mają być udostępnione przez producenta lub dostawcę produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa lub przez podmiot, którego cyberbezpieczeństwo podlega certyfikacji;

g) wszelkie mechanizmy wzajemnej oceny ustanowione w ramach systemu dla organów lub podmiotów wydających europejskie certyfikaty cyberbezpieczeństwa zgodnie z art. 85 ust. 4, które nie mają wpływu na wzajemną ocenę przewidzianą w art. 90;

h) poufność informacji i danych uzyskanych przez wszystkie strony w ramach wykonywania zadań i działań związanych z wdrażaniem przepisów określonych w niniejszym tytule;

i) format i procedury, których powinni przestrzegać producenci lub dostawcy produktów, usług lub procesów ICT przy dostarczaniu i aktualizowaniu uzupełniających informacji dotyczących cyberbezpieczeństwa zgodnie z art. 84; oraz

j) ciągłość działań certyfikacyjnych w nadzwyczajnych sytuacjach kryzysowych, które są nieuniknione i utrudniają stosowanie zasad systemu certyfikacji.

3. Europejski system certyfikacji cyberbezpieczeństwa obejmuje również, w stosownych przypadkach, następujące elementy:

a jeden lub więcej poziomów zapewnienia i odpowiadających im poziomów oceny;

b) profile ochrony określające wymagania bezpieczeństwa mające zastosowanie do danej kategorii produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa;

c) profile rozszerzeń określające dodatkowe wymogi bezpieczeństwa, w tym, w stosownych przypadkach, wymogi bezpieczeństwa określone w przepisach krajowych transponujących prawo Unii;

d) wyjaśnienie, które działania w zakresie oceny zgodności, w tym kalibracja, badania, certyfikacja i kontrola, dla poziomu zapewnienia „wysokiego” lub w celu wykazania zgodności i przyznania domniemania zgodności, są dozwolone poza Europejskim Obszarem Gospodarczym (EOG);

e) określenie krajowych lub międzynarodowych systemów certyfikacji cyberbezpieczeństwa obejmujących ten sam rodzaj lub kategorie produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów;

f) dodatkowe lub szczególne wymagania, którym podlegają jednostki oceniające zgodność w celu zagwarantowania ich kompetencji technicznych do oceny wymagań w zakresie cyberbezpieczeństwa;

g) informacje niezbędne do certyfikacji, które wnioskodawca ma obowiązek dostarczyć lub w inny sposób udostępnić organom oceny zgodności;

h) znaki lub etykiety oraz warunki, na jakich można stosować takie znaki lub etykiety;

i warunki międzynarodowego uznawania europejskich certyfikatów cyberbezpieczeństwa zgodnie z art. 87.

4. Określone wymagania europejskiego systemu certyfikacji cyberbezpieczeństwa są zgodne z wymogami prawodawstwa unijnego.

5. Komisja jest uprawniona do przyjmowania aktów wykonawczych ustanawiających wspólne zasady i wzorcowe przepisy dotyczące elementów określonych w ust. 1, 2 i 3 we wszystkich europejskich systemach certyfikacji w zakresie cyberbezpieczeństwa. W stosownych przypadkach i o ile jest to możliwe, europejski system certyfikacji w zakresie cyberbezpieczeństwa może zawierać odniesienia do tych zasad i wzorcowych przepisów.

6. Akty wykonawcze, o których mowa w ust. 5, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2. Przy opracowywaniu lub zmianie wspólnych zasad i wzorcowych przepisów dotyczących elementów europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa Komisja konsultuje się z ENISA i uwzględnia, w stosownych przypadkach, opinie wyrażone przez ECCG, zainteresowane strony i inne właściwe organy.

Artykuł 82
Poziomy zapewnienia i oceny europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa

1. Europejski system certyfikacji cyberbezpieczeństwa może określać jeden lub więcej z następujących poziomów zapewnienia dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberpostury podmiotów: „podstawowy”, „znaczny” lub „wysoki”. Poziomy zapewnienia bezpieczeństwa są proporcjonalne do poziomu ryzyka związanego z zamierzonym wykorzystaniem produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub do charakteru podmiotów, których cyberbezpieczeństwo podlega certyfikacji, oraz ich środowiska operacyjnego, pod względem prawdopodobieństwa wystąpienia incydentu i jego skutków.

2. Europejskie certyfikaty cyberbezpieczeństwa odnoszą się do każdego poziomu zapewnienia określonego w europejskim systemie certyfikacji cyberbezpieczeństwa, w ramach którego certyfikaty te są wydawane. Deklaracje zgodności UE odnoszą się do poziomu zapewnienia „podstawowego”.

3. Wymogi bezpieczeństwa odpowiadające każdemu poziomowi zapewnienia są określone w odpowiednim europejskim systemie certyfikacji cyberbezpieczeństwa, w tym odpowiednie środki kontroli bezpieczeństwa i odpowiednia ocena, której ma zostać poddany produkt ICT, usługa ICT, proces ICT, zarządzana usługa bezpieczeństwa lub cyberbezpieczeństwo podmiotu.

4. Europejski certyfikat cyberbezpieczeństwa lub unijne oświadczenie o zgodności odnoszą się do specyfikacji technicznych, norm i procedur z nimi związanych, w tym

środków kontroli technicznej, których celem jest zmniejszenie ryzyka wystąpienia incydentów cyberbezpieczeństwa lub zapobieganie im.

5. Europejski certyfikat cyberbezpieczeństwa lub unijne oświadczenie o zgodności, które odnoszą się do poziomu zapewnienia „podstawowego", zapewniają, że produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub cyberpostura podmiotów, dla których wydano ten certyfikat lub unijne oświadczenie o zgodności, spełniają odpowiednie wymogi bezpieczeństwa, w tym kontrole bezpieczeństwa, oraz że zostały one ocenione na poziomie mającym na celu zminimalizowanie znanych podstawowych ryzyk incydentów i cyberataków. Przeprowadzane działania oceniające obejmują co najmniej przegląd dokumentacji technicznej. W przypadku gdy taki przegląd nie jest właściwy, przeprowadza się zastępcze działania oceniające o równoważnym skutku.

6. Europejski certyfikat cyberbezpieczeństwa odnoszący się do poziomu zapewnienia „znacznego" gwarantuje, że produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub cyberbezpieczeństwo podmiotów, dla których wydano ten certyfikat, spełniają odpowiednie wymogi bezpieczeństwa, w tym kontrole bezpieczeństwa, oraz że zostały one ocenione na poziomie mającym na celu zminimalizowanie znanych zagrożeń incydentami i cyberatakami oraz ryzyka cyberataków przeprowadzanych przez podmioty o ograniczonych umiejętnościach i zasobach. Przeprowadzane działania oceniające obejmują co najmniej przegląd mający na celu wykazanie braku publicznie znanych luk w zabezpieczeniach oraz testy mające na celu wykazanie, że produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub podmioty prawidłowo wdrażają niezbędne kontrole bezpieczeństwa. W przypadku gdy takie działania oceniające nie są odpowiednie, podejmuje się zastępcze działania oceniające o równoważnym skutku.

7. Europejski certyfikat cyberbezpieczeństwa odnoszący się do poziomu zapewnienia „wysokiego" gwarantuje, że produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub cyberpostura podmiotów, dla których wydano ten certyfikat, spełniają odpowiednie wymogi bezpieczeństwa, w tym kontrole bezpieczeństwa, oraz że zostały one ocenione na poziomie mającym na celu zminimalizowanie ryzyka incydentów i najnowocześniejszych cyberataków przeprowadzanych przez podmioty dysponujące znacznymi umiejętnościami i zasobami. Przeprowadzane działania oceniające obejmują co najmniej:

   a) przegląd mający na celu wykazanie braku publicznie znanych luk w zabezpieczeniach;

   b) testy mające na celu wykazanie, że produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub podmioty prawidłowo wdrażają niezbędne najnowocześniejsze środki kontroli bezpieczeństwa;

   c) ocena odporności produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiotów na ataki wykwalifikowanych hakerów, z wykorzystaniem w stosownych przypadkach testów penetracyjnych.

   W przypadku gdy takie działania oceniające nie są właściwe, podejmuje się działania zastępcze o równoważnym skutku. Wszelkie działania związane z oceną zgodności, w tym kalibracja, testowanie, certyfikacja i kontrola, dla poziomu zapewnienia „wysokiego" są podejmowane w Europejskim Obszarze Gospodarczym, chyba że europejski system certyfikacji cyberbezpieczeństwa stanowi inaczej.

8. W przypadku gdy europejski system certyfikacji w zakresie cyberbezpieczeństwa ma na celu wykazanie zgodności i przyznanie domniemania zgodności z określonym aktem prawnym Unii, europejski certyfikat cyberbezpieczeństwa zapewnia gwarancję, że certyfikowane produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub cyberpostura podmiotów spełniają odpowiednie wymogi w zakresie cyberbezpieczeństwa określone w tym akcie prawnym. Wszelkie działania związane z oceną zgodności, w tym kalibracja, testowanie, certyfikacja i kontrola, mające na celu domniemanie zgodności, są przeprowadzane w Europejskim Obszarze Gospodarczym, chyba że europejski system certyfikacji w zakresie cyberbezpieczeństwa stanowi inaczej.

9. Europejski system certyfikacji w zakresie cyberbezpieczeństwa może określać kilka poziomów oceny dla danego poziomu zapewnienia. Każdy z poziomów oceny odpowiada jednemu z poziomów zapewnienia.

Artykuł 83
Samoocena zgodności

1. Europejski system certyfikacji cyberbezpieczeństwa może dopuszczać samoocenę zgodności, za którą wyłączną odpowiedzialność ponosi producent lub dostawca produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiot, którego cyberbezpieczeństwo podlega certyfikacji. Samoocena zgodności jest dozwolona wyłącznie w odniesieniu do produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów, które charakteryzują się niskim ryzykiem odpowiadającym poziomowi zapewnienia „podstawowemu”.

2. Producent lub dostawca produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiot, którego cyberbezpieczeństwo podlega certyfikacji, może wydać unijne oświadczenie o zgodności stwierdzające, że wykazano spełnienie wymagań określonych w europejskim systemie certyfikacji cyberbezpieczeństwa. Wydając takie oświadczenie, producent, dostawca lub podmiot ponosi odpowiedzialność ną za zgodność produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub stanu cyberbezpieczeństwa z wymogami określonymi w tym systemie.

3. Producent lub dostawca produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiot, którego cyberbezpieczeństwo podlega certyfikacji, udostępnia krajowemu organowi certyfikacji cyberbezpieczeństwa wyznaczonemu zgodnie z art. 89 oświadczenie UE o zgodności, dokumentację techniczną oraz wszelkie inne istotne informacje dotyczące zgodności produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa z europejskim systemem certyfikacji cyberbezpieczeństwa przez okres przewidziany w tym systemie. Kopia oświadczenia UE o zgodności jest przekazywana bez zbędnej zwłoki krajowemu organowi certyfikacji cyberbezpieczeństwa oraz ENISA.

Artykuł 84
Dodatkowe informacje dotyczące cyberbezpieczeństwa certyfikowanych produktów ICT, usług ICT i procesów ICT

1. Producent lub dostawca produktów ICT, usług ICT lub procesów ICT, dla których wydano unijne oświadczenie o zgodności lub europejski certyfikat

cyberbezpieczeństwa, udostępnia użytkownikowi następujące dodatkowe informacje dotyczące cyberbezpieczeństwa:

a) przeznaczenie danego produktu ICT, usługi ICT lub procesu ICT, w tym środowisko bezpieczeństwa zapewnione przez producenta lub dostawcę;

b) wytyczne i zalecenia mające na celu pomoc użytkownikom w bezpiecznej konfiguracji, instalacji, wdrażaniu, eksploatacji i konserwacji produktów lub usług ICT;

c) rodzaj wsparcia technicznego w zakresie bezpieczeństwa oferowanego przez producenta lub dostawcę oraz datę zakończenia okresu wsparcia, w którym użytkownicy mogą oczekiwać usunięcia luk w zabezpieczeniach i otrzymania aktualizacji zabezpieczeń;

d) jeżeli producent lub dostawca zdecyduje się udostępnić użytkownikowi wykaz komponentów oprogramowania, informacje o tym, gdzie można uzyskać do niego dostęp.

2. Producent lub dostawca produktów ICT, usług ICT lub procesów ICT, dla których wydano unijne oświadczenie o zgodności lub europejski certyfikat cyberbezpieczeństwa, podaje do wiadomości publicznej następujące dodatkowe informacje dotyczące cyberbezpieczeństwa:

a) jedyny punkt kontaktowy, w którym można zgłaszać i otrzymywać informacje o lukach w zabezpieczeniach oraz w którym można znaleźć politykę producenta dotyczącą skoordynowanego ujawniania luk w zabezpieczeniach;

(b) informacje o usuniętych lukach w zabezpieczeniach, w tym opis tych luk, w tym informacje umożliwiające użytkownikom identyfikację produktu z elementami cyfrowymi, na które mają wpływ te luki, skutki tych luk, ich powagę oraz jasne i dostępne informacje pomagające użytkownikom w usunięciu tych luk; w należycie uzasadnionych przypadkach, gdy producenci uznają, że ryzyko związane z publikacją informacji przewyższa korzyści w zakresie bezpieczeństwa, mogą oni opóźnić podanie do wiadomości publicznej informacji dotyczących usuniętej luki w zabezpieczeniach do czasu, aż użytkownicy będą mieli możliwość zastosowania odpowiedniej poprawki.

3. Informacje, o których mowa w ust. 1 i 2, są dostępne w formie elektronicznej i pozostają dostępne oraz są w razie potrzeby aktualizowane w okresie ważności oraz co najmniej przez okres pięciu lat po wygaśnięciu lub wycofaniu odpowiedniego europejskiego certyfikatu cyberbezpieczeństwa lub unijnego oświadczenia o zgodności.

4. Obowiązki określone w ust. 1 i 2 nie mają zastosowania, jeżeli publiczne udostępnienie informacji mogłoby zagrozić bezpieczeństwu danego produktu, usługi lub procesu ICT.

ROZDZIAŁ III
Zarządzanie europejskimi ramami certyfikacji w zakresie cyberbezpieczeństwa

Sekcja 1
Ogólne zasady i zarządzanie europejskimi systemami certyfikacji w zakresie cyberbezpieczeństwa

Artykuł 85
Wydawanie europejskich certyfikatów cyberbezpieczeństwa

1. Produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub cyberbezpieczeństwo podmiotów, które uzyskały certyfikat w ramach europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa, uznaje się za zgodne z wymogami tego systemu.

2. Jednostki oceniające zgodność, o których mowa w art. 91, wydają europejskie certyfikaty cyberbezpieczeństwa na podstawie kryteriów zawartych w europejskim systemie certyfikacji cyberbezpieczeństwa przyjętym zgodnie z art. 74.

3. W drodze odstępstwa od ust. 2 europejski system certyfikacji w zakresie cyberbezpieczeństwa może przewidywać, że europejskie certyfikaty cyberbezpieczeństwa wynikające z tego systemu są wydawane wyłącznie przez jedną z następujących instytucji publicznych:

   a) krajowy organ certyfikacji w zakresie cyberbezpieczeństwa, o którym mowa w art. 88, akredytowany jako organ oceny zgodności zgodnie z art. 91 ust. 1;

   b) organ publiczny akredytowany jako jednostka oceniająca zgodność zgodnie z art. 91 ust. 1.

4. W przypadku gdy europejski system certyfikacji cyberbezpieczeństwa przyjęty zgodnie z art. 74 ustanawia poziom zapewnienia „wysoki” lub gdy taki system stanowi inaczej, europejski certyfikat cyberbezpieczeństwa w ramach tego systemu wydaje wyłącznie krajowy organ certyfikacji cyberbezpieczeństwa, o którym mowa w art. 88, akredytowany jako jednostka oceniająca zgodność zgodnie z art. 91 ust. 1, lub w następujących przypadkach:

   a) przez jednostkę oceniającą zgodność na podstawie modelu uprzedniego zatwierdzenia; lub

   b) przez jednostkę oceniającą zgodność na podstawie modelu ogólnego przekazania uprawnień.

5. Komisja jest uprawniona do przyjmowania aktów wykonawczych określających procedury dotyczące modeli uprzedniego zatwierdzania lub ogólnego przekazywania uprawnień, o których mowa w ust. 4 niniejszego artykułu. W trakcie przygotowywania tych aktów wykonawczych Komisja konsultuje się z ECCG. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.

6. Osoba fizyczna lub prawna, która przedkłada produkty ICT, usługi ICT, procesy ICT lub zarządzane usługi bezpieczeństwa do certyfikacji, lub podmiot, który ubiega się o certyfikację swojego stanu cyberbezpieczeństwa, udostępnia wszystkie informacje niezbędne do przeprowadzenia certyfikacji krajowemu organowi certyfikacji cyberbezpieczeństwa wyznaczonemu zgodnie z art. 89 rozporządzenia (UE) nr , jeżeli organ ten jest organem wydającym europejski certyfikat cyberbezpieczeństwa, lub organowi oceny zgodności, o którym mowa w art. 91.

7. Jednostki oceniające zgodność oraz, w stosownych przypadkach, krajowe organy certyfikacji cyberbezpieczeństwa informują ENISA bez zbędnej zwłoki o swoich decyzjach mających wpływ na status europejskich certyfikatów cyberbezpieczeństwa i unijnych oświadczeń o zgodności zgodnie z art. 94.

8. Posiadacz europejskiego certyfikatu cyberbezpieczeństwa informuje jednostkę oceniającą zgodność oraz, w stosownych przypadkach, krajowy organ certyfikacji

cyberbezpieczeństwa, o których mowa w ust. 7, o wszelkich wykrytych później lukach w zabezpieczeniach lub niezgodnościach dotyczących certyfikowanego produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub stanu cyberbezpieczeństwa podmiotu, które mogą mieć wpływ na jego zgodność z certyfikatem. Jednostka ta przekazuje te informacje bez zbędnej zwłoki właściwemu krajowemu organowi certyfikacji w zakresie cyberbezpieczeństwa i ocenia wpływ na certyfikat zgodnie z warunkami systemu, o których mowa w art. 81 ust. 2 lit. d).

9. W odniesieniu do certyfikowanych produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa, które zostały uznane w całości lub w części za kluczowe aktywa zgodnie z art. 102, posiadacze europejskiego certyfikatu cyberbezpieczeństwa nie mogą wykorzystywać, instalować ani w inny sposób integrować komponentów ICT lub komponentów zawierających komponenty ICT pochodzących od dostawców wysokiego ryzyka w certyfikowanych produktach ICT, usługach ICT, procesach ICT lub zarządzanych usługach bezpieczeństwa.

10. Europejski certyfikat cyberbezpieczeństwa wydaje się na okres przewidziany w europejskim systemie certyfikacji cyberbezpieczeństwa i może być odnawiany, pod warunkiem że nadal spełniane są odpowiednie wymagania.

11. Komisja współpracuje z państwami członkowskimi w celu zapewnienia stosowania przepisów dotyczących wydawania europejskich certyfikatów cyberbezpieczeństwa, również w kontekście stosowania art. 100 ust. 4 lit. b). Jednostka oceniająca zgodność oraz, w stosownych przypadkach, krajowy organ certyfikacji cyberbezpieczeństwa przekazują Komisji, na jej wniosek i bez zbędnej zwłoki, wszelkie informacje dotyczące wydania odpowiednich europejskich certyfikatów cyberbezpieczeństwa lub unijnych oświadczeń o zgodności.

Artykuł 86

Krajowe systemy certyfikacji w zakresie cyberbezpieczeństwa i certyfikaty

1. Krajowe systemy certyfikacji w zakresie cyberbezpieczeństwa oraz związane z nimi procedury dotyczące produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberpostury podmiotów objętych przedmiotem i zakresem europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa przestają obowiązywać od daty określonej w akcie wykonawczym przyjętym zgodnie z art. 74 ust. 9. Krajowe systemy certyfikacji w zakresie cyberbezpieczeństwa oraz związane z nimi procedury dotyczące produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberpostury podmiotów, które nie są objęte przedmiotem i zakresem europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa, mogą nadal istnieć.

2. Państwa członkowskie nie wprowadzają nowych krajowych systemów certyfikacji w zakresie cyberbezpieczeństwa ani powiązanych procedur dotyczących produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberbezpieczeństwa podmiotów już objętych przedmiotem i zakresem europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa.

3. Istniejące certyfikaty, które zostały wydane w ramach krajowych systemów certyfikacji cyberbezpieczeństwa i są objęte przedmiotem i zakresem europejskiego systemu certyfikacji cyberbezpieczeństwa, pozostają ważne do upływu terminu ich ważności.

4. Państwa członkowskie powiadamiają Komisję i ECCG przed przyjęciem nowych krajowych systemów certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberpostury podmiotów.

5. Komisja może zaproponować państwu członkowskiemu wycofanie krajowego systemu certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberpostury podmiotów, jeżeli zgodnie z art. 73 złożono już wniosek o opracowanie europejskiego systemu certyfikacji cyberbezpieczeństwa obejmującego takie produkty, usługi, procesy lub cyberposturę, z uwzględnieniem planu rozwoju takiego systemu.

Artykuł 87

Międzynarodowe uznawanie europejskich certyfikatów cyberbezpieczeństwa

1. Certyfikaty państw trzecich dotyczące produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberbezpieczeństwa podmiotów mogą zostać uznane, w drodze aktu wykonawczego lub poprzez zawarcie umowy między Unią a danym państwem trzecim lub organizacją międzynarodową, za równoważne z europejskimi certyfikatami cyberbezpieczeństwa, jeżeli wymogi odpowiedniego systemu państwa trzeciego lub systemu organizacji międzynarodowej uznaje się za równoważne z wymogami europejskich systemów certyfikacji cyberbezpieczeństwa. Komisja jest uprawniona do przyjmowania takich aktów wykonawczych. Akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.

2. Akty wykonawcze i umowy, o których mowa w ust. 1, opierają się na warunkach międzynarodowego uznawania europejskich certyfikatów cyberbezpieczeństwa określonych zgodnie z art. 74 ust. 11.

3. Umowy w sprawie uznawania certyfikatów państw trzecich lub certyfikatów organizacji międzynarodowych, o których mowa w ust. 1, są zawierane wyłącznie wtedy, gdy uznają one również europejskie certyfikaty w zakresie cyberbezpieczeństwa za równoważne certyfikatom państw trzecich.

Artykuł 88

Krajowe organy certyfikacji w zakresie cyberbezpieczeństwa

1. Każde państwo członkowskie wyznacza na swoim terytorium co najmniej jeden krajowy organ certyfikacji w dziedzinie cyberbezpieczeństwa lub, za zgodą innego państwa członkowskiego, co najmniej jeden krajowy organ certyfikacji w dziedzinie cyberbezpieczeństwa w tym innym państwie członkowskim, który jest odpowiedzialny za zadania nadzorcze w państwie członkowskim dokonującym wyznaczenia.

2. Każde państwo członkowskie informuje Komisję o tożsamości wyznaczonych krajowych organów certyfikacji w zakresie cyberbezpieczeństwa. W przypadku gdy państwo członkowskie wyznacza więcej niż jeden organ, informuje ono również Komisję o zadaniach przypisanych każdemu z tych organów.

3. Każdy krajowy organ certyfikacji w zakresie cyberbezpieczeństwa jest niezależny od podmiotów, które nadzoruje, pod względem swojej organizacji, decyzji dotyczących finansowania, struktury prawnej i procesu decyzyjnego.

4. Działania krajowych organów certyfikacji w zakresie cyberbezpieczeństwa związane z wydawaniem europejskich certyfikatów cyberbezpieczeństwa na mocy niniejszego rozporządzenia są ściśle oddzielone od ich działań nadzorczych określonych w niniejszym artykule oraz w art. 85 ust. 4 lit. a) i b), a działania te są prowadzone niezależnie od siebie.

5. Państwa członkowskie zapewniają, aby krajowe organy certyfikacji w zakresie cyberbezpieczeństwa dysponowały odpowiednimi zasobami do wykonywania swoich uprawnień i zadań w sposób skuteczny i wydajny.

6. Krajowe organy certyfikacji w zakresie cyberbezpieczeństwa mają następujące zadania:

   a) udział w pracach ECCG zgodnie z art. 90 ust. 2;

   b) nadzorować i egzekwować przepisy zawarte w europejskich systemach certyfikacji cyberbezpieczeństwa zgodnie z art. 81 ust. 2 lit. a), aby zapewnić zgodność produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberbezpieczeństwa podmiotów z wymogami europejskich certyfikatów cyberbezpieczeństwa, które zostały wydane na ich terytoriach, we współpracy z odpowiednimi organami nadzoru rynku lub organami nadzorczymi, w tym właściwymi organami na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555[82] lub rozporządzenia (UE) 2024/2847;

   c) monitorowanie, we współpracy z odpowiednimi organami nadzoru rynku, zgodności z obowiązkami producentów lub dostawców produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiotów, których cyberbezpieczeństwo jest certyfikowane zgodnie z niniejszym rozporządzeniem, które mają siedzibę na ich terytoriach i które przeprowadzają samoocenę zgodności w ramach odpowiedniego europejskiego systemu certyfikacji cyberbezpieczeństwa;

   d) bez uszczerbku dla art. 91 ust. 3, aktywnie pomagać krajowym organom akredytacyjnym lub innym właściwym organom w monitorowaniu i nadzorowaniu działalności organów oceny zgodności do celów niniejszego rozporządzenia;

   e) współpracować z Komisją w przypadku zakwestionowania kompetencji jednostki oceniającej zgodność zgodnie z art. 94;

   f) monitorować i nadzorować działalność organów publicznych, o których mowa w art. 85 ust. 3;

   g) w stosownych przypadkach udzielać upoważnień organom oceny zgodności zgodnie z art. 93, monitorować zgodność organów oceny zgodności z dodatkowymi lub szczególnymi wymogami określonymi w europejskich systemach certyfikacji w zakresie cyberbezpieczeństwa zgodnie z art. 81 ust. 3 lit. f) oraz egzekwować wypełnianie przez nie tych wymogów, a także ograniczać, zawieszać lub cofać istniejące upoważnienia, jeżeli organy oceny zgodności nie spełniają wymogów niniejszego rozporządzenia;

---

[82] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa cybernetycznego 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).

h) rozpatrywać skargi osób fizycznych lub prawnych dotyczące europejskich certyfikatów cyberbezpieczeństwa wydanych przez krajowe organy certyfikacji cyberbezpieczeństwa lub europejskich certyfikatów cyberbezpieczeństwa wydanych przez organy oceny zgodności zgodnie z art. 85 ust. 4 lub dotyczących oświadczeń UE o zgodności z normą międzynarodową ( ) wydanych na podstawie art. 83, badać przedmiot takich skarg w odpowiednim zakresie oraz informować skarżącego o postępach i wynikach badania w rozsądnym terminie;

(i) przedkładać Komisji, ENISA i ECCG roczne sprawozdanie z głównych działań do dnia 31 marca [rok wejścia w życie + 12 miesięcy] każdego roku oraz udostępniać te sprawozdania zespołowi ds. wzajemnej oceny, jeżeli krajowy organ certyfikacji w zakresie cyberbezpieczeństwa podlega wzajemnej ocenie zgodnie z art. 89;

j) współpracować z innymi krajowymi organami certyfikacji w zakresie cyberbezpieczeństwa, organami nadzoru rynku lub innymi organami publicznymi, w tym poprzez wymianę informacji na temat ewentualnej niezgodności produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberpostury podmiotów z wymogami niniejszego rozporządzenia lub z wymogami określonych europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa;

k) monitorowanie istotnych zmian w dziedzinie certyfikacji w zakresie cyberbezpieczeństwa.

7. Każdy krajowy organ certyfikacji w zakresie cyberbezpieczeństwa posiada co najmniej następujące uprawnienia:

a) żądanie od organów oceny zgodności, posiadaczy europejskich certyfikatów cyberbezpieczeństwa i wydawców unijnych oświadczeń o zgodności dostarczenia wszelkich informacji niezbędnych do wykonywania swoich zadań;

b) przeprowadzanie dochodzeń w formie audytów organów oceny zgodności, posiadaczy europejskich certyfikatów cyberbezpieczeństwa i wydawców unijnych oświadczeń o zgodności w celu sprawdzenia, czy spełniają one wymogi określone w niniejszym tytule;

c) podejmowania odpowiednich środków, zgodnie z prawem krajowym, w celu zapewnienia, aby jednostki oceniające zgodność, posiadacze europejskich certyfikatów cyberbezpieczeństwa i wystawcy unijnych oświadczeń o zgodności przestrzegali niniejszego rozporządzenia lub europejskiego systemu certyfikacji cyberbezpieczeństwa;

d) uzyskiwanie dostępu do pomieszczeń organów oceny zgodności lub posiadaczy europejskich certyfikatów cyberbezpieczeństwa w celu przeprowadzenia dochodzeń zgodnie z prawem unijnym lub krajowym prawem proceduralnym;

e) cofnąć, zgodnie z prawem krajowym, europejskie certyfikaty cyberbezpieczeństwa wydane przez krajowe organy certyfikacji cyberbezpieczeństwa lub przez jednostki oceniające zgodność zgodnie z art. 85 ust. 4, jeżeli certyfikaty te nie są zgodne z niniejszym rozporządzeniem lub europejskim systemem certyfikacji cyberbezpieczeństwa;

f) nakładania kar zgodnie z prawem krajowym, zgodnie z art. 97, oraz żądania natychmiastowego zaprzestania naruszania obowiązków określonych w niniejszym rozporządzeniu.

8. Krajowe organy certyfikacji w zakresie cyberbezpieczeństwa współpracują ze sobą oraz z Komisją, w szczególności poprzez wymianę informacji, doświadczeń i dobrych praktyk w zakresie certyfikacji w zakresie cyberbezpieczeństwa oraz kwestii technicznych dotyczących cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa oraz cyberbezpieczeństwa podmiotów.

9 Do dnia [wejścia w życie + 6 miesięcy] ENISA opracowuje wzór sprawozdania, o którym mowa w ust. 6 lit. i) niniejszego artykułu, we współpracy z Komisją i ECCG.

Artykuł 89
Wzajemna ocena

1. Krajowe organy certyfikacji w zakresie cyberbezpieczeństwa podlegają wzajemnej ocenie.

2. Ocena wzajemna przeprowadzana jest w oparciu o rzetelne i przejrzyste kryteria i procedury oceny, w szczególności dotyczące wymagań strukturalnych, kadrowych i proceduralnych, poufności i skarg.

3. W ramach wzajemnej oceny ocenia się:

   a w stosownych przypadkach, czy działania krajowych organów certyfikacji cyberbezpieczeństwa związane z wydawaniem europejskich certyfikatów cyberbezpieczeństwa, o których mowa w niniejszym rozporządzeniu, są ściśle oddzielone od ich działań nadzorczych określonych w art. 88 oraz czy działania te są prowadzone niezależnie od siebie;

   b) procedury nadzorowania i egzekwowania zasad monitorowania zgodności produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberbezpieczeństwa podmiotów posiadających europejskie certyfikaty cyberbezpieczeństwa zgodnie z art. 88 ust. 7 lit. a);

   c) procedury monitorowania i egzekwowania obowiązków producentów lub dostawców produktów ICT, usług ICT, procesów ICT lub zarządzanych usług bezpieczeństwa lub podmiotów, których cyberbezpieczeństwo jest certyfikowane, zgodnie z art. 88 ust. 7 lit. b);

   d) procedury monitorowania, autoryzacji i nadzorowania działalności organów oceny zgodności.

4. Ocena wzajemna jest przeprowadzana co najmniej raz na pięć lat przez co najmniej dwa krajowe organy certyfikacji cyberbezpieczeństwa innych państw członkowskich oraz przez Komisję. ENISA uczestniczy również w ocenie wzajemnej w charakterze obserwatora. Zespół ds. oceny wzajemnej sporządza sprawozdanie końcowe i podsumowanie oceny wzajemnej.

5. ENISA wspiera organizację mechanizmu wzajemnej oceny i wzajemnych ocen, w tym poprzez opracowywanie odpowiednich wytycznych i wzorów we współpracy z Komisją i ECCG.

6. Komisja jest uprawniona do przyjmowania aktów wykonawczych ustanawiających plan wzajemnej oceny obejmujący okres co najmniej pięciu lat, określający kryteria dotyczące składu zespołu ds. wzajemnej oceny, metodologię stosowaną w ramach wzajemnej oceny oraz harmonogram, częstotliwość i inne zadania związane z wzajemną oceną. Przygotowując te akty wykonawcze, Komisja konsultuje się z ECCG

i ENISA. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.

7. Sprawozdanie końcowe, zawierające ewentualne wytyczne lub zalecenia, oraz streszczenie wzajemnej oceny są badane przez ECCG, która zatwierdza streszczenie do publikacji na stronie internetowej, o której mowa w art. 79 ust. 2.

Artykuł 90
Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa

1 Ustanawia się Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa (ECCG).

2 W skład ECCG wchodzą przedstawiciele krajowych organów certyfikacji w dziedzinie cyberbezpieczeństwa lub przedstawiciele innych właściwych organów krajowych. Członek ECCG nie może reprezentować więcej niż dwóch państw członkowskich.

3. ECCG ma następujące zadania:

a) doradzanie Komisji i wspieranie jej w pracach mających na celu zapewnienie spójnego wdrażania i stosowania przepisów określonych w niniejszym tytule, kwestii związanych z polityką certyfikacji w zakresie cyberbezpieczeństwa oraz koordynacji podejść politycznych;

b) doradzanie Komisji i wspieranie jej w przygotowywaniu wniosków dotyczących europejskich systemów certyfikacji cyberbezpieczeństwa zgodnie z art. 73;

c) wspieranie, doradzanie i współpracowanie z ENISA w zakresie przygotowywania systemu kandydującego zgodnie z art. 74 oraz specyfikacji technicznych zgodnie z art. 77;

d) wspieranie, doradzanie i współpracowanie z ENISA i Komisją w zakresie działań związanych z utrzymaniem zgodnie z art. 75;

e) wspieranie Komisji, doradzanie jej i współpraca z nią w zakresie przeglądu lub wycofania istniejących europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa zgodnie z art. 76;

f) wnioskowanie o przedłożenie Komisji wniosku dotyczącego przygotowania kandydackiego europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa zgodnie z art. 73 ust. 2;

g) przyjmowanie opinii skierowanych do Komisji dotyczących utrzymania, przeglądu i wycofania istniejących europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa;

h) analizowanie istotnych zmian w dziedzinie certyfikacji w zakresie cyberbezpieczeństwa, w tym na szczeblu krajowym zgodnie z art. 86, oraz wymiana informacji i dobrych praktyk dotyczących systemów certyfikacji w zakresie cyberbezpieczeństwa;

i) ułatwianie współpracy między krajowymi organami certyfikacji w zakresie cyberbezpieczeństwa zgodnie z zasadami określonymi w niniejszym tytule poprzez budowanie potencjału i wymianę informacji, w szczególności w odniesieniu do kwestii dotyczących certyfikacji w zakresie cyberbezpieczeństwa;

j) wspieranie wdrażania mechanizmu wzajemnej oceny zgodnie z art. 89 oraz mechanizmów wzajemnej oceny zgodnie z zasadami ustanowionymi w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa zgodnie z art. 81 ust. 2 lit. g);

k) ułatwianie dostosowywania europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa do uznanych międzynarodowych norm, w tym w ramach utrzymania istniejących europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, oraz, w stosownych przypadkach, przedstawianie ENISA zaleceń dotyczących współpracy z odpowiednimi europejskimi lub międzynarodowymi organizacjami normalizacyjnymi w celu usunięcia niedociągnięć lub luk w dostępnych normach europejskich lub uznanych międzynarodowych.

4. Komisja, przy wsparciu ENISA, przewodniczy ECCG i zapewnia jej sekretariat.

5. Komisja może powołać podgrupy ECCG w jednym z następujących celów:

a) zbadanie konkretnych kwestii na podstawie zakresu zadań ustalonego przez Komisję;

b) utrzymywanie i przegląd europejskich systemów certyfikacji zgodnie z niniejszym rozporządzeniem i na podstawie zakresu zadań ustalonego przez Komisję.

6. Podgrupy składają sprawozdania ECCG.

7. Podgrupy są współprzewodniczące przez Komisję i ENISA, a sekretariat podgrup zapewnia ENISA.

8. ECCG i jej podgrupy przyjmują regulamin wewnętrzny zwykłą większością głosów swoich członków, na podstawie wniosku Komisji i w porozumieniu z nią.

Sekcja 2
Jednostki oceniające zgodność

Artykuł 91
Kompetencje organów oceny zgodności

1 Jednostki oceniające zgodność są akredytowane przez krajowe jednostki akredytujące wyznaczone zgodnie z rozporządzeniem (WE) nr 765/2008. Akredytacja taka jest wydawana wyłącznie w przypadku, gdy jednostka oceniająca zgodność spełnia wymagania określone w załączniku I do niniejszego rozporządzenia.

2. W przypadku wydania europejskiego certyfikatu cyberbezpieczeństwa przez krajowy organ certyfikacji cyberbezpieczeństwa zgodnie z niniejszym rozporządzeniem, jednostka certyfikująca krajowego organu certyfikacji cyberbezpieczeństwa jest akredytowana jako jednostka oceniająca zgodność zgodnie z ust. 1.

3. Akredytacja, o której mowa w ust. 1, jest wydawana jednostkom oceniającym zgodność na okres maksymalnie pięciu lat i może zostać przedłużona, pod warunkiem że jednostka oceniająca zgodność spełnia wymagania określone w niniejszym artykule. Krajowe jednostki akredytujące podejmują wszelkie odpowiednie środki w rozsądnym terminie w celu ograniczenia, zawieszenia lub cofnięcia akredytacji jednostki oceniającej zgodność wydanej zgodnie z ust. 1, jeżeli warunki akredytacji

nie zostały spełnione lub przestały być spełnione lub jeżeli jednostka oceniająca zgodność nie spełnia wymogów niniejszego rozporządzenia.

4. Przy ustalaniu dodatkowych lub szczególnych wymagań akredytacyjnych dla europejskiego systemu certyfikacji cyberbezpieczeństwa obejmującego produkty ICT, zgodnie z art. 92, w stosownych przypadkach dąży się do osiągnięcia synergii z wymaganiami dotyczącymi jednostek notyfikowanych na mocy rozporządzenia (UE) 2024/2847 oraz wymaganiami akredytacyjnymi na mocy systemów certyfikacji cyberbezpieczeństwa, które zostały już przyjęte.

5. W przypadku gdy jednostka oceniająca zgodność jest akredytowana zgodnie z rozporządzeniem (UE) 2024/2847, właściwe organy mogą ponownie wykorzystać wyniki poprzedniego procesu akredytacji dotyczące wszelkich pokrywających się wymogów jako dowód w procesie akredytacji na mocy niniejszego rozporządzenia.

Artykuł 92

Dodatkowa harmonizacja kompetencji jednostek oceniających zgodność

1. W przypadku gdy europejski system certyfikacji w zakresie cyberbezpieczeństwa określa dodatkowe lub szczególne wymagania zgodnie z art. 81 ust. 3 lit. f), jednostki oceniające zgodność są upoważnione przez krajowy organ certyfikacji w zakresie cyberbezpieczeństwa wyznaczony zgodnie z art. 88 ust. 1 do wykonywania zadań w ramach takiego systemu. Upoważnienie takie wydaje się wyłącznie w przypadku, gdy jednostka oceniająca zgodność została akredytowana i spełnia dodatkowe lub szczególne wymagania określone w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa.

2. W przypadku gdy jednostka oceniająca zgodność występuje o upoważnienie na mocy niniejszego artykułu, przedkłada wniosek krajowemu organowi certyfikacji w zakresie cyberbezpieczeństwa państwa członkowskiego, w którym ma siedzibę, lub krajowemu organowi certyfikacji w zakresie cyberbezpieczeństwa, do którego państwo członkowskie zwróciło się zgodnie z art. 88 ust. 1.

3. Jednostka oceniająca zgodność może zwrócić się o upoważnienie do krajowego organu certyfikacji w zakresie cyberbezpieczeństwa innego niż organ, o którym mowa w ust. 2, w każdej z następujących sytuacji:

   a) gdy krajowy organ certyfikacji w zakresie cyberbezpieczeństwa, o którym mowa w ust. 1, nie wydaje upoważnienia w odniesieniu do działań w zakresie oceny zgodności, których dotyczy wniosek o upoważnienie;

   b) gdy krajowy organ certyfikacji w zakresie cyberbezpieczeństwa, o którym mowa w ust. 1, nie został poddany wzajemnej ocenie zgodnie z art. 89 w odniesieniu do działań w zakresie oceny zgodności, których dotyczy wniosek o upoważnienie.

4. W przypadku gdy krajowy organ certyfikacji w dziedzinie cyberbezpieczeństwa otrzyma wniosek zgodnie z ust. 3, informuje on o tym krajowy organ certyfikacji w dziedzinie cyberbezpieczeństwa państwa członkowskiego, w którym ma siedzibę organ oceny zgodności składający wniosek. W takich przypadkach krajowy organ certyfikacji w dziedzinie cyberbezpieczeństwa tego państwa członkowskiego może uczestniczyć w procesie udzielania upoważnienia w charakterze obserwatora.

5. Krajowy organ certyfikacji w zakresie cyberbezpieczeństwa może zwrócić się do innego krajowego organu certyfikacji w zakresie cyberbezpieczeństwa o

przeprowadzenie części czynności oceny. W takim przypadku certyfikat upoważnienia wydaje organ wnioskujący.

6. Upoważnienie, o którym mowa w ust. 1, jest ważne przez okres nie dłuższy niż okres ważności akredytacji i może zostać odnowione, pod warunkiem że jednostka oceniająca zgodność spełnia wymagania określone w ust. 1, a jej akredytacja również została odnowiona.

7. Krajowe organy certyfikacji w dziedzinie cyberbezpieczeństwa podejmują w rozsądnym terminie wszelkie odpowiednie środki w celu ograniczenia, zawieszenia lub cofnięcia upoważnienia jednostki oceniającej zgodność wydanego zgodnie z ust. 1, jeżeli warunki udzielenia upoważnienia nie są spełnione lub przestały być spełnione lub jeżeli jednostka oceniająca zgodność nie spełnia wymogów niniejszego rozporządzenia.

8. Komisja jest uprawniona do przyjmowania aktów wykonawczych w celu ustanowienia procedur, w tym dotyczących współpracy transgranicznej, w zakresie udzielania upoważnień organom oceny zgodności. W procesie przygotowywania aktów wykonawczych Komisja konsultuje się z ENISA i ECCG. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.

Artykuł 93
Powiadomienie organów oceny zgodności

1. W odniesieniu do każdego europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa krajowe organy certyfikacji w zakresie cyberbezpieczeństwa państwa członkowskiego powiadamiają Komisję i pozostałe państwa członkowskie o jednostkach oceniających zgodność, które zostały akredytowane i, w stosownych przypadkach, upoważnione zgodnie z art. 92.

2 Krajowe organy certyfikacji w zakresie cyberbezpieczeństwa dokonują powiadomienia, o którym mowa w ust. 1, przy użyciu elektronicznego narzędzia do powiadamiania opracowanego i zarządzanego przez Komisję.

3. Komisja jest uprawniona do przyjmowania aktów wykonawczych w celu określenia okoliczności, formatów i procedur powiadamiania, o których mowa w ust. 1 niniejszego artykułu, w tym procedury zgłaszania sprzeciwu przez inne państwa członkowskie w trakcie procesu powiadamiania, niepowtarzalnej identyfikacji organów oceny zgodności, a także okoliczności ograniczenia, zawieszenia lub cofnięcia powiadomienia. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.

Artykuł 94
Zarzuty dotyczące kompetencji jednostek oceniających zgodność

1. Komisja bada wszelkie przypadki, w których ma wątpliwości lub w których powiadomiono ją o wątpliwościach dotyczących kompetencji jednostki oceniającej zgodność w zakresie spełniania lub dalszego spełniania przez tę jednostkę wymagań i obowiązków, którym podlega.

2 Krajowy organ certyfikacji w zakresie cyberbezpieczeństwa przekazuje Komisji, na jej wniosek, wszelkie informacje dotyczące podstawy zgłoszenia lub utrzymania kompetencji danego organu oceny zgodności.

3. Komisja zapewnia poufność wszystkich informacji wrażliwych uzyskanych w trakcie dochodzeń.

4. W przypadku stwierdzenia przez Komisję, że jednostka oceniająca zgodność nie spełnia lub przestała spełniać wymogi dotyczące jej notyfikacji, Komisja informuje o tym krajowy organ certyfikacji cyberbezpieczeństwa i zwraca się do niego o podjęcie niezbędnych środków naprawczych, w tym, w razie potrzeby, o cofnięcie notyfikacji.

5. Państwa członkowskie zapewniają dostępność procedury odwoławczej od decyzji jednostek notyfikowanych.

Artykuł 95

Obowiązek informacyjny i przechowywania danych przez jednostki oceniające zgodność

1. Jednostki oceniające zgodność informują krajowy organ certyfikacji cyberbezpieczeństwa o następujących kwestiach:

   a) wszelkie odmowy, ograniczenia, zawieszenia lub cofnięcia certyfikatu;

   b) wszelkie okoliczności mające wpływ na zakres i warunki powiadomienia, o którym mowa w art. 93 ust. 1;

   c) wszelkie wnioski o udzielenie informacji, które otrzymały od organów nadzoru rynku w odniesieniu do działań związanych z oceną zgodności;

   d) na żądanie, wszelkie działania w zakresie oceny zgodności przeprowadzone w ramach zakresu ich zgłoszenia oraz wszelkie inne działania, w tym działania transgraniczne i podwykonawstwo.

2. Jednostki oceniające zgodność przekazują również ENISA informacje, o których mowa w ust. 1 lit. a), w celu ułatwienia wykonywania zadań ENISA zgodnie z art. 79.

3 Jednostki oceniające zgodność przekazują innym jednostkom oceniającym zgodność objętym niniejszym rozporządzeniem, które prowadzą podobną działalność w zakresie oceny zgodności obejmującą te same produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub podmioty, których cyberbezpieczeństwo jest certyfikowane, bez zbędnej zwłoki odpowiednie informacje dotyczące kwestii związanych z negatywnymi, a na żądanie również pozytywnymi wynikami oceny zgodności.

4. Jednostki oceniające zgodność prowadzą system ewidencji zawierający wszystkie dokumenty i dowody sporządzone lub otrzymane w związku z każdą przeprowadzoną przez nie oceną i certyfikacją. Ewidencja jest przechowywana w bezpieczny i dostępny sposób przez okres niezbędny do celów certyfikacji oraz przez co najmniej pięć lat po wygaśnięciu lub cofnięciu odpowiedniego europejskiego certyfikatu cyberbezpieczeństwa.

Sekcja 3
Inne przepisy

Artykuł 96

Prawo do wniesienia skargi i prawo do skutecznego środka odwoławczego

1. Osoby fizyczne i prawne mają prawo do wniesienia skargi do wydawcy europejskiego certyfikatu cyberbezpieczeństwa lub, w przypadku gdy skarga dotyczy europejskiego

certyfikatu cyberbezpieczeństwa wydanego przez jednostkę oceniającą zgodność działającą zgodnie z art. 85 ust. 4, do właściwego krajowego organu certyfikacji cyberbezpieczeństwa.

2 Organ lub jednostka, do których złożono skargę, informują skarżącego o przebiegu postępowania, podjętej decyzji oraz prawie do skutecznego środka odwoławczego, o którym mowa w ust. 3 i 4.

3. Niezależnie od wszelkich środków administracyjnych lub innych środków pozasądowych osoby fizyczne i prawne mają prawo do skutecznego środka odwoławczego w odniesieniu do:

a) decyzji podjętych przez organ lub podmiot, o których mowa w ust. 1, w tym, w stosownych przypadkach, w odniesieniu do niewłaściwego wydania, niewydania lub uznania europejskiego certyfikatu cyberbezpieczeństwa posiadanego przez te osoby fizyczne i prawne;

b) braku działania w sprawie skargi złożonej do organu lub podmiotu, o których mowa w ust. 1.

4. Postępowania na podstawie niniejszego artykułu toczą się przed sądami państwa członkowskiego, w którym znajduje się organ lub podmiot, przeciwko któremu wniesiono środek odwoławczy.

Artykuł 97
Kary

Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszenia przepisów niniejszego tytułu oraz naruszenia europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa i podejmują wszelkie niezbędne środki w celu zapewnienia ich wykonania. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie niezwłocznie powiadamiają Komisję o tych przepisach i środkach oraz powiadamiają ją o wszelkich późniejszych zmianach mających wpływ na te przepisy i środki.

TYTUŁ IV
BEZPIECZEŃSTWO ŁAŃCUCHÓW DOSTAW TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNYCH

ROZDZIAŁ I
Ramy zaufanego łańcucha dostaw ICT

Artykuł 98
Zakres ram

1 Ramy zaufanego łańcucha dostaw ICT zapewniają mechanizm bezpieczeństwa na poziomie Unii w celu przeciwdziałania ryzyku nietechnicznemu w sektorach o wysokim znaczeniu krytycznym i innych sektorach krytycznych, o których mowa w dyrektywie (UE) 2022/2555. Mechanizm ten określa kluczowe aktywa ICT w krytycznych łańcuchach dostaw ICT oraz ustanawia odpowiednie i proporcjonalne środki ograniczające ryzyko w odniesieniu do podmiotów, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555.

2. Obowiązki określone w niniejszym tytule pozostają bez uszczerbku dla obowiązków określonych w art. 13 rozporządzenia (UE) 2024/2847 oraz w przepisach krajowych transponujących art. 21 dyrektywy (UE) 2022/2555.

3. Przepisy niniejszego rozdziału nie wykluczają możliwości przyjęcia lub utrzymania przez państwa członkowskie przepisów zapewniających wyższy poziom cyberbezpieczeństwa w łańcuchach dostaw ICT, pod warunkiem że przepisy te są zgodne z ich zobowiązaniami wynikającymi z prawa Unii.

Artykuł 99
Oceny ryzyka bezpieczeństwa

1. Komisja lub grupa co najmniej trzech państw członkowskich może zwrócić się do grupy ds. współpracy ustanowionej na mocy art. 14 dyrektywy (UE) 2022/2555 („grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji") o przeprowadzenie skoordynowanej na poziomie Unii oceny ryzyka dla bezpieczeństwa zgodnie z art. 22 tej dyrektywy. W przypadku przeprowadzenia oceny ryzyka dla bezpieczeństwa na wniosek, ocena ta obejmuje w szczególności proponowaną identyfikację kluczowych aktywów ICT danego łańcucha dostaw ICT, a także głównych podmiotów stanowiących zagrożenie, ryzyka i słabe punkty mające wpływ na te aktywa. W ramach skoordynowanych ocen ryzyka dla bezpieczeństwa na poziomie Unii opracowuje się scenariusze ryzyka i proponuje środki mające na celu ograniczenie zidentyfikowanych zagrożeń.

2. Skoordynowane oceny ryzyka w zakresie bezpieczeństwa na poziomie Unii są przeprowadzane w ciągu sześciu miesięcy od złożenia wniosku, o którym mowa w ust. 1. Na wniosek Komisji grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji może uzgodnić krótszy termin.

3. Jeżeli Komisja ma wystarczające powody, aby sądzić, że istnieje poważne zagrożenie cybernetyczne dla bezpieczeństwa Unii w odniesieniu do łańcucha dostaw ICT i że konieczne jest podjęcie działań w celu zachowania prawidłowego funkcjonowania rynku wewnętrznego, Komisja niezwłocznie:

   a) konsultuje się z państwami członkowskimi w sprawie konieczności podjęcia jednego lub kilku środków łagodzących, o których mowa w art. 103; oraz

   b) przeprowadza ocenę ryzyka dla bezpieczeństwa, uwzględniając konsultacje z państwami członkowskimi. Ocena ryzyka dla bezpieczeństwa obejmuje proponowaną identyfikację kluczowych aktywów ICT, a także głównych podmiotów stanowiących zagrożenie, ryzyka i słabe punkty mające wpływ na te aktywa. W ramach oceny ryzyka dla bezpieczeństwa opracowuje się scenariusze ryzyka i proponuje środki mające na celu ograniczenie zidentyfikowanych rodzajów ryzyka.

Artykuł 100
Wyznaczenie państw trzecich budzących obawy w zakresie cyberbezpieczeństwa

1. Jeżeli w wyniku oceny ryzyka dla bezpieczeństwa, o której mowa w art. 99, lub na podstawie innych źródeł, takich jak publiczne oświadczenie w imieniu Unii lub państwa członkowskiego, okaże się, że państwo trzecie stwarza poważne i strukturalne ryzyko nietechniczne dla łańcuchów dostaw ICT, Komisja weryfikuje ryzyko stwarzane przez to państwo, uwzględniając następujące elementy:

a) istnienie w państwie trzecim przepisów wymagających od podmiotów podlegających jego jurysdykcji zgłaszania organom tego państwa trzeciego informacji o lukach w oprogramowaniu lub sprzęcie komputerowym, zanim zostanie stwierdzone, że luki te zostały wykorzystane;

b) istniejące w państwie trzecim praktyki, potwierdzone przez niezależne źródła, które wymagają od podmiotów podlegających jurysdykcji tego państwa trzeciego zgłaszania organom tego państwa trzeciego informacji o lukach w oprogramowaniu lub sprzęcie komputerowym, zanim zostanie stwierdzone, że luki te zostały wykorzystane;

c) brak skutecznych środków prawnych oraz niezależnych i demokratycznych mechanizmów kontroli, które mogłyby zaradzić stwierdzonym problemom w zakresie bezpieczeństwa, w tym problemom związanym z istniejącymi praktykami, o których mowa w lit. b);

d) potwierdzone informacje o jednym lub kilku incydentach związanych z podmiotami stanowiącymi zagrożenie, kontrolowanymi z tego kraju i działającymi z terytorium tego kraju, prowadzącymi złośliwe działania lub kampanie cybernetyczne, oraz brak zdolności lub chęci państwa trzeciego do współpracy z Komisją lub państwami członkowskimi w celu przeciwdziałania ryzyku wynikającemu z działalności takich podmiotów stanowiących zagrożenie;

e) istotne informacje pochodzące ze skoordynowanych na szczeblu unijnym ocen ryzyka bezpieczeństwa lub sprawozdań państw członkowskich lub organizacji międzynarodowych.

2. Jeżeli po przeprowadzeniu weryfikacji, o której mowa w ust. 1, Komisja stwierdzi, że państwo trzecie stwarza poważne i strukturalne zagrożenia nietechniczne dla łańcuchów dostaw ICT, może ona w drodze aktu wykonawczego uznać to państwo trzecie za państwo stwarzające zagrożenie dla cyberbezpieczeństwa łańcuchów dostaw ICT. Akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.

3. Komisja regularnie dokonuje przeglądu aktów wykonawczych przyjętych zgodnie z ust. 2.

4. Dostawcy wysokiego ryzyka nie są uprawnieni do:

a) uczestniczenia w opracowywaniu, ocenie, konsultacjach lub podejmowaniu decyzji dotyczących norm europejskich i wyników normalizacji europejskiej, o których mowa w art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012, oraz wspólnych specyfikacji, o których mowa w art. 27 rozporządzenia (UE) nr 2024/2847, w dziedzinie cyberbezpieczeństwa;

b) ubiegania się o europejskie certyfikaty w zakresie cyberbezpieczeństwa zgodnie z tytułem III lub bycia posiadaczem takich certyfikatów;

c) uzyskać akredytację jako jednostka oceniająca zgodność zgodnie z tytułem III;

d) ubiegać się o status autoryzowanego dostawcy europejskich poświadczeń indywidualnych umiejętności w zakresie cyberbezpieczeństwa zgodnie z tytułem II sekcja 4;

e) uczestniczyć w procedurach udzielania zamówień publicznych, organizowanych zgodnie z przepisami transponującymi dyrektywy 2014/24/UE i 2014/25/UE w

odniesieniu do dostarczania komponentów ICT lub komponentów zawierających komponenty ICT, które mają być wykorzystywane w kluczowych zasobach ICT określonych zgodnie z art. 102;

f) uczestniczyć w działaniach w ramach programów i instrumentów finansowych Unii realizowanych w ramach zarządzania bezpośredniego i pośredniego zgodnie z art. 136 rozporządzenia (UE, Euratom) nr 2024/2509 i przepisami sektorowymi Unii, a także w działaniach finansowych Unii realizowanych w ramach zarządzania dzielonego w odniesieniu do dostarczania komponentów ICT lub komponentów zawierających komponenty ICT, które mają być wykorzystywane w kluczowych zasobach ICT określonych zgodnie z art. 102.

Organy odpowiedzialne za procedury, o których mowa w lit. a)–f), przeprowadzają oceny niezbędne do celów niniejszego ustępu. Organy te mogą również opierać się w tym celu na wykazie, o którym mowa w art. 104.

5. W przypadkach, gdy dostawca wysokiego ryzyka uzyskał już europejski certyfikat cyberbezpieczeństwa zgodnie z tytułem III, właściwy organ cofa go bez zbędnej zwłoki.

Artykuł 101
Ogólny mechanizm bezpieczeństwa łańcucha dostaw ICT

W przypadku gdy grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji przeprowadziła skoordynowaną ocenę ryzyka bezpieczeństwa na poziomie Unii zgodnie z art. 99 ust. 1 niniejszego rozporządzenia lub po zakończeniu procedury w przypadku znaczącego zagrożenia cybernetycznego zgodnie z art. 99 ust. 3 dla łańcucha dostaw ICT, Komisja może podjąć środki przewidziane w art. 102 i art. 103 ust. 1 i 2.

Artykuł 102
Identyfikacja kluczowych aktywów ICT

1. Jeżeli ocena ryzyka przeprowadzona zgodnie z art. 99 ust. 1 lub 3 wskazuje na istotne zagrożenia dla cyberbezpieczeństwa w odniesieniu do łańcucha dostaw ICT, Komisja jest uprawniona do przyjęcia aktów wykonawczych określających kluczowe aktywa ICT wykorzystywane do wytwarzania produktów lub świadczenia usług przez podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555 . Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2 niniejszego rozporządzenia.

2. Przy określaniu kluczowych aktywów ICT, o których mowa w ust. 1, Komisja uwzględnia następujące elementy:

a) czy aktywa te pełnią funkcje istotne i wrażliwe dla funkcjonowania produktów wytwarzanych lub usług świadczonych przez podmiot typu, o którym mowa w załącznikach I i II do dyrektywy (UE) 2022/2555;

b) czy incydenty, w tym spowodowane wykorzystaniem luk w zabezpieczeniach tych aktywów, mogą prowadzić do poważnych zakłóceń w łańcuchach dostaw ICT na rynku wewnętrznym lub do wycieku danych;

c) czy istnieje zależność od ograniczonej liczby dostawców tych aktywów;

d) wyniki ocen ryzyka, o których mowa w art. 99.

Artykuł 103
Środki ograniczające ryzyko w łańcuchu dostaw ICT

1. Komisja jest uprawniona do przyjmowania aktów wykonawczych ustanawiających, w razie konieczności w celu zapewnienia wysokiego poziomu cyberbezpieczeństwa, odporności cybernetycznej i zaufania w Unii, że określonym rodzajom podmiotów, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, zabrania się stosowania, instalowania lub integrowania w jakiejkolwiek formie komponentów ICT lub komponentów zawierających komponenty ICT pochodzących od dostawców wysokiego ryzyka, określonych zgodnie z art. 104, w kluczowych zasobach ICT określonych zgodnie z art. 102. W takich aktach wykonawczych przewiduje się odpowiednie okresy przejściowe, podczas których Komisja publikuje wykaz dostawców wysokiego ryzyka, o których mowa w art. 104, a także dodatkowe okresy na wycofanie odpowiednich komponentów ICT i komponentów zawierających komponenty ICT. W takim akcie wykonawczym można również określić te komponenty ICT lub komponenty zawierające komponenty ICT.

2. Komisja jest uprawniona do przyjmowania aktów wykonawczych ustanawiających, w razie konieczności w celu zapewnienia wysokiego poziomu cyberbezpieczeństwa, odporności cybernetycznej i zaufania w Unii, że określone rodzaje podmiotów, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, podlegają jednemu lub kilku z następujących środków ograniczających ryzyko w odniesieniu do ich łańcucha dostaw ICT, a w szczególności kluczowych aktywów ICT określonych zgodnie z art. 102, w celu ograniczenia ryzyka zidentyfikowanego w ocenach ryzyka bezpieczeństwa przeprowadzonych zgodnie z art. 99:

   a) stosowanie wymogów dotyczących przejrzystości w odniesieniu do przekazywania właściwym organom informacji o dostawcach w łańcuchu dostaw ICT dla kluczowych aktywów ICT wyznaczonych zgodnie z art. 102;

   b) zakaz przekazywania danych do państw trzecich i zdalnego przetwarzania danych z państwa trzeciego;

   c) środki techniczne podlegające audytowi przeprowadzanemu przez stronę trzecią, w tym:

      (i) wykorzystanie przetwarzania w urządzeniu;

      (ii) szczególną segmentację systemów sieciowych;

      (iii) uniemożliwienie zdalnego lub fizycznego dostępu do kluczowych zasobów ICT;

      (iv) wyłączenie zbędnych funkcji;

      (v) monitorowanie operacyjne sieci;

      (vi) testowanie sprzętu i oprogramowania.

   (d) ograniczenia związane z kontrolą operacyjną, w tym outsourcing funkcji organizacyjnych do dostawców usług zarządzanych;

   (e) ograniczenia związane z relacjami umownymi podmiotu z dostawcami;

   (f) wymóg, aby usługa była świadczona, zarządzana, utrzymywana lub wspierana przez personel sprawdzony przez właściwe krajowe organy;

   g) dywersyfikacja dostaw komponentów ICT lub komponentów wchodzących w skład komponentów ICT.

3. Wprowadzając środki, o których mowa w ust. 2, Komisja może określić wymagania techniczne i metodologiczne dotyczące tych środków.

4. Przed przyjęciem aktów wykonawczych, o których mowa w ust. 1 i 2, Komisja ocenia potencjalne ryzyka i zależności, a w szczególności:

   a) w stosownych przypadkach, poziom ryzyka związanego z wykorzystaniem, instalacją lub integracją, w jakiejkolwiek formie, komponentów ICT lub komponentów zawierających komponenty ICT pochodzących od dostawców wysokiego ryzyka w kluczowych zasobach ICT;

   b) potencjalny wpływ gospodarczy i społeczny, jaki obowiązek ten może mieć na podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555;

   c) dostępność dostawców alternatywnych w stosunku do dostawców wysokiego ryzyka;

   d) potencjalne zakłócenia transgranicznej działalności gospodarczej i społecznej spowodowane incydentem mającym wpływ na łańcuch dostaw ICT podmiotu.

5. Akty wykonawcze, o których mowa w ust. 1 i 2 niniejszego artykułu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2, i poddaje się przeglądowi co najmniej co 36 miesięcy.

6. W wyjątkowych okolicznościach, które uzasadniają interwencję w celu zachowania prawidłowego funkcjonowania rynku wewnętrznego, oraz w przypadku gdy Komisja ma wystarczające powody, aby uznać, że wykorzystanie, instalacja lub integracja komponentów ICT lub komponentów zawierających komponenty ICT pochodzących od określonego podmiotu mającego siedzibę w państwie trzecim lub kontrolowanego przez państwo trzecie lub od podmiotów z państwa trzeciego lub od obywatela państwa trzeciego stanowi istotne nietechniczne zagrożenie dla cyberbezpieczeństwa działalności gospodarczej lub społecznej co najmniej trzech państw członkowskich, Komisja niezwłocznie konsultuje się z państwami członkowskimi w sprawie konieczności podjęcia środków na szczeblu unijnym.

7. Komisja jest uprawniona do przyjmowania aktów wykonawczych w celu ustalenia, że określonym rodzajom podmiotów, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, zabrania się stosowania, instalowania lub integrowania komponentów ICT lub komponentów zawierających komponenty ICT pochodzących od podmiotu, o którym mowa w ust. 6. W tym celu konsultuje się z podmiotami, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, które mogą być objęte zakazem. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2. W stosownych przypadkach obejmują one odpowiednie okresy na wycofanie tych komponentów ICT lub komponentów zawierających komponenty ICT. W takim akcie wykonawczym można również określić te komponenty ICT lub komponenty zawierające komponenty ICT, które podlegają zakazowi. Zakaz ten dotyczy również komponentów ICT lub komponentów zawierających komponenty ICT pochodzących od wszystkich podmiotów kontrolowanych przez konkretny podmiot, o którym mowa w ust. 6.

8. Akty wykonawcze, o których mowa w ust. 1, 2 i 7, mogą również określać, że środki łagodzące mają zastosowanie wyłącznie do rodzajów podmiotów, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, o określonej wielkości.

9. Artykuł 100 ust. 4 ma zastosowanie do określonego podmiotu mającego siedzibę w państwie trzecim lub kontrolowanego przez państwo trzecie lub podmiot z państwa trzeciego lub obywatela państwa trzeciego, o którym mowa w ust. 7.

10 Akty wykonawcze przyjęte zgodnie z ust. 1, 2 i 7, które mają zastosowanie do rodzajów podmiotów, o których mowa w załączniku I pkt 10 do dyrektywy (UE) 2022/2555, stosuje się odpowiednio do instytucji, organów, urzędów i agencji europejskich.

Artykuł 104
Identyfikacja dostawców wysokiego ryzyka

1. W drodze aktów wykonawczych Komisja ustanawia wykazy dostawców wysokiego ryzyka, których dotyczą zakazy określone w aktach wykonawczych przyjętych zgodnie z art. 103 ust. 1, art. 103 ust. 7 lub zakazem, o którym mowa w art. 111 ust. 1.

2 W tym celu Komisja sporządza mapę dostawców dostarczających komponenty ICT oraz komponenty zawierające komponenty ICT, które są istotne dla zakazu, o którym mowa w ust. 1.

Na tej podstawie Komisja dokonuje wstępnej oceny w celu ustalenia, którzy z zidentyfikowanych dostawców są potencjalnie mającymi siedzibę w państwie trzecim wyznaczonym zgodnie z art. 100 lub kontrolowani przez takie państwo trzecie, przez podmiot mający siedzibę w takim państwie trzecim lub przez obywatela takiego państwa trzeciego. Komisja dokonuje również wstępnej identyfikacji dostawców potencjalnie kontrolowanych przez podmiot, o którym mowa w art. 103 ust. 6.

3. Komisja ocenia miejsce siedziby oraz strukturę własnościową i kontrolną dostawców wstępnie zidentyfikowanych zgodnie z ust. 2 akapit drugi.

4. Do celów oceny, o której mowa w ust. 3, Komisja jest uprawniona do żądania od dostawców niezbędnych informacji. W przypadku gdy dostawca nie dostarczy niezbędnych informacji w wyznaczonym terminie, Komisja może stwierdzić, że dostawca ma siedzibę w państwie trzecim wyznaczonym zgodnie z art. 100 lub jest kontrolowany przez takie państwo trzecie, przez podmioty z tego państwa trzeciego lub przez obywateli takiego państwa trzeciego. W przypadku gdy Komisja przeprowadza ocenę do celów art. 103 ust. 7, a dostawca nie dostarczy niezbędnych informacji w wyznaczonym terminie, Komisja może stwierdzić, że dostawca jest kontrolowany przez podmiot wyznaczony zgodnie z tym artykułem. Właściwe organy, o których mowa w art. 112, również przekazują Komisji na jej wniosek odpowiednie informacje.

5. Komisja przekazuje zainteresowanemu dostawcy wstępne ustalenia dotyczące oceny siedziby, kontroli i własności. Komisja zapewnia dostawcy możliwość przedstawienia uwag na temat tych wstępnych ustaleń.

6. Komisja może zwrócić się do właściwego organu o przeprowadzenie wstępnej oceny ustanowienia, własności i kontroli dostawcy, jeżeli jest to uzasadnione ze względu na charakter działalności tego dostawcy. Właściwy organ może zaproponować dostawcy przeprowadzenie takiej wstępnej oceny. Komisja weryfikuje te wstępne ustalenia w celu podjęcia decyzji, czy dostawca powinien zostać umieszczony w wykazie dostawców wysokiego ryzyka.

7. Komisja regularnie aktualizuje wykaz dostawców wysokiego ryzyka w celu usunięcia lub dodania dostawców wysokiego ryzyka. Dostawcy wysokiego ryzyka ujęci w wykazie mogą zwrócić się do Komisji o ponowną ocenę ich struktury własnościowej, kontroli i siedziby po przedstawieniu dowodów potwierdzających istotne zmiany.

8. W przypadku gdy właściwy organ dowie się, w tym na podstawie informacji przekazanych przez podmiot, o którym mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, że dostawca może wymagać umieszczenia w wykazie dostawców wysokiego ryzyka, informuje o tym bez zbędnej zwłoki Komisję.

Artykuł 105

Zwolnienie dla podmiotów mających siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowanych przez takie podmioty

1. Podmiot mający siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowany przez podmioty z takiego państwa, wyznaczony zgodnie z art. 100, może zwrócić się do Komisji z uzasadnionym wnioskiem o zwolnienie:

   (a) od zakazu nałożonego na podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, dotyczącego wykorzystywania, instalowania lub integrowania w jakiejkolwiek formie swoich komponentów ICT lub komponentów zawierających swoje komponenty ICT w kluczowych zasobach ICT tych podmiotów, w drodze odstępstwa od art. 111 lub aktów wykonawczych przyjętych na podstawie art. 103 ust. 1;

   b) od zakazu udziału w procedurach udzielania zamówień publicznych, organizowanych zgodnie z przepisami transponującymi dyrektywę 2014/24/UE i dyrektywę 2014/25/UE w odniesieniu do dostarczania komponentów ICT lub komponentów zawierających komponenty ICT, które mają być wykorzystywane w kluczowych zasobach ICT określonych zgodnie z art. 102, w drodze odstępstwa od art. 100 ust. 4.

2. Wniosek, o którym mowa w ust. 1, powinien:

   a) określać interes podmiotu mającego siedzibę w państwie trzecim lub kontrolowanego przez podmioty z państwa trzeciego budzącego obawy w zakresie cyberbezpieczeństwa, wyznaczonego zgodnie z art. 100, w uzyskaniu zwolnienia, o którym mowa w ust. 1 niniejszego artykułu; oraz

   b) wykazywać na podstawie jasnych dowodów, że zostaną wprowadzone skuteczne środki łagodzące w celu wyeliminowania ryzyka nietechnicznego i zapewnienia braku jakiejkolwiek możliwości wywierania nieuzasadnionej ingerencji przez państwo trzecie wyznaczone zgodnie z art. 100 w odniesieniu do dostarczania komponentów ICT lub komponentów zawierających komponenty ICT do użytku, instalacji lub integracji w kluczowych zasobach ICT podmiotu, o którym mowa w załącznikach I i II do dyrektywy (UE) 2022/2555.

3. Komisja jest uprawniona do przyjmowania aktów wykonawczych w celu dalszego określenia warunków, o których mowa w ust. 2 lit. b), oraz do ustanowienia szczegółowych zasad dotyczących procedur, o których mowa w niniejszym artykule. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.

4. Komisja ocenia wniosek, o którym mowa w ust. 1, w ramach sprawiedliwego i przejrzystego procesu, biorąc pod uwagę:

   a) okoliczności i dodatkowe elementy, o których mowa w art. 100 ust. 1 i 2, w odniesieniu do wyznaczonego kraju stwarzającego zagrożenie dla cyberbezpieczeństwa łańcuchów dostaw ICT, w którym podmiot ma siedzibę lub z którego jest kontrolowany;

   b) skuteczność środków łagodzących, o których mowa w ust. 2 lit. b);

   c) czy zwolnienie podmiotu mającego siedzibę w państwie trzecim lub kontrolowanego przez podmioty z państwa trzeciego, które budzi obawy dotyczące cyberbezpieczeństwa łańcuchów dostaw ICT, nie byłoby szkodliwe dla interesów Unii.

5. Jeżeli po dokonaniu oceny, o której mowa w ust. 3, Komisja stwierdzi, że przyznanie zwolnienia jest uzasadnione, podejmuje decyzję w tej sprawie i powiadamia o niej wnioskodawcę w terminie dziewięciu miesięcy od otrzymania wniosku.

6. Przyjmując decyzję, o której mowa w ust. 4, Komisja może ograniczyć zwolnienie do określonego okresu i może uzależnić zwolnienie od spełnienia przez podmiot określonych warunków, w tym:

   a) harmonogram wdrożenia środków łagodzących, o których mowa w ust. 2 lit. b);

   b) regularne audyty przeprowadzane przez strony trzecie w celu zapewnienia skutecznego wdrożenia środków łagodzących;

   c) obowiązki sprawozdawcze dotyczące zgodności.

7. Jeżeli po dokonaniu oceny zgodnie z ust. 3 Komisja stwierdzi, że nie ma uzasadnienia dla przyznania zwolnienia, podejmuje decyzję w tej sprawie i powiadamia o tym wnioskodawców w terminie dziewięciu miesięcy od otrzymania wniosku.

8. Komisja może z własnej inicjatywy wycofać lub zmienić decyzję, o której mowa w ust. 4, w jednej lub kilku z następujących sytuacji:

   a) nastąpiła istotna zmiana w stanie faktycznym, na którym oparto decyzję;

   b) podmiot, który wystąpił o zwolnienie, działa w sposób sprzeczny ze swoimi zobowiązaniami;

   c) zwolnienie zostało udzielone na podstawie niekompletnych, nieprawidłowych lub wprowadzających w błąd informacji przekazanych przez podmiot składający wniosek.

Artykuł 106
Prawa do obrony

Komisja zapewnia, aby przed przyjęciem aktu wykonawczego na mocy art. 103 ust. 7 lub przed przyjęciem decyzji odmawiającej przyznania zwolnienia na mocy art. 105 ust. 7 na podstawie elementów nieprzedłożonych przez wnioskodawcę lub przed wycofaniem decyzji na mocy art. 105 ust. 8 zainteresowany podmiot miał możliwość przedstawienia swojego stanowiska, z uwzględnieniem konieczności zastosowania w niektórych przypadkach trybu pilnego.

Artykuł 107
Rejestr

Komisja prowadzi publicznie dostępny rejestr swoich decyzji, o których mowa w art. 105 ust. 5. W rejestrze tym podaje się nazwy podmiotów, których dotyczą takie decyzje. Komisja regularnie aktualizuje rejestr.

Artykuł 108
Poufność

Informacje otrzymane przez Komisję zgodnie z art. 105 i 106 są wykorzystywane wyłącznie do celów, dla których zostały uzyskane.

Artykuł 109
Opłaty

1. Komisja pobiera opłaty za wnioski złożone zgodnie z art. 105 ust. 1.
2. Opłaty są wyrażane i płatne w euro.
3. Opłaty są proporcjonalne do kosztów związanych z rozpatrywaniem wniosków, o których mowa w art. 105 ust. 1, oceną kryteriów i informacji, o których mowa w art. 105 ust. 2, oraz utworzeniem, prowadzeniem i funkcjonowaniem rejestru, o którym mowa w art. 107. Wszystkie wydatki Komisji związane z personelem zaangażowanym w te działania są uwzględniane w tych kosztach.
4. Komisja przyjmuje akty wykonawcze ustanawiające szczegółowe zasady dotyczące opłat, określające wysokość opłat i sposób ich uiszczania. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.

ROZDZIAŁ II
Łańcuchy dostaw ICT w sieciach łączności elektronicznej

Artykuł 110
Kluczowe aktywa ICT dla sieci łączności elektronicznej ruchomej, stacjonarnej i satelitarnej

1. Kluczowe aktywa ICT dla sieci łączności elektronicznej ruchomej, stacjonarnej i satelitarnej są określone w załączniku II.
2. Komponenty ICT lub komponenty zawierające komponenty ICT dostarczane przez dostawców wysokiego ryzyka są stopniowo wycofywane z kluczowych aktywów ICT sieci łączności elektronicznej, w tym sieci komórkowych, stacjonarnych i satelitarnych.
3. Okres wycofywania elementów ICT lub elementów zawierających elementy ICT dostarczanych przez dostawców wysokiego ryzyka w odniesieniu do sieci łączności elektronicznej to nie może przekraczać 36 miesięcy od opublikowania wykazu dostawców wysokiego ryzyka, o którym mowa w art. 104, mającego zastosowanie do sieci łączności elektronicznej.
4. Komisja jest uprawniona do przyjmowania aktów wykonawczych zgodnie z art. 118 ust. 2 w celu określenia terminów wycofania komponentów ICT lub komponentów zawierających komponenty ICT dostarczanych przez dostawców wysokiego ryzyka w odniesieniu do stacjonarnych i satelitarnych sieci łączności elektronicznej.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 119 w celu zmiany załącznika II do niniejszego rozporządzenia w celu dostosowania go do rozwoju technologicznego, z uwzględnieniem elementów, o których mowa w art. 103 ust. 4.

Artykuł 111

Zakazy dotyczące sieci łączności elektronicznej ruchomej, stacjonarnej i satelitarnej

1. Dostawcy mobilnych, stacjonarnych i satelitarnych sieci łączności elektronicznej nie mogą wykorzystywać, instalować ani integrować w jakiejkolwiek formie komponentów ICT lub komponentów zawierających komponenty ICT pochodzących od dostawców wysokiego ryzyka w ramach eksploatacji kluczowych aktywów ICT, o których mowa w załączniku II.

2. W przypadkach, gdy właściwy organ wyznaczony na mocy niniejszego rozporządzenia w państwie członkowskim różni się od właściwego organu zgodnie z rozporządzeniem (UE) XX/XXXX [wniosek DNA], właściwy organ wyznaczony na mocy niniejszego rozporządzenia niezwłocznie informuje właściwy organ zgodnie z rozporządzeniem (UE) XX/XXXX [wniosek DNA] o środkach nałożonych na dostawców sieci łączności elektronicznej, w tym sieci komórkowych, stacjonarnych i satelitarnych, zgodnie z art. 114. Organy zapewniają ścisłą współpracę w celu skutecznego nadzorowania i egzekwowania tych środków.

ROZDZIAŁ III

Właściwe organy, nadzór i egzekwowanie, jurysdykcja, prawo do obrony

Artykuł 112

Właściwe organy

1. Każde państwo członkowskie wyznacza właściwe organy, o których mowa w art. 8 dyrektywy (UE) 2022/2555, jako organy odpowiedzialne za podejmowanie środków nadzoru i egzekwowania, o których mowa w art. 114.

2 Właściwe organy są całkowicie bezstronne pod względem strukturalnym i funkcjonalnym oraz wolne od wszelkich wpływów zewnętrznych, bezpośrednich lub pośrednich; w szczególności nie zwracają się one o instrukcje do żadnego innego organu publicznego ani podmiotu prywatnego ani nie przyjmują takich instrukcji.

3. Państwa członkowskie zapewniają, aby ich właściwe organy dysponowały odpowiednimi uprawnieniami, wystarczającymi zasobami ludzkimi i technicznymi oraz odpowiednią wiedzą fachową, aby skutecznie wykonywać środki nadzoru i egzekwowania, o których mowa w art. 114.

4. Każde państwo członkowskie bez zbędnej zwłoki powiadamia Komisję o nazwach właściwych organów wyznaczonych zgodnie z ust. 1, o odpowiednich zadaniach tych organów oraz o wszelkich późniejszych zmianach w tym zakresie. Każde państwo członkowskie podaje również do wiadomości publicznej nazwy właściwych organów wyznaczonych zgodnie z ust. 1.

Artykuł 113
Sieć współpracy i usług wsparcia Komisji

W celu zapewnienia skutecznego nadzoru Komisja ustanawia sieć współpracy właściwych organów państw członkowskich, o których mowa w art. 112, oraz Komisji, która służy jako platforma współpracy i wymiany informacji, w szczególności do celów ustanowienia, kontroli i oceny własności, o których mowa w art. 104. Komisja zapewnia wsparcie administracyjne dla sieci.

Artykuł 114
Środki nadzorcze i egzekucyjne

1. Właściwe organy, o których mowa w art. 112, są uprawnione do podejmowania środków nadzoru i egzekwowania wobec podmiotów, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555. Państwa członkowskie zapewniają, aby wyżej wymienione środki były skuteczne, proporcjonalne i odstraszające, z uwzględnieniem okoliczności każdego indywidualnego przypadku. Państwa członkowskie powiadamiają Komisję o przepisach przyjętych w tym celu oraz o ich późniejszych zmianach.

2. Wykonując zadania nadzorcze w odniesieniu do podmiotów, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, właściwe organy są uprawnione do poddania tych podmiotów następującym środkom:

   a) wnioskom o przedstawienie szczegółowego i aktualnego wykazu ich odpowiednich dostawców i usługodawców;

   b) wnioski o dostęp do danych, dokumentów i informacji niezbędnych do sprawdzenia zgodności z niniejszym rozporządzeniem;

   c) kontrole na miejscu i nadzór poza siedzibą, w tym wyrywkowe kontrole przeprowadzane przez przeszkolonych specjalistów;

   d wnioski dotyczące składu produktów sprzętowych lub oprogramowania zainstalowanych lub zintegrowanych w jakiejkolwiek formie z siecią lub systemem, w tym komponentów i zależności przejściowych, w powszechnie używanym formacie nadającym się do odczytu maszynowego.

3. Wykorzystując swoje uprawnienia wykonawcze w odniesieniu do podmiotów, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, właściwe organy są uprawnione do:

   a) wydawać ostrzeżenia dotyczące naruszeń niniejszego rozporządzenia przez zainteresowane podmioty, określając istotne fakty i kwestie prawne;

   b) przyjmować decyzje nakładające na zainteresowane podmioty obowiązek usunięcia naruszenia niniejszego rozporządzenia lub nieprawidłowości stwierdzonych w zakresie wdrażania środków łagodzących;

   c) nakazać zainteresowanym podmiotom zaprzestanie działań naruszających niniejsze rozporządzenie i powstrzymanie się od powtarzania takich działań; oraz

   d) nakładać kary zgodnie z przepisami dotyczącymi kwot określonych w art. 115 lub wnioskować o nałożenie takich kar przez właściwe organy, sądy lub trybunały zgodnie z prawem krajowym.

4. Podejmując środki egzekucyjne, o których mowa w poprzednim ustępie, właściwe organy uwzględniają okoliczności każdej sprawy z osobna i biorą pod uwagę następujące czynniki:

a) wagę naruszenia i znaczenie przepisów, które zostały naruszone;

b) czas trwania naruszenia;

c) obroty podmiotu, którego dotyczy naruszenie;

(d) wszelkie istotne wcześniejsze naruszenia przepisów przez dany podmiot;

e) w stosownych przypadkach wszelkie szkody materialne lub niematerialne spowodowane naruszeniem, w tym wszelkie straty finansowe lub gospodarcze, skutki dla innych podmiotów oraz liczba użytkowników, których dotyczy naruszenie;

f) wszelkie zamiary lub zaniedbania ze strony danego podmiotu;

g) wszelkie środki podjęte przez podmiot w celu zapobieżenia lub złagodzenia szkód materialnych lub niematerialnych;

h) poziom współpracy z właściwymi organami osób fizycznych lub prawnych uznanych za odpowiedzialne.

Do celów lit. a) akapitu pierwszego za poważne naruszenie uznaje się:

(i) powtarzające się naruszenia;

j) niepowiadomienie o istotnych incydentach lub niepodjęcie działań naprawczych w związku z nimi;

k) nieusunięcie nieprawidłowości pomimo wiążących instrukcji wydanych przez właściwe organy.

5. Właściwe organy powiadamiają zainteresowane podmioty o swoich wstępnych ustaleniach przed podjęciem środków egzekucyjnych. Zainteresowanym podmiotom przyznaje się rozsądny termin na zgłoszenie uwag dotyczących wstępnych ustaleń. Właściwe organy przedstawiają szczegółowe uzasadnienie swoich środków egzekucyjnych.

6. Właściwe organy przestrzegają zasad poufności oraz tajemnicy zawodowej i handlowej.

7. Właściwe organy współpracują ze sobą oraz z Komisją w celu sprawowania nadzoru i egzekwowania przepisów na mocy niniejszego tytułu zgodnie z art. 116.

Artykuł 115
Kary

1. Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszenia niniejszego rozporządzenia i podejmują wszelkie niezbędne środki w celu zapewnienia ich wykonania.

2 Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach oraz niezwłocznie powiadamiają ją o wszelkich późniejszych zmianach mających wpływ na te przepisy i środki.

3. Kary nakłada się dodatkowo do środków, o których mowa w art. 114 ust. 3 lit. a), b) i c).

4. Przy podejmowaniu decyzji o nałożeniu kary i ustalaniu jej wysokości w każdym indywidualnym przypadku należy uwzględnić co najmniej czynniki, o których mowa w art. 114 ust. 4 akapit pierwszy.

5. Naruszenia art. 103 ust. 2 lit. a) podlegają, zgodnie z ust. 3 niniejszego artykułu, karom w wysokości maksymalnie 1 % całkowitego światowego rocznego obrotu w poprzednim roku obrotowym przedsiębiorstwa, do którego należy dany podmiot.

6. Naruszenia art. 103 ust. 2 lit. b)–g) podlegają, zgodnie z ust. 3 niniejszego artykułu, karom w wysokości maksymalnie 2 % całkowitego światowego obrotu rocznego w poprzednim roku obrotowym przedsiębiorstwa, do którego należy dany podmiot.

7. Naruszenia art. 103 ust. 1 i art. 111 podlegają, zgodnie z ust. 3 niniejszego artykułu, karom w wysokości maksymalnie 7 % całkowitego światowego rocznego obrotu w poprzednim roku obrotowym przedsiębiorstwa, do którego należy dany podmiot.

Artykuł 116
Wzajemna pomoc

1. W przypadku gdy podmiot typu określonego w załącznikach I lub II do dyrektywy (UE) 2022/2555 świadczy usługi w więcej niż jednym państwie członkowskim lub świadczy usługi w jednym lub kilku państwach członkowskich, a jego kluczowe aktywa ICT znajdują się w jednym lub kilku innych państwach członkowskich, właściwe organy zainteresowanych państw członkowskich współpracują ze sobą oraz z Komisją i udzielają sobie nawzajem oraz Komisji pomocy w celu zapewnienia skutecznego i efektywnego stosowania rozporządzenia. W tym celu stosuje się co najmniej następujące zasady:

   a) właściwe organy stosujące środki nadzoru lub egzekwowania w państwie członkowskim informują właściwe organy w innych zainteresowanych państwach członkowskich o podjętych środkach nadzoru i egzekwowania oraz konsultują się z nimi w tej sprawie;

   b) właściwy organ w państwie członkowskim może zwrócić się do innego właściwego organu w innym państwie członkowskim o podjęcie środków nadzoru lub egzekwowania;

   c) właściwy organ w państwie członkowskim, po otrzymaniu uzasadnionego wniosku od innego właściwego organu w innym państwie członkowskim, udziela temu organowi wzajemnej pomocy, dokładając wszelkich starań, aby środki nadzoru lub egzekwowania przepisów mogły być wdrażane w sposób skuteczny, wydajny i spójny.

2. Wzajemna pomoc, o której mowa w ust. 1 lit. c), może obejmować wnioski o udzielenie informacji i środki nadzorcze, w tym wnioski o przeprowadzenie kontroli na miejscu lub nadzoru zdalnego lub ukierunkowanych audytów bezpieczeństwa. Właściwy organ, do którego skierowano wniosek o pomoc, nie odrzuca tego wniosku, chyba że ustalono, iż nie ma on kompetencji do udzielenia żądanej pomocy, żądana pomoc nie jest proporcjonalna do zadań nadzorczych właściwego organu lub wniosek dotyczy informacji lub działań, których ujawnienie lub przeprowadzenie byłoby sprzeczne z istotnymi interesami bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obrony państwa członkowskiego. Przed odrzuceniem takiego

wniosku właściwy organ konsultuje się z innymi zainteresowanymi właściwymi organami, a także, na wniosek jednego z zainteresowanych państw członkowskich, z Komisją.

3. W stosownych przypadkach i za wspólną zgodą właściwe organy różnych państw członkowskich mogą prowadzić wspólne działania nadzorcze.

4. Ze względu na obowiązek przestrzegania zasad poufności oraz tajemnicy zawodowej i handlowej, o których mowa w art. 114 ust. 6, wszelkie informacje wymieniane w kontekście wniosku o pomoc i przekazywane zgodnie z niniejszym artykułem są wykorzystywane wyłącznie w odniesieniu do sprawy, której dotyczyły.

Artykuł 117
Jurysdykcja i terytorialność

1. Podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, objęte zakresem stosowania niniejszego rozporządzenia, uznaje się za podlegające jurysdykcji państwa członkowskiego, w którym mają siedzibę, z wyjątkiem przypadków, gdy:

   a) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej, którzy są uznawani za podlegających jurysdykcji państwa członkowskiego, w którym świadczą swoje usługi;

   b) dostawców usług DNS, rejestrów nazw domen najwyższego poziomu (TLD), 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, dostawców wyszukiwarek internetowych lub dostawców platform usług społecznościowych, którzy są uznawani za podlegających jurysdykcji państwa członkowskiego, w którym mają swoją główną siedzibę w Unii zgodnie z ust. 2;

   c) podmioty administracji publicznej, które uznaje się za podlegające jurysdykcji państwa członkowskiego, do którego należą;

   d) przewoźnicy lotniczy, którzy są uznawani za podlegających jurysdykcji państwa członkowskiego, którego właściwy organ wydający koncesje udzielił podmiotowi koncesji na prowadzenie działalności zgodnie z rozporządzeniem (WE) nr 1008/2008 Parlamentu Europejskiego i Rady[83] , lub, w przypadku gdy koncesja na prowadzenie działalności lub jej odpowiednik nie zostały udzielone zgodnie z tym rozporządzeniem, są oni uznawani za podlegających jurysdykcji państwa członkowskiego, w którym mają swoją główną siedzibę w Unii zgodnie z ust. 2.

2. Do celów niniejszego rozporządzenia uznaje się, że podmiot, o którym mowa w ust. 1 lit. b), ma swoją główną siedzibę w Unii w państwie członkowskim, w którym podejmowane są głównie decyzje dotyczące środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa. Jeżeli nie można określić takiego państwa członkowskiego lub jeżeli takie decyzje nie są podejmowane w Unii, uznaje się, że

[83] 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. 3–20, ELI: https://eur-lex.europa.eu/eli/reg/2008/1008/oj/eng).

główna siedziba znajduje się w państwie członkowskim, w którym prowadzona jest większość działań w zakresie cyberbezpieczeństwa. Jeżeli nie można określić takiego państwa członkowskiego, za główne miejsce prowadzenia działalności uznaje się państwo członkowskie, w którym dany podmiot ma zakład zatrudniający największą liczbę pracowników w Unii.

3. Jeżeli podmiot typu, o którym mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, nie ma siedziby w Unii, ale świadczy usługi w Unii, 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. W przypadku gdy podmiot taki jest podmiotem, o którym mowa w ust. 1 lit. a), uznaje się, że podlega on 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 niniejszego rozporządzenia.

4. Wyznaczenie przedstawiciela przez podmiot, o którym mowa w ust. 1 lit. b), pozostaje bez uszczerbku dla działań prawnych, które mogą zostać podjęte przeciwko samemu podmiotowi.

5. Państwa członkowskie, które otrzymały wniosek o wzajemną pomoc w odniesieniu do podmiotu, o którym mowa w ust. 1 lit. b), mogą, w granicach tego wniosku, podjąć odpowiednie środki nadzorcze i egzekucyjne w odniesieniu do danego podmiotu, jeżeli podmiot ten świadczy usługi lub posiada system sieci i informacji na ich terytorium.

TYTUŁ VI
PRZEPISY KOŃCOWE

Artykuł 118
Procedura komitetowa

1. Komisję wspomaga komitet. Komitet ten działa w dwóch składach. W odniesieniu do tytułów II i III Komisję wspomaga komitet w pierwszym składzie, natomiast w odniesieniu do tytułu IV Komisję wspomaga komitet w drugim składzie. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2 W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 119
Wykonywanie przekazanych uprawnień

1. Uprawnienia do przyjęcia aktów delegowanych powierza się Komisji na warunkach określonych w niniejszym artykule.

2 Uprawnienia do przyjęcia aktów delegowanych zgodnie z art. 80 ust. 2 i art. 110 ust. 5 powierza się Komisji na czas nieokreślony od dnia wejścia w życie niniejszego rozporządzenia.

3. Przekazanie uprawnień, o którym mowa w art. 80 ust. 2 i art. 110 ust. 5, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub Radę. Decyzja o

odwołaniu kończy przekazanie uprawnień określonych w tej decyzji. Decyzja ta staje się skuteczna następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie ma ona wpływu na ważność aktów delegowanych już obowiązujących.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja powiadamia o tym jednocześnie Parlament Europejski i Radę.

6. Akt delegowany przyjęty na podstawie art. 80 ust. 2 i art. 110 ust. 5 wchodzi w życie tylko wtedy, gdy ani Parlament Europejski, ani Rada nie wyrażą sprzeciwu w terminie dwóch miesięcy od powiadomienia Parlamentu Europejskiego i Rady o tym akcie lub gdy przed upływem tego terminu zarówno Parlament Europejski, jak i Rada poinformują Komisję, że nie wyrażą sprzeciwu . Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 120
Ocena i przegląd

1. Do dnia [DD MM RRRR], a następnie co pięć lat, Komisja zleca przeprowadzenie oceny zgodnie z wytycznymi Komisji.

2. Ocena, o której mowa w ust. 1, obejmuje ocenę następujących elementów:

   a) wyników ENISA w odniesieniu do jej celów, mandatu, misji, zadań, zarządzania i lokalizacji;

   b) skuteczność, efektywność i wartość dodaną dla UE europejskich systemów indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa, określonych w tytule II rozdział II sekcja 4 niniejszego rozporządzenia;

   c) wpływ, skuteczność i efektywność przepisów tytułu III niniejszego rozporządzenia w odniesieniu do celów zapewnienia odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i podmiotów w Unii oraz poprawy funkcjonowania rynku wewnętrznego;

   d) wpływ, skuteczność i efektywność przepisów tytułu IV niniejszego rozporządzenia w odniesieniu do celów dotyczących ram zaufanego łańcucha dostaw ICT.

3. Ocena, o której mowa w ust. 1 lit. a), dotyczy w szczególności ewentualnej potrzeby zmiany mandatu ENISA oraz skutków finansowych takiej zmiany.

4 Przy okazji każdej drugiej oceny, o której mowa w ust. 1 lit. a), Komisja ocenia wyniki osiągnięte przez ENISA, biorąc pod uwagę jej cele, mandat, misję, zarządzanie i zadania, w tym ocenia, czy dalsze funkcjonowanie ENISA jest nadal uzasadnione w odniesieniu do tych celów, mandatu, misji, zarządzania i zadań.

5. Komisja przedstawia Parlamentowi Europejskiemu, Radzie i zarządowi sprawozdanie z wyników oceny. Wyniki oceny podaje się do wiadomości publicznej.

Artykuł 121
Uchylenie i kontynuacja działalności

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 traci moc z dniem DDMMYYYY.

2. Odesłania do rozporządzenia (UE) 2019/881, ENISA i europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa ustanowionych tym rozporządzeniem traktuje się jako odesłania do niniejszego rozporządzenia i odczytuje się zgodnie z tabelą korelacji zawartą w załączniku III do niniejszego rozporządzenia.

3. ENISA podlegająca niniejszemu rozporządzeniu kontynuuje działalność ENISA ustanowionej rozporządzeniem (UE) 2019/881 w odniesieniu do wszelkich praw własności, umów, zobowiązań prawnych, umów o pracę, zobowiązań finansowych i zobowiązań z tytułu ubezpieczenia społecznego ( ). Wszystkie decyzje zarządu i rady wykonawczej przyjęte zgodnie z rozporządzeniem (UE) 2019/881 pozostają ważne, pod warunkiem że są zgodne z niniejszym rozporządzeniem.

4. Dyrektor wykonawczy mianowany zgodnie z art. 15 ust. 1 lit. n) rozporządzenia (UE) 2019/881 pozostaje na stanowisku i wykonuje zadania i obowiązki dyrektora wykonawczego, o których mowa w art. 32 niniejszego rozporządzenia, przez pozostałą część swojej kadencji. Pozostałe warunki umowy pozostają bez zmian.

5. Systemy kandydujące, o których przygotowanie zwrócono się zgodnie z art. 49 rozporządzenia (UE) 2019/881, uznaje się za zgłoszone zgodnie z odpowiednimi przepisami niniejszego rozporządzenia. Przepisy tytułu III niniejszego rozporządzenia stosuje się odpowiednio do tych systemów kandydujących.

6. Członkowie zarządu mianowani przez Komisję oraz zastępcy członków mianowani zgodnie z art. 14 rozporządzenia (UE) 2019/881 pozostają na stanowiskach i pełnią funkcje zarządu, o których mowa w art. 27 niniejszego rozporządzenia, przez pozostałą część swojej kadencji. Członkowie zarządu mianowani przez państwa członkowskie zgodnie z art. 14 rozporządzenia (UE) 2019/881 pozostają na stanowiskach i pełnią funkcje zarządu, o których mowa w art. 27 niniejszego rozporządzenia, pod warunkiem że pełnią funkcje, o których mowa w art. 24 ust. 3 niniejszego rozporządzenia.

Artykuł 122
Wejście w życie

Niniejsze rozporządzenie wchodzi w życie […] dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Strasburgu,

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*

OŚWIADCZENIE FINANSOWE I CYFROWE

1. RAMY WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

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 oraz uchylającego rozporządzenie (UE) 2019/881 (ustawa o cyberbezpieczeństwie 2)

(Tekst mający znaczenie dla EOG)

Skrócony tytuł: Ustawa o cyberbezpieczeństwie 2 (CSA2)

I

Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę (UE) 2022/2555 w odniesieniu do środków upraszczających i dostosowania do [wniosku dotyczącego ustawy o cyberbezpieczeństwie 2]

1.2. Dziedziny polityki, których dotyczy *wniosek*

Dziedzina polityki: 09 – Sieci, treści i technologie komunikacyjne

Działanie: 09.02 jednolity rynek cyfrowy

1.3 Cele

1.3.1 Cel(e) ogólny(e)

Główne cele interwencji są następujące:

(1) Wzmocnienie zdolności i odporności w zakresie cyberbezpieczeństwa

Przyczynianie się do wzmocnienia zarządzania cyberbezpieczeństwem w Unii oraz pomoc w zapewnieniu, aby odpowiednie instytucje, organy i inne zainteresowane strony były lepiej przygotowane do zapobiegania zagrożeniom dla cyberbezpieczeństwa, ich wykrywania i reagowania na nie w skoordynowany i skuteczny sposób.

(2) Zapobieganie fragmentacji rynku wewnętrznego poprzez:

wspieranie opracowywania, wdrażania i przyjmowania wspólnych unijnych instrumentów w zakresie cyberbezpieczeństwa, takich jak systemy certyfikacji, oraz zapewnienie zharmonizowanych ram budujących zaufanie i interoperacyjność między państwami członkowskimi.

Te ogólne cele stanowią odpowiedź na kluczowe wyzwania wskazane w opisie problemu zawartym w ocenie skutków proponowanej inicjatywy. Odzwierciedlają one nadrzędny cel polityczny, jakim jest wzmocnienie zarządzania cyberbezpieczeństwem w Unii oraz wspieranie rozwoju bezpiecznego, odpornego i konkurencyjnego jednolitego rynku cyfrowego.

1.3.2. Cele szczegółowe

Zajęcie się rozbieżnością między ramami polityki UE w zakresie cyberbezpieczeństwa a potrzebami zainteresowanych stron:

Cel szczegółowy nr 1: Stworzenie zdolności do skutecznego wdrażania unijnych polityk w zakresie cyberbezpieczeństwa oraz ciągłej współpracy operacyjnej

umożliwiającej bardziej ustrukturyzowaną współpracę między państwami członkowskimi.

Cel szczegółowy nr 2: Opracowanie i wdrożenie środków i mechanizmów skutecznie wspierających i zaspokajających potrzeby państw członkowskich, przemysłu i innych zainteresowanych stron.

Aby zaradzić ograniczonemu wykorzystaniu i skuteczności europejskich ram certyfikacji w zakresie cyberbezpieczeństwa (ECCF):

Cel szczegółowy nr 3: Stworzenie warunków wstępnych dla szybszego wdrażania systemów certyfikacji w zakresie cyberbezpieczeństwa, dostosowanych do potrzeb rynku, poprzez rozszerzenie zakresu ECCF, zapewnienie skutecznego utrzymania i sprawnych procedur oraz zwiększenie przejrzystości.

Aby zaradzić fragmentaryczności przepisów dotyczących zgodności oraz złożoności ram horyzontalnych i sektorowych:

Cel szczegółowy nr 4: Stworzenie mechanizmów i warunków ułatwiających zgodność z wymogami w zakresie cyberbezpieczeństwa, a tym samym zapewnienie bardziej spójnego i skutecznego wdrażania tych wymogów.

Aby zaradzić zagrożeniom dla cyberbezpieczeństwa w łańcuchu dostaw:

Cel szczegółowy nr 5: Ograniczenie ryzyka związanego z krytycznymi łańcuchami dostaw ICT od podmiotów mających siedzibę w krajach budzących obawy w zakresie cyberbezpieczeństwa (dostawcy wysokiego ryzyka) lub kontrolowanych przez takie podmioty oraz zmniejszenie krytycznej zależności poprzez opracowanie spójnych i skutecznych ram na szczeblu UE w celu przeciwdziałania zagrożeniom dla bezpieczeństwa łańcucha dostaw ICT.

1.3.3. Oczekiwane wyniki i wpływ

Należy określić skutki, jakie wniosek/inicjatywa powinien mieć dla beneficjentów/grup docelowych.

Oczekiwane wyniki są następujące:

(1) Reforma funkcjonalna ENISA

(2) Reforma ECCF – rozszerzenie zakresu, nowa procedura i zmienione zasady zarządzania

(3) Dalsze uproszczenie zgodności z odpowiednimi unijnymi ramami prawnymi w zakresie cyberbezpieczeństwa

(4) Kompleksowe i horyzontalne ramy dotyczące przeciwdziałania zagrożeniom dla cyberbezpieczeństwa łańcuchów dostaw ICT

Ogólny wpływ:

Wniosek będzie miał ogromny wpływ na cyberbezpieczeństwo w Unii, ponieważ dotyczy wielu obszarów, takich jak konieczne wzmocnienie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, wzmocnienie wsparcia dla wdrażania prawa UE, wprowadzenie reform mających na celu sprawne wdrożenie europejskich ram certyfikacji, wspieranie wspólnego rozumienia zagrożeń cybernetycznych przez Unię oraz łagodzenie ryzyka związanego z cyberbezpieczeństwem zgodnie z rzeczywistością geopolityczną. Wdrożenie proponowanych przepisów zapewni wysoki poziom skuteczności i spójności oraz pozwoli uniknąć nadmiernych obciążeń regulacyjnych. Pakiet został zaprojektowany tak, aby był odporny na wyzwania

związane z wdrażaniem i wspierał długoterminową spójność polityki w całym ekosystemie cyfrowym i cyberbezpieczeństwa. Poprawia on przejrzystość, eliminuje nieefektywność i ujednolica procedury w różnych ramach prawnych, przyczyniając się jednocześnie do osiągnięcia wysokiego poziomu cyberbezpieczeństwa w całej UE. Jako jeden z głównych priorytetowych celów Komisji Europejskiej, przewidywane działania na rzecz uproszczenia przyniosą znaczne korzyści gospodarcze dla przedsiębiorstw, w tym MŚP, w wysokości ponad 14,63 mld EUR, a dla organów publicznych – 7,5 mln EUR.

Konkretne wyniki obejmują:

- zwiększenie świadomości i poprawę koordynacji operacyjnej, co może przynieść znaczne oszczędności kosztów związane z szybszym wykrywaniem incydentów i reagowaniem na nie przez przedsiębiorstwa, organy publiczne i obywateli;
- wyjaśnienie zakresu i kompetencji ENISA, przy jednoczesnym zapewnieniu niezbędnego priorytetowego traktowania jej podstawowych zadań;
- zapewnienie zainteresowanym stronom odpowiedniego wsparcia w zakresie wdrażania polityki, działań operacyjnych i ogólnej koordynacji;
- wspieranie wspólnej świadomości sytuacyjnej Unii
- wzmocnienie współpracy z EU-CyCLONe, siecią CSIRT, Komisją, Europolem i CERT-EU oraz odpowiednimi podmiotami unijnymi w celu stworzenia bazy sprawdzonych i wiarygodnych informacji o cyberzagrożeniach;
- wspieranie wysiłków na rzecz łagodzenia skutków ataków ransomware;
- wzmocnienie koordynacji z sektorem prywatnym w kwestiach związanych z cyberbezpieczeństwem;
- rozpowszechnianie aktualnych informacji poprzez wczesne ostrzeganie o znaczących lub zakrojonych na szeroką skalę incydentach lub zagrożeniach cybernetycznych o charakterze transgranicznym, w odniesieniu do sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555;
- wspieranie skutecznej synergii z innymi organami i agencjami UE;
- obniżenie kosztów certyfikacji umiejętności, w tym poprzez zwiększenie podaży na rynku poprzez wprowadzenie europejskich systemów poświadczania umiejętności;
- wspierać niwelowanie luki w umiejętnościach w Europie poprzez indywidualne certyfikaty umiejętności w zakresie cyberbezpieczeństwa oraz wspierać państwa członkowskie i przemysł w wzmacnianiu ich siły roboczej;
- rozwiązanie problemu braku jasności ram ECCF i ich ograniczonego wpływu poprzez rozszerzenie ich zakresu i poprawę modelu zarządzania;
- zwiększenie renomy przyjętych systemów poprzez ustanowienie struktury utrzymania oraz wprowadzenie terminowego i przejrzystego procesu rozwoju;
- wprowadzenie mechanizmu opłat w związku z kosztami ponoszonymi w związku z opracowywaniem i utrzymywaniem europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa oraz rozpatrywaniem wniosków i udzielaniem zezwoleń dostawcom, a także

utrzymywaniem systemów przyjętych w ramach ECCF, co przyczyni się do stabilności finansowej Agencji i pozwoli na oszczędności w budżecie UE;

- dostosowanie europejskich systemów certyfikacji do istniejących ram prawnych, a tym samym lepsze wsparcie wysiłków wdrożeniowych i potrzeb przedsiębiorstw w zakresie zgodności z przepisami;
- umożliwienie przyjęcia obecnie zablokowanych systemów;
- wspieranie konkurencyjności przedsiębiorstw europejskich poprzez promowanie dostosowania norm międzynarodowych do norm europejskich;
- ograniczenie fragmentacji środków i wymogów w zakresie cyberbezpieczeństwa;
- zapewnienie jasności prawnej i znaczne zmniejszenie obciążeń administracyjnych, bez powodowania znacznej niepewności prawnej wśród zainteresowanych stron, które są w trakcie dostosowywania się do niedawno przyjętych ram prawnych;
- ułatwienie podmiotom objętym dyrektywą NIS2 zapewnienia zgodności z przepisami, co przyczyniłoby się również do poprawy ogólnego wskaźnika zgodności i wprowadzenia bardziej znaczących środków w zakresie cyberbezpieczeństwa, a jednocześnie zwiększyłoby efektywność procesu nadzoru ze strony organów;

Inne

- Inicjatywa ta miałaby wiele pozytywnych skutków dla MŚP, biorąc pod uwagę poprawę konkurencyjności na rynku cyberbezpieczeństwa w UE, a także zmniejszenie kosztów i obciążeń administracyjnych:

1. *Pozytywny wpływ na MŚP, które skorzystałyby na zwiększonej odporności cybernetycznej dzięki wzmocnionej roli ENISA i wytycznym technicznym udzielanym przez agencję.*
2. *MŚP jako uprawnieni dostawcy wydający certyfikaty w ramach europejskiego systemu certyfikacji umiejętności zyskają rozpoznawalność, reputację i nowych klientów. Ponadto europejskie certyfikaty indywidualnych umiejętności w zakresie cyberbezpieczeństwa pomogą MŚP w identyfikacji kandydatów posiadających odpowiednie umiejętności.*
3. *Dobrze funkcjonujące europejskie systemy certyfikacji mogą ułatwić MŚP wybór zaufanych technologii ICT i przyczynić się do zwiększenia ich ogólnej cyberodporności.*
4. *Jako dostawcy usług DNS MŚP skorzystają na środkach związanych z wdrożeniem dyrektywy NIS2 ze względu na wyłączenia z zakresu stosowania dyrektywy dotyczące dostawców usług DNS.*
5. *MŚP skorzystałyby na doprecyzowaniu zakresu, które ograniczyłoby stosowanie obowiązków do niektórych podmiotów w niektórych sektorach wymienionych w dyrektywie NIS2.*
6. *W przypadku środków bezpieczeństwa łańcucha dostaw ICT MŚP ogólnie skorzystałyby na stosowaniu zaufanych technologii. Jako dostawcy działający w sektorach podlegających ograniczeniom, poniosłyby one większe skutki związane z kosztami substytucji i transakcji niż większe przedsiębiorstwa. Jednak MŚP jako zaufani dostawcy skorzystają z nowych możliwości rynkowych.*

- Nie przewiduje się znaczącego wpływu na środowisko w odniesieniu do żadnego z celów.

- W odniesieniu do budżetu UE można oczekiwać wzrostu efektywności dzięki zacieśnieniu współpracy i koordynacji działań między instytucjami, agencjami i organami UE. W perspektywie długoterminowej oczekuje się oszczędności dzięki wprowadzeniu mechanizmów opłat.

1.3.4. Wskaźniki wykonania

Należy określić wskaźniki służące monitorowaniu postępów i osiągnięć.

Cel: Stworzenie zdolności do skutecznego wdrażania polityki UE w zakresie cyberbezpieczeństwa oraz regularnej/ciągłej współpracy operacyjnej umożliwiającej bardziej ustrukturyzowaną współpracę między państwami członkowskimi.

Liczba istotnych wkładów ENISA w realizację polityki UE i polityki krajowej oraz inicjatyw legislacyjnych

- Pozytywne opinie zainteresowanych stron dotyczące odpowiednich wkładów ENISA

Wzrost o 25 % w porównaniu z poziomem bazowym z 2023 r., zgodnie z rocznym sprawozdaniem z działalności ENISA (w odniesieniu do liczby istotnych wkładów) oraz zgodnie z corocznym badaniem satysfakcji ENISA (w odniesieniu do pozytywnych opinii).

- Statystyki dotyczące wykorzystania unijnej bazy danych podatności

- Wzrost liczby użytkowników o 25 % w porównaniu z 2025 r.

Dostępność, bezpieczeństwo i funkcjonowanie platformy CRA

- Zmniejszenie o 25 % czasu przestoju platformy i liczby incydentów w porównaniu z 2025 r. Statystyki dotyczące czasu przestoju i incydentów na platformie

Cel: Opracowanie i wdrożenie środków i mechanizmów skutecznie wspierających i zaspokajających potrzeby państw członkowskich, przemysłu i innych zainteresowanych stron.

- Liczba podmiotów wspieranych przez ENISA i jakość udzielanego wsparcia.

- Liczba środków wdrożonych w celu wsparcia zainteresowanych stron.

- Wzrost o 10% liczby wspieranych zainteresowanych stron i wzrost o 10% poziomu zadowolenia wspieranych zainteresowanych stron w porównaniu z rokiem 2025

Cel: Stworzenie warunków niezbędnych do szybszego wdrażania systemów certyfikacji cyberbezpieczeństwa dostosowanych do potrzeb rynku poprzez rozszerzenie zakresu ECCF, zapewnienie skutecznej konserwacji i sprawnych procedur oraz zwiększenie przejrzystości.

- Liczba przyjętych programów

- Skrócenie czasu opracowania programu o 50% w porównaniu z 2025 r.

- Liczba ważnych certyfikatów wydawanych rocznie

- Wzrost o 25 % w stosunku do poziomu bazowego z 2025 r.

- Pozytywne opinie zainteresowanych stron dotyczące ich udziału w opracowywaniu programów i przejrzystości ECCF

- Wzrost o 25 % w stosunku do poziomu bazowego w corocznym badaniu satysfakcji ENISA w porównaniu z 2027 r.

Cel: Ustanowienie mechanizmów i warunków ułatwiających zgodność z wymogami w zakresie cyberbezpieczeństwa, a tym samym zapewnienie bardziej spójnego i skutecznego wdrażania tych wymogów.

- Odsetek kosztów ponoszonych przez MŚP w związku z przestrzeganiem przepisów NIS2 i przepisów dotyczących cyberbezpieczeństwa w stosunku do wszystkich kosztów związanych z zapewnieniem zgodności

- >70 % MŚP zgłaszających zmniejszenie kosztów zapewnienia zgodności z przepisami dotyczącymi cyberbezpieczeństwa w porównaniu z 2025 r.

- Liczba ataków ransomware i kwota szkód w EUR

- Zmniejszenie liczby ataków ransomware o > 1 % w porównaniu z 2027 r.

- Odsetek incydentów transgranicznych, podczas których lub po których organy państw członkowskich skorzystały z mechanizmów wzajemnej pomocy

- Zwiększenie odsetka przypadków, w których skorzystano z wzajemnej pomocy, o >20 punktów procentowych w porównaniu z 2025 r.

Cel: Zmniejszenie krytycznych zależności poprzez opracowanie spójnych i skutecznych ram na szczeblu UE w celu przeciwdziałania zagrożeniom dla bezpieczeństwa łańcucha dostaw ICT.

- Liczba przyjętych środków

- Zwiększenie o 25 % liczby przyjętych środków i zidentyfikowanych kluczowych aktywów w porównaniu z datą przyjęcia + 6 miesięcy

- Zmniejszenie zależności od dostawców wysokiego ryzyka w zakresie kluczowych aktywów ICT o 25 % w porównaniu z 2025 r.

1.4. Wniosek/inicjatywa odnosi się do:

☒ nowym działaniem *(tytuł IV Łańcuch dostaw, tytuł V Uproszczenie)*

☐ nowym działaniem wynikającym z projektu pilotażowego/działania przygotowawczego[84]

☒ rozszerzenie istniejącego działania (*tytuł II Mandat ENISA i tytuł III Certyfikacja*)

☐ połączenie lub przekierowanie jednego lub więcej działań w kierunku innego/nowego działania

[84] O których mowa w art. 58 ust. 2 lit. a) lub b) rozporządzenia finansowego.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Wymogi, które należy spełnić w perspektywie krótko- lub długoterminowej, w tym szczegółowy harmonogram wdrażania inicjatywy

W lipcu 2024 r. w swoich wytycznych politycznych[85] przewodnicząca Komisji Europejskiej Ursula von der Leyen wezwała do uproszczenia, konsolidacji i kodyfikacji prawodawstwa UE w celu wyeliminowania wszelkich nakładających się na siebie przepisów i sprzeczności przy zachowaniu wysokich standardów. W liście misji skierowanym do wiceprzewodniczącego Komisji Europejskiej Virkkunena[86] wspomniano w szczególności o usprawnieniu procesu przyjmowania europejskich systemów certyfikacji cyberbezpieczeństwa oraz o potrzebie ochrony naszych gałęzi przemysłu, obywateli i administracji publicznej przed zagrożeniami wewnętrznymi i zewnętrznymi. Ponadto w raporcie Niinistö z 2024 r.[87] wzywa się do ograniczenia ryzyka związanego z niepożądanymi zależnościami łańcucha dostaw w zakresie technologii krytycznych. Główne aspekty raportów zleconych przez przewodniczącego UE Draghiego[88] i Letty[89] odzwierciedlały potrzebę utrzymania konkurencyjności jednolitego rynku poprzez uproszczenie i zapewnienie najwyższego poziomu bezpieczeństwa i autonomii strategicznej. W związku z tym zmiana CSA stanowi kamień węgielny prac Komisji w zakresie bezpieczeństwa i wprowadzenie ambitnej zmiany europejskiego ekosystemu regulacyjnego w zakresie cyberbezpieczeństwa. Wniosek CSA2 wprowadza mechanizmy mające na celu przeciwdziałanie zagrożeniom dla cyberbezpieczeństwa w łańcuchu dostaw oraz mechanizmy mające na celu zmniejszenie fragmentacji przepisów dotyczących zgodności oraz złożoności ram horyzontalnych i sektorowych. Oczekuje się, że ENISA będzie również narzędziem prowadzącym do większego uproszczenia obowiązków sprawozdawczych poprzez integrację jednego punktu kontaktowego.

Ponadto, biorąc pod uwagę liczbę przepisów sektorowych wprowadzonych po przyjęciu CSA w 2019 r., a także szybko zmieniające się zagrożenia w zakresie cyberbezpieczeństwa, należy dokonać przeglądu mandatu ENISA w celu ustalenia bardziej ukierunkowanego i zaktualizowanego zestawu zadań, tak aby skutecznie i efektywnie wspierać wysiłki państw członkowskich, instytucji UE i innych zainteresowanych stron na rzecz zapewnienia bezpiecznej cyberprzestrzeni w Unii Europejskiej. Dzięki wzmocnieniu europejskich ram certyfikacji w zakresie cyberbezpieczeństwa (ECCF) wniosek zapewnia, że UE dysponuje sprawnym, nowoczesnym i elastycznym systemem certyfikacji, który będzie służył celom działań w zakresie u łańcucha dostaw oraz szybkiemu wdrożeniu aktu prawnego w sprawie cyberodporności. Podsumowując, proponowany zakres mandatu został określony w taki sposób, aby wzmocnić te obszary, w których agencja wykazała wyraźną wartość dodaną, oraz dodać nowe obszary, w których potrzebne jest wsparcie w świetle nowych priorytetów i instrumentów politycznych oraz w celu wzmocnienia ECCF.

Zmiana CSA ma zatem stanowić znaczącą zmianę w podejściu UE do cyberbezpieczeństwa oraz ogólnym bezpieczeństwie, gotowości i odporności Unii Europejskiej.

85 Wytyczne polityczne na rok 2024
86 List misji EVP Virkkunen
87 Sprawozdanie Sauli Niinistö
88 Raport Draghiego na temat konkurencyjności UE
89 Enrico Letta – Znacznie więcej niż rynek (kwiecień 2024 r.)

1.5.2. Wartość dodana zaangażowania UE (może wynikać z różnych czynników, np. korzyści wynikających z koordynacji, pewności prawnej, większej skuteczności lub komplementarności). Do celów niniejszej sekcji „wartość dodana zaangażowania UE" oznacza wartość wynikającą z działań UE, która stanowi dodatek do wartości, jaką w przeciwnym razie stworzyłyby same państwa członkowskie.

Ustawa o cyberbezpieczeństwie została przyjęta w 2019 r. na podstawie art. 114 TFUE, który upoważnia prawodawcę UE do przyjmowania środków harmonizujących krajowe przepisy ustawowe i wykonawcze, których celem jest ustanowienie i funkcjonowanie rynku wewnętrznego.

Zmieniony wniosek dotyczący CSA ma na celu usprawnienie przepisów dotyczących cyberbezpieczeństwa na szczeblu UE poprzez uzupełnienie i przegląd obecnego aktu prawnego w sprawie cyberbezpieczeństwa, obowiązującego od 2019 r. (CSA1). Cele CSA1, polegające na przyznaniu stałego mandatu Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, której zadaniem jest wspieranie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej UE, a także zapobieganie fragmentacji rynku wewnętrznego w odniesieniu do systemów certyfikacji cyberbezpieczeństwa, zostały utrzymane w ramach zainicjowanej zmiany. Cele te, które zostały już należycie przeanalizowane we wniosku dotyczącym ustawy o cyberbezpieczeństwie z 2017 r., nie mogą zostać osiągnięte w wystarczającym stopniu przez państwa członkowskie, a jedynie na poziomie Unii Europejskiej zgodnie z art. 5 Traktatu o Unii Europejskiej.

Wniosek dotyczący zmiany CSA wyraźnie koncentruje się na usprawnieniu, ustaleniu priorytetów i kodyfikacji zadań w ramach przepisów dotyczących cyberbezpieczeństwa, co można osiągnąć wyłącznie na szczeblu UE, a obecnie nie istnieje żadna taka inicjatywa. Nowy wniosek dodatkowo wzmacnia bezpieczeństwo łańcucha dostaw i sektor cyberbezpieczeństwa w UE oraz zwiększa gotowość i odporność państw członkowskich i przemysłu. Uzależnienie od podmiotów mających siedzibę w państwach trzecich lub kontrolowanych przez podmioty z państw trzecich budzących obawy w zakresie cyberbezpieczeństwa (dostawcy wysokiego ryzyka) ma wpływ na podmioty w całej Unii, a poważne incydenty związane z cyberbezpieczeństwem łańcucha dostaw często wykraczają poza granice państwowe. Rozwiązanie tej kwestii wyłącznie na szczeblu krajowym prawdopodobnie nie będzie skuteczne.

Nowe zadania powierzone ENISA mają kluczowe znaczenie dla osiągnięcia wysokiego poziomu cyberbezpieczeństwa w całej UE. Pomimo faktu, że agencja współpracuje z innymi organami UE zajmującymi się bezpieczeństwem, takimi jak Europol, a także z Europejskim Centrum Kompetencji w zakresie Cyberbezpieczeństwa, Technologii i Badań (ECCC), które jest odpowiedzialne za finansowanie wdrażania, misja i zadania agencji są wyjątkowe i obecnie nie ma innego organu pełniącego tego rodzaju obowiązki. W ekosystemie cyberbezpieczeństwa UE wszystkie zaangażowane podmioty ściśle ze sobą współpracują i działają w ramach jasno określonych mandatów. W związku z tym wniosek CSA2 wzmacnia tylko te elementy, które mają wyraźną wartość dodaną, zapewniając brak niejasności w zakresie powielania zadań, zarówno pod względem merytorycznym, jak i finansowania przez inne organy w ramach ekosystemu cyberbezpieczeństwa.

Więcej szczegółów

Mandat ENISA został rozszerzony w wyniku kolejnych aktów prawnych, bez kompleksowej zmiany jej podstawowych obowiązków i zasobów. Doprowadziło to do

nakładania się zadań, nieefektywności i niewystarczającego priorytetowego traktowania podstawowych zadań wsparcia dla państw członkowskich.

Kilka państw członkowskich wdrożyło własne krajowe systemy certyfikacji w zakresie cyberbezpieczeństwa, które znacznie różnią się pod względem zakresu i procedur oceny zgodności. Powoduje to fragmentację rynku i powielanie obciążeń dla operatorów i MŚP, które chcą uzyskać certyfikat jednokrotny i prowadzić działalność w całej UE. W CSA utworzono ECCF w celu rozwiązania problemu fragmentacji rynku, ale jego wdrażanie przebiega powoli i niejednolicie.

Podobnie, kilka horyzontalnych i sektorowych aktów prawnych określa środki w zakresie cyberbezpieczeństwa o różnych celach i zadaniach, co prowadzi również do różnic w podejściach państw członkowskich do kontroli zgodności i nadzoru. W rezultacie podmioty, zwłaszcza MŚP lub przedsiębiorstwa działające w kilku państwach członkowskich, ponoszą dodatkowe obciążenia związane z zapewnieniem zgodności, co negatywnie wpływa na ich konkurencyjność.

Różnorodne podejścia do bezpieczeństwa łańcucha dostaw ICT i różne środki podejmowane przez państwa członkowskie prowadzą do fragmentacji rynku i różnych wymogów dotyczących zgodności dla podmiotów. W szczególności, biorąc pod uwagę transgraniczny charakter łańcuchów dostaw ICT, fragmentacja wymogów dotyczących zgodności na rynku wewnętrznym podważyłaby pewność prawną dla podmiotów. Różnice w krajowych ramach dotyczących ograniczeń dla dostawców wysokiego ryzyka mogą stworzyć bariery dla przepływu towarów i usług przez granice w ramach rynku wewnętrznego. Wreszcie, ponieważ łańcuchy dostaw ICT mogą obejmować podmioty i infrastrukturę o znaczeniu krytycznym, niezależnie od miejsca siedziby tych dostawców, fragmentacja i luki w środkach bezpieczeństwa cybernetycznego stwarzają dodatkowe zagrożenia dla bezpieczeństwa tych podmiotów.

Ponadto wnioski dotyczące programów wieloletnich ram finansowych (WRF) zawierają przepis horyzontalny, który nakazuje wykluczenie dostawców wysokiego ryzyka zidentyfikowanych na mocy prawa UE w celu ochrony integralności budżetu UE i zapewnienia, aby wydatki Unii nie były sprzeczne z podstawowymi interesami bezpieczeństwa Unii. Ramy łańcucha dostaw CSA byłyby mechanizmem umożliwiającym taką identyfikację w obszarze łańcuchów dostaw ICT i dlatego mogą być realizowane wyłącznie na poziomie UE.

Z natury rzeczy cyberataki mają charakter transgraniczny, zwłaszcza biorąc pod uwagę skutki uboczne, które mogą wynikać z początkowo pojedynczego punktu wejścia. Zagrożenia i ryzyko dla cyberbezpieczeństwa mają wpływ na całą Unię Europejską, dlatego zbiorowy obraz sytuacji mógłby znacznie poprawić poziom cyberbezpieczeństwa podmiotów w Unii Europejskiej. Wnioski zawarte w zmienionym mandacie ENISA dotyczą tej kwestii i mają na celu znaczne zwiększenie cyberodporności UE.

Podsumowując, interwencja UE ma kluczowe znaczenie, ponieważ zagrożenia dla cyberbezpieczeństwa i związane z nimi wyzwania wykraczają poza granice poszczególnych państw członkowskich. Fragmentaryczne rozwiązania krajowe okazały się niewystarczające do osiągnięcia zaufania i koordynacji na całym rynku. Zmienione ramy prawne UE są niezbędne do usunięcia barier, zapewnienia spójnego wdrażania i wsparcia państw członkowskich w coraz bardziej złożonym środowisku regulacyjnym i zagrożeń.

1.5.3. Wnioski wyciągnięte z podobnych doświadczeń w przeszłości

Agencja ENISA została utworzona w 2004 r. z mandatem na czas określony. W 2019 r. weszła w życie ustawa o cyberbezpieczeństwie, której przepisy nadały agencji ENISA stały mandat i wyznaczyły jej cel, jakim jest stanie się centrum wiedzy specjalistycznej w dziedzinie cyberbezpieczeństwa w Europie. Obecnie agencja ENISA jest uznaną marką i zaufanym partnerem wśród zainteresowanych stron w UE. Kompetencje agencji były stopniowo budowane w ciągu 25 lat, odzwierciedlając ewoluujący ekosystem cyberprzestrzeni.

Zgodnie z art. 67 CSA co pięć lat Komisja ocenia wpływ, skuteczność i efektywność ENISA oraz jej praktyk roboczych, ewentualną potrzebę wprowadzenia zmian oraz skutki finansowe takich zmian. Ocena obejmuje również wpływ, skuteczność i efektywność przepisów dotyczących europejskich ram certyfikacji.

Zgodnie z przepisami Komisja przeprowadziła ocenę Agencji i europejskich ram certyfikacji w zakresie cyberbezpieczeństwa, która obejmowała konsultacje społeczne i niezależne badanie. Zgodnie z zasadami lepszego stanowienia prawa Komisja rozpoczęła również konsultacje społeczne dotyczące w szczególności przeglądu CSA, a także zaproszenie do zgłaszania dowodów w celu zebrania danych od grup zainteresowanych stron. W wyniku oceny stwierdzono, że ENISA wypełniła swój mandat, osiągając prawie wszystkie zaplanowane wyniki. Cele agencji pozostają aktualne, a jej wyniki zostały szczególnie docenione przez zainteresowane strony w trudnych czasach, takich jak pandemia COVID-19 i rosyjska agresja wojenna na Ukrainę. Pomimo ogólnie pozytywnych opinii zainteresowanych stron na temat wyników ENISA, wykazano również, że istnieje znaczna przestrzeń do poprawy, aby konsekwentnie spełniać oczekiwania zainteresowanych stron.

Wnioski płynące z doświadczeń pokazują, że aby podnieść poziom efektywności, ENISA potrzebuje bardziej strategicznego ukierunkowania, ustalenia priorytetów zadań oraz wzmocnienia zdolności do dostarczania na czas informacji na temat pojawiających się zagrożeń i strategicznych narzędzi do ich zwalczania. Ponadto, jak wskazało wielu zainteresowanych, ENISA mogłaby ustanowić bardziej ustrukturyzowane i przejrzyste metody współpracy z podmiotami prywatnymi, kładąc nacisk na wspieranie MŚP. We wszystkich konsultacjach zewnętrznych podkreślono znaczenie zwiększenia finansowania, zatrudnienia i zdolności operacyjnych ENISA, aby umożliwić jej sprostanie rosnącym wymaganiom w zakresie cyberbezpieczeństwa w UE. W sprawozdaniu z oceny, sporządzonym po przeprowadzeniu badania, służby Komisji oceniły wyraźną potrzebę wprowadzenia przyszłościowych przepisów, które będą mogły dostosować się do złożonego i szybko zmieniającego się środowiska cyberzagrożeń, a także odpowiednio wzmocnić agencję niezbędnymi zasobami, aby zapewnić wsparcie dla najwyższego poziomu cyberbezpieczeństwa w Europie. Na podstawie zebranych danych i doświadczeń zdobytych podczas wdrażania CSA stwierdzono, że należy usprawnić koordynację z innymi organami, a także położyć nacisk na wsparcie ze strony ENISA w zakresie wdrażania prawa UE oraz wsparcie dla Komisji, na jej wniosek, w zakresie opracowywania przepisów dotyczących cyberbezpieczeństwa. We wniosku rozważa się synergię z priorytetami geopolitycznymi Komisji w celu przeciwdziałania takim zagrożeniom, jak rosnąca zależność od podmiotów mających siedzibę w krajach budzących obawy w zakresie cyberbezpieczeństwa (dostawcy wysokiego ryzyka) i kontrolowanych przez te kraje w Europie. Jako centrum wiedzy specjalistycznej ENISA jest obecnie również istotnym repozytorium informacji, które mają kluczowe znaczenie dla budowania wspólnego zrozumienia zagrożeń i ryzyka dla podmiotów UE. W związku z tym

proponowane ramy opierają się na doświadczeniach zdobytych w ramach CSA1 i mobilizują koordynację przepływu informacji w celu stworzenia całościowego obrazu sytuacji.

Ocena ECCF zawiera kilka strategicznych zaleceń. Pomimo kluczowej roli ENISA w promowaniu współpracy i spójności operacyjnej między państwami członkowskimi i innymi zainteresowanymi stronami, ograniczenia dotyczące wydajności i skuteczności ECCF były widoczne głównie ze względu na złożoność procesów przyjmowania programów. Kwestie te podkreśliły konieczność istotnej zmiany struktur zarządzania w celu zwiększenia przejrzystości operacyjnej i odpowiedzialności na wszystkich poziomach, , którą zajmuje się wniosek CSA dotyczący zmiany. Doświadczenia związane z funkcjonowaniem obecnego ECCF wykazały potrzebę modernizacji i wyjaśnienia ram certyfikacji oraz wprowadzenia procedury utrzymania systemów certyfikacji, aby umożliwić im dostosowanie się do potrzeb rynku i zagrożeń. Wreszcie, pierwotne ramy nie przewidywały ryzyka nietechnicznego, które można uznać za przyczynę opóźnień we wdrażaniu ECCF w systemach 5G i chmurze.

Złożoność ekosystemu cyberbezpieczeństwa w UE wzrasta wraz z ewolucją zagrożeń cybernetycznych. W pisemnych opiniach zainteresowanych stron panowała silna zgoda co do potrzeby zmniejszenia obciążeń administracyjnych, zwłaszcza dla MŚP, i wezwano do uproszczenia procedur zgodności. Chociaż główne działania na rzecz uproszczenia będą realizowane w ramach inicjatywy Digital Omnibus, wniosek odzwierciedla potrzeby zainteresowanych stron, wprowadzając zmiany do dyrektywy NIS2 w celu ułatwienia procesu wdrażania.

1.5.4. Zgodność z wieloletnimi ramami finansowymi i możliwe synergie z innymi odpowiednimi instrumentami

CSA2 wprowadza niezbędne zmiany, aby wyposażyć UE w narzędzia i mechanizmy umożliwiające reagowanie na sytuację w zakresie cyberbezpieczeństwa i realizację celów polityki. Proponowane rozporządzenie dodatkowo wzmocni ENISA, zapewniając jej niezbędne zdolności do wspierania państw członkowskich we wdrażaniu prawa UE i przeciwdziałaniu zagrożeniom cybernetycznym. Biorąc pod uwagę wspomniane powyżej sprawozdania Draghiego i Letty, wniosek dotyczący wieloletnich ram finansowych (WRF) na lata 2028–2034 koncentruje się na konkurencyjności, bezpieczeństwie i autonomii strategicznej.

W rezultacie wnioski zawarte w pakiecie horyzontalnym MFF 2028–2034, w szczególności wnioski dotyczące Europejskiego Funduszu Konkurencyjności i programu „Horyzont Europa", wprowadzają nowe kryteria kwalifikowalności oparte na zasadzie wykluczenia „dostawców wysokiego ryzyka" z otrzymywania funduszy UE. CSA2 jest w pełni zgodny z tą zasadą, a ponadto stanowi narzędzie umożliwiające wdrożenie nowych wymogów dotyczących „dostawców wysokiego ryzyka", ponieważ zapewnia ramy proceduralne do wyznaczania krajów budzących obawy w zakresie cyberbezpieczeństwa na poziomie UE. Pod tym względem CSA2 jest propozycją strategiczną, zgodną z priorytetami Komisji w zakresie osiągnięcia suwerenności technologicznej i zwiększenia konkurencyjności w Europie.

Przezwyciężenie istniejącej fragmentacji zostanie osiągnięte poprzez dalszą harmonizację rynku certyfikacji w UE, dzięki czemu europejski proces certyfikacji stanie się bardziej wydajny i zrównoważony.

Wnioski dotyczące wieloletnich ram finansowych na lata 2028–2034 traktują uproszczenie jako priorytet w całym systemie. Pozycje budżetowe zostały

zredukowane z 7 do 4, a liczba horyzontalnych programów finansowania została znacznie zmniejszona z 52 do 16, co zapewnia elastyczność i możliwość dostosowania do aktualnych potrzeb. W ocenie skutków dotyczącej zmiany ustawy o cyberbezpieczeństwie podkreślono właśnie te cele: konieczność uproszczenia wymogów w zakresie cyberbezpieczeństwa w wielu ramach prawnych, skodyfikowanie i skoncentrowanie zadań ENISA na obszarach mających największy wpływ na osiągnięcie większej odporności ekosystemu cybernetycznego UE. W związku z tymi ustaleniami proponowane przepisy zwiększają konkurencyjność poprzez uproszczenie; zapewniają wysoki poziom bezpieczeństwa dzięki lepszej koordynacji i analizie ryzyka i słabych punktów; wspierają wyższy poziom harmonizacji poprzez przezwyciężenie fragmentacji spowodowanej liczbą krajowych programów. Ponadto ENISA została zaprojektowana jako główny instrument, który będzie napędzał działania na rzecz uproszczenia cyfrowego, ponieważ zintegruje ona pojedynczy punkt kontaktowy dla zgłoszeń, zgodnie z inicjatywą Digital Omnibus[90] .

Istotną częścią pakietu MFF 28-34 jest wniosek dotyczący nowego Funduszu Konkurencyjności (ECF), który skupia pod jednym dachem ponad 16 programów finansowania, takich jak program „Cyfrowa Europa” (DEP), Health4EU, Europejski Fundusz Obronny itp. Program „Horyzont Europa” (HEP) pozostanie programem samodzielnym, ściśle powiązanym z ECF. Nowe ramy programowania wymagają ścisłej koordynacji i finansowania odpowiadającego aktualnym priorytetom. W związku z tym proponowane przepisy w CSA2 stanowią podstawę do pogłębienia koordynacji między ENISA a ECCC, odpowiedzialnymi za realizację programów związanych z cyberbezpieczeństwem w ramach DEP i HEP. Proponowane przepisy zapewniają spójność i kładą nacisk na synergię między ENISA a ECCC. Takie samo podejście przyjęto w odniesieniu do współpracy z innymi agencjami i organami, takimi jak Europol.

Kolejnym aspektem dostosowania wniosku CSA2 do WRF 28-34 jest zasada elastyczności. W ramach zmiany Komisja proponuje mechanizm „opłat”, który zapewni ENISA elastyczny sposób częściowego finansowania jej działań, w szczególności związanych z opracowywaniem i utrzymywaniem systemów poświadczania umiejętności w zakresie cyberbezpieczeństwa, przetwarzaniem i udzielaniem zezwoleń dostawcom oraz utrzymywaniem europejskich systemów certyfikacji cyberbezpieczeństwa. Dzięki tej zmianie agencja zyska elastyczność i skalowalność, które pozwolą jej reagować na potrzeby zainteresowanych stron i zapewnią jej zrównoważone wydatki poprzez refinansowanie jej usług.

1.5.5. Ocena różnych dostępnych opcji finansowania, w tym możliwości przeniesienia środków

Od ostatniej zmiany mandatu ENISA w 2019 r. obserwuje się tendencję do wykładniczego wzrostu oczekiwanego wkładu Agencji we wspieranie wdrażania prawa UE. Doprowadziło to do wniosków o zwiększenie rocznego budżetu i zatrudnienia powyżej pierwotnie zaplanowanych poziomów. Proponowana zmiana wprowadza ważne nowe zadania, a także uwzględnia zadania wynikające z mandatu ENISA, które zostały nałożone na agencję w innych aktach prawnych po przyjęciu CSA1, rozszerzając tym samym możliwości ENISA, co wymaga dodatkowego wzmocnienia finansowego i kadrowego. Kierując się celem uczynienia bezpieczeństwa cyfrowego przewagą konkurencyjną Europy, we wniosku wzywa się do wywarcia rzeczywistego wpływu na ekosystem cyberprzestrzeni. Byłoby to

90 Zostanie dodane po opublikowaniu

możliwe jedynie dzięki znacznym inwestycjom odpowiadającym pożądanemu efektowi, a przede wszystkim potrzebom państw członkowskich i innych zainteresowanych stron. Nowe zadania wiążą się z potrzebą zatrudnienia personelu technicznego i wyspecjalizowanego, a także inwestycji finansowych (tj. w narzędzia i platformy), które można zapewnić jedynie poprzez dodatkowe środki finansowe z budżetu UE.

W celu zwiększenia elastyczności, a jednocześnie zapewnienia długoterminowej stabilności budżetu Agencji, w ramach przeglądu proponuje się wprowadzenie mechanizmu opłat, który będzie częściowo finansował usługi świadczone w zakresie utrzymania ram certyfikacji cyberbezpieczeństwa oraz związane z opracowywaniem i utrzymywaniem europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa oraz przetwarzaniem i udzielaniem zezwoleń dostawcom.

Wszystkie szacunki dotyczące dodatkowych zasobów w ramach przeglądu CSA są dokonywane z perspektywy budżetu bazowego ENISA na 2025 r. (koszty operacyjne i etaty). Komisja przeprowadziła szczegółową analizę możliwości przesunięcia zasobów w ramach Agencji w celu dostosowania się do nowych zadań przewidzianych w zmienionym mandacie. Fakt, że agencja pracuje na maksymalnych obrotach, nie ma możliwości ograniczenia zadań, a zarząd podjął już w 2023 r. działania mające na celu zmniejszenie priorytetowości niektórych zadań, wyraźnie prowadzi do wniosku, że w obecnej strukturze nie można uwzględnić żadnych nowych zadań bez zwiększenia zarówno budżetu, jak i zasobów ludzkich. Ponadto wiele obecnych zadań jest objętych umowami o wkładzie między ENISA a Komisją. W związku z tym wniosek ma na celu dodanie tych zadań do mandatu ENISA i zapewnienie stabilnego budżetu na najbliższe lata.

Bez uszczerbku dla negocjacji w sprawie kolejnych wieloletnich ram finansowych środki przyznane agencji od 2028 r. zostaną zrekompensowane poprzez przesunięcia z programów w ramach wieloletnich ram finansowych na lata 2028–2034. Jeżeli konieczne będzie kompensacyjne zmniejszenie środków, może zaistnieć potrzeba zmiany zasobów przyznanych agencji oraz ich strumieni i źródeł finansowania. Środki wprowadzone w proponowanych ramach CSA2 wiążą się również z podjęciem dodatkowych zadań przez partnerską DG ENISA (Dyrekcję Generalną ds. Sieci Komunikacyjnych, Treści i Technologii, DG CNECT). Należy zwrócić szczególną uwagę na fakt, że ramy dotyczące łańcucha dostaw ICT zostaną w pełni wdrożone na poziomie Komisji, w tym analiza rynku towarzysząca ocenom ryzyka i przygotowanie aktów wykonawczych. Ponadto konieczne będzie opracowanie i przyjęcie przez Komisję dodatkowego zestawu aktów wykonawczych dotyczących warunków funkcjonowania mechanizmów opłat. Wymagany będzie dodatkowy nadzór i pomoc na szczeblu Komisji w celu egzekwowania europejskich ram certyfikacji w zakresie cyberbezpieczeństwa, opracowania wzorcowych przepisów, utrzymania systemów cyberbezpieczeństwa, umów o wzajemnym uznawaniu z państwami trzecimi oraz nadzoru ENISA.

1.6. Czas trwania wniosku/inicjatywy i jego skutków finansowych

☐ **ograniczony czas trwania**

– ☐ obowiązuje od [DD/MM]RRRR do [DD/MM]RRRR

– ☐ skutki finansowe od RRRR do RRRR w odniesieniu do środków na zobowiązania i od RRRR do RRRR w odniesieniu do środków na płatności.

☒ **czas trwania nieograniczony**

– Wdrożenie z okresem rozruchu od RRRR do RRRR,

– a następnie pełną eksploatacją.

1.7. Planowane metody wykonania budżetu

☐ **Zarządzanie bezpośrednie** przez Komisję

– ☐ przez jej departamenty, w tym przez personel delegatur Unii;

– ☐ przez agencje wykonawcze

☐ **Zarządzanie dzielone** z państwami członkowskimi

☒ **Zarządzanie pośrednie** poprzez powierzenie zadań związanych z realizacją budżetu:

– ☐ państwom trzecim lub wyznaczonym przez nie organom

– ☐ organizacjom międzynarodowym i ich agencjom (do określenia)

– ☐ Europejskiemu Bankowi Inwestycyjnemu i Europejskiemu Funduszowi Inwestycyjnemu

– ☒ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego

– ☐ podmiotom prawa publicznego

– ☐ podmioty prawa prywatnego realizujące zadania użyteczności publicznej, o ile dysponują one odpowiednimi gwarancjami finansowymi

– ☐ podmioty prawa prywatnego państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego i które posiadają odpowiednie gwarancje finansowe

– ☐ podmioty lub osoby, którym powierzono realizację określonych działań w ramach wspólnej polityki zagranicznej i bezpieczeństwa zgodnie z tytułem V Traktatu o Unii Europejskiej i które zostały wskazane w odpowiednim akcie podstawowym

– ☐ podmioty mające siedzibę w państwie członkowskim, podlegające prawu prywatnemu państwa członkowskiego lub prawu Unii i kwalifikujące się do powierzenia im, zgodnie z przepisami sektorowymi, realizacji funduszy unijnych lub gwarancji budżetowych, o ile podmioty te są kontrolowane przez podmioty prawa publicznego lub podmioty prawa prywatnego realizujące zadania służby publicznej i posiadają odpowiednie gwarancje finansowe w postaci odpowiedzialności solidarnej podmiotów kontrolujących lub równoważnych gwarancji finansowych, które mogą być, w odniesieniu do każdego działania, do maksymalnej kwoty wsparcia unijnego.

Uwagi

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady monitorowania i sprawozdawczości

Monitorowanie i sprawozdawczość będą zgodne z zasadami określonymi w obowiązującym rozporządzeniu w sprawie CSA[91] , rozporządzeniu finansowym[92] oraz zgodnie ze wspólnym podejściem do agencji zdecentralizowanych[93] .

Zgodnie z art. 40 rozporządzenia finansowego ENISA musi co roku przesyłać Komisji, Parlamentowi Europejskiemu i Radzie jednolity dokument programowy (SPD) zawierający wieloletnie i roczne programy prac oraz programowanie zasobów. Ponadto wniosek Komisji dotyczący zmiany mandatu ENISA wprowadza wymóg, aby Komisja, jako członek zarządu, oddała głos za przyjęciem przez zarząd ENISA jednolitego dokumentu programowego w sprawach związanych z zasobami ludzkimi i budżetem. Komisja wyda również opinię na temat projektu jednolitego dokumentu programowego przed przeprowadzeniem głosowania w zarządzie, które powinno nastąpić przed przyjęciem jednolitego dokumentu programowego[94] .

ENISA musi przedłożyć zarządowi skonsolidowane roczne sprawozdanie z działalności. Sprawozdanie to zawiera w szczególności informacje na temat realizacji celów i wyników określonych w jednolitym dokumencie programowym. Sprawozdanie należy również przesłać Komisji, Parlamentowi Europejskiemu i Radzie. Dyrektor wykonawczy ENISA powinien co dwa lata przedstawiać zarządowi ocenę ex post działalności ENISA. Agencja powinna również przygotować plan działań następczych w odniesieniu do wniosków z ocen retrospektywnych i co dwa lata składać Komisji sprawozdanie z postępów. Zarząd powinien być odpowiedzialny za monitorowanie odpowiednich działań następczych w związku z tymi wnioskami.

Domniemane przypadki niewłaściwego administrowania w działalności Agencji mogą podlegać dochodzeniom prowadzonym przez Europejskiego Rzecznika Praw Obywatelskich zgodnie z przepisami art. 228 Traktatu.

Źródłami danych do planowanego monitorowania będą głównie ENISA, Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, Grupa ds. Współpracy w zakresie NIS, sieć CSIRT oraz organy państw członkowskich. Oprócz danych pochodzących ze sprawozdań (w tym rocznych sprawozdań z działalności) ENISA, Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa, Grupy Współpracy NIS i sieci CSIRT, w razie potrzeby wykorzystywane będą specjalne narzędzia Komisji do gromadzenia danych (na przykład ankiety przeprowadzane wśród organów krajowych, Eurobarometr, specjalistyczne badania i sprawozdania z ogólnoeuropejskich ćwiczeń).

Wniosek Komisji dotyczący CSA2 stanowi kontynuację ustalonej praktyki przeglądu i oceny Agencji. Jak określono w art. 119 wniosku dotyczącego CSA2, Komisja musi zlecić ocenę ENISA do dnia [DD MM RRRR], a następnie co pięć lat. Ocena ta będzie dotyczyła w szczególności ewentualnej potrzeby zmiany mandatu ENISA oraz skutków finansowych takiej zmiany. Przy okazji każdej drugiej oceny przeprowadza się ocenę wyników osiągniętych przez ENISA w odniesieniu do jej celów, mandatu, misji, zarządzania opartego na zasadach wspólnego podejmowania decyzji ( ) oraz

91 Ustawa UE o cyberbezpieczeństwie | EUR-Lex

92 Rozporządzenie finansowe mające zastosowanie do budżetu ogólnego Unii (przekształcenie) – Urząd Publikacji Unii Europejskiej

93 https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf

94 Rozporządzenie delegowane – 2019/715 – PL – EUR-Lex

zadań, w tym ocenę, czy dalsze funkcjonowanie ENISA jest nadal uzasadnione w odniesieniu do tych celów, mandatu, misji, zarządzania i zadań.

W ramach oceny ocenia się również wpływ, skuteczność i efektywność przepisów tytułu III rozporządzenia w odniesieniu do celów europejskich ram certyfikacji w zakresie cyberbezpieczeństwa, zapewniających odpowiedni poziom cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i podmiotów w Unii oraz poprawiających funkcjonowanie rynku wewnętrznego.

W ramach oceny ocenia się również wpływ, skuteczność i efektywność przepisów tytułu IV rozporządzenia w odniesieniu do celów ram bezpieczeństwa łańcucha dostaw ICT.

Komisja przedstawia Parlamentowi Europejskiemu i Radzie wszystkie ustalenia, a zarządowi – ustalenia z oceny tytułu II rozporządzenia. Ustalenia z oceny podaje się do wiadomości publicznej.

2.2. Systemy zarządzania i kontroli

2.2.1. Uzasadnienie proponowanych metod wykonania budżetu, mechanizmów realizacji finansowania, warunków płatności i strategii kontroli

Biorąc pod uwagę, że wniosek ma wpływ na roczny wkład UE na rzecz ENISA, budżet UE będzie realizowany w ramach zarządzania pośredniego.

Zgodnie z zasadą należytego zarządzania finansami budżet ENISA będzie realizowany zgodnie z zasadami skutecznej i wydajnej kontroli wewnętrznej. ENISA jest zatem zobowiązana do wdrożenia odpowiedniej strategii kontroli skoordynowanej między odpowiednimi podmiotami zaangażowanymi w łańcuch kontroli.

W odniesieniu do kontroli ex post ENISA, jako agencja zdecentralizowana, podlega w szczególności:

- audytowi wewnętrznemu przeprowadzanemu przez Służbę Audytu Wewnętrznego Komisji
- sprawozdaniom rocznym Europejskiego Trybunału Obrachunkowego, zawierającym poświadczenie wiarygodności rocznego sprawozdania finansowego oraz legalności i prawidłowości transakcji leżących u jego podstaw
- coroczne absolutorium udzielane przez Parlament Europejski
- ewentualne dochodzenia prowadzone przez OLAF w celu zapewnienia, w szczególności, właściwego wykorzystania środków przydzielonych agencjom.
- Jako partner DG ENISA, DG CNECT wdroży swoją strategię kontroli agencji zdecentralizowanych w celu zapewnienia wiarygodnej sprawozdawczości w ramach rocznego sprawozdania z działalności (AAR). Podczas gdy agencje zdecentralizowane ponoszą pełną odpowiedzialność za wykonanie swojego budżetu, DG CNECT jest odpowiedzialna za regularne wypłacanie rocznych składek ustalonych przez władzę budżetową.
- Wreszcie Europejski Rzecznik Praw Obywatelskich zapewnia dodatkową warstwę kontroli i odpowiedzialności w ENISA.

Na podstawie oceny Agencji oraz oceny skutków przeprowadzonej w związku z przedstawieniem wniosku dotyczącego rozporządzenia CSA2 stwierdzono, że zapewnienie odpowiednich środków finansowych ma zasadnicze znaczenie dla

umożliwienia ENISA wykonywania zadań powierzonych jej w ramach nowego mandatu. Ważną nowością w zmienionym mandacie Agencji będzie wprowadzenie mechanizmu opłat, który ma służyć finansowaniu kosztów utrzymania europejskich systemów certyfikacji cyberbezpieczeństwa, przyjętych w ramach ECCF. Zmieniony ECCF sformalizuje procedurę utrzymania. Działania związane z utrzymaniem będą prowadzone przez ENISA i częściowo finansowane z opłat, aby uwzględnić ich skalowalny charakter (więcej systemów wymaga więcej personelu do utrzymania). Agencja będzie również wyposażona w możliwość dostarczania narzędzi testowych wspierających wdrażanie procedur oceny zgodności zarówno w ramach ECCF, jak i innych odpowiednich przepisów UE dotyczących cyberbezpieczeństwa. Warunki dotyczące opłat zostaną określone w akcie wykonawczym przyjętym przez Komisję. Ponadto w ramach zmiany przewiduje się opracowanie i utrzymanie europejskich systemów indywidualnych poświadczeń oraz wydawanie decyzji w sprawie upoważniania dostawców do wydawania europejskich indywidualnych poświadczeń umiejętności w zakresie cyberbezpieczeństwa.

2.2.2. Informacje dotyczące zidentyfikowanych zagrożeń i systemów kontroli wewnętrznej ustanowionych w celu ich ograniczenia

Wniosek dotyczący CSA2 jako taki ma na celu ograniczenie zidentyfikowanych zagrożeń w ramach mandatu ENISA i ram ECCF, w tym ram bezpieczeństwa łańcucha dostaw ICT i przepisów dotyczących uproszczenia. W szczególności ENISA jest agencją Unii Europejskiej, która już istnieje, a w ramach zmiany jej mandat został dokładniej określony, wzmacniając obszary, w których agencja wykazała wyraźną wartość dodaną, oraz dodając nowe obszary, w których potrzebne jest wsparcie w świetle nowych priorytetów i instrumentów politycznych, takich jak uproszczenie poprzez integrację jednego punktu kontaktowego do zgłaszania incydentów; wsparcie dla wspólnego europejskiego obrazu sytuacji i współpracy operacyjnej, wzmocnione i usprawnione europejskie ramy certyfikacji w zakresie cyberbezpieczeństwa.

Kolejnym zidentyfikowanym ryzykiem, którym zajęto się we wniosku, jest liczba umów o wkładzie finansowym zawartych przez Komisję i agencję w ostatnich latach. Ze względu na obecną sytuację geopolityczną i szybko zmieniające się zagrożenia dla cyberbezpieczeństwa Komisja zawarła z agencją umowy o wkładzie finansowym o łącznej wartości ponad 75 mln EUR od 2019 r. Biorąc pod uwagę, że zadania powierzone ENISA w tych umowach mają obecnie charakter stały, niestabilny przepływ środków budżetowych w ramach umów o wkładzie stanowi zagrożenie dla długoterminowej realizacji zadań ENISA.

W związku z tym obecny wniosek ma między innymi na celu wzmocnienie potencjału zasobowego Agencji, ponowne zdefiniowanie jej zadań i zwiększenie efektywności. W szczególności możliwość pobierania opłat będzie w perspektywie długoterminowej wspierać zrównoważony obieg finansowy Agencji poprzez refinansowanie kosztów związanych z utrzymaniem europejskich systemów certyfikacji przyjętych w ramach ECCF, testowaniem narzędzi oraz opracowywaniem, utrzymywaniem i wdrażaniem europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa. W perspektywie długoterminowej szacuje się, że pozwoli to osiągnąć oszczędności w budżecie UE w wysokości 18,5 mln EUR rocznie. Komisja będzie kierować pracami nad warunkami pobierania opłat i ich strukturą poprzez przyjęcie aktów wykonawczych.

Zwiększenie zakresu zadań operacyjnych Agencji nie stanowi rzeczywistego ryzyka. Zadania te będą uzupełniać działania państw członkowskich i wspierać je na ich

wniosek. Będą one również ograniczone do wcześniej określonych usług, analogicznie do ustawy o cyberbezpieczeństwie (UE) 2019/881[95] . Nowe elementy/zadania zawarte we wniosku przyniosą wartość dodaną europejskim zainteresowanym stronom, które skorzystają z faktu, że ENISA jest centrum informacyjnym, przyczyniającym się do wymiany informacji i przekazywania powiadomień o zagrożeniach swoim podmiotom.

Ponadto proponowany model agencji jest zgodny ze wspólnym podejściem Komisji do agencji zdecentralizowanych, zapewniającym wystarczającą kontrolę, aby przewidzieć, że ENISA będzie działać na rzecz realizacji swoich celów. Ryzyko operacyjne i finansowe związane z proponowanymi zmianami wydaje się ograniczone, ponieważ przepisy mają na celu złagodzenie obecnego ryzyka. Niemniej jednak w perspektywie długoterminowej można spodziewać się pewnych negatywnych aspektów związanych z:

- ograniczonych zasobów operacyjnych ze względu na rosnące potrzeby operacyjne państw członkowskich oraz stale ewoluujące cyberzagrożenia i cyberryzyko w dziedzinie cyberbezpieczeństwa.

- gwałtownego wzrostu budżetu przy oczekiwaniach szybkiego wdrożenia.

- brakiem odpowiednich zasobów finansowych i ludzkich, aby sprostać potrzebom operacyjnym.

2.2.3. Oszacowanie i uzasadnienie opłacalności kontroli (stosunek kosztów kontroli do wartości zarządzanych środków) oraz ocena oczekiwanego poziomu ryzyka błędu (w momencie płatności i zamknięcia)

Koszt poniesiony przez DG CNECT w związku z monitorowaniem i nadzorem powierzonych podmiotów, w tym ENISA, wynosi około 5,25 mln EUR, zgodnie z rocznym sprawozdaniem z działalności za 2024 r.[96] . Kwota ta obejmuje przede wszystkim koszty osobowe i stanowi 0,50 % płatności operacyjnych dokonanych na rzecz tych podmiotów w 2024 r. Ogólny wskaźnik kosztów kontroli nieznacznie wzrósł do 0,50 % w 2024 r. z 0,46 % w 2023 r., ale pozostaje stosunkowo stabilny w porównaniu z poprzednimi latami.

W odniesieniu do ENISA koszty kontroli w 2024 r. wyniosły 0,32 mln EUR, co stanowi 0,70 % kosztów kontroli w 2024 r., w porównaniu z 0,69 % w 2023 r. i 1,22 % w 2022 r. Analiza pokazuje, że wyższe koszty kontroli są związane głównie z przygotowaniem i monitorowaniem umów o wkładzie między Komisją a Agencją (głównie koszty zasobów ludzkich), które zgodnie z oczekiwaniami zostaną znacznie zmniejszone w nowym mandacie, co powinno przynieść wyższy poziom efektywności. Pod względem całkowitych kosztów dla DG CNECT w porównaniu z innymi podmiotami, którym powierzono zadania, ENISA plasuje się w środku stawki wśród 11 innych podmiotów.

Wniosek dotyczący CSA2 przewiduje zwiększenie liczby pracowników DG CNECT o 50 etatów w przeliczeniu na pełne etaty, z czego 1 dodatkowy etat w przeliczeniu na pełne etaty zostanie przydzielony specjalnie do zadań związanych z pełnieniem przez DG CNECT funkcji partnera DG dla Agencji. Osoba ta będzie wspierać przygotowanie opinii Komisji w sprawie jednolitego dokumentu programowego ENISA i monitorować jego wdrażanie; wspierać nadzór nad przygotowaniem budżetu Agencji i monitorować

95 https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

96 CNECT_AAR_2024_final

jego wdrażanie. Będzie ona również wspierać Agencję w rozwijaniu jej działalności zgodnie z polityką Unii, w tym poprzez udział w odpowiednich posiedzeniach. Działanie to jest uzasadnione zwiększonymi zadaniami monitorującymi DG CNECT, które między innymi przewidują oddanie pozytywnego głosu Komisji w kwestiach związanych z budżetem i zasobami ludzkimi. Należy zauważyć, że wdrożenie przepisów dotyczących wyznaczania krajów stwarzających strategiczne zagrożenia dla cyberbezpieczeństwa w odniesieniu do określonych kluczowych aktywów dostawców wysokiego ryzyka będzie procesem w pełni kierowanym przez Komisję. Szacowana liczba pracowników potrzebnych do przeprowadzenia ocen ryzyka w związku z powyższym wynosi 25 etatów w przeliczeniu na pełne etaty. Działanie to jest uzasadnione nakładem pracy wymaganym do wdrożenia ram polityki, a dokładniej wsparciem dla koordynowanych przez UE ocen ryzyka; analizą ekonomiczną każdego produktu/usługi ICT; przygotowaniem odpowiednich aktów wykonawczych i monitorowaniem wdrażania ram; przeprowadzaniem ocen własności i kontroli ( ). Oczekuje się, że na koszty kontroli ponoszone przez Komisję w związku z wdrażaniem ram dotyczących łańcucha dostaw szczególny wpływ będzie miała liczba ocen własności i kontroli (OCA), które Komisja będzie przeprowadzać. Wyniki tego zadania przyczynią się jednak w znacznym stopniu do oszczędności dla państw członkowskich w zakresie nadzorowania wdrażania środków łagodzących i obowiązków nałożonych na podmioty NIS2 przez ramy. Państwa członkowskie będą mogły bezpośrednio wykorzystać wyniki ocen OCA, zamiast indywidualnie wydawać środki na te same potrzeby w zakresie ocen. Wzmocnienie europejskich ram certyfikacji w zakresie cyberbezpieczeństwa, normalizacja i wdrożenie powiązanych działań, wdrożenie dyrektywy NIS2 (w tym odpowiednie potrzeby wdrożeniowe, opłaty za akty wykonawcze oraz wsparcie utrzymania systemów certyfikacji i systemów poświadczania umiejętności) oszacowano na 19 etatów w przeliczeniu na pełne etaty, natomiast polityka współpracy operacyjnej i świadomości sytuacyjnej wymaga dodatkowych 5 etatów w przeliczeniu na pełne etaty. Pełny opis zadań znajduje się w sekcji 3.2.4.

W swoim skonsolidowanym rocznym sprawozdaniu z działalności za 2023 r.[97] ENISA pozytywnie oceniła swoje systemy kontroli wewnętrznej i przedstawiła czyste poświadczenie wiarygodności. W swoim rocznym sprawozdaniu dotyczącym agencji UE za rok budżetowy 2023 ETO wydała czystą opinię z audytu dotyczącą sprawozdań finansowych oraz opinię z zastrzeżeniem dotyczącą legalności i prawidłowości płatności leżących u podstaw sprawozdań finansowych (o czym mowa również w pkt 2.2.2). DG CNECT przyjęła do wiadomości sprawozdanie, stwierdzając jednak, że nie ma ono wpływu na skuteczność nadzoru sprawowanego przez CNECT. ENISA regularnie składa również sprawozdania na temat środków podjętych w celu zapobieżenia ponownemu wystąpieniu stwierdzonych nieprawidłowości i na chwilę obecną nic nie wskazuje na to, aby w nadchodzących latach wskaźnik błędów uległ pogorszeniu/przekroczył 2 %.

Ponadto art. 80 ust. 2 przepisów finansowych ENISA[98] przewiduje możliwość współdzielenia przez agencję zdolności w zakresie audytu wewnętrznego z innymi organami Unii działającymi w tym samym obszarze polityki, jeżeli zdolność w zakresie audytu wewnętrznego pojedynczego organu Unii nie jest opłacalna.

97 enisa.europa.eu/sites/default/files/2024-11/2023_Skonsolidowane_roczne_sprawozdanie_z_działalności_1.pdf

98 Decyzja MB 2019_8 Zasady finansowe_przyjęte.pdf

Podsumowując, biorąc pod uwagę proponowane zwiększenie wielkości agencji o ponad 100 % w porównaniu ze stosunkowo niewielkim wzrostem kosztów kontroli, analiza wykazuje zadowalający stosunek opłacalności. Biorąc pod uwagę wszystkie dostępne dane, nic nie wskazuje na to, aby oczekiwany poziom błędu mógł przekroczyć 2 %.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa będzie stosować najwyższe standardy w zakresie zapobiegania nadużyciom finansowym i nieprawidłowościom.

Płatności za wszelkie zamówione usługi lub badania są sprawdzane przez pracowników agencji przed dokonaniem płatności, z uwzględnieniem wszelkich zobowiązań umownych, zasad ekonomicznych oraz dobrych praktyk finansowych lub zarządzania. Przepisy dotyczące zwalczania nadużyć finansowych (nadzór, wymogi sprawozdawcze itp.) zostaną uwzględnione we wszystkich umowach i kontraktach zawieranych między agencją a odbiorcami wszelkich płatności.

W celu zwalczania nadużyć finansowych, korupcji i innych niezgodnych z prawem działań bez ograniczeń stosuje się przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013.

3. SZACOWANY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Pozycja(-e) wieloletnich ram finansowych i pozycja(-e) wydatków w budżecie, na które ma wpływ wniosek

- Istniejące pozycje w budżecie

W kolejności zgodnej z pozycjami wieloletnich ram finansowych i pozycjami budżetowymi.

Pozycja wieloletnich ram finansowych	Pozycja w budżecie	Rodzaj wydatków	Wkład			
	Liczba	Zróżnicowane/Niezróżnicowane[99]	z krajów EFTA[100]	z krajów kandydujących i potencjalnych krajów kandydujących[101]	Z innych państw trzecich	inne dochody przeznaczone na określony cel
	[XX.YY.YY.YY]	Środki niepodzielone	TAK	NIE	NIE	TAK/NIE
	[XX.YY.YY.YY]	Różnica/ Brak różnicy	TAK/NIE	TAK/NIE	TAK/NIE	TAK/NIE

99 Diff. = Środki zróżnicowane / Non-diff. = Środki niezróżnicowane.

100 EFTA: Europejskie Stowarzyszenie Wolnego Handlu.

101 Kraje kandydujące oraz, w stosownych przypadkach, potencjalni kandydaci z regionu Bałkanów Zachodnich.

	[XX.YY.YY.YY]	Różnica/ Brak różnicy	TAK/NIE	TAK/NIE	TAK/NIE	TAK/NIE

- Nowe wnioskowane pozycje budżetowe

W kolejności zgodnej z pozycjami wieloletnich ram finansowych i pozycjami budżetowymi.

Pozycja wieloletnich ram finansowych	Pozycja budżetowa	Rodzaj wydatków	Wkład			
	Liczba	Zróżnicowane/Niezróżnicowane	z krajów EFTA	z krajów kandydujących i potencjalnych kandydatów	z innych państw trzecich	inne dochody przeznaczone na określony cel
	[XX.YY.YY.YY]	Różnica/ Brak różnicy	TAK/NIE	TAK/NIE	TAK/NIE	TAK/NIE
	[XX.YY.YY.YY]	Różnica/ Brak różnicy	TAK/NIE	TAK/NIE	TAK/NIE	TAK/NIE
	[XX.YY.YY.YY]	Różnica/ Brak różnicy	TAK/NIE	TAK/NIE	TAK/NIE	TAK/NIE

3.2. Szacowany wpływ wniosku na środki finansowe

3.2.1. Podsumowanie szacowanego wpływu na środki operacyjne

– ☐ Wniosek/inicjatywa nie wymaga wykorzystania środków operacyjnych

– ☒ Wniosek/inicjatywa wymaga wykorzystania środków operacyjnych, jak wyjaśniono poniżej

3.2.1.1. Środki z budżetu uchwalonego

w mln EUR (do trzech miejsc po przecinku)

Agencja: ENISA	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**ŁĄCZNA KWOTA WWFR 2028–2034**
Pozycja w budżecie: <…….> / Dodatkowy wkład z budżetu UE na rzecz agencji	20 900	20 594	25 338	26 801	26 801	26 301	26 301	173 006

Środki / wkład z budżetu UE na rzecz agencji zostaną zrekompensowane zmniejszeniem puli środków przeznaczonych na następujący program <…….> / pozycję budżetową: <…….> / w roku (latach): <…….>.

			Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**ŁĄCZNA KWOTA WWFR 2028–2034**
ŚRODKI OPERACYJNE OGÓŁEM	Zobowiązania	(4)	20 900	20 594	25 338	26 801	26 801	26 301	26 301	173 006
	Płatności	(5)	20 900	20 594	25 338	26 801	26 801	26 301	26 301	173 006
ŁĄCZNE środki administracyjne finansowane z puli środków przeznaczonych na konkretne programy		(6)	1 365	1 365	1 470	1 785	2100	2415	2625	**13 125**

ŁĄCZNE środki w ramach DZIAŁU 2 wieloletnich ram finansowych	Zobowiązania	=4+6	22 265	21 959	26 808	28 586	28 901	28 716	28 926	186 161
	Płatności	=5+6	22 265	20 890	24 851	26 254	26 254	25 754	25 754	186 161

DG: CNECT	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**ŁĄCZNA KWOTA WWPR 2028–2034**
• Zasoby ludzkie	**3693**	**3693**	**4574**	**5 277**	**5 980**	**6 683**	**7 475**	**37 375**
• Inne wydatki administracyjne	0	0	0	0	0	0	0	**0**

RAZEM DG CNECT	Środki	**3 693**	**3 693**	**4 574**	**5 277**	**6 980**	**6 683**	**7 475**	**37 375**

ŁĄCZNE środki w ramach DZIAŁU 4 wieloletnich ram finansowych	(Zobowiązania ogółem = Płatności ogółem)	**2 328**	**2 328**	**3 104**	**3 492**	**3 880**	**4 268**	**4 850**	**24,25**

mln EUR (do trzech miejsc po przecinku)

	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**ŁĄCZNA KWOTA WWFR 2028–2034**

ŁĄCZNE środki w ramach DZIELNIC 1–4	Zobowiązania	24 594	24 257	29 912	32 078	32 781	32 984	33 776	210,38
wieloletnich ram finansowych	Płatności	24 594	24 257	29 912	32 078	32 781	32 984	33 776	210,38

3.2.2. Szacunkowa wartość wyników finansowanych ze środków operacyjnych (nie dotyczy agencji zdecentralizowanych)

Środki na zobowiązania w mln EUR (z dokładnością do trzech miejsc po przecinku)

Wskazać cele i wyniki ⇩			Rok **2028**		Rok **2029**		Rok **2030**		Rok **2031**		Wprowadź tyle lat, ile jest konieczne, aby pokazać czas trwania wpływu (patrz sekcja 1.6)						**RAZEM**	
	WYNIKI																	
	Typ[102]	Średni koszt	Nie	Koszt	Nie	Koszt	Nie	Koszt	Nie	Koszt	Nie	Koszt	Nie	Koszt	Nie	Koszt	Razem Nie	Całkowity koszt
CEL SZCZEGÓŁOWY nr 1[103] …																		
- Wynik																		
- Wynik																		
- Wynik																		
Suma częściowa dla celu szczegółowego nr 1																		
CEL SZCZEGÓŁOWY nr 2 ...																		

102 Wyniki to produkty i usługi, które mają zostać dostarczone (np. liczba sfinansowanych wymian studenckich, liczba kilometrów wybudowanych dróg itp.

103 Zgodnie z opisem w sekcji 1.3.2. „Cele szczegółowe”.

- Wynik																		
Suma częściowa dla celu szczegółowego nr 2																		
RAZEM																		

3.2.3. Podsumowanie szacowanego wpływu na środki administracyjne

– ☐ Wniosek/inicjatywa nie wymaga wykorzystania środków administracyjnych

– ☒ Wniosek/inicjatywa wymaga wykorzystania środków administracyjnych, jak wyjaśniono poniżej

3.2.3.1. Środki z budżetu uchwalonego

(dodatkowe)

ŚRODKI ZATWIERDZONE	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**RAZEM 2028–2034**
POZYCJA 4								
Zasoby ludzkie	2 328	2 328	3 104	3 492	3 880	4 268	4 840	24,25
Inne wydatki administracyjne	0	0	0	0,00	0,00	0,000	0,000	0,000
Suma częściowa POZYCJA 4	2 328	2 328	3 104	3 492	3880	4268	4 840	24,25
Poza POZYCJĄ 4								
Zasoby ludzkie	1 365	1 365	1 470	1785	2100	2415	2625	**13 125**
Inne wydatki o charakterze administracyjnym	0	0	0	0,00	0,00	0,000	0,000	**0,000**
Suma częściowa poza POZYCJĄ 4	**1 365**	**1 365**	**1 470**	**1 785**	**2 100**	**2415**	**2625**	**13 125**
RAZEM	**3 693**	**3 693**	**4 574**	**5 277**	**5 980**	**6 683**	**7 475**	**37 375**

3.2.4. Szacunkowe zapotrzebowanie na zasoby ludzkie (dodatkowe)

– ☐ Wniosek/inicjatywa nie wymaga wykorzystania zasobów ludzkich

– ☒ Wniosek/inicjatywa wymaga wykorzystania zasobów ludzkich, jak wyjaśniono poniżej

3.2.4.1. Finansowane z budżetu uchwalonego

Szacunki wyrażone w ekwiwalentach pełnego czasu pracy (EPT)[104]

ŚRODKI PRZYZNANE	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**
• Stanowiska przewidziane w planie zatrudnienia (urzędnicy i pracownicy tymczasowi)							
20 01 02 01 (centrala i przedstawicielstwa Komisji)	12	12	16	18	20	22	25
20 01 02 03 (delegatury UE)	0	0	0	0	0	0	0
(Badania pośrednie)	0	0	0	0	0	0	0
(Badania bezpośrednie)	0	0	0	0	0	0	0
Inne pozycje budżetowe (proszę określić)	0	0	0	0	0	0	0
• Personel zewnętrzny (w pełnych etatach)							
20 02 01 (AC, END z „globalnej koperty”)	0	0	0	0	0	0	0

[104] W tabeli poniżej należy podać, ile etatów w ramach wskazanej liczby jest już przypisanych do zarządzania działaniem i/lub może zostać przeniesionych w ramach danej dyrekcji generalnej, a także jakie są potrzeby netto.

20 02 03 (AC, AL, END i JPD w delegaturach UE)		0	0	0	0	0	0	0
Linia wsparcia administracyjnego	- w siedzibie głównej	0	0	0	0	0	0	0
[XX.01.YY.YY]	- w delegaturach UE	0	0	0	0	0	0	0
(AC, END – badania pośrednie)		0	0	0	0	0	0	0
(AC, END – badania bezpośrednie)		0	0	0	0	0	0	0
Inne pozycje budżetowe (proszę określić) – Dział 4		0	0	0	0	0	0	0
Inne pozycje budżetowe (proszę określić) – poza działem 4		13	13	14	17	20	23	25
RAZEM		**25**	**25**	**30**	**35**	**40**	**45**	**50**

Personel niezbędny do realizacji wniosku (w etatach):

	Zostanie pokryty przez obecny personel dostępny w służbach Komisji	**Wyjątkowy dodatkowy personel**		
		Finansowanie z pozycji 7 lub z budżetu na badania	**Finansowanie z pozycji BA**	**Finansowanie z opłat**
Stanowiska przewidziane w planie zatrudnienia		25		
Personel zewnętrzny (CA, SNE, INT)			25	

Szacowany wpływ na wydatki i zatrudnienie w 2028 r. i w kolejnych latach ma charakter orientacyjny i nie przesądza o kształcie kolejnych wieloletnich ram finansowych. Źródło finansowania i zakres zobowiązań finansowych Unii w okresie po 2027 r. pozostają uzależnione od wyniku negocjacji międzyinstytucjonalnych dotyczących wieloletnich ram finansowych na lata 2028–2034 oraz rocznej procedury budżetowej i mechanizmu sterującego.

Opis zadań, które ma wykonać sektorowa dyrekcja generalna w ramach Komisji

Urzędnicy i pracownicy zatrudnieni na czas określony	**Koordynacja ENISA (1)**: Reprezentowanie Komisji w zarządzie agencji. Opracowywanie opinii Komisji w sprawie jednolitego dokumentu programowego ENISA i monitorowanie jego realizacji. Nadzorowanie przygotowywania budżetu agencji i monitorowanie jego realizacji. Pomoc agencji w rozwijaniu jej działalności zgodnie z polityką Unii, w tym poprzez udział w odpowiednich posiedzeniach. **Systemy poświadczania umiejętności / Akademia Umiejętności (2)**: W CNECT potrzebni będą dodatkowi pracownicy do przygotowania aktów wykonawczych ustanawiających opłaty, które ENISA będzie pobierać od wnioskodawców ubiegających się o status autoryzowanego dostawcy. Aktów wykonawczych będzie co najmniej 12, po jednym dla każdego profilu ECSF. **Łańcuch dostaw** (25) Wspieranie przygotowywania skoordynowanych ocen ryzyka Unii. Przeprowadzanie analiz ekonomicznych dla każdego rozpatrywanego produktu lub usługi ICT. Opracowywanie odpowiednich aktów wykonawczych dotyczących identyfikacji kluczowych aktywów, proponowanych środków łagodzących i wyznaczania krajów stanowiących strategiczne zagrożenie dla cyberbezpieczeństwa określonych kluczowych aktywów, identyfikacji dostawców wysokiego ryzyka, weryfikacji wniosków o zwolnienie i przygotowywania decyzji Komisji. Wspieranie wdrażania i nadzorowania przyjętych środków. **Europejskie ramy certyfikacji cyberbezpieczeństwa, normalizacja i wdrażanie powiązanych działań, wdrożenie dyrektywy NIS2 (17)**: Egzekwowanie CSA, w szczególności zarządzanie CAB (wyzwanie związane z obowiązkami) Zaangażowanie zainteresowanych stron (i zgromadzenie) Wzajemne uznawanie z państwami trzecimi Opracowanie znormalizowanego aktu wykonawczego (szczegółowe wnioski podlegające konsultacjom i opracowaniu wzorcowych przepisów) Utrzymanie systemu, przegląd prawny, procedura komitologii Koordynacja z NIS CG i utrzymanie systemu podmiotów Akty wykonawcze na mocy dyrektywy NIS2 Dostosowanie CAB do CSA, domniemanie zgodności + normalizacja Koordynacja między nadzorem rynku a NCCA Dostosowanie techniczne między CRA a systemami certyfikacji **Koordynacja operacyjna i świadomość sytuacyjna (5)**: Wiedza ekspercka w zakresie sektorów i podmiotów stanowiących zagrożenie, przyczyniająca się do świadomości sytuacyjnej na poziomie UE w zakresie zagrożeń dla infrastruktury krytycznej, w tym poprzez nowe technologie Koordynacja z ENISA i innymi podmiotami i sieciami UE w celu przygotowania się na poważne i zakrojone na szeroką skalę incydenty cybernetyczne
Personel zewnętrzny	Jak powyżej

Opis dodatkowych zadań, które ma wykonać ENISA:

Urzędnicy i pracownicy tymczasowi	Zarządzanie rezerwą UE ds. cyberbezpieczeństwa (kierownicy krajowi i wsparcie dla wdrażania, przy czym rzeczywiste koszty operacyjne rezerwy są pokrywane zgodnie z przepisami ustawy o solidarności cybernetycznej) (10) Zarządzanie CRA w ramach jednolitej platformy sprawozdawczej (SRP) (działalność operacyjna) (9) Usługi związane z podatnością na zagrożenia powiązane z SRP (4) Rozszerzenie SRP na pojedynczy punkt kontaktowy (rozwój i eksploatacja) (8) Opracowanie wytycznych technicznych, wiedzy specjalistycznej w zakresie bezpieczeństwa produktów i analizy rynku w celu wsparcia wdrożenia CRA (7) Standaryzacja w celu wsparcia wdrożenia CRA / certyfikacja / NIS2 (4) Wspieranie działań CRA w zakresie nadzoru rynku (4) Wspieranie badań zgodności i ocen bezpieczeństwa produktów (4) Wspieranie państw członkowskich w zakresie wzajemnej pomocy (3) Świadczenie usług w zakresie zarządzania podatnością na zagrożenia, utrzymywanie EUVD oraz pełnienie funkcji doradczych i wzbogacających (CVD) (15) Współpraca operacyjna i świadomość sytuacyjna – platformy łagodzące skutki i wspierające, takie jak CNW/CyCLONe; wspieranie zadań związanych z powiadomieniami o zagrożeniach; wspieranie lepszej koordynacji z innymi odpowiednimi podmiotami w celu opracowania repozytoriów zweryfikowanych, wiarygodnych informacji o cyberzagrożeniach (art. 11 ust. 1a CSA2) (5) Wsparcie odporności sektorów krytycznych (w tym wdrożenie planu działania w zakresie cyberbezpieczeństwa w służbie zdrowia) (4) Opracowanie systemu poświadczania umiejętności (2) Utrzymanie i nadzór nad systemem poświadczania umiejętności (6) Administracja (księgowość opłat/HR/IT) (8) Utrzymanie systemów certyfikacji (11) Zadania horyzontalne – zwiększenie zaangażowania zainteresowanych stron, opracowywanie specyfikacji technicznych i udział w działaniach normalizacyjnych wspierających systemy (1)
Personel zewnętrzny	Jak powyżej Dwóch obowiązkowych oddelegowanych ekspertów krajowych (SNEs) z każdego państwa członkowskiego w celu wsparcia działań Agencji i pełnienia funkcji krajowych oficerów łącznikowych, ze szczególnym uwzględnieniem współpracy operacyjnej i skoordynowanego ujawniania luk w zabezpieczeniach. (13) Pozostałe 27 oddelegowanych ekspertów krajowych nie generuje żadnych kosztów, a zatem nie ma wpływu na budżet.

Dodatkowe koszty operacyjne ENISA w latach 2028–2034:

Koszt	Budżet	Harmonogram	Wyjaśnienie
Strona internetowa poświęcona umiejętnościom w	750 000 EUR	50 % w 2029 r. 50 % w 2030 r.	Aby zapewnić przejrzystość procedur, wniosek wymaga od ENISA prowadzenia

zakresie cyberbezpieczeństwa			strony internetowej zawierającej profile ECFS, systemy certyfikacji , informacje o opłatach za każdy system, zalecane opłaty za każdą certyfikację oraz wykaz uprawnionych podmiotów certyfikujących.
Skoordynowane ujawnianie luk w zabezpieczeniach (CVD)	1 mln EUR	Od 2028 r.	Bezpieczeństwo produktów i usług wykorzystywanych w naszej infrastrukturze krytycznej w dużym stopniu zależy od terminowego udostępniania informacji o wykrytych lukach w zabezpieczeniach i sposobach ich ograniczania.
Analiza zagrożeń cyberbezpieczeństwa	3 mln EUR	Od 2028 r.	W celu stworzenia wspólnego obrazu sytuacji we współpracy z ENISA i Komisją.
Pojedynczy punkt kontaktowy	8 mln EUR	6 mln EUR w 2028 r. 500 tys. EUR w 2029 r. 500 tys. EUR w 2030 r. 500 tys. EUR w 2031 r. 500 tys. EUR w 2032 r.	Aby móc zrealizować wniosek Komisji dotyczący pakietu cyfrowego, mającego na celu uproszczenie zgodności z obowiązkami w zakresie zgłaszania incydentów związanych z cyberbezpieczeństwem i naruszeniami danych poprzez opracowanie i utrzymanie jednego punktu kontaktowego.
Utrzymanie CRA SRP i inne	3 mln EUR	Od 2028 r.	SRP wprowadzony przez współprawodawców jest największym

			systemem informatycznym, jaki kiedykolwiek opracowano w historii ENISA, i stanowi kluczowy filar CRA. Utworzenie systemu jest obecnie finansowane w ramach umowy o wkładzie, ale jego bieżące zarządzanie będzie wymagało etatów (zob. powyżej) oraz pokrycia kosztów operacyjnych. ENISA ma do odegrania kluczową rolę w zapewnieniu sukcesu unijnych ram bezpieczeństwa produktów, czyli CRA.
Bezpieczna komunikacja i dojrzałość ENISA w zakresie cyberbezpieczeństwa	2 mln EUR +	1,1 mln EUR inwestycji w 2028 r. (platformy CyCLONe/CSIRT + bezpieczna komunikacja) 1 mln EUR rocznie na utrzymanie od 2029 r. 1,5 mln EUR na dojrzałość cyberbezpieczeństwa	Zapewnienie cyberbezpieczeństwa agencji i narzędzi komunikacyjnych.
Utrzymanie certyfikatu cyberbezpieczeństwa	1 400 000 mln EUR	2028 600 tys. 2029 1 000 000 2030 1 200 000 2031 1 400 00 2032 1 400 000 2033 1 400 000 2034 1 400 000	Pokryte opłatami (w całości od 2032 r.)

Systemy certyfikacji cyberbezpieczeństwa	212920 EUR	Od 2030 r. w 50 % pokryte z budżetu UE	W całości pokryte z opłat od 2033 r.

3.2.5. Przegląd szacowanego wpływu na inwestycje związane z technologiami cyfrowymi

Obowiązkowe: w poniższej tabeli należy podać najlepsze szacunki dotyczące inwestycji związanych z technologiami cyfrowymi wynikających z wniosku/inicjatywy.

W wyjątkowych przypadkach, gdy jest to konieczne do realizacji wniosku/inicjatywy, środki w ramach działu 4 należy przedstawić w wyznaczonej pozycji.

Środki w ramach działów 1–3 należy wykazać jako „Wydatki na politykę informatyczną w ramach programów operacyjnych”. Wydatki te odnoszą się do budżetu operacyjnego, który ma być wykorzystany na ponowne wykorzystanie/zakup/opracowanie platform/narzędzi informatycznych bezpośrednio związanych z realizacją inicjatywy oraz związanych z nimi inwestycji (np. licencji, badań, przechowywania danych itp.). Informacje podane w tej tabeli powinny być zgodne ze szczegółowymi danymi przedstawionymi w sekcji 4 „Wymiar cyfrowy”.

ŁĄCZNE środki na technologie cyfrowe i IT	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**ŁĄCZNA KWOTA WWFR 2028–2034**
POZYCJA 4								
Wydatki na IT (korporacyjne)	0	0	0	0	0	0	0	**0**
Suma częściowa POZYCJA 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Poza POZYCJĄ 4								
Polityka Wydatki na IT w ramach programów operacyjnych	0	0	0	0	0	0	0	**0**
Suma częściowa poza POZYCJĄ 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
RAZEM	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

3.2.6. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

Wniosek/inicjatywa:

– ☒ może być w całości sfinansowana poprzez przesunięcie środków w ramach odpowiedniego działu wieloletnich ram finansowych (WRF)

Bez uszczerbku dla negocjacji w sprawie kolejnych WRF, środki przyznane agencji od 2028 r. zostaną zrekompensowane poprzez przesunięcia z programów w ramach WRF na lata 2028–2034. Jeżeli konieczne będzie dokonanie redukcji wyrównawczej, może zaistnieć potrzeba zmiany środków przyznanych agencji oraz ich strumieni i źródeł finansowania.

– ☐ wymaga wykorzystania nieprzydzielonego marginesu w ramach odpowiedniej pozycji WRF i/lub wykorzystania specjalnych instrumentów określonych w rozporządzeniu w sprawie WRF

– ☐ wymaga zmiany WRF

3.2.7. Wkłady stron trzecich

Wniosek/inicjatywa:

– ☒ nie przewiduje współfinansowania przez osoby trzecie

– ☐ przewiduje współfinansowanie przez strony trzecie w wysokości szacowanej poniżej:

Środki w mln EUR (z dokładnością do trzech miejsc po przecinku)

	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Razem
Określić organ współfinansujący					
ŁĄCZNA kwota środków współfinansowanych					

3.2.8 Szacunkowe zasoby ludzkie i wykorzystanie środków wymaganych w zdecentralizowanej agencji

Dodatkowe zapotrzebowanie na personel (jednostki ekwiwalentu pełnego czasu pracy)

Agencja: ENISA	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**
Pracownicy tymczasowi (stopnie AD)	5	11	17	19	19	19	19
Pracownicy tymczasowi (stopnie AST)	4	7	11	12	12	12	12
Pracownicy tymczasowi (AD+AST) – suma częściowa	***9***	***18***	***28***	***31***	***31***	***31***	***31***
Agenci kontraktowi	22	44	66	74	74	74	74
Oddelegowani eksperci krajowi	4	8	11	13	13	13	13
Agenci kontraktowi i oddelegowani eksperci krajowi – suma częściowa	26	52	77	87	87	87	87
ŁĄCZNA LICZBA PRACOWNIKÓW	35	70	105	118	118	118	118

Środki objęte wkładem z budżetu UE w mln EUR (z dokładnością do trzech miejsc po przecinku)

Agencja: ENISA	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**RAZEM 2028–2034**
Tytuł 1: Wydatki na personel	4 488	8 466	12 507	13 648	10 584	10 012	9 537	**87 766**
Tytuł 2: Infrastruktura i wydatki operacyjne								
Tytuł 3: Wydatki operacyjne	16 413	11 588	11 528	11 788	11 613	11 613	11 113	**85 240**
ŁĄCZNA kwota środków przewidzianych w budżecie UE	**20 901**	**20 054**	**24 035**	**25 437**	**22 197**	**21 625**	**21 151**	**155,4**

Środki pokryte z opłat, jeśli dotyczy, w mln EUR (z dokładnością do trzech miejsc po przecinku)

Agencja: ENISA	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**RAZEM 2028–2034**
Tytuł 1: Wydatki na personel		0,510	1 043	1 539	4 604	5 176	5 650	**18 522**
Tytuł 2: Infrastruktura i wydatki operacyjne								**0**
Tytuł 3: Wydatki operacyjne								**0,00**
OGÓŁEM środki pokryte z opłat	**0,000**	**0,510**	**1 043**	**1 539**	**4 604**	**5 176**	**5 650**	**18 522**

Przegląd/podsumowanie zasobów ludzkich i środków finansowych (w mln EUR) wymaganych w związku z wnioskiem/inicjatywą w zdecentralizowanej agencji

Agencja: ENISA	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**RAZEM 2028–2034**
Pracownicy tymczasowi (AD+AST)	9	18	28	31	31	31	31	*31*
Agenci kontraktowi	22	44	66	74	74	74	74	74
Oddelegowani eksperci krajowi	4	8	11	13	13	13	13	13
Całkowita liczba pracowników	35	70	105	118	118	118	118	**118**

Środki finansowe pokrywane z budżetu UE	**20 901**	**20 054**	**24 035**	**25 437**	**22 197**	**21 625**	**21 151**	**155,4**
Środki pokryte z opłat (jeśli dotyczy)	**0**	**0,510**	**1 043**	**1 539**	**4 604**	**5 176**	**5 650**	**18 522**
Środki współfinansowane (jeśli dotyczy)	0,000	0,00	0,00	0,00	0,00	0,000	0,000	**0,000**
ŚRODKI OGÓŁEM	**20 901**	**20 564**	**25 078**	**26 976**	**26 801**	**26 801**	**26 801**	**173 922**

3,3 Szacowany wpływ na dochody

– ☒ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

– ☐ Wniosek/inicjatywa ma następujący wpływ finansowy:

  – ☐ na zasoby własne

  – ☐ na inne dochody

  – ☐ proszę wskazać, czy dochody są przypisane do pozycji wydatków

w mln EUR (z dokładnością do trzech miejsc po przecinku)

Pozycja w dochodach budżetu:	Środki dostępne w bieżącym roku budżetowym	Wpływ wniosku/inicjatywy[105]						
		Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**
Artykuł …….								

W przypadku dochodów przeznaczonych na określony cel należy określić pozycję lub pozycje wydatków budżetowych, których dotyczy dana zmiana.

Inne uwagi (np. metoda/wzór zastosowany do obliczenia wpływu na dochody lub inne informacje).

Mechanizmy opłat są związane z trzema obszarami działalności ENISA:

- Opłaty związane z udzielaniem zezwoleń dostawcom w ramach europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa.

Opłaty związane z tą działalnością zostaną ustalone w akcie wykonawczym po przyjęciu zmienionej ustawy o cyberbezpieczeństwie. Aby jednak móc oszacować niezbędne inwestycje i koszty, obliczenia dokonano przy użyciu modelu istniejącego w jednym z państw członkowskich UE[106] . Model ten obejmuje opłatę jednorazową i opłatę roczną.

105 W odniesieniu do tradycyjnych zasobów własnych (cła, opłaty cukrowe) wskazane kwoty muszą być kwotami netto, tj. kwotami brutto po odliczeniu 20 % kosztów poboru.

106 Decyzja RR-02: Cennik usług SNAS: https://www.snas.sk/storage/app/uploads/public/677/e79/e4c/677e79e4cac62903312474.pdf,

Koszty stałe: 8540 EUR

Opłata roczna: 800 EUR

Opłaty mają na celu refinansowanie kosztów tej konkretnej działalności. Koszty oszacowano na 1 064 600 EUR w okresie 5 lat. Szczegółowe koszty działań uwzględnione w tej kwocie są związane z opracowaniem i utrzymaniem systemów, w tym z wydatkami członków grupy roboczej ad hoc, która wspierałaby ENISA w opracowywaniu systemów (zwrot kosztów i wynagrodzenie sprawozdawców), misjami kontrolnymi u dostawców na miejscu oraz szkoleniem oceniających w celu zapewnienia jednolitego stosowania systemów:

A) grupa robocza ad hoc kosztowałaby 800 000 EUR

B) szkolenie dwóch oceniających na państwo członkowskie wyniosłoby 129 600 EUR

C) kontrola jednego podmiotu w każdym państwie członkowskim wyniosłaby 135 000 EUR

(A + B + C) / 5 = 212 920 EUR kosztów rocznie

Wniosek przewidywał okres przejściowy i początkowe inwestycje w ciągu pierwszych trzech lat. W okresie przejściowym koszty będą pokrywane z budżetu UE, a w czwartym i piątym roku pokrycie wyniesie 50%, w szóstym i siódmym roku – pełne zastosowanie opłat.

Rok	Opłaty
2028	0
2029	0
2030	0
2031	106 460 (przychody)
2032	106 460 (przychody)
2033	212 920 (przychody)
2034	212 920 (przychody)

- Opłaty związane z pokryciem kosztów utrzymania systemu certyfikacji cyberbezpieczeństwa, przyjętego w ramach europejskich ram certyfikacji cyberbezpieczeństwa (ECCF).

Opłaty związane z tą działalnością zostaną określone w akcie wykonawczym po przyjęciu zmienionej ustawy o cyberbezpieczeństwie. Szacunki kosztów utrzymania systemu opierają się na analizie rynku zawartej w ocenie skutków wniosku dotyczącego zmiany ustawy o cyberbezpieczeństwie. Łączne koszty działalności w okresie 5 lat wynoszą 5 600 000 EUR w przypadku kosztów operacyjnych i 7 100 000 EUR w przypadku etatów.

Roczny koszt działań związanych z utrzymaniem systemu szacuje się na podstawie dotychczasowych doświadczeń na 200 000 EUR za jeden rok utrzymania

systemu[107] i 2 etaty w pełnym wymiarze czasu pracy przeznaczone na takie działania (przy rocznym koszcie 125 887 EUR na etat w pełnym wymiarze czasu pracy), biorąc pod uwagę przewidywany rok przyjęcia takich systemów. Oczekuje się, że przychody z tych opłat będą rosły wraz z przyjęciem każdego nowego systemu i stopniowym wdrażaniem takich systemów. Jak dotąd przyjęto jeden system (EUCC) w ramach ECCF, a pierwsze przychody z utrzymania tego systemu spodziewane są w 2029 r. Oczekuje się, że koszty zostaną pokryte do 2032 r.

Szacunkowe przychody zostały obliczone przy przyjęciu konkretnych założeń dla każdego potencjalnego systemu w odniesieniu do następujących aspektów: oczekiwane wykorzystanie (liczba certyfikatów, które mają zostać wydane), okres ważności każdego certyfikatu oraz liczba aktywnych jednostek oceniających zgodność. Oczekuje się, że znaczne przychody będą pochodzić z wykorzystania przyszłego systemu cyberbezpieczeństwa.

Rok Przychody (procent kosztów pokrytych/opłaconych z budżetu UE)

2028 0

2029 250 000 (11 %/ - 1 350 000 EUR) – jeden program (EUCC)

2030 783 000 (29 %/ - 2 000 000 EUR) – trzy programy (EUCC, ID Wallet, MSS)

2031 783 000 (25 %/ - 1 930 000 EUR) – trzy programy (EUCC, ID Wallet, MSS)

2032 3 850 000 (122 %/ - 2 400 000 EUR) – pięć programów (EUCC, ID Wallet, MSS, EUCS, 5G)

2033 4 000 000 (126 %/ + 685 000 EUR) – sześć programów (EUCC, ID Wallet, MSS, EUCS, 5G, Cyberposture)

2034 4 500 000 (141 %/ + 825 000 EUR) – siedem programów

Opłaty związane z narzędziami testowymi wspierającymi procedury oceny zgodności

Opłaty związane z tą działalnością zostaną ustalone w akcie wykonawczym po przyjęciu zmienionej ustawy o cyberbezpieczeństwie. Jednakże w celu wskazania szacunkowych kosztów i oczekiwanych dochodów dokonano obliczeń na podstawie szacunków przedstawionych przez ENISA i uwzględnionych w ocenie skutków wniosku dotyczącego zmiany ustawy o cyberbezpieczeństwie. Koszty związane ze wsparciem działań w zakresie testowania i oceny szacuje się na:

Pełne etaty: 4 rocznie

Koszty operacyjne: 800 tys. rocznie

Koszty ogółem: 6 500 000 mln (5 lat); rocznie: 1 300 000 EUR

[107] W szczególności utrzymanie obejmuje 2 spotkania z ekspertami w ciągu roku (100 000 EUR), koszty wykonawców wspierających opracowywanie i przegląd dokumentacji uzupełniającej dla systemu, wdrażanie systemów certyfikacji, wspieranie ocen wzajemnych i wdrażanie ocen zgodności (4 x 15 000 = 60 000 EUR). Koszt obejmuje również część operacyjną platformy CEF i stronę internetową ENISA poświęconą certyfikacji (40 000 EUR).

Oczekuje się, że w przypadku ENISA w pierwszym roku poniesione zostaną jednorazowe inwestycje, a następnie koszty utrzymania. Koszty te będą stopniowo pokrywane z dochodów uzyskanych z opłat.

Rok	Przychody
2028	0
2029	260 000
2030	260 000
2031	650 000
2032	650 000
2033	975 000
2034	975 000

4. WYMIARY CYFROWE

4.1. Wymagania dotyczące znaczenia cyfrowego

Ogólny opis wymagań dotyczących znaczenia cyfrowego i powiązanych kategorii (dane, cyfryzacja i automatyzacja procesów, rozwiązania cyfrowe i/lub cyfrowe usługi publiczne)

Odniesienie do wymogu	**Opis wymogu**	**Podmioty, których dotyczy lub które są zainteresowane wymogiem**	**Procesy wysokiego poziomu**	**Kategorie**
Artykuł 5 ust. 1 lit. a) Wsparcie wdrażania prawa UE	a) pomoc państwom członkowskim w spójnym wdrażaniu polityki i prawa Unii w zakresie cyberbezpieczeństwa, w tym **poprzez wydawanie wytycznych technicznych i sprawozdań, udzielanie porad i dzielenie się najlepszymi praktykami oraz ułatwianie wymiany najlepszych praktyk między właściwymi organami w tym zakresie**;	- ENISA - Państwa członkowskie	- przetwarzanie danych w celu wydawania wytycznych technicznych, sprawozdań, udzielania porad i dzielenia się najlepszymi praktykami oraz ułatwianie wymiany najlepszych praktyk między właściwymi organami - ułatwianie wymiany najlepszych praktyk	Przetwarzanie danych Przepływ danych
Artykuł 5 ust. 1 lit. b) Wsparcie w zakresie wdrażania prawa UE	b) wspieranie **wymiany informacji w ramach sektorów i pomiędzy nimi, w szczególności w odniesieniu do sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555** oraz produktów zawierających elementy cyfrowe objętych zakresem rozporządzenia (UE) 2024/2847, **poprzez udostępnianie najlepszych praktyk i wytycznych dotyczących dostępnych narzędzi i procedur**	– ENISA – sektory wymienione w załącznikach I i II do dyrektywy (UE) 2022/2555 - zainteresowane strony, na które ma wpływ rozporządzenie (UE) 2024/2847	zapewnienie najlepszych praktyk i wytycznych dotyczących dostępnych narzędzi i procedur w zakresie wymiany informacji	Przetwarzanie danych Przepływ danych

Artykuł 5 ust. 1 lit. c) Wsparcie w zakresie wdrażania prawa UE	c na wniosek Komisji, wspieranie państw członkowskich poprzez zapewnianie pomocy, takiej jak **wytyczne techniczne, w tym dotyczące środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa, narzędzi oceny dojrzałości cyberbezpieczeństwa oraz podręczników reagowania na incydenty**, dostosowanych do sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555, w celu ułatwienia poprawy poziomu dojrzałości cyberbezpieczeństwa tych państw oraz zapewnienia zgodności z prawem Unii w zakresie cyberbezpieczeństwa;	– Komisja Europejska - ENISA - sektory wymienione w załącznikach I i II do dyrektywy (UE) 2022/2555	Zapewnienie wsparcia technicznego	Przetwarzanie danych Przepływ danych
Artykuł 5 ust. 1 lit. e)	e) wspieranie państw członkowskich i odpowiednich podmiotów unijnych w **opracowywaniu i promowaniu polityki w zakresie cyberbezpieczeństwa** związanej z utrzymaniem ogólnej dostępności i integralności publicznej podstawowej struktury otwartego internetu;	ENISA Państwa członkowskie Podmioty UE	Pomoc w opracowywaniu i promowaniu polityki w zakresie cyberbezpieczeństwa	Przetwarzanie danych Przepływ danych
Artykuł 5 ust. 1 lit. f) Wsparcie w zakresie wdrażania prawa UE	f) zgodnie z rozporządzeniem (UE) 2024/2847, **zapewnianie doradztwa technicznego i wsparcia** w kwestiach związanych z wdrażaniem i egzekwowaniem tego rozporządzenia	– ENISA - zainteresowane strony, na które ma wpływ rozporządzenie (UE) 2024/2847	Udzielanie porad technicznych i wsparcia wymaga przetwarzania i udostępniania informacji na temat wymogów regulacyjnych, wyzwań związanych z wdrażaniem oraz wytycznych dotyczących zgodności.	Przetwarzanie danych Przepływ danych
Artykuł 5 ust. 1 lit. h)	h) na wniosek Europejskiej Rady Ochrony Danych – doradztwo w zakresie wdrażania określonych aspektów polityki i prawa Unii dotyczących cyberbezpieczeństwa w odniesieniu do ochrony danych i prywatności.	ENISA EGPD	Udzielanie porad na wniosek	Przetwarzanie danych Przepływ danych

Artykuł 5 ust. 2 Wkład w ocenę ryzyka w zakresie cyberbezpieczeństwa na poziomie Unii	ENISA wnosi wkład w skoordynowane oceny ryzyka w zakresie cyberbezpieczeństwa na poziomie Unii, w tym oceny przeprowadzane zgodnie z art. 22 dyrektywy (UE) 2022/2555.	ENISA Państwa członkowskie Ogół społeczeństwa	Przyczynianie się do skoordynowanych ocen ryzyka, co wymaga przetwarzania danych i przepływu danych	Przetwarzanie danych Przepływ danych
Artykuł 5 ust. 3 ENISA wydaje wytyczne	ENISA **wydaje wytyczne** dotyczące interoperacyjności sieci i systemów informatycznych wykorzystywanych do wymiany informacji, w tym w odniesieniu do transgranicznych centrów cyberbezpieczeństwa, o których mowa w art. 6 ust. 3 rozporządzenia (UE) 2025/38.	ENISA Państwa członkowskie	ENISA wydaje wytyczne	Przetwarzanie danych Przepływ danych
Artykuł 5 ust. 5 Wsparcie dla Komisji	Na **wniosek Komisji** ENISA **zapewnia wiedzę fachową, doradztwo techniczne, informacje lub analizy lub wykonuje prace przygotowawcze** dotyczące konkretnych kwestii związanych z cyberbezpieczeństwem w celu dostarczenia Komisji informacji przydatnych w kształtowaniu polityki i monitorowaniu wdrażania prawodawstwa unijnego.	Komisja Europejska ENISA	Przygotowywanie i przesyłanie informacji do Komisji	Przetwarzanie danych Przepływ danych

Artykuł 6 Budowanie potencjału	ENISA udziela wsparcia poprzez udostępnianie wiedzy i doświadczenia, najlepszych praktyk itp.	ENISA Państwa członkowskie Podmioty UE Podmioty publiczne i prywatne Organy nadzoru rynku Członkowie ECCG ECCC	Dostarczanie wiedzy i doświadczenia	Przetwarzanie danych Przepływ danych
Artykuł 7 Podnoszenie świadomości i baza talentów	ENISA wspiera państwa członkowskie w ich działaniach na rzecz podnoszenia świadomości na temat polityki i prawodawstwa Unii w zakresie cyberbezpieczeństwa oraz promowania ich widoczności **poprzez opracowywanie praktycznych narzędzi i wytycznych**. ENISA wspiera inicjatywy mające na celu zwiększenie puli europejskich talentów w dziedzinie cyberbezpieczeństwa, w szczególności poprzez koordynację konkursów.	ENISA Państwa członkowskie	Opracowywanie praktycznych narzędzi i wytycznych	Przetwarzanie danych
Artykuł 8 ust. 1 Znajomość rynku i analizy	ENISA **przeprowadza i rozpowszechnia analizy** głównych trendów rynkowych na rynku cyberbezpieczeństwa, zarówno po stronie popytu, jak i podaży, w szczególności w odniesieniu do obszarów, w których istnieją lub są planowane europejskie systemy certyfikacji cyberbezpieczeństwa, sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555 oraz kategorii produktów objętych rozporządzeniem (UE) 2024/2847, w tym załącznikami III i IV do tego rozporządzenia.	ENISA Sektory wymienione w załącznikach I i II do dyrektywy (UE) 2022/2555 Kategorie produktów objęte rozporządzeniem (UE) 2024/2847	Przeprowadzanie i rozpowszechnianie analiz	Przetwarzanie danych Przepływ danych

Artykuł 8 ust. 2 Znajomość rynku i analizy	ENISA **przeprowadza i rozpowszechnia analizy** trendów technologicznych w zakresie cyberbezpieczeństwa, w szczególności w odniesieniu do działań i podmiotów objętych zakresem stosowania dyrektywy (UE) 2022/2555 oraz produktów zawierających elementy cyfrowe objętych zakresem stosowania rozporządzenia (UE) 2024/2847.	ENISA Ogół społeczeństwa, zainteresowane strony w rozumieniu dyrektywy (UE) 2022/2555 i rozporządzenia (UE) 2024/2847	Przeprowadzanie i rozpowszechnianie analiz	Przetwarzanie danych Przepływ danych
Artykuł 8 ust. 3 Znajomość rynku i wsparcie dla ekosystemów	ENISA gromadzi wiedzę oraz **rozpowszechnia porady techniczne i analizy** dotyczące najnowocześniejszych narzędzi, ram, standardów i najlepszych praktyk w zakresie cyberbezpieczeństwa.	ENISA Ogół społeczeństwa	Rozpowszechnianie porad technicznych i analiz dotyczących najnowocześniejszych narzędzi, ram, standardów i najlepszych praktyk w zakresie cyberbezpieczeństwa.	Przetwarzanie danych Przepływ danych
Artykuł 9 Współpraca międzynarodowa	ENISA wnosi wkład poprzez analizowanie wyników międzynarodowych ćwiczeń i składanie sprawozdań z nich zarządowi, ułatwianie wymiany najlepszych praktyk oraz zapewnianie Komisji wiedzy fachowej i doradztwa.	Międzynarodowa publiczność ENISA Zarząd ENISA Komisja Europejska	Analizowanie i raportowanie; udzielanie porad itp.	Przetwarzanie danych Przepływ danych
Artykuł 10 ust. 2 i 3 Współpraca operacyjna	2. ENISA jest członkiem sieci krajowych zespołów CSIRT ustanowionych zgodnie z art. 15 ust. 1 dyrektywy (UE) 2022/2555 i **pełni funkcję sekretariatu** sieci CSIRT zgodnie z art. 15 ust. 2 dyrektywy (UE) 2022/2555.	ENISA CSIRT (art. 15 ust. 1 dyrektywy (UE) 2022/2555) EU-CyCLONe (art. 16 ust. 2 dyrektywy (UE) 2022/2555)	Ułatwianie wymiany informacji, pełnienie funkcji sekretariatu sieci	Przepływ danych Rozwiązanie cyfrowe

	3. ENISA **pełni funkcję sekretariatu** europejskiej sieci organizacji łącznikowych ds. cyberkryzysów (EU-CyCLONe) zgodnie z art. 16 ust. 2 akapit drugi dyrektywy (UE) 2022/2555.			Cyfrowa usługa publiczna
Artykuł 11 ust. 1 lit. b) Świadomość sytuacyjna Artykuł 12 Wczesne ostrzeganie	**wydawanie wczesnych ostrzeżeń** zgodnie z art. 12	Komisja Europejska ENISA Europol EU-CyCLONe Sieć CSIRT CERT-EU Podmioty wymienione w załącznikach I i II do dyrektywy (UE) 2022/2555	Wydawanie wczesnych ostrzeżeń	Przetwarzanie danych Przepływ danych Cyfrowa usługa publiczna
Artykuł 10 ust. 4 lit. b) Współpraca operacyjna	b) na wniosek jednego lub kilku państw członkowskich, **udzielanie porad i ocen w odniesieniu do konkretnego potencjalnego lub trwającego incydentu lub cyberzagrożenia**, w tym poprzez zapewnienie wiedzy fachowej i **ułatwianie technicznego postępowania w przypadku takich incydentów** oraz poprzez **wspieranie dobrowolnej wymiany odpowiednich informacji i rozwiązań technicznych między państwami członkowskimi;**	ENISA Państwa członkowskie	Udzielanie porad i ocen w odniesieniu do konkretnego potencjalnego lub trwającego incydentu lub zagrożenia cybernetycznego; Ułatwianie technicznej obsługi takich incydentów; Wspieranie dobrowolnej wymiany odpowiednich informacji i rozwiązań technicznych między państwami członkowskimi	Przetwarzanie danych Przepływ danych Cyfrowe usługi publiczne

Artykuł 10 ust. 4 lit. c) Współpraca operacyjna	c) analizowanie słabych punktów, zagrożeń i incydentów;	ENISA Państwa członkowskie	Gromadzenie danych ze źródeł publicznych i wymiana danych z państwami członkowskimi	Przetwarzanie danych Przepływ danych
Artykuł 10 ust. 4 lit. d) Współpraca operacyjna	d) na **wniosek jednego lub kilku państw członkowskich**, **zapewnianie wsparcia** w zakresie *ex post* zapytań technicznych dotyczących znaczących incydentów w rozumieniu dyrektywy (UE) 2022/2555;	ENISA Państwa członkowskie	Analiza i wsparcie w odpowiedzi na zapytania techniczne dotyczące incydentów	Przetwarzanie danych Przepływ danych
Artykuł 10 ust. 4 lit. e) Współpraca operacyjna	e) wspieranie skoordynowanego zarządzania incydentami i kryzysami związanymi z cyberbezpieczeństwem na dużą skalę na poziomie operacyjnym, w szczególności poprzez **pomoc EU-CyCLONe w przygotowywaniu sprawozdań dla szczebla politycznego poprzez ułatwianie i usprawnianie terminowej wymiany informacji między siecią CSIRT a EU-CyCLONe;**	ENISA EU-CyCLONe Sieć CSIRT	Analizowanie danych w celu wsparcia przygotowywania sprawozdań; ułatwianie terminowej wymiany informacji między sieciami	Przetwarzanie danych Przepływ danych Cyfrowa usługa publiczna
Artykuł 10 ust. 5 Współpraca operacyjna	Na **wniosek państwa członkowskiego** lub podmiotu unijnego we współpracy z CERT-EU ENISA wspiera spójną komunikację publiczną dotyczącą incydentu lub zagrożenia cybernetycznego.	ENISA Państwa członkowskie	Przyjmowanie wniosków i przekazywanie informacji w razie potrzeby	Przepływ danych

Artykuł 10 ust. 6 Współpraca operacyjna	ENISA **wspiera** współpracę między państwami członkowskimi oraz, za pośrednictwem CERT-EU, między podmiotami unijnymi w zakresie **wdrażania bezpiecznych narzędzi komunikacyjnych.** ENISA korzysta w ramach sieci CSIRT i EU-CyCLONe z bezpiecznych narzędzi komunikacyjnych dostarczanych przez podmioty prawne, które nie mają siedziby w państwach trzecich ani nie są kontrolowane przez państwa trzecie lub obywateli państw trzecich.	ENISA Komisja Europejska Państwa członkowskie Podmioty UE Sieć CSIRT EU-CyCLONe	Wspieranie wdrażania bezpiecznych narzędzi komunikacyjnych i korzystanie z takich narzędzi w ramach sieci CSIRT i EU-CyCLONe.	Rozwiązanie cyfrowe Cyfrowa usługa publiczna
Artykuł 11 ust. 1 lit. a) Wspólna świadomość sytuacji w zakresie cyberbezpieczeństwa	a) **opracowanie** we współpracy z EU-CyCLONe, siecią CSIRT, Komisją, CERT-EU, Europolem i innymi odpowiednimi podmiotami unijnymi **repozytoriów** zweryfikowanych, wiarygodnych informacji wywiadowczych dotyczących cyberzagrożeń, w tym trendów w zakresie incydentów, taktyk, technik i procedur;	Komisja Europejska ENISA EU-CyCLONe sieć CSIRT Europol Podmioty UE CERT-EU	Opracowanie repozytoriów	Przepływ cyfrowy Rozwiązanie cyfrowe Cyfrowa usługa publiczna
Artykuł 11 ust. 1 lit. c) do g) Wspólna świadomość sytuacji w zakresie cyberbezpieczeństwa	Dostarczanie aktualnych analiz *ad hoc* (niektóre na żądanie); dostarczanie analiz i porad technicznych; przygotowywanie raportów dotyczących sytuacji technicznej we współpracy z innymi podmiotami; monitorowanie trendów i dzielenie się nimi	ENISA Państwa członkowskie Komisja Europejska Podmioty UE EU-CyCLONe Sieć CSIRT	Analiza danych, wymiana informacji i sporządzanie raportów (niektóre na żądanie)	Przetwarzanie danych Przepływ danych

Artykuł 11 ust. 2 lit. a) Wspólna ocena sytuacji w zakresie cyberbezpieczeństwa	ENISA **przeprowadza analizy** zagrożeń cybernetycznych, incydentów, trendów, nowych technologii i ich skutków, w tym regularną **analizę** dotyczącą sektorów wymienionych w załącznikach I i II do dyrektywy (UE) 2022/2555 oraz odpowiednich kategorii produktów objętych rozporządzeniem (UE) 2024/2847;	ENISA Ogół społeczeństwa	Analiza danych w celu dostarczenia informacji mających znaczenie dla cyberbezpieczeństwa; regularne sprawozdania	Przetwarzanie danych Przepływ danych
Artykuł 11 ust. 2 lit. b) Wspólna ocena sytuacji w zakresie cyberbezpieczeństwa	ENISA**, we współpracy z Komisją oraz, w stosownych przypadkach, z siecią CSIRT, wydaje porady, wytyczne i najlepsze praktyki** dotyczące bezpieczeństwa sieci i systemów informatycznych, w szczególności bezpieczeństwa infrastruktur wspierających sektory wymienione w załącznikach I i II do dyrektywy (UE) 2022/2555;	Komisja Europejska CERT-EU Sieć CSIRT Ogół społeczeństwa	Wydawanie porad, wytycznych i najlepszych praktyk	Przetwarzanie danych Przepływ danych
Artykuł 11 ust. 2 lit. c) Wspólna ocena sytuacji w zakresie cyberbezpieczeństwa	ENISA przeprowadza **długoterminowe analizy strategiczne zagrożeń** i incydentów **cybernetycznych** w celu **identyfikacji** pojawiających się trendów i zapobiegania incydentom.	ENISA Ogół społeczeństwa	Analiza danych i identyfikacja pojawiających się zagrożeń	Przetwarzanie danych
Artykuł 11 ust. 3 Wspólna ocena sytuacji w zakresie cyberbezpieczeństwa	ENISA może **podawać do wiadomości publicznej analizy**, porady, wytyczne, najlepsze praktyki i sprawozdania, o których mowa w ust. 2, w porozumieniu z podmiotami, o których mowa w ust. 2.	ENISA Ogół społeczeństwa	Podawanie informacji do wiadomości publicznej	Przepływ danych Cyfrowa usługa publiczna

Artykuł 13 ust. 2 Wsparcie w reagowaniu na incydenty	2. Na wniosek Komisji lub EU-CyCLONe ENISA, przy wsparciu sieci CSIRT i za zgodą zainteresowanego państwa członkowskiego, dokonuje **przeglądu i oceny znaczących incydentów związanych z cyberbezpieczeństwem** lub incydentów związanych z cyberbezpieczeństwem na dużą skalę zgodnie z art. 21 rozporządzenia (UE) 2025/38.	Komisja Europejska ENISA EU-CyCLONe Sieć CSIRT Państwa członkowskie	Przegląd i ocena istotnych incydentów związanych z cyberbezpieczeństwem	Przetwarzanie danych
Artykuł 14 ust. 2 Ćwiczenia w zakresie cyberbezpieczeństwa na szczeblu Unii	2. ENISA **prowadzi rejestr** wniosków wyciągniętych z ćwiczeń, o których mowa w ust. 1, i zaleca państwom członkowskim oraz, w stosownych przypadkach, podmiotom unijnym, jak skutecznie i efektywnie wdrożyć wyciągnięte wnioski.	ENISA Państwa członkowskie Podmioty UE	Prowadzenie repozytorium	Przetwarzanie danych Rozwiązanie cyfrowe Cyfrowa usługa publiczna
Artykuł 14 Ćwiczenia w zakresie cyberbezpieczeństwa na poziomie Unii	Na wniosek EU-CyCLONe, Komisji, państw członkowskich lub CERT-EU ENISA organizuje ćwiczenia w zakresie cyberbezpieczeństwa lub uczestniczy w ich organizacji. ENISA wspiera Komisję w opracowywaniu rocznego programu ćwiczeń w zakresie cyberbezpieczeństwa na poziomie Unii.	ENISA Komisja Państwa członkowskie Podmioty UE CERT-EU	Przyjmowanie wniosków o zorganizowanie lub wsparcie organizacji ćwiczeń	Przepływ danych Przetwarzanie danych

Artykuł 15 Przepisy dotyczące narzędzi i platform	1. **ENISA ustanawia, udostępnia, obsługuje, utrzymuje i w razie potrzeby aktualizuje operacyjne narzędzia techniczne, w tym platformy** związane z cyberbezpieczeństwem na poziomie Unii, w szczególności jednolitą platformę zgłaszania incydentów ustanowioną zgodnie z art. 16 ust. 1 rozporządzenia (UE) 2024/2847 [oraz pojedynczy punkt kontaktowy ustanowiony zgodnie z art. 23a dyrektywy (UE) 2022/2555], oraz narzędzia testowe wspierające wdrażanie procedur oceny zgodności zgodnie z odpowiednim prawodawstwem Unii. 2. W stosownych przypadkach do celów ust. 1 **ENISA współpracuje i wymienia informacje** z siecią CSIRT oraz, w stosownych przypadkach, z organami nadzoru rynku.	ENISA Sieć CSIRT Ogół społeczeństwa Organy nadzoru rynku	ENISA ustanawia, zapewnia, obsługuje, utrzymuje i aktualizuje w razie potrzeby operacyjne narzędzia techniczne, takie jak platformy	Rozwiązanie cyfrowe Cyfrowa usługa publiczna Przepływ danych
Artykuł 16 ust. 2 Usługi zarządzania podatnością na zagrożenia	a) prowadzenie europejskiej bazy danych o podatnościach ustanowionej zgodnie z art. 12 ust. 2 dyrektywy (UE) 2022/2555; b) świadczenie usług zarządzania podatnością na zagrożenia na rzecz **zainteresowanych stron** w oparciu o europejską bazę danych podatności na zagrożenia i z wykorzystaniem odpowiednich informacji dostępnych dla ENISA; (c) w stosownych przypadkach nawiązanie zorganizowanej współpracy z **organizacjami** zapewniającymi programy, rejestry lub bazy danych podobne do europejskiej bazy danych dotyczących podatności na zagrożenia; d) aktywne wspieranie zespołów **CSIRT** wyznaczonych jako koordynatorzy zgodnie z art. 12 ust. 1 dyrektywy (UE) 2022/2555 w	ENISA Krajowe zespoły CSIRT Sieć CSIRT Krajowe właściwe organy Przemysł Środowisko naukowe Ogół społeczeństwa Międzynarodowe podmioty zapewniające programy, rejestry lub bazy danych	Świadczenie usług w zakresie zarządzania podatnością na zagrożenia; nawiązywanie współpracy strukturalnej w stosownych przypadkach; współpraca z zainteresowanymi stronami	Rozwiązanie cyfrowe Cyfrowa usługa publiczna Przepływ danych

	zakresie zarządzania skoordynowanym ujawnianiem podatności, które mogą mieć znaczący wpływ na podmioty w więcej niż jednym państwie członkowskim ( ); e) opracowywanie i utrzymywanie metodologii i mechanizmów zarządzania służących identyfikacji luk w zabezpieczeniach i skoordynowanemu ujawnianiu informacji, **we współpracy z właściwymi organami krajowymi, zespołami CSIRT, przemysłem i środowiskiem badawczym**			
Artykuł 17 Certyfikacja cyberbezpieczeństwa Artykuł 18 Normalizacja, specyfikacje techniczne i wytyczne	Artykuł 17 ust. 1 a) **przygotowywanie kandydackich europejskich systemów certyfikacji cyberbezpieczeństwa („systemy kandydackie”)** dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberpostury podmiotów oraz związanych z nimi specyfikacji technicznych zgodnie z art. 74; b) **utrzymywanie przyjętych europejskich systemów certyfikacji cyberbezpieczeństwa** zgodnie z art. 75, w tym z myślą o ewentualnym przeglądzie przyjętych europejskich systemów certyfikacji cyberbezpieczeństwa zgodnie z art. 76; c) promowanie stosowania przyjętych systemów oraz prowadzenie specjalnej strony internetowej zawierającej informacje na temat europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, europejskich certyfikatów cyberbezpieczeństwa i unijnych oświadczeń	ENISA Ogół społeczeństwa	Analiza danych i wymiana przepływów danych z Komisją i innymi zainteresowanymi stronami; przygotowanie kandydackiego systemu certyfikacji; utrzymanie strony internetowej ENISA	Przetwarzanie danych Przepływy danych Cyfrowe usługi publiczne

	o zgodności oraz ich upowszechnianie zgodnie z art. 79; Artykuł 17 ust. 2 e) **przygotowywanie** wzorcowych przepisów, do których należy odwoływać się w europejskich systemach certyfikacji cyberbezpieczeństwa („systemy kandydujące”) w odniesieniu do produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberpostury podmiotów zgodnie z art. 81 ust. 5. Artykuł 18 1. ENISA opracowuje specyfikacje techniczne i wytyczne w celu wsparcia wdrażania prawodawstwa Unii w dziedzinie cyberbezpieczeństwa. 2. ENISA **monitoruje** działania **w zakresie normalizacji** na poziomie Unii oraz, zgodnie z art. 9, na poziomie międzynarodowym**, uczestniczy w nich i kieruje nimi**. 3. ENISA wspiera opracowywanie i ocenę algorytmów kryptograficznych. W przypadku pozytywnej oceny algorytmu kryptograficznego ENISA współpracuje, zgodnie z rozporządzeniem (UE) nr 1025/2012, z europejskimi organami normalizacyjnymi w celu wsparcia jego normalizacji. 4. ENISA **zapewnia** Komisji i ECCG **wiedzę techniczną** na temat odpowiednich norm lub specyfikacji technicznych wspierających politykę Unii w zakresie cyberbezpieczeństwa, w szczególności rozporządzenie (UE) 2024/2847, w tym w odniesieniu do unijnych			

	przepisów harmonizacyjnych w dziedzinie cyberbezpieczeństwa i europejskich systemów certyfikacji cyberbezpieczeństwa zgodnie z art. 81 ust. 1 lit. d). 5. ENISA wspiera Komisję w ocenie projektów zharmonizowanych norm w celu wsparcia wdrażania unijnych przepisów harmonizacyjnych w dziedzinie cyberbezpieczeństwa.			
Artykuł 19 – Europejskie ramy kwalifikacji w zakresie cyberbezpieczeństwa	ENISA **opracowuje i podaje do wiadomości publicznej europejskie ramy umiejętności w zakresie cyberbezpieczeństwa („ECSF”).** Przed podaniem ECSF do wiadomości publicznej lub aktualizacją zgodnie z ust. 4 ENISA **konsultuje się z Komisją.** Korzystanie z ECSF jest **dobrowolne dla podmiotów publicznych i prywatnych**. ENISA może **konsultować się z zainteresowanymi stronami** w sprawie opracowania i wdrożenia ECSF.	ENISA Komisja Ogół społeczeństwa Państwa członkowskie Podmioty UE Podmioty publiczne i prywatne	Utrzymanie ECSF; konsultacje z zainteresowanymi stronami; wdrożenie ECSF	Przetwarzanie danych Przepływ danych Rozwiązanie cyfrowe
Artykuły 20–23 – Europejskie systemy certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa	ENISA **opracowuje, przyjmuje i utrzymuje europejskie systemy poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa**. Korzystanie z europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa jest **dobrowolne dla krajowych organów publicznych i podmiotów prywatnych**, chyba że prawo krajowe stanowi inaczej. Przed uruchomieniem nowego europejskiego systemu poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa ENISA **konsultuje się z Komisją**. ENISA	ENISA Komisja Ogół społeczeństwa Państwa członkowskie Podmioty UE Podmioty publiczne i prywatne (przyczyniające się do opracowania systemu certyfikacji; wnioskodawcy i europejscy dostawcy indywidualnych certyfikatów umiejętności w zakresie cyberbezpieczeństwa, w tym oceniający)	Opracowywanie i utrzymywanie systemów; konsultacje z zainteresowanymi stronami; rozpatrywanie wniosków; wydawanie decyzji; utrzymywanie strony internetowej	Przetwarzanie danych Przepływ danych Rozwiązanie cyfrowe Cyfrowa usługa publiczna

	przyjmuje taki system wyłącznie po **uzyskaniu** pozytywnej **opinii Komisji**. Przygotowując europejski system poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, ENISA może **konsultować się z odpowiednimi zainteresowanymi stronami.** ENISA zapewnia **ścisłą współpracę z państwami członkowskimi** podczas przygotowywania europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa. Upoważnieni dostawcy certyfikatów **oceniają, czy osoby fizyczne spełniają wymogi** europejskiego systemu certyfikacji umiejętności w zakresie cyberbezpieczeństwa, a w przypadku spełnienia tych wymogów wydają europejskie certyfikaty umiejętności w zakresie cyberbezpieczeństwa. ENISA **zapewnia wytyczne dla oceniających i przeprowadza obowiązkowe szkolenia dla nich** w zakresie wymogów i metod oceny zawartych w europejskim systemie poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, o którym mowa w art. 20 ust. 3 lit. b). Podmioty, które chcą uzyskać upoważnienie na świadczenie usług certyfikacji lub odnowić swoje upoważnienie **(„wnioskodawcy"), składają wniosek** do ENISA. Upoważnieni dostawcy certyfikatów zapewniają, aby **na wniosek osoby fizycznej** europejskie certyfikaty indywidualnych umiejętności w			

	zakresie cyberbezpieczeństwa były wydawane jako certyfikaty elektroniczne atrybutów w formacie**,** który można przechowywać w europejskich portfelach tożsamości cyfrowej określonych w rozporządzeniu (UE) nr 910/2014. Wnioskodawcy i uprawnieni dostawcy poświadczeń umożliwiają **ENISA przeprowadzenie ocen** w ramach wstępnego procesu składania wniosków, utrzymania upoważnienia lub jego odnowienia oraz udostępniają wszystkie istotne informacje w celu zapewnienia, że wymogi określone w ust. 3 i 4 oraz obowiązki określone w ust. 5 są spełnione lub nadal są spełniane zgodnie z art. 22 ust. 2. Upoważnieni dostawcy poświadczeń niezwłocznie **informują ENISA**, jeżeli którekolwiek z wymogów wymienionych w ust. 3 nie jest już spełniane lub jeżeli pojawiają się jakiekolwiek wątpliwości co do spełnienia tych wymogów, w tym dotyczące niezależności oceniających. Wnioskodawcy **uiszczają opłatę na rzecz ENISA** za ocenę ich wniosku. Upoważnieni dostawcy poświadczeń **uiszczają opłatę na rzecz ENISA** za utrzymanie ich upoważnienia. **ENISA ocenia,** czy wnioskodawcy i uprawnieni dostawcy poświadczeń spełniają lub nadal spełniają wymogi określone w art. 21 ust. 3 i 4 oraz obowiązki określone w art. 21 ust. 5. Po zbadaniu wniosku pod kątem wymogów określonych w art.			

	21 ust. 3 i 4 **ENISA może wydać decyzję**. **ENISA może zmienić, zawiesić lub uchylić takie decyzje**. **ENISA prowadzi i regularnie aktualizuje specjalną stronę internetową** zawierającą informacje publiczne na temat: (a) ECSF, w tym ramy i harmonogram aktualizacji; b) europejskie systemy certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa, postępy w ich opracowywaniu oraz harmonogramy ich rozwoju; c) opłaty związane z każdym europejskim systemem poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa przyjętym zgodnie z art. 47 niniejszego rozporządzenia; d) orientacyjny koszt europejskiego certyfikatu indywidualnych umiejętności w zakresie cyberbezpieczeństwa zgodnie z art. 20 ust. 4;			

	e) wykaz uprawnionych podmiotów wydających certyfikaty.			
Artykuł 25 Skład zarządu	**Mianowanie członków** zarządu ENISA.	ENISA Komisja Europejska Państwa członkowskie	Mianowanie członków	Przepływ danych Przetwarzanie danych
Artykuł 28 ust. 1 Funkcje zarządu Artykuł 30 Zarząd	b. przyjmuje projekt jednolitego dokumentu programowego ENISA, o którym mowa w art. 44, przed **przedłożeniem** go **Komisji do zaopiniowania**; f) **ocenia** i przyjmuje skonsolidowane sprawozdanie roczne z działalności ENISA, w tym sprawozdanie finansowe i opis sposobu, w jaki ENISA osiągnęła swoje wskaźniki wykonania, **przedkłada zarówno sprawozdanie roczne, jak i** jego **ocenę** do dnia 1 lipca następnego roku Parlamentowi Europejskiemu, Radzie, Komisji i Europejskiemu Trybunałowi Obrachunkowemu; podaje sprawozdanie roczne do wiadomości publicznej; (i) zapewnia odpowiednie **działania następcze w związku z ustaleniami** i zaleceniami wynikającymi z wewnętrznych lub zewnętrznych sprawozdań z audytu i ocen oraz z dochodzeń Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych (OLAF) i Prokuratury Europejskiej (EPPO);	ENISA Komisja Europejska Parlament Europejski Rada UE Trybunał Obrachunkowy Państwa członkowskie Ogół społeczeństwa	Przedłożenie SPD Komisji w celu uzyskania opinii; Ocena i przyjęcie skonsolidowanego sprawozdania rocznego z działalności ENISA, w tym sprawozdania finansowego i opisu sposobu realizacji przez ENISA wskaźników efektywności, przedłożenie zarówno sprawozdania rocznego, jak i oceny; Dalsze działania w związku z ustaleniami	Przepływ danych Przetwarzanie danych

Artykuł 31 ust. 8 Mianowanie, odwołanie i przedłużenie kadencji	**Zarząd informuje Parlament Europejski** o zamiarze przedłużenia kadencji dyrektora wykonawczego zgodnie z ust. 6. W ciągu trzech miesięcy przed takim przedłużeniem dyrektor wykonawczy, na zaproszenie, składa oświadczenie przed właściwą komisją Parlamentu Europejskiego i odpowiada na pytania posłów.	ENISA Zarząd ENISA Parlament	Zarząd informuje Parlament Europejski	Przepływ danych
Artykuł 32 ust. 3 Zadania i obowiązki dyrektora wykonawczego Artykuł 32 ust. 5	3. **Dyrektor wykonawczy składa Parlamentowi Europejskiemu sprawozdanie** z wykonywania swoich zadań, gdy zostanie o to poproszony. Rada może poprosić dyrektora wykonawczego o złożenie sprawozdania z wykonywania swoich zadań. Przygotowywanie projektów planów budżetowych, strategii i dokumentów strategicznych.	Dyrektor wykonawczy ENISA Parlament Europejski	Sprawozdania z wyników	Przepływ danych Przetwarzanie danych
Artykuł 35 ust. 5 i 6 Grupa doradcza ENISA	5. Grupa doradcza ENISA **doradza ENISA** w zakresie wykonywania zadań ENISA, z wyjątkiem stosowania przepisów tytułów III, IV i V niniejszego rozporządzenia. W szczególności doradza dyrektorowi wykonawczemu w sprawie sporządzenia wniosku dotyczącego rocznego programu prac ENISA oraz zapewnienia komunikacji z odpowiednimi zainteresowanymi stronami w kwestiach związanych z rocznym programem prac. 6. Grupa doradcza ENISA regularnie **informuje zarząd** o swoich działaniach.	ENISA Członkowie grupy doradczej ENISA Zarząd ENISA Dyrektor wykonawczy ENISA	Doradztwo i informowanie o swoich działaniach	Przetwarzanie danych Przepływ danych

Artykuł 36–43 Komisja odwoławcza	ENISA **powołuje komisję odwoławczą** na mocy decyzji zarządu. Komisja odwoławcza składa się z przewodniczącego i trzech innych członków. Każdy członek komisji odwoławczej ma zastępcę. Zastępca reprezentuje członka w przypadku jego nieobecności. Zarząd **mianuje przewodniczącego, pozostałych członków i ich zastępców** z **listy wykwalifikowanych kandydatów sporządzonej przez Komisję**. Lista wykwalifikowanych kandydatów jest ważna przez cztery lata. Zarząd może przedłużyć ważność tej listy na kolejne czteroletnie okresy na wniosek Komisji. Jeżeli Komisja Odwoławcza uzna, że wymaga tego charakter odwołania, może zwrócić się do **zarządu o powołanie dwóch dodatkowych członków i ich zastępców** z listy, o której mowa w ust. 3. Komisja odwoławcza przyjmuje i **podaje do wiadomości publicznej swój regulamin wewnętrzny.** Jeżeli z jednego z powodów wymienionych w ust. 1 lub z jakiegokolwiek innego powodu członek komisji odwoławczej uzna, że nie powinien brać udziału w postępowaniu odwoławczym, **informuje o tym komisję odwoławczą**. Komisja Odwoławcza podejmuje **decyzję w sprawie działań, które należy podjąć** w przypadkach wymienionych w ust. 2 i 3, bez udziału danego członka. W celu podjęcia tej decyzji danego członka zastępuje w Komisji	Zarząd ENISA Zarząd ENISA Komisja Komisja Wnioskodawcy (podmioty prawne, które chcą uzyskać status uprawnionego dostawcy poświadczeń, utrzymać lub odnowić swoje uprawnienia)	Wydawanie decyzji na podstawie odwołań Rozpatrywanie odwołań Przygotowywanie i publikowanie regulaminów postępowania Przepływ informacji	Przetwarzanie danych Przepływ danych Cyfrowa usługa publiczna

	Odwoławczej jego zastępca. Odwołanie wniesione zgodnie z ust. 1 podlega kontroli międzyinstancyjnej zgodnie z art. 41, zanim zostanie przekazane Komisji Odwoławczej do rozpatrzenia. Wnioskodawcy w rozumieniu art. 21 ust. 3 mogą **odwołać się od: decyzji ENISA** skierowanej do nich zgodnie z art. 22 ust. 3, zaniechania działania przez ENISA w odniesieniu do wniosku złożonego przez nich do ENISA w terminie określonym w art. 22 ust. 4. W przypadku, o którym mowa w ust. 1 lit. a), odwołanie wraz z uzasadnieniem **składa się na piśmie** zgodnie z regulaminem wewnętrznym, o którym mowa w art. 36 ust. 5, w terminie dwóch miesięcy od powiadomienia zainteresowanego wnioskodawcy o decyzji lub, w przypadku braku takiego powiadomienia, od dnia, w którym wnioskodawca dowiedział się o decyzji. W przypadku, o którym mowa w ust. 1 lit. b), odwołanie **składa** się **do ENISA na piśmie** zgodnie z regulaminem wewnętrznym, o którym mowa w art. 36 ust. 5, w terminie dwóch miesięcy od dnia upływu terminu określonego w art. 22 ust. 4. Jeżeli ENISA uzna odwołanie za dopuszczalne i uzasadnione, **koryguje decyzję lub zaniechanie działania,** o których mowa w art. 40 ust. 1. Jeżeli ENISA nie zmieni decyzji w terminie jednego miesiąca od otrzymania odwołania, niezwłocznie **podejmuje decyzję o zawieszeniu stosowania swojej decyzji i przekazuje odwołanie do komisji odwoławczej**.			

	Komisja odwoławcza podejmuje decyzję w sprawie uwzględnienia lub odrzucenia odwołania w terminie trzech miesięcy od jego wniesienia. Rozpatrując odwołanie, komisja odwoławcza działa w terminach określonych w jej regulaminie wewnętrznym. W razie potrzeby **wzywa strony postępowania odwoławczego do przedstawienia w określonym terminie uwag dotyczących jej zawiadomień lub komunikatów innych stron postępowania odwoławczego**. Strony postępowania odwoławczego mają prawo do składania **ustnych oświadczeń.** Jeżeli Komisja Odwoławcza uzna, że podstawy odwołania są uzasadnione, **przekazuje sprawę do ENISA.** ENISA **podejmuje ostateczną decyzję** zgodnie z ustaleniami Komisji Odwoławczej i **przedstawia uzasadnienie tej decyzji**. ENISA **informuje** o tym **strony** postępowania odwoławczego. Skargi o stwierdzenie nieważności decyzji ENISA podjętych na podstawie art. 22 ust. 3 lub o zaniechanie działania w przewidzianym terminie na podstawie art. 22 ust. 4 mogą **być wnoszone do Trybunału Sprawiedliwości Unii Europejskiej** po wyczerpaniu wewnętrznej procedury odwoławczej ENISA określonej w art. 39–42 lub w przypadku zaniechania działania w przewidzianym terminie na podstawie art. 41(2). ENISA **podejmuje wszelkie niezbędne środki w** celu wykonania wyroku Trybunału Sprawiedliwości Unii Europejskiej			

Artykuł 44 Jednolity dokument programowy	2. Każdego roku dyrektor wykonawczy sporządza projekt jednolitego dokumentu programowego, o którym mowa w ust. 1, wraz z odpowiednim planem zasobów finansowych i ludzkich zgodnie z art. 32 rozporządzenia delegowanego Komisji (UE) 2019/715 i z uwzględnieniem wytycznych określonych przez Komisję. 3. Do dnia 30 listopada każdego roku zarząd przyjmuje jednolity dokument programowy, o którym mowa w ust. 1, uwzględniając opinię Komisji, o której mowa w art. 32 ust. 7 rozporządzenia delegowanego (UE) 2019/715. Jeżeli zarząd postanowi nie uwzględnić niektórych elementów opinii Komisji, przedstawia szczegółowe uzasadnienie tej decyzji. Zarząd przekazuje jednolity dokument programowy Parlamentowi Europejskiemu, Radzie i Komisji do dnia 31 stycznia następnego roku, a także wszelkie późniejsze aktualizacje tego dokumentu.	Dyrektor wykonawczy ENISA Zarząd ENISA Komisja Europejska Parlament Europejski Rada	Opracowywanie, przyjmowanie i przekazywanie co roku jednego dokumentu programowego	Przepływ danych
Artykuł 45 Ustanowienie budżetu ENISA	4 **Komisja przesyła projekt preliminarza do władzy budżetowej** wraz z projektem budżetu ogólnego Unii. Projekt preliminarza udostępnia się również ENISA.	ENISA Komisja	Wymiana informacji	Przepływ danych

Artykuł 47 Opłaty	W odniesieniu do działań w ramach europejskich systemów indywidualnych certyfikatów określonych w art. 22 ust. 1, od wnioskodawców w rozumieniu art. 21 ust. 3 lub od uprawnionych podmiotów certyfikujących **pobiera się następujące opłaty** w celu pokrycia pełnych kosztów działań wykonywanych przez ENISA: a. wydawanie zezwoleń po zbadaniu wymogów określonych w art. 21 ust. 3 i 4, w tym przeprowadzanie ocen; b. coroczne utrzymywanie zezwolenia; c. odnawianie zezwoleń dla podmiotów wydających europejskie indywidualne certyfikaty umiejętności w zakresie cyberbezpieczeństwa, w tym przeprowadzanie ocen. W odniesieniu do certyfikacji **od organów oceny zgodności pobiera się następujące opłaty** za utrzymanie europejskich systemów certyfikacji w dziedzinie cyberbezpieczeństwa, w ramach których wydawane są europejskie certyfikaty w dziedzinie cyberbezpieczeństwa, w szczególności: opłata roczna za udział w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa; opłata za wydawanie europejskich certyfikatów w zakresie cyberbezpieczeństwa w ramach europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa. Opłaty, o których mowa w lit. b), są pobierane, gdy jednostka oceniająca zgodność przedkłada europejskie certyfikaty w zakresie	Komisja ENISA Podmioty wydające zaświadczenia Jednostki oceniające zgodność	Przetwarzanie informacji; uiszczanie opłat; sprawozdawczość dotycząca opłat	Przetwarzanie danych Przepływ danych

	cyberbezpieczeństwa do ENISA w celu opublikowania ich na stronie internetowej zgodnie z art. 79. **Komisja przyjmuje akty wykonawcze** ustanawiające szczegółowe zasady dotyczące opłat pobieranych przez ENISA. ENISA dołącza **sprawozdanie dotyczące pobranych opłat i ich wpływu na** budżet **Agencji** w ramach procedury przedstawiania sprawozdań finansowych.			
Artykuł 48 Artykuł 49 Skutki dla budżetu	Artykuł 48 3. Każdego roku dyrektor wykonawczy **przesyła władzy budżetowej wszystkie informacje** istotne dla wyników procedur oceny. Artykuł 49 1. Księgowy ENISA **przesyła tymczasowe sprawozdanie finansowe za dany rok budżetowy** (rok N) księgowemu Komisji i Trybunałowi Obrachunkowemu do dnia 1 marca następnego roku budżetowego (rok N + 1). 2. Księgowy ENISA **przekazuje** również księgowemu **Komisji wymagane informacje księgowe do celów konsolidacji**, w sposób i formacie wymaganym przez tego ostatniego, do dnia 1 marca roku N + 1. 3. **ENISA przesyła sprawozdanie z zarządzania budżetem i finansami za rok N do Parlamentu Europejskiego, Rady, Komisji** i Trybunału Obrachunkowego do dnia 31 marca roku N + 1. 4. **Po otrzymaniu uwag Trybunału Obrachunkowego dotyczących tymczasowego sprawozdania finansowego ENISA za rok N**	ENISA Zarząd ENISA Komisja Europejska Rada Parlament	Przetwarzanie i udostępnianie informacji dotyczących budżetu ENISA.	Przetwarzanie danych Przepływ danych

	księgowy agencji sporządza ostateczne sprawozdanie finansowe ENISA. 5. **Zarząd wydaje opinię** na temat ostatecznego sprawozdania finansowego ENISA za rok N. **Księgowy agencji sporządza ostateczne sprawozdanie finansowe ENISA na własną odpowiedzialność. Dyrektor wykonawczy przedkłada je zarządowi do zaopiniowania.**			
Artykuł 52 Oświadczenie o braku konfliktu interesów	Strony **składają oświadczenie o zobowiązaniach oraz oświadczenie wskazujące** na **brak lub** obecność jakichkolwiek bezpośrednich lub pośrednich interesów, które mogłyby zostać uznane za szkodliwe dla ich niezależności.	Kierownictwo ENISA (dyrektor wykonawczy, zastępca dyrektora wykonawczego); zarząd, Oddelegowani eksperci krajowi	Przetwarzanie i udostępnianie danych dotyczących deklaracji interesów	Przetwarzanie danych Przepływ danych
Artykuł 58 Oficerowie łącznikowi	1. **Każde państwo członkowskie wyznacza co najmniej dwóch oficerów łącznikowych** [z krajowego organu ds. cyberbezpieczeństwa] jako oddelegowanych ekspertów krajowych do ENISA, którzy będą pracować w siedzibie lub lokalnym biurze agencji, zgodnie z art. 59 ust. 2. Komisja może również wyznaczyć oficera łącznikowego. 2. Oficerowie łącznikowi wyznaczeni przez swoje państwa członkowskie są uprawnieni do **żądania i otrzymywania wszystkich istotnych**	ENISA Państwa członkowskie	Wyznaczanie oficerów łącznikowych i wymiana informacji	Przetwarzanie danych Przepływ danych

	informacji od swoich państw członkowskich, zgodnie z niniejszym rozporządzeniem, przy pełnym poszanowaniu prawa krajowego lub praktyki swoich państw członkowskich, w szczególności w odniesieniu do ochrony danych i zasad dotyczących poufności.			
Artykuł 67 Postępowanie z informacjami niejawnymi	Po **konsultacji z Komisją** ENISA przyjmuje zasady bezpieczeństwa stosujące zasady bezpieczeństwa zawarte w zasadach bezpieczeństwa Komisji dotyczących ochrony informacji niejawnych o charakterze wrażliwym i informacji niejawnych UE, określonych w decyzjach (UE, Euratom) 2015/443 i 2015/444. Zasady bezpieczeństwa ENISA zawierają **przepisy dotyczące wymiany, przetwarzania i przechowywania takich informacji.**	ENISA Zarząd Komisja	Postępowanie z informacjami niejawnymi	Przetwarzanie danych Przepływ danych
Artykuł 68, 69, 70 Współpraca z podmiotami unijnymi i organami krajowymi Współpraca z zainteresowanymi stronami Współpraca z państwami trzecimi	ENISA współpracuje i wymienia informacje w sprawach związanych z cyberbezpieczeństwem z odpowiednimi podmiotami unijnymi, organami nadzoru rynku i organami nadzorczymi, odpowiednimi zainteresowanymi stronami, właściwymi organami z państw trzecich lub organizacjami międzynarodowymi.	ENISA Europol ECCC Europejska Rada Ochrony Danych Ogół społeczeństwa Rada	Wymiana informacji	Przepływ danych

Artykuł 72 dotyczący informacji publicznej i konsultacji w sprawie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa	2. Komisja prowadzi i regularnie aktualizuje specjalną stronę internetową zawierającą informacje na temat następujących aspektów: a) europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa, o których opracowanie zwrócono się; b) strategiczne priorytety w zakresie harmonizacji produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub wymogów bezpieczeństwa określonych w przepisach unijnych, w tym potencjalne obszary, w których można by wnioskować o ustanowienie europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa. 3. Komisja podaje do wiadomości publicznej na stronie internetowej, o której mowa w ust. 2 niniejszego artykułu, informacje dotyczące jej wniosku skierowanego do ENISA o przygotowanie systemu kandydującego, o którym mowa w art. 73, oraz swojej decyzji o przyjęciu, odrzuceniu lub wycofaniu systemu kandydującego przekazanego przez ENISA zgodnie z art. 74 ust. 7.	Komisja Europejska Ogół społeczeństwa ENISA	Utrzymywanie strony internetowej zawierającej informacje Zobowiązuje to Komisję do udostępniania informacji na publicznie dostępnej stronie internetowej oraz do prowadzenia bieżących działań związanych z zarządzaniem danymi.	Cyfrowe usługi publiczne Rozwiązanie cyfrowe
Artykuł 72 dotyczący informacji publicznej i konsultacji w sprawie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa	Podczas przygotowywania systemu kandydującego przez ENISA zgodnie z art. 74 **Parlament Europejski i Rada mogą zwrócić się do Komisji**, pełniącej funkcję przewodniczącego ECCG, oraz do ENISA o przedstawienie odpowiednich informacji na temat projektu systemu kandydującego. **Na wniosek Parlamentu Europejskiego lub Rady ENISA, w porozumieniu z Komisją** i bez	ENISA Rada UE Parlament Europejski	Wnioskowanie o informacje i przesyłanie informacji na temat projektu systemu kandydującego przygotowanego przez ENISA	Przepływ danych

	uszczerbku dla art. 54, może **udostępnić Parlamentowi Europejskiemu i Radzie odpowiednie części projektu systemu kandydującego** w sposób odpowiedni do wymaganego poziomu poufności oraz, w stosownych przypadkach, w sposób ograniczony. **Parlament Europejski i Rada mogą zaprosić Komisję i ENISA do omówienia** kwestii dotyczących wdrażania europejskich systemów certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów.			
Artykuł 73 Wniosek o europejski system certyfikacji cyberbezpieczeństwa Artykuł 74 Przygotowanie i przyjęcie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa **(objęte art. 17)**	**Artykuł 73** **1. Komisja może zwrócić się do ENISA o przygotowanie projektu europejskiego systemu certyfikacji cyberbezpieczeństwa** dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów. W należycie uzasadnionych przypadkach ECCG może zaproponować Komisji złożenie wniosku, o którym mowa w ust. 1. 4. Przygotowując wniosek, o którym mowa w ust. 1, **Komisja** należycie konsultuje się z ENISA i ECCG, a także uwzględnia opinie wszystkich **zainteresowanych stron** i innych podmiotów unijnych, w tym, w stosownych przypadkach, tych, które są istotne w świetle przepisów unijnych, w których europejski system certyfikacji w zakresie cyberbezpieczeństwa zapewnia domniemanie zgodności.	Komisja Europejska ENISA ECCG Zainteresowane strony będące ekspertami	Przygotowanie wniosku i systemu certyfikacji oraz związane z tym konsultacje z zainteresowanymi stronami	Przetwarzanie danych Przepływ danych Cyfrowa usługa publiczna (objęte art. 17)

	Artykuł 74 3. Przygotowując system kandydujący, ENISA **ściśle współpracuje z ECCG**. **ECCG zapewnia ENISA pomoc** i doradztwo eksperckie w związku z przygotowaniem systemu kandydującego oraz, w stosownych przypadkach, uzupełniającej specyfikacji technicznej. **ENISA zwraca się do członków ECCG o przedstawienie pisemnej opinii na temat systemu kandydującego.** 4. **ENISA konsultuje się z zainteresowanymi stronami** w odpowiednim czasie w ramach formalnego, otwartego, przejrzystego i integracyjnego procesu konsultacji. **ENISA współpracuje również z odpowiednimi organami publicznymi w państwach członkowskich oraz z odpowiednimi podmiotami unijnymi w celu uzyskania ich fachowej porady** w związku z przygotowaniem projektu systemu i, w stosownych przypadkach, uzupełniającej specyfikacji technicznej. 6. **ENISA przekazuje** Komisji **projekt systemu** najpóźniej w ciągu 60 dni od daty złożenia wniosku, o którym mowa w ust. 5. 7. Po otrzymaniu projektu **systemu Komisja ocenia**, czy system ten odpowiada wnioskowi złożonemu zgodnie z art. 73. 8. W przypadku gdy Komisja zwraca ENISA projekt programu do ponownego rozpatrzenia zgodnie z ust. 7 lit. b) „ponowne rozpatrzenie”, stosuje się odpowiednio ust. 4, 5 i 7 niniejszego artykułu.			

Artykuł 75 Utrzymanie europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa	2. ENISA, we współpracy z Komisją i przy wsparciu ECCG oraz odpowiedniej podgrupy ds. utrzymania, zapewnia utrzymanie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, w tym z myślą o ewentualnym przeglądzie takich systemów przez Komisję. ENISA współpracuje i wymienia informacje z odpowiednimi podmiotami i grupami unijnymi zajmującymi się cyberbezpieczeństwem ( ) w odniesieniu do działań związanych z utrzymaniem. 5. ECCG może wydać opinię w sprawie utrzymania europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa.	Komisja Europejska ENISA ECCG Jednostki oceniające zgodność	ENISA zapewnia utrzymanie. Obejmuje to okresowe spotkania hybrydowe lub online, gromadzenie informacji, analizowanie i dzielenie się nimi (w odniesieniu do europejskiego systemu certyfikacji cyberbezpieczeństwa).	Przetwarzanie danych Przepływ danych
Artykuł 76 Ocena, przegląd i wycofanie europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa	1. Co najmniej co cztery lata po wejściu w życie europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa ENISA ocenia wpływ i skuteczność tego systemu we współpracy z odpowiednią podgrupą ds. utrzymania ECCG oraz z uwzględnieniem opinii otrzymanych od zainteresowanych stron. ENISA przeprowadza ocenę, dokonując niezbędnej analizy rynku zgodnie z art. 8 ust. 1. 3. Przy przeglądzie lub wycofaniu europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa Komisja konsultuje się z ENISA, ECCG i odpowiednią podgrupą ds. utrzymania, a także uwzględnia opinie odpowiednich zainteresowanych stron i innych podmiotów unijnych. 4. ECCG może wydać opinię w sprawie przeglądu lub wycofania europejskiego systemu	Komisja Europejska ENISA ECCG	Komisja dokonuje przeglądu systemów w porozumieniu z odpowiednimi zainteresowanymi stronami.	Przetwarzanie danych Przepływ danych

	certyfikacji cyberbezpieczeństwa. Komisja należycie uwzględnia tę opinię przy przeglądzie lub wycofaniu europejskiego systemu certyfikacji cyberbezpieczeństwa.			
Artykuł 77 Specyfikacje techniczne europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa	3. W przypadku gdy w europejskim systemie certyfikacji cyberbezpieczeństwa, o którym mowa w art. 74 ust. 10, zawarto odniesienia do specyfikacji technicznych, są one udostępniane na stronie internetowej, o której mowa w art. 79. 4. W należycie uzasadnionych przypadkach, w szczególności gdy specyfikacje techniczne zawierają informacje, które mogłyby zagrozić bezpieczeństwu certyfikowanych produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów, są one udostępniane wyłącznie zainteresowanym stronom, których dotyczą wymogi systemu. System taki nie jest wymieniony w europejskim systemie certyfikacji w zakresie cyberbezpieczeństwa, o którym mowa w art. 74 ust. 10.	ENISA Państwa członkowskie Jednostki oceniające zgodność	Udostępnianie informacji na stronie internetowej ENISA poświęconej certyfikacji	Przepływ danych Cyfrowe usługi publiczne
Artykuł 79 Strona internetowa poświęcona europejskim systemom certyfikacji w zakresie cyberbezpieczeństwa	1. ENISA organizuje działania mające na celu promowanie stosowania przyjętych europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, w tym poprzez prowadzenie strony internetowej, o której mowa w ust. 2 niniejszego artykułu. 2. ENISA prowadzi i regularnie aktualizuje specjalną stronę internetową zawierającą informacje publiczne na temat:	ENISA Państwa członkowskie Jednostki oceniające zgodność	Utrzymanie informacji Strona internetowa zobowiązuje ENISA do gromadzenia, przetwarzania i utrzymywania kompleksowych baz danych zawierających informacje dotyczące certyfikacji, co wymaga ciągłych działań w zakresie zarządzania danymi.	Cyfrowa usługa publiczna Rozwiązanie cyfrowe Przetwarzanie danych Przepływ danych

	a) europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa; b) opłatach związanych z utrzymaniem każdego europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa; c) odpowiednie specyfikacje techniczne ENISA; (d) europejskie certyfikaty cyberbezpieczeństwa i unijne deklaracje zgodności, w tym informacje dotyczące certyfikatów i deklaracji, które straciły ważność, zostały zawieszone, cofnięte lub wygasły; e) odpowiednie uzupełniające informacje dotyczące cyberbezpieczeństwa przekazane zgodnie z art. 84 ust. 2; f) podsumowania wzajemnych ocen zgodnie z art. 89 ust. 7; g) specyfikacje techniczne, do których odwołuje się europejski system certyfikacji cyberbezpieczeństwa zgodnie z art. 74 ust. 10. 3. W stosownych przypadkach **strona internetowa**, **o której mowa w ust. 2**, **zawiera również informacje** o krajowych systemach certyfikacji w zakresie cyberbezpieczeństwa, które zostały zastąpione europejskim systemem certyfikacji w zakresie cyberbezpieczeństwa.			
Artykuł 81 Elementy europejskiego systemu certyfikacji cyberbezpieczeństwa	5. Komisja jest uprawniona do przyjmowania aktów wykonawczych ustanawiających wspólne zasady i wzorcowe przepisy dotyczące elementów określonych w ust. 1, 2 i 3 we wszystkich europejskich systemach certyfikacji w zakresie cyberbezpieczeństwa. W stosownych przypadkach i o ile jest to możliwe, europejski system certyfikacji w zakresie	ENISA Ogół społeczeństwa Organy państw członkowskich	Konsultacje z odpowiednimi zainteresowanymi stronami wymagającymi przepływu i przetwarzania danych	Przepływ danych Przetwarzanie danych

	cyberbezpieczeństwa może zawierać odniesienia do tych zasad i wzorcowych przepisów. Akty wykonawcze, o których mowa w ust. 5, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2. **Przy opracowywaniu lub zmianie wspólnych zasad i wzorcowych przepisów dotyczących elementów europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa Komisja konsultuje się z ENISA i uwzględnia, w stosownych przypadkach, opinie wyrażone przez ECCG, odpowiednie zainteresowane strony i inne właściwe organy.**			
Artykuł 83 Samoocena zgodności	3. Producent lub dostawca produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiot, którego cyberbezpieczeństwo podlega certyfikacji, udostępnia krajowemu organowi certyfikacji cyberbezpieczeństwa wyznaczonemu zgodnie z art. 89, na okres przewidziany w europejskim systemie certyfikacji cyberbezpieczeństwa, oświadczenie UE o zgodności, dokumentację techniczną oraz wszelkie inne istotne informacje dotyczące zgodności produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa z europejskim systemem certyfikacji cyberbezpieczeństwa. **Kopia oświadczenia UE o zgodności jest przekazywana bez zbędnej zwłoki krajowemu organowi certyfikacji cyberbezpieczeństwa oraz ENISA.**	ENISA Ogół społeczeństwa Organy państw członkowskich	Dostępność informacji; wymiana danych Wymiana danych wymaga przetwarzania przez ENISA i organy państw członkowskich	Przepływ danych Przetwarzanie danych

Artykuł 84 Dodatkowe informacje dotyczące cyberbezpieczeństwa certyfikowanych produktów, usług i procesów ICT	1. Producent lub dostawca produktów ICT, usług ICT lub procesów ICT, dla których wydano unijne oświadczenie o zgodności lub europejski certyfikat cyberbezpieczeństwa, **podaje do wiadomości publicznej następujące dodatkowe informacje dotyczące cyberbezpieczeństwa**.	Producent lub dostawca produktów ICT, usług ICT lub procesów ICT Ogół społeczeństwa Jednostki oceniające zgodność	Udostępnianie informacji w formie elektronicznej.	Przepływ danych
Artykuł 85 Wydawanie europejskich certyfikatów cyberbezpieczeństwa	2. Organy oceny zgodności, o których mowa w art. 91, wydają europejskie certyfikaty cyberbezpieczeństwa na podstawie kryteriów zawartych w europejskim systemie certyfikacji cyberbezpieczeństwa przyjętym zgodnie z art. 74. 6. Osoba fizyczna lub prawna, która przedkłada produkty ICT, usługi ICT, procesy ICT lub zarządzane usługi bezpieczeństwa do certyfikacji, lub podmiot, który ubiega się o certyfikację swojego stanu cyberbezpieczeństwa, **udostępnia wszystkie informacje niezbędne do przeprowadzenia certyfikacji krajowemu organowi certyfikacji cyberbezpieczeństwa** wyznaczonemu zgodnie z art. 89, jeżeli organ ten jest organem wydającym europejski certyfikat cyberbezpieczeństwa, lub organowi oceny zgodności, o którym mowa w art. 91. 7. Jednostki oceniające zgodność oraz, w stosownych przypadkach, krajowe **organy** certyfikacji cyberbezpieczeństwa **informują ENISA** bez zbędnej zwłoki o swoich decyzjach mających wpływ na status europejskich certyfikatów cyberbezpieczeństwa i unijnych oświadczeń o zgodności zgodnie z art. 94. 8. **Posiadacz europejskiego certyfikatu cyberbezpieczeństwa informuje jednostkę**	ENISA Ogół społeczeństwa Organy państw członkowskich Jednostki oceniające zgodność	Wymiana informacji istotnych dla procesów certyfikacji	Przepływ danych Przetwarzanie danych

	oceniającą zgodność oraz, w stosownych przypadkach, krajowy organ certyfikacji cyberbezpieczeństwa, o których mowa w ust. 7, o wszelkich wykrytych później lukach w zabezpieczeniach lub niezgodnościach dotyczących certyfikowanego produktu ICT, usługi ICT, procesu ICT, zarządzanej usługi bezpieczeństwa lub stanu cyberbezpieczeństwa podmiotu, które mogą mieć wpływ na jego zgodność z certyfikatem. **Jednostka ta przekazuje te informacje bez zbędnej zwłoki** właściwemu krajowemu organowi certyfikacji w zakresie cyberbezpieczeństwa i ocenia wpływ na certyfikat zgodnie z warunkami systemu, o których mowa w art. 81 lit. f).			
Artykuł 86 Krajowe systemy certyfikacji w zakresie cyberbezpieczeństwa	4. **Państwa członkowskie informują Komisję i ECCG przed przyjęciem nowych krajowych systemów certyfikacji cyberbezpieczeństwa** dla produktów ICT, usług ICT, procesów ICT ( ), zarządzanych usług bezpieczeństwa i cyberpostury podmiotów.	ENISA Państwa członkowskie Komisja	Wymiana informacji	Przepływ danych
Artykuł 88 Krajowe organy certyfikacji w zakresie cyberbezpieczeństwa	2. Każde państwo członkowskie **informuje Komisję o tożsamości wyznaczonych krajowych organów certyfikacji w zakresie cyberbezpieczeństwa**. W przypadku wyznaczenia przez państwo członkowskie więcej niż jednego organu, informuje ono również Komisję o zadaniach przypisanych każdemu z tych organów. 6. Krajowe organy certyfikacji w zakresie cyberbezpieczeństwa: c) **monitorują, we współpracy z odpowiednimi organami nadzoru rynku, zgodność z obowiązkami producentów lub dostawców**	ENISA Organy państw członkowskich Komisja Ogół społeczeństwa Jednostki oceniające zgodność	Państwo członkowskie informuje Komisję o wyznaczonych organach oceny zgodności Organy państw członkowskich wykonują różne zadania w zakresie monitorowania, nadzoru i współpracy, które wymagają przepływu danych i ich przetwarzania.	Przepływ danych Przetwarzanie danych

	produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub podmiotów, których cyberbezpieczeństwo jest certyfikowane zgodnie z niniejszym rozporządzeniem, które mają siedzibę na ich terytorium i które przeprowadzają samoocenę zgodności oraz w ramach odpowiedniego europejskiego systemu certyfikacji cyberbezpieczeństwa ; d) bez uszczerbku dla art. 91 ust. 3, **aktywnie pomagać krajowym jednostkom akredytującym lub innym właściwym organom w monitorowaniu i nadzorowaniu** działalności jednostek oceniających zgodność do celów niniejszego rozporządzenia; e) współpracować z Komisją Europejską w przypadku zakwestionowania kompetencji jednostki oceniającej zgodność zgodnie z art. 94; f) **monitorować i nadzorować działalność** organów publicznych, o których mowa w art. 85 ust. 3; g) w stosownych przypadkach, udzielać upoważnień organom oceny zgodności zgodnie z art. 93, monitorować zgodność organów oceny zgodności z określonymi lub dodatkowymi wymogami określonymi w europejskich systemach certyfikacji w zakresie cyberbezpieczeństwa zgodnie z art. 81 ust. 3 lit. f) oraz egzekwować wypełnianie przez nie tych wymogów, a także ograniczać, zawieszać lub cofać istniejące upoważnienia, jeżeli organy oceny zgodności nie spełniają wymogów niniejszego rozporządzenia;			

	h) **rozpatrywać skargi** osób fizycznych lub prawnych dotyczące europejskich certyfikatów cyberbezpieczeństwa wydanych przez krajowe organy certyfikacji cyberbezpieczeństwa lub europejskich certyfikatów cyberbezpieczeństwa wydanych przez organy oceny zgodności zgodnie z [art. 85 ust. 4] lub dotyczących unijnych oświadczeń o zgodności wydanych na podstawie art. 83, badać przedmiot takich skarg w odpowiednim zakresie oraz informować skarżącego o postępach i wynikach postępowania w rozsądnym terminie; i) przedkładać Komisji, ENISA i ECCG roczne sprawozdanie z głównych działań do dnia 31 marca [rok wejścia w życie + 12 miesięcy] każdego roku oraz udostępniać te sprawozdania zespołowi ds. wzajemnej oceny, jeżeli krajowy organ certyfikacji w zakresie cyberbezpieczeństwa podlega wzajemnej ocenie zgodnie z art. 89; j) **współpracować z innymi krajowymi organami certyfikacji w zakresie cyberbezpieczeństwa**, organami nadzoru rynku lub innymi organami publicznymi, w tym poprzez wymianę informacji na temat ewentualnej niezgodności produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberbezpieczeństwa podmiotów z wymogami niniejszego rozporządzenia lub z wymogami określonych europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa;			

	k) **monitorowanie istotnych zmian w dziedzinie certyfikacji w zakresie cyberbezpieczeństwa**. 8. Krajowe organy certyfikacji w zakresie cyberbezpieczeństwa współpracują ze sobą oraz z Komisją, w szczególności poprzez **wymianę informacji, doświadczeń i dobrych praktyk** w zakresie certyfikacji w zakresie cyberbezpieczeństwa oraz kwestii technicznych dotyczących cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberbezpieczeństwa podmiotów. 9. Do dnia [wejścia w życie + 6 miesięcy] ENISA opracowuje wzór sprawozdania, o którym mowa w ust. 6 lit. i) niniejszego artykułu, we współpracy z Komisją i ECCG.			
Artykuł 89 Wzajemna ocena	5. **ENISA wspiera** organizację mechanizmu wzajemnej oceny i wzajemnych ocen, w tym **poprzez opracowywanie odpowiednich wytycznych i wzorów** we współpracy z Komisją i ECCG. 7. **Sprawozdanie końcowe zawierające ewentualne** wytyczne lub zalecenia oraz podsumowanie wzajemnej oceny są analizowane przez ECCG ( ), która zatwierdza podsumowanie do publikacji, o której mowa w art. 79 ust. 2.	UE ENISA ECCG	Udostępnianie danych online	Przepływ danych Przetwarzanie danych

Artykuł 90 Europejska grupa ds. certyfikacji cyberbezpieczeństwa (ECCG)	3. ECCG ma następujące zadania: [odniesienie do innych artykułów] h) badanie istotnych zmian w dziedzinie certyfikacji w zakresie cyberbezpieczeństwa, w tym na szczeblu krajowym zgodnie z art. 86, oraz wymiana informacji i dobrych praktyk dotyczących systemów certyfikacji w zakresie cyberbezpieczeństwa; (i) ułatwianie współpracy między krajowymi organami certyfikacji w zakresie cyberbezpieczeństwa zgodnie z zasadami określonymi w niniejszym tytule poprzez budowanie potencjału i wymianę informacji, w szczególności dotyczących kwestii związanych z certyfikacją w zakresie cyberbezpieczeństwa; [odniesienie do innych artykułów] k) ułatwianie dostosowywania europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa do uznanych międzynarodowych norm, w tym w ramach utrzymania istniejących europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa, oraz, w stosownych przypadkach, przedstawianie ENISA zaleceń dotyczących współpracy z odpowiednimi europejskimi lub międzynarodowymi organizacjami normalizacyjnymi w celu usunięcia niedociągnięć lub luk w dostępnych normach europejskich lub uznanych międzynarodowych.	Państwa członkowskie ENISA Komisja Europejska	Analiza, wymiana informacji i współpraca między organami państw członkowskich a organizacjami międzynarodowymi w zakresie europejskiej certyfikacji cyberbezpieczeństwa	Przetwarzanie danych Przepływ danych

Artykuł 92 Dodatkowa harmonizacja kompetencji organów oceny zgodności	4. W przypadku gdy krajowy organ certyfikacji w zakresie cyberbezpieczeństwa otrzyma wniosek zgodnie z ust. 3, **informuje** on **o tym krajowy organ certyfikacji w zakresie cyberbezpieczeństwa państwa członkowskiego, w którym ma siedzibę organ oceniający zgodność składający wniosek**. W takich przypadkach krajowy organ certyfikacji w zakresie cyber u tego państwa członkowskiego może uczestniczyć w procedurze udzielania upoważnienia w charakterze obserwatora.	Organy państw członkowskich Jednostki oceniające zgodność	Wymiana i przechowywanie informacji	Przepływ danych Przetwarzanie danych
Artykuł 93 Powiadomienia dotyczące organów oceny zgodności	1. W odniesieniu do każdego europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa krajowe **organy** certyfikacji **w zakresie** cyberbezpieczeństwa **państwa członkowskiego powiadamiają Komisję i pozostałe państwa członkowskie** o jednostkach oceniających zgodność, które zostały akredytowane i, w stosownych przypadkach, upoważnione zgodnie z art. 92. 2. **Krajowe organy certyfikacji w zakresie cyberbezpieczeństwa dokonują powiadomienia, o którym mowa w ust. 1,** przy użyciu elektronicznego narzędzia do powiadamiania opracowanego i zarządzanego przez Komisję.	ENISA Państwa członkowskie Komisja Jednostki oceniające zgodność	Powiadomienia akredytowanych i upoważnionych organów oceny zgodności	Przepływ danych Przetwarzanie danych
Artykuł 94 Kwestionowanie kompetencji organów oceny zgodności	1. 1. **Komisja bada** wszelkie przypadki, w których ma wątpliwości lub w których powiadomiono ją o wątpliwościach dotyczących kompetencji jednostki oceniającej zgodność w zakresie spełniania lub dalszego spełniania przez tę jednostkę wymagań i obowiązków, którym podlega.	Komisja Państwa członkowskie ENISA	Kwestionowanie kompetencji organów oceny zgodności	Przepływ danych Przetwarzanie danych Cyfrowe usługi publiczne

	2. **Krajowy organ certyfikacji w zakresie cyberbezpieczeństwa przekazuje Komisji,** na jej wniosek, wszelkie informacje dotyczące podstawy zgłoszenia lub utrzymania kompetencji danego organu oceny zgodności. 3. **Komisja zapewnia poufność wszystkich informacji szczególnie chronionych uzyskanych w trakcie dochodzeń.** 4. Jeżeli Komisja stwierdzi, że jednostka oceniająca zgodność nie spełnia lub przestała spełniać wymogi dotyczące jej notyfikacji, **informuje o tym krajowy organ certyfikacji w zakresie cyberbezpieczeństwa** i zwraca się do niego o podjęcie niezbędnych środków naprawczych, w tym, w razie potrzeby, o cofnięcie notyfikacji.			
Artykuł 95 Obowiązek informacyjny i przechowywania danych przez jednostki oceniające zgodność	1. Jednostki oceniające zgodność **informują krajowy organ certyfikacji cyberbezpieczeństwa** o następujących kwestiach: a) wszelkie odmowy, ograniczenia, zawieszenia lub cofnięcia certyfikatu; b) wszelkie okoliczności mające wpływ na zakres i warunki powiadomienia, o którym mowa w art. 93 ust. 1; c) wszelkie wnioski o udzielenie informacji, które otrzymały od organów nadzoru rynku w odniesieniu do działań związanych z oceną zgodności; d) na żądanie, wszelkie działania w zakresie oceny zgodności przeprowadzone w ramach zakresu ich zgłoszenia oraz wszelkie inne przeprowadzone działania, w tym działania transgraniczne i podwykonawstwo.	Organy państw członkowskich Jednostki oceniające zgodność	Wymiana informacji od organów oceny zgodności	Przepływ danych Przetwarzanie danych

	2. **Jednostki oceniające zgodność przekazują również ENISA informacje,** o których mowa w ust. 1 lit. a), w celu ułatwienia wykonywania zadań ENISA zgodnie z art. 79. 3. **Jednostki oceniające zgodność przekazują innym jednostkom oceniającym zgodność** działającym na podstawie niniejszego rozporządzenia, które prowadzą podobną działalność w zakresie oceny zgodności obejmującą te same produkty ICT, usługi ICT, procesy ICT, zarządzane usługi bezpieczeństwa lub podmioty, których cyberbezpieczeństwo jest certyfikowane**,** bez zbędnej zwłoki **odpowiednie informacje** dotyczące kwestii związanych z negatywnymi, a na żądanie również pozytywnymi wynikami oceny zgodności. 4. **Jednostki oceniające zgodność prowadzą system ewidencji** zawierający wszystkie dokumenty i dowody sporządzone lub otrzymane w związku z każdą przeprowadzoną przez nie oceną i certyfikacją. Ewidencja jest przechowywana w bezpieczny i dostępny sposób przez okres niezbędny do celów certyfikacji oraz przez co najmniej pięć lat po wygaśnięciu lub cofnięciu odpowiedniego europejskiego certyfikatu cyberbezpieczeństwa.			

Artykuł 96 Prawo do wniesienia skargi i prawo do skutecznego środka odwoławczego	2. Organ lub jednostka, do której wniesiono skargę**, informuje skarżącego o przebiegu** postępowania, podjętej decyzji oraz prawie do skutecznego środka odwoławczego, o którym mowa w ust. 3 i 4. 4. Postępowanie na podstawie niniejszego artykułu toczy się przed sądami państwa członkowskiego, w któr ie znajduje się organ lub podmiot, przeciwko któremu wniesiono środek odwoławczy.	Organy państw członkowskich Komisja Europejska Ogół społeczeństwa Posiadacze certyfikatów	Przepływ informacji między organami a ogółem społeczeństwa w sprawie skarg Postępowania przed sądami państw członkowskich	Przepływ danych
Artykuł 97 Kary	**Państwa członkowskie niezwłocznie powiadamiają Komisję** o tych przepisach i środkach oraz powiadamiają ją o wszelkich późniejszych zmianach mających wpływ na te przepisy i środki.	Organy państw członkowskich Komisja Europejska	Przepływ informacji związanych z powiadamianiem Komisji przez państwa członkowskie o sankcjach.	Przepływ danych
Artykuł 99 Oceny ryzyka bezpieczeństwa	Komisja lub co najmniej trzy państwa członkowskie mogą zwrócić się do NIS CG o przeprowadzenie skoordynowanych ocen ryzyka w ciągu 6 miesięcy. Komisja może zwrócić się o skrócenie terminów. Oceny ryzyka obejmują opracowanie scenariuszy ryzyka i analizę danych. Przygotowanie skoordynowanych ocen ryzyka dla bezpieczeństwa W przypadkach uzasadniających natychmiastową interwencję Komisja niezwłocznie konsultuje się z państwami członkowskimi i przeprowadza ocenę ryzyka. Decyzje dotyczące przeprowadzenia oceny ryzyka (przetwarzanie/analiza danych).	Komisja Europejska Państwa członkowskie UE Grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji ENISA	Wnioskowanie o informacje i ich otrzymywanie; analiza danych do celów skoordynowanej oceny ryzyka Konsultacje z państwami członkowskimi i przeprowadzanie oceny ryzyka	Przetwarzanie danych Przepływ danych

Artykuł 100 ust. 1 i 2 Wyznaczenie państw trzecich budzących obawy w zakresie cyberbezpieczeństwa	1. Jeżeli w wyniku oceny ryzyka dla bezpieczeństwa, o której mowa w art. 99, lub na podstawie innych źródeł, takich jak publiczne oświadczenie w imieniu Unii lub państwa członkowskiego, okaże się, że państwo trzecie stwarza poważne i strukturalne ryzyko nietechniczne dla łańcuchów dostaw ICT, Komisja weryfikuje zagrożenie stwarzane przez to państwo, biorąc pod uwagę szereg elementów , co prowadzi do przetwarzania/analizy danych. 2. Jeżeli po przeprowadzeniu weryfikacji, o której mowa w ust. 1, Komisja stwierdzi, że państwo trzecie stwarza poważne i strukturalne zagrożenia nietechniczne dla łańcuchów dostaw ICT, może ona w drodze aktu wykonawczego podjąć decyzję o uznaniu tego państwa trzeciego za państwo stwarzające zagrożenie dla cyberbezpieczeństwa łańcuchów dostaw ICT, co prowadzi do przetwarzania i analizy danych oraz przepływu danych.	Państwa członkowskie UE Komisja Europejska	Otrzymywanie informacji, analiza informacji, wymiana informacji.	Przepływy danych Przetwarzanie danych

Artykuł 101 Ogólny mechanizm łańcucha dostaw ICT Artykuł 102 Identyfikacja kluczowych aktywów ICT i Artykuł 103 Środki łagodzące w łańcuchach dostaw ICT	1. W przypadku gdy grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji przeprowadziła skoordynowaną ocenę ryzyka bezpieczeństwa na poziomie Unii zgodnie z art. 99 ust. 1 i 2 niniejszego rozporządzenia lub po zakończeniu procedury w przypadku znaczącego zagrożenia cybernetycznego zgodnie z art. 99 ust. 3, Komisja może podjąć środki przewidziane w art. 102 i 103. Komisja jest uprawniona do przyjmowania aktów wykonawczych, które będą określać kluczowe aktywa ICT i środki łagodzące, w tym ograniczenia i zakazy dotyczące łańcuchów dostaw ICT (szczegółowo opisane w sekcji 4.5 poniżej). Przygotowując się do tego procesu, Komisja uwzględni i weźmie pod uwagę kilka aspektów, które odnoszą się do **przetwarzania/analizy danych , a w niektórych przypadkach** do **przepływu danych**: Artykuł 102 lit. a)–f) Artykuł 103 ust. 4 lit. a)–d) Artykuł 103 ust. 6	Komisja Europejska Grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji Odpowiednie zainteresowane strony	Analiza danych/przetwarzanie danych; konsultacje z odpowiednimi zainteresowanymi stronami	Przetwarzanie danych Przepływ danych

Artykuł 104 Identyfikacja dostawców wysokiego ryzyka	W drodze aktów wykonawczych Komisja ustanawia wykazy dostawców wysokiego ryzyka, których dotyczą zakazy określone w aktach wykonawczych przyjętych zgodnie z art. 103 ust. 1 lub zakaz, o którym mowa w art. 111 ust. 1. Komisja sporządza mapę dostawców dostarczających komponenty ICT oraz komponenty zawierające komponenty ICT i dokonuje wstępnej oceny, którzy dostawcy są potencjalnie mający siedzibę w państwach trzecich wyznaczonych zgodnie z art. 100 lub są przez nie kontrolowani. Komisja ocenia miejsce siedziby, a także strukturę własnościową i kontrolną. Komisja jest uprawniona do żądania od dostawców niezbędnych informacji oraz przekazuje zainteresowanym dostawcom wstępne ustalenia dotyczące oceny miejsca prowadzenia działalności, struktury własnościowej i kontroli oraz zapewnia im możliwość przedstawienia swojego stanowiska. Komisja może zwrócić się do właściwego organu o przeprowadzenie wstępnej oceny siedziby, struktury własnościowej i kontroli dostawcy, jeżeli jest to uzasadnione ze względu na charakter działalności tego dostawcy. Właściwy organ może zaproponować przeprowadzenie takiej	Komisja Europejska Właściwe organy Dostawcy	Analiza danych/przetwarzanie danych; konsultacje z właściwymi organami, konsultacje z dostawcami	Przetwarzanie danych Przepływ danych

	wstępnej oceny. Komisja weryfikuje te wstępne ustalenia w celu podjęcia decyzji, czy dostawca powinien zostać umieszczony w wykazie dostawców wysokiego ryzyka. Komisja regularnie aktualizuje wykazy dostawców wysokiego ryzyka w celu usunięcia lub dodania dostawców wysokiego ryzyka. Dostawcy wysokiego ryzyka ujęci w wykazie mogą zwrócić się do Komisji o ponowną ocenę ich struktury zakładu, kontroli i własności po przedstawieniu dowodów potwierdzających, że nastąpiły istotne zmiany.			
Artykuł 105 Zwolnienie podmiotów mających siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowanych przez takie państwo Artykuł 108 Poufność	(1) Podmiot mający siedzibę w wyznaczonym państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowany przez takie państwo **może złożyć** do Komisji **uzasadniony wniosek**. (3) Komisja ocenia i przyjmuje decyzję, **biorąc pod uwagę kilka aspektów** prowadzących do analizy danych. (Artykuł 105 ust. 3 i 4) Informacje otrzymane przez Komisję są wykorzystywane wyłącznie do celów, dla których zostały pozyskane.	Komisja Europejska Podmioty mające siedzibę w wyznaczonym państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowane przez takie podmioty	Komisja otrzymuje wniosek; analizuje dane.	Przepływ danych Przetwarzanie danych

Artykuł 107 Rejestr	Komisja prowadzi publicznie dostępny rejestr swoich decyzji, o których mowa w art. 105. W rejestrze tym podaje się nazwy podmiotów, których dotyczą decyzje.	Komisja Podmioty mające siedzibę w wyznaczonym państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowane z takiego państwa	Komisja prowadzi publicznie dostępny rejestr.	Rozwiązanie cyfrowe
Artykuł 111 Zakazy dotyczące mobilnych, stacjonarnych i satelitarnych sieci łączności elektronicznej	Właściwy organ wyznaczony na mocy niniejszego rozporządzenia niezwłocznie **informuje** właściwy organ zgodnie z rozporządzeniem (UE) XX/XXXX [wniosek DNA] o środkach nałożonych na dostawców mobilnych, stacjonarnych i satelitarnych sieci łączności elektronicznej.	Właściwy organ w rozumieniu art. 9 lub 20 rozporządzenia (UE) XX/XXXX [wniosek DNA] Operatorzy mobilnych, stacjonarnych i satelitarnych sieci łączności elektronicznej	Przepływ informacji od właściwego organu do podmiotów w związku z zezwoleniami.	Przepływ danych
Artykuł 112 ust. 1 i 4 Właściwe organy	(1) **Każde państwo członkowskie wyznacza** co najmniej jeden właściwy organ odpowiedzialny za zadania w zakresie nadzoru i egzekwowania przepisów, o których mowa w art. 114. (4) Każde państwo członkowskie bez zbędnej zwłoki powiadamia Komisję o nazwach właściwych organów wyznaczonych zgodnie z ust. 1, o odpowiednich zadaniach tych organów oraz o wszelkich późniejszych zmianach w tym zakresie. Każde państwo członkowskie podaje również do wiadomości publicznej	Państwa członkowskie UE Komisja Europejska Ogół społeczeństwa	Państwa członkowskie wyznaczające właściwe organy i powiadamiające o tym Komisję.	Przepływ danych

	nazwy właściwych organów wyznaczonych zgodnie z ust. 1.			
Artykuł 113 Sieć współpracy i usług wsparcia Komisji	1. Komisja ustanawia sieć współpracy właściwych organów państw członkowskich i Komisji, która służy jako platforma współpracy i wymiany informacji. Komisja zapewnia wsparcie administracyjne dla sieci. 2. Aby wspierać państwa członkowskie w wykonywaniu zadań nadzorczych, Komisja ocenia, czy dostawcy, których mogą dotyczyć określone zakazy, mają siedzibę w państwach trzecich budzących obawy w zakresie cyberbezpieczeństwa, wyznaczonych zgodnie z art. 100, lub są przez nie kontrolowani. W tym celu właściwy organ udostępnia Komisji odpowiednie informacje. 3. Do celów oceny Komisja jest uprawniona do żądania niezbędnych informacji od dostawców, których mogą dotyczyć określone zakazy, mających siedzibę w państwach trzecich wyznaczonych zgodnie z art. 100 lub kontrolowanych z tych państw.	Komisja Właściwe organy Podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555	Komisja ocenia dostawców i dzieli się informacjami z właściwymi organami, które dzielą się nimi z podmiotami, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555 Komisja zwraca się do dostawców o udzielenie informacji Właściwe organy informujące Komisję	Przetwarzanie danych Przepływ danych

	4. Po zakończeniu oceny Komisja przekazuje ustalenia właściwym organom w ramach sieci ustanowionej zgodnie z ust. 1. Właściwe organy w odpowiednim czasie informują zainteresowane podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, o ustaleniach. 5. W przypadku gdy właściwy organ poweźmie wiadomość o dostawcy, który może podlegać szczególnym zakazom, ma siedzibę w państwach trzecich budzących obawy w zakresie cyberbezpieczeństwa lub jest przez nie kontrolowany i który nie został poddany ocenie, niezwłocznie informuje o tym Komisję.			
Artykuł 114 Środki nadzorcze i egzekucyjne	Wymogi wobec państw członkowskich, które zapewnią przepływ informacji z podmiotami, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555. właściwe organy. Przed przyjęciem środków właściwe organy powiadamiają zainteresowane podmioty o swoich wstępnych ustaleniach. Właściwe organy współpracują ze sobą oraz z Komisją.	Państwa członkowskie UE Komisja Europejska Podmioty w kontekście załączników I i II do dyrektywy (UE) 2022/2555	Wymogi zapewniające przepływ informacji;	Przepływ danych Przetwarzanie danych

Artykuł 115 Kary	Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach oraz niezwłocznie powiadamiają ją o wszelkich późniejszych zmianach mających wpływ na te przepisy i środki.	Komisja Europejska Państwa członkowskie UE	Państwa członkowskie powiadamiające Komisję	Przepływ danych
Artykuł 116 Wzajemna pomoc	W przypadku gdy podmiot, o którym mowa w załączniku I lub II do dyrektywy (UE) 2022/2555, świadczy usługi w więcej niż jednym państwie członkowskim lub świadczy usługi w jednym lub kilku państwach członkowskich, a jego kluczowe aktywa znajdują się w jednym lub kilku innych państwach członkowskich, **właściwe organy zainteresowanych państw członkowskich współpracują ze sobą i udzielają sobie wzajemnej pomocy w razie potrzeby**. Wzajemna pomoc, o której mowa w akapicie pierwszym lit. c), może obejmować wnioski o udzielenie informacji i środki nadzorcze, w tym wnioski o przeprowadzenie kontroli na miejscu lub nadzoru zdalnego lub ukierunkowanych audytów bezpieczeństwa. Właściwy organ, do którego skierowano wniosek o pomoc, nie odrzuca tego wniosku, chyba że zostanie ustalone, że nie ma on kompetencji do udzielenia żądanej pomocy, żądana pomoc nie jest proporcjonalna do	Państwa członkowskie UE	Wzajemna pomoc w działaniach nadzorczych.	Przepływ danych Przetwarzanie danych

	zadań nadzorczych właściwego organu lub wniosek dotyczy informacji lub działań, których ujawnienie lub przeprowadzenie byłoby sprzeczne z istotnymi interesami bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obrony państwa członkowskiego. Przed odmową udzielenia pomocy właściwy organ konsultuje się z innymi właściwymi organami, których dotyczy sprawa, a także, na wniosek jednego z zainteresowanych państw członkowskich, z Komisją. W stosownych przypadkach i za wspólną zgodą właściwe organy różnych państw członkowskich mogą prowadzić wspólne działania nadzorcze.			
Artykuł 1 pkt 8 dyrektywy Zgłaszanie ataków ransomware (art. 27 ust. 13 NIS2)	w art. 23 dodaje się ust. 12 i 13 w brzmieniu: „13. Państwa członkowskie zapewniają, aby w przypadku znaczącego incydentu spowodowanego atakiem 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: czy podmiot otrzymał żądanie okupu i, w stosownych przypadkach, od kogo; czy okup został zapłacony, a jeśli tak, to w jakiej wysokości, za pomocą jakich środków płatniczych i na rzecz jakiego odbiorcy lub	Państwa członkowskie UE Podmioty o znaczeniu kluczowym i istotnym	Zgłaszanie	Przepływ danych

	adresata, w tym dostawcy kryptowalut i usług związanych z kryptowalutami, w stosownych przypadkach”.			
Artykuł 1 pkt 10 dyrektywy Wykaz podmiotów i rejestr (art. 27 ust. 1 NIS2)	**ENISA tworzy i prowadzi rejestr podmiotów o znaczeniu krytycznym i istotnym, a także podmiotów świadczących usługi rejestracji nazw domen, na podstawie informacji otrzymanych od pojedynczych punktów kontaktowych zgodnie z ust. 2.**	ENISA Państwa członkowskie UE (podmioty o znaczeniu kluczowym i istotnym zgodnie z NIS2, podmioty świadczące usługi rejestracji nazw domen)	ENISA tworzy i prowadzi rejestr	Rozwiązanie cyfrowe Cyfrowa usługa publiczna
Artykuł 1 pkt 11 dyrektywy Wykaz podmiotów i rejestr (art. 27 ust. 4 NIS2)	**„4. Po otrzymaniu informacji, o których mowa w art. 3 ust. 4, pojedynczy punkt kontaktowy danego państwa członkowskiego niezwłocznie przekazuje je do ENISA”.**	ENISA Państwa członkowskie UE	Państwa członkowskie dzielące się informacjami z ENISA	Przepływ danych
Artykuł 1 pkt 12 dyrektywy Wzajemna pomoc (art. 37a NIS2 ust. 1, 2, 3)	**1. ENISA wspiera państwa członkowskie** w udzielaniu wzajemnej pomocy w rozumieniu art. 37 i **pomaga w ułatwianiu takich procesów współpracy** w odniesieniu do podmiotów o znaczeniu kluczowym i istotnym (…). 2. ENISA **przeprowadza kompleksową analizę** (…) **ENISA we współpracy z** Komisją i grupą ds. współpracy opracowuje metodologię. Sprawozdanie jest aktualizowane co roku.	ENISA Państwa członkowskie UE Istotne i kluczowe podmioty w rozumieniu dyrektywy NIS2 Komisja Europejska	ENISA wspiera państwa członkowskie i ułatwia proces współpracy. Przeprowadza analizy, opracowuje wytyczne, metodologię i sprawozdania.	Przetwarzanie danych Przepływ danych

	(3.) ENISA w stosownych przypadkach wydaje zalecenia, opracowuje wytyczne, udziela pomocy (...)			
Artykuł 1 pkt 12 dyrektywy Wzajemna pomoc (art. 37a NIS2 ust. 4)	4. Do celów ust. 4 lit. e) niniejszego artykułu właściwe organy **zainteresowanych państw członkowskich przekazują ENISA, w miarę możliwości, następujące informacje** (...). 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.	ENISA Państwa członkowskie UE	Wymiana informacji	Przepływ danych
Artykuł 119 Wykonywanie przekazanych uprawnień	3. Niezwłocznie po przyjęciu aktu delegowanego Komisja **powiadamia o tym jednocześnie** Parlament Europejski i Radę.	Komisja Parlament Europejski Rada	Informacje przekazane do PE i Rady	Przepływ danych
Artykuł 120 Ocena i przegląd	1. Do dnia [DD MM RRRR], a następnie co pięć lat, Komisja zleca przeprowadzenie oceny wyników ENISA w odniesieniu do jej celów, mandatu, misji, zadań, zarządzania i lokalizacji zgodnie z wytycznymi Komisji. 5. Komisja przedstawia Parlamentowi Europejskiemu, Radzie i zarządowi sprawozdanie z wyników oceny. Wyniki oceny podaje się do wiadomości publicznej.	ENISA Komisja Ogół społeczeństwa	Gromadzenie i analiza danych; publiczne udostępnianie informacji	Przetwarzanie danych Przepływ danych

4.2. Dane

Ogólny opis danych objętych zakresem oraz wszelkich powiązanych norm/specyfikacji

Rodzaj danych	Odniesienia do wymagań	Norma i/lub specyfikacja (jeśli dotyczy)
Dane związane z analizami/raportami mającymi znaczenie dla odporności cyberbezpieczeństwa i społeczeństwa	**Artykuł 5 ust. 1 lit. a), b), c), e), f) i h)** **Artykuł 5 ust. 2, 3 i 4** **Artykuł 6** **Artykuł 7** **Artykuł 8** **Artykuł 9** **Artykuł 10** **Artykuł 11 ust. 2 lit. b) i c)** **Artykuł 12 ust. 4** **Artykuł 15** **Artykuł 1 pkt 7 dyrektywy**	Wykonując działania wymienione w art. 11 ust. 1 lit. a)–e) oraz ust. 2, ENISA korzysta z własnych analiz oraz, w stosownych przypadkach, z informacji otrzymanych w trakcie wykonywania swoich zadań, w tym: a) informacje pochodzące ze źródeł publicznie dostępnych, w tym publicznie znane luki w zabezpieczeniach produktów lub usług ICT dostępnych w europejskiej bazie danych luk w zabezpieczeniach utworzonej zgodnie z art. 12 ust. 2 dyrektywy (UE) 2022/2555; b) informacje udostępnione przez państwa członkowskie, podmioty unijne, CERT-EU, partnerów z sektora prywatnego lub pozarządowego oraz państwa trzecie i organizacje międzynarodowe, z zastrzeżeniem wszelkich ograniczeń dotyczących dalszego rozpowszechniania tych informacji, oznaczonych w widoczny sposób. ENISA wydaje wytyczne dotyczące interoperacyjności systemów informacji sieciowej wykorzystywanych do wymiany informacji, w tym w odniesieniu do transgranicznych centrów cyberbezpieczeństwa, o których mowa w art. 6 ust. 3 rozporządzenia (UE) 2025/38.
Dane istotne dla współpracy operacyjnej i świadomości sytuacyjnej	**Artykuł 10 ust. 4 lit. a)–g)** **Artykuł 10 ust. 6** **Artykuł 11 ust. 1 lit. a)–g)** **Artykuł 11 ust. 2 lit. a), b) i c)** **Artykuł 11 ust. 3**	**Standardy dotyczące poufności i postępowania z informacjami wrażliwymi** Wykonując działania wymienione w art. 11 ust. 1 lit. a)–e) oraz ust. 2, ENISA korzysta z własnych analiz oraz, w stosownych przypadkach, z informacji otrzymanych w trakcie wykonywania swoich zadań, w tym:

	Artykuł 11 ust. 4 **Artykuł 13 ust. 2** **Artykuł 15** **Artykuł 16 ust. 2 lit. e)**	a) informacje pochodzące ze źródeł publicznie dostępnych, w tym publicznie znane luki w zabezpieczeniach produktów lub usług ICT dostępnych w europejskiej bazie danych luk w zabezpieczeniach utworzonej zgodnie z art. 12 ust. 2 dyrektywy (UE) 2022/2555; b) informacje udostępnione przez państwa członkowskie, podmioty unijne, CERT-EU, partnerów z sektora prywatnego lub pozarządowego oraz organizacje z państw trzecich i organizacje międzynarodowe, z zastrzeżeniem wszelkich ograniczeń dotyczących dalszego rozpowszechniania tych informacji, oznaczonych w widoczny sposób.
Dane mające znaczenie dla europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa i autoryzacji dostawców **Dane mające znaczenie dla celów, przeznaczenia i treści europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa**	**Artykuł 17** **Artykuł 18** **Artykuły 19–23** **Artykuły 72, 73, 74, 75, 76, 77, 79, 81, 83, 84**	Europejski system poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa obejmuje (...): zasady dotyczące przechowywania dokumentacji przez uprawnionych dostawców poświadczeń Upoważnieni dostawcy zapewniają, aby na wniosek osoby fizycznej europejskie certyfikaty umiejętności w zakresie cyberbezpieczeństwa były wydawane jako certyfikaty elektroniczne atrybutów w formacie, który można przechowywać w europejskich portfelach tożsamości cyfrowej określonych w rozporządzeniu (UE) nr 910/2014. . Komisja i ENISA powinny przestrzegać odpowiednich przepisów prawa Unii przy ustanawianiu europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa w odniesieniu do danych.
Dane związane z zarządzaniem europejskimi ramami certyfikacji w zakresie cyberbezpieczeństwa	**Artykuły 85, 86, 88, 89, 90, 92, 93, 94, 95, 96, 97**	ENISA, organy oceny zgodności i krajowe organy certyfikacji w zakresie cyberbezpieczeństwa powinny zapewnić poufność danych i przestrzegać przepisów odpowiedniego systemu odnoszącego się do międzynarodowych norm określających wymagania.

Dane mające znaczenie dla wewnętrznych funkcji ENISA (budżet, SPD, strategie wewnętrzne)	**Artykuł 25** **Artykuł 28 ust. 1** **Artykuł 30** **Artykuł 31 ust. 8** **Artykuł 32 ust. 3 i 5** **Artykuł 35 ust. 5, 6** **Artykuł 36–43** **Artykuł 44** **Artykuł 45** **Artykuł 47 ust. 10** **Artykuły 48–49** **Artykuł 52, artykuł 58**	**Wzory i wytyczne dotyczące regulacji finansowych; wytyczne wewnętrzne**
Dane osobowe	**Artykuł 22** **Tytuł II, rozdział III, sekcja 6 Komisja odwoławcza** **Artykuł 66** **Artykuł 80 ust. 1 lit. c) i x)** **Artykuł 81 ust. 2** **Artykuł 88 ust. 6 lit. h)** **Artykuł 95** **Artykuł 96**	**Rozporządzenie (UE) 2018/1725** **Rozporządzenie (UE) 2016/679**
Dane gromadzone i analizowane w kontekście przeprowadzania skoordynowanych ocen ryzyka, opracowywania scenariuszy ryzyka i identyfikacji kluczowych zasobów ICT	**Artykuł 98** **Artykuł 99** **Artykuł 102** **Artykuł 103** **Artykuł 105**	Bez uszczerbku dla art. 13 rozporządzenia (UE) 2024/2847 i art. 21 dyrektywy (UE) 2022/2555

Dane dotyczące państw trzecich/podmiotów z państw trzecich	**Artykuł 100 ust. 1, 3 i 4** **Artykuł 104** **Artykuł 105** **Artykuł 107** **Artykuł 113**	Nie dotyczy
Dane dotyczące organów krajowych	**Artykuł 112** **Artykuł 114** **Artykuł 116**	Nie dotyczy
Dane istotne dla oceny ryzyka	**Artykuł 5 ust. 2**	**Standardy dotyczące poufności i postępowania z informacjami wrażliwymi**
Wzajemna pomoc między państwami członkowskimi	**Rozporządzenie 5 ust. 1 lit. g) i art. 1 pkt 12 dyrektywy**	**/**

Zgodność z europejską strategią w zakresie danych

Wyjaśnienie, w jaki sposób wymogi są zgodne z europejską strategią w zakresie danych

Wymogi zawarte we wniosku CSA2 są zgodne z europejską strategią w zakresie danych i nie mają na nią żadnego konkretnego wpływu.

Zgodność z zasadą jednokrotnego gromadzenia danych

Wyjaśnij, w jaki sposób uwzględniono zasadę jednokrotnego wypełniania formularzy i zbadano możliwość ponownego wykorzystania istniejących danych

Jednym z celów wniosku jest maksymalizacja wysiłków Komisji na rzecz uproszczenia procedur oraz zmniejszenie obciążenia administracyjnego dla państw członkowskich i zainteresowanych stron. W ostatnich latach ENISA stała się centrum informacyjnym, gromadzącym informacje z różnych źródeł. W tym sensie wiele zadań ENISA wiąże się z ponownym wykorzystaniem i recyklingiem informacji do celów różnych analiz. Na przykład: do niektórych celów ponowne wykorzystanie informacji zgłoszonych zgodnie z art. 23 i 30 dyrektywy (UE) 2022/2555; zgłoszonych, udostępnionych lub przeanalizowanych zgodnie z art. 14 ust. 1–3, art. 15 i art. 17 ust. 1 i 3 rozporządzenia (UE) 2024/2847. Przepisy dotyczące ram łańcucha dostaw zakładają, że ich wdrożenie będzie wspierane przez dane otrzymane na podstawie art. 22 dyrektywy (UE) 2022/2555, co wskazuje na ponowne wykorzystanie informacji i koordynację.

Wyjaśnij, w jaki sposób nowo utworzone dane są możliwe do znalezienia, dostępne, interoperacyjne i możliwe do ponownego wykorzystania oraz spełniają wysokie standardy jakości.

Wniosek ustawodawczy wyraźnie wskazuje, kiedy dane powinny być udostępniane publicznie. We wniosku uwzględniono charakter przepisów dotyczących wyłącznie kwestii bezpieczeństwa i poufności, dlatego nie wszystkie dane utworzone w ramach przeglądu CSA będą przeznaczone do publicznego użytku . W odniesieniu do niezbędnych przepisów zapewniono zgodność z europejskim cyfrowym portfelem tożsamości. ENISA ma za zadanie oferować usługę wczesnego ostrzegania w formacie nadającym się do odczytu maszynowego.

Przepływy danych

Ogólny opis danych objętych zakresem oraz wszelkich powiązanych norm/specyfikacji

Rodzaj danych	**Wyjaśnienie przepływu danych**	**Referencje**

ENISA dostarcza raporty i analizy, wytyczne techniczne i najlepsze praktyki.	Jest to przepływ danych skierowany do zainteresowanych stron ENISA, wspierający wdrażanie polityki i prawa UE. W ramach tych przepływów danych ENISA gromadzi informacje, najczęściej ze źródeł publicznych, dokonuje analizy i dzieli się wynikami z zainteresowanymi stronami. ENISA realizuje również określone zadania na wniosek Komisji.	Artykuł 5 ust. 1 lit. a), b), c), e), f) i h) Artykuł 5 ust. 2; art. 5 ust. 3; art. 5 ust. 5 Artykuł 6 Artykuł 7 Artykuł 8 Artykuł 9 Artykuł 10 Artykuł 11 ust. 2 Artykuł 11 ust. 4 Artykuł 14
Przepływ danych między Komisją, ENISA, państwami członkowskimi i innymi odpowiednimi podmiotami w ramach ekosystemu cyberbezpieczeństwa UE w ramach współpracy operacyjnej.	Tego rodzaju przepływ danych ma na celu współpracę operacyjną i zapewnienie świadomości sytuacyjnej. Wymiana informacji odbywa się w obu kierunkach, zarówno przychodzącym, jak i wychodzącym. Wymiana dotyczy danych operacyjnych.	Artykuł 10 ust. 4 lit. a)–g) Artykuł 11 ust. 1 lit. b)–g) Artykuł 11 ust. 2 lit. a) i b) Artykuł 11 ust. 3 Artykuł 15 Artykuł 16 ust. 2 lit. e)
Przepływy danych ustanowione w celu wsparcia ECSF i europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa oraz ich wdrażania	Przepływy danych wspierają wymianę danych w celu: - utrzymania i wdrażania ECSF, z przepływami między ENISA a członkami jej grupy roboczej ad hoc oraz między ENISA a Komisją; - opracowywania i utrzymywania europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, z przepływami między ENISA a członkami jej grupy roboczej ad hoc oraz między ENISA, Komisją i państwami członkowskimi; - wdrażania europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, z przepływami danych między wnioskodawcami a ENISA; - przepływ danych między komisją odwoławczą, ENISA, Komisją i wnioskodawcami.	Artykuły 19–23 Artykuły 36–43

Dane mające znaczenie dla celów, przeznaczenia i treści europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa	Ten rodzaj przepływu danych ma znaczenie dla planowania, wnioskowania, opracowywania, przyjmowania i utrzymywania (w tym ewentualnego przeglądu) europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa. Jest on w szczególności związany z zaangażowaniem i doradztwem ekspertów zainteresowanych stron, ENISA, organów państw członkowskich za pośrednictwem ECCG na różnych etapach procedury. Ponadto dodatkowy przepływ danych jest związany z dostarczaniem odpowiednich informacji ogółowi społeczeństwa za pośrednictwem specjalnych stron internetowych Komisji i ENISA. Wreszcie, ramy przewidują publiczną dostępność dodatkowych informacji dotyczących cyberbezpieczeństwa przez producentów lub dostawców produktów ICT, usług ICT lub procesów ICT, dla których wydano oświadczenie UE o zgodności lub europejski certyfikat cyberbezpieczeństwa z własnych środków.	Artykuł 18 Artykuł 19 Artykuły 72, 73, 74, 75, 76, 77, 79, 81, 83, 84
Dane związane z zarządzaniem europejskimi ramami certyfikacji w zakresie cyberbezpieczeństwa	Przepływy tych danych wspierają wymianę w celu: - koordynacji i zarządzania europejskimi systemami certyfikacji w zakresie cyberbezpieczeństwa - akredytacji i autoryzacji organów oceny zgodności, a także ich późniejszego powiadamiania za pośrednictwem odpowiedniej platformy i powiązanych procedur - procedur odwoławczych, takich jak prawo do złożenia skargi, środki odwoławcze lub odwołania oraz procedury zmian	Artykuły 85, 86, 88, 89, 90, 92, 93, 94, 95, 96

Przepływy danych związane z działalnością administracyjną Agencji	Przepływy między ENISA, zarządem, państwami członkowskimi, Komisją. Informacje dotyczą działalności administracyjnej Agencji w obu kierunkach. W niektórych przypadkach informacje są również przesyłane do Parlamentu Europejskiego (przepływ danych w tym zakresie przedstawiono poniżej).	Artykuł 25 Artykuł 28 ust. 1 Artykuł 30 Artykuł 31 ust. 8 Artykuł 32 ust. 3 i 5 Artykuł 35 ust. 5, 6 Artykuł 36–43 Artykuł 44 Artykuł 45
Dane przekazywane Parlamentowi Europejskiemu	Przekazywane Parlamentowi Europejskiemu informacje dotyczące działalności ENISA i wykonywania zadań; budżetu i zarządzania finansami, współpracy z państwami trzecimi i organizacjami międzynarodowymi, przesłuchania kandydata na dyrektora wykonawczego; kwestii związanych z europejską certyfikacją w zakresie cyberbezpieczeństwa	Artykuł 28 ust. 1 lit. f), art. 31 ust. 8, art. 32 ust. 3, art. 44 ust. 3, art. 49 ust. 6, art. 49 ust. 9, art. 70 ust. 5, art. 72 ust. 4 i 5, art. 119 ust. 3 Wykonywanie przekazanych uprawnień, art. 120 Ocena i przegląd
Dane przekazane Radzie UE	Przepływy informacji do Parlamentu Europejskiego dotyczące działalności ENISA i wykonywania zadań; budżet i zarządzanie finansami, współpraca z państwami trzecimi i organizacjami międzynarodowymi ( ), przesłuchanie kandydata na stanowisko dyrektora wykonawczego; programy kandydackie opracowywane zgodnie z europejskimi ramami certyfikacji w zakresie cyberbezpieczeństwa.	Artykuł 28 ust. 1 lit. f), art. 31 ust. 8, art. 32 ust. 3, art. 32 ust. 7, art. 49 ust. 6, art. 49 ust. 9, art. 70 ust. 5, art. 72 ust. 4, art. 72 ust. 5, art. 119 ust. 3 Wykonywanie przekazanych uprawnień, art. 120 Ocena i przegląd
Przepływ danych w związku ze złożeniem skargi	Rozpatrywanie skarg osób fizycznych lub prawnych dotyczących europejskich certyfikatów cyberbezpieczeństwa wydanych przez krajowe organy certyfikacji cyberbezpieczeństwa lub europejskich certyfikatów cyberbezpieczeństwa	Artykuł 55 ust. 3; art. 88 ust. 7 lit. f); art. 96

	wydanych przez organy oceny zgodności zgodnie z art. 84 ust. 4 lub dotyczących unijnych oświadczeń o zgodności Osoby fizyczne i prawne mają prawo złożyć skargę do wydawcy europejskiego certyfikatu cyberbezpieczeństwa lub, jeżeli skarga dotyczy europejskiego certyfikatu cyberbezpieczeństwa wydanego przez organ oceny zgodności	
Przepływ danych dotyczących ataków ransomware	Zgłaszanie określonych informacji w przypadku ataków z użyciem oprogramowania ransomware	Artykuł 1 pkt 8 dyrektywy

Rodzaj danych	**Odniesienia do wymogów**	**Podmioty dostarczające dane**	**Podmioty otrzymujące dane**	**Czynnik wyzwalający wymianę danych**	**Częstotliwość (jeśli dotyczy)**
Przepływ danych między Komisją a państwami członkowskimi w kontekście przeprowadzania skoordynowanych ocen ryzyka bezpieczeństwa na szczeblu unijnym.	Artykuł 99 Oceny ryzyka bezpieczeństwa	Komisja i państwa członkowskie	Państwa członkowskie (grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji)	Artykuł 99 Oceny ryzyka bezpieczeństwa	Nie dotyczy
Przepływ danych między Komisją a Radą w związku z wyznaczeniem państw trzecich budzących obawy w zakresie cyberbezpieczeństwa	Artykuł 100 Wyznaczenie państw trzecich budzących obawy w zakresie cyberbezpieczeństwa	Komisja	Rada	Artykuł 100 Weryfikacja przez Komisję zagrożenia stwarzanego przez państwo trzecie	

Rodzaj danych	**Odniesienia do wymogów**	**Podmioty dostarczające dane**	**Podmioty otrzymujące dane**	**Czynnik wyzwalający wymianę danych**	**Częstotliwość (jeśli dotyczy)**
Przepływ danych między Komisją a państwami członkowskimi w odniesieniu do środków łagodzących w wyjątkowych okolicznościach	Artykuł 103 ust. 6 Środki łagodzące w łańcuchach dostaw ICT	Komisja	Państwa członkowskie	Wyjątkowe okoliczności	Nie dotyczy
Przepływ danych między Komisją a dostawcami oraz między Komisją a właściwymi organami w zakresie oceny zakładów oraz własności i kontroli dostawców	104 (4), (5), (6) Identyfikacja dostawców wysokiego ryzyka	Dostawcy Komisja Właściwe organy	Właściwe organy Dostawcy Komisja	Akty wykonawcze przyjęte zgodnie z art. 103 ust. 1 oraz w odniesieniu do zakazu określonego w art. 111 ust. 1	Nie dotyczy
Przepływ danych między Komisją a państwami członkowskimi w odniesieniu do uprawnień nadzorczych związanych z wdrażaniem ram bezpieczeństwa zaufanego łańcucha dostaw ICT	Artykuł 112 ust. 1 i 4 Właściwe organy Artykuł 114 Środki nadzorcze i egzekucyjne	Państwa członkowskie	Komisja	Artykuł 112 ust. 1 i 4 Właściwe organy Artykuł 114 Środki nadzorcze i egzekucyjne (Komisja we współpracy z państwami członkowskimi publikuje wykaz podmiotów powiązanych z	Nie dotyczy

Rodzaj danych	Odniesienia do wymogów	Podmioty dostarczające dane	Podmioty otrzymujące dane	Czynnik wyzwalający wymianę danych	Częstotliwość (jeśli dotyczy)
				dostawcami wysokiego ryzyka).	
Przepływ danych między Komisją a stronami trzecimi w zakresie zwolnień	Artykuł 105 Zwolnienie podmiotów mających siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowanych z takiego państwa	Strony trzecie (podmioty mające siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowane przez takie podmioty (w rozumieniu art. 100) (przy składaniu wniosku o zwolnienie) Komisja Europejska (przy wydawaniu decyzji)	Komisja (przy przyjmowaniu wniosku o zwolnienie) Strony trzecie (podmioty mające siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa (w rozumieniu art. 100) lub kontrolowane przez takie podmioty (przy otrzymywaniu decyzji Komisji w sprawie)	Decyzja na mocy art. 100 Wyznaczenie państw trzecich budzących obawy w zakresie cyberbezpieczeństwa	Nie dotyczy
Przepływ danych między państwami członkowskimi a stronami trzecimi w związku z zakazami w sieciach łączności elektronicznej	Artykuł 111 Zakazy dotyczące mobilnych, stacjonarnych i satelitarnych sieci	Państwa członkowskie (właściwe organy)	Strony trzecie (dostawcy sieci łączności elektronicznej ruchomej,	Właściwy organ wyznaczony na mocy niniejszego rozporządzenia niezwłocznie	Nie dotyczy

Rodzaj danych	Odniesienia do wymogów	Podmioty dostarczające dane	Podmioty otrzymujące dane	Czynnik wyzwalający wymianę danych	Częstotliwość (jeśli dotyczy)
	łączności elektronicznej		stacjonarnej i satelitarnej)	informuje właściwy organ zgodnie z rozporządzeniem (UE) XX/XXXX [wniosek DNA] o środkach nałożonych na dostawców sieci łączności elektronicznej ruchomej, stacjonarnej i satelitarnej.	
Przepływ danych między Komisją a państwami członkowskimi w kontekście sieci współpracy i usług wsparcia	Artykuł 113 Sieć współpracy i usług wsparcia Komisji	Komisja Państwa członkowskie (właściwe organy)	Komisja Państwa członkowskie (właściwe organy)	Wyznaczenie państw trzecich budzących obawy w zakresie cyberbezpieczeństwa	
Przepływ danych między państwami członkowskimi a stronami trzecimi w związku ze środkami nadzoru i egzekwowania	Artykuł 114 Środki nadzorcze i egzekucyjne	Strony trzecie (podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555)	Państwa członkowskie (właściwe organy)	Wdrożenie środków przewidzianych w tytule IV	

Rodzaj danych	Odniesienia do wymogów	Podmioty dostarczające dane	Podmioty otrzymujące dane	Czynnik wyzwalający wymianę danych	Częstotliwość (jeśli dotyczy)
Przepływ danych między państwami członkowskimi w ramach wzajemnej pomocy	Artykuł 116 Wzajemna pomoc	Państwa członkowskie	Państwa członkowskie	W przypadku gdy podmiot, o którym mowa w załączniku I lub II do dyrektywy (UE) 2022/2555, świadczy usługi w więcej niż jednym państwie członkowskim lub świadczy usługi w jednym lub kilku państwach członkowskich, a jego kluczowe aktywa ICT znajdują się w jednym lub kilku innych państwach członkowskich, właściwe organy zainteresowanych państw członkowskich współpracują ze sobą i w razie potrzeby udzielają	Nie dotyczy

Rodzaj danych	Odniesienia do wymogów	Podmioty dostarczające dane	Podmioty otrzymujące dane	Czynnik wyzwalający wymianę danych	Częstotliwość (jeśli dotyczy)
				sobie wzajemnej pomocy.	

4.3. Rozwiązania cyfrowe

Ogólny opis rozwiązań cyfrowych

W odniesieniu do każdego rozwiązania cyfrowego wyjaśnienie, w jaki sposób rozwiązanie cyfrowe jest zgodne z obowiązującymi politykami cyfrowymi i aktami prawnymi

Rozwiązanie cyfrowe	Odniesienia do wymagań	Główne wymagane funkcje	Organ odpowiedzialny	W jaki sposób zapewniono dostępność?	W jaki sposób uwzględniono możliwość ponownego wykorzystania?	Wykorzystanie technologii sztucznej inteligencji (jeśli dotyczy)
ENISA pełni funkcję **sekretariatu sieci CSIRT i EU-CyCLONe** oraz wdraża w ramach sieci CSIRT i EU-CyCLONe **bezpieczne narzędzia komunikacyjne** dostarczane przez podmioty prawne, które nie mają siedziby w państwach trzecich ani nie są kontrolowane przez państwa trzecie lub obywateli państw trzecich.	Artykuł 10 ust. 2, 3 i 5	Informacje niepubliczne	ENISA	Informacja niepubliczna	Informacje niepubliczne	Informacja niepubliczna
Opracowanie we współpracy z EU-CyCLONe, siecią CSIRT, Komisją, Europolem i CERT-EU oraz odpowiednimi podmiotami	Artykuł 11 ust. 1 lit. a)	zweryfikowane, wiarygodne informacje wywiadowcze dotyczące	ENISA EU-CyCLONe, sieć CSIRT, Komisja, Europol	Nie dotyczy	N/A	N/A

unijnymi **repozytoriów zweryfikowanych, wiarygodnych informacji wywiadowczych dotyczących cyberzagrożeń**, w tym trendów w zakresie incydentów, taktyk, technik i procedur.		cyberzagrożeń, w tym trendy w zakresie incydentów, taktyk, technik i procedur	i CERT-EU oraz odpowiednie podmioty unijne			
ENISA **prowadzi rejestr zdobytych doświadczeń.**	Artykuł 14 ust. 2	ENISA prowadzi zbiór wniosków wyciągniętych z ćwiczeń i zaleca państwom członkowskim oraz, w stosownych przypadkach, podmiotom unijnym, jak skutecznie i efektywnie wdrażać wyciągnięte wnioski.	ENISA	Nie dotyczy	N/A	Nie dotyczy
ENISA ustanawia, zapewnia, obsługuje, utrzymuje i aktualizuje w razie potrzeby operacyjne narzędzia techniczne, takie jak **platformy** związane z cyberbezpieczeństwem na poziomie Unii, w szczególności jednolitą platformę zgłaszania incydentów ustanowioną zgodnie z art. 16 ust. 1 rozporządzenia (UE) 2024/2847 [oraz jednolitego punktu zgłoszeniowego incydentów ustanowionego zgodnie z art. 23a dyrektywy (UE) 2022/2555], lub narzędzi testowych wspierających wdrażanie procedur oceny zgodności zgodnie z odpowiednim prawodawstwem Unii.	Artykuł 15	Jednolita platforma sprawozdawcza Artykuł 16 ust. 1 rozporządzenia (UE) 2024/2847 [jedyny punkt kontaktowy Artykuł 23a dyrektywy (UE) 2022/2555]	ENISA	Nie dotyczy	Nie dotyczy	Nie dotyczy

Prowadzenie europejskiej bazy danych dotyczących podatności ustanowionej zgodnie z art. 12 ust. 2 dyrektywy (UE) 2022/2555 oraz **świadczenie usług w zakresie zarządzania podatnością.**	Artykuł 16 ust. 2	Artykuł 12 ust. 2 dyrektywy (UE) 2022/2555 Prowadzenie bazy danych i świadczenie usług w zakresie zarządzania podatnością na zagrożenia	ENISA	Nie dotyczy	Nie dotyczy	Nie dotyczy
ENISA prowadzi i regularnie aktualizuje specjalną stronę internetową zawierającą informacje publiczne.	Artykuł 19–23	Utrzymywanie i regularna aktualizacja specjalnej strony internetowej zawierającej informacje publiczne na temat ECSF, w tym ramy i harmonogram aktualizacji; europejskie systemy certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa, postępy w ich opracowywaniu i harmonogramy ich rozwoju; opłaty związane z każdym europejskim systemem certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa;	ENISA	Nie dotyczy	N/A	Nie dotyczy

		orientacyjny koszt europejskiej certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa; wykaz uprawnionych podmiotów certyfikujących.				
Komisja prowadzi i regularnie aktualizuje specjalną publiczną stronę internetową	Artykuł 72	Następujące informacje: a) europejskie systemy certyfikacji cyberbezpieczeństwa, o których opracowanie zwrócono się; b) priorytety strategiczne w zakresie harmonizacji produktów ICT , usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub wymogów bezpieczeństwa określonych w przepisach unijnych, w tym potencjalne obszary, w których można by zażądać opracowania europejskiego systemu certyfikacji cyberbezpieczeństwa.	Komisja Europejska	Zgodność z wytycznymi	Zgodność z wytycznymi	Nie dotyczy

ENISA prowadzi specjalną stronę internetową poświęconą certyfikacji.	Artykuł 79	Dostarczanie informacji na temat: a) europejskich systemach certyfikacji w zakresie cyberbezpieczeństwa; b) opłatach związanych z utrzymaniem każdego europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa; c) odpowiednich specyfikacji technicznych ENISA; d) europejskich certyfikatach cyberbezpieczeństwa i unijnych oświadczeniach o zgodności, w tym informacje dotyczące certyfikatów i oświadczeń, które straciły ważność, zostały zawieszone, cofnięte lub wygasły; e) odpowiednich dodatkowych informacji dotyczących cyberbezpieczeństwa	ENISA	Zgodność z wytycznymi	Zgodność z wytycznymi	Nie dotyczy

		przekazanych zgodnie z art. 84 ust. 2; f) podsumowania wzajemnych ocen zgodnie z art. 89 ust. 7; g) specyfikacje techniczne, do których odwołuje się europejski system certyfikacji w zakresie cyberbezpieczeństwa zgodnie z art. 74 ust. 10.				
Rejestr (zwolnień dla podmiotów mających siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowanych przez takie podmioty)	Artykuł 107 Rejestr	Komisja prowadzi publicznie dostępny rejestr swoich decyzji, o których mowa w art. 105 ust. 4. W rejestrze tym podaje się nazwy podmiotów, których dotyczą decyzje. Komisja regularnie aktualizuje ten rejestr.	Komisja	„Komisja prowadzi publicznie dostępny rejestr”	Nie dotyczy	Nie dotyczy

Platforma (do współpracy i wymiany informacji między Komisją a właściwymi organami)	Artykuł 113	Komisja ustanawia sieć współpracy właściwych organów państw członkowskich i Komisji, która służy jako platforma współpracy i wymiany informacji. Komisja zapewnia wsparcie administracyjne dla sieci.	Komisja	Niepubliczna, tylko dla właściwych organów	Nie dotyczy	Nie dotyczy
ENISA utworzy i będzie prowadzić rejestr podmiotów o znaczeniu podstawowym i istotnym, a także podmiotów świadczących usługi rejestracji nazw domen.	Artykuł 1 pkt 11 dyrektywy	Rejestr podmiotów o znaczeniu kluczowym i istotnym, a także podmiotów świadczących usługi rejestracji nazw domen	ENISA	Nie dotyczy	Na podstawie informacji otrzymanych od pojedynczych punktów kontaktowych zgodnie z ust. 2. (Artykuł 27 dyrektywy NIS2)	Nie dotyczy

Rozwiązania cyfrowe uwzględnione w powyższej tabeli

Polityka cyfrowa i/lub sektorowa (jeśli ma zastosowanie)	**Wyjaśnienie dotyczące sposobu dostosowania**
Ustawa o sztucznej inteligencji	Nie dotyczy

Ramy UE dotyczące cyberbezpieczeństwa	Nie dotyczy
eIDAS	Nie dotyczy
Jednolita brama cyfrowa i IMI	Nie dotyczy
Inne	Nie dotyczy

Ogólny opis usług publicznych świadczonych drogą elektroniczną, których dotyczą wymagania

Cyfrowa usługa publiczna lub kategoria cyfrowych usług publicznych	**Opis**	**Odniesienia do wymogów**	**Rozwiązania interoperacyjnej Europy (NIE DOTYCZY)**	**Inne rozwiązania w zakresie interoperacyjności**
ENISA jako sekretariat sieci i wdrażanie bezpiecznych narzędzi komunikacyjnych	ENISA pełni funkcję sekretariatu sieci CSIRT zgodnie z art. 15 ust. 2 dyrektywy (UE) 2022/2555. ENISA pełni funkcję sekretariatu EU-CyCLONe zgodnie z art. 16 ust. 2 dyrektywy (UE) 2022/2555 [oraz pojedynczego punktu kontaktowego do zgłaszania incydentów ustanowionego zgodnie z art. 23a dyrektywy (UE) 2022/2555] oraz narzędzi testowych wspierających wdrażanie procedur oceny zgodności zgodnie z odpowiednim prawodawstwem unijnym. ENISA wdraża w ramach sieci CSIRT i EU-CyCLONe bezpieczne narzędzia komunikacyjne dostarczane przez podmioty prawne z , które nie mają siedziby w państwach trzecich ani nie	Artykuł 11	//	Nie dotyczy

	są kontrolowane przez państwa trzecie lub obywateli państw trzecich.			
Wczesne ostrzeganie	Wydawanie wczesnych ostrzeżeń	Artykuł 11 Artykuł 12		
Wsparcie w związku z konkretnym potencjalnym lub trwającym incydentem lub cyberzagrożeniem	Na wniosek jednego lub kilku państw członkowskich udzielanie porad i ocen w odniesieniu do konkretnego potencjalnego lub trwającego incydentu lub cyberzagrożenia, w tym poprzez zapewnienie wiedzy fachowej i ułatwianie technicznego postępowania w przypadku takich incydentów oraz poprzez wspieranie dobrowolnej wymiany odpowiednich informacji i rozwiązań technicznych między państwami członkowskimi;	Artykuł 10		
Wspieranie skoordynowanego zarządzania incydentami i kryzysami związanymi z cyberbezpieczeństwem na dużą skalę na poziomie operacyjnym	Przyczynianie się do wspierania skoordynowanego zarządzania incydentami i kryzysami związanymi z cyberbezpieczeństwem na dużą skalę na poziomie operacyjnym, w szczególności poprzez pomoc EU-CyCLONe w przygotowywaniu sprawozdań dla szczebla politycznego poprzez ułatwianie i ułatwianie terminowej wymiany informacji między siecią CSIRT a EU-CyCLONe.	Artykuł 10		
Repozytoria zweryfikowanych, wiarygodnych informacji wywiadowczych dotyczących cyberzagrożeń	We współpracy z EU-CyCLONe, siecią CSIRT, Komisją, Europolem i CERT-EU oraz odpowiednimi podmiotami unijnymi opracowuje repozytoria zweryfikowanych, wiarygodnych informacji o cyberzagrożeniach, w tym o trendach w zakresie incydentów, taktyk, technik i procedur.	Artykuł 11		

Repozytorium wniosków	ENISA prowadzi zbiór wniosków wyciągniętych z tych ćwiczeń i zaleca państwom członkowskim oraz, w stosownych przypadkach, podmiotom unijnym, jak skutecznie i efektywnie wdrożyć wyciągnięte wnioski.	Artykuł 14		
ENISA ustanawia, udostępnia, obsługuje, utrzymuje i w razie potrzeby aktualizuje operacyjne narzędzia techniczne, takie jak platformy	ENISA ustanawia, udostępnia, obsługuje, utrzymuje i w razie potrzeby aktualizuje operacyjne narzędzia techniczne, takie jak platformy związane z cyberbezpieczeństwem na poziomie Unii, w szczególności jednolitą platformę zgłaszania incydentów ustanowioną zgodnie z art. 16 ust. 1 rozporządzenia (UE) 2024/2847 [oraz jednolitego punktu zgłoszeniowego incydentów ustanowionego zgodnie z art. 23a dyrektywy (UE) 2022/2555] oraz narzędzia testowe wspierające wdrażanie procedur oceny zgodności zgodnie z odpowiednim prawodawstwem Unii.	Artykuł 15		
Utrzymanie europejskiej bazy danych o podatnościach ustanowionej zgodnie z art. 12 ust. 2 dyrektywy (UE) 2022/2555 ( ).	Prowadzenie europejskiej bazy danych podatności ustanowionej zgodnie z art. 12 ust. 2 dyrektywy (UE) 2022/2555. Świadczenie usług w zakresie zarządzania podatnością na zagrożenia na rzecz zainteresowanych stron w oparciu o europejską bazę danych podatności na zagrożenia i z wykorzystaniem odpowiednich informacji dostępnych dla ENISA. Nawiązanie zorganizowanej współpracy z organizacjami zapewniającymi programy, rejestry lub bazy danych podobne do europejskiej	Artykuł 16		

	bazy danych dotyczących luk w zabezpieczeniach. Aktywne wspieranie zespołów CSIRT wyznaczonych jako koordynatorzy zgodnie z art. 12 ust. 1 dyrektywy (UE) 2022/2555 w zakresie zarządzania skoordynowanym ujawnianiem luk w zabezpieczeniach, które mogą mieć znaczący wpływ na podmioty w więcej niż jednym państwie członkowskim. Opracowywanie i utrzymywanie metodologii i mechanizmów zarządzania służących identyfikacji luk w zabezpieczeniach i skoordynowanemu ujawnianiu informacji, we współpracy z właściwymi organami krajowymi, zespołami CSIRT, przemysłem i środowiskiem badawczym.			
Przygotowanie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa „systemy kandydujące”	Przygotowanie europejskich systemów certyfikacji cyberbezpieczeństwa będących w fazie przygotowawczej („systemy w fazie przygotowawczej”) dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów oraz związanych z nimi specyfikacji technicznych zgodnie z art. 74. Utrzymywanie przyjętych europejskich systemów certyfikacji cyberbezpieczeństwa zgodnie z art. 75, w tym z uwzględnieniem ewentualnego przeglądu przyjętych europejskich systemów certyfikacji cyberbezpieczeństwa zgodnie z art. 76.	Artykuł 17		

ENISA opracowuje i utrzymuje europejskie systemy poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa.	ENISA opracowuje i utrzymuje europejskie systemy certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa. ENISA wydaje uzasadnioną decyzję o udzieleniu wnioskodawcy upoważnienia do wydawania europejskich indywidualnych certyfikatów w celu wdrożenia i utrzymania systemów oraz upoważnienia, o nieudzielaniu upoważnienia lub o zamknięciu postępowania w sprawie wniosku z powodu niewystarczających informacji dostarczonych przez wnioskodawcę lub jego braku działania po wezwaniu do dostarczenia dodatkowych informacji.	Artykuły 20–22		
ENISA prowadzi i regularnie aktualizuje specjalną stronę internetową.	ENISA prowadzi i regularnie aktualizuje specjalną stronę internetową zawierającą informacje publiczne dotyczące: a) ECSF, w tym ramy i harmonogram aktualizacji; b) europejskich systemów poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa, postępów w ich opracowywaniu oraz harmonogramu ich rozwoju; c) opłaty związane z każdym europejskim systemem poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa przyjętym zgodnie z art. 47 niniejszego rozporządzenia;	Artykuł 23		

	d) orientacyjny koszt europejskiego certyfikatu indywidualnych umiejętności w zakresie cyberbezpieczeństwa zgodnie z art. 20 ust. 4; e) wykaz uprawnionych podmiotów certyfikujących.			
Komisja prowadzi i regularnie aktualizuje specjalną publiczną stronę internetową	Komisja prowadzi i regularnie aktualizuje specjalną stronę internetową zawierającą informacje na temat następujących aspektów: a) europejskich systemów certyfikacji cyberbezpieczeństwa, o których opracowanie zwrócono się; b) strategiczne priorytety w zakresie harmonizacji produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub wymogów bezpieczeństwa określonych w przepisach unijnych, w tym potencjalne obszary, w których można by wnioskować o europejski system certyfikacji w zakresie cyberbezpieczeństwa.	Artykuł 72		
ENISA prowadzi specjalną stronę internetową poświęconą certyfikacji	ENISA prowadzi i regularnie aktualizuje specjalną stronę internetową zawierającą informacje publiczne na temat: a) europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa; b) opłaty związane z utrzymaniem każdego europejskiego systemu certyfikacji w zakresie cyberbezpieczeństwa; c) odpowiednie specyfikacje techniczne ENISA; d) europejskie certyfikaty cyberbezpieczeństwa i unijne	Artykuł 79		

	deklaracje zgodności, w tym informacje dotyczące certyfikatów i deklaracji, które straciły ważność, zostały zawieszone, cofnięte lub wygasły; e) odpowiednie uzupełniające informacje dotyczące cyberbezpieczeństwa przekazane zgodnie z art. 84 ust. 2; f) podsumowania wzajemnych ocen zgodnie z art. 89 ust. 7; g) specyfikacje techniczne, do których odwołuje się europejski system certyfikacji w zakresie cyberbezpieczeństwa zgodnie z art. 74 ust. 10.			
Dochodzenia	Komisja prowadzi dochodzenia w sprawach, w których ma wątpliwości lub w których powiadomiono ją o wątpliwościach dotyczących kompetencji jednostki oceniającej zgodność w zakresie spełnienia lub dalszego spełniania przez tę jednostkę wymogów i obowiązków, którym podlega. Komisja zapewnia poufność wszystkich informacji wrażliwych uzyskanych w trakcie dochodzeń.	Artykuł 94		
ENISA tworzy i prowadzi rejestr podmiotów o znaczeniu podstawowym i istotnym, a także podmiotów świadczących usługi rejestracji nazw domen	Rejestr podmiotów o znaczeniu kluczowym i istotnym, a także podmiotów świadczących usługi rejestracji nazw domen. Na wniosek ENISA umożliwia właściwym organom dostęp do informacji dotyczących dostawców usług DNS, rejestrów nazw TLD, podmiotów świadczących usługi rejestracji nazw domen, dostawców	Artykuł 1 pkt 11 dyrektywy		

	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 serwisów społecznościowych, przechowywanych w tym rejestrze, zapewniając jednocześnie ochronę poufności informacji, w stosownych przypadkach.			

4.4. Ocena interoperacyjności

Wpływ wymogów dotyczących cyfrowych usług publicznych na interoperacyjność transgraniczną

Repozytoria/platformy/wczesne ostrzeganie/sekretariat/współpraca operacyjna/baza danych CVD

Ocena	Środki	Potencjalne pozostałe bariery
Ocena zgodności z istniejącymi politykami cyfrowymi i sektorowymi **Proszę wymienić odpowiednie zidentyfikowane polityki cyfrowe i sektorowe**	*Cyberbezpieczeństwo*	*Brak znanych barier*
Ocena środków organizacyjnych zapewniających sprawne świadczenie transgranicznych usług publicznych w dziedzinie cyfrowej **Proszę wymienić przewidziane środki zarządzania**	*Zarząd ENISA* *Sieć CSIRT* *EU-CyCLONe* *Grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji*	*Nie dotyczy*

	Wszystkie te fora służą do zgłaszania problemów.	
Ocena środków podjętych w celu zapewnienia wspólnego zrozumienia danych **Proszę wymienić takie środki**	*Nie dotyczy*	*Nie dotyczy*
Ocenić stosowanie powszechnie uzgodnionych otwartych specyfikacji technicznych i norm **Proszę wymienić takie środki**	*Nie dotyczy*	*Nie dotyczy*

Europejskie systemy certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa

Ocena	Środki	Potencjalne pozostałe bariery
Ocena zgodności z istniejącymi politykami cyfrowymi i sektorowymi **Proszę wymienić odpowiednie polityki cyfrowe i sektorowe**	*Wniosek opiera się na COM(2023)207 final (Akademia Umiejętności w zakresie Cyberbezpieczeństwa) „ENISA opracuje projekt pilotażowy, badający możliwość ustanowienia europejskiego systemu poświadczania umiejętności w zakresie cyberbezpieczeństwa”.* *Wykorzystuje rozporządzenie (UE) 2024/1183 (portfel EUDI), ustanawiając, że „ENISA i upoważnieni dostawcy certyfikatów zapewniają, aby elektroniczne certyfikaty europejskiego indywidualnego certyfikatu umiejętności w zakresie cyberbezpieczeństwa były wydawane do europejskich portfeli tożsamości cyfrowej”.* *Cyberbezpieczeństwo* *RODO (przechowywanie dokumentacji przez dostawców)*	*Brak znanych przeszkód*

Ocena środków organizacyjnych zapewniających sprawne świadczenie transgranicznych usług publicznych w formie cyfrowej **Proszę wymienić przewidywane środki zarządzania**	*Konsultacje z zainteresowanymi stronami podczas przygotowywania europejskiego systemu poświadczania indywidualnych umiejętności w zakresie cyberbezpieczeństwa* *Rozdzielenie działań w ramach ENISA w celu zapewnienia ich niezależności* *Komisja odwoławcza*	*Korzystanie z europejskich systemów certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa i uznawanie tych systemów pozostaje dobrowolne dla podmiotów publicznych i prywatnych.*
Ocena środków podjętych w celu zapewnienia wspólnego rozumienia danych **Proszę wymienić takie środki.**	*Opracowanie systemów określających między innymi zasady dotyczące treści i formatu certyfikatów* *Upoważnieni dostawcy zapewniają, aby na wniosek osoby fizycznej europejskie certyfikaty indywidualnych umiejętności w zakresie cyberbezpieczeństwa były wydawane jako elektroniczne certyfikaty atrybutów w formacie, który można przechowywać w europejskich portfelach tożsamości cyfrowej ENISA zapewnia wytyczne dla oceniających i przeprowadza obowiązkowe szkolenia dla nich w zakresie wymagań i metod oceny zawartych w europejskim systemie certyfikacji indywidualnych umiejętności w zakresie cyberbezpieczeństwa* *Udostępnianie informacji publicznych na stronie internetowej* *Akty wykonawcze dotyczące opłat*	*Chociaż systemy powinny być na tyle szczegółowe, aby zapewnić wspólne zrozumienie i ułatwić wdrożenie, a ENISA będzie udzielać wskazówek i przeprowadzać obowiązkowe szkolenia dla oceniających w celu zapewnienia spójnego wdrożenia systemów, mogą pojawić się nieprzewidziane sytuacje, w których uprawnieni dostawcy zaświadczeń będą musieli współpracować z ENISA, innymi dostawcami lub oceniającymi.*
Ocena stosowania wspólnie uzgodnionych otwartych specyfikacji technicznych i norm **Proszę wymienić takie środki.**	*Europejskie indywidualne systemy poświadczania umiejętności w zakresie cyberbezpieczeństwa są opracowywane przy wsparciu odpowiednich zainteresowanych stron*	*Nie dotyczy*

Przygotowanie europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa „systemy kandydujące”/przypisanie numerów organom certyfikacji zgodności

Ocena	Środki	Potencjalne pozostałe bariery
Ocena zgodności z istniejącymi politykami cyfrowymi i sektorowymi **Proszę wymienić odpowiednie polityki cyfrowe i sektorowe**	*Wniosek ma na celu dostosowanie zarządzania do nowych ram prawnych, w szczególności w odniesieniu do rozporządzenia (WE) nr 765/2008*[26]*.* *Wniosek ma na celu ułatwienie zgodności z odpowiednimi przepisami sektorowymi w zakresie cyberbezpieczeństwa poprzez opracowanie specjalnych europejskich systemów certyfikacji cyberbezpieczeństwa.*	*Brak znanych barier*
Ocena środków organizacyjnych zapewniających sprawne świadczenie transgranicznych usług publicznych w dziedzinie cyfrowej **Proszę wymienić przewidziane środki zarządzania**	*Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa;* *ENISA;* *Grupy robocze ad hoc;* *Europejskie Zgromadzenie ds. Certyfikacji Cyberbezpieczeństwa;* *Konsultacje z zainteresowanymi stronami przy składaniu wniosków, opracowywaniu i przyjmowaniu europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa;* *Procedury komitologii dotyczące planowanych aktów wykonawczych związanych z europejskimi systemami certyfikacji cyberbezpieczeństwa.*	*Stosowanie europejskiej certyfikacji w zakresie cyberbezpieczeństwa jest dobrowolne, chyba że przepisy europejskie stanowią inaczej.*
Ocena środków podjętych w celu zapewnienia wspólnego rozumienia danych **Proszę wymienić takie środki**	*Akty wykonawcze wymienione w sekcji 4.5.*	*Stosowanie europejskiej certyfikacji w zakresie cyberbezpieczeństwa jest dobrowolne, chyba że przepisy europejskie stanowią inaczej.*

Ocena stosowania wspólnie uzgodnionych otwartych specyfikacji technicznych i norm **Proszę wymienić takie środki**	*Akty wykonawcze wymienione w sekcji 4.5. Określone wymagania europejskiego systemu certyfikacji cyberbezpieczeństwa powinny być zgodne z wymogami prawodawstwa unijnego. Europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa wykorzystują i odwołują się do międzynarodowych, europejskich lub krajowych norm stosowanych w ocenie lub, w przypadku gdy takie normy nie są dostępne lub nie są odpowiednie, do specyfikacji technicznych opracowanych przez ENISA.*	*Nie dotyczy*

Publicznie dostępne strony internetowe

Ocena	Środki	Potencjalne pozostałe bariery
Ocena zgodności z istniejącymi politykami cyfrowymi i sektorowymi **Proszę wymienić odpowiednie polityki cyfrowe i sektorowe**	*Ustawa UE o dostępności i dyrektywa w sprawie dostępności stron internetowych* *Cyberbezpieczeństwo*	*Brak znanych barier*
Ocena środków organizacyjnych zapewniających sprawne świadczenie transgranicznych usług publicznych w formie cyfrowej **Proszę wymienić przewidywane środki zarządzania**	*Nie dotyczy*	*Nie dotyczy*
Ocena środków podjętych w celu zapewnienia wspólnego zrozumienia danych **Proszę wymienić takie środki**		*Nie dotyczy*
Ocena stosowania wspólnie uzgodnionych otwartych specyfikacji technicznych i norm **Proszę wymienić takie środki**		*Nie dotyczy*

4.5. Środki wspierające wdrażanie technologii cyfrowych

Ogólny opis środków wspierających wdrażanie technologii cyfrowych

Opis środka	**Odniesienia do wymogów**	**Rola Komisji** (jeśli dotyczy)	**Podmioty, które mają być zaangażowane** (jeśli dotyczy)	**Przewidywany harmonogram** (jeśli dotyczy)
Komisja, na podstawie przyjętego programu kandydackiego przygotowanego przez ENISA, jest uprawniona do przyjęcia aktów wykonawczych przewidujących europejski system certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa lub cyberbezpieczeństwa podmiotów, który spełnia wymogi określone w art. 80 i 81. Akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.	Artykuł 75 ust. 9	Komisja jest uprawniona do przyjmowania aktów wykonawczych		Nie dotyczy
Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 119 w celu zmiany ust. 1 niniejszego artykułu poprzez dodanie lub zmianę celów bezpieczeństwa, aby zapewnić, że odzwierciedlają one najnowszy rozwój technologiczny i nowe związane z nim zagrożenia, a także przyjęcie nowych przepisów unijnych ustanawiających domniemanie zgodności poprzez europejską	Artykuł 80 ust. 2	Komisja jest uprawniona do przyjmowania aktów delegowanych		Nie dotyczy

certyfikację w zakresie cyberbezpieczeństwa z odpowiednimi wymogami w zakresie cyberbezpieczeństwa określonymi w tych przepisach.				
Komisja jest uprawniona do przyjmowania aktów wykonawczych ustanawiających wspólne zasady i wzorcowe przepisy dotyczące elementów określonych w ust. 1, 2 i 3 w europejskich systemach certyfikacji w zakresie cyberbezpieczeństwa. W stosownych przypadkach i o ile jest to możliwe, europejski system certyfikacji w zakresie cyberbezpieczeństwa może zawierać odniesienia do tych zasad i wzorcowych przepisów. Akty wykonawcze, o których mowa w akapicie pierwszym, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2. Przy opracowywaniu lub zmianie wspólnych zasad i wzorcowych przepisów dotyczących elementów europejskich systemów certyfikacji w zakresie cyberbezpieczeństwa Komisja konsultuje się z ENISA i uwzględnia, w stosownych przypadkach, opinie wyrażone przez ECCG, zainteresowane strony i inne właściwe organy.	Artykuł 81 ust. 5	Komisja jest uprawniona do przyjmowania aktów wykonawczych	ENISA ECCG	Nie dotyczy
Komisja jest uprawniona do przyjmowania aktów wykonawczych określających procedury uprzedniego zatwierdzania lub modele ogólnego przekazywania	Artykuł 85 ust. 5	Komisja jest uprawniona do przyjmowania	ECCG	Nie dotyczy

uprawnień, o których mowa w ust. 4 niniejszego artykułu. W trakcie przygotowywania tych aktów wykonawczych Komisja konsultuje się z ECCG. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.		aktów wykonawczych		
Certyfikaty państw trzecich dotyczące produktów ICT, usług ICT, procesów ICT, zarządzanych usług bezpieczeństwa i cyberbezpieczeństwa podmiotów mogą zostać uznane, w drodze aktu wykonawczego lub poprzez zawarcie umowy między Unią a danym państwem trzecim lub organizacją międzynarodową, za równoważne z europejskimi certyfikatami cyberbezpieczeństwa, jeżeli wymogi odpowiedniego systemu państwa trzeciego lub organizacji międzynarodowej uznaje się za równoważne z wymogami europejskich systemów certyfikacji cyberbezpieczeństwa. Komisja jest uprawniona do przyjmowania takich aktów wykonawczych. Akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.	Artykuł 87 ust. 1	Komisja jest uprawniona do przyjmowania aktów wykonawczych		Nie dotyczy
Komisja jest uprawniona do przyjmowania aktów wykonawczych ustanawiających plan wzajemnej oceny obejmujący okres co najmniej pięciu lat, określający kryteria	Artykuł 89 ust. 6	Komisja jest uprawniona do przyjmowania		Nie dotyczy

dotyczące składu zespołu ds. wzajemnej oceny, metodologię stosowaną w ramach wzajemnej oceny oraz harmonogram, częstotliwość i inne zadania związane z wzajemną oceną. Przygotowując te akty wykonawcze, Komisja konsultuje się z ECCG i ENISA. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.		aktów wykonawczych		
Komisja jest uprawniona do przyjmowania aktów wykonawczych w celu ustanowienia procedur, w tym dotyczących współpracy transgranicznej, w zakresie udzielania upoważnień organom oceny zgodności. W procesie przygotowywania aktów wykonawczych Komisja konsultuje się z ENISA i ECCG. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.	Artykuł 92 ust. 8	Komisja jest uprawniona do przyjmowania aktów wykonawczych	ENISA ECCG	Nie dotyczy
Komisja jest uprawniona do przyjmowania aktów wykonawczych w celu określenia okoliczności, formatów i procedur dotyczących powiadomień, o których mowa w ust. 1 niniejszego artykułu, w tym procedury zgłaszania sprzeciwu przez inne państwa członkowskie w trakcie procesu powiadamiania, jednolitego identyfikowania organów oceny zgodności, a także okoliczności ograniczenia,	Artykuł 93 ust. 3	Komisja jest uprawniona do przyjmowania aktów wykonawczych		Nie dotyczy

zawieszenia lub cofnięcia powiadomienia. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2.				
Komisja może przyjmować akty wykonawcze zgodnie z art. 100 w celu wskazania państwa trzeciego stwarzającego zagrożenie dla cyberbezpieczeństwa łańcuchów dostaw ICT.	Artykuł 100 ust. 2 Wyznaczenie państw trzecich budzących obawy w zakresie cyberbezpieczeństwa	Przyjmowanie aktów wykonawczych		Nie dotyczy Brak harmonogramu, ale akty wykonawcze powinny być regularnie poddawane przeglądowi
Komisja może przyjąć akty wykonawcze w celu wprowadzenia jednego lub kilku środków łagodzących, o których mowa w art. 103 ust. 2.	Artykuł 103 ust. 2 Środki łagodzące w łańcuchu dostaw ICT	Przyjmowanie aktów wykonawczych	Nie dotyczy	Nie dotyczy Brak harmonogramu, ale przegląd co 36 miesięcy (zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 2)
Komisja może przyjąć akty wykonawcze zgodnie z art. 102 w celu określenia kluczowych aktywów ICT wykorzystywanych do wytwarzania produktów lub świadczenia usług przez rodzaje podmiotów, o których mowa w załączniku I i załączniku II do dyrektywy (UE) 2022/2555.	Artykuł 102 ust. 1 Identyfikacja kluczowych aktywów ICT	Przyjmowanie aktów wykonawczych	Nie dotyczy	Nie dotyczy
Komisja może przyjąć akty wykonawcze zakazujące stosowania, instalowania lub integrowania w jakiejkolwiek formie	Artykuł 103 ust. 1 Środki łagodzące w łańcuchu dostaw ICT	Przyjmowanie aktów wykonawczych	Nie dotyczy	Nie dotyczy

komponentów ICT lub komponentów zawierających komponenty ICT pochodzących od dostawców wysokiego ryzyka, wyznaczonych zgodnie z art. 100 ust. 2, w kluczowych zasobach ICT określonych zgodnie z art. 102.				
Komisja może przyjąć akty wykonawcze w celu ustalenia, że podmioty, o których mowa w załącznikach I i II do dyrektywy (UE) 2022/2555, nie mogą wykorzystywać, instalować ani integrować komponentów ICT lub komponentów zawierających komponenty ICT pochodzące od określonego podmiotu.	Artykuł 103 ust. 7	Przyjmowanie aktów wykonawczych	Konsultacje z państwami członkowskimi i zainteresowanymi podmiotami	Nie dotyczy
W drodze aktów wykonawczych Komisja ustanawia wykazy dostawców wysokiego ryzyka, których dotyczą zakazy określone w aktach wykonawczych przyjętych zgodnie z art. 103 ust. 1 lub zakaz, o którym mowa w art. 1110 ust. 1.	Artykuł 104 ust. 1	Przyjmowanie aktów wykonawczych	Nie dotyczy	Nie dotyczy
Komisja może przyjmować akty wykonawcze w celu dalszego określenia warunków, o których mowa w art. 105 ust. 2 lit. b), oraz w celu ustanowienia szczegółowych zasad dotyczących procedur, o których mowa w art. 105.	Artykuł 105 Zwolnienie podmiotów mających siedzibę w państwie trzecim budzącym obawy w zakresie cyberbezpieczeństwa lub kontrolowanych przez takie państwo	Przyjmowanie aktów wykonawczych	Nie dotyczy	Nie dotyczy
Komisja może przyjąć akty wykonawcze ustanawiające szczegółowe zasady	Artykuł 109 Opłaty	Przyjmowanie aktów wykonawczych	Nie dotyczy	Nie dotyczy

dotyczące opłat, określające wysokość opłat i sposób ich uiszczania.				
Komisja przyjmuje akty wykonawcze w celu określenia terminów wycofania elementów ICT lub elementów zawierających elementy ICT dostarczanych przez dostawców wysokiego ryzyka w odniesieniu do stacjonarnych i satelitarnych sieci łączności elektronicznej.	Artykuł 110 ust. 4 Kluczowe aktywa ICT dla sieci łączności elektronicznej ruchomej, stacjonarnej i satelitarnej	Przyjmowanie aktów wykonawczych	Nie dotyczy	Nie dotyczy
Komisja może przyjmować akty delegowane zgodnie z art. 119 w celu zmiany załącznika II, aby dostosować go do rozwoju technologicznego, uwzględniając elementy, o których mowa w art. 103 ust. 3.	Artykuł 110 ust. 5	Przyjmowanie aktów delegowanych	Nie dotyczy	Nie dotyczy
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	Artykuł 1 pkt 7 dyrektywy Maksymalna harmonizacja	Komisja może przyjąć akty wykonawcze		Nie dotyczy

funkcjonowania rynku wewnętrznego. Na podstawie wyników tych ocen Komisja może zaproponować takie akty wykonawcze dla określonych sektorów lub rodzajów podmiotów. 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) po akapicie czwartym dodaje się akapit w brzmieniu: „W przypadku przyjęcia przez Komisję aktów wykonawczych, o których mowa w akapicie pierwszym i drugim niniejszego ustępu, państwa członkowskie nie nakładają żadnych dodatkowych wymogów technicznych lub metodologicznych dotyczących środków, o których mowa w art. 21 ust. 2 dyrektywy (UE) 2022/2555, na podmioty objęte zakresem tych aktów wykonawczych”.				