KOMISJA
EUROPEJSKA

Bruksela, dnia 22.2.2018 r.
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie „Agencji UE ds. Cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa")

(Tekst mający znaczenie dla EOG)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Unia Europejska podjęła liczne działania, mające na celu zwiększenie odporności i wzmocnienie swojej gotowości w zakresie cyberbezpieczeństwa. W pierwszej strategii dotyczącej cyberbezpieczeństwa UE[1], przyjętej w 2013 r., określono strategiczne cele i konkretne działania, prowadzące – w odniesieniu do UE – do uzyskania odporności, ograniczenia cyberprzestępczości, stworzenia polityki cyberobrony i zdolności w tym zakresie, rozbudowy zasobów przemysłowych i technologicznych oraz ustanowienia spójnej międzynarodowej polityki dotyczącej cyberprzestrzeni. Od tamtej pory wiele się wydarzyło, między innymi zwłaszcza udzielono kolejnego mandatu Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)[2] i przyjęto **dyrektywę w sprawie bezpieczeństwa sieci i systemów informatycznych**[3] (dyrektywę w sprawie cyberbezpieczeństwa), które to działania stanowią podstawę dla niniejszego wniosku.

Ponadto **w 2016 r. Komisja Europejska przyjęła komunikat „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego”**[4], w którym zapowiedziano wprowadzenie dalszych środków, mających na celu przyspieszenie współpracy, wymiany informacji i wiedzy oraz zwiększenie odporności i gotowości UE, także z uwzględnieniem możliwości wystąpienia w przyszłości incydentów na dużą skalę i potencjalnego ogólnoeuropejskiego cyberkryzysu. W związku z tym Komisja zapowiedziała, że przedstawi **ocenę** i **przegląd** rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 526/2013 w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji oraz uchylającego rozporządzenie (WE) nr 460/2004 (rozporządzenia w sprawie ENISA). Procedura oceny może doprowadzić do ewentualnej reformy Agencji i zwiększenia jej zdolności i potencjału do wspierania państw członkowskich w sposób trwały. Nadałoby to Agencji bardziej operacyjną i centralną rolę w uzyskiwaniu odporności w zakresie cyberbezpieczeństwa i potwierdziło w jej nowym mandacie nowe obowiązki w ramach dyrektywy w sprawie cyberbezpieczeństwa.

Dyrektywa w sprawie cyberbezpieczeństwa jest pierwszym ważnym krokiem prowadzącym do propagowania kultury zarządzania ryzykiem przez wprowadzenie wymogów w zakresie bezpieczeństwa jako zobowiązań prawnych dla kluczowych zainteresowanych podmiotów gospodarczych, zwłaszcza świadczących usługi o zasadniczym znaczeniu (operatorzy usług kluczowych) oraz dostawców niektórych kluczowych usług cyfrowych (dostawcy usług cyfrowych). W sytuacji, gdy wymogi bezpieczeństwa są postrzegane jako niezbędne do zapewnienia korzyści wynikających z rozwoju cyfryzacji społeczeństwa, oraz z uwagi na gwałtowne rozpowszechnienie urządzeń podłączonych do internetu (internet rzeczy – ang. *the*

---

[1] Wspólny komunikat Komisji Europejskiej i Europejskiej Służby Działań Zewnętrznych: Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń – JOIN(2013).

[2] Rozporządzenie (UE) nr 526/2013 w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004.

[3] Dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

[4] Komunikat Komisji „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego”, COM(2016) 410 final.

Internet of Things, IoT) w komunikacie z 2016 r. wysunięto też pomysł utworzenia ram certyfikacji bezpieczeństwa produktów i usług ICT w celu zwiększenia poziomu zaufania i bezpieczeństwa na jednolitym rynku cyfrowym. Certyfikacja cyberbezpieczeństwa ICT staje się szczególnie istotna w świetle zwiększonego stosowania technologii wymagających wysokiego poziomu cyberbezpieczeństwa, takich jak automatyczne i zintegrowane z siecią samochody, e-zdrowie bądź systemy sterowania automatyki przemysłowej (IACS).

Wspomniane środki polityczne i komunikaty zostały dodatkowo wzmocnione przez **konkluzje Rady** z 2016 r., w których przyznano, że „zagrożenia i słabości cybernetyczne ciągle ewoluują i wzmagają się, co będzie wymagać stałej i bliższej współpracy, zwłaszcza w obliczu transgranicznych incydentów na dużą skalę dotyczących bezpieczeństwa cybernetycznego". W konkluzjach ponownie podkreślono, że „rozporządzenie w sprawie ENISA jest jednym z głównych elementów unijnych ram odporności cybernetycznej"[5], i wezwano Komisję do podjęcia dalszych działań w celu rozwiązania kwestii certyfikacji na poziomie europejskim.

Ustanowienie systemu certyfikacji wymagałoby wprowadzenia stosownego systemu administrowania na poziomie unijnym, obejmującego dogłębną wiedzę ekspercką zapewnianą przez niezależną agencję UE. W odniesieniu do tej kwestii w niniejszym wniosku wskazano ENISA jako nasuwający się w sposób oczywisty podmiot unijny, właściwy w zakresie zagadnień cyberbezpieczeństwa, który powinien przyjąć taką rolę w celu zintegrowania i koordynacji działań krajowych właściwych podmiotów zajmujących się certyfikacją.

W komunikacie w sprawie **śródokresowego przeglądu strategii jednolitego rynku cyfrowego z maja 2017 r.** Komisja stwierdziła następnie, że do września 2017 r. dokona przeglądu mandatu ENISA. Ma to na celu określenie roli tej agencji w zmienionym ekosystemie cyberbezpieczeństwa i opracowanie środków dotyczących norm cyberbezpieczeństwa, certyfikacji i etykietowania, tak aby zwiększyć poziom cyberbezpieczeństwa systemów opartych na technologiach informacyjno-telekomunikacyjnych, w tym urządzeń podłączonych do internetu[6]. W **konkluzjach Rady Europejskiej** z czerwca 2017 r.[7] z zadowoleniem przyjęto fakt, że Komisja zamierza we wrześniu dokonać przeglądu strategii cyberbezpieczeństwa i przed końcem roku 2017 zaproponować kolejne ukierunkowane działania.

W proponowanym rozporządzeniu przewidziano kompleksowy zestaw środków, które opierają się na dotychczasowych działaniach i wspierają osiągniecie wzajemnie się wzmacniających celów szczegółowych:

- zwiększenie **zdolności i gotowości państw** członkowskich i przedsiębiorstw;
- poprawa **współpracy i koordynacji** między państwami członkowskimi a instytucjami, agencjami i organami UE;
- zwiększenie **zdolności na poziomie unijnym do uzupełniania działań państw członkowskich**, zwłaszcza w przypadku transgranicznych cyberkryzysów;

---

5 Konkluzje Rady w sprawie wzmacniania europejskiego systemu cyberodporności cybernetycznej oraz wspierania konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego, 15 listopada 2016 r.

6 Komunikat Komisji w sprawie przeglądu śródokresowego realizacji strategii jednolitego rynku cyfrowego, COM(2017) 228.

7 Posiedzenie Rady Europejskiej (22 i 23 czerwca 2017 r.), konkluzje EUCO 8/17.

- podnoszenie **poziomu świadomości** obywateli i przedsiębiorstw na temat cyberbezpieczeństwa;
- zwiększanie ogólnej **przejrzystości procesu zapewniania cyberbezpieczeństwa**[8] produktów i usług ICT w celu wzmocnienia zaufania do jednolitego rynku cyfrowego i innowacji cyfrowych; oraz
- unikanie **rozdrobnienia systemów certyfikacji** w UE oraz powiązanych wymogów w zakresie bezpieczeństwa i kryteriów oceny we wszystkich państwach członkowskich i sektorach.

Poniższa część uzasadnienia wyjaśnia bardziej szczegółowo powody niniejszej inicjatywy w odniesieniu do proponowanych działań dotyczących agencji ENISA i certyfikacji cyberbezpieczeństwa.

ENISA

ENISA działa jako ośrodek wiedzy specjalistycznej, mający za zadanie zwiększanie bezpieczeństwa sieci i informacji w Unii oraz wspieranie budowania zdolności państw członkowskich.

ENISA została powołana w 2004 r.[9] z zadaniem przyczynienia się do osiągnięcia ogólnego celu, którym jest zapewnienie wysokiego poziomu bezpieczeństwa sieci i informacji w UE. W 2013 r. rozporządzeniem (UE) nr 526/2013 ustanowiono nowy mandat Agencji na okres siedmiu lat, do 2020 r. Biura Agencja znajdują się w Grecji; siedzibą administracyjną jest Heraklion (na Krecie), a podstawowa działalność jest prowadzona w Atenach.

W porównaniu ze wszystkimi agencjami UE ENISA jest niewielką agencją o niskim budżecie i małej liczbie pracowników. Jej mandat jest określony czasowo.

ENISA wspomaga instytucje europejskie, państwa członkowskie oraz sektor przedsiębiorczości w **rozwiązywaniu problemów związanych z bezpieczeństwem sieci i informacji, reagowaniu na nie, a przede wszystkim zapobieganiu im**. Dokonuje tego za pomocą ciągu działań w pięciu obszarach określonych w jej strategii:[10]:

- Wiedza fachowa: dostarczanie informacji i wiedzy specjalistycznej na temat kluczowych kwestii dotyczących bezpieczeństwa sieci i informacji.
- Działania polityczne: wspieranie kształtowania polityki i jej realizowania w Unii.
- Potencjał: wspomaganie budowania potencjału w całej Unii (np. za pomocą szkoleń, zaleceń, działań podnoszących poziom wiedzy).
- Wspólnota: sprzyjanie tworzeniu wspólnoty bezpieczeństwa sieci i informacji (np. wspieranie zespołów reagowania na incydenty komputerowe (CERT), koordynacja ogólnoeuropejskich ćwiczeń w dziedzinie cyberbezpieczeństwa).

---

8 Przejrzystość środków zapewniania cyberbezpieczeństwa oznacza zapewnienie użytkownikom informacji na temat właściwości z zakresu cyberbezpieczeństwa, które umożliwiają im obiektywne określenie poziomu bezpieczeństwa danego produktu, usługi bądź procesu ICT.

9 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).

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

- Ułatwianie (np. wchodzenie w relacje z zainteresowanymi stronami i kontakty międzynarodowe).

W trakcie uzgadniania treści dyrektywy w sprawie cyberbezpieczeństwa unijni współprawodawcy postanowili przypisać ENISA istotną rolę we wdrażaniu tej dyrektywy. W szczególności Agencja zapewnia sekretariat sieci CSIRT (utworzonej w celu wspierania sprawnej i skutecznej współpracy operacyjnej między państwami członkowskimi w zakresie konkretnych cyberincydentów i wymiany informacji o ryzyku). Jej zadaniem jest również pomoc grupie współpracy w wykonywaniu jej zadań. Ponadto dyrektywa nakłada na ENISA obowiązek pomocy państwom członkowskim i Komisji przez zapewnianie wiedzy fachowej i doradztwa oraz ułatwianie wymiany najlepszych praktyk.

Zgodnie z rozporządzeniem ws. ENISA Komisja przeprowadziła ocenę Agencji, która obejmuje przeprowadzenie niezależnego badania oraz konsultacje publiczne. W ramach oceny analizowano istotność, wpływ, skuteczność, wydajność, spójność działań Agencji oraz wnoszoną przez nią europejską wartość dodaną w odniesieniu do osiągnięć Agencji, zarządzania, wewnętrznej struktury organizacyjnej i praktyki działania w latach 2013–2016.

Ogólne wyniki ENISA zostały pozytywnie ocenione przez większość respondentów[11] (74 %) uczestniczących w konsultacjach publicznych. Poza tym większość respondentów uznała, że ENISA osiąga swoje różne cele (co najmniej 63 % w odniesieniu do każdego z celów). Usługi i produkty ENISA są regularnie (co miesiąc lub częściej) wykorzystywane przez prawie połowę respondentów (46 %) i doceniane ze względu na fakt, iż ich źródłem jest jednostka na szczeblu unijnym (83 %), oraz z racji swojej jakości (62 %).

Znaczna większość (88 %) respondentów uważa jednak, że obecne instrumenty i mechanizmy dostępne na szczeblu UE są niewystarczające lub jedynie częściowo odpowiednie, by stawić czoło aktualnym wyzwaniom w dziedzinie cyberbezpieczeństwa. Przeważająca większość respondentów (98 %) wskazywała, że kwestią tych potrzeb powinien się zająć podmiot unijny, a ENISA została uznana przez 99 % respondentów za właściwą do tego organizację. Ponadto 67,5 % respondentów było zdania, że ENISA może odgrywać rolę w tworzeniu zharmonizowanych ram certyfikacji bezpieczeństwa produktów i usług IT.

W wyniku ogólnej oceny (nie tylko w oparciu o konsultacje publiczne, ale również o szereg indywidualnych wywiadów, dodatkowych ukierunkowanych badań i warsztatów) sformułowano następujące wnioski:

- Cele ENISA pozostają aktualne. W warunkach szybkiego rozwoju technologicznego i zmieniających się zagrożeń i w świetle rosnącego globalnego cyberryzyka istnieje w UE wyraźna potrzeba wspierania i dalszego pogłębienia fachowej wiedzy technicznej w zakresie cyberbezpieczeństwa. W państwach członkowskich należy budować potencjał do rozumienia zagrożeń i reagowania na nie, a zainteresowane strony muszą współpracować przekrojowo w obszarach tematycznych i międzyinstytucjonalnie.

[11] 90 zainteresowanych stron z 19 państw członkowskich uczestniczyło w konsultacjach (88 odpowiedzi i 2 stanowiska na piśmie), w tym organy krajowe z 15 państw członkowskich i 8 organizacji patronackich reprezentujących znaczną liczbę przedsiębiorstw europejskich

- Mimo niskiego budżetu Agencja jest operacyjnie skuteczna w wykorzystywaniu zasobów oraz w wykonywaniu swoich zadań. Rozdzielenie siedzib między Atenami i Heraklionem powodowało jednak również dodatkowe koszty administracyjne.
- ENISA częściowo spełniła swoje cele pod względem skuteczności. Agencja z powodzeniem przyczyniła się do poprawy bezpieczeństwa sieci i informacji w Europie poprzez zapewnienie budowania zdolności w 28 państwach członkowskich[12], ułatwianie współpracy między państwami członkowskimi a zainteresowanymi stronami z obszaru bezpieczeństwa sieci i informacji w Europie oraz poprzez zapewnianie wiedzy specjalistycznej, tworzenie wspólnoty i wspieranie kształtowania polityki. Generalnie ENISA z należytą starannością skupiła się na realizacji swojego programu prac i działała jako wiarygodny partner na rzecz zainteresowanych stron w dziedzinie, którą dopiero niedawno uznano za tak istotną w wymiarze transgranicznym.
- ENISA zdołała zaznaczyć swój wpływ, przynajmniej w pewnym wymiarze, w rozległym obszarze bezpieczeństwa sieci i informacji, ale nie osiągnęła pełnego sukcesu w budowaniu silnej marki oraz nie uzyskała pozycji wystarczającej do uznania jej za główny ośrodek wiedzy specjalistycznej w Europie. Wyjaśnienie tego kryje się w szerokim zakresie mandatu ENISA, która nie została odpowiednio wyposażona w wystarczające środki. Ponadto ENISA jest jedyną agencją UE z mandatem na czas określony, co ogranicza jej zdolność do opracowania długofalowej wizji i odpowiedniego świadczenia działalności na rzecz zainteresowanych stron. Stoi to również w sprzeczności z przepisami dyrektywy w sprawie cyberbezpieczeństwa, w której powierzono ENISA zadania bez daty końcowej. Wreszcie, z oceny wynika, że ograniczoną skuteczność można częściowo wytłumaczyć dużą zależnością od zewnętrznej wiedzy specjalistycznej przeważającej nad doświadczeniem własnym oraz trudnościami w pozyskaniu i zatrzymywaniu wyspecjalizowanych pracowników.
- Ostatnim, ale nie najmniej istotnym wnioskiem z oceny jest stwierdzenie, że wartość dodana ENISA polega przede wszystkim na jej zdolności ułatwiania współpracy głównie między państwami członkowskimi, zwłaszcza zaś między powiązanymi wspólnotami z obszaru bezpieczeństwa sieci i informacji (w szczególności między CSIRT). Na poziomie UE nie ma innego podmiotu, który obsługiwałby tak szeroki zakres podmiotów związanych z bezpieczeństwem sieci i informacji. Wskutek konieczności ścisłego określenia priorytetów działań program prac ENISA ukształtowany jest jednak głównie pod kątem potrzeb państw członkowskich. W rezultacie Agencja nie odpowiada w wystarczającym stopniu na potrzeby innych zainteresowanych stron, zwłaszcza przemysłu. Powoduje to również, że działanie Agencji jest reaktywne w stosunku do potrzeb kluczowych zainteresowanych

[12] Uczestników konsultacji publicznych poproszono o przedstawienie uwag na temat tego, co uważają za największe osiągnięcia ENISA w latach 2013 – 2016. Respondenci ze wszystkich grup (łącznie 55, w tym 13 organów krajowych, 20 podmiotów z sektora prywatnego i 22 „inne" podmioty) wskazali następujące główne osiągnięcia ENISA: 1. koordynowanie ćwiczeń Cyber Europe; 2. zapewnienie zespołom CERT/CSIRT wsparcia za pomocą szkoleń i warsztatów sprzyjających koordynacji i wymianie; 3. publikacje ENISA (wytyczne i zalecenia, przegląd zagrożeń, strategie zgłaszania incydentów i zarządzania kryzysowego itp.), które uznano za przydatne do opracowania i aktualizacji krajowych ram bezpieczeństwa, a także jako dokumenty odniesienia dla decydentów politycznych i praktyków w zakresie cyberprzestrzeni; 4. pomoc w propagowaniu dyrektywy w sprawie cyberbezpieczeństwa; 5. działania na rzecz podniesienia poziomu świadomości na temat cyberbezpieczeństwa za pomocą miesiąca cyberbezpieczeństwa.

podmiotów i uniemożliwia jej osiągnięcie większego wpływu. Dlatego wartość dodana zapewniana przez Agencję była różna, w zależności od różnych potrzeb zainteresowanych stron i od zakresu, w jakim Agencja była w stanie na nie reagować (np. potrzeby dużych państw wobec potrzeb państw małych; państwa członkowskie a przemysł).

Ogólnie, wyniki konsultacji z zainteresowanymi stronami i oceny wskazywały, że należy dostosować zasoby i mandat ENISA, tak aby mogła ona odgrywać odpowiednią rolę w reagowaniu na obecne i przyszłe wyzwania.

Biorąc pod uwagę te wyniki, w niniejszym wniosku dokonuje się przeglądu obecnego mandatu ENISA i ustanawia nowy szereg zadań i funkcji w celu skutecznego i wydajnego wspierania działań państw członkowskich, instytucji UE i innych zainteresowanych stron na rzecz zagwarantowania bezpiecznej cyberprzestrzeni w Unii Europejskiej. Nowy zaproponowany mandat Agencji jest próbą zapewnienia silniejszej i bardziej centralnej roli, w szczególności poprzez wspieranie państw członkowskich we wdrażaniu dyrektywy w sprawie cyberbezpieczeństwa oraz aktywniejsze przeciwdziałanie zagrożeniom (zdolności operacyjne), a także w wyniku przekształcenia w ośrodek wiedzy fachowej wspomagający państwa członkowskie i Komisję w sprawie certyfikacji cyberbezpieczeństwa. W ramach niniejszego wniosku:

- ENISA otrzyma stały mandat i w ten sposób uzyska stabilne podstawy na przyszłość. Mandat, cele i zadania powinny nadal podlegać regularnemu przeglądowi.
- W proponowanym mandacie dookreślona zostanie rola ENISA jako agencji UE ds. cyberbezpieczeństwa i punktu odniesienia w ramach unijnego ekosystemu cyberbezpieczeństwa, działającej w ścisłej współpracy ze wszystkimi innymi odpowiednimi podmiotami tego ekosystemu.
- Organizacja i sposób zarządzania Agencją, które uzyskały pozytywną ocenę, zostaną nieco zmienione, zwłaszcza po to, aby zapewnić lepsze odzwierciedlenie potrzeb szerszej społeczności zainteresowanych stron w pracach Agencji.
- Wyznaczając proponowany zakres mandatu, wzmocniono te obszary, w których Agencja wniosła wyraźną wartość dodaną, i dodano nowe obszary, wymagające wsparcia z uwagi na nowe priorytety i instrumenty polityczne, w szczególności takie jak: dyrektywa w sprawie cyberbezpieczeństwa, przegląd strategii UE w zakresie bezpieczeństwa cybernetycznego, przygotowywany unijny plan działania na rzecz współpracy w sytuacjach kryzysowych w dziedzinie cyberbezpieczeństwa oraz certyfikacja bezpieczeństwa ICT:
    - **Opracowanie i wdrożenie polityki UE:** ENISA miałaby za zadanie aktywne przyczynianie się do rozwoju polityki w dziedzinie bezpieczeństwa sieci i informacji, a także innych inicjatyw politycznych z elementami cyberbezpieczeństwa w różnych sektorach (np. energetyce, transporcie, finansach). Do tego celu uzyska silną rolę doradczą, którą będzie mogła wypełnić przez dostarczanie niezależnych opinii i prac przygotowawczych na potrzeby opracowania i aktualizacji polityki oraz przepisów prawa. ENISA będzie również wspierać unijne działania i prawo w obszarach łączności elektronicznej, tożsamości elektronicznej i usług zaufania, aby propagować wyższy poziom cyberbezpieczeństwa. Na etapie wdrażania, w szczególności w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji, ENISA pomoże państwom członkowskim w osiągnięciu spójnego w wymiarze ponadgranicznym i ponadsektorowym podejścia do wdrożenia odnośnej

dyrektywy oraz innych właściwych strategii politycznych i przepisów. Aby wesprzeć regularne przeglądy strategii politycznych oraz przepisów w obszarze cyberbezpieczeństwa, ENISA będzie także składać regularne sprawozdania na temat stanu wdrożenia unijnych ram prawnych.

- **Budowanie zdolności:** ENISA będzie przyczyniać się do zwiększenia zdolności i wiedzy fachowej organów unijnych i krajowych organów publicznych, w tym w zakresie reagowania na cyberincydenty i nadzoru nad środkami regulacyjnymi związanymi z cyberbezpieczeństwem. Od Agencji będzie się również wymagać uczestnictwa w tworzeniu ośrodków wymiany i analizy informacji (ang. Information Sharing and Analysis Centre, ISAC) w różnych sektorach poprzez zapewnienie najlepszych praktyk i wytycznych na temat dostępnych narzędzi i procedur, a także przez odpowiednie rozwiązanie kwestii regulacyjnych związanych z wymianą informacji.
- **Wiedza i informacje, podnoszenie poziomu świadomości:** ENISA mogłaby stać się unijnym centrum wymiany informacji. Oznaczałoby to propagowanie i wymianę najlepszych praktyk i inicjatyw w całej UE poprzez gromadzenie informacji na temat cyberbezpieczeństwa, pochodzących z instytucji, agencji i organów unijnych i krajowych. Agencja świadczyłaby również doradztwo, udostępniała wskazówki i najlepsze praktyki w zakresie ochrony infrastruktury krytycznej. W następstwie poważnych transgranicznych cyberincydentów ENISA mogłaby ponadto sporządzać zbiorcze sprawozdania w celu zaoferowania wskazówek przedsiębiorstw i obywatelom w całej UE. Ten nurt działań mógłby również obejmować regularne organizowanie w koordynacji z organami państw członkowskich wydarzeń mających na celu upowszechnienie wiedzy.
- **Zadania związane z rynkiem (normalizacja, certyfikacja cyberbezpieczeństwa):** ENISA pełniłaby szereg funkcji w szczególny sposób wspierających rynek wewnętrzny i objęłaby swoim działaniem centrum monitorowania rynku cyberbezpieczeństwa przez analizę odpowiednich tendencji w ramach rynku cyberbezpieczeństwa, aby lepiej spełniał on wymogi podaży i popytu, a także przez wspomaganie kształtowania polityki UE w obszarach normalizacji ICT i certyfikacji cyberbezpieczeństwa ICT. W szczególności w odniesieniu do normalizacji ENISA ułatwiałaby tworzenie i wdrażanie norm dotyczących cyberbezpieczeństwa. Agencja wykonywałaby także zadania określone w odniesieniu do przyszłych ram certyfikacji (zob. sekcja poniżej).
- **Badania naukowe i innowacje:** ENISA wniesie swoją fachową wiedzę poprzez doradzanie UE i organom krajowym w kwestii priorytetów w zakresie badań i rozwoju, w tym w ramach umownego partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa (cPPP). Opinie ENISA na temat badań zostaną uwzględnione w nowym Europejskim Centrum Badań i Kompetencji w dziedzinie Cyberbezpieczeństwa, ujętym w kolejnych wieloletnich ramach finansowych. ENISA będzie również uczestniczyć, na prośbę Komisji, we wdrażaniu unijnych programów finansowania badań i innowacji.
- **Współpraca operacyjna i zarządzanie kryzysowe:** Ten nurt działań powinien być oparty na wzmacnianiu istniejącej zdolności operacyjnej w zakresie prewencji, zwłaszcza doskonaleniu ogólnoeuropejskich ćwiczeń

w tej dziedzinie (Cyber Europe) przez ich coroczną organizację oraz na wspierającej roli Agencji we współpracy operacyjnej jako sekretariatu sieci CSIRT (zgodnie z dyrektywą w sprawie cyberbezpieczeństwa) za pośrednictwem, między innymi, dobrze funkcjonującej infrastruktury informatycznej i kanałów komunikacji sieci CSIRT. W tym zakresie potrzebna będzie uporządkowana współpraca z CERT-UE, Europejskim Centrum ds. Cyberprzestępczości (EC3) oraz innymi odnośnymi podmiotami unijnymi. Poza tym efektem uporządkowanej współpracy z CERT-UE, w bliskim fizycznym sąsiedztwie, powinno być zapewnienie pomocy technicznej w przypadku wystąpienia poważnych incydentów oraz wsparcie analizy incydentów. Państwa członkowskie otrzymałyby na żądanie pomoc w postępowaniu w przypadku incydentów i wsparcie analizy luk w zabezpieczeniach, artefaktów i incydentów w celu wzmocnienia ich zdolności w zakresie prewencji i zdolności reagowania.

- ENISA miałaby również do odegrania rolę w ramach **unijnego planu działania w zakresie cyberbezpieczeństwa**, przedstawionego w ramach niniejszego pakietu, oraz w ustalaniu zaleceń Komisji dla państw członkowskich na potrzeby skoordynowanego reagowania na szczeblu unijnym na transgraniczne cyberincydenty na dużą skalę i cyberkryzysy[13]. ENISA będzie ułatwiać współpracę między poszczególnymi państwami członkowskimi w razie konieczności reagowania w sytuacjach kryzysowych poprzez analizę i agregowanie krajowych raportów sytuacyjnych w oparciu o informacje udostępnione Agencji przez państwa członkowskie i inne podmioty na zasadzie dobrowolności.

- **Certyfikacja cyberbezpieczeństwa produktów i usług ICT**

W celu ustanowienia i utrzymania zaufania i bezpieczeństwa produkty i usługi ICT muszą bezpośrednio obejmować zabezpieczenia na wczesnym etapie projektowania i rozwoju technicznego („bezpieczeństwo na etapie projektowania”). Ponadto klienci i użytkownicy muszą mieć możliwość określenia poziomu zapewnienia bezpieczeństwa produktów i usług, które zamawiają lub kupują.

Certyfikacja, która polega na formalnej ocenie produktów, usług i procesów przez niezależną i akredytowaną jednostkę w oparciu o określony zestaw norm i kryteriów oraz wydaniu świadectwa potwierdzającego zgodność, odgrywa ważną rolę w zwiększaniu zaufania do produktów i usług oraz ich bezpieczeństwa. Oceny bezpieczeństwa pozostają kwestią raczej techniczną, certyfikacja ma jednak na celu poinformowanie nabywców i użytkowników o właściwościach bezpieczeństwa nabywanych przez nich produktów i usług ICT oraz upewnienie ich o tych właściwościach. Jak wspomniano powyżej, jest to szczególnie istotne w przypadku nowych systemów, które w znacznym stopniu korzystają z technologii cyfrowych i które wymagają wysokiego poziomu bezpieczeństwa, takich jak np. samochody

[13] Plan działania będzie miał zastosowanie do cyberincydentów, które powodują zakłócenie na skalę na tyle szeroką, że żadne państwo członkowskie nie zdoła się z nimi uporać, lub dotykają co najmniej dwóch państw członkowskich i mają tak rozległy i znaczący wpływ lub znaczenie polityczne, że wymagają terminowej koordynacji polityki i reakcji na szczeblu politycznym w Unii.

automatyczne połączone z systemami informatycznymi, e-zdrowie, systemy sterowania automatyki przemysłowej (IACS)[14] lub inteligentne sieci.

Aktualnie obszar certyfikacji cyberbezpieczeństwa produktów i usług ICT w UE jest dość rozczłonkowany. Pojawił się szereg inicjatyw międzynarodowych, takich jak tzw. wspólne kryteria (CC) oceny bezpieczeństwa technologii informatycznych (ISO 15408), które są normą międzynarodową na potrzeby oceny bezpieczeństwa komputerowego. Opierają się one na ocenie dokonanej przez osobę trzecią i obejmują siedem poziomów uzasadnionego zaufania (EAL). CC i towarzysząca im wspólna metodyka oceny bezpieczeństwa technologii informatycznych (CEM) stanowią techniczną podstawę zawarcia międzynarodowego porozumienia w sprawie wspólnych kryteriów uznawania (CCRA), które zapewnia, aby świadectwa CC były uznawane przez wszystkich sygnatariuszy CCRA. W obecnym brzmieniu CCRA tylko oceny do poziomu EAL 2 są jednak wzajemnie uznawane. Ponadto jedynie 13 państw członkowskich podpisało porozumienie.

Organy odpowiedzialne za certyfikację z 12 państw członkowskich zawarły porozumienie w sprawie wzajemnego uznawania w odniesieniu do świadectw wydanych zgodnie z porozumieniem na podstawie wspólnych kryteriów[15]. Poza tym w państwach członkowskich funkcjonuje obecnie lub jest w fazie powoływania pewna liczba inicjatyw w zakresie certyfikacji technologii informacyjno-komunikacyjnych. Choć inicjatywy te są ważne, stwarzają ryzyko fragmentacji rynku i pojawienia się problemów dotyczących interoperacyjności. W konsekwencji przedsiębiorstwo może być zmuszone do poddania się kilku procedurom certyfikacji w różnych państwach członkowskich, aby móc oferować swój produkt na wielu rynkach. Na przykład wytwórca inteligentnego miernika, który chce sprzedawać swoje produkty w trzech państwach członkowskich, np. Niemczech, Francji i Zjednoczonym Królestwie, musi obecnie spełniać wymogi trzech różnych systemów certyfikacji. Są to: Commercial Product Assurance (CPA) w Zjednoczonym Królestwie, Certification de Sécurité de Premier Niveau (CSPN) we Francji (CSPN) i określony profil ochrony oparty na wspólnych kryteriach w Niemczech

Sytuacja ta powoduje wyższe koszty i stanowi znaczne obciążenie administracyjne dla przedsiębiorstw prowadzących działalność w kilku państwach członkowskich. Koszty certyfikacji mogą wprawdzie znacznie się różnić w zależności od danego produktu/usługi, wymaganego poziomu uzasadnionego zaufania lub innych składników, ogólnie jednak są one dość wysokie dla przedsiębiorstw. Na przykład koszt certyfikatu BSI dla bramki sieciowej inteligentnego licznika wynosi ponad milion euro (najwyższy poziom badań i uzasadnionego zaufania; odnosi się nie tylko do jednego produktu, ale także do całej otaczającej infrastruktury). Koszty certyfikacji w przypadku inteligentnych liczników w Zjednoczonym Królestwie wynoszą prawie 150 000 EUR. We Francji koszty są podobne jak w Zjednoczonym Królestwie; wynoszą ok. 150 000 EUR lub więcej.

---

[14] DG Wspólne Centrum Badawcze (JRC) opublikowało sprawozdanie, w którym zaproponowano wstępny zestaw wspólnych europejskich wymogów związanych z cyberbezpieczeństwem oraz ogólne wytyczne dotyczące certyfikacji cyberbezpieczeństwa komponentów IACS. Dostępne na stronie internetowej: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[15] Grupa wyższych urzędników ds. bezpieczeństwa systemów informatycznych (SOG-IS) obejmuje 12 państw członkowskich oraz Norwegię i opracowała kilka profili ochrony w odniesieniu do ograniczonej liczby produktów, takich jak podpis cyfrowy, tachograf cyfrowy i inteligentne karty. Uczestnicy współpracują nad koordynacją normalizacji profili ochrony zgodnych z CC i koordynują opracowywanie profili ochrony. Państwa członkowskie często wymagają certyfikacji według SOG-IS na potrzeby krajowych przetargów na zamówienia publiczne.

Kluczowe zainteresowane strony z sektora publicznego i prywatnego przyznały, że w sytuacji braku ogólnounijnego systemu certyfikacji cyberbezpieczeństwa przedsiębiorstwa w wielu okolicznościach muszą indywidualnie poddawać się certyfikacji w poszczególnych państwach członkowskich, co prowadzi do fragmentacji rynku. Najważniejsze jest jednak, że wobec braku harmonizacji przepisów unijnych dotyczących produktów i usług ICT różnice w zakresie norm i praktyk certyfikacji cyberbezpieczeństwa w państwach członkowskich mogą praktycznie stworzyć 28 oddzielnych rynków bezpieczeństwa w UE, z których każdy będzie posiadać własne wymagania techniczne, metodykę przeprowadzania prób i procedury certyfikacji cyberbezpieczeństwa. Te rozbieżne podejścia na poziomie krajowym mogą powodować – w przypadku braku odpowiednich działań na szczeblu unijnym – znaczne przeszkody dla realizacji jednolitego rynku cyfrowego, spowalnianie lub uniemożliwienie uzyskania powiązanych pozytywnych efektów pod względem wzrostu gospodarczego i zatrudnienia.

W oparciu o powyższe elementy w proponowanym rozporządzeniu ustanawia się europejskie ramy certyfikacji cyberbezpieczeństwa („**ramy**”) w odniesieniu do produktów i usług ICT oraz określa zasadnicze funkcje i zadania agencji ENISA w dziedzinie certyfikacji cyberbezpieczeństwa. W niniejszym wniosku określono ogólne zasady europejskiego systemu certyfikacji cyberbezpieczeństwa. Wniosek nie wprowadza bezpośrednio operacyjnych systemów certyfikacji, stwarza raczej system (ramy) ustanowienia poszczególnych systemów certyfikacji dla określonych produktów/usług ICT („europejskie systemy certyfikacji cyberbezpieczeństwa”). Stworzenie europejskich systemów certyfikacji cyberbezpieczeństwa zgodnie z ramami sprawi, że certyfikaty wydane w ramach tych systemów będą ważne i uznawane we wszystkich państwach członkowskich, oraz umożliwi uporządkowanie obecnej fragmentacji rynku.

Generalnym celem europejskiego systemu certyfikacji cyberbezpieczeństwa jest potwierdzenie, że produkty i usługi ICT, które były certyfikowane zgodnie z takim systemem, spełniają określone wymogi w zakresie cyberbezpieczeństwa. Obejmowałoby to na przykład ich zdolności do ochrony danych (przechowywanych, przekazywanych lub przetwarzanych w inny sposób) przed przypadkowym lub nieupoważnionym przechowywaniem, przetwarzaniem, dostępem do nich, ujawnieniem, zniszczeniem, przypadkową utratą lub zmianą. Unijne systemy certyfikacji cyberbezpieczeństwa wykorzystywałyby istniejące normy w odniesieniu do wymogów technicznych i procedur oceny, z którymi te produkty muszą być zgodne, i w ich ramach nie opracowywano by własnych norm technicznych[16]. Na przykład dzięki ogólnounijnej certyfikacji produktów takich jak inteligentne karty, które są obecnie badane pod kątem międzynarodowych norm CC w ramach wielostronnego systemu SOG-IS (opisanego powyżej), system ten zyskałby ważność w całej UE.

Oprócz opracowania określonego zestawu celów w zakresie bezpieczeństwa, które należy brać pod uwagę przy projektowaniu konkretnego europejskiego systemu certyfikacji cyberbezpieczeństwa, we wniosku wskazano, jaki powinien być minimalny zakres treści takich systemów. W niektórych systemach konieczne będzie między innymi wskazanie pewnej liczby szczególnych elementów określających zakres i cel certyfikacji cyberbezpieczeństwa. Obejmuje to określenie kategorii produktów i usług objętych certyfikacją, szczegółową specyfikację wymogów cyberbezpieczeństwa (na przykład przez odesłanie do odnośnych norm lub specyfikacji technicznych), specyficzne kryteria i metody

[16] W przypadku norm europejskich odbywa się to poprzez europejskie organizacje normalizacyjne i jest zatwierdzane przez Komisję Europejską w postaci publikacji w *Dzienniku Urzędowym* (zob. rozporządzenie (UE) nr 1025/2012).

oceny oraz poziom pewności, które mają one zapewnić (tj. podstawowy, znaczny bądź wysoki).

Europejskie systemy certyfikacji cyberbezpieczeństwa zostaną opracowane przez ENISA przy pomocy i w ścisłej współpracy z Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa (zob. poniżej) i przyjęte przez Komisję w drodze aktów wykonawczych. W przypadku stwierdzenia potrzeby stworzenia systemu certyfikacji cyberbezpieczeństwa Komisja zwróci się do ENISA o przygotowanie takiego systemu w odniesieniu do konkretnych produktów lub usług ICT. ENISA będzie pracować nad systemem w ścisłej współpracy z krajowymi organami nadzorczymi odpowiedzialnymi za certyfikację, reprezentowanymi w grupie. Państwa członkowskie i grupa mogą zaproponować Komisji wystąpienie do ENISA o przygotowanie konkretnego systemu.

Certyfikacja może być bardzo kosztownym procesem, co z kolei może prowadzić do wyższych cen dla klientów i konsumentów. Potrzeba certyfikacji może być też zróżnicowana w zależności od specyficznego kontekstu stosowania produktów i usług oraz szybkiego tempa zmian technologicznych. Skorzystanie z europejskiej certyfikacji cyberbezpieczeństwa powinno zatem pozostać dobrowolne, chyba że w unijnych przepisach określających wymogi w zakresie bezpieczeństwa produktów i usług ICT postanowiono inaczej.

Aby zapewnić harmonizację i uniknąć rozdrobnienia, krajowe systemy lub procedury certyfikacji cyberbezpieczeństwa, odnoszące się do produktów i usług ICT objętych europejskim systemem certyfikacji cyberbezpieczeństwa, przestają obowiązywać od daty ustalonej w akcie wykonawczym przyjmującym przedmiotowy system. Państwa członkowskie nie powinny ponadto wprowadzać nowych krajowych systemów certyfikacji cyberbezpieczeństwa produktów i usług ICT objętych istniejącym europejskim systemem certyfikacji cyberbezpieczeństwa.

Po przyjęciu europejskiego systemu certyfikacji cyberbezpieczeństwa wytwórcy produktów ICT i dostawcy usług ICT będą mogli złożyć wniosek o certyfikację swoich produktów lub usług do wybranej jednostki oceniającej zgodność. Jednostki oceniające zgodność powinny być akredytowane przez jednostkę akredytującą, jeśli spełniają pewne określone wymogi. Akredytacji udziela się na maksymalny okres pięciu lat i można ją odnowić na tych samych warunkach, o ile jednostka oceniająca zgodność spełnia wymogi. Jednostka akredytująca cofa akredytację danej jednostki oceniającej zgodność, jeżeli warunki akredytacji nie są lub już nie są spełnione, bądź w przypadku gdy działania podejmowane przez jednostkę oceniającą zgodność naruszają przepisy niniejszego rozporządzenia.

Zgodnie z wnioskiem zadania związane z monitorowaniem, nadzorowaniem i egzekwowaniem przepisów pozostają w gestii państw członkowskich. Każde państwo członkowskie będzie musiało ustanowić jeden organ nadzoru ds. certyfikacji. Zadaniem tego organu będzie nadzorowanie zgodności jednostek oceniających zgodność oraz certyfikatów wydawanych przez jednostki oceniające zgodność mające siedzibę na terytorium danego państwa z wymogami określonymi w niniejszym rozporządzeniu i stosownymi europejskimi systemami certyfikacji cyberbezpieczeństwa. Krajowe organy nadzoru ds. certyfikacji będą właściwe do rozpatrywania skarg składanych przez osoby fizyczne i prawne w odniesieniu do certyfikatów wydawanych przez jednostki oceniające zgodność mające siedzibę na danym terytorium. W odpowiednim wymiarze będą one badać przedmiot skargi i informować skarżącego o postępach i wyniku dochodzenia w rozsądnym terminie. Ponadto będą współpracować z innymi organami nadzoru ds. certyfikacji bądź innymi organami publicznymi, na przykład poprzez wymianę informacji na temat ewentualnej niezgodności produktów i usług ICT z wymogami niniejszego rozporządzenia lub określonych europejskich systemów certyfikacji cyberbezpieczeństwa.

We wniosku przewidziano też ustanowienie Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa („Grupy”), złożonej z krajowych organów nadzoru ds. certyfikacji wszystkich państw członkowskich. Głównym zadaniem Grupy jest doradzanie Komisji w kwestiach dotyczących polityki certyfikacji cyberbezpieczeństwa oraz współpraca z ENISA przy opracowywaniu projektów europejskich systemów certyfikacji cyberbezpieczeństwa. ENISA będzie wspierać Komisję w zapewnieniu Grupie sekretariatu oraz utrzymywaniu i aktualizowaniu publicznego wykazu systemów zatwierdzonych zgodnie z europejskimi ramami certyfikacji cyberbezpieczeństwa. ENISA będzie również pozostawać w kontakcie z organami normalizacyjnymi w celu zapewnienia adekwatności norm stosowanych w zatwierdzonych systemach oraz określenia obszarów wymagających ustanowienia norm cyberbezpieczeństwa.

Europejskie ramy certyfikacji cyberbezpieczeństwa („ramy”) przyniosą obywatelom i przedsiębiorstwom pewne korzyści. W szczególności:

- Dzięki stworzeniu ogólnounijnych systemów certyfikacji cyberbezpieczeństwa w odniesieniu do poszczególnych produktów lub usług powstanie swego rodzaju „punkt kontaktowy” dla przedsiębiorstw w zakresie certyfikacji cyberbezpieczeństwa w UE. Przedsiębiorstwa będą mogły poddawać swoje produkty certyfikacji tylko raz i otrzymać certyfikat ważny we wszystkich państwach członkowskich. Nie będą one zobowiązane do ponownej certyfikacji produktów przez różne krajowe organy certyfikacji. Obniży to znacznie koszty dla przedsiębiorstw, ułatwi działalność transgraniczną i ostatecznie zmniejszy i pozwoli uniknąć rozdrobnienia rynku wewnętrznego w odniesieniu do przedmiotowych produktów.
- Ramy te wprowadzają zasadę pierwszeństwa europejskich systemów certyfikacji cyberbezpieczeństwa nad systemami krajowymi: zgodnie z tą zasadą przyjęcie europejskiego systemu certyfikacji cyberbezpieczeństwa zastąpi wszystkie istniejące równolegle systemy krajowe w odniesieniu do tych samych produktów lub usług ICT na danym poziomie pewności. Poprawi to przejrzystość i ograniczy obecne rozpowszechnienie nakładających się i potencjalnie sprzecznych krajowych systemów certyfikacji cyberbezpieczeństwa.
- Wniosek wspiera i uzupełnia wdrożenie dyrektywy w sprawie cyberbezpieczeństwa poprzez zapewnienie przedsiębiorstwom podlegającym dyrektywie bardzo przydatnego narzędzia w celu wykazania zgodności z jej wymaganiami w całej Unii. Przy opracowywaniu nowych systemów certyfikacji cyberbezpieczeństwa Komisja i ENISA zwrócą szczególną uwagę na potrzebę zapewnienia, aby wymogi dyrektywy w sprawie cyberbezpieczeństwa znalazły odzwierciedlenie w systemach certyfikacji cyberbezpieczeństwa.
- Wniosek wesprze i ułatwi opracowywanie europejskiej polityki w zakresie cyberbezpieczeństwa przez harmonizację warunków i wymogów materialnych dotyczących certyfikacji cyberbezpieczeństwa produktów i usług ICT w Unii Europejskiej. Europejskie systemy certyfikacji cyberbezpieczeństwa będą się odwoływać do wspólnych norm bądź kryteriów oceny i metod badań. Przyczyni się to w znacznym stopniu, aczkolwiek niebezpośrednio, do wprowadzenia w UE wspólnych rozwiązań w zakresie bezpieczeństwa i w ten sposób usunie bariery w funkcjonowaniu rynku wewnętrznego.
- Ramy zostały pomyślane w taki sposób, aby zapewnić niezbędną elastyczność systemów certyfikacji cyberbezpieczeństwa. W zależności od konkretnych potrzeb w zakresie cyberbezpieczeństwa produkt lub usługa może uzyskać certyfikację w odniesieniu do wyższego lub niższego poziomu bezpieczeństwa. Europejskie

systemy certyfikacji cyberbezpieczeństwa będą projektowane z uwzględnieniem tej elastyczności i w związku z tym będą odpowiednie dla różnych poziomów pewności (tj. podstawowego, znacznego lub wysokiego), tak by można je było stosować do różnych celów lub w różnych sytuacjach.

- Dzięki tym wszystkim omówionym wyżej elementom certyfikacja cyberbezpieczeństwa stanie się atrakcyjniejsza dla przedsiębiorstw jako skuteczny środek informowania o zapewnieniu cyberbezpieczeństwa produktów i usług ICT. W miarę jak certyfikacja cyberbezpieczeństwa będzie się stawać tańsza, skuteczniejsza i atrakcyjna pod względem komercyjnym, przedsiębiorcy będą mieli większą motywację do poddawania swoich produktów certyfikacji pod kątem zagrożeń w zakresie cyberbezpieczeństwa i w ten sposób do rozpowszechniania lepszych praktyk z dziedziny cyberbezpieczeństwa w procesie projektowania produktów i usług ICT (cyberbezpieczeństwo na etapie projektowania).

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

Zgodnie z dyrektywą w sprawie cyberbezpieczeństwa operatorzy prowadzący działalność w sektorach o kluczowym znaczeniu dla naszej gospodarki i społeczeństwa, takich jak energetyka, transport, zaopatrzenie w wodę pitną i jej dystrybucja, bankowość, infrastruktura rynków finansowych, służba zdrowia oraz infrastruktura cyfrowa, jak również dostawcy usług cyfrowych (tj. wyszukiwarek, usług przetwarzania w chmurze i internetowych platform handlowych), są zobowiązywani podejmować działania w celu właściwego zarządzania ryzykiem w obszarze bezpieczeństwa. Nowe przepisy niniejszego wniosku uzupełniają przepisy dyrektywy w sprawie cyberbezpieczeństwa i zapewniają z nimi spójność, aby wzmocnić odporność UE na zagrożenia dla cyberbezpieczeństwa za pomocą zwiększenia zdolności, ściślejszej współpracy, lepszego zarządzania ryzykiem i podnoszenia poziomu świadomości w kwestii zagrożeń.

Ponadto przepisy dotyczące certyfikacji cyberbezpieczeństwa stanowią ważne narzędzie dla przedsiębiorstw objętych zakresem dyrektywy w sprawie cyberbezpieczeństwa, gdyż będą one mogły poddawać swoje produkty i usługi ICT certyfikacji pod kątem zagrożeń w zakresie cyberbezpieczeństwa w oparciu o systemy certyfikacji cyberbezpieczeństwa ważne i uznawane na terytorium całej UE. Przepisy te będą również uzupełnieniem wymogów bezpieczeństwa, o których mowa w rozporządzeniu eIDAS[17] i dyrektywie w sprawie urządzeń radiowych[18].

- **Spójność z innymi politykami Unii**

W rozporządzeniu (UE) 2016/679 (**ogólnym rozporządzeniu o ochronie danych**)[19] ustanowiono przepisy odnoszące się do ustanawiania mechanizmów certyfikacji oraz znaków

[17] 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.

[18] Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE.

[19] 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 w sprawie swobodnego

jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z tym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Przepisy niniejszego rozporządzenia nie naruszają certyfikacji operacji przetwarzania danych, także wówczas gdy takie operacje są wbudowane w produkty i usługi, zgodnie z ogólnym rozporządzeniem o ochronie danych.

Rozporządzenie objęte niniejszym wnioskiem zapewni spójność z rozporządzeniem (WE) nr 765/2008 w sprawie akredytacji i nadzoru rynku[20] przez odwołanie się do przepisów tych ram prawnych w odniesieniu do krajowych jednostek akredytujących i jednostek oceniających zgodność. W odniesieniu do organów nadzoru w proponowanym rozporządzeniu wprowadza się wymóg wyznaczenia przez państwa członkowskie krajowych organów nadzoru ds. certyfikacji z obowiązkami w zakresie nadzoru, monitorowania i egzekwowania przepisów. Organy te pozostaną podmiotami odrębnymi od jednostek oceniających zgodność, jak określono w rozporządzeniu (WE) nr 765/2008.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawą prawną działania UE jest art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), który odnosi się do zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, do urzeczywistnienia celów określonych w artykule 26 TFUE, mianowicie zapewnienia właściwego funkcjonowania rynku wewnętrznego.

Podstawę prawną ustanowienia ENISA umocowaną w ramach rynku wewnętrznego podtrzymał Trybunał Sprawiedliwości (sprawa C-217/04 Zjednoczone Królestwo przeciwko Parlamentowi Europejskiemu i Radzie) i została ona potwierdzona w rozporządzeniu z 2013 r., ustanawiającym obecny mandat Agencji. Ponadto działania, które odzwierciedlają cele zwiększenia współpracy i koordynacji między państwami członkowskimi, oraz te, które dodają zdolności na szczeblu UE w uzupełnieniu działań państw członkowskich, mieszczą się kategorii „współpracy operacyjnej”. Została ona konkretnie wskazana w dyrektywie w sprawie cyberbezpieczeństwa (dla której podstawą prawną jest art. 114 TFUE) jako cel, do którego należy dążyć, w ramach sieci CSIRT, dla której „ENISA zapewnia sekretariat oraz aktywnie wspiera współpracę” (art. 12 ust. 2). W szczególności w art.12 ust. 3 lit. f) bliżej określono dalsze formy współpracy operacyjnej jako zadania sieci CSIRT, w tym w związku z: (i) kategoriami ryzyk i incydentów; (ii) wczesnym ostrzeganiem; (iii) wzajemną pomocą; oraz (iv) zasadami i uzgodnieniami dotyczącymi koordynacji, gdy państwa członkowskie reagują na transgraniczne ryzyka i incydenty.

- Obecne rozdrobnienie systemów certyfikacji produktów i usług ICT jest także rezultatem braku wspólnych prawnie wiążących i skutecznych ram procesu mających zastosowanie do państw członkowskich. Przeszkadza to w budowaniu rynku wewnętrznego produktów i usług ICT oraz utrudnia konkurowanie europejskiego przemysłu w tym sektorze. Celem niniejszego wniosku jest usunięcie obecnego rozdrobnienia i związanych z nim przeszkód w funkcjonowaniu rynku wewnętrznego

przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1–88).

[20] Rozporządzenie (WE) nr 765/2008 ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93.

przez zapewnienie wspólnych ram do utworzenia systemów certyfikacji cyberbezpieczeństwa obowiązujących w całej UE.

Pomocniczość (w przypadku kompetencji niewyłącznych)

Zasada pomocniczości wymaga oceny konieczności podjęcia działań przez UE i ich wartości dodanej. Poszanowanie zasady pomocniczości w tej dziedzinie zostało już uznane w momencie przyjęcia obecnego rozporządzenia w sprawie ENISA[21].

cyberbezpieczeństwo jest kwestią wspólnego zainteresowania Unii. Współzależności między sieciami i systemami informatycznymi są tego typu, że indywidualne podmioty (zarówno publiczne, jak i prywatne, w tym obywatele) bardzo często nie są w stanie w pojedynkę stawić czoła zagrożeniom, zarządzać ryzykiem i poradzić sobie z ewentualnymi skutkami cyberincydentów. Z jednej strony wzajemne zależności między państwami członkowskimi, w tym w odniesieniu do funkcjonowania infrastruktury krytycznej (energetycznej, transportowej, wodociągowej, aby wymienić tylko niektóre przykłady), powodują, że interwencja publiczna na szczeblu europejskim jest nie tylko korzystna, ale także potrzebna. Z drugiej strony interwencja unijna może wywołać korzystny efekt „rozlewania się" ze względu na wymianę dobrych praktyk między państwami członkowskimi, co może prowadzić do zwiększonego cyberbezpieczeństwa Unii.

Podsumowując, w obecnej sytuacji i biorąc pod uwagę przyszłe scenariusze, wydaje się, że do **wzmocnienia wspólnej odporności na zagrożenia w zakresie cyberbezpieczeństwa** cechującej Unię nie wystarczą **indywidualne działania podejmowane przez państwa członkowskie i rozproszone podejście do cyberbezpieczeństwa**.

Działanie unijne uważa się zatem za konieczne do rozwiązania problemu rozdrobnienia obecnych systemów certyfikacji cyberbezpieczeństwa. Pozwoli ono producentom na korzystanie w pełni z rynku wewnętrznego i przyniesie znaczne oszczędności w zakresie badań i kosztów przeprojektowania. Obecne porozumienie w sprawie wzajemnego uznawania zawarte przez grupę wyższych urzędników ds. bezpieczeństwa systemów informatycznych (SOG-IS) doprowadziło wprawdzie na przykład do osiągnięcia ważnych rezultatów w tej dziedzinie, wykazało jednak również istotne ograniczenia, które stoją na przeszkodzie jego przydatności jako sposobu zapewnienia na dłuższą metę trwałych rozwiązań w zakresie wykorzystania w pełni potencjału rynku wewnętrznego.

Wartość dodana działania na szczeblu unijnym, zwłaszcza dla wzmocnienia współpracy między państwami członkowskimi, ale także między społecznościami z obszaru bezpieczeństwa sieci i informacji, została potwierdzona w konkluzjach Rady z 2016 r.[22] i wynika także wyraźnie z oceny ENISA.

- **Proporcjonalność**

Przewidziane środki nie wykraczają poza to, co jest konieczne do osiągnięcia określonych w nich celów. Poza tym zakres interwencji UE nie narusza żadnych dalszych działań

[21] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004.

[22] Konkluzje Rady w sprawie wzmacniania europejskiego systemu odporności cybernetycznej oraz wspierania konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego, 15 listopada 2016 r.

krajowych w zakresie kwestii związanych z bezpieczeństwem narodowym. Działanie unijne ma zatem uzasadnienie na gruncie zasady pomocniczości i proporcjonalności.

- **Wybór instrumentu**

W niniejszym wniosku dokonuje się przeglądu rozporządzenia (UE) nr 526/2013, w którym określono obecny mandat i zadania ENISA. Ponadto, z uwagi na ważną rolę ENISA w tworzeniu unijnych ram certyfikacji cyberbezpieczeństwa i zarządzaniu nimi, nowy mandat ENISA i wspomniane ramy zostaną najlepiej umocowane w ramach jednego instrumentu prawnego, przy wykorzystaniu instrumentu rozporządzenia.

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

Oceny *ex post*/kontrole sprawności obowiązującego prawodawstwa

Zgodnie z planem oceny[23] Komisja przeanalizowała **istotność, wpływ, skuteczność, wydajność, spójność działań Agencji oraz wartość dodaną** w odniesieniu do osiągnięć Agencji, zarządzania, wewnętrznej struktury organizacyjnej i praktyki działania w latach 2013–2016. Główne ustalenia można podsumować następująco (więcej informacji w dokumencie roboczym służb Komisji, towarzyszącym ocenie skutków).

- **Istotność** W warunkach rozwoju technologicznego i zmieniających się zagrożeń oraz z uwagi na znaczącą potrzebę zwiększenia cyberbezpieczeństwa w UE cele ENISA okazały się istotne. Państwa członkowskie i organy UE faktycznie opierają się na szerokiej wiedzy fachowej Agencji na temat kwestii cyberbezpieczeństwa. Poza tym w państwach członkowskich należy budować potencjał do lepszego rozumienia zagrożeń i reagowania na nie, a zainteresowane strony muszą współpracować przekrojowo w obszarach tematycznych i międzyinstytucjonalnie. Cyberbezpieczeństwo jest nadal kluczowym priorytetem politycznym UE i od ENISA oczekuje się, aby stanowiła na niego odpowiedź, jednakże konstrukcja ENISA jako Agencji funkcjonującej w oparciu o określony czasowo mandat: (i) nie pozwala na długofalowe planowanie i trwałe wsparcie dla państw członkowskich i instytucji unijnych; (ii) może prowadzić do powstania próżni prawnej, ponieważ przepisy dyrektywy w sprawie cyberbezpieczeństwa powierzające ENISA określone zadania mają charakter stały[24]; (iii) jest niespójna z wizją wiążącą ENISA ze wzmocnionym unijnym ekosystemem cyberbezpieczeństwa UE.
- **Skuteczność:** ENISA generalnie spełnia swoje cele i wykonuje swoje zadania. Przyczyniła się do poprawy bezpieczeństwa sieci i informacji w Europie przez swoje główne działania (budowanie zdolności, udostępnianie wiedzy fachowej, tworzenie społeczności i wspieranie działań politycznych). Są jeszcze jednak rezerwy w odniesieniu do doskonalenia każdego z nich. W ocenie stwierdzono, że ENISA skutecznie stworzyła silne i oparte na zaufaniu relacje z niektórymi z zainteresowanych stron, zwłaszcza z państwami członkowskimi i społecznością CSIRT. Działania w obszarze budowania zdolności zostały uznane za skuteczne, zwłaszcza w przypadku państw członkowskich dysponujących mniejszymi zasobami. Pobudzanie szerokiej współpracy było jednym z najbardziej docenianych

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

[24] Odwołanie do art. 7, 9, 11, 12 i 19 dyrektywy w sprawie cyberbezpieczeństwa.

aspektów działalności Agencji – zainteresowane strony zgodnie podkreślały pozytywną rolę, jaką ENISA odgrywała w zacieśnianiu kontaktów. ENISA napotkała jednak trudności w wywarciu znacznego wpływu w obrębie rozległego obszaru bezpieczeństwa sieci i informacji. Przyczyną były też dość ograniczone zasoby ludzkie i finansowe w stosunku do bardzo szeroko zakrojonego mandatu. W ocenie stwierdzono również, że ENISA częściowo osiągnęła cel polegający na zapewnieniu wiedzy fachowej w związku z problemami w rekrutowaniu specjalistów (zob. też poniżej w części dotyczącej wydajności).

- **Wydajność**: Mimo niewielkiego budżetu – jednego z najniższych wśród agencji UE – ENISA zdołała wnieść wkład w realizację zamierzonych celów, wykazując ogólną wydajność w wykorzystywaniu zasobów. Z oceny wynika, że procesy były generalnie skuteczne, a jasne określenie obowiązków w obrębie organizacji prowadziło do prawidłowego wykonywania prac. Jedno z głównych wyzwań dla wydajności ENISA jest związane w trudnościami Agencji z rekrutacją i zatrzymywaniem wysoko wykwalifikowanych specjalistów. Wyniki oceny wykazują, że wynika to z połączenia szeregu czynników, obejmujących ogólne trudności w sektorze publicznym do konkurowania z sektorem prywatnym przy próbach pozyskania wysoko wyspecjalizowanych ekspertów, rodzaj umowy (na czas określony), jaką Agencja może w większości przypadków oferować, i w pewnym sensie dość niski poziom atrakcyjności powodowany miejscem działalności ENISA, związany na przykład z trudnościami, jakie napotykają małżonkowie przy poszukiwaniu pracy. Rozdział siedzib między Atenami i Heraklionem wymagał dodatkowych działań w zakresie koordynacji i powodował powstawanie dodatkowych kosztów, ale przeniesienie w 2013 r. do Aten zasadniczego wydziału operacyjnego zwiększyło operacyjną skuteczność Agencji.
- **Spójność**: Działania ENISA były generalnie spójne z obszarami polityki i działalności zainteresowanych stron zarówno na szczeblu krajowym, jak również unijnym, potrzebne jest jednak bardziej skoordynowane podejście do cyberbezpieczeństwa na szczeblu UE. Potencjał współpracy między ENISA i innymi organami UE nie został jeszcze w pełni wykorzystany. Przemiany unijnego otoczenia prawnego i politycznego sprawiają, że obecny mandat jest mniej spójny.
- **Unijna wartość dodana**: Wartość dodana ENISA polega głównie na zdolności Agencji do ułatwiania współpracy, głównie między państwami członkowskimi, ale również z powiązanymi społecznościami związanymi z bezpieczeństwem sieci i informacji. Na poziomie UE nie ma innego podmiotu, który wspomagałby współpracę tak szerokiego zakresu podmiotów związanych z bezpieczeństwem sieci i informacji. Wartość dodana zapewniana przez Agencję jest zróżnicowana w zależności od potrzeb i zasobów różnych zainteresowanych stron (np. dużych państw członkowskich wobec państw małych; państw członkowskich wobec przemysłu) oraz potrzeby nowego uszeregowania przez Agencję działań pod względem ich ważności. W ocenie stwierdzono, że potencjalne zaprzestanie działalności ENISA mogłoby oznaczać straconą szansę dla wszystkich państw członkowskich. Zapewnienie tego samego poziomu budowania wspólnoty i współpracy między państwami członkowskimi w obszarze cyberbezpieczeństwa nie będzie możliwe. Bez bardziej scentralizowanej agencji UE obraz sytuacji byłby bardziej rozproszony, a rozwijająca się współpraca dwustronna lub regionalna wypełniałaby pustkę pozostałą po działalności ENISA.

W odniesieniu do dotychczasowych osiągnięć i przyszłości ENISA na podstawie przeprowadzonych w 2017 r. konsultacji rysują się następujące główne tendencje[25]:

- Ogólne wyniki działalności ENISA w latach 2013–2016 zostały ocenione pozytywnie przez większość respondentów (74 %). Poza tym większość respondentów uznała, że ENISA osiąga swoje cele (co najmniej 63 % w odniesieniu do każdego z celów). Usługi i produkty ENISA są regularnie (co miesiąc lub częściej) wykorzystywane przez prawie połowę respondentów (46 %) i doceniane ze względu na fakt, iż ich źródłem jest jednostka na szczeblu unijnym (83 %), oraz z racji swojej jakości (62 %).
- Respondenci wskazali szereg niedociągnięć i wyzwań, odnoszących się do przyszłości cyberbezpieczeństwa w UE, jako pięć głównych (wśród 16) najczęściej wymieniano: współpracę między państwami członkowskimi; zdolność do zapobiegania cyberatakom na dużą skalę, ich wykrywania i rozwiązywania problemu; współpracę między państwami członkowskimi w kwestiach związanych z cyberbezpieczeństwem; współpracę i wymianę informacji między różnymi podmiotami, w tym współpracę publiczno-prywatną; ochronę infrastruktury krytycznej przed cyberatakami.
- Znaczna większość (88 %) respondentów była zdania, że obecne instrumenty i mechanizmy dostępne na szczeblu UE są niewystarczające lub jedynie częściowo odpowiednie do rozwiązania tych kwestii. Przeważająca większość respondentów (98 %) wskazywała, że kwestią tych potrzeb powinien się zająć podmiot unijny, a ENISA została uznana przez 99 % respondentów za właściwą do tego organizację.

Konsultacje z zainteresowanymi stronami

- Komisja zorganizowała publiczne konsultacje w sprawie przeglądu ENISA w dniach od 12 kwietnia do 5 lipca 2016 r. i otrzymała 421 odpowiedzi[26]. Z konsultacji wynikało, że 67,5 % respondentów uważa, iż ENISA może odgrywać rolę w tworzeniu zharmonizowanych ram certyfikacji bezpieczeństwa produktów i usług IT.

Wyniki przeprowadzonych w 2016 r. konsultacji na temat cPPP[27] w dziedzinie cyberbezpieczeństwa w części dotyczącej certyfikacji wskazują, że:

---

[25] W konsultacjach uczestniczyło 90 podmiotów z 19 państw członkowskich (udzielono 88 odpowiedzi i przesłano 2 stanowiska); wśród respondentów były organy krajowe z 15 państw członkowskich, m.in. Francji, Włoch, Irlandii i Grecji, oraz 8 organizacji patronackich, reprezentujących znaczną liczbę organizacji europejskich, np. Europejska Federacja Bankowa, stowarzyszenie Digital Europe (reprezentujące sektor technologii cyfrowej w Europie), Europejskie Stowarzyszenie Operatorów Sieci Telekomunikacyjnych (ETNO). Publiczne konsultacje w sprawie ENISA zostały uzupełnione materiałem z kilku innych źródeł, obejmującym: (i) pogłębione wywiady z 50 kluczowymi podmiotami w społeczności cyberbezpieczeństwa; (ii) ankietę adresowaną do sieci CSIRT; (iii) ankietę adresowaną do zarządu i rady wykonawczej ENISA oraz działającej przy niej Stałej Grupy Przedstawicieli Zainteresowanych Stron.

[26] 162 opinie od obywateli, 33 – od organizacji społeczeństwa obywatelskiego oraz organizacji konsumenckich; 186 – od podmiotów branżowych oraz 40 – od organów publicznych, w tym właściwych organów egzekwujących dyrektywę o prywatności i łączności elektronicznej.

[27] Na pytania w sekcji dotyczącej certyfikacji uzyskano odpowiedzi od 240 zainteresowanych stron reprezentujących krajowe administracje publiczne, duże przedsiębiorstwa, MŚP i mikroprzedsiębiorstwa oraz organizacje badawcze

- 50,4 % (tj. 121 spośród 240) respondentów nie wie, czy krajowe systemy certyfikacji są wzajemnie uznawane we wszystkich państwach członkowskich UE. 25,8 % (62 spośród 240) odpowiedziało „Nie”, 23,8 % (57 spośród 240) udzieliło natomiast odpowiedzi „Tak”.
- 37,9 % respondentów (91 spośród 240) uważa, że istniejące systemy certyfikacji nie odpowiadają na potrzeby przemysłu europejskiego. Z drugiej jednak strony, 17,5 % (42 spośród 240) – głównie przedsiębiorstwa o zasięgu globalnym działające na rynku europejskim – było przeciwnego zdania.
- 49,6 % (119 spośród 240) respondentów twierdzi, że wykazanie równoważności norm, systemów certyfikacji i oznakowań nie jest łatwe. 379 % (91 spośród 240) odpowiedziało „Nie wiem”, a jedynie 12,5 % (30 spośród 240) udzieliło odpowiedzi „Tak”.

Gromadzenie i wykorzystanie wiedzy eksperckiej

Komisja uwzględniła następujące dokumenty zawierające opinie ekspertów zewnętrznych:

- Badanie na temat oceny ENISA (Ramboll/Carsa 2017; SMART 20160077).
- *Study on ICT Security Certification and Labelling – Evidence gathering and impact assessment* (Badanie dotyczące etykietowania i certyfikacji ICT – Gromadzenie dowodów i ocena skutków) (PriceWaterhouseCoopers 2017; SMART 2016/0029).

Ocena skutków

- W sprawozdaniu z oceny skutków dotyczącym tej inicjatywy wskazano następujące główne problemy do rozwiązania:
- rozdrobnienie działań politycznych i podejścia do kwestii cyberbezpieczeństwa w różnych państwach członkowskich;
- rozproszenie zasobów i fragmentaryczność podejścia do kwestii cyberbezpieczeństwa w instytucjach, agencjach i organach UE; oraz
- niewystarczający poziom świadomości i wiedzy u obywateli i przedsiębiorstw, w połączeniu z narastającym pojawianiem się wielu krajowych i sektorowych systemów certyfikacji.

W sprawozdaniu oceniono następujące warianty w odniesieniu do mandatu ENISA:

- utrzymanie obecnego stanu, co oznacza rozszerzenie mandatu w dalszym ciągu ograniczone w czasie (wariant podstawowy);
- wygaśnięcie obecnego mandatu ENISA bez jego odnowienia i zakończenie działalności ENISA (brak działań);
- „zreformowana ENISA”; oraz
- agencja UE ds. cyberbezpieczeństwa z pełnymi zdolnościami operacyjnymi.

W sprawozdaniu oceniono następujące warianty w odniesieniu do certyfikacji cyberbezpieczeństwa:

- brak działań (wariant podstawowy);

- środki nielegislacyjne („prawo miękkie”);
- unijny akt prawny w celu utworzenia obowiązkowego systemu dla wszystkich państw członkowskich w oparciu o system SOG-IS; oraz
- unijne ogólne ramy certyfikacji cyberbezpieczeństwa w odniesieniu do ICT.

Z analizy wynikło, że „zreformowana ENISA” w połączeniu z ogólnymi unijnymi ramami certyfikacji bezpieczeństwa ICT jest wariantem preferowanym.

Wariat preferowany został oceniony jako najskuteczniejszy do celów osiągnięcia przez UE zwiększonych zdolności w zakresie cyberbezpieczeństwa, gotowości, współpracy, świadomości zagrożeń, przejrzystości oraz uniknięcia fragmentacji rynku. Uznano go również za najbardziej spójny z priorytetami politycznymi strategii UE w zakresie cyberbezpieczeństwa i związanych z nią działań (np. z dyrektywą w sprawie cyberbezpieczeństwa) oraz ze strategią jednolitego rynku cyfrowego. Ponadto z procesu konsultacji wynikło, że preferowany wariant cieszy się poparciem większości zainteresowanych stron. Poza tym analiza przeprowadzona w ramach oceny skutków wykazała, że preferowany wariant może zapewnić osiągnięcie celów poprzez racjonalne wykorzystywanie zasobów.

Działająca przy Komisji Rada ds. Kontroli Regulacyjnej wydała pierwotnie negatywną opinię w dniu 24 lipca, a następnie pozytywną opinię w dniu 25 sierpnia 2017 r. po ponownym przedłożeniu sprawozdania. W poprawionym sprawozdaniu z oceny skutków uwzględniono dodatkowe dowody, potwierdzające ostateczne wnioski z oceny ENISA, oraz dodatkowe wyjaśnienia na temat wariantów politycznych i ich skutków. W załączniku 1 do sprawozdania końcowego z oceny skutków podsumowano sposób uwzględnienia uwag Rady w drugiej opinii. W szczególności sprawozdanie to zostało uaktualnione, aby przedstawić dokładniej unijny kontekst odnoszący się do cyberbezpieczeństwa, w tym środki ujęte we wspólnym komunikacie „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej” (JOIN(2017) 450) i mające szczególne znaczenie dla ENISA: unijny plan działania w zakresie cyberbezpieczeństwa oraz Europejskie Centrum Badań Naukowych i Kompetencji w dziedzinie Cyberbezpieczeństwa, z którymi Agencja powiązałaby swoją rolę doradczą w odniesieniu do potrzeb badawczych UE.

W sprawozdaniu wyjaśniono, w jaki sposób reforma Agencji, w tym nowe zadania, lepsze warunki zatrudnienia oraz współpraca strukturalna z organami UE z tej dziedziny, podniosłaby jej atrakcyjność jako pracodawcy i pomogła rozwiązać problemy związane z pozyskiwaniem specjalistów. W załączniku nr 6 do sprawozdania przedstawiono również skorygowane szacowane koszty związane z wariantami strategicznymi dotyczącymi ENISA. Jeżeli chodzi o zagadnienie certyfikacji, sprawozdanie zostało poprawione, aby zapewnić bardziej szczegółowe wyjaśnienia, w tym w formie graficznej, dotyczące preferowanego wariantu, a także szacunkowe dane dotyczące kosztów dla państw członkowskich i Komisji, związane z nowymi ramami certyfikacji. Uzasadnienie wyboru ENISA jako kluczowego podmiotu w zakresie ram zostało wyjaśnione bardziej szczegółowo w oparciu o jej wiedzę fachową w tej dziedzinie oraz fakt, że jest ona jedyną agencją na szczeblu UE w zakresie cyberbezpieczeństwa. Przejrzano tez część poświęconą certyfikacji, aby doprecyzować aspekty związane z różnicą między obecnym systemem SOG-IS, wykazać korzyści wynikające z różnych wariantów i wyjaśnić, że rodzaj produktów i usług ICT objętych europejskim systemem certyfikacji zostanie określony w samym zatwierdzonym systemie.

Sprawność regulacyjna i uproszczenie

Nie dotyczy

Wpływ na prawa podstawowe

Cyberbezpieczeństwo odgrywa zasadniczą rolę w zakresie ochrony prywatności i danych osobowych osób fizycznych zgodnie z art. 7 i 8 Karty praw podstawowych Unii Europejskiej. W przypadku cyberincydentów prywatność i ochrona danych osobowych są wyraźnie zagrożone. Dlatego cyberbezpieczeństwo jest warunkiem koniecznym poszanowania prywatności i poufności naszych danych osobowych. W tym ujęciu, mając na celu wzmocnienie cyberbezpieczeństwa w Europie, wniosek stanowi ważne uzupełnienie istniejących przepisów chroniących podstawowe prawo do prywatności i ochrony danych osobowych. Cyberbezpieczeństwo ma również zasadnicze znaczenie dla ochrony poufności łączności elektronicznej i w związku z tym także do korzystania z prawa wolności wypowiedzi i informacji oraz innych powiązanych praw, takich jak prawo do wolności myśli, sumienia i wyznania.

4. WPŁYW NA BUDŻET

Zob. część finansowa

5. ELEMENTY FAKULTATYWNE

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

Komisja będzie monitorować stosowanie rozporządzenia i przedkładać sprawozdanie ze swojej oceny Parlamentowi Europejskiemu i Radzie oraz Europejskiemu Komitetowi Ekonomiczno-Społecznemu co pięć lat. Sprawozdania te będą dostępne dla opinii publicznej i będą zawierały szczegółowy opis skutecznego stosowania i egzekwowania przepisów niniejszego rozporządzenia.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Tytuł I niniejszego rozporządzenia zawiera przepisy ogólne: przedmiot i zakres (art. 1), definicje (art. 2), w tym odniesienia do stosownych definicji z innych instrumentów unijnych, takich jak dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa w sprawie cyberbezpieczeństwa), rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 w sprawie normalizacji europejskiej.

Tytuł II niniejszego rozporządzenia zawiera podstawowe przepisy dotyczące ENISA: Agencji UE ds. Cyberbezpieczeństwa.

W rozdziale I tego tytułu ustanowiono mandat (art. 3), cele (art. 4) i zadania (art. 5–11) Agencji .

W rozdziale II określono organizację ENISA i ujęto podstawowe przepisy odnoszące się do jej struktury (art. 12). Określono skład, zasady głosowania i funkcje zarządu (sekcja 1, art. 13–17), rady wykonawczej (sekcja 2, art. 18) oraz dyrektora wykonawczego (sekcja 3,

art. 19). Rozdział ten zawiera również przepisy dotyczące składu i roli Stałej Grupy Przedstawicieli Zainteresowanych Stron (sekcja 4, art. 20). W sekcji 5 tego rozdziału określono szczegółowe zasady operacyjne Agencji, w tym w odniesieniu do planowania działalności, konfliktu interesów, przejrzystości, poufności i dostępu do dokumentów (art. 25–21).

Rozdział III odnosi się do uchwalania budżetu Agencji i jego struktury (art. 26 i 27), a także zasad jego wykonywania (art. 28 i 29). Ujęto w nim także przepisy ułatwiające zwalczanie nadużyć finansowych, korupcji i innych bezprawnych działań (art. 30).

Rozdział IV odnosi się do pracowników Agencji. Obejmuje on ogólne przepisy regulaminu pracowniczego i warunków zatrudnienia oraz zasad rządzących przywilejami i immunitetami (art. 31 i 32). Sprecyzowano w nim także zasady angażowania i mianowania dyrektora wykonawczego Agencji (art. 33). Rozdział ten zawiera także przepisy regulujące korzystanie z usług oddelegowanych ekspertów krajowych lub innych pracowników niezatrudnionych przez Agencję (art. 34).

Rozdział V zawiera przepisy ogólne odnoszące się do Agencji. Określono w nim status prawny (art. 35) i ujęto przepisy regulujące kwestie odpowiedzialności, uzgodnienia dotyczące języka i ochrony danych osobowych (art. 36–38), a także przepisy bezpieczeństwa odnoszące się do ochrony informacji niejawnych oraz szczególnie chronionych informacji jawnych (art. 40). Opisano zasady współpracy Agencji z państwami trzecimi i organizacjami międzynarodowymi (art. 39). Rozdział ten zawiera również przepisy dotyczące siedziby Agencji i warunków działania, a także kontroli administracyjnej sprawowanej przez Europejskiego Rzecznika Praw Obywatelskich (art. 41 i 42).

Tytuł III rozporządzenia zawiera przepisy ustanawiające status *lex generalis* (art. 1) dla europejskich ram certyfikacji cyberbezpieczeństwa („**ram certyfikacji**”) produktów i usług ICT. W tytule tym określono ogólny cel europejskich systemów certyfikacji cyberbezpieczeństwa, którym jest zapewnienie, aby produkty i usługi ICT były zgodne z określonymi wymogami bezpieczeństwa pod względem odporności, przy danym poziomie pewności, na działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych bądź związanych z nimi funkcji lub usług (art. 43). Ponadto tytuł ten zawiera wykaz celów w zakresie bezpieczeństwa, które mają spełniać europejskie systemy certyfikacji cyberbezpieczeństwa (art. 45), obejmujących m.in.: zdolność do ochrony danych przed przypadkowym lub nieuprawnionym uzyskaniem dostępu lub ujawnieniem, zniszczeniem lub zmianą, oraz treść (tj. elementy) europejskich systemów certyfikacji cyberbezpieczeństwa, np. szczegółowe określenie ich zakresu, cele związane z bezpieczeństwem, kryteria oceny itp. (art. 47).

W tytule III określono również główne skutki prawne europejskich systemów certyfikacji cyberbezpieczeństwa, mianowicie: (i) zobowiązanie do wdrożenia systemu na szczeblu krajowym i dobrowolny charakter certyfikacji; (ii) unieważnienie przez europejskie systemy certyfikacji cyberbezpieczeństwa systemów krajowych w odniesieniu do tych samych produktów lub usług (art. 48 i 49).

Tytuł ten zawiera także ustanowienie procedury przyjęcia europejskich systemów certyfikacji cyberbezpieczeństwa i odnośne role Komisji, ENISA i Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa („Grupy”) (art. 44). W tytule tym ustanowiono też przepisy dotyczące jednostek oceniających zgodność, w tym odnoszących się do nich wymogów, uprawnień i zadań, krajowych organów nadzoru ds. certyfikacji, a także kar.

Przepisami tego samego tytułu ustanowiono również Grupę jako istotny organ składający się z przedstawicieli krajowych organów nadzoru ds. certyfikacji, której głównym zadaniem jest

wspólna z ENISA praca nad przygotowywaniem europejskich systemów certyfikacji cyberbezpieczeństwa oraz doradzanie Komisji na temat ogólnych i szczegółowych kwestii dotyczących polityki certyfikacji cyberbezpieczeństwa.

Tytuł IV rozporządzenia zawiera przepisy końcowe opisujące wykonywanie przekazanych uprawnień, wymogi dotyczące oceny, uchylenie oraz przejęcie praw i obowiązków, a także wejście rozporządzenia w życie.

2017/0225 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie „Agencji UE ds. Cyberbezpieczeństwa” ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa”)

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[28],

uwzględniając opinię Komitetu Regionów[29],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Sieci i systemy informatyczne oraz sieci i usługi telekomunikacyjne odgrywają kluczową rolę w społeczeństwie i stały się podstawą wzrostu gospodarczego. Technologie informacyjno-komunikacyjne stanowią podstawę złożonych systemów wspierających działania społeczne, zapewniają funkcjonowanie naszej gospodarki w kluczowych sektorach, takich jak opieka zdrowotna, energetyka, finanse i transport, a zwłaszcza wspomagają funkcjonowanie rynku wewnętrznego.

(2) Korzystanie z sieci i systemów informatycznych przez obywateli, przedsiębiorstwa i administrację rządową w całej Unii jest obecnie bardzo rozpowszechnione. Digitalizacja i połączalność stają się podstawowymi cechami coraz większej liczby produktów i usług, a wraz z nastaniem internetu rzeczy w następnym dziesięcioleciu spodziewana jest instalacja milionów, jeśli nie miliardów połączonych urządzeń cyfrowych w całej UE. Coraz więcej urządzeń jest połączonych z internetem, a jednocześnie zabezpieczenia i odporność nie są wystarczająco uwzględnione w projektowaniu, co powoduje, że cyberbezpieczeństwo jest niewystarczające. W związku z powyższym ograniczone korzystanie z certyfikacji prowadzi do niewystarczającego informowania użytkowników instytucjonalnych i indywidualnych o właściwościach produktów i usług ICT w zakresie cyberbezpieczeństwa, co podważa zaufanie do rozwiązań cyfrowych.

(3) Coraz większa digitalizacja i połączalność prowadzą do zwiększonych zagrożeń dla cyberbezpieczeństwa, zwiększając tym samym podatność ogółu społeczeństwa na

[28] Dz.U. C [...] z [...], s. [...].
[29] Dz.U. C [...] z [...], s. [...].

cyberzagrożenia i potęgując zagrożenia dla jednostek, w tym osób bardziej podatnych na zagrożenia, takich jak dzieci. W celu ograniczenia tych zagrożeń dla społeczeństwa należy podjąć wszystkie niezbędne działania na rzecz poprawy cyberbezpieczeństwa w UE, aby lepiej chronić przed cyberzagrożeniami sieci i systemy informatyczne, sieci telekomunikacyjne oraz produkty, usługi i urządzenia cyfrowe używane przez obywateli, administrację i przedsiębiorstwa – od MŚP aż po operatorów infrastruktur krytycznych.

(4) Cyberataki nasilają się, a gospodarka oparta na łączności i społeczeństwo, które jest bardziej podatne na cyberzagrożenia i cyberataki, wymagają silniejszej ochrony. Tymczasem jednak, mimo że cyberataki mają często charakter transgraniczny, reakcje polityczne ze strony organów odpowiedzialnych za cyberbezpieczeństwo i kompetencje w zakresie egzekwowania prawa są w głównej mierze krajowe. Cyberincydenty na dużą skalę mogłyby zakłócić świadczenie usług kluczowych w całej UE. Taka sytuacja wymaga skutecznego reagowania oraz zarządzania kryzysowego na szczeblu UE w oparciu o specjalne rozwiązania polityczne oraz szerzej zakrojone instrumenty europejskiej solidarności i wzajemnej pomocy. Ponadto regularna ocena stanu cyberbezpieczeństwa i odporności w Unii, oparta na wiarygodnych danych unijnych oraz na systematycznej prognozie przyszłych zmian, wyzwań i zagrożeń, zarówno na szczeblu unijnym, jak i ogólnoświatowym, ma duże znaczenie dla decydentów politycznych, przemysłu oraz użytkowników.

(5) Wobec narastających wyzwań w zakresie cyberbezpieczeństwa, wobec których stoi Unia, potrzebny jest kompleksowy zestaw środków, które byłyby oparte na wcześniejszych działaniach unijnych i sprzyjały osiąganiu wzajemnie wspierających się celów. Cele te to m.in. potrzeba dodatkowego zwiększenia potencjału i gotowości do reagowania państw członkowskich i przedsiębiorstw oraz poprawy współpracy i koordynacji wśród państw członkowskich oraz instytucji, agencji i organów UE. Ponadto z uwagi na ponadgraniczny charakter cyberzagrożeń konieczne jest zwiększenie na szczeblu Unii tych zdolności, które mogłyby uzupełniać działania państw członkowskich, zwłaszcza w przypadku transgranicznych cyberincydentów na dużą skalę i cyberkryzysów. Potrzebne są również dodatkowe wysiłki na rzecz zwiększenia wiedzy obywateli i przedsiębiorstw o zagadnieniach cyberbezpieczeństwa. Należy poza tym nadal zwiększać zaufanie do jednolitego rynku cyfrowego, oferując przejrzyste informacje o poziomie bezpieczeństwa produktów i usług ICT. Można to ułatwić dzięki ogólnounijnej certyfikacji, ustanawiając wspólne wymogi w zakresie cyberbezpieczeństwa i kryteria oceny na wszystkich rynkach i we wszystkich sektorach krajowych.

(6) W roku 2004 Parlament Europejski i Rada przyjęły rozporządzenie (WE) nr 460/2004[30] ustanawiające ENISA, aby przyczynić się do realizacji celów w zakresie zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji w Unii oraz rozwijania kultury bezpieczeństwa sieci i informacji na rzecz obywateli, konsumentów, przedsiębiorstw oraz administracji publicznej. W roku 2008 Parlament Europejski i Rada przyjęły rozporządzenie (WE) nr 1007/2008[31] przedłużające mandat

[30] 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).

[31] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1007/2008 z dnia 24 września 2008 r. zmieniające rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania (Dz.U. L 293 z 31.10.2008, s. 1)

Agencji do marca 2012 r. Rozporządzeniem (WE) nr 580/2011[32] dodatkowo przedłużono mandat Agencji do dnia 13 września 2013 r. W roku 2013 Parlament Europejski i Rada przyjęły rozporządzenie (UE) nr 526/2013[33] w sprawie ENISA oraz uchylające rozporządzenie (WE) nr 460/2004, którym przedłużono mandat Agencji do czerwca 2020 r.

(7) Unia przedsięwzięła już istotne kroki w celu zapewnienia cyberbezpieczeństwa i zwiększenia zaufania do technologii cyfrowych. W roku 2013 przyjęto strategię UE w zakresie cyberbezpieczeństwa, dyktującą reakcję polityczną Unii na cyberzagrożenia i cyberryzyko. W ramach starań, aby lepiej chronić obywateli europejskich w internecie, Unia przyjęła w roku 2016 pierwszy akt ustawodawczy w dziedzinie cyberbezpieczeństwa – dyrektywę (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii („dyrektywę w sprawie cyberbezpieczeństwa"). W dyrektywie w sprawie cyberbezpieczeństwa wprowadzono wymogi dotyczące zdolności krajowych w dziedzinie cyberbezpieczeństwa, ustanowiono pierwsze mechanizmy zacieśniania strategicznej i operacyjnej współpracy państw członkowskich oraz wprowadzono obowiązki dotyczące środków bezpieczeństwa i zgłaszania incydentów w podstawowych dla gospodarki i społeczeństwa sektorach, takich jak energetyka, transport, zaopatrzenie w wodę, bankowość, infrastruktury rynku finansowego, opieka zdrowotna, infrastruktura cyfrowa, jak też w odniesieniu do dostawców kluczowych usług cyfrowych (wyszukiwarek, usług przetwarzania w chmurze i internetowych platform handlowych). Kluczową rolę we wspieraniu wdrażania tej dyrektywy wyznaczono agencji ENISA. Skuteczna walka z cyberprzestępczością stanowi ponadto ważny priorytet Europejskiej agendy bezpieczeństwa, przyczyniając się do realizacji ogólnego celu, jakim jest osiągnięcie wysokiego poziomu cyberbezpieczeństwa.

(8) Jest rzeczą wiadomą, że od czasu przyjęcia w 2013 r. strategii UE w zakresie bezpieczeństwa cybernetycznego oraz ostatniej zmiany mandatu Agencji ogólny kontekst polityczny znacznie się zmienił, również w związku z bardziej niepewnym i mniej bezpiecznym otoczeniem ogólnoświatowym. W tych warunkach i w ramach nowej unijnej polityki w zakresie cyberbezpieczeństwa konieczne jest dokonanie przeglądu mandatu agencji ENISA, aby określić jej rolę w zmienionym ekosystemie cyberbezpieczeństwa i zapewnić jej skuteczny wkład w reakcję Unii na wyzwania w dziedzinie cyberbezpieczeństwa wynikające z tego radykalnie przekształconego profilu zagrożeń, w odniesieniu do którego, jak uznano w ocenie, jakiej poddano Agencję, obecny mandat nie jest wystarczający.

(9) Agencja ustanowiona niniejszym rozporządzeniem powinna być następcą agencji ENISA ustanowionej rozporządzeniem (UE) nr 526/2013. Agencja powinna wykonywać zadania powierzone jej na mocy niniejszego rozporządzenia oraz aktów prawnych Unii w dziedzinie cyberbezpieczeństwa poprzez, między innymi, zapewnianie wiedzy fachowej i doradztwa oraz działanie w charakterze unijnego centrum informacji i wiedzy. Powinna ona propagować wymianę najlepszych praktyk

---

[32] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 580/2011 z dnia 8 czerwca 2011 r. zmieniające rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania (Dz.U. L 165 z 24.6.2011, s. 3).

[33] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 (Dz.U. L 165 z 18.6.2013, s. 41).

między państwami członkowskimi i prywatnymi zainteresowanymi stronami, przedstawiając Komisji Europejskiej i państwom członkowskim sugestie dotyczące polityki, działając jako punkt odniesienia dla unijnych sektorowych inicjatyw strategicznych odnoszących się do kwestii cyberbezpieczeństwa oraz wspierając współpracę operacyjną pomiędzy państwami członkowskimi oraz między państwami członkowskimi a instytucjami, agencjami i organami UE.

(10) W decyzji 2004/97/WE, Euratom przyjętej na posiedzeniu Rady Europejskiej w dniu 13 grudnia 2003 r. przedstawiciele państw członkowskich postanowili, że ENISA będzie miała siedzibę w Grecji, w mieście, które określić ma rząd grecki. Państwo członkowskie przyjmujące Agencję powinno zapewnić jej możliwie najlepsze warunki sprawnego i skutecznego działania. Właściwa lokalizacja Agencji ma zasadnicze znaczenie dla prawidłowego i skutecznego wykonywania przez nią zadań, naboru i zatrzymania pracowników oraz zwiększenia efektywności sieci współpracy, zapewniając między innymi odpowiednie połączenia transportowe i infrastrukturę dla małżonków i dzieci towarzyszących pracownikom Agencji. Umowa między Agencją a przyjmującym państwem członkowskim, zawarta po uzyskaniu zgody zarządu Agencji, powinna zawierać niezbędne uzgodnienia w tym zakresie.

(11) Ze względu na narastające wyzwania w zakresie cyberbezpieczeństwa, z jakimi boryka się Unia, należy zwiększyć przydzielone Agencji zasoby finansowe i ludzkie, aby odzwierciedlić jej poszerzoną rolę i zadania oraz jej kluczową pozycję w ekosystemie organizacji chroniących europejski ekosystem cyfrowy.

(12) Agencja powinna rozwijać i utrzymywać wysoki poziom wiedzy fachowej oraz działać jako punkt odniesienia służący budowie zaufania i wiarygodności na jednolitym rynku z racji swojej niezależności, jakości oferowanego doradztwa i rozpowszechnianych informacji, przejrzystości procedur i metod działania, a także staranności w realizacji swoich zadań. Agencja powinna aktywnie włączać się w działania krajowe i unijne, a jednocześnie wykonywać swoje zadania w pełnej współpracy z instytucjami, organami i jednostkami organizacyjnymi Unii oraz państwami członkowskimi. Ponadto Agencja powinna bazować na wkładzie i współpracy ze strony sektora prywatnego, jak również innych odpowiednich zainteresowanych stron. Zakres zadań powinien określać sposób, w jaki Agencja ma osiągnąć swoje cele, pozwalając jej jednocześnie na elastyczne działanie.

(13) Agencja powinna wspomagać Komisję poprzez doradztwo, opinie i analizy we wszystkich sprawach Unii związanych z opracowywaniem, aktualizacją i przeglądem polityki i prawa w dziedzinie cyberbezpieczeństwa, w tym w zakresie ochrony infrastruktury krytycznej oraz cyberodporności. Agencja powinna działać jako punkt odniesienia w zakresie doradztwa i wiedzy fachowej na rzecz unijnych sektorowych inicjatyw w dziedzinie polityki i prawa, dotyczących kwestii związanych z cyberbezpieczeństwem.

(14) Podstawowym zadaniem Agencji jest wspieranie konsekwentnego wprowadzania odpowiednich ram prawnych, a w szczególności skutecznego wdrożenia dyrektywy w sprawie cyberbezpieczeństwa, co ma kluczowe znaczenie dla zwiększenia cyberodporności. W obliczu szybko ewoluującego profilu cyberzagrożeń jasne jest, że państwa członkowskie muszą mieć wsparcie w postaci bardziej kompleksowego, przekrojowego pod względem politycznym podejścia do budowania cyberodporności.

(15) Agencja powinna wspierać państwa członkowskie oraz unijne instytucje, organy i jednostki organizacyjne w ich staraniach na rzecz budowy i umocnienia zdolności i gotowości do zapobiegania problemom i incydentom w dziedzinie

cyberbezpieczeństwa, wykrywania ich i reagowania na nie oraz w odniesieniu do bezpieczeństwa sieci i systemów informatycznych. Agencja powinna w szczególności wspierać rozwój i wzmocnienie krajowych CSIRT z myślą o osiągnięciu wysokiego wspólnego poziomu ich zaawansowania w Unii. Agencja powinna również pomagać w opracowaniu i aktualizacji strategii Unii i państw członkowskich w zakresie bezpieczeństwa sieci i systemów informatycznych, w szczególności w odniesieniu do cyberbezpieczeństwa, propagować ich upowszechnienie i śledzić postępy w ich realizacji. Agencja powinna również oferować szkolenia i materiały szkoleniowe organom publicznym, a w razie potrzeby „szkolić szkoleniowców", aby pomóc państwom członkowskim w rozwoju własnych zdolności szkoleniowych.

(16) Agencja powinna wspierać grupę współpracy ustanowioną na mocy dyrektywy w sprawie cyberbezpieczeństwa w wykonywaniu jej zadań, w szczególności poprzez zapewnianie wiedzy fachowej i doradztwa oraz ułatwianie wymiany najlepszych praktyk, zwłaszcza w odniesieniu do identyfikowania przez państwa członkowskie operatorów usług kluczowych, w tym odnośnie do transgranicznych zależności, dotyczących ryzyk i incydentów.

(17) Z myślą o pobudzaniu współpracy między sektorem publicznym a prywatnym oraz w ramach sektora prywatnego, aby w szczególności wspierać ochronę infrastruktur krytycznych, Agencja powinna ułatwiać ustanowienie sektorowych ośrodków wymiany i analizy informacji, udostępniając najlepsze praktyki i oferując wytyczne na temat dostępnych narzędzi i procedur oraz sposobu traktowania kwestii regulacyjnych związanych z wymianą informacji.

(18) Agencja powinna gromadzić i analizować raporty krajowe przekazywane przez CSIRT i CERT-UE, ustalając wspólne zasady, język i terminologię do celów wymiany informacji. Agencja powinna również angażować sektor prywatny, działając w ramach wyznaczonych przez dyrektywę w sprawie cyberbezpieczeństwa, w której wraz z utworzeniem sieci CSIRT położono podstawy pod dobrowolną wymianę informacji technicznych na poziomie operacyjnym.

(19) Agencja powinna wnosić wkład w reakcję na szczeblu UE w przypadku transgranicznych cyberincydentów na dużą skalę i cyberkryzysów. Funkcja ta powinna obejmować gromadzenie odpowiednich informacji i działanie w charakterze pośrednika ułatwiającego współpracę sieci CSIRT i środowiska technicznego, jak również decydentów odpowiedzialnych za zarządzanie w sytuacji kryzysowej. Agencja mogłaby ponadto wspierać postępowania w przypadku incydentów z perspektywy technicznej, ułatwiając odpowiednią wymianę rozwiązań technicznych między państwami członkowskimi i oferując wkład w komunikację publiczną. Agencja powinna wspierać cały ten proces, testując sposoby takiej współpracy poprzez przeprowadzanie corocznych ćwiczeń w dziedzinie cyberbezpieczeństwa.

(20) Aby wykonywać swoje zadania operacyjne, Agencja powinna korzystać z dostępnej wiedzy fachowej CERT-UE w ramach strukturalnej współpracy i w bezpośredniej styczności. Współpraca strukturalna ułatwi powstanie niezbędnej synergii i poszerzenie wiedzy fachowej agencji ENISA. W stosownych przypadkach należy poczynić specjalne ustalenia między obiema tymi organizacjami, aby określić sposób praktycznej realizacji takiej współpracy.

(21) Zgodnie ze swoimi zadaniami operacyjnymi Agencja powinna być w stanie zapewniać wsparcie państwom członkowskim, na przykład oferując doradztwo lub pomoc techniczną, bądź zapewniając analizy zagrożeń i incydentów. W zaleceniu Komisji w sprawie skoordynowanego reagowania na cyberincydenty na dużą skalę

i cyberkryzysy zaleca się, aby państwa członkowskie współpracowały w dobrej wierze i bez zbędnej zwłoki wymieniały między sobą i z agencją ENISA informacje o cyberincydentach na dużą skalę i cyberkryzysach. Takie informacje powinny dodatkowo pomóc agencji ENISA w wykonywaniu zadań operacyjnych.

(22) Jako element regularnej współpracy na poziomie technicznym służącej wzmocnieniu unijnej orientacji sytuacyjnej Agencja powinna regularnie przygotowywać techniczny raport sytuacyjny na temat cyberbezpieczeństwa w UE dotyczący incydentów i zagrożeń, oparty na publicznie dostępnych informacjach, swojej własnej analizie i sprawozdaniach przekazanych przez CSIRT państw członkowskich (na zasadzie dobrowolności) lub pojedyncze punkty kontaktowe powołane zgodnie z dyrektywą w sprawie cyberbezpieczeństwa, Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu i CERT-UE oraz – w stosownych przypadkach – Centrum Analiz Wywiadowczych Unii Europejskiej (INTCEN) Europejskiej Służby Działań Zewnętrznych (ESDZ). Raport ten należy udostępniać odpowiednim instancjom Rady, Komisji, Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa oraz sieci CSIRT.

(23) Techniczne postępowania wyjaśniające *ex post* dotyczące incydentów o istotnych skutkach w więcej niż jednym państwie członkowskim, wspierane lub podejmowane przez Agencję na wniosek lub za zgodą zainteresowanych państw członkowskich, powinny się koncentrować na zapobieganiu przyszłym incydentom i być przeprowadzane bez uszczerbku dla jakichkolwiek postępowań sądowych lub administracyjnych mających na celu przypisanie winy lub odpowiedzialności.

(24) Zainteresowane państwa członkowskie powinny zapewniać Agencji informacje i pomoc niezbędne do celów postępowań wyjaśniających, bez uszczerbku dla postanowień art. 346 Traktatu o funkcjonowaniu Unii Europejskiej lub innych względów porządku publicznego.

(25) Państwa członkowskie mogą wzywać przedsiębiorstwa, których dotyczy dany incydent, do współpracy, polegającej na zapewnieniu Agencji niezbędnych informacji i pomocy, bez uszczerbku dla ich prawa do ochrony szczególnie chronionych informacji handlowych.

(26) Aby lepiej pojmować wyzwania w dziedzinie cyberbezpieczeństwa i z myślą o zapewnianiu strategicznego długoterminowego doradztwa państwom członkowskim i instytucjom Unii, Agencja musi analizować bieżące i pojawiające się zagrożenia. W tym celu Agencja powinna, we współpracy z państwami członkowskimi oraz, w stosownych przypadkach, z urzędami statystycznymi i innymi podmiotami, gromadzić odpowiednie informacje, przeprowadzać analizy powstających technologii oraz zapewniać oceny tematyczne dotyczące spodziewanego wpływu społecznego, prawnego, gospodarczego i regulacyjnego wywieranego przez innowacje technologiczne na bezpieczeństwo sieci i informacji, a w szczególności na cyberbezpieczeństwa. Agencja powinna ponadto – poprzez przeprowadzanie analiz zagrożeń i incydentów – wspierać państwa członkowskie oraz instytucje, agencje i organy Unii w identyfikowaniu pojawiających się tendencji i zapobieganiu problemom związanym z cyberbezpieczeństwem.

(27) W celu wzmocnienia odporności Unii Agencja powinna przyczyniać się do osiągnięcia doskonałości w dziedzinie bezpieczeństwa infrastruktury internetowej i infrastruktur krytycznych, zapewniając doradztwo, wytyczne i najlepsze praktyki. Z myślą o zapewnieniu łatwiejszego dostępu do bardziej usystematyzowanych informacji na temat zagrożeń dla cyberbezpieczeństwa i potencjalnych środków

zaradczych Agencja powinna rozwijać i utrzymywać unijny „węzeł informacyjny” – portal stanowiący punkt kompleksowej obsługi zapewniający ogółowi społeczeństwa informacje na temat cyberbezpieczeństwa pochodzące od unijnych i krajowych instytucji, agencji i organów.

(28) Agencja powinna działać na rzecz podniesienia poziomu świadomości ogółu społeczeństwa na temat różnych postaci ryzyka związanego z cyberbezpieczeństwem i przedstawiać skierowane do obywateli i organizacji wytyczne na temat dobrych praktyk, które powinni stosować użytkownicy końcowi. Agencja powinna również przyczyniać się do propagowania najlepszych praktyk i rozwiązań na poziomie jednostek i organizacji poprzez gromadzenie i analizowanie publicznie dostępnych informacji dotyczących istotnych incydentów oraz poprzez sporządzanie raportów w celu dostarczenia wytycznych przedsiębiorstwom i obywatelom oraz poprawy ogólnego poziomu gotowości i odporności. Agencja powinna ponadto organizować, we współpracy z państwami członkowskimi oraz instytucjami, organami i jednostkami organizacyjnymi Unii, regularne działania informacyjne i publiczne kampanie edukacyjne skierowane do użytkowników końcowych, mające na celu propagowanie bezpieczniejszych zachowań użytkowników w internecie oraz podnoszenie poziomu wiedzy o potencjalnych zagrożeniach występujących w cyberprzestrzeni, w tym o cyberprzestępstwach takich jak ataki phishingowe (wyłudzanie informacji), botnety oraz oszustwa finansowe i bankowe, a także mające na celu promocję podstawowego doradztwa w kwestii uwierzytelniania i ochrony danych. Agencja powinna odgrywać centralną rolę w przyspieszaniu rozwoju wiedzy użytkowników końcowych na temat bezpieczeństwa urządzeń.

(29) W celu wspierania przedsiębiorstw działających w sektorze cyberbezpieczeństwa, jak również użytkowników rozwiązań w tym zakresie, Agencja powinna rozwijać i utrzymywać „centrum monitorowania rynku” poprzez przeprowadzanie regularnych analiz i upowszechnianie wiedzy o głównych tendencjach na rynku cyberbezpieczeństwa, zarówno po stronie popytu, jak i podaży.

(30) Dla zapewnienia pełnej realizacji swoich celów Agencja powinna współpracować z odpowiednimi instytucjami, agencjami i organami, w tym z CERT-UE, Europejskim Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu, Europejską Agencją Obrony (EDA), Europejską Agencją ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi (eu-LISA), Europejską Agencją Bezpieczeństwa Lotniczego (EASA) i każdą inną agencją UE zaangażowaną w kwestie cyberbezpieczeństwa. Agencja powinna również współpracować z organami zajmującymi się ochroną danych, aby wymieniać know-how i najlepsze praktyki oraz zapewniać doradztwo dotyczące tych aspektów cyberbezpieczeństwa, które mogą mieć wpływ na ich pracę. Przedstawiciele krajowych i unijnych organów ds. egzekwowania prawa oraz ochrony danych powinni być uprawnieni do przynależności do istniejącej przy Agencji Stałej Grupy Przedstawicieli Zainteresowanych Stron. Utrzymując kontakty z organami egzekwowania prawa w kwestiach z zakresu bezpieczeństwa sieci i informacji, które mogłyby mieć wpływ na ich pracę, Agencja powinna respektować istniejące kanały informacji i ustanowione sieci.

(31) Agencja jako członek, który ponadto zapewnia sieci CSIRT obsługę sekretariatu, powinna wspierać CSIRT państw członkowskich i CERT-UE we współpracy operacyjnej dotyczącej wszystkich odpowiednich zadań sieci CSIRT określonych w dyrektywie w sprawie cyberbezpieczeństwa. Agencja powinna ponadto propagować i wspierać współpracę między odpowiednimi zespołami CSIRT w przypadku incydentów, ataków bądź zakłóceń dotyczących sieci lub infrastruktury zarządzanej

lub chronionej przez zespoły CSIRT i angażujących lub potencjalnie angażujących co najmniej dwa zespoły CSIRT, z należytym uwzględnieniem standardowych procedur operacyjnych sieci CSIRT.

(32) W celu zwiększenia gotowości Unii do reagowania na cyberincydenty Agencja powinna organizować coroczne ćwiczenia w dziedzinie cyberbezpieczeństwa na szczeblu unijnym i wspierać państwa członkowskie oraz instytucje, agencje i organy UE – na ich wniosek – przy organizacji ćwiczeń.

(33) Agencja powinna dodatkowo rozwijać i utrzymywać swoją wiedzę fachową w dziedzinie certyfikacji cyberbezpieczeństwa w celu wspierania polityki Unii w tej dziedzinie. Agencja powinna propagować wprowadzenie certyfikacji cyberbezpieczeństwa w Unii, w tym poprzez przyczynianie się do utworzenia i utrzymywania ram certyfikacji cyberbezpieczeństwa na szczeblu unijnym, z myślą o zwiększeniu przejrzystości w zakresie zapewniania cyberbezpieczeństwa produktów i usług ICT i zwiększeniu dzięki temu zaufania do wewnętrznego rynku cyfrowego.

(34) Skuteczna polityka cyberbezpieczeństwa powinna opierać się na dobrze opracowanych metodach oceny ryzyka, zarówno w sektorze publicznym, jak i prywatnym. Metody oceny ryzyka są używane na różnych poziomach bez wspólnej praktyki dotyczącej sposobu ich skutecznego stosowania. Propagowanie i rozwój najlepszych praktyk w zakresie oceny ryzyka oraz interoperacyjnych rozwiązań w zakresie zarządzania ryzykiem w organizacjach sektora publicznego i prywatnego zwiększy poziom cyberbezpieczeństwa w Unii. W tym celu Agencja powinna wspierać współpracę między zainteresowanymi stronami na szczeblu Unii, ułatwiając im utworzenie i wprowadzenie europejskich i międzynarodowych norm dotyczących zarządzania ryzykiem oraz wymiernych wskaźników bezpieczeństwa produktów, systemów, sieci i usług elektronicznych, które wraz z oprogramowaniem współtworzą sieć i systemy informatyczne.

(35) Agencja powinna zachęcać państwa członkowskie i usługodawców do podnoszenia ich ogólnych standardów bezpieczeństwa, tak aby wszyscy użytkownicy internetu mogli zastosować niezbędne kroki celem zapewnienia sobie własnego cyberbezpieczeństwa. Dostawcy usług i wytwórcy produktów powinni w szczególności wycofywać lub przetwarzać produkty i usługi niespełniające norm cyberbezpieczeństwa. We współpracy z właściwymi organami ENISA może rozpowszechniać informacje dotyczące poziomu cyberbezpieczeństwa produktów i usług oferowanych na rynku wewnętrznym oraz wydawać ostrzeżenia skierowane do dostawców i producentów, żądając od nich poprawy poziomu bezpieczeństwa – w tym cyberbezpieczeństwa – ich produktów i usług.

(36) Agencja powinna w pełni uwzględniać bieżącą działalność w zakresie badań naukowych, rozwoju i oceny technologicznej, w szczególności prowadzoną w ramach różnych unijnych inicjatyw badawczych, w celu doradzania instytucjom, organom i jednostkom organizacyjnym Unii, a także – w stosownych przypadkach i na ich wniosek – państwom członkowskim w kwestii potrzeb badawczych w dziedzinie bezpieczeństwa sieci i informacji, a w szczególności cyberbezpieczeństwa.

(37) Problemy cyberbezpieczeństwa mają charakter globalny. Istnieje potrzeba zacieśnienia współpracy międzynarodowej w celu poprawy norm bezpieczeństwa – w tym zdefiniowania wspólnych norm zachowania – oraz wymiany informacji, propagowania sprawniejszej współpracy międzynarodowej w reakcji na kwestie bezpieczeństwa sieci i informacji oraz w celu wypracowania wspólnego globalnego podejścia do tych kwestii. W tym celu Agencja powinna wspierać dalsze zaangażowanie Unii oraz

współpracę z państwami trzecimi i organizacjami międzynarodowymi, udostępniając, w stosownych przypadkach, właściwym instytucjom, organom i jednostkom organizacyjnym Unii niezbędną wiedzę fachową i analizy.

(38) Agencja powinna być w stanie odpowiadać na wchodzące w zakres celów Agencji doraźne wnioski o doradztwo i pomoc ze strony państw członkowskich oraz instytucji, agencji i organów UE.

(39) Konieczne jest wdrożenie określonych zasad dotyczących zarządzania Agencją, aby spełnić wymogi wspólnego oświadczenia i wspólnego podejścia, uzgodnionych w ramach międzyinstytucjonalnej grupy roboczej ds. agencji zdecentralizowanych UE w lipcu 2012 r., których celem jest usprawnienie działań agencji i zwiększenie ich skuteczności. Wspólne oświadczenie i wspólne podejście powinny również znaleźć odpowiednie odzwierciedlenie w programach prac Agencji, jej ocenach, a także w sprawozdawczości Agencji i jej praktyce administracyjnej.

(40) Zarząd składający się z przedstawicieli państw członkowskich i Komisji powinien określać ogólny kierunek działalności Agencji oraz zapewniać, aby wykonywała ona swoje zadania zgodnie z niniejszym rozporządzeniem. Zarząd powinien posiadać uprawnienia niezbędne do uchwalania budżetu, kontroli jego wykonania, przyjmowania stosownych przepisów finansowych, ustalania przejrzystych procedur pracy w zakresie podejmowania decyzji przez Agencję, przyjmowania jednolitego dokumentu programowego Agencji, uchwalania jej regulaminu wewnętrznego, powoływania dyrektora wykonawczego oraz podejmowania decyzji o przedłużeniu jego kadencji lub jej zakończeniu.

(41) Aby Agencja mogła prawidłowo i skutecznie funkcjonować, Komisja i państwa członkowskie powinny zapewnić, aby osoby, które mają zostać powołane na członków zarządu, posiadały odpowiednią zawodową wiedzę fachową i doświadczenie w dziedzinach funkcjonalnych. Komisja i państwa członkowskie powinny również dołożyć starań, aby ograniczyć rotację swoich przedstawicieli w zarządzie, tak aby zapewnić ciągłość jego pracy.

(42) Sprawne funkcjonowanie Agencji wymaga, aby dyrektor wykonawczy był powoływany w oparciu o względy merytoryczne oraz udokumentowane umiejętności administracyjne i zarządcze, a także kompetencje i doświadczenie w zakresie cyberbezpieczeństwa, oraz aby wykonywał swoje obowiązki w sposób całkowicie niezależny. Dyrektor wykonawczy powinien opracowywać propozycję programu prac Agencji, po uprzednim zasięgnięciu opinii Komisji, oraz podjąć wszystkie niezbędne czynności w celu zapewnienia prawidłowego wykonania tego programu. Dyrektor wykonawczy powinien przygotowywać sprawozdanie roczne przedkładane zarządowi, sporządzać projekt preliminarza dochodów i wydatków Agencji oraz wykonywać budżet. Dyrektor wykonawczy powinien mieć ponadto możliwość powoływania grup roboczych *ad hoc* w celu rozwiązywania określonych kwestii, w szczególności o charakterze naukowym, technicznym, prawnym lub społeczno-gospodarczym. Dyrektor wykonawczy powinien zapewnić, aby członkowie grup roboczych *ad hoc* byli wybierani według najbardziej rygorystycznych kryteriów dotyczących kompetencji zawodowych, z należytym uwzględnieniem zrównoważonej reprezentacji – w zależności od specyfiki rozpatrywanych kwestii – przedstawicieli administracji publicznej państw członkowskich, instytucji Unii i sektora prywatnego, w tym przemysłu, użytkowników oraz ekspertów akademickich w dziedzinie bezpieczeństwa sieci i informacji.

(43) Rada wykonawcza powinna przyczyniać się do skutecznego funkcjonowania zarządu. W ramach swoich prac przygotowawczych dotyczących decyzji zarządu powinna ona szczegółowo badać odpowiednie informacje, analizować dostępne warianty oraz oferować doradztwo i rozwiązania w celu przygotowania odpowiednich decyzji zarządu.

(44) Agencja powinna posiadać organ doradczy w postaci Stałej Grupy Przedstawicieli Zainteresowanych Stron w celu zapewnienia regularnego dialogu z sektorem prywatnym, organizacjami konsumenckimi i innymi odpowiednimi zainteresowanymi stronami. Stała Grupa Przedstawicieli Zainteresowanych Stron, ustanowiona przez zarząd na wniosek dyrektora wykonawczego, powinna skupiać się na zagadnieniach istotnych dla zainteresowanych stron i kierować na nie uwagę Agencji. Skład Stałej Grupy Przedstawicieli Zainteresowanych Stron oraz przydzielone jej zadania, w tym fakt zasięgania jej opinii w szczególności w sprawie projektu programu prac, powinny zapewniać wystarczającą reprezentację zainteresowanych stron w pracach Agencji.

(45) Agencja powinna posiadać przepisy dotyczące zapobiegania konfliktom interesów i zarządzania nimi. Agencja powinna również stosować odpowiednie przepisy unijne dotyczące publicznego dostępu do dokumentów zawarte w rozporządzeniu (WE) nr 1049/2001 Parlamentu Europejskiego i Rady[34]. Przetwarzanie danych osobowych przez Agencję powinno podlegać przepisom rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[35]. Agencja powinna przestrzegać przepisów mających zastosowanie do instytucji Unii oraz przepisów krajowych dotyczących postępowania z informacjami, w szczególności z szczególnie chronionymi informacjami jawnymi i informacjami niejawnymi UE.

(46) W celu zagwarantowania pełnej autonomii i niezależności Agencji oraz umożliwienia jej wykonywania dodatkowych oraz nowych zadań, w tym również nieprzewidzianych, nagłych zadań nadzwyczajnych, należy przyznać Agencji wystarczający i niezależny budżet, którego dochody pochodziłyby przede wszystkim z wkładu Unii oraz z wkładów państw trzecich uczestniczących w pracach Agencji. Większość personelu Agencji powinna pracować bezpośrednio przy operacyjnym wykonywaniu jej mandatu. Przyjmujące państwo członkowskie bądź jakiekolwiek inne państwo członkowskie powinno mieć możliwość dobrowolnego wnoszenia wkładu na rzecz dochodów Agencji. Procedura budżetowa Unii powinna nadal mieć zastosowanie do wszelkich dotacji pochodzących z budżetu ogólnego Unii. Ponadto Trybunał Obrachunkowy powinien przeprowadzać kontrolę sprawozdań finansowych Agencji w celu zapewnienia przejrzystości i odpowiedzialności.

(47) Ocena zgodności jest to proces wykazujący, czy zostały spełnione określone wymagania odnoszące się do produktu, procesu, usługi, systemu, osoby lub jednostki. Do celów niniejszego rozporządzenia certyfikację należy traktować jako rodzaj oceny zgodności odnoszącej się do właściwości danego produktu, procesu, usługi, systemu lub ich połączenia („produktów i usług ICT") w zakresie cyberbezpieczeństwa, przeprowadzanej przez niezależną stronę trzecią, inną niż wytwórca produktu lub

---

[34] 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).

[35] Dz.U. L 8 z 12.1.2001, s. 1.

dostawca usług. Certyfikacja nie jest w stanie sama w sobie zagwarantować cyberbezpieczeństwa produktów i usług ICT. Poświadczanie, że produkty i usługi ICT zostały zbadane i że spełniają określone wymogi w zakresie cyberbezpieczeństwa ustanowione w innych regulacjach, na przykład określone w normach technicznych, jest raczej rolą procedury i metodyki technicznej.

(48) Certyfikacja cyberbezpieczeństwa odgrywa ważną rolę, jeżeli chodzi o zwiększanie zaufania do produktów i usług ICT oraz ich bezpieczeństwa. Jednolity rynek cyfrowy, a w szczególności gospodarka oparta na danych i internet rzeczy, mogą się prawidłowo rozwijać jedynie wtedy, gdy istnieje ogólne publiczne zaufanie, że takie produkty i usługi zapewniają określony poziom pewności co do ich cyberbezpieczeństwa. Połączone z siecią i zautomatyzowane pojazdy, elektroniczne wyroby medyczne, systemy sterowania automatyki przemysłowej lub też inteligentne sieci stanowią tylko niektóre przykłady sektorów, w których certyfikacja jest już szeroko stosowana lub najprawdopodobniej będzie stosowana w najbliższej przyszłości. Sektory regulowane przepisami dyrektywy w sprawie cyberbezpieczeństwa są również sektorami, w których certyfikacja cyberbezpieczeństwa ma krytyczne znaczenie.

(49) W komunikacie z roku 2016 „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego” Komisja przedstawiła potrzebę wysokojakościowych, dostępnych cenowo i interoperacyjnych produktów i rozwiązań w dziedzinie cyberbezpieczeństwa. Podaż produktów i usług ICT na jednolitym rynku jest wciąż bardzo nierównomierna pod względem geograficznym. Jest to spowodowane tym, że branża cyberbezpieczeństwa w Europie rozwijała się głównie w oparciu o krajowe zamówienia rządowe. Do luk mających wpływ na jednolity rynek cyberbezpieczeństwa należy ponadto – między innymi – brak interoperacyjnych rozwiązań (norm technicznych), praktyk i ogólnounijnych mechanizmów certyfikacji. Z jednej strony sprawia to, że przedsiębiorstwa europejskie mają trudności w konkurowaniu na poziomie krajowym, europejskim i globalnym. Z drugiej strony sytuacja ta powoduje, że wybór opłacalnych i nadających się do użytku technologii z dziedziny cyberbezpieczeństwa, do których mają dostęp jednostki i przedsiębiorstwa, jest ograniczony. Podobnie w przeglądzie śródokresowym realizacji strategii jednolitego rynku cyfrowego Komisja podkreśliła zapotrzebowanie na bezpieczne podłączone do sieci produkty i systemy oraz wskazała, że ustanowienie europejskich ram bezpieczeństwa ICT określających zasady certyfikacji bezpieczeństwa ICT w Unii mogłoby zarówno podtrzymać zaufanie do internetu, jak i przeciwdziałać obecnemu rozdrobnieniu rynku cyberbezpieczeństwa.

(50) Obecnie certyfikacja cyberbezpieczeństwa produktów i usług ICT jest stosowana jedynie w ograniczonym stopniu. Tam, gdzie się ją stosuje, istnieje ona głównie na szczeblu państw członkowskich lub w ramach systemów inicjowanych przez przemysł. W związku z powyższym certyfikat wydany przez dany krajowy organ ds. cyberbezpieczeństwa nie jest co do zasady uznawany w innych państwach członkowskich. Przedsiębiorstwa muszą zatem certyfikować swoje produkty i usługi w poszczególnych państwach członkowskich, w których działają, na przykład z myślą o uczestniczeniu w krajowych postępowaniach o udzielenie zamówień publicznych. Co więcej, w sytuacji gdy powstają nowe systemy, najwyraźniej brak jest spójnego i całościowego podejścia w odniesieniu do horyzontalnych kwestii cyberbezpieczeństwa, na przykład w obszarze internetu rzeczy. Istniejące systemy

mają istotne niedociągnięcia i różnią się pod względem zakresu produktów, poziomów pewności, kryteriów merytorycznych i faktycznego wykorzystania.

(51) W przeszłości poczyniono pewne starania na rzecz doprowadzenia do wzajemnego uznawania certyfikatów w Europie. Działania te były jednak tylko częściowo skuteczne. Najważniejszym przykładem w tym zakresie jest umowa o wzajemnym uznawaniu przyjęta przez grupę wyższych urzędników ds. bezpieczeństwa systemów informatycznych (SOG-IS). Mimo że stanowi ona najważniejszy wzór współpracy i wzajemnego uznawania w dziedzinie certyfikacji bezpieczeństwa, umowa o wzajemnym uznawaniu przyjęta przez SOG-IS obarczona jest istotnymi wadami związanymi z wysokimi kosztami jej funkcjonowania i jej ograniczonym zakresem. Dotychczas opracowano jedynie kilka profili ochrony produktów cyfrowych, takich jak podpis cyfrowy, tachograf cyfrowy i karty inteligentne. Co najważniejsze, do SOG-IS należy jedynie część państw członkowskich Unii. Ograniczyło to skuteczność przyjętej przez SOG-IS umowy o wzajemnym uznawaniu z punktu widzenia rynku wewnętrznego.

(52) W związku z powyższym konieczne jest ustanowienie europejskich ram certyfikacji cyberbezpieczeństwa, określających wymogi horyzontalne dotyczące europejskich systemów certyfikacji cyberbezpieczeństwa, które mają zostać opracowane, oraz umożliwiających uznawanie i stosowanie we wszystkich państwach członkowskich certyfikatów odnoszących się do produktów i usług ICT. Te europejskie ramy powinny mieć dwojaki cel: z jednej strony powinny działać na rzecz zwiększenia zaufania do produktów i usług ICT, które uzyskały certyfikację zgodnie ze wspomnianymi systemami. Z drugiej strony powinny pozwalać uniknąć mnożenia się sprzecznych lub nakładających się wzajemnie krajowych systemów certyfikacji cyberbezpieczeństwa i ograniczać dzięki temu koszty ponoszone przez przedsiębiorstwa działające na jednolitym rynku cyfrowym. Systemy powinny mieć charakter niedyskryminujący i opierać się normach międzynarodowych lub unijnych, o ile normy te nie są nieskuteczne lub nieodpowiednie na potrzeby realizacji uzasadnionych celów UE w tym zakresie.

(53) Komisja powinna być uprawniona do przyjęcia europejskich systemów certyfikacji cyberbezpieczeństwa dotyczących określonych grup produktów i usług ICT. Systemy te powinny być wprowadzane i nadzorowane przez krajowe organy nadzoru ds. certyfikacji, a certyfikaty wydawane w ramach tych systemów powinny być ważne i uznawane w całej Unii. Systemy certyfikacji prowadzone przez przemysł lub inne organizacje prywatne nie powinny być objęte zakresem niniejszego rozporządzenia. Organy zarządzające takimi systemami mogą jednak wnioskować do Komisji o wzięcie takich systemów pod uwagę jako podstawy zatwierdzenia ich jako systemu europejskiego.

(54) Przepisy niniejszego rozporządzenia nie powinny naruszać przepisów Unii ustanawiających szczegółowe zasady certyfikacji produktów i usług ICT. W szczególności w ogólnym rozporządzeniu o ochronie danych wprowadzono przepisy dotyczące ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych mających świadczyć o zgodności z tym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Takie mechanizmy certyfikacji oraz znaki jakości i oznaczenia w zakresie ochrony danych powinny umożliwiać osobom, których dane dotyczą, szybką ocenę poziomu ochrony danych zapewnianego przez odnośne produkty i usługi. Przepisy niniejszego rozporządzenia nie powodują uszczerbku dla certyfikacji operacji przetwarzania danych, także wówczas, gdy takie operacje są

wbudowane w produkty i usługi, zgodnie z ogólnym rozporządzeniem o ochronie danych.

(55) Celem europejskich systemów certyfikacji cyberbezpieczeństwa powinno być zapewnienie, aby produkty i usługi ICT certyfikowane w ramach danego systemu spełniały określone wymogi. Wymogi takie dotyczą odporności, przy danym poziomie pewności, na działania, których celem jest naruszenie dostępności, autentyczności, integralności i poufności przechowywanych lub przekazywanych lub przetwarzanych danych, lub też powiązanych funkcji bądź usług oferowanych lub dostępnych za pośrednictwem tych produktów, procesów, usług i systemów w rozumieniu niniejszego rozporządzenia. Nie jest możliwe szczegółowe określenie w niniejszym rozporządzeniu wymogów w zakresie cyberbezpieczeństwa odnoszących się do wszystkich produktów i usług ICT. Produkty i usługi ICT oraz powiązane z nimi potrzeby w zakresie cyberbezpieczeństwa są tak zróżnicowane, że przedstawienie ogólnych wymogów w zakresie cyberbezpieczeństwa obowiązujących dla wszystkich przypadków jest bardzo trudne. Konieczne jest zatem przyjęcie szerokiego i ogólnego pojęcia cyberbezpieczeństwa do celów certyfikacji, uzupełnionego zestawem szczegółowych celów w zakresie cyberbezpieczeństwa, które muszą być uwzględniane przy projektowaniu europejskich systemów certyfikacji cyberbezpieczeństwa. Metody osiągania tych celów w przypadku określonych produktów i usług ICT należy następnie doprecyzować na poziomie poszczególnych systemów certyfikacji przyjmowanych przez Komisję, na przykład poprzez odniesienie do norm lub specyfikacji technicznych.

(56) Komisja powinna zostać uprawniona do zwracania się do agencji ENISA z wnioskiem o przygotowanie kandydujących systemów w odniesieniu do określonych produktów lub usług ICT. Następnie Komisja, w oparciu o kandydujący system zaproponowany przez agencję ENISA, powinna zostać uprawniona do przyjęcia w drodze aktów wykonawczych danego europejskiego systemu certyfikacji cyberbezpieczeństwa. Ze względu na cel ogólny oraz cele w zakresie bezpieczeństwa określone w niniejszym rozporządzeniu europejskie systemy certyfikacji cyberbezpieczeństwa przyjęte przez Komisję powinny zawierać minimalny zbiór elementów dotyczących przedmiotu, zakresu i funkcjonowania poszczególnych systemów. Elementy te to między innymi zakres i przedmiot certyfikacji cyberbezpieczeństwa, w tym kategorie objętych nią produktów i usług ICT, dokładne wyszczególnienie wymogów w zakresie cyberbezpieczeństwa, na przykład poprzez odniesienie do norm lub specyfikacji technicznych, szczegółowe kryteria oceny i metody oceny, jak również docelowy poziom pewności: podstawowy, znaczny lub wysoki.

(57) Korzystanie z europejskiej certyfikacji cyberbezpieczeństwa powinno pozostać dobrowolne, chyba że przepisy unijne lub krajowe stanowią inaczej. Jednakże w celu osiągnięcia celów określonych w niniejszym rozporządzeniu i uniknięcia rozdrobnienia rynku wewnętrznego krajowe systemy lub procedury certyfikacji cyberbezpieczeństwa, dotyczące produktów i usług ICT objętych europejskim systemem certyfikacji cyberbezpieczeństwa, powinny przestać wywoływać skutki z dniem określonym przez Komisję w trybie aktu wykonawczego. Państwa członkowskie nie powinny ponadto wprowadzać nowych krajowych systemów certyfikacji będących systemami certyfikacji cyberbezpieczeństwa produktów i usług ICT objętych już istniejącym europejskim systemem certyfikacji cyberbezpieczeństwa.

(58) Po przyjęciu europejskiego systemu certyfikacji cyberbezpieczeństwa wytwórcy produktów ICT lub dostawcy usług ICT powinni móc złożyć wniosek o certyfikację

swoich produktów lub usług do wybranej jednostki oceniającej zgodność. Jednostki oceniające zgodność powinny uzyskiwać akredytację ze strony jednostki akredytującej, jeśli spełniają określone szczegółowe wymogi ustanowione w niniejszym rozporządzeniu. Akredytacji powinno się udzielać na maksymalny okres pięciu lat i można by ją odnowić na tych samych warunkach, o ile jednostka oceniająca zgodność spełnia wymogi. Jednostki akredytujące powinny cofać akredytację danej jednostki oceniającej zgodność, jeżeli warunki akredytacji nie są lub przestały być spełnione, bądź w przypadku gdy działania podejmowane przez jednostkę oceniającą zgodność naruszają niniejsze rozporządzenie.

(59) Należy zobowiązać wszystkie państwa członkowskie do wyznaczenia jednego organu nadzoru ds. certyfikacji cyberbezpieczeństwa odpowiedzialnego za nadzór nad stosowaniem się jednostek oceniających zgodność do wymogów niniejszego rozporządzenia oraz nad zgodnością z tymi wymogami certyfikatów wydanych przez jednostki oceniające zgodność mające siedzibę na podlegającym organowi nadzoru terytorium, jak również odpowiednich systemów certyfikacji cyberbezpieczeństwa. Krajowe organy nadzoru ds. certyfikacji powinny rozpatrywać skargi składane przez osoby fizyczne lub prawne w związku z certyfikatami wydanymi przez jednostki oceniające zgodność mające siedzibę na podlegających tym organom terytoriach, badać w odpowiednim zakresie przedmiot skarg oraz informować skarżących w stosownym terminie o postępach i wynikach badania. Powinny one ponadto współpracować z innymi krajowymi organami nadzoru ds. certyfikacji lub innymi organami publicznymi, w tym poprzez wymianę informacji na temat ewentualnej niezgodności produktów i usług ICT z wymogami niniejszego rozporządzenia lub określonych systemów certyfikacji cyberbezpieczeństwa.

(60) Z myślą o zapewnieniu konsekwentnego stosowania europejskich ram certyfikacji cyberbezpieczeństwa należy ustanowić Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa („Grupę”), w której skład wchodzić powinni przedstawiciele krajowych organów nadzoru ds. certyfikacji. Głównymi zadaniami Grupy powinny być doradzanie i pomaganie Komisji przy pracach nad zapewnieniem konsekwentnego wprowadzania i stosowania europejskich ram certyfikacji cyberbezpieczeństwa, pomoc Agencji i ścisła z nią współpraca przy przygotowywaniu kandydujących systemów certyfikacji cyberbezpieczeństwa, rekomendowanie Komisji zwrócenia się do Agencji o przygotowanie kandydującego europejskiego systemu certyfikacji cyberbezpieczeństwa oraz przyjmowanie skierowanych do Komisji opinii dotyczących utrzymania i przeglądu istniejących europejskich systemów certyfikacji cyberbezpieczeństwa.

(61) W celu poszerzania wiedzy na temat przyszłych unijnych systemów certyfikacji cyberbezpieczeństwa oraz ułatwienia ich akceptacji Komisja Europejska może wydawać ogólne lub sektorowe wytyczne dotyczące cyberbezpieczeństwa, np. na temat dobrych praktyk lub odpowiedzialnego zachowania w zakresie cyberbezpieczeństwa, podkreślające pozytywne konsekwencje stosowania certyfikowanych produktów i usług ICT.

(62) Wsparcie Agencji na rzecz certyfikacji cyberbezpieczeństwa powinno również obejmować współpracę z działającym przy Radzie Komitetem ds. Bezpieczeństwa oraz właściwymi organami krajowymi w odniesieniu do zatwierdzania funkcji kryptograficznych produktów, które mają być stosowane w sieciach niejawnych.

(63) W celu doprecyzowania kryteriów akredytacji jednostek oceniających zgodność należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 Traktatu

o funkcjonowaniu Unii Europejskiej: W czasie prac przygotowawczych Komisja powinna prowadzić stosowne konsultacje, w tym na poziomie ekspertów. Konsultacje te powinny być prowadzone zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r. W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te powinny otrzymywać wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji powinni móc systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(64) Aby zapewnić jednolite warunki wdrażania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze, tak jak to przewiduje niniejsze rozporządzenie. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011.

(65) Należy stosować procedurę sprawdzającą w celu przyjęcia aktów wykonawczych dotyczących europejskich systemów certyfikacji cyberbezpieczeństwa produktów i usług ICT, metod prowadzenia przez Agencję postępowań wyjaśniających oraz okoliczności, formatów i procedur notyfikowania Komisji akredytowanych jednostek oceniających zgodność przez krajowe organy nadzoru ds. certyfikacji.

(66) Działalność Agencji powinna być oceniana w sposób niezależny. Ocena ta powinna dotyczyć realizacji przez Agencję jej celów, jej metod pracy i zasadności jej zadań. Ocena powinna również dotyczyć wpływu, skuteczności i efektywności europejskich ram certyfikacji cyberbezpieczeństwa.

(67) Należy uchylić rozporządzenie (UE) nr 526/2013.

(68) Ponieważ cele niniejszego rozporządzenia nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, lecz możliwe jest lepsze ich osiągnięcie na poziomie Unii, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

TYTUŁ I
PRZEPISY OGÓLNE

Artykuł 1
Przedmiot i zakres

Z myślą o zapewnieniu należytego funkcjonowania rynku wewnętrznego, a jednocześnie dążąc do wysokiego poziomu cyberbezpieczeństwa, cyberodporności i zaufania w obrębie Unii, w niniejszym rozporządzeniu:

a) określa się cele, zadania i aspekty organizacyjne „Agencji UE ds. Cyberbezpieczeństwa" ENISA, zwanej dalej „Agencją"; oraz

b) określa się ramy ustanawiania europejskich systemów certyfikacji cyberbezpieczeństwa w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa produktów i usług ICT w Unii. Ramy te stosuje się, nie naruszając przepisów szczegółowych dotyczących dobrowolnej lub obowiązkowej certyfikacji zawartych w innych aktach Unii.

Artykuł 2
Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „cyberbezpieczeństwo" obejmuje wszystkie działania niezbędne do ochrony przed cyberzagrożeniami sieci i systemów informatycznych, ich użytkowników oraz osób, których zagrożenia te dotyczą;

2) „sieci i systemy informatyczne" oznaczają systemy w rozumieniu art. 4 pkt 1 dyrektywy (UE) 2016/1148;

3) „krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych" oznacza ramy w rozumieniu art. 4 pkt 3 dyrektywy (UE) 2016/1148;

4) „operator usług kluczowych" oznacza podmiot publiczny lub prywatny zdefiniowany w art. 4 pkt 4 dyrektywy (UE) 2016/1148;

5) „dostawca usług cyfrowych" oznacza każdą osobę prawną, która świadczy usługi cyfrowe, zdefiniowaną w art. 4 pkt 6 dyrektywy (UE) 2016/1148;

6) „incydent" oznacza każde zdarzenie zdefiniowane w art. 4 pkt 7 dyrektywy (UE) 2016/1148;

7) „postępowanie w przypadku incydentu" oznacza każdą procedurę zdefiniowaną w art. 4 pkt 8 dyrektywy (UE) 2016/1148;

8) „cyberzagrożenie" oznacza wszelkie potencjalne okoliczności lub zdarzenia, które mogą niekorzystnie wpływać na sieci i systemy informatyczne, ich użytkowników oraz osoby, których zagrożenie to dotyczy;

9) „europejski system certyfikacji cyberbezpieczeństwa" oznacza kompleksowy zbiór przepisów, wymagań technicznych, norm i procedur określonych na poziomie Unii i mających zastosowanie do certyfikacji produktów i usług z zakresu technologii informacyjno-komunikacyjnych (ICT) objętych zakresem danego systemu;

10) „europejski certyfikat cyberbezpieczeństwa” oznacza dokument wydany przez jednostkę oceniającą zgodność i poświadczający, że dany produkt lub dana usługa ICT spełniają szczegółowe wymagania określone w europejskim systemie certyfikacji cyberbezpieczeństwa;

11) „produkty i usługi ICT” oznaczają każdy element lub każdą grupę elementów sieci i systemów informatycznych;

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

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

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

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

16) „norma” oznacza normę zdefiniowaną w art. 2 pkt 1 rozporządzenia (UE) nr 1025/2012.

TYTUŁ II
ENISA – „Agencja UE ds. Cyberbezpieczeństwa”

ROZDZIAŁ I
MANDAT, CELE I ZADANIA

Artykuł 3
Mandat

1. Agencja podejmuje zadania przypisane jej na mocy niniejszego rozporządzenia w celu przyczyniania się do wysokiego poziomu cyberbezpieczeństwa w Unii.
2. Agencja wykonuje zadania powierzone jej na mocy aktów Unii określających środki zbliżania przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które to przepisy dotyczą cyberbezpieczeństwa.
3. Cele i zadania Agencji pozostają bez uszczerbku dla kompetencji państw członkowskich w zakresie cyberbezpieczeństwa, a w każdym przypadku bez uszczerbku dla działań związanych z bezpieczeństwem publicznym, obroną i bezpieczeństwem narodowym oraz dla działań państwa w dziedzinie prawa karnego.

Artykuł 4
Cele

1. Agencja stanowi ośrodek wiedzy fachowej z dziedziny cyberbezpieczeństwa z racji swojej niezależności, jakości naukowo-technicznej oferowanego doradztwa i pomocy oraz przekazywanych informacji, przejrzystości procedur i metod działania, a także staranności w realizacji swoich zadań.
2. Agencja pomaga instytucjom, agencjom i organom Unii oraz państwom członkowskim w opracowywaniu i realizacji polityki dotyczącej cyberbezpieczeństwa.
3. Agencja wspiera budowanie potencjału i gotowości w całej Unii, pomagając Unii, państwom członkowskim oraz zainteresowanym stronom z sektora publicznego i prywatnego w celu zwiększenia ochrony ich sieci i systemów informatycznych, rozwoju umiejętności i kompetencji z dziedziny cyberbezpieczeństwa oraz osiągnięcia cyberodporności.
4. Agencja propaguje współpracę i koordynację na szczeblu unijnym pomiędzy państwami członkowskimi, instytucjami, agencjami i organami Unii oraz właściwymi zainteresowanymi stronami, w tym z sektora prywatnego, w kwestiach związanych z cyberbezpieczeństwem.
5. Agencja zwiększa zdolności w zakresie cyberbezpieczeństwa na poziomie unijnym w celu uzupełnienia działań państw członkowskich na rzecz zapobiegania cyberzagrożeniom i reagowania na nie, zwłaszcza w przypadku incydentów transgranicznych.
6. Agencja propaguje stosowanie certyfikacji, w tym poprzez przyczynianie się do utworzenia i utrzymywania ram certyfikacji cyberbezpieczeństwa na szczeblu

unijnym zgodnie z tytułem III niniejszego rozporządzenia, z myślą o zwiększeniu przejrzystości w zakresie zapewniania cyberbezpieczeństwa produktów i usług ICT, zwiększając w ten sposób zaufanie do wewnętrznego rynku cyfrowego.

7. Agencja działa na rzecz wysokiego poziomu wiedzy obywateli i przedsiębiorstw o zagadnieniach związanych z cyberbezpieczeństwa.

Artykuł 5

Zadania związane z opracowywaniem i wdrażaniem polityki i prawa Unii

Agencja przyczynia się do opracowywania i wdrażania polityki i prawa Unii poprzez:

1. pomoc i doradztwo, w szczególności przez wydawanie niezależnych opinii i wykonywanie prac przygotowawczych, w sprawach opracowywania i przeglądu polityki i prawa Unii w dziedzinie cyberbezpieczeństwa, jak również w odniesieniu do inicjatyw dotyczących polityki i prawa Unii w poszczególnych sektorach, w których występują kwestie związane z cyberbezpieczeństwem;
2. pomoc dla państw członkowskich przy jednolitym wdrażaniu polityki i prawa Unii w dziedzinie cyberbezpieczeństwa, zwłaszcza w związku z dyrektywą (UE) 2016/1148, w tym za pomocą opinii, wytycznych, porad i najlepszych praktyk dotyczących takich tematów jak zarządzanie ryzykiem, zgłaszanie incydentów i wymiana informacji, jak również ułatwianie wymiany najlepszych praktyk w tej dziedzinie między właściwymi organami;
3. wkład w prace grupy współpracy na podstawie art. 11 dyrektywy (UE) 2016/1148, przez zapewnianie wiedzy fachowej i pomocy;
4. wspieranie:
    1) opracowywania i wdrażania polityki Unii w dziedzinie tożsamości elektronicznej i usług zaufania, w szczególności przez zapewnianie doradztwa i wytycznych technicznych, jak również ułatwianie wymiany najlepszych praktyk między właściwymi organami;
    2) działań na rzecz podwyższonego poziomu bezpieczeństwa łączności elektronicznej, w tym przez zapewnianie wiedzy fachowej i doradztwa, jak również ułatwianie wymiany najlepszych praktyk między właściwymi organami;
5. wspieranie regularnego przeglądu działań w ramach polityki Unii poprzez przedstawianie sprawozdania rocznego na temat stanu wdrożenia odpowiednich ram prawnych w odniesieniu do:
    a) zgłoszeń incydentów w państwach członkowskich, przekazywanych grupie współpracy przez pojedyncze punkty kontaktowe na podstawie art. 10 ust. 3 dyrektywy (UE) 2016/1148;
    b) zawiadomień o naruszeniach bezpieczeństwa i utracie integralności dotyczących dostawców usług zaufania, przekazywanych Agencji przez organy nadzoru na podstawie art. 19 ust. 3 rozporządzenia (UE) nr 910/2014;
    c) zawiadomień o naruszeniach bezpieczeństwa przesyłanych przez przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej, przekazywanych Agencji

przez właściwe organy na podstawie art. 40 [dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej].

Artykuł 6

Zadania związane z budowaniem potencjału

1. Agencja pomaga:

a) państwom członkowskim w ich staraniach na rzecz poprawy w zakresie zapobiegania problemom i incydentom w dziedzinie cyberbezpieczeństwa, wykrywania i analizowania tych problemów i incydentów oraz zdolności reagowania na nie – poprzez zapewnianie państwom członkowskim niezbędnej wiedzy fachowej;

b) instytucjom, organom i jednostkom organizacyjnym Unii w ich staraniach na rzecz poprawy w zakresie zapobiegania problemom i incydentom w dziedzinie cyberbezpieczeństwa, wykrywania i analizowania tych problemów i incydentów oraz zdolności reagowania na nie – poprzez odpowiednie wsparcie zespołu CERT działającego w unijnych instytucjach, organach i agencjach (CERT-UE);

c) państwom członkowskim, na ich wniosek, w tworzeniu krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) na podstawie art. 9 ust. 5 dyrektywy (UE) 2016/1148;

d) państwom członkowskim, na ich wniosek, w opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych na podstawie art. 7 ust. 2 dyrektywy (UE) 2016/1148; Agencja działa również na rzecz upowszechnienia tych strategii w całej Unii i śledzi postępy w ich realizacji w celu propagowania najlepszych praktyk;

e) instytucjom Unii w opracowywaniu unijnych strategii dotyczących cyberbezpieczeństwa, działaniu na rzecz ich upowszechnienia i śledzeniu postępów w ich realizacji;

f) krajowym i unijnym zespołom CSIRT w podnoszeniu poziomu ich zdolności, w tym poprzez propagowanie dialogu i wymiany informacji, w celu zapewnienia, aby każdy zespół CSIRT, zgodnie ze stanem wiedzy, spełniał szereg wspólnych minimalnych wymogów dotyczących kompetencji oraz działał zgodnie z najlepszymi praktykami;

g) państwom członkowskim, organizując na szczeblu unijnym coroczne ćwiczenia na wielką skalę w dziedzinie cyberbezpieczeństwa, o których mowa w art. 7 ust. 6, oraz wydając zalecenia dotyczące polityki w oparciu o proces oceny tych ćwiczeń i wyciągnięte z nich doświadczenia;

h) odpowiednim organom publicznym, oferując szkolenia dotyczące cyberbezpieczeństwa, w stosownych przypadkach we współpracy z zainteresowanymi stronami;

i) grupie współpracy, poprzez wymianę najlepszych praktyk, w szczególności w odniesieniu do identyfikowania operatorów usług kluczowych przez państwa członkowskie, w tym odnośnie do transgranicznych zależności, dotyczących ryzyk i incydentów, na podstawie art. 11 ust. 3 lit. l) dyrektywy (UE) 2016/1148.

2. Agencja ułatwia utworzenie sektorowych ośrodków wymiany i analizy informacji oraz stale je wspiera, w szczególności w sektorach wymienionych w załączniku II do

dyrektywy (UE) 2016/1148, udostępniając najlepsze praktyki i wytyczne dotyczące dostępnych narzędzi, procedury, jak również sposobu postępowania w kwestiach regulacyjnych związanych z wymianą informacji.

Artykuł 7

Zadania związane ze współpracą operacyjną na szczeblu unijnym

1. Agencja wspiera współpracę operacyjną między właściwymi organami publicznymi oraz między zainteresowanymi stronami.

2. Agencja współpracuje na poziomie operacyjnym i tworzy synergię z instytucjami, organami i jednostkami organizacyjnymi Unii, w tym z zespołem CERT-UE, ze służbami zajmującymi się cyberprzestępczością i z organami nadzoru zajmującymi się ochroną prywatności i danych osobowych, w celu rozwiązywania kwestii będących przedmiotem wspólnego zainteresowania, obejmujących:

   a) wymianę know-how i najlepszych praktyk;

   b) zapewnianie porad i wytycznych w istotnych kwestiach związanych z cyberbezpieczeństwem;

   c) dokonanie, po konsultacji z Komisją, praktycznych ustaleń dotyczących wykonania określonych zadań.

3. Agencja zapewnia sekretariat sieci CSIRT na podstawie art. 12 ust. 2 dyrektywy (UE) 2016/1148 oraz aktywnie ułatwia wymianę informacji i współpracę między jej członkami.

4. Agencja wnosi wkład we współpracę operacyjną w ramach sieci CSIRT, zapewniając państwom członkowskim wsparcie poprzez:

   a) doradzanie, w jaki sposób podnosić ich zdolność zapobiegania incydentom, wykrywania incydentów i reagowania na nie;

   b) świadczenie, na ich wniosek, pomocy technicznej w przypadku incydentów o znacznych lub istotnych skutkach;

   c) analizę podatności na zagrożenia, artefaktów i incydentów.

Realizując te zadania, Agencja i CERT-UE angażują się we współpracę strukturalną w celu czerpania korzyści z efektów synergii, w szczególności w odniesieniu do aspektów operacyjnych.

5. Na wniosek co najmniej dwóch zainteresowanych państw członkowskich, oraz w wyłącznym celu udzielania porad dotyczących zapobiegania przyszłym incydentom, Agencja wspiera przeprowadzenie technicznego postępowania wyjaśniającego *ex post* lub przeprowadza takie postępowanie w wyniku zawiadomień o incydentach o znacznych lub istotnych skutkach, złożonych przez poszkodowane przedsiębiorstwa na podstawie dyrektywy (UE) 2016/1148. Agencja przeprowadza również takie postępowanie wyjaśniające na należycie uzasadniony wniosek Komisji, złożony w porozumieniu z zainteresowanymi państwami członkowskimi, w przypadku takich incydentów mających wpływ na więcej niż dwa państwa członkowskie.

Zakres postępowania i procedurę, której należy przestrzegać, prowadząc takie postępowanie, uzgadniają zainteresowane państwa członkowskie i Agencja, a ustalenia te pozostają bez uszczerbku dla jakichkolwiek toczących się dochodzeń dotyczących tego samego incydentu. Na zakończenie postępowania Agencja sporządza końcowe sprawozdanie techniczne, w oparciu w szczególności o informacje i uwagi przekazane przez zainteresowane państwa członkowskie i przedsiębiorstwo lub przedsiębiorstwa, które to sprawozdanie uzgadnia się z zainteresowanymi państwami członkowskimi. Streszczenie sprawozdania koncentrujące się na zaleceniach dotyczących zapobiegania przyszłym incydentom udostępnia się sieci CSIRT.

6. Agencja organizuje coroczne ćwiczenia w dziedzinie cyberbezpieczeństwa na szczeblu unijnym i wspiera państwa członkowskie oraz instytucje, agencje i organy UE w organizacji ćwiczeń w odpowiedzi na ich wnioski. Coroczne ćwiczenia na szczeblu unijnym obejmują elementy techniczne, operacyjne i strategiczne oraz pomagają przygotować wspólną reakcję na szczeblu unijnym na transgraniczne cyberincydenty na dużą skalę. W stosownych przypadkach Agencja wnosi również wkład w sektorowe ćwiczenia w dziedzinie cyberbezpieczeństwa i pomaga w ich organizacji wspólnie z odpowiednimi ośrodkami wymiany i analizy informacji oraz zezwala tym ośrodkom na udział również w ćwiczeniach w dziedzinie cyberbezpieczeństwa na szczeblu unijnym.

7. Agencja przygotowuje regularne unijny raport techniczny z zakresu cyberbezpieczeństwa na temat incydentów i zagrożeń, w oparciu o informacje ze źródeł otwartych, własne analizy oraz raporty udostępniane przez, między innymi: zespoły CSIRT w państwach członkowskich (na zasadzie dobrowolności) lub pojedyncze punkty kontaktowe wyznaczone na podstawie dyrektywy w sprawie cyberbezpieczeństwa (zgodnie z art. 14 ust. 5 dyrektywy w sprawie cyberbezpieczeństwa), Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu, CERT-UE.

8. Agencja wnosi wkład w opracowanie wspólnej reakcji, na szczeblu Unii i państw członkowskich, na związane z cyberbezpieczeństwem transgraniczne incydenty na dużą skalę lub kryzysy, głównie poprzez:

   a) gromadzenie raportów ze źródeł krajowych w celu przyczynienia się do ustalenia wspólnej orientacji sytuacyjnej;

   b) zapewnienie skutecznego przepływu informacji i mechanizmów eskalacji między siecią CSIRT a decydentami technicznymi i politycznymi na szczeblu unijnym;

   c) wsparcie techniczne przy postępowaniu w przypadku incydentu lub kryzysu, w tym ułatwianie wymiany rozwiązań technicznych między państwami członkowskimi;

   d) wsparcie w zakresie komunikacji publicznej w związku z incydentem lub kryzysem;

   e) testowanie planów współpracy mającej na celu reakcję na takie incydenty lub kryzysy.

Artykuł 8

Zadania związane z rynkiem, certyfikacją cyberbezpieczeństwa i normalizacją

Agencja:

a) wspiera i propaguje opracowanie i realizację polityki Unii w zakresie certyfikacji cyberbezpieczeństwa produktów i usług ICT, ustanowionej w tytule III niniejszego rozporządzenia, poprzez:

   1) przygotowywanie kandydujących europejskich systemów certyfikacji cyberbezpieczeństwa w odniesieniu do produktów i usług ICT zgodnie z art. 44 niniejszego rozporządzenia;

   2) pomoc udzielaną Komisji przy zapewnianiu obsługi sekretariatu dla Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa na podstawie art. 53 niniejszego rozporządzenia;

   3) sporządzanie i publikowanie wytycznych oraz opracowywanie dobrych praktyk dotyczących wymogów w zakresie cyberbezpieczeństwa produktów i usług ICT, we współpracy z krajowymi organami nadzoru ds. certyfikacji oraz z przemysłem;

b) ułatwia ustanowienie i upowszechnienie europejskich i międzynarodowych norm dotyczących zarządzania ryzykiem i bezpieczeństwa produktów i usług ICT, jak również opracowuje, we współpracy z państwami członkowskimi, porady i wytyczne dotyczące kwestii technicznych związanych z wymogami bezpieczeństwa odnoszącymi się do operatorów usług kluczowych i dostawców usług cyfrowych, a także dotyczące już istniejących norm, w tym norm krajowych państw członkowskich, na podstawie art. 19 ust. 2 dyrektywy (UE) 2016/1148;

c) przeprowadza regularne analizy głównych tendencji na rynku cyberbezpieczeństwa, zarówno po stronie popytu, jak i podaży, i rozpowszechnia wyniki tych analiz w celu pobudzania rozwoju rynku cyberbezpieczeństwa w Unii.

Artykuł 9

Zadania związane z wiedzą, informacjami i podnoszeniem poziomu świadomości

Agencja:

a) przeprowadza analizy powstających technologii i przedstawia odnoszące się do danych tematów oceny dotyczące społecznego, prawnego, gospodarczego i regulacyjnego wpływu innowacji technologicznych na cyberbezpieczeństwo;

b) przeprowadza długoterminowe analizy strategiczne zagrożeń i cyberincydentów w celu określenia powstających tendencji i pomocy w zapobieganiu problemom związanym z cyberbezpieczeństwem;

c) zapewnia, we współpracy z ekspertami z organów państw członkowskich, doradztwo, wytyczne i najlepsze praktyki dotyczące bezpieczeństwa sieci i systemów informatycznych, w szczególności w odniesieniu do bezpieczeństwa infrastruktury internetowej i tych infrastruktur, które stanowią wsparcie sektorów wymienionych w załączniku II do dyrektywy (UE) 2016/1148;

d) gromadzi, systematyzuje i podaje do wiadomości publicznej za pośrednictwem specjalnego portalu informacje na temat cyberbezpieczeństwa przekazane przez instytucje, agencji i organy Unii;

e) działa na rzecz podniesienia poziomu świadomości ogółu społeczeństwa na temat różnych postaci cyberryzyka i przedstawia wytyczne na temat dobrych praktyk dla użytkowników końcowych, skierowane do obywateli i organizacji;

f) gromadzi i analizuje publicznie dostępne informacje dotyczące istotnych incydentów oraz sporządza sprawozdania w celu zapewnienia wytycznych przedsiębiorstwom i obywatelom w całej Unii;

g) organizuje, we współpracy z państwami członkowskimi oraz instytucjami, organami i jednostkami organizacyjnymi Unii, regularne kampanie informacyjne na rzecz zwiększenia cyberbezpieczeństwa i jego wyeksponowania w Unii.

Artykuł 10

Zadania związane z badaniami naukowymi i innowacjami

W odniesieniu do badań naukowych i innowacji Agencja:

a) doradza Unii i państwom członkowskim w zakresie potrzeb badawczych i priorytetów w dziedzinie cyberbezpieczeństwa z myślą o umożliwieniu skutecznego reagowania na bieżące i pojawiające się ryzyko i zagrożenia, w tym również w odniesieniu do nowych i powstających technologii informacyjno-komunikacyjnych, a także z myślą o skutecznym stosowaniu technologii zapobiegania ryzyku;

b) uczestniczy, w przypadku gdy Komisja przekazała jej stosowne uprawnienia, w fazie realizacji programów finansowania badań naukowych i innowacji lub występuje jako beneficjent.

Artykuł 11

Zadania związane ze współpracą międzynarodową

Agencja wnosi wkład w starania Unii na rzecz współpracy z państwami trzecimi i organizacjami międzynarodowymi w celu propagowania współpracy międzynarodowej w kwestiach związanych z cyberbezpieczeństwem, przez:

a) udział, w stosownych przypadkach, w charakterze obserwatora w organizacji międzynarodowych ćwiczeń, oraz analizowanie ich wyników i składanie zarządowi sprawozdań z tych wyników;

b) ułatwianie, na wniosek Komisji, wymiany najlepszych praktyk między odpowiednimi organizacjami międzynarodowymi;

c) zapewnianie Komisji, na wniosek, wiedzy fachowej.

ROZDZIAŁ II
ORGANIZACJA AGENCJI

Artykuł 12
Struktura

Strukturę administracyjną i kierowniczą Agencji tworzą:

a) zarząd, który pełni funkcje określone w art. 14;

b) rada wykonawcza, która pełni funkcje określone w art. 18;

c) dyrektor wykonawczy, który wykonuje obowiązki określone w art. 19; oraz

d) Stała Grupa Przedstawicieli Zainteresowanych Stron, która pełni funkcje określone w art. 20.

SEKCJA 1
ZARZĄD

Artykuł 13
Skład zarządu

1. W skład zarządu wchodzi po jednym przedstawicielu każdego z państw członkowskich oraz dwóch przedstawicieli wyznaczonych przez Komisję. Prawo głosu przysługuje wszystkim przedstawicielom.

2. Każdy z członków zarządu posiada zastępcę, który reprezentuje członka w przypadku jego nieobecności.

3. Członków zarządu i ich zastępców powołuje się przez wzgląd na ich wiedzę w dziedzinie cyberbezpieczeństwa, biorąc pod uwagę odpowiednie umiejętności kierownicze, administracyjne i budżetowe. Komisja i państwa członkowskie dokładają starań, aby ograniczyć rotację swoich przedstawicieli w zarządzie w celu zapewnienia ciągłości jego prac. Komisja i państwa członkowskie dążą do zapewnienia zrównoważonej reprezentacji kobiet i mężczyzn w zarządzie.

4. Kadencja członków zarządu i ich zastępców wynosi cztery lata. Kadencja ta jest odnawialna.

Artykuł 14
Funkcje zarządu

1. Zarząd:

   a) określa ogólny kierunek działalności Agencji oraz zapewnia również, aby praca Agencji odbywała się zgodnie z przepisami i zasadami określonymi w niniejszym rozporządzeniu. Zarząd zapewnia również spójność pracy Agencji z działaniami prowadzonymi przez państwa członkowskie oraz na szczeblu unijnym;

   b) przyjmuje projekt jednolitego dokumentu programowego Agencji, o którym mowa w art. 21, przed przedłożeniem go do zaopiniowania przez Komisję;

c) przyjmuje, uwzględniając opinię Komisji, jednolity dokument programowy Agencji większością dwóch trzecich głosów członków i zgodnie z art. 17;

d) przyjmuje, większością dwóch trzecich głosów członków, budżet roczny Agencji oraz pełni inne funkcje związane z budżetem Agencji na podstawie rozdziału III;

e) ocenia i przyjmuje skonsolidowane sprawozdanie roczne z działalności Agencji oraz do dnia 1 lipca następnego roku przesyła zarówno sprawozdanie, jak i jego ocenę Parlamentowi Europejskiemu, Radzie, Komisji i Trybunałowi Obrachunkowemu. Sprawozdanie roczne zawiera sprawozdanie finansowe i opis sposobu osiągnięcia przez Agencję wskaźników skuteczności jej działania. Sprawozdanie roczne podaje się do wiadomości publicznej;

f) przyjmuje zgodnie z art. 29 przepisy finansowe mające zastosowanie do Agencji;

g) przyjmuje strategię zwalczania nadużyć finansowych, która jest proporcjonalna do istniejących w tym zakresie zagrożeń i uwzględnia analizę kosztów i korzyści wynikających z wdrażanych środków;

h) przyjmuje przepisy, których celem jest zapobieganie konfliktom interesów i zarządzanie nimi, w odniesieniu do swoich członków;

i) zapewnia podjęcie odpowiednich działań następczych w związku z ustaleniami i zaleceniami wynikającymi z dochodzeń przeprowadzanych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz z różnych sprawozdań z kontroli i ocen, zarówno wewnętrznych, jak i zewnętrznych;

j) przyjmuje swój regulamin wewnętrzny;

k) zgodnie z ust. 2 wykonuje – w odniesieniu do pracowników Agencji – uprawnienia powierzone organowi powołującemu na mocy regulaminu pracowniczego urzędników oraz uprawnienia, które organowi uprawnionemu do zawierania umów o pracę powierzono na mocy warunków zatrudnienia innych pracowników Unii Europejskiej („uprawnienia organu powołującego”);

l) przyjmuje przepisy wykonawcze do regulaminu pracowniczego i do warunków zatrudnienia innych pracowników zgodnie z procedurą przewidzianą w art. 110 regulaminu pracowniczego;

m) mianuje dyrektora wykonawczego oraz w stosownych przypadkach podejmuje decyzje o przedłużeniu jego kadencji lub odwołaniu go ze stanowiska zgodnie z art. 33 niniejszego rozporządzenia;

n) mianuje księgowego, którym może być księgowy Komisji i który jest całkowicie niezależny w wykonywaniu swoich obowiązków;

o) podejmuje wszystkie decyzje dotyczące ustanowienia wewnętrznej struktury Agencji, a w razie potrzeby jej modyfikacji, uwzględniając potrzeby w zakresie działań Agencji i mając na uwadze należyte zarządzanie budżetem;

p) wydaje zgodę na dokonanie ustaleń roboczych zgodnie z art. 7 i 39.

2. Zgodnie z art. 110 regulaminu pracowniczego, na podstawie art. 2 ust. 1 regulaminu pracowniczego i art. 6 warunków zatrudnienia innych pracowników zarząd przyjmuje decyzję przekazującą odpowiednie uprawnienia organu powołującego dyrektorowi wykonawczemu i określającą warunki, zgodnie z którymi możliwe jest zawieszenie przekazania tych uprawnień. Dyrektor wykonawczy jest uprawniony do dalszego przekazania tych uprawnień.

3. Jeżeli wymagają tego wyjątkowe okoliczności, zarząd może w drodze decyzji zawiesić tymczasowo przekazanie uprawnień organu powołującego dyrektorowi wykonawczemu i uprawnienia dalej przez niego przekazane oraz wykonywać je samodzielnie lub przekazać je jednemu ze swoich członków lub też pracownikowi innemu niż dyrektor wykonawczy.

Artykuł 15
Przewodniczący zarządu

Większością dwóch trzecich głosów członków zarząd wybiera spośród swoich członków przewodniczącego i zastępcę przewodniczącego na okres trzech lat z możliwością jednokrotnego odnowienia. Jeżeli jednak w dowolnym momencie swojej kadencji stracą oni status członka zarządu, kadencja ich kończy się automatycznie w tym samym dniu. Zastępca przewodniczącego zastępuje z urzędu przewodniczącego, jeżeli przewodniczący nie jest w stanie pełnić swoich obowiązków.

Artykuł 16
Posiedzenia zarządu

1. Posiedzenia zarządu zwoływane są przez przewodniczącego zarządu.

2. Zarząd zbiera się co najmniej dwa razy do roku na posiedzeniach zwyczajnych. Na wniosek przewodniczącego, na wniosek Komisji lub na wniosek co najmniej jednej trzeciej członków zarządu odbywają się również posiedzenia nadzwyczajne zarządu.

3. Dyrektor wykonawczy bierze udział w posiedzeniach zarządu bez prawa głosu.

4. Członkowie Stałej Grupy Przedstawicieli Zainteresowanych Stron mogą brać udział w posiedzeniach zarządu, na zaproszenie przewodniczącego, bez prawa głosu.

5. Członkowie zarządu i ich zastępcy mogą korzystać podczas posiedzeń z pomocy doradców lub ekspertów, z zastrzeżeniem przepisów regulaminu wewnętrznego.

6. Agencja zapewnia zarządowi obsługę sekretariatu.

Artykuł 17
Zasady głosowania zarządu

1. Zarząd podejmuje decyzje większością głosów swoich członków.

2. W odniesieniu do jednolitego dokumentu programowego, budżetu rocznego oraz mianowania, przedłużenia kadencji lub odwołania dyrektora wykonawczego wymagana jest większość głosów dwóch trzecich wszystkich członków zarządu.

3. Każdemu członkowi przysługuje jeden głos. W przypadku nieobecności członka jego zastępca jest uprawniony do wykonywania prawa głosu.

4. Przewodniczący bierze udział w głosowaniu.

5. Dyrektor wykonawczy nie może brać udziału w głosowaniu.

6. W regulaminie wewnętrznym zarządu ustala się bardziej szczegółowy tryb głosowania, a zwłaszcza okoliczności, w których jeden członek zarządu może występować w imieniu innego członka.

SEKCJA 2
RADA WYKONAWCZA

Artykuł 18
Rada wykonawcza

1. Zarządowi pomaga rada wykonawcza.

2. Rada wykonawcza:

   a) przygotowuje decyzje, które mają zostać przyjęte przez zarząd;

   b) wraz z zarządem zapewnia odpowiednie działania następcze w związku z ustaleniami i zaleceniami wynikającymi z dochodzeń przeprowadzanych przez OLAF oraz z różnych sprawozdań z kontroli i ocen, zarówno wewnętrznych, jak i zewnętrznych;

   c) bez uszczerbku dla obowiązków dyrektora wykonawczego, określonych w art. 19, wspiera dyrektora wykonawczego i doradza mu przy wdrażaniu decyzji zarządu w sprawach administracyjnych i budżetowych na podstawie art. 19.

3. W skład rady wykonawczej wchodzi pięciu członków powołanych spośród członków zarządu, w tym przewodniczący zarządu, który może również przewodniczyć radzie wykonawczej, oraz jeden z przedstawicieli Komisji. Dyrektor wykonawczy bierze udział w posiedzeniach rady wykonawczej, ale nie posiada prawa głosu.

4. Kadencja członków rady wykonawczej wynosi cztery lata. Kadencja ta jest odnawialna.

5. Posiedzenia rady wykonawczej odbywają się co najmniej raz na trzy miesiące. Przewodniczący rady wykonawczej zwołuje dodatkowe posiedzenia na wniosek jej członków.

6. Zarząd ustanawia regulamin wewnętrzny rady wykonawczej.

7. W przypadku pilnej potrzeby rada wykonawcza może podejmować określone decyzje tymczasowe w imieniu zarządu, w szczególności w kwestiach zarządzania administracyjnego, w tym w zakresie zawieszenia przekazania uprawnień organu powołującego oraz w kwestiach związanych z budżetem.

SEKCJA 3
DYREKTOR WYKONAWCZY

Artykuł 19
Obowiązki dyrektora wykonawczego

1. Agencja jest zarządzana przez dyrektora wykonawczego, który zachowuje niezależność podczas pełnienia swoich obowiązków. Dyrektor wykonawczy odpowiada przed zarządem.

2. Dyrektor wykonawczy na wezwanie Parlamentu Europejskiego informuje go o wykonywaniu swoich obowiązków. Rada może wezwać dyrektora wykonawczego do poinformowania jej o wykonywaniu powierzonych mu obowiązków.

3. Dyrektor wykonawczy odpowiada za:

   a) bieżące zarządzanie Agencją;

   b) wykonanie decyzji przyjętych przez zarząd;

   c) przygotowanie projektu jednolitego dokumentu programowego i przedłożenie go zarządowi do zatwierdzenia przed przedłożeniem go Komisji;

   d) wdrażanie jednolitego dokumentu programowego i składanie sprawozdań z jego wdrażania zarządowi;

   e) przygotowanie skonsolidowanego sprawozdania rocznego z działalności Agencji i przedstawienie go zarządowi do oceny i przyjęcia;

   f) przygotowanie planu działania w następstwie wniosków z wcześniejszych ocen oraz przedkładanie Komisji co dwa lata sprawozdania z postępów;

   g) przygotowanie planu działania w następstwie wniosków ze sprawozdań z kontroli wewnętrznej lub zewnętrznej, a także z dochodzeń przeprowadzanych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), oraz za składanie sprawozdania z postępów dwa razy w roku Komisji, a regularnie – zarządowi;

   h) przygotowanie projektu przepisów finansowych mających zastosowanie do Agencji;

   i) przygotowanie projektu preliminarza dochodów i wydatków Agencji oraz wykonanie jej budżetu;

   j) ochronę interesów finansowych Unii poprzez stosowanie środków zapobiegających nadużyciom finansowym, korupcji i wszelkim innym nielegalnym działaniom, za pomocą skutecznych kontroli, a w przypadku wykrycia nieprawidłowości – poprzez odzyskanie nienależnie wypłaconych kwot, a także – w stosownych przypadkach – poprzez skuteczne, proporcjonalne i odstraszające kary administracyjne i finansowe;

   k) przygotowanie strategii Agencji na rzecz przeciwdziałania nadużyciom i przedstawienie jej zarządowi do zatwierdzenia;

l) nawiązywanie i utrzymywanie kontaktów ze środowiskiem przedsiębiorców i organizacjami konsumenckimi w celu zapewnienia regularnego dialogu z odpowiednimi zainteresowanymi stronami;

m) realizację innych zadań powierzonych dyrektorowi wykonawczemu na mocy niniejszego rozporządzenia.

4. W razie potrzeby oraz w ramach mandatu Agencji i zgodnie z jej celami i zadaniami dyrektor wykonawczy może tworzyć grupy robocze *ad hoc* złożone z ekspertów, w tym ekspertów reprezentujących właściwe organy państw członkowskich. Zarząd jest o tym informowany z wyprzedzeniem. Procedury dotyczące w szczególności składu grup roboczych, powoływania ekspertów grup roboczych przez dyrektora wykonawczego oraz działania grup roboczych określa się w wewnętrznych zasadach działania Agencji.

5. Dyrektor wykonawczy podejmuje decyzję, czy do celów wykonywania zadań Agencji w skuteczny i wydajny sposób konieczne jest rozmieszczenie pracowników w jednym lub kilku państwach członkowskich. Przed podjęciem decyzji o utworzeniu biura lokalnego dyrektor wykonawczy uzyskuje wcześniejszą zgodę Komisji, zarządu i państwa członkowskiego (państw członkowskich), którego (których) to dotyczy. W decyzji określa się zakres działań prowadzonych w biurze lokalnym w sposób pozwalający uniknąć niepotrzebnych kosztów i powielania administracyjnych funkcji Agencji. W stosownych przypadkach, lub gdy jest to wymagane, z państwem członkowskim (państwami członkowskimi), którego (których) to dotyczy, zawiera się umowę.

SEKCJA 4
STAŁA GRUPA PRZEDSTAWICIELI ZAINTERESOWANYCH STRON

Artykuł 20
Stała Grupa Przedstawicieli Zainteresowanych Stron

1. Działając na wniosek dyrektora wykonawczego, zarząd ustanawia Stałą Grupę Przedstawicieli Zainteresowanych Stron złożoną z uznanych ekspertów reprezentujących odpowiednie zainteresowane strony, takie jak sektor ICT, dostawcy publicznie dostępnych sieci lub usług łączności elektronicznej, grupy konsumenckie, eksperci akademiccy w dziedzinie cyberbezpieczeństwa oraz przedstawiciele właściwych organów zgłoszonych na podstawie [dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej], a także organy nadzorcze ds. egzekwowania prawa i ochrony danych.

2. Procedury dotyczące Stałej Grupy Przedstawicieli Zainteresowanych Stron, w szczególności liczby jej członków, jej składu i powoływania jej członków przez zarząd, wniosku dyrektora wykonawczego, a także działania grupy, określa się w wewnętrznych zasadach działania Agencji i podaje do wiadomości publicznej.

3. Stałej Grupie Przedstawicieli Zainteresowanych Stron przewodniczy dyrektor wykonawczy lub inna osoba wyznaczona w danym przypadku przez dyrektora wykonawczego.

4. Kadencja członków Stałej Grupy Przedstawicieli Zainteresowanych Stron wynosi dwa i pół roku. Członkowie zarządu nie mogą być członkami Stałej Grupy

Przedstawicieli Zainteresowanych Stron. Eksperci z Komisji i z państw członkowskich mają prawo do udziału w posiedzeniach i pracach Stałej Grupy Przedstawicieli Zainteresowanych Stron. Przedstawiciele innych organów uznanych przez dyrektora wykonawczego za właściwe, którzy nie są członkami Stałej Grupy Przedstawicieli Zainteresowanych Stron, mogą być zapraszani na jej posiedzenia i uczestniczyć w jej pracach.

5. Stała Grupa Przedstawicieli Zainteresowanych Stron doradza Agencji w związku z realizacją jej działań. Grupa doradza w szczególności dyrektorowi wykonawczemu w sprawie sporządzenia wniosku dotyczącego programu prac Agencji oraz w sprawie zapewnienia komunikacji z odpowiednimi zainteresowanymi stronami we wszystkich kwestiach związanych z programem prac.

SEKCJA 5
DZIAŁALNOŚĆ

Artykuł 21
Jednolity dokument programowy

1. Agencja prowadzi działalność zgodnie z jednolitym dokumentem programowym obejmującym jej programowanie wieloletnie i roczne, w którym uwzględnia się wszystkie jej planowane działania.

2. Każdego roku dyrektor wykonawczy sporządza projekt jednolitego dokumentu programowego obejmującego programowanie wieloletnie i roczne wraz z odpowiadającym mu planowaniem w odniesieniu do zasobów ludzkich i finansowych zgodnie z art. 32 rozporządzenia delegowanego Komisji (UE) nr 1271/2013[36] i z uwzględnieniem wytycznych ustanowionych przez Komisję.

3. Do dnia 30 listopada każdego roku zarząd przyjmuje jednolity dokument programowy, o którym mowa w ust. 1, i nie później niż w dniu 31 stycznia następnego roku przekazuje go Parlamentowi Europejskiemu, Radzie i Komisji; zarząd przekazuje także wszelkie późniejsze zaktualizowane wersje tego dokumentu.

4. Jednolity dokument programowy staje się ostateczny po ostatecznym przyjęciu budżetu ogólnego Unii i w razie potrzeby podlega odpowiednim dostosowaniom.

5. Roczny program prac zawiera szczegółowe cele i oczekiwane wyniki, w tym wskaźniki skuteczności. Zawiera on również opis działań, które mają być finansowane, oraz wskazanie zasobów finansowych i ludzkich przydzielonych do każdego działania zgodnie z zasadami budżetowania zadaniowego i zarządzania kosztami działań. Roczny program prac musi być spójny z wieloletnim programem prac, o którym mowa w ust. 7. Jednoznacznie określa on zadania, które zostały dodane, zmienione lub skreślone w stosunku do poprzedniego roku budżetowego.

---

36 Rozporządzenie delegowane Komisji (UE) nr 1271/2013 z dnia 30 września 2013 r. w sprawie ramowego rozporządzenia finansowego dotyczącego organów, o których mowa w art. 208 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 966/2012 (Dz.U. L 328 z 7.12.2013, s. 42).

6. Zarząd dokonuje zmiany przyjętego rocznego programu prac w przypadku przekazania Agencji nowego zadania. Wszelkie istotne zmiany w rocznym programie prac przyjmuje się w drodze tej samej procedury co pierwotny roczny program prac. Zarząd może przekazać dyrektorowi wykonawczemu uprawnienia do dokonywania w rocznym programie prac zmian innych niż istotne.

7. W wieloletnim programie prac określa się ogólne programowanie strategiczne, w tym cele, oczekiwane rezultaty i wskaźniki skuteczności. Wyznacza się w nim również programowanie w zakresie zasobów, w tym budżetu wieloletniego i personelu.

8. Programowanie w zakresie zasobów jest co roku aktualizowane. Programowanie strategiczne aktualizuje się w razie potrzeby, a w szczególności gdy jest to niezbędne w celu uwzględnienia wyników oceny, o której mowa w art. 56.

Artykuł 22
Deklaracja interesów

1. Członkowie zarządu, dyrektor wykonawczy oraz urzędnicy oddelegowani czasowo przez państwa członkowskie składają oświadczenie dotyczące zobowiązań oraz oświadczenie wskazujące na brak lub istnienie jakichkolwiek bezpośrednich lub pośrednich interesów, które mogłyby zostać uznane za szkodzące ich niezależności. Oświadczenia te muszą być dokładne i wyczerpujące, składane co roku na piśmie i w razie konieczności aktualizowane.

2. Członkowie zarządu, dyrektor wykonawczy i eksperci zewnętrzni uczestniczący w grupach roboczych *ad hoc* dokładnie i wyczerpująco zgłaszają najpóźniej na początku każdego posiedzenia wszelkie interesy, które mogłyby zostać uznane za szkodzące ich niezależności w odniesieniu do zagadnień przewidzianych w porządku obrad, oraz powstrzymują się od udziału w dyskusjach i głosowaniach dotyczących tych punktów.

3. W wewnętrznych zasadach działania Agencja określa praktyczne rozwiązania w zakresie zasad dotyczących deklaracji interesów, o których mowa w ust. 1 i 2.

Artykuł 23
Przejrzystość

1. Agencja wykonuje swoje działania z zachowaniem wysokiego stopnia przejrzystości oraz zgodnie z art. 25.

2. Agencja zapewnia, aby społeczeństwo i wszelkie inne zainteresowane strony otrzymywały odpowiednie, obiektywne, wiarygodne i łatwo dostępne informacje, w szczególności dotyczące wyników jej pracy. Agencja podaje również do wiadomości publicznej deklaracje interesów złożone zgodnie z art. 22.

3. Zarząd, działając na wniosek dyrektora wykonawczego, może upoważnić zainteresowane strony do obserwowania przebiegu niektórych działań Agencji.

4. W wewnętrznych zasadach działania Agencja określa praktyczne rozwiązania w zakresie wdrażania zasad przejrzystości, o których mowa w ust. 1 i 2.

Artykuł 24
Poufność

1. Nie naruszając przepisów art. 25, Agencja nie ujawnia stronom trzecim przetwarzanych lub otrzymywanych przez siebie informacji, w odniesieniu do których, w całości lub w części, zgłoszono uzasadniony wniosek o zachowanie poufności.

2. Członkowie zarządu, dyrektor wykonawczy, członkowie Stałej Grupy Przedstawicieli Zainteresowanych Stron, eksperci zewnętrzni uczestniczący w pracach grup roboczych *ad hoc* oraz pracownicy Agencji, w tym również urzędnicy oddelegowani czasowo przez państwa członkowskie, podlegają wymogom dotyczącym poufności określonym w art. 339 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), nawet po zakończeniu pełnienia swoich obowiązków.

3. W wewnętrznych zasadach działania Agencja określa praktyczne rozwiązania w zakresie wdrażania zasad poufności, o których mowa w ust. 1 i 2.

4. Jeżeli wymaga tego realizacja zadań Agencji, zarząd podejmuje decyzję o zezwoleniu Agencji na korzystanie z informacji niejawnych. W takim przypadku zarząd, w porozumieniu ze służbami Komisji, przyjmuje wewnętrzne zasady działania uwzględniające zasady bezpieczeństwa określone w decyzjach Komisji (UE, Euratom) 2015/443[37] i 2015/444[38]. Zasady te obejmują przepisy dotyczące wymiany, przetwarzania i przechowywania informacji niejawnych.

Artykuł 25
Dostęp do dokumentów

1. Rozporządzenie (WE) nr 1049/2001 ma zastosowanie do dokumentów pozostających w posiadaniu Agencji.

2. Zarząd przyjmuje ustalenia dotyczące wykonania rozporządzenia (WE) nr 1049/2001 w ciągu sześciu miesięcy od ustanowienia Agencji.

3. Decyzje podjęte przez Agencję na podstawie art. 8 rozporządzenia (WE) nr 1049/2001 mogą być przedmiotem skarg składanych do Europejskiego Rzecznika Praw Obywatelskich na podstawie art. 228 TFUE lub skarg wnoszonych do Trybunału Sprawiedliwości Unii Europejskiej na podstawie art. 263 TFUE.

[37] 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).

[38] Decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 72 z 17.3.2015, s. 53).

ROZDZIAŁ III
USTANOWIENIE I STRUKTURA BUDŻETU

Artykuł 26
Ustanowienie budżetu

1. Każdego roku dyrektor wykonawczy sporządza projekt preliminarza dochodów i wydatków Agencji w następnym roku budżetowym oraz przekazuje ten projekt zarządowi wraz z projektem planu zatrudnienia. Dochody i wydatki muszą się równoważyć.

2. Każdego roku zarząd opracowuje, na podstawie projektu preliminarza dochodów i wydatków, o którym mowa w ust. 1, preliminarz dochodów i wydatków Agencji w następnym roku budżetowym.

3. Do dnia 31 stycznia każdego roku zarząd przesyła Komisji oraz państwom trzecim, z którymi Unia zawarła umowy zgodnie z art. 39, preliminarz, o którym mowa w ust. 2, stanowiący część projektu jednolitego dokumentu programowego.

4. Na podstawie tego preliminarza Komisja wprowadza do projektu budżetu Unii przewidywane kwoty, które uważa za niezbędne w związku z planem zatrudnienia, oraz kwotę wkładu, który ma być wniesiony z budżetu ogólnego, oraz przedkłada ten projekt Parlamentowi Europejskiemu i Radzie zgodnie z art. 313 i 314 TFUE.

5. Parlament Europejski i Rada zatwierdzają środki na wkład na rzecz Agencji.

6. Parlament Europejski i Rada przyjmują plan zatrudnienia Agencji.

7. Zarząd przyjmuje budżet Agencji równocześnie z jednolitym dokumentem programowym. Budżet staje się ostateczny po ostatecznym przyjęciu budżetu ogólnego Unii. W stosownych przypadkach zarząd dostosowuje budżet i jednolity dokument programowy Agencji zgodnie z budżetem ogólnym Unii.

Artykuł 27
Struktura budżetu

1. Bez uszczerbku dla innych zasobów na dochody Agencji składają się:

   a) wkład z budżetu Unii;

   b) dochody przypisane do określonych pozycji wydatków zgodnie z przepisami finansowymi Agencji, o których mowa w art. 29;

   c) finansowanie unijne w formie umów o delegowaniu zadań lub dotacji *ad hoc* zgodnie z przepisami finansowymi Agencji, o których mowa w art. 29, oraz postanowieniami odpowiednich instrumentów wspierających politykę Unii;

   d) wkłady państw trzecich uczestniczących w pracach Agencji, zgodnie z przepisami art. 39;

   e) wszelkie dobrowolne finansowe lub rzeczowe wkłady państw członkowskich; państwa członkowskie dobrowolnie wnoszące wkład nie mogą domagać się przyznania im w zamian żadnych specjalnych praw ani świadczeń.

2. Wydatki Agencji obejmują wydatki na personel, wsparcie administracyjne i techniczne oraz infrastrukturę, wydatki operacyjne oraz wydatki wynikające z umów zawartych ze stronami trzecimi.

Artykuł 28
Wykonanie budżetu

1. Dyrektor wykonawczy jest odpowiedzialny za wykonanie budżetu Agencji.
2. Audytor wewnętrzny Komisji ma te same uprawnienia wobec Agencji co wobec departamentów Komisji.
3. Do dnia 1 marca następującego po każdym roku budżetowym (1 marca roku N + 1) księgowy Agencji przesyła wstępne sprawozdanie finansowe księgowemu Komisji oraz Trybunałowi Obrachunkowemu.
4. Otrzymawszy uwagi Trybunału Obrachunkowego dotyczące wstępnego sprawozdania finansowego Agencji, księgowy Agencji sporządza na własną odpowiedzialność ostateczne sprawozdanie finansowe Agencji.
5. Dyrektor wykonawczy przedkłada ostateczne sprawozdanie finansowe zarządowi do zaopiniowania.
6. Do dnia 31 marca roku N + 1 dyrektor wykonawczy przesyła sprawozdanie z zarządzania budżetem i finansami Parlamentowi Europejskiemu, Radzie, Komisji i Trybunałowi Obrachunkowemu.
7. Do dnia 1 lipca roku N + 1 księgowy przesyła ostateczne sprawozdanie finansowe wraz z opinią zarządu Parlamentowi Europejskiemu, Radzie, księgowemu Komisji i Trybunałowi Obrachunkowemu.
8. W dniu przesłania ostatecznego sprawozdania finansowego księgowy przesyła Trybunałowi Obrachunkowemu – wraz z kopią dla księgowego Komisji – również oświadczenie potwierdzające prawidłowość i rzetelność danych zawartych w tym sprawozdaniu.
9. Dyrektor wykonawczy publikuje ostateczne sprawozdanie finansowe do dnia 15 listopada następnego roku.
10. Do dnia 30 września roku N + 1 dyrektor wykonawczy przesyła Trybunałowi Obrachunkowemu odpowiedź na jego uwagi, a kopię tej odpowiedzi przesyła także zarządowi i Komisji.
11. Dyrektor wykonawczy przedkłada Parlamentowi Europejskiemu, na jego wniosek, wszystkie informacje niezbędne do sprawnego stosowania procedury udzielenia absolutorium za dany rok budżetowy, zgodnie z art. 165 ust. 3 rozporządzenia finansowego.
12. Parlament Europejski, działając na podstawie zalecenia Rady, udziela dyrektorowi wykonawczemu, do dnia 15 maja roku N + 2, absolutorium z wykonania budżetu w roku N.

Artykuł 29

Przepisy finansowe

Przepisy finansowe mające zastosowanie do Agencji przyjmuje zarząd po konsultacji z Komisją. Przepisy te nie odbiegają od rozporządzenia (UE) nr 1271/2013, chyba że takie różnice są specjalnie wymagane dla funkcjonowania Agencji, a Komisja wydała na nie uprzednią zgodę.

Artykuł 30

Zwalczanie nadużyć finansowych

1. W celu ułatwienia zwalczania nadużyć finansowych, korupcji i innych nielegalnych działań na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013[39] Agencja, w ciągu sześciu miesięcy od dnia rozpoczęcia swojej działalności, przystępuje do Porozumienia międzyinstytucjonalnego z dnia 25 maja 1999 r. dotyczącego dochodzeń wewnętrznych prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz przyjmuje odpowiednie przepisy mające zastosowanie do wszystkich pracowników Agencji, wykorzystując w tym celu wzór określony w załączniku do tego porozumienia.

2. Trybunał Obrachunkowy jest uprawniony do kontroli, na podstawie dokumentacji i na miejscu, wszystkich beneficjentów dotacji, wykonawców i podwykonawców, którzy otrzymują od Agencji unijne środki finansowe.

3. OLAF może przeprowadzać dochodzenia, w tym kontrole na miejscu i inspekcje, zgodnie z przepisami i procedurami określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 oraz w rozporządzeniu 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[40], aby ustalić, czy miały miejsce nadużycia finansowe, korupcja lub jakakolwiek inna nielegalna działalność na szkodę interesów finansowych Unii w związku z dokonywanym przez Agencję finansowaniem dotacji lub umowy.

4. Nie naruszając przepisów ust. 1, 2 i 3, w zawieranych przez Agencję umowach o współpracy z państwami trzecimi i organizacjami międzynarodowymi, udzielanych przez nią zamówieniach, zawieranych umowach o udzielenie dotacji i przyjmowanych decyzjach o udzieleniu dotacji zamieszcza się postanowienia wyraźnie upoważniające Trybunał Obrachunkowy i OLAF do prowadzenia takich kontroli i dochodzeń zgodnie z ich odpowiednimi uprawnieniami.

---

39 Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz uchylające rozporządzenie (WE) nr 1073/1999 Parlamentu Europejskiego i Rady i rozporządzenie Rady (Euratom) nr 1074/1999 (Dz.U. L 248 z 18.9.2013, s. 1).

40 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).

ROZDZIAŁ IV
PERSONEL AGENCJI

Artykuł 31
Przepisy ogólne

Do personelu Agencji mają zastosowanie regulamin pracowniczy i warunki zatrudnienia innych pracowników oraz przepisy przyjęte w drodze porozumienia między instytucjami Unii w celu nadania skuteczności regulaminowi pracowniczemu.

Artykuł 32
Przywileje i immunitety

Do Agencji i jej personelu ma zastosowanie Protokół nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej, załączony do Traktatu o Unii Europejskiej i do TFUE.

Artykuł 33
Dyrektor wykonawczy

1. Dyrektor wykonawczy zatrudniany jest w Agencji na czas określony, zgodnie z art. 2 lit. a) warunków zatrudnienia innych pracowników.
2. Dyrektor wykonawczy jest powoływany przez zarząd na podstawie listy kandydatów zaproponowanych przez Komisję w następstwie otwartej i przejrzystej procedury selekcji.
3. Do celu zawarcia umowy z dyrektorem wykonawczym Agencję reprezentuje przewodniczący zarządu.
4. Przed powołaniem kandydat wybrany przez zarząd zostaje wezwany do złożenia oświadczenia przed odpowiednią komisją Parlamentu Europejskiego i udzielenia odpowiedzi na pytania posłów.
5. Kadencja dyrektora wykonawczego trwa pięć lat. Przed upływem tego okresu Komisja przeprowadza ocenę, w której uwzględnia ocenę wykonywania zadań przez dyrektora wykonawczego oraz przyszłe zadania i wyzwania Agencji.
6. Zarząd podejmuje decyzje w sprawie powołania, przedłużenia kadencji lub odwołania ze stanowiska dyrektora wykonawczego większością dwóch trzecich głosów członków z prawem głosu.
7. Zarząd, działając na wniosek Komisji, w którym uwzględniono ocenę, o której mowa w ust. 5, może przedłużyć kadencję dyrektora wykonawczego jeden raz, na okres nie dłuższy niż pięć lat.
8. Zarząd informuje Parlament Europejski o swoim zamiarze przedłużenia kadencji dyrektora wykonawczego. W ciągu trzech miesięcy poprzedzających takie przedłużenie dyrektor wykonawczy, jeżeli zostanie wezwany, składa oświadczenie przed odpowiednią komisją Parlamentu Europejskiego i udziela odpowiedzi na pytania posłów.
9. Dyrektor wykonawczy, którego kadencję przedłużono, nie może brać udziału w kolejnej procedurze selekcji na to samo stanowisko.

10. Dyrektor wykonawczy może zostać odwołany ze stanowiska jedynie na mocy decyzji zarządu działającego na wniosek Komisji.

Artykuł 34
Oddelegowani eksperci krajowi i inni pracownicy

1. Agencja może korzystać z pomocy oddelegowanych ekspertów krajowych lub innych pracowników niezatrudnionych przez Agencję. Do takich pracowników nie ma zastosowania regulamin pracowniczy i warunki zatrudnienia innych pracowników.
2. Zarząd przyjmuje decyzję określającą zasady oddelegowania ekspertów krajowych do Agencji.

ROZDZIAŁ V
PRZEPISY OGÓLNE

Artykuł 35
***Status prawny* Agencji**

1. Agencja jest organem Unii i posiada osobowość prawną.
2. W każdym państwie członkowskim Agencja ma najszerszy zakres zdolności prawnej, jaki można nadać osobie prawnej na mocy prawa krajowego. W szczególności Agencja może nabywać lub zbywać ruchomości i nieruchomości, może być stroną w postępowaniach sądowych lub korzystać z obu tych uprawnień.
3. Agencję reprezentuje jej dyrektor wykonawczy.

Artykuł 36
Odpowiedzialność Agencji

1. Odpowiedzialność umowną Agencji reguluje prawo właściwe dla danej umowy.
2. Trybunał Sprawiedliwości Unii Europejskiej jest właściwy do rozstrzygania sporów na podstawie klauzul arbitrażowych zamieszczonych w umowach zawartych przez Agencję.
3. W przypadku odpowiedzialności pozaumownej Agencja, zgodnie z ogólnymi zasadami wspólnymi dla praw państw członkowskich, rekompensuje wszelkie szkody wyrządzone przez Agencję lub jej pracowników w trakcie wykonywania swoich obowiązków.
4. Trybunał Sprawiedliwości Unii Europejskiej jest właściwy do orzekania we wszelkich sporach dotyczących rekompensaty za tego rodzaju szkody.
5. Odpowiedzialność osobista pracowników Agencji wobec Agencji jest regulowana odpowiednimi warunkami mającymi zastosowanie do jej personelu.

Artykuł 37

System językowy

1. Do Agencji ma zastosowanie rozporządzenie Rady nr 1[41]. Państwa członkowskie i inne organy przez nie wyznaczone mogą zwracać się do Agencji i otrzymywać odpowiedzi w wybranym przez siebie języku urzędowym instytucji Unii.

2. Usługi tłumaczeniowe niezbędne dla funkcjonowania Agencji zapewnia Centrum Tłumaczeń dla Organów Unii Europejskiej.

Artykuł 38

Ochrona danych osobowych

1. Przetwarzanie danych osobowych przez Agencję podlega przepisom rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady[42].

2. Zarząd przyjmuje środki wykonawcze, o których mowa w art. 24 ust. 8 rozporządzenia (WE) nr 45/2001. Zarząd może przyjąć dodatkowe środki niezbędne do stosowania rozporządzenia (WE) nr 45/2001 przez Agencję.

Artykuł 39

Współpraca z państwami trzecimi i organizacjami międzynarodowymi

1. W zakresie, w jakim jest to niezbędne do osiągnięcia celów określonych w niniejszym rozporządzeniu, Agencja może współpracować z właściwymi organami państw trzecich lub z organizacjami międzynarodowymi, bądź też z jednymi i drugimi. W tym celu, pod warunkiem uzyskania uprzedniej zgody Komisji, Agencja może poczynić ustalenia robocze z organami państw trzecich i organizacjami międzynarodowymi. Ustalenia te nie mogą powodować powstania zobowiązań prawnych dla Unii ani jej państw członkowskich.

2. Agencja jest otwarta na udział państw trzecich, które zawarły w tym celu odpowiednie umowy z Unią. Na podstawie odpowiednich postanowień tych umów dokonuje się ustaleń określających w szczególności charakter, zakres i sposób uczestniczenia tych państw w pracach Agencji, obejmujących postanowienia dotyczące udziału w inicjatywach podejmowanych przez Agencję, wkładów finansowych oraz personelu. W odniesieniu do kwestii kadrowych ustalenia te muszą być w każdym przypadku zgodne z regulaminem pracowniczym.

3. Zarząd przyjmuje strategię dotyczącą stosunków z państwami trzecimi lub organizacjami międzynarodowymi w kwestiach należących do kompetencji Agencji. Poprzez zawarcie odpowiednich ustaleń roboczych z dyrektorem wykonawczym Agencji Komisja zapewnia, aby Agencja działała w obrębie swojego mandatu i istniejących ram instytucjonalnych.

---

41 Rozporządzenie nr 1 w sprawie określenia systemu językowego Europejskiej Wspólnoty Energii Atomowej (Dz.U. 17 z 6.10.1958, s. 401).

42 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

Artykuł 40

Przepisy bezpieczeństwa w zakresie ochrony informacji niejawnych oraz szczególnie chronionych informacji jawnych

Konsultując się z Komisją, Agencja przyjmuje własne przepisy bezpieczeństwa wprowadzające zasady bezpieczeństwa zawarte w przepisach bezpieczeństwa Komisji dotyczących ochrony informacji niejawnych UE (EUCI) oraz szczególnie chronionych informacji jawnych, określone w decyzjach Komisji (UE, Euratom) 2015/443 i 2015/444. Obejmuje to między innymi postanowienia dotyczące wymiany, przetwarzania i przechowywania takich informacji.

Artykuł 41

Umowa w sprawie siedziby i warunki działania

1. Niezbędne ustalenia dotyczące pomieszczeń, które przyjmujące państwo członkowskie ma przeznaczyć dla Agencji, oraz wyposażenia, które ma zostać udostępnione przez to państwo członkowskie, wraz ze szczegółowymi przepisami mającymi zastosowanie w przyjmującym państwie członkowskim do dyrektora wykonawczego, członków zarządu, pracowników agencji i członków ich rodzin określa się w umowie w sprawie siedziby między Agencją a państwem członkowskim, w którym siedziba ta została zlokalizowana, zawartej po uzyskaniu zgody zarządu i nie później niż [2 lata po wejściu w życie niniejszego rozporządzenia].
2. Państwo członkowskie przyjmujące Agencję zapewnia możliwie najlepsze warunki dla zapewnienia właściwego funkcjonowania Agencji, w tym dostępność lokalizacji, odpowiednią infrastrukturę szkolną dla dzieci członków personelu, odpowiedni dostęp do rynku pracy, zabezpieczenie społeczne i opiekę zdrowotną zarówno dla dzieci, jak i dla małżonków.

Artykuł 42

Kontrola administracyjna

Zgodnie z art. 228 TFUE Europejski Rzecznik Praw Obywatelskich nadzoruje działalność Agencji.

TYTUŁ III
RAMY CERTYFIKACJI CYBERBEZPIECZEŃSTWA

Artykuł 43

Europejskie systemy certyfikacji cyberbezpieczeństwa

Europejski system certyfikacji cyberbezpieczeństwa poświadcza, że produkty i usługi ICT, które zostały poddane certyfikacji zgodnie z takim systemem, spełniają określone wymogi w odniesieniu do swojej odporności, przy danym poziomie pewności, na działania, których celem jest naruszenie dostępności, autentyczności, integralności lub poufności przechowywanych lub przekazywanych lub przetwarzanych danych, lub też funkcji bądź usług oferowanych lub dostępnych za pośrednictwem tych produktów, procesów, usług i systemów.

Artykuł 44

Przygotowanie i przyjęcie europejskiego systemu certyfikacji cyberbezpieczeństwa

1. Po otrzymaniu wniosku Komisji ENISA przygotowuje kandydujący europejski system certyfikacji cyberbezpieczeństwa, który spełnia wymogi określone w art. 45, 46 i 47 niniejszego rozporządzenia. Państwa członkowskie lub Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa („Grupa”) ustanowiona na mocy art. 53 mogą zaproponować Komisji przygotowanie kandydującego europejskiego systemu certyfikacji cyberbezpieczeństwa.
2. Przygotowując kandydujące systemy, o których mowa w ust. 1 niniejszego artykułu, ENISA konsultuje się z wszystkimi odpowiednimi zainteresowanymi stronami i ściśle współpracuje z Grupą. ENISA uzyskuje od Grupy pomoc i fachowe doradztwo, których potrzebuje w związku z przygotowywaniem kandydującego systemu, w tym – w razie potrzeby – opinie.
3. ENISA przekazuje Komisji kandydujący europejski system certyfikacji cyberbezpieczeństwa przygotowany zgodnie z ust. 2 niniejszego artykułu.
4. Komisja, w oparciu o kandydujący system zaproponowany przez ENISA, może zgodnie z art. 55 ust. 2 przyjąć akty wykonawcze ustanawiające europejskie systemy certyfikacji cyberbezpieczeństwa produktów i usług ICT spełniające wymogi art. 45, 46 i 47 niniejszego rozporządzenia.
5. ENISA utrzymuje specjalną stronę internetową zawierającą informacje na temat europejskich systemów certyfikacji cyberbezpieczeństwa i propagującą te systemy.

Artykuł 45

Cele w zakresie bezpieczeństwa europejskich systemów certyfikacji cyberbezpieczeństwa

Europejski system certyfikacji cyberbezpieczeństwa musi być tak zaprojektowany, aby odpowiednio uwzględniać następujące cele w zakresie bezpieczeństwa:

a) ochronę przechowywanych, przekazywanych lub w inny sposób przetwarzanych danych przed przypadkowym lub nieuprawnionym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem;

b) ochronę przechowywanych, przekazywanych lub w inny sposób przetwarzanych danych przed przypadkowym lub nieuprawnionym zniszczeniem, przypadkową utratą lub zmianą;

c) zapewnienie możliwości dostępu uprawnionych osób, programów lub maszyn wyłącznie do tych danych, usług lub funkcji, do których odnoszą się ich prawa dostępu;

d) rejestrację tego, które dane, funkcje lub usługi zostały przekazane, kiedy i przez kogo;

e) zapewnienie możliwości kontroli, do których danych, usług lub funkcji uzyskano dostęp lub z których danych, usług lub funkcji korzystano, kiedy to miało miejsce i kto tego dokonał;

f) przywracanie w odpowiednim czasie dostępności danych, usług i funkcji oraz dostępu do nich w przypadku incydentu fizycznego lub technicznego;

g) zapewnienie oferowania produktów i usług ICT wraz z aktualnym oprogramowaniem niezawierającym znanych luk w zabezpieczeniach oraz istnienia mechanizmów bezpiecznej aktualizacji oprogramowania.

Artykuł 46

Poziomy pewności europejskich systemów certyfikacji cyberbezpieczeństwa

1. W odniesieniu do produktów i usług ICT certyfikowanych w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa można określić jeden lub więcej następujących poziomów pewności: podstawowy, znaczny lub wysoki.

2. Poziomy pewności podstawowy, znaczny lub wysoki spełniają odpowiednio następujące kryteria:

a) podstawowy poziom pewności odnosi się do certyfikatu wydanego w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa, który to certyfikat zapewnia ograniczony poziom ufności odnośnie do deklarowanych lub postulowanych właściwości w zakresie cyberbezpieczeństwa produktu lub usługi ICT i charakteryzuje się odniesieniem do związanych z nim specyfikacji technicznych, norm i procedur, w tym kontroli technicznych, których celem jest zmniejszenie ryzyka wystąpienia cyberincydentów;

b) znaczny poziom pewności odnosi się do certyfikatu wydanego w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa, który to certyfikat zapewnia znaczny poziom ufności odnośnie do deklarowanych lub postulowanych właściwości w zakresie cyberbezpieczeństwa produktu lub usługi ICT i charakteryzuje się odniesieniem do związanych z nim specyfikacji technicznych, norm i procedur, w tym kontroli technicznych, których celem jest znaczne zmniejszenie ryzyka wystąpienia cyberincydentów;

c) wysoki poziom pewności odnosi się do certyfikatu wydanego w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa, który to certyfikat zapewnia wyższy poziom ufności odnośnie do deklarowanych lub postulowanych właściwości w zakresie cyberbezpieczeństwa produktu lub usługi ICT niż certyfikaty poświadczające znaczny poziom pewności i charakteryzuje się odniesieniem do związanych z nim specyfikacji

technicznych, norm i procedur, w tym kontroli technicznych, których celem jest zapobieganie cyberincydentom.

Artykuł 47

Elementy europejskich systemów certyfikacji cyberbezpieczeństwa

1. Europejski system certyfikacji cyberbezpieczeństwa obejmuje następujące elementy:

   a) przedmiot i zakres certyfikacji, w tym rodzaj lub kategorie objętych danym systemem produktów i usług ICT;

   b) szczegółową specyfikację wymogów w zakresie cyberbezpieczeństwa, w stosunku do których oceniane są produkty i usługi ICT, na przykład poprzez odniesienie do norm unijnych lub międzynarodowych bądź specyfikacji technicznych;

   c) w stosownych przypadkach jeden lub więcej poziomów pewności;

   d) szczegółowe kryteria oceny i metody, w tym rodzaje oceny, stosowane w celu wykazania, że zostały osiągnięte szczegółowe cele, o których mowa w art. 45;

   e) informacje, które wnioskodawca ma dostarczać jednostkom oceniającym zgodność i które są niezbędne do celów certyfikacji;

   f) w przypadku gdy system przewiduje stosowanie znaków lub etykiet – warunki, na jakich takie znaki lub etykiety mogą być stosowane;

   g) jeżeli nadzór stanowi część systemu – zasady monitorowania zgodności z wymogami certyfikatów, w tym mechanizmy wykazywania ciągłej zgodności z określonymi wymogami w zakresie cyberbezpieczeństwa;

   h) warunki przyznawania, utrzymania, kontynuowania oraz rozszerzania i zmniejszania zakresu certyfikacji;

   i) zasady dotyczące konsekwencji niezgodności certyfikowanych produktów i usług ICT z wymogami w zakresie certyfikacji;

   j) zasady dotyczące sposobu zgłaszania uprzednio niewykrytych luk w cyberzabezpieczeniach produktów i usług ICT oraz sposobu postępowania z takimi lukami;

   k) zasady dotyczące zachowywania zarejestrowanych danych przez jednostki oceniające zgodność;

   l) identyfikację krajowych systemów certyfikacji cyberbezpieczeństwa, obejmujących ten sam rodzaj lub kategorie produktów i usług ICT;

   m) treść wydanego certyfikatu.

2. Określone wymogi systemu nie mogą być sprzeczne z żadnymi obowiązującymi wymogami prawnymi, w szczególności z wymogami wynikającymi ze zharmonizowanego prawodawstwa Unii.

3. Jeżeli dany akt unijny tak stanowi, certyfikacja w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa może być stosowana do wykazania domniemania zgodności z wymogami tego aktu.

4. W przypadku braku zharmonizowanego prawodawstwa Unii przepisy prawa państwa członkowskiego mogą również stanowić, że europejski system certyfikacji

cyberbezpieczeństwa może być stosowany do ustanowienia domniemania zgodności z wymogami prawnymi.

Artykuł 48

Certyfikacja cyberbezpieczeństwa

1. Przyjmuje się, że produkty i usługi ICT, które uzyskały certyfikację w ramach przyjętego na podstawie art. 44 europejskiego systemu certyfikacji cyberbezpieczeństwa, są zgodne z wymogami takiego systemu.
2. Certyfikacja jest dobrowolna, o ile prawo Unii nie stanowi inaczej.
3. Europejski certyfikat cyberbezpieczeństwa na podstawie niniejszego artykułu jest wydawany przez jednostki oceniające zgodność, o których mowa w art. 51, w oparciu o kryteria uwzględnione w europejskim systemie certyfikacji cyberbezpieczeństwa przyjętym na podstawie art. 44.
4. Na zasadzie odstępstwa od ust. 3, w należycie uzasadnionych przypadkach, określony europejski system certyfikacji cyberbezpieczeństwa może przewidywać, że europejski certyfikat cyberbezpieczeństwa będący wynikiem tego systemu może być wydawany jedynie przez podmiot publiczny. Takim podmiotem publicznym musi być jeden z wymienionych poniżej podmiotów:
   a) krajowy organ nadzoru ds. certyfikacji, o którym mowa w art. 50 ust. 1;
   b) podmiot akredytowany jako jednostka oceniająca zgodność na podstawie art. 51 ust. 1; lub
   c) podmiot ustanowiony na mocy przepisów ustawowych, instrumentów prawnych lub innych urzędowych procedur administracyjnych zainteresowanego państwa członkowskiego i spełniający wymogi dotyczące podmiotów certyfikujących produkty, procesy i usługi zgodnie z normą ISO/IEC 17065:2012.
5. Osoba fizyczna lub prawna, która poddaje swoje produkty lub usługi ICT mechanizmowi certyfikacji, przekazuje jednostce oceniającej zgodność, o której mowa w art. 51, wszystkie informacje niezbędne do przeprowadzenia procedury certyfikacji.
6. Certyfikaty wydaje się na maksymalny okres trzech lat i mogą one zostać odnowione, na tych samych warunkach, o ile nadal spełnione są odpowiednie wymogi.
7. Europejski certyfikat cyberbezpieczeństwa wydany na podstawie niniejszego artykułu jest uznawany we wszystkich państwach członkowskich.

Artykuł 49

Krajowe systemy certyfikacji cyberbezpieczeństwa i certyfikaty cyberbezpieczeństwa

1. Nie naruszając przepisów ust. 3, krajowe systemy certyfikacji cyberbezpieczeństwa i powiązane procedury dotyczące produktów i usług ICT objętych europejskim systemem certyfikacji cyberbezpieczeństwa przestają wywoływać skutki z dniem określonym w akcie wykonawczym przyjętym na podstawie art. 44 ust. 4. Istniejące krajowe systemy certyfikacji cyberbezpieczeństwa i powiązane procedury dotyczące

produktów i usług ICT nieobjętych europejskim systemem certyfikacji cyberbezpieczeństwa nadal funkcjonują.

2. Państwa członkowskie nie wprowadzają nowych krajowych systemów certyfikacji cyberbezpieczeństwa dotyczących produktów i usług ICT objętych obowiązującym europejskim systemem certyfikacji cyberbezpieczeństwa.

3. Istniejące certyfikaty wydane w ramach krajowych systemów certyfikacji cyberbezpieczeństwa pozostają ważne do upływu ich terminu ważności.

Artykuł 50

Krajowe organy nadzoru ds. certyfikacji

1. Każde państwo członkowskie powołuje krajowy organ nadzoru ds. certyfikacji.

2. Każde państwo członkowskie informuje Komisję o tożsamości powołanego organu.

3. Każdy krajowy organ nadzoru ds. certyfikacji pozostaje – w zakresie swojej organizacji, decyzji w sprawie finansowania, struktury prawnej i procesu podejmowania decyzji – niezależny od jednostek, nad którymi sprawuje nadzór.

4. Państwa członkowskie zapewniają, aby krajowe organy nadzoru ds. certyfikacji posiadały odpowiednie zasoby na potrzeby wykonywania swoich uprawnień i wywiązywania się w skuteczny i wydajny sposób z przydzielonych im zadań.

5. W celu skutecznego wykonania niniejszego rozporządzenia organy te powinny uczestniczyć w aktywny, skuteczny, wydajny i bezpieczny sposób w pracach Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa ustanowionej na mocy art. 53.

6. Krajowe organy nadzoru ds. certyfikacji:

   a) monitorują i egzekwują stosowanie przepisów niniejszego tytułu na poziomie krajowym oraz sprawują nadzór nad zgodnością certyfikatów wydanych przez jednostki oceniające zgodność mające siedzibę na odpowiednio podlegających tym organom terytoriach z wymogami określonymi w niniejszym tytule i w odpowiednim europejskim systemie certyfikacji cyberbezpieczeństwa;

   b) monitorują i nadzorują działalność jednostek oceniających zgodność do celów niniejszego rozporządzenia, w tym w związku z notyfikacją jednostek oceniających zgodność i związanymi z tym zadaniami określonymi w art. 52 niniejszego rozporządzenia;

   c) rozpatrują skargi złożone przez osoby fizyczne lub prawne w związku z certyfikatami wydanymi przez jednostki oceniające zgodność mające siedzibę na podlegających tym organom terytoriach, badają w odpowiednim zakresie przedmiot skarg oraz informują skarżących w stosownym terminie o postępach i wynikach badania;

   d) współpracują z innymi krajowymi organami nadzoru ds. certyfikacji lub innymi organami publicznymi, w tym poprzez wymianę informacji na temat ewentualnej niezgodności produktów i usług ICT z wymogami niniejszego rozporządzenia lub określonych europejskich systemów certyfikacji cyberbezpieczeństwa;

   e) śledzą odpowiednie zmiany w dziedzinie certyfikacji cyberbezpieczeństwa.

7. Każdy krajowy organ nadzoru ds. certyfikacji posiada co najmniej następujące uprawnienia:

a) prawo żądania od jednostek oceniających zgodność oraz posiadaczy europejskich certyfikatów cyberbezpieczeństwa przekazania wszelkich informacji, których organ ten potrzebuje do wykonania swojego zadania;

b) prawo przeprowadzania dochodzeń, w trybie kontroli, w stosunku do jednostek oceniających zgodność oraz posiadaczy europejskich certyfikatów cyberbezpieczeństwa, w celu weryfikacji zgodności z przepisami tytułu III;

c) prawo stosowania odpowiednich środków, zgodnie z prawem krajowym, w celu zapewnienia przestrzegania przepisów niniejszego rozporządzenia lub unormowań danego europejskiego systemu certyfikacji cyberbezpieczeństwa przez jednostki oceniające zgodność lub posiadaczy certyfikatów;

d) prawo uzyskania dostępu do wszelkich pomieszczeń jednostek oceniających zgodność oraz posiadaczy europejskich certyfikatów cyberbezpieczeństwa do celów prowadzenia dochodzeń zgodnie z prawem procesowym Unii lub danego państwa członkowskiego;

e) prawo cofania certyfikatów, zgodnie z prawem krajowym, które nie są zgodne z niniejszym rozporządzeniem lub danym europejskim systemem certyfikacji cyberbezpieczeństwa;

f) prawo nakładania kar, jak przewidziano w art. 54, zgodnie z prawem krajowym oraz żądania natychmiastowego zaprzestania naruszeń obowiązków określonych w niniejszym rozporządzeniu.

8. Krajowe organy nadzoru ds. certyfikacji współpracują ze sobą i z Komisją, a w szczególności wymieniają informacje, doświadczenia i dobre praktyki odnoszące się do certyfikacji cyberbezpieczeństwa i kwestii technicznych dotyczących cyberbezpieczeństwa produktów i usług ICT.

Artykuł 51

Jednostki oceniające zgodność

1. Jednostki oceniające zgodność są akredytowane przez krajową jednostkę akredytującą wyznaczoną na podstawie rozporządzenia (WE) nr 765/2008 jedynie wtedy, gdy spełniają one wymagania określone w załączniku do niniejszego rozporządzenia.

2. Akredytacji udziela się na maksymalnie pięć lat i można ją odnowić na tych samych warunkach, o ile jednostka oceniająca zgodność spełnia wymogi określone w niniejszym artykule. Jednostki akredytujące cofają akredytację jednostki oceniającej zgodność udzieloną na podstawie ust. 1 niniejszego artykułu, jeżeli warunki udzielenia akredytacji nie są spełnione, przestały być spełniane lub gdy działania podejmowane przez jednostkę oceniającą zgodność naruszają przepisy niniejszego rozporządzenia.

Artykuł 52
Notyfikacja

1. W odniesieniu do każdego europejskiego systemu certyfikacji cyberbezpieczeństwa przyjętego na podstawie art. 44 krajowe organy nadzoru ds. certyfikacji notyfikują Komisji akredytowane jednostki oceniające zgodność, które na podstawie udzielonej im akredytacji są uprawnione do wydawania certyfikatów poświadczających określone poziomy pewności, o których mowa w art. 46, oraz bez zbędnej zwłoki powiadamiają o wszelkich późniejszych zmianach w tym zakresie.

2. Po upływie roku od wejścia w życie danego europejskiego systemu certyfikacji cyberbezpieczeństwa Komisja publikuje w Dzienniku Urzędowym wykaz notyfikowanych jednostek oceniających zgodność.

3. Jeżeli Komisja otrzyma notyfikację po upływie okresu, o którym mowa w ust. 2, w ciągu dwóch miesięcy od daty otrzymania tej notyfikacji publikuje w *Dzienniku Urzędowym Unii Europejskiej* zmiany w wykazie, o którym mowa w ust. 2.

4. Krajowy organ nadzoru ds. certyfikacji może wystąpić do Komisji z wnioskiem o usunięcie jednostki oceniającej zgodność notyfikowanej przez ten krajowy organ nadzoru ds. certyfikacji z wykazu, o którym mowa w ust. 2 niniejszego artykułu. W ciągu miesiąca od daty otrzymania wniosku krajowego organu nadzoru ds. certyfikacji Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* odpowiednie zmiany w wykazie.

5. Komisja może w drodze aktów wykonawczych określać okoliczności, formaty i procedury dotyczące notyfikacji, o których mowa w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 55 ust. 2.

Artykuł 53
Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa

1. Ustanawia się Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa („Grupę”).

2. W skład Grupy wchodzą krajowe organy nadzoru ds. certyfikacji. Organy te są reprezentowane przez kierowników lub innych przedstawicieli wysokiego szczebla krajowych organów nadzoru ds. certyfikacji.

3. Zadania Grupy są następujące:

   a) doradzanie i pomaganie Komisji przy pracach nad zapewnieniem konsekwentnego wprowadzania i stosowania przepisów niniejszego tytułu, w szczególności w odniesieniu do kwestii związanych z polityką certyfikacji cyberbezpieczeństwa, koordynacji mechanizmów kształtowania polityki oraz przygotowywania europejskich systemów certyfikacji cyberbezpieczeństwa;

   b) pomoc, doradztwo i współpraca z ENISA w związku z przygotowywaniem kandydującego systemu zgodnie z art. 44 niniejszego rozporządzenia;

   c) proponowanie Komisji, aby zwróciła się do Agencji o przygotowanie kandydującego europejskiego systemu certyfikacji cyberbezpieczeństwa zgodnie z art. 44 niniejszego rozporządzenia;

d) przyjmowanie skierowanych do Komisji opinii dotyczących utrzymania i przeglądu istniejących europejskich systemów certyfikacji cyberbezpieczeństwa;

e) śledzenie odpowiednich zmian w dziedzinie certyfikacji cyberbezpieczeństwa i wymiana dobrych praktyk odnoszących się do systemów certyfikacji cyberbezpieczeństwa;

f) ułatwianie współpracy między krajowymi organami nadzoru ds. certyfikacji na mocy przepisów niniejszego tytułu poprzez wymianę informacji, a w szczególności poprzez ustanowienie metod efektywnej wymiany informacji związanych z wszystkimi kwestiami dotyczącymi certyfikacji cyberbezpieczeństwa.

4. Komisja przewodniczy Grupie i zapewnia jej obsługę sekretariatu, z pomocą ze strony ENISA, jak określono w art. 8 lit. a).

Artykuł 54
Kary

Państwa członkowskie ustanawiają przepisy o karach nakładanych w przypadku naruszenia przepisów niniejszego tytułu i unormowań europejskich systemów certyfikacji cyberbezpieczeństwa oraz stosują wszelkie niezbędne środki, aby zapewnić ich wykonanie. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie [najpóźniej do dnia … r./niezwłocznie] powiadamiają Komisję o tych przepisach i środkach, a następnie powiadamiają ją o wszelkich zmianach mających wpływ na te przepisy.

TYTUŁ IV
PRZEPISY KOŃCOWE

Artykuł 55
Procedura komitetowa

1. Komisję wspomaga komitet. 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 56
Ocena i przegląd

1. Nie później niż po pięciu latach od dnia, o którym mowa w art. 58, a następnie co pięć lat, Komisja ocenia wpływ, skuteczność i efektywność Agencji oraz jej metody pracy, a także ewentualną potrzebę zmiany mandatu Agencji oraz skutki finansowe wszelkich takich zmian. W ocenie tej uwzględnia się wszelkie informacje zwrotne przekazane Agencji w reakcji na jej działalność. Jeżeli Komisja uzna, że dalsze działanie Agencji w odniesieniu do powierzonych jej celów, mandatu i zadań nie jest już uzasadnione, może wnioskować o zmianę niniejszego rozporządzenia w zakresie przepisów dotyczących Agencji.
2. Ocena dotyczy również wpływu, skuteczności i efektywności przepisów tytułu III w odniesieniu do celów, którymi są zapewnienie odpowiedniego poziomu cyberbezpieczeństwa produktów i usług ICT w Unii oraz poprawa funkcjonowania rynku wewnętrznego.
3. Komisja przekazuje sprawozdanie z oceny wraz z wnioskami do Parlamentu Europejskiego, Rady i zarządu. Ustalenia zawarte w sprawozdaniu oceny podaje się do wiadomości publicznej.

Artykuł 57
Uchylenie oraz przejęcie praw i obowiązków

1. Rozporządzenie (WE) nr 526/2013 traci moc ze skutkiem od dnia [...] r.
2. Odniesienia do rozporządzenia (WE) nr 526/2013 i do ENISA odczytuje się jako odniesienia do niniejszego rozporządzenia i do Agencji.
3. Agencja jest następcą agencji, która została ustanowiona rozporządzeniem (WE) nr 526/2013, w odniesieniu do wszystkich praw własności, umów, zobowiązań prawnych, umów o pracę, zobowiązań finansowych i odpowiedzialności. Wszystkie obowiązujące decyzje zarządu i rady wykonawczej zachowują ważność, pod warunkiem że nie są sprzeczne z przepisami niniejszego rozporządzenia.
4. Agencję ustanawia się na czas nieokreślony, począwszy od dnia [...] r.

5. Dyrektor wykonawczy powołany na podstawie art. 24 ust. 4 rozporządzenia (WE) nr 526/2013 jest dyrektorem wykonawczym Agencji na pozostałą część kadencji.

6. Członkowie i zastępcy członków zarządu powołani na podstawie art. 6 rozporządzenia (WE) nr 526/2013 są członkami i zastępcami członków zarządu Agencji na pozostałą część kadencji.

Artykuł 58

Wejście w życie

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

2. Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie „agencji UE ds. cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji bezpieczeństwa technologii informacyjno-komunikacyjnych („akt/rozporządzenie ws. cyberbezpieczeństwa")

1.2. Dziedziny polityki, których dotyczy wniosek/inicjatywa

Dziedzina polityki: 09 – Sieci komunikacyjne, treści i technologie

Działanie: 09.02 Jednolity rynek cyfrowy

1.3. Charakter wniosku/inicjatywy

☒ Wniosek/inicjatywa dotyczy **nowego działania (Tytuł III – Certyfikacja)**

☐ Wniosek/inicjatywa dotyczy **nowego działania będącego następstwem projektu pilotażowego/działania przygotowawczego**[43]

☒ Wniosek/inicjatywa wiąże się z **przedłużeniem bieżącego działania (Tytuł II – Mandat ENISA)**

☐ Wniosek/inicjatywa dotyczy **działania, które zostało przekształcone pod kątem nowego działania**

1.4. Cele

1.4.1. Wieloletnie cele strategiczne Komisji wskazane we wniosku/inicjatywie

1. Zwiększenie odporności państw członkowskich, przedsiębiorstw i UE jako całości.

2. Zapewnienie prawidłowego funkcjonowania unijnego rynku wewnętrznego produktów i usług ICT.

3. Zwiększenie ogólnoświatowej konkurencyjności firm unijnych działających w sektorze ICT.

4. Zbliżenie przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich zawierających wymogi dotyczące cyberbezpieczeństwa.

1.4.2. Cele szczegółowe

Z myślą o ogólnych celach, w szerszym kontekście poddanej przeglądowi strategii cyberbezpieczeństwa, przedmiotowy instrument – poprzez wyznaczenie zakresu i mandatu ENISA oraz ustanowienie europejskich ram certyfikacji produktów i usług ICT – ma w zamyśle doprowadzić do osiągnięcia następujących celów szczegółowych:

1. Zwiększenie **zdolności i gotowości** państw członkowskich i przedsiębiorstw.
2. Poprawa **współpracy i koordynacji** między państwami członkowskimi oraz instytucjami, agencjami i organami UE.
3. Zwiększenie **zdolności na poziomie unijnym do uzupełniania działań państw członkowskich**, zwłaszcza w przypadku transgranicznych cyberkryzysów.

[43] O którym mowa w art. 54 ust. 2 lit. a) lub b) rozporządzenia finansowego.

4. Podnoszenie **poziomu świadomości** obywateli i przedsiębiorstw na temat cyberbezpieczeństwa.
5. Wzmocnienie zaufania do jednolitego rynku cyfrowego i innowacji cyfrowych dzięki zwiększeniu ogólnej **przejrzystości procesu zapewniania cyberbezpieczeństwa**[44] produktów i usług ICT.

ENISA będzie przyczyniać się do osiągnięcia wyżej wymienionych celów poprzez:

Zwiększone wsparcie w zakresie kształtowania polityki – zapewnianie Komisji i państwom członkowskim wytycznych i doradztwa w celu aktualizacji i rozwoju całościowych ram normatywnych w dziedzinie cyberbezpieczeństwa, jak również sektorowych inicjatyw polityczno-prawnych w obszarach dotyczących kwestii cyberbezpieczeństwa; wkład w prace grupy współpracy (art. 11 dyrektywy (UE) 2016/1148) poprzez zapewnianie wiedzy fachowej i pomocy; wspieranie opracowywania i wdrażania polityki w dziedzinie tożsamości elektronicznej i usług zaufania; propagowanie wymiany najlepszych praktyk między właściwymi organami.

Zwiększone wsparcie w zakresie budowania potencjału – zapewnianie wsparcia państwom członkowskim oraz unijnym instytucjom, organom i jednostkom organizacyjnym w celu rozwoju i usprawnienia zapobiegania problemom i incydentom w zakresie cyberbezpieczeństwa, ich wykrywania, analizowania, jak również zdolności do reagowania na nie; pomoc państwom członkowskim, na ich wniosek, w rozwoju krajowych zespołów CSIRT i opracowywaniu krajowych strategii cyberbezpieczeństwa; pomoc instytucjom Unii w opracowywaniu i przeglądzie unijnych strategii cyberbezpieczeństwa; zapewnianie szkoleń w zakresie cyberbezpieczeństwa; pomoc państwom członkowskim, poprzez grupę współpracy, w wymianie najlepszych praktyk; ułatwianie tworzenia sektorowych ośrodków wymiany i analizy informacji.

Wspieranie współpracy operacyjnej i zarządzania kryzysowego – wspieranie współpracy między właściwymi organami publicznymi oraz między zainteresowanymi stronami poprzez ustanowienie systematycznej współpracy z unijnymi instytucjami, organami i jednostkami organizacyjnymi zajmującymi się cyberbezpieczeństwem, cyberprzestępczością oraz ochroną prywatności i danych osobowych; zapewnienie obsługi sekretariatu sieci CSIRT (art. 12 ust. 2 dyrektywy (UE) 2016/1148), jak również wkład we współpracę operacyjną w ramach sieci poprzez zapewnienie, we współpracy z CERT-UE, wsparcia państwom członkowskim, na ich wniosek; organizowanie regularnych ćwiczeń w dziedzinie cyberbezpieczeństwa; wkład w opracowanie wspólnego reagowania na transgraniczne cyberincydenty na dużą skalę i cyberkryzysy; prowadzenie, we współpracy z CERT-UE, technicznych postępowań wyjaśniających *ex post* dotyczących istotnych incydentów i wydawanie zaleceń w następstwie tych postępowań.

Zadania związane z rynkiem (normalizacja, certyfikacja) – wykonywanie szeregu funkcji w określony sposób wspierających rynek wewnętrzny: „centrum monitorowania rynku" cyberbezpieczeństwa, analizujące istotne tendencje na rynku cyberbezpieczeństwa w celu lepszego dopasowania popytu i podaży; wspieranie i propagowanie opracowywania i realizacji polityki unijnej w zakresie certyfikacji cyberbezpieczeństwa produktów i usług ICT poprzez przygotowywanie kandydujących europejskich systemów certyfikacji cyberbezpieczeństwa produktów i usług ICT, zapewnienie obsługi sekretariatu unijnej Grupie ds. Certyfikacji Cyberbezpieczeństwa, zapewnianie wytycznych i dobrych praktyk

[44] Przejrzystość środków zapewniania cyberbezpieczeństwa oznacza zapewnienie użytkownikom informacji na temat właściwości z zakresu cyberbezpieczeństwa, które umożliwiają im obiektywne określenie poziomu bezpieczeństwa danego produktu, usługi bądź procesu ICT.

dotyczących wymogów w zakresie cyberbezpieczeństwa produktów i usług ICT, we współpracy z krajowymi organami nadzoru ds. certyfikacji oraz z przemysłem. **Wspieranie poszerzania wiedzy, informowania i podnoszenia poziomu świadomości** – pomoc i doradztwo dla Komisji i państw członkowskich w celu osiągnięcia wysokiego poziomu wiedzy w całej Unii na temat kwestii związanych z bezpieczeństwem sieci i informacji oraz ich zastosowaniem do zainteresowanych stron z branży. Obejmuje to również gromadzenie, organizowanie i podawanie do wiadomości publicznej, za pośrednictwem specjalnego portalu, informacji na temat bezpieczeństwa sieci i systemów informatycznych [lub cyberbezpieczeństwa]. Innym ważnym elementem są działania na rzecz podnoszenia poziomu świadomości i kampanie informacyjne dotyczące zagrożeń dla cyberbezpieczeństwa, skierowane do ogółu społeczeństwa.

Zwiększone wsparcie w zakresie badań naukowych i innowacji – doradztwo w zakresie potrzeb badawczych i określanie priorytetów w dziedzinie cyberbezpieczeństwa.

Wspieranie współpracy międzynarodowej – wspieranie starań Unii na rzecz współpracy z państwami trzecimi i organizacjami międzynarodowymi w celu propagowania współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa.

CERTYFIKACJA

Ramy certyfikacji przyczynią się do osiągnięcia celów poprzez zwiększenie ogólnej przejrzystości procesu zapewniania cyberbezpieczeństwa[45] produktów i usług ICT i wzmocnienie w ten sposób zaufania do jednolitego rynku cyfrowego i innowacji cyfrowych. Powinny one również pomóc uniknąć rozdrobnienia systemów certyfikacji w UE oraz powiązanych wymogów w zakresie bezpieczeństwa i kryteriów oceny we wszystkich państwach członkowskich i sektorach.

1.4.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Wzmocniona ENISA (zdolności wspierania, zapobieganie, współpraca i świadomość na poziomie UE, tym samym predestynowana do zwiększenia ogólnej cyberodporności UE), jak również wspieranie unijnych ram certyfikacji produktów i usług ICT, powinny zgodnie z oczekiwaniami przynieść następujące skutki (niewyczerpujący wykaz):

Ogólny wpływ:

– Ogólny pozytywny wpływ na rynek wewnętrzny dzięki ograniczeniu fragmentacji rynku i budowaniu zaufania do technologii cyfrowych poprzez lepszą współpracę, bardziej zharmonizowane podejście do polityki UE w dziedzinie cyberbezpieczeństwa oraz zwiększone zdolności na poziomie UE. Powinno to przynieść pozytywne skutki gospodarcze, pomagając ograniczyć koszty cyberincydentów i cyberprzestępstw, których skutki gospodarcze w Unii szacuje się na 0,41 % unijnego PKB (tj. ok. 55 mld EUR).

Wyniki szczegółowe:

Lepsza zdolność i gotowość państw członkowskich i przedsiębiorstw w zakresie cyberbezpieczeństwa

[45] Przejrzystość środków zapewniania cyberbezpieczeństwa oznacza zapewnienie użytkownikom informacji na temat właściwości z zakresu cyberbezpieczeństwa, które umożliwiają im obiektywne określenie poziomu bezpieczeństwa danego produktu, usługi bądź procesu ICT.

– Lepsza zdolność i gotowość państw członkowskich w zakresie cyberbezpieczeństwa (dzięki długoterminowej analizie strategicznej zagrożeń dla cyberbezpieczeństwa i cyberincydentów, wytycznym i sprawozdaniom, wymianie wiedzy fachowej i dobrych praktyk, dostępności szkoleń i materiałów szkoleniowych, zintensyfikowanym ćwiczeniom Cyber Europe).

– Lepsze zdolności podmiotów prywatnych dzięki wsparciu tworzenia ośrodków wymiany i analizy informacji w różnych sektorach.

– Lepsza gotowość państw członkowskich i UE w zakresie cyberbezpieczeństwa dzięki dostępności dobrze przećwiczonych i uzgodnionych planów na wypadek transgranicznego cyberincydentu na dużą skalę wypróbowanych w ramach ćwiczeń Cyber Europe.

Poprawa współpracy i koordynacji między państwami członkowskimi oraz instytucjami, agencjami i organami UE

– Poprawa współpracy zarówno w obrębie sektora publicznego i prywatnego, jak i między tymi sektorami.

– Bardziej spójne podejście do wdrażania dyrektywy w sprawie cyberbezpieczeństwa w różnych państwach i sektorach.

– Poprawa współpracy w dziedzinie certyfikacji dzięki ramom instytucjonalnym umożliwiającym rozwój europejskich systemów certyfikacji cyberbezpieczeństwa oraz opracowanie wspólnej polityki w tej dziedzinie.

Większe możliwości uzupełniania działań państw członkowskich na poziomie UE

– Lepsza „zdolność operacyjna UE" do uzupełniania i wspierania działań państw członkowskich, na ich wniosek i w odniesieniu do ograniczonej liczby wcześniej ustalonych usług. Oczekuje się, że będzie to miało pozytywny wpływ na skuteczne zapobieganie incydentom, ich wykrywanie i reagowanie na nie zarówno na szczeblu państw członkowskich, jak i Unii.

Wyższy poziom świadomości obywateli i przedsiębiorstw w kwestiach cyberbezpieczeństwa

– Szersza ogólna wiedza obywateli i przedsiębiorstw na temat cyberbezpieczeństwa.

– Lepsze możliwości podejmowania świadomych decyzji o zakupach w odniesieniu do produktów i usług ICT dzięki certyfikacji cyberbezpieczeństwa.

Wzmocnienie zaufania do jednolitego rynku cyfrowego i innowacji cyfrowych dzięki zwiększeniu przejrzystości procesu zapewniania cyberbezpieczeństwa produktów i usług ICT

– Większa przejrzystość procesu zapewniania cyberbezpieczeństwa[46] produktów i usług ICT dzięki uproszczeniu procedur certyfikacji bezpieczeństwa za pomocą ram ogólnounijnych.

– Wyższy poziom pewności cech bezpieczeństwa produktów i usług ICT.

– Szersze upowszechnienie certyfikacji bezpieczeństwa dzięki uproszczonym procedurom, ograniczonym kosztom i perspektywom ogólnounijnych możliwości rynkowych, nieutrudnianym przez fragmentację rynku.

[46] Przejrzystość środków zapewniania cyberbezpieczeństwa oznacza zapewnienie użytkownikom informacji na temat właściwości z zakresu cyberbezpieczeństwa, które umożliwiają im obiektywne określenie poziomu bezpieczeństwa danego produktu, usługi bądź procesu ICT.

– Większa konkurencyjność na unijnym rynku cyberbezpieczeństwa ze względu na ograniczenie kosztów i obciążeń administracyjnych dla MŚP oraz wyeliminowanie potencjalnych barier utrudniających wejście na rynek, wynikających z istnienia licznych krajowych systemów certyfikacji.

Inne

– Nie przewiduje się istotnego wpływu na środowisko w związku z realizacją któregokolwiek celu.

– Jeżeli chodzi o budżet UE, można spodziewać się przyrostu wydajności dzięki ściślejszej współpracy i koordynacji działań między instytucjami, agencjami i organami UE.

1.4.4. Wskaźniki wyników i wpływu

Należy określić wskaźniki, które umożliwią monitorowanie realizacji wniosku/inicjatywy.

a)

Cel: Zwiększenie zdolności i gotowości państw członkowskich i przedsiębiorstw:

- Liczba szkoleń zorganizowanych przez ENISA
- Zasięg geograficzny (liczba państw i obszarów) bezpośredniej pomocy świadczonej przez ENISA
- Osiągnięty przez państwa członkowskie poziom gotowości pod względem zaawansowania zespołów CSIRT i nadzoru nad środkami regulacyjnymi związanymi z cyberbezpieczeństwem
- Liczba zapewnionych przez ENISA ogólnounijnych dobrych praktyk dotyczących infrastruktur krytycznych
- Liczba zapewnionych przez ENISA ogólnounijnych dobrych praktyk dotyczących MŚP
- Publikacja przez ENISA corocznych analiz strategicznych na temat zagrożeń dla cyberbezpieczeństwa i cyberincydentów w celu określenia pojawiających się tendencji
- Regularny wkład ENISA w prace grup roboczych ds. cyberbezpieczeństwa działających przy europejskich organizacjach normalizacyjnych

Cel: Poprawa współpracy i koordynacji między państwami członkowskimi oraz instytucjami, agencjami i organami UE:

- Liczba państw członkowskich, które zastosowały zalecenia i opinie Agencji w procesie kształtowania swojej polityki
- Liczba instytucji, agencji i organów UE, które zastosowały zalecenia i opinie Agencji w procesie kształtowania swojej polityki
- Regularna realizacja programu prac sieci CSIRT oraz dobre funkcjonowanie infrastruktury informatycznej i kanałów komunikacyjnych sieci CSIRT
- Liczba raportów technicznych udostępnionych grupie współpracy i wykorzystanych przez nią
- Spójne podejście do wdrażania dyrektywy w sprawie cyberbezpieczeństwa w różnych państwach i sektorach

- Liczba przeprowadzonych przez ENISA ocen zgodności regulacyjnej
- Liczba ośrodków wymiany i analizy informacji utworzonych w różnych sektorach, w szczególności w odniesieniu do infrastruktur krytycznych
- Utworzenie platformy informacyjnej, rozpowszechniającej informacje na temat cyberbezpieczeństwa pochodzące od instytucji, agencji i organów UE oraz regularne nią zarządzanie
- Regularny wkład w przygotowanie unijnych programów prac w zakresie badań naukowych i innowacji
- Zawarcie umowy o współpracy między ENISA, EC3 i CERT-UE
- Liczba systemów certyfikacji uwzględnionych i opracowanych za pomocą ram

Cel: Zwiększenie zdolności do uzupełniania działań państw członkowskich na poziomie UE, zwłaszcza w przypadku transgranicznych cyberkryzysów:

- Publikacja przez ENISA corocznych analiz strategicznych na temat zagrożeń dla cyberbezpieczeństwa i cyberincydentów w celu określenia pojawiających się tendencji
- Publikacja przez ENISA zagregowanych informacji na temat incydentów zgłoszonych zgodnie z dyrektywą w sprawie cyberbezpieczeństwa
- Liczba ogólnoeuropejskich ćwiczeń koordynowanych przez Agencję oraz liczba uczestniczących państw członkowskich i organizacji
- Liczba kierowanych przez państwa członkowskie do ENISA i podjętych przez Agencję wniosków o wsparcie reagowania na incydenty/kryzysy
- Liczba przeprowadzonych przez ENISA we współpracy z CERT-UE analiz dotyczących luk w zabezpieczeniach, artefaktów i incydentów
- Dostępność ogólnounijnych raportów sytuacyjnych opartych na informacjach udostępnianych agencji ENISA przez państwa członkowskie i inne podmioty w przypadku transgranicznego cyberincydentu na dużą skalę

Cel: Wyższy poziom świadomości obywateli i przedsiębiorstw w kwestiach cyberbezpieczeństwa:

- Regularne organizowanie ogólnounijnych i krajowych kampanii podnoszenia poziomu świadomości i regularna aktualizacja tematów zgodnie z powstającymi potrzebami edukacyjnymi
- Podnoszenie poziomu cyberświadomości obywateli UE
- Regularne przeprowadzanie quizu badającego poziom świadomości w kwestiach cyberbezpieczeństwa i zwiększający się na przestrzeni czasu odsetek prawidłowych odpowiedzi
- Regularna publikacja dobrych praktyk w zakresie cyberbezpieczeństwa

i higieny cyberbezpieczeństwa ukierunkowana na pracowników i organizacje

Cel: Wzmocnienie zaufania do jednolitego rynku cyfrowego i innowacji cyfrowych dzięki zwiększeniu ogólnej przejrzystości procesu zapewniania cyberbezpieczeństwa[47] produktów i usług ICT.

- Liczba systemów zgodnych z ramami unijnymi
- Obniżony koszt uzyskania certyfikatu dotyczącego bezpieczeństwa ICT
- Liczba jednostek oceniających zgodność specjalizujących się w certyfikacji ICT, w poszczególnych państwach członkowskich
- Utworzenie Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa i regularna organizacja jej posiedzeń
- Wytyczne dotyczące certyfikacji zgodnie z obowiązującymi ramami unijnymi
- Regularna publikacja analiz głównych tendencji na unijnym rynku cyberbezpieczeństwa
- Liczba produktów i usług ICT certyfikowanych zgodnie z zasadami europejskich ram certyfikacji bezpieczeństwa ICT
- Większa liczba użytkowników końcowych orientujących się w cechach bezpieczeństwa produktów i usług ICT

b)

1.4.5. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej

W obliczu wymogów regulacyjnych i szybko ewoluującego profilu zagrożeń w zakresie cyberbezpieczeństwa należy dokonać przeglądu mandatu ENISA, aby określić uaktualniony zestaw zadań i funkcji z myślą o skutecznym i wydajnym wspieraniu starań państw członkowskich, instytucji unijnych i innych zainteresowanych stron, podejmowanych w celu zapewnienia bezpiecznej cyberprzestrzeni w Unii Europejskiej. Wyznaczono sugerowany zakres mandatu, wzmacniając te obszary, w których agencja niewątpliwie zapewniała wartość dodaną, i dodając nowe obszary, w których potrzebne jest wsparcie ze względu na nowe priorytety i instrumenty polityczne, w szczególności dyrektywę w sprawie cyberbezpieczeństwa, przegląd strategii bezpieczeństwa cybernetycznego UE, plan działania UE w zakresie bezpieczeństwa cybernetycznego dotyczący współpracy na wypadek kryzysu cybernetycznego i certyfikacji bezpieczeństwa ICT. Nowy zaproponowany mandat jest próbą zapewnienia Agencji silniejszej i bardziej centralnej roli, w szczególności poprzez także aktywniejsze wspieranie państw członkowskich w przeciwdziałaniu zagrożeniom (zdolności operacyjne), a także poprzez przekształcenie jej w ośrodek wiedzy fachowej, wspomagający państwa członkowskie i Komisję w zakresie certyfikacji cyberbezpieczeństwa.

We wniosku ustanawia się jednocześnie europejskie ramy certyfikacji cyberbezpieczeństwa produktów i usług ICT oraz określa zasadnicze funkcje i zadania agencji ENISA w dziedzinie certyfikacji cyberbezpieczeństwa. W ramach tych określono wspólne przepisy i procedury umożliwiające tworzenie ogólnounijnych systemów certyfikacji cyberbezpieczeństwa w odniesieniu do określonych produktów i usług ICT lub zagrożeń dla cyberbezpieczeństwa. Stworzenie europejskich systemów certyfikacji cyberbezpieczeństwa zgodnie z ramami sprawi, że certyfikaty wydane w ramach tych

[47] Przejrzystość środków zapewniania cyberbezpieczeństwa oznacza zapewnienie użytkownikom informacji na temat właściwości z zakresu cyberbezpieczeństwa, które umożliwiają im obiektywne określenie poziomu bezpieczeństwa danego produktu, usługi bądź procesu ICT.

systemów będą ważne i uznawane we wszystkich państwach członkowskich, oraz umożliwi uporządkowanie obecnej fragmentacji rynku.

1.4.6. Wartość dodana z tytułu zaangażowania Unii

Cyberbezpieczeństwo to problem o prawdziwie globalnym charakterze, z natury transgraniczny i coraz bardziej międzysektorowy ze względu na wzajemne zależności między sieciami i systemami informatycznymi. Liczba, złożoność i skala cyberincydentów oraz ich wpływ na gospodarkę i społeczeństwo rosną z upływem czasu i można się spodziewać dalszego wzrostu w tym zakresie wraz z rozwojem technologii, na przykład rozprzestrzenianiem się internetu rzeczy. To sprawia, że nie można się spodziewać, iż potrzeba intensywniejszych wspólnych starań państw członkowskich, instytucji UE i prywatnych zainteresowanych stron, aby stawić czoło zagrożeniom dla cyberbezpieczeństwa, stanie się w przyszłości mniej paląca.

Od czasu jej utworzenia w roku 2004 ENISA starała się wspierać współpracę między państwami członkowskimi a stronami zainteresowanymi bezpieczeństwem sieci i informacji, również poprzez wsparcie współpracy publiczno-prywatnej. To wspieranie współpracy obejmowało prace techniczne w celu określenia ogólnounijnego obrazu profilu zagrożeń, utworzenie grup eksperckich oraz organizację ogólnoeuropejskich ćwiczeń w zarządzaniu cyberincydentami i cyberkryzysami dla sektora publicznego i prywatnego (zwłaszcza „Cyber Europe"). Dyrektywą w sprawie cyberbezpieczeństwa powierzono agencji ENISA dodatkowe zadania, w tym pełnienie roli sekretariatu sieci CSIRT na potrzeby współpracy operacyjnej między państwami członkowskimi.

Wartość dodana wynikająca z działania na szczeblu UE, w szczególności na rzecz zacieśnienia współpracy między państwami członkowskimi, lecz również między środowiskami działającymi na rzecz bezpieczeństwa sieci i informacji, znalazła uznanie w konkluzjach Rady z roku 2016[48], co również jasno wynika z dokonanej w 2017 roku oceny ENISA, która pokazuje, że wartość dodana generowana przez Agencję polega przede wszystkim na jej umiejętności umacniania współpracy między wspomnianymi zainteresowanymi stronami. Na poziomie UE nie ma innego podmiotu, który wspomagałby współpracę w obrębie tak szerokiego zakresu podmiotów związanych z bezpieczeństwem sieci i informacji.

Wartość dodana generowana przez ENISA dzięki łączeniu środowisk i zainteresowanych stron aktywnych w obszarze cyberbezpieczeństwa ma również znaczenie w dziedzinie certyfikacji. Wzrost cyberprzestępczości i zagrożeń dla bezpieczeństwa spowodował uruchomienie inicjatyw krajowych, ustanawiających rygorystyczne wymogi w zakresie cyberbezpieczeństwa i certyfikacji komponentów ICT stosowanych w tradycyjnej infrastrukturze. Choć inicjatywy te są ważne, stwarzają ryzyko fragmentacji jednolitego rynku i pojawienia się barier dla interoperacyjności. Sprzedawca z sektora ICT może być zmuszony do przejścia kilku procedur certyfikacji, aby móc prowadzić sprzedaż w kilku państwach członkowskich. Bez interwencji ze strony UE rozwiązanie problemu nieskuteczności/niewydajności obecnych systemów certyfikacji jest mało prawdopodobne. Przy braku działania bardzo prawdopodobne jest pogłębienie się fragmentacji rynku w perspektywie krótko- i średnioterminowej (w ciągu następnych 5–10 lat) w związku z powstaniem nowych systemów certyfikacji. Brak koordynacji i interoperacyjności takich systemów stanowi element, który osłabia potencjał jednolitego

[48] Konkluzje Rady w sprawie wzmacniania europejskiego systemu odporności cybernetycznej oraz wspierania konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego, 15 listopada 2016 r.

rynku cyfrowego. Dowodzi to istnienia wartości dodanej, jaką może przynieść ustanowienie europejskich ram certyfikacji cyberbezpieczeństwa produktów i usług ICT, które to ramy stworzą odpowiednie warunki do skutecznego rozwiązania problemów związanych ze współistnieniem rozlicznych procedur certyfikacji w poszczególnych państwach członkowskich, obniżenia kosztów certyfikacji i podniesienia w ten sposób ogólnej atrakcyjności certyfikacji w UE z perspektywy handlowej i konkurencyjnej.

1.4.7. Główne wnioski wyciągnięte z podobnych działań

Zgodnie z podstawą prawną funkcjonowania agencji ENISA Komisja przeprowadziła ocenę Agencji, która objęła przeprowadzenie niezależnego badania oraz konsultacje publiczne. Z oceny wynika, że cele ENISA nie straciły na znaczeniu. W warunkach rozwoju technologicznego i zmieniających się zagrożeń oraz w obliczu wyraźnej potrzeby większego bezpieczeństwa sieci i informacji w UE potrzebna jest fachowa wiedza techniczna dotycząca ewolucji kwestii bezpieczeństwa sieci i informacji. W państwach członkowskich należy budować potencjał do rozumienia zagrożeń i reagowania na nie, a zainteresowane strony muszą współpracować przekrojowo w obszarach tematycznych i międzyinstytucjonalnie.

Agencja z powodzeniem przyczyniła się do zwiększenia bezpieczeństwa sieci i informacji w Europie, oferując budowanie potencjału w 28 państwach członkowskich, zacieśnienie współpracy między państwami członkowskimi a stronami zainteresowanymi bezpieczeństwem sieci i informacji, zapewnianie wiedzy specjalistycznej, tworzenie wspólnoty i wspieranie kształtowania polityki.

ENISA zdołała zaznaczyć swój wpływ, przynajmniej w pewnym stopniu, w rozległym obszarze bezpieczeństwa sieci i informacji, jednak nie osiągnęła pełnego sukcesu w budowaniu silnej marki oraz nie uzyskała pozycji wystarczającej do uznania jej za główny ośrodek wiedzy specjalistycznej w Europie. Wyjaśnienie tego kryje się w szerokim zakresie mandatu ENISA, z którym nie korespondowały odpowiednio duże środki. Ponadto ENISA pozostaje jedyną agencją UE z mandatem na czas określony, co ogranicza jej zdolność do opracowania długofalowej wizji i stabilnego wspierania zainteresowanych stron. Stoi to również w sprzeczności z przepisami dyrektywy w sprawie cyberbezpieczeństwa, w której powierzono ENISA zadania bez daty końcowej.

Jeżeli chodzi o certyfikację cyberbezpieczeństwa produktów i usług ICT, obecnie nie istnieją jej europejskie ramy. Wzrost cyberprzestępczości i zagrożeń dla bezpieczeństwa spowodował jednak zainicjowanie inicjatyw krajowych, co grozi fragmentacją jednolitego rynku.

1.4.8. Spójność z innymi właściwymi instrumentami oraz możliwa synergia

Inicjatywa jest w wysokim stopniu spójna z obecnymi strategiami politycznymi, w szczególności w dziedzinie rynku wewnętrznego. Jest ona w istocie pomyślana zgodnie z ogólnym podejściem do cyberbezpieczeństwa, określonym w przeglądzie strategii jednolitego rynku cyfrowego, tak aby uzupełniać kompleksowy zbiór działań, do których należą przegląd strategii bezpieczeństwa cybernetycznego UE, plan działania dotyczący współpracy na wypadek kryzysu cybernetycznego oraz inicjatywy w zakresie zwalczania cyberprzestępczości. Zapewni dostosowanie do obowiązujących przepisów w dziedzinie cyberbezpieczeństwa, w szczególności dyrektywy w sprawie cyberbezpieczeństwa, i oprze się na nich, aby wzmocnić cyberodporność UE za pomocą zwiększenia zdolności, ściślejszej współpracy, lepszego zarządzania ryzykiem i podnoszenia poziomu świadomości w kwestiach cyberbezpieczeństwa.

Proponowane środki w zakresie certyfikacji powinny zaradzić potencjalnej fragmentacji powodowanej przez istniejące i powstające krajowe systemy certyfikacji, przyczyniając się w ten sposób do rozwoju jednolitego rynku cyfrowego. Inicjatywa wspiera również i uzupełnia wdrożenie dyrektywy w sprawie cyberbezpieczeństwa poprzez zapewnienie przedsiębiorstwom podlegającym dyrektywie narzędzia do wykazywania zgodności z jej wymogami w całej Unii.

Proponowane europejskie ramy certyfikacji cyberbezpieczeństwa w sektorze ICT nie naruszają przepisów ogólnego rozporządzenia o ochronie danych[49], a w szczególności odpowiednich jego przepisów dotyczących certyfikacji[50], ponieważ przepisy te mają zastosowanie do bezpieczeństwa przetwarzania danych osobowych. Co niemniej ważne, należy podkreślić, że systemy proponowane jako element przyszłych europejskich ram powinny w możliwie największym stopniu bazować na normach międzynarodowych, aby unikać tworzenia barier handlowych i zapewnić spójność z inicjatywami międzynarodowymi.

[49] Rozporządzenie (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[50] Takich jak art. 42 (Certyfikacja) i art. 43 (Podmiot certyfikujący), jak również art. 57, 58 i 70 dotyczące odpowiednio stosownych zadań i uprawnień niezależnych organów nadzorczych oraz zadań Europejskiej Rady Ochrony Danych,

1.5. Okres trwania działania i jego wpływ finansowy

☐ Wniosek/inicjatywa o **ograniczonym okresie trwania**

– ☐ Okres trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

– ☐ Okres trwania wpływu finansowego: od RRRR r. do RRRR r.

☒ Wniosek/inicjatywa o **nieograniczonym okresie trwania**

– Wprowadzenie w życie z okresem rozruchu od 2019 r. do 2020 r.,

– po którym następuje faza operacyjna.

1.6. Planowane tryby zarządzania[51]

☒ **Bezpośrednie zarządzanie** przez Komisję (Tytuł III – Certyfikacja)

– ☐ agencje wykonawcze

☐ **Zarządzanie dzielone** z państwami członkowskimi

☒ **Zarządzanie pośrednie** poprzez przekazanie zadań związanych z wykonaniem budżetu:

☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

☐ EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

☒ organom, o których mowa w art. 208 i 209 rozporządzenia finansowego (Tytuł II – ENISA);

☐ organom prawa publicznego;

☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile zapewniają one odpowiednie gwarancje finansowe;

☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego oraz które zapewniają odpowiednie gwarancje finansowe;

☐ osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym.

Uwagi

Rozporządzenie obejmuje: – w tytule II proponowanego rozporządzenia zmianę mandatu Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) poprzez nadanie jej ważnej roli w procesie certyfikacji, natomiast – w tytule III ustanowienie ram umożliwiających tworzenie europejskich systemów certyfikacji cyberbezpieczeństwa produktów i usług ICT, w czym ENISA odgrywa kluczową rolę.

[51] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Należy określić częstotliwość i warunki.

Monitorowanie rozpocznie się zaraz po przyjęciu aktu prawnego i skupi się na jego stosowaniu. Komisja będzie organizować posiedzenia z udziałem ENISA, przedstawicieli państw członkowskich (np. grup ekspertów) i odpowiednich zainteresowanych stron, aby w szczególności ułatwić wykonanie przepisów dotyczących certyfikacji, takich jak ustanowienie zarządu.

Pierwsza ocena powinna odbyć się po upływie 5 lat od daty wejścia w życie instrumentu prawnego, pod warunkiem że dostępne są wystarczające dane. Instrument prawny zawiera wyraźną klauzulę oceny i przeglądu [art. XXX], na podstawie której Komisja będzie przeprowadzać niezależną ocenę. Następnie Komisja będzie przedstawiać Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny, któremu w stosownych przypadkach towarzyszyć będzie wniosek o dokonanie przeglądu w celu zmierzenia wpływu wywieranego przez rozporządzenie i generowanej przez nie wartości dodanej. Kolejne oceny będą się odbywać co pięć lat. Komisja stosować będzie metodykę oceny służącą lepszemu stanowieniu prawa. Oceny te będą przeprowadzane ze wsparciem w postaci ukierunkowanych fachowych dyskusji, badań i szerokich konsultacji z zainteresowanymi stronami.

Dyrektor wykonawczy ENISA co dwa lata powinien przedstawiać zarządowi ocenę *ex post* działalności ENISA. Agencja powinna również sporządzać plan działań następczych w odniesieniu do wniosków z retrospektywnych ocen i co dwa lata składać Komisji sprawozdanie z postępów. Zarząd powinien odpowiadać za dopilnowanie wdrożenia odpowiednich działań następczych w związku ze wspomnianymi wnioskami.

Domniemane przypadki niewłaściwego administrowania w ramach działań Agencji mogą podlegać dochodzeniom prowadzonym przez Europejskiego Rzecznika Praw Obywatelskich zgodnie z postanowieniami art. 228 Traktatu.

Źródłami danych na potrzeby planowanego monitorowania byłyby przede wszystkim ENISA, europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, grupa współpracy, sieć CSIRT i organy państw członkowskich. Oprócz danych pochodzących ze sprawozdań (w tym corocznych sprawozdań z działalności) składanych przez ENISA, europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa, grupę współpracy i sieć CSIRT wykorzystywane będą w razie potrzeby określone narzędzia gromadzenia danych (na przykład ankiety kierowane do organów krajowych, Eurobarometr oraz sprawozdania z kampanii „miesiąc cyberbezpieczeństwa” i z ćwiczeń ogólnoeuropejskich).

2.2. System zarządzania i kontroli

2.2.1. Zidentyfikowane ryzyko

Zidentyfikowane ryzyko jest ograniczone: agencja unijna już istnieje, a jej mandat zostanie wyznaczony poprzez wzmocnienie tych obszarów, w których Agencja wniosła wyraźną wartość dodaną, i dodanie nowych obszarów, wymagających wsparcia z uwagi na nowe priorytety i instrumenty polityczne, w szczególności takie jak: dyrektywa w sprawie

cyberbezpieczeństwa, przegląd strategii bezpieczeństwa cybernetycznego UE, przygotowywany unijny plan działania w zakresie bezpieczeństwa cybernetycznego dotyczący współpracy na wypadek kryzysu cybernetycznego i certyfikacji bezpieczeństwa ICT.

Wniosek precyzuje zatem funkcje Agencji i prowadzi do przyrostu wydajności. Zwiększenie kompetencji i zadań operacyjnych nie stanowi realnego zagrożenia, ponieważ będą one uzupełniać działania państw członkowskich i wspierać je, na wniosek i w odniesieniu do ograniczonej liczby wcześniej ustalonych usług.

Ponadto proponowany model agencji, zgodny ze wspólnym podejściem, gwarantuje istnienie wystarczającej kontroli zapewniającej działanie ENISA na rzecz osiągnięcia jej celów. Ryzyko operacyjne i finansowe związane z proponowanymi zmianami wydaje się ograniczone.

Jednocześnie konieczne jest zapewnienie odpowiednich środków finansowych, aby ENISA mogła wypełniać zadania powierzone jej w ramach nowego mandatu, w tym w dziedzinie certyfikacji.

2.2.2. Przewidywane metody kontroli

Sprawozdanie finansowe Agencji będzie przedkładane Trybunałowi Obrachunkowemu do zatwierdzenia i będzie objęte procedurą udzielania absolutorium; przewidywane są również kontrole.

Działania Agencji podlegają również nadzorowi Rzecznika Praw Obywatelskich zgodnie z postanowieniami art. 228 Traktatu.

Zob. również pkt 2.1 oraz pkt 2.2.1 powyżej.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony

ENISA stosowałaby środki zapobiegania i ochrony, a mianowicie:

– Przed dokonaniem płatności pracownicy Agencji dokonują weryfikacji płatności za usługi lub badania będące przedmiotem wniosku, z uwzględnieniem zobowiązań umownych, zasad gospodarczych oraz dobrej praktyki finansowej lub zarządczej. Postanowienia dotyczące zwalczania nadużyć finansowych (odnoszące się do nadzoru, wymogów sprawozdawczych itp.) będą umieszczane we wszystkich umowach zawieranych przez Agencję z beneficjentami płatności i składanych przez nią u nich zamówieniach.

W celu zwalczania nadużyć finansowych, korupcji i innych działań bezprawnych stosuje się bez ograniczeń przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczącego dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF).

– W ciągu sześciu miesięcy od daty wejście w życie niniejszego rozporządzenia Agencja przystępuje do Porozumienia międzyinstytucjonalnego z dnia 25 maja 1999 r. między Parlamentem Europejskim, Radą Unii Europejskiej i Komisją Wspólnot Europejskich dotyczącego postępowań wewnętrznych prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz wprowadza niezwłocznie właściwe przepisy mające zastosowanie do wszystkich pracowników Agencji.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

- Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
		Zróżnicowane/ niezróżnicowane[52]	państw EFTA[53]	krajów kandydujących[54]	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
1a Konkurencyjność na rzecz wzrostu gospodarczego i zatrudnienia	09.0203 ENISA oraz certyfikacja bezpieczeństwa technologii informacyjno-komunikacyjnych	Zróżnicowane	TAK	NIE	NIE	NIE
5 Wydatki administracyjne	09.0101 Wydatki związane z personelem czynnie zatrudnionym w obszarze polityki: sieci komunikacyjne, treści i technologie 09.0102 Wydatki związane z personelem	Niezróżnicowane	NIE	NIE	NIE	NIE

[52] Środki zróżnicowane/ środki niezróżnicowane.

[53] EFTA: Europejskie Stowarzyszenie Wolnego Handlu.

[54] Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

	zewnętrznym czynnie zatrudnionym w obszarze polityki: sieci komunikacyjne, treści i technologie 09.010211 Inne wydatki na zarządzanie					

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	1a	Konkurencyjność na rzecz wzrostu gospodarczego i zatrudnienia

ENISA			**Poziom referencyjny** **2017 (31.12.2016)**		**2019** ***(od 01.07.2019)***	**2020**	**2021**	**2022**	**OGÓŁEM**
Tytuł 1: Wydatki na personel *(w tym również wydatki związane z rekrutacją personelu, szkoleniami, infrastrukturą socjalno-medyczną i usługami zewnętrznymi)*	Środki na zobowiązania	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Środki na płatności	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Tytuł 2: Wydatki na infrastrukturę i wydatki administracyjne	Środki na zobowiązania	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Środki na płatności	(2 a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Tytuł 3: Wydatki operacyjne	Środki na zobowiązania	(3 a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Środki na płatności	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**

OGÓŁEM środki dla ENISA	Środki na zobowiązania	=1+1 a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Środki na płatności	=2+2 a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Dział wieloletnich ram finansowych	**5**	„Wydatki administracyjne”

w mln EUR (do trzech miejsc po przecinku)

		2019 *(od 1.07.2019)*	**2020**	**2021**	**2022**	**OGÓŁEM**
DG: CNECT						
• Zasoby ludzkie		0,216	0,846	0,846	0,846	**2,754**
• Pozostałe wydatki administracyjne		0,102	0,235	0,238	0,242	**0,817**
OGÓŁEM DG CNECT	Środki	0,318	1,081	1,084	1,088	**3,571**

Koszty personelu obliczono stosownie do planowanej daty zatrudnienia (przewiduje się rozpoczęcie zatrudnienia począwszy od 1.07.2019).

Perspektywa dotycząca zasobów po roku 2020 jest orientacyjna i bez uszczerbku dla wniosków Komisji dotyczących wieloletnich ram finansowych po 2020 roku.

OGÓŁEM środki na DZIAŁ 5 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	0,318	1,081	1,084	1,088	**3,571**

w mln EUR (do trzech miejsc po przecinku)

		2019	2020	2021	2022	OGÓŁEM
OGÓŁEM środki na DZIAŁY 1 do 5 wieloletnich ram finansowych	Środki na zobowiązania	16,868	21,727	23,332	24,11	**86,038**
	Środki na płatności	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Szacunkowy wpływ na środki agencji

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty[55] ⇩	**2019**	**2020**	**2021**	**2022**	**OGÓŁEM**
Zwiększenie zdolności i gotowości państw członkowskich i przedsiębiorstw	1,408	1,900	1,931	1,969	7,208
Poprawa współpracy i koordynacji między państwami członkowskimi oraz instytucjami, agencjami i organami UE	0,939	1,266	1,288	1,313	4,806
Zwiększenie możliwości uzupełniania działań państw członkowskich na poziomie UE, w szczególności w przypadku transgranicznych cyberkryzysów	0,704	0,950	0,965	0,985	3,604
Podniesienie poziomu świadomości obywateli i przedsiębiorstw w kwestiach cyberbezpieczeństwa	0,704	0,950	0,965	0,985	3,604
Wzmocnienie zaufania do jednolitego rynku cyfrowego i innowacji cyfrowych dzięki zwiększeniu ogólnej przejrzystości procesu zapewniania cyberbezpieczeństwa produktów i usług ICT	0,939	1,266	1,288	1,313	4,806
KOSZT OGÓŁEM	4 694	6,332	6,437	6,565	24,028

[55] W tej tabeli przedstawiono jedynie wydatki operacyjne dotyczące tytułu 3.

3.2.3. Szacunkowy wpływ na zasoby ludzkie Agencji

3.2.3.1. Streszczenie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	3. i 4. kw. 2019	**2020**	**2021**	**2022**
Urzędnicy zatrudnieni na czas określony (grupa zaszeregowania AD)	4,242	5,695	6,381	6,709
Urzędnicy zatrudnieni na czas określony (grupa zaszeregowania AST)	1,601	1,998	2,217	2,217
Pracownicy kontraktowi	2,041	2,041	2,041	2,041
Oddelegowani eksperci krajowi	0,306	0,447	0,656	0,796
OGÓŁEM	**8,190**	**10,181**	**11,295**	**11,763**

Koszty personelu obliczono stosownie do planowanej daty zatrudnienia (dla obecnego personelu ENISA przyjęto pełne zatrudnienie począwszy od 1.01.2019). Dla nowego personelu przewidziano stopniowe zatrudnianie począwszy od 1.07.2019 i osiągnięcie pełnego zatrudnienia w roku 2022. Perspektywa dotycząca zasobów po roku 2020 jest orientacyjna i bez uszczerbku dla wniosków Komisji dotyczących wieloletnich ram finansowych po 2020 roku.

Szacunkowy wpływ na personel (dodatkowe EPC) – plan zatrudnienia

Grupa funkcyjna i grupa zaszeregowania	2017 **ENISA obecnie**	3. i 4. kw. 2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2

AD6 AD5			3	3	
Ogółem AD	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Ogółem AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Ogółem AST/SC					
SUMA CAŁKOWITA	48	12	10	7	3

Zadania dodatkowego personelu AD/AST wykonywane w celu osiągnięcia celów instrumentu zgodnie z opisem w pkt 1.4.2:

Zadania	AD	AST	SNE (oddelegowani eksperci krajowi)	Ogółem
Polityka i budowanie potencjału	8	1		9
Współpraca operacyjna	8	1	7	16
Certyfikacja (zadania związane z rynkiem)	9	3	2	14
Wiedza, informacje i świadomość	1	1		2
OGÓŁEM	26	6	9	41

Opis zadań do wykonania:

Zadania	Wymagane dodatkowe zasoby
Opracowanie i wdrożenie polityki UE oraz budowanie potencjału	Zadania obejmowałyby pomoc grupie współpracy, wspieranie spójnego wdrażania dyrektywy w sprawie cyberbezpieczeństwa w poszczególnych państwach, regularną sprawozdawczość na temat stanu realizacji unijnych ram prawnych, doradztwo i koordynację przy sektorowych inicjatywach dotyczących cyberbezpieczeństwa, w tym w dziedzinie energetyki, transportu (np. lotnictwo / transport drogowy i morski / pojazdy połączone z siecią), opieki zdrowotnej i finansów, zapewnianie wsparcia przy tworzeniu ośrodków wymiany i analizy informacji w różnych sektorach.
Współpraca operacyjna i zarządzanie kryzysowe	**Zadania obejmowałyby:** Zapewnienie obsługi sekretariatu sieci CSIRT poprzez zapewnienie, między innymi, sprawnego funkcjonowania infrastruktury informatycznej sieci CSIRT i kanałów komunikacyjnych. Zapewnienie współpracy strukturalnej z CERT-UE, EC3 i innymi odpowiednimi organami UE. Organizację **ćwiczeń Cyber Europe**[56] – zadania związane ze zwiększeniem częstotliwości ćwiczeń – na coroczne zamiast odbywających się co dwa lata – oraz zapewnieniem, aby ćwiczenia dotyczyły całego incydentu, od początku do końca. **Pomoc techniczną** – zadania obejmowałyby współpracę strukturalną z CERT-UE w celu zapewnienia pomocy technicznej w przypadku istotnych incydentów i wsparcia analizy incydentów. Obejmowałoby to zapewnienie państwom członkowskim pomocy przy postępowaniach w przypadku incydentów i analizie luk w zabezpieczeniach, artefaktów i incydentów. Ułatwianie współpracy między poszczególnymi państwami członkowskimi w razie konieczności reagowania w sytuacjach

[56] Cyber Europe to jak do tej pory największe i najbardziej kompleksowe unijne ćwiczenia w dziedzinie cyberbezpieczeństwa, w których uczestniczy 700 osób zawodowo zajmujących się cyberbezpieczeństwem z 28 państw członkowskich. Odbywają się co dwa lata. W ocenie ENISA oraz w strategii bezpieczeństwa cybernetycznego UE z 2013 r. zwrócono uwagę na fakt, że wiele zainteresowanych stron opowiada się za częstszym, tj. corocznym przeprowadzaniem ćwiczeń Cyber Europe, z uwagi na szybko zmieniający się charakter cyberzagrożeń. Obecnie nie jest to jednak wykonalne ze względu na ograniczone zasoby Agencji.

	kryzysowych poprzez analizę i agregowanie krajowych raportów sytuacyjnych w oparciu o informacje udostępnione Agencji przez państwa członkowskie i inne podmioty. **Plan działania dotyczący skoordynowanej reakcji na transgraniczne cyberincydenty na dużą skalę** – Agencja wniesie wkład w opracowanie wspólnej reakcji, na szczeblu Unii i państw członkowskich, na związane z cyberbezpieczeństwem transgraniczne incydenty na dużą skalę lub kryzysy, poprzez szereg zadań, począwszy od wkładu w ustalenie orientacji sytuacyjnej na szczeblu Unii, aż po testowanie planów współpracy na wypadek incydentów. **Postępowania wyjaśniające *ex post* dotyczące incydentów** – przeprowadzanie postępowań technicznych *ex post* dotyczących incydentów lub wkład w takie postępowania, we współpracy z siecią CSIRT, w celu wydania zaleceń i zwiększenia zdolności, w postaci publicznych sprawozdań, aby lepiej zapobiegać przyszłym incydentom.
Zadania związane z rynkiem (normalizacja, certyfikacja)	Zadania obejmowałyby aktywne wsparcie prac podejmowanych w obrębie ram certyfikacji, w tym zapewnianie wiedzy fachowej na potrzeby przygotowania kandydujących europejskich systemów certyfikacji cyberbezpieczeństwa. Zadania obejmą również wsparcie opracowywania i wdrażania unijnej polityki w zakresie normalizacji, certyfikacji i centrum monitorowania rynku, co będzie wymagać ułatwiania wprowadzania standardów zarządzania ryzykiem w odniesieniu do produktów, sieci i usług elektronicznych oraz doradzania operatorom usług kluczowych i dostawcom usług cyfrowych w sprawie technicznych wymogów w zakresie bezpieczeństwa. Do zadań będzie także należeć dostarczanie analiz głównych tendencji na rynku cyberbezpieczeństwa.
Wiedza i informacje, podnoszenie poziomu świadomości	Z myślą o zapewnieniu łatwiejszego dostępu do bardziej usystematyzowanych informacji na temat zagrożeń dla cyberbezpieczeństwa i potencjalnych środków zaradczych we wniosku powierza się Agencji nowe zadanie polegające na rozwoju i utrzymywaniu unijnego „węzła informacyjnego”. Zadania obejmowałyby gromadzenie, systematyzowanie i podawanie do

	wiadomości publicznej za pośrednictwem specjalnego portalu informacji na temat bezpieczeństwa sieci i systemów informatycznych, a w szczególności cyberbezpieczeństwa, przekazanych przez instytucje, agencji i organy UE. Do zadań należałoby również wspieranie działań ENISA w dziedzinie podnoszenia poziomu świadomości, aby umożliwić Agencji rozszerzenie działalności.

3.2.3.2. Szacowane zapotrzebowanie na zasoby ludzkie macierzystej DG

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy (lub najwyżej z dokładnością do jednego miejsca po przecinku)

		Dodatkowy personel			
	Poziom referencyjny 2017	3. i 4. kw. 2019	2020	2021	2020
• **Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)**					
09 01 01 01 (w centrali i w biurach przedstawicielstw Komisji)	1	2	3		
• **Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC)**[57]					
09 01 02 01 (CA, SNE, INT z globalnej koperty finansowej)	1	2			
OGÓŁEM		**4**	**3**		

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	Reprezentowanie Komisji w zarządzie agencji. Sporządzanie opinii Komisji na temat jednolitego dokumentu programowego ENISA i monitorowanie jego wprowadzenia w życie. Nadzorowanie sporządzania budżetu agencji i monitorowanie jego wykonania. Wspomaganie agencji w prowadzeniu działalności zgodnie z kierunkiem polityki Unii, w tym poprzez udział w odpowiednich posiedzeniach. Nadzorowanie wprowadzenia w życie ram europejskich systemów certyfikacji cyberbezpieczeństwa produktów i usług

[57] CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JED = młodszy oddelegowany ekspert.

	ICT. Utrzymywanie kontaktów z państwami członkowskimi i innymi odpowiednimi zainteresowanymi stronami w związku z działalnością certyfikacyjną. Współpraca z ENISA w odniesieniu do kandydujących systemów. Przygotowywanie kandydujących europejskich systemów certyfikacji cyberbezpieczeństwa.
Personel zewnętrzny	Jak wyżej.

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

– ☐ Wniosek/inicjatywa jest zgodny(-a) z obowiązującymi wieloletnimi ramami finansowymi.

– ☒ Wniosek/inicjatywa wymaga przeprogramowania odpowiedniego działu w wieloletnich ramach finansowych.

Wniosek będzie wymagał przeprogramowania art. 09 02 03 ze względu na zmianę mandatu ENISA powodującą powierzenie agencji nowych zadań związanych – między innymi – z wdrażaniem dyrektywy w sprawie cyberbezpieczeństwa oraz z europejskimi ramami certyfikacji cyberbezpieczeństwa. Odpowiednie kwoty:

Rok	Przewidziane	Wnioskowane
2019	10,739	16,550
2020	10,954	20,646
2021	Nie dotyczy.	22,248*
2022	Nie dotyczy.	23,023*

* Kwota szacunkowa. Finansowanie ze strony UE po roku 2020 zostanie przeanalizowane w ramach debaty prowadzonej wewnątrz Komisji dotyczącej wszystkich wniosków dla okresu po roku 2020. Oznacza to, że po sporządzeniu wniosku dotyczącego kolejnych wieloletnich ram finansowych Komisja przedstawi zmienioną ocenę skutków finansowych regulacji z uwzględnieniem wniosków wynikających z oceny skutków[58].

– ☐ Wniosek/inicjatywa wymaga zastosowania instrumentu elastyczności lub zmiany wieloletnich ram finansowych[59].

3.2.5. Udział osób trzecich w finansowaniu

– ☐ Wniosek/inicjatywa nie przewiduje współfinansowania ze strony osób trzecich

[58] Link do strony, na której znajduje się ocena skutków.

[59] Zob. art. 11 i 17 rozporządzenia Rady (UE, Euratom) nr 1311/2013 określającego wieloletnie ramy finansowe na lata 2014–2020.

– ☒ Wniosek/inicjatywa przewiduje współfinansowanie szacowane zgodnie z poniższym:

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**
EFTA	p.m.[60]	p.m.	p.m.	p.m.

3.3. Szacunkowy wpływ na dochody

– ☒ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

– ☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

  – ☐ wpływ na zasoby własne

  – ☐ wpływ na dochody różne.

[60] Dokładna kwota na następne lata będzie znana, gdy zostanie ustalony współczynnik proporcjonalności dla EFTA na dany rok.