Rada
Unii Europejskiej

Bruksela, 29 maja 2018 r.
(OR. en)

9350/18

Międzyinstytucjonalny numer referencyjny:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

NOTA

Od:	Prezydencja
Do:	Rada
Nr poprz. dok.:	8834/18
Nr dok. Kom.:	12183/17
Dotyczy:	Wniosek dotyczący ROZPORZĄDZENIA 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”) – Podejście ogólne

I. WPROWADZENIE

1. W dniu 13 września 2017 r. w kontekście swojej strategii jednolitego rynku cyfrowego Komisja przyjęła i przekazała Radzie i Parlamentowi Europejskiemu wyżej wymieniony wniosek[1], którego podstawą prawną jest art. 14 TFUE. Jako część tzw. „pakietu w sprawie cyberbezpieczeństwa" niniejszy wniosek ma na celu zapewnienie wysokiego poziomu cyberbezpieczeństwa, cyberodporności i zaufania na terenie Unii z myślą o zapewnieniu właściwego funkcjonowania rynku wewnętrznego.

2. Proponowane rozporządzenie określa cele, zadania i aspekty organizacyjne ENISA – Agencji UE ds. Cyberbezpieczeństwa oraz tworzy ramy ustanawiania europejskich systemów certyfikacji cyberbezpieczeństwa w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa produktów i usług ICT w Unii. Wnioskowi Komisji towarzyszy ocena skutków, w której przeanalizowano konkretny zestaw ośmiu wariantów polityki, w tym przegląd agencji ENISA i certyfikację cyberbezpieczeństwa w dziedzinie ICT.

3. Proponowane rozporządzenie zawiera dwa główne komponenty:

   - stały i określony co do zakresu mandat Agencji z myślą o potrzebach powstałych w związku z nowymi politycznymi priorytetami i instrumentami oraz odnowiony zestaw zadań i funkcji Agencji, by mogła ona efektywnie i skutecznie wspierać działania państw członkowskich, instytucji UE i innych interesariuszy nakierowane na zapewnienie bezpiecznej cyberprzestrzeni;

   - europejskie ramy certyfikacji cyberbezpieczeństwa produktów i usług ICT oraz przepisy dotyczące europejskich systemów certyfikacji cyberbezpieczeństwa, dzięki którym certyfikaty wydawane w ramach tych systemów będą ważne i uznawane we wszystkich państwach członkowskich, i co pozwoli na zajęcie się kwestią obecnego rozdrobnienia rynku.

[1] Dok. 12183/17; 12183/1/17 REV 1; 12183/2/17 REV 2.

4. W październiku 2017 r. Rada Europejska[2] wezwała do opracowania w sposób całościowy i w stosownym terminie wniosków Komisji dotyczących cyberbezpieczeństwa, a następnie ich bezzwłoczne przeanalizowanie, zgodnie z planem działania, który ma ustanowić Rada.

5. W dniu 12 grudnia 2017 r. Rada do Spraw Ogólnych przyjęła plan działania[3] w celu wdrożenia konkluzji Rady[4] w sprawie wspólnego komunikatu[5] do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE". Plan działania odzwierciedla zamiar Rady do wypracowania podejścia ogólnego w sprawie wniosku do czerwca 2018 r.

6. W Parlamencie Europejskim na sprawozdawcę powołano Angelikę NIEBLER (ITRE, PPE). Głosowanie na forum komisji ITRE w sprawie odnośnego sprawozdania zaplanowano na 19 czerwca 2018 r.

7. Europejski Komitet Ekonomiczno-Społeczny przyjął opinię w dniu 14 lutego 2018 r.

II. PRACE W RADZIE

8. Komisja przedstawiła przedmiotowy wniosek i stosowną ocenę skutków Horyzontalnej Grupie Roboczej ds. Cyberprzestrzeni (zwanej dalej „grupą roboczą") w dniu 26 września 2017 r.; następnie na forum grupy roboczej w dniu 20 października 2017 r. przeprowadzono analizę oceny skutków. Kolejne dyskusje koncentrowały się na zdolności operacyjnej Agencji i zakresie interakcji z krajowymi właściwymi organami, a także na wpływie ram certyfikacji na rynek i konkurencyjność przedsiębiorstw. Delegacje ogólnie pozytywnie zareagowały zarówno na ocenę skutków, jak i na otrzymany wniosek.

---

[2] Dok. EUCO 14/17, pkt 11.
[3] Dok. 15748/17.
[4] Dok. 14435/17.
[5] Dok. 12211/17.

9. Analizę samego wniosku na forum grupy roboczej rozpoczęto w listopadzie 2017 r., podczas prezydencji estońskiej, i kontynuowano w ramach prezydencji bułgarskiej. W związku z tą analizą odbyło się 12 posiedzeń, w wyniku których opracowano osiem kolejnych zmienionych wersji wniosku z myślą o uzgodnieniu podejścia ogólnego na nadchodzącym posiedzeniu Rady ds. TTE (Telekomunikacja), które odbędzie się w dniu 8 czerwca 2018 r.

10. Wynik dyskusji na forum grupy roboczej, która odbyła się w dniach 14–15 maja 2018 r., a także zmieniona wersja tekstu kompromisowego prezydencji znajduje się w załączniku do niniejszej noty. Motywy zostały dostosowane w celu odzwierciedlenia zmian w przepisach merytorycznych. Zmiany względem wniosku Komisji zostały **wytłuszczone** lub oznaczone symbolem [...]. Zmiany względem ostatniego przygotowanego przez grupę roboczą dokumentu (8834/18) oznaczono **wytłuszczeniem i podkreśleniem**, a tekst usunięty symbolem **[...]**.

III. PODSUMOWANIE

11. Kompromisowy tekst prezydencji przedstawiony w załączniku odzwierciedla starania prezydencji i państw członkowskich na rzecz osiągnięcia odpowiedniej równowagi w tekście.

12. W dniu 25 maja 2018 r. Komitet Stałych Przedstawicieli osiągnął porozumienie co do kompromisowego tekstu prezydencji, z zastrzeżeniem zmian w art. 19 ust. 5 i art. 48 ust. 5 w wersji przedstawionej w załączniku.

13. W związku z powyższym Rada jest proszona o przyjęcie podejścia ogólnego na swoim posiedzeniu w dniu 8 czerwca 2018 r. i upoważnienie prezydencji do rozpoczęcia negocjacji z przedstawicielami Parlamentu Europejskiego i Komisji Europejskiej w sprawie przedmiotowego dossier.

ZAŁĄCZNIK

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[6],

uwzględniając opinię Komitetu Regionów[7],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

[6] Dz.U. C […] z […], s. […].
[7] Dz.U. C […] z […], s. […].

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 zagrożenia dla cyberbezpieczeństwa 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 zagrożeniami dla cyberbezpieczeństwa 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 zagrożenia dla cyberbezpieczeństwa 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, w obliczu 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 zagrożeń dla cyberbezpieczeństwa 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[8] 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[9] przedłużające mandat Agencji do marca 2012 r. Rozporządzeniem (WE) nr 580/2011[10] dodatkowo przedłużono mandat Agencji do dnia 13 września 2013 r. W roku 2013 Parlament Europejski i Rada przyjęły rozporządzenie (UE) nr 526/2013[11] w sprawie ENISA oraz uchylające rozporządzenie (WE) nr 460/2004, którym przedłużono mandat Agencji do czerwca 2020 r.

---

[8] 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).

[9] 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).

[10] 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).

[11] 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).

(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 zagrożenia dla cyberbezpieczeństwa i ryzyka w cyberprzestrzeni. 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 bezpieczeństwa sieci i informacji"). W dyrektywie w sprawie bezpieczeństwa sieci i informacji 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 cyberbezpieczeństwa 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 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 europejskimi instytucjami, agencjami i organami.

(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 **wspierać** [...] działania krajowe i **proaktywnie włączać się w** działania unijne, a jednocześnie wykonywać swoje zadania w pełnej współpracy z instytucjami, [...] agencjami i **organami** 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, a **także kwestii specyficznych dla tego sektora w celu zwiększenia roli unijnych polityk i przepisów dotyczących cyberbezpieczeństwa i umożliwienia spójności w ich wdrażaniu na szczeblu krajowym** [...]. 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 bezpieczeństwa sieci i informacji, co ma kluczowe znaczenie dla zwiększenia cyberodporności. W obliczu szybko ewoluującego profilu zagrożeń dla cyberbezpieczeństwa 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, [...] agencje i **organy** w ich staraniach na rzecz budowy i umocnienia zdolności i gotowości do zapobiegania [...] **zagrożeniom** dla cyberbezpieczeństwa i cyberincydentom, 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. **Prowadzone przez agencję ENISA działania związane ze zdolnościami operacyjnymi państw członkowskich powinny mieć wyłącznie charakter uzupełniający do działań podejmowanych przez państwa członkowskie w celu wypełnienia ich zobowiązań wynikających z dyrektywy w sprawie bezpieczeństwa sieci i informacji, a więc nie powinny takich działań zastępować** [...].

(15a) Agencja powinna również pomagać w opracowaniu i aktualizacji strategii Unii i – na wniosek – strategii państw członkowskich w zakresie bezpieczeństwa sieci i systemów informatycznych, w szczególności w odniesieniu do cyberbezpieczeństwa, propagować ich upowszechnienie i śledzić ich realizację. 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 bezpieczeństwa sieci i informacji 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 [...] **Agencja powinna** wspierać **wymianę informacji w ramach samych sektorów i między sektorami, szczególnie w przypadku sektorów wymienionych w załączniku II do dyrektywy (UE) 2016/1148, poprzez przedstawianie najlepszych praktyk i wytycznych w zakresie dostępnych narzędzi, i procedur oraz wytycznych na temat rozwiązywania kwestii regulacyjnych związanych z wymianą informacji, na przykład dzięki ułatwianiu** [...] ustanawiania sektorowych ośrodków wymiany i analizy informacji [...].

(18) Agencja powinna gromadzić i analizować **dobrowolnie udostępniane** raporty krajowe przekazywane przez zespoły CSIRT i CERT-UE, **by pomagać państwom członkowskim** w ustalaniu wspólnych [...] **procedur**, języka i terminologii do celów wymiany informacji. Agencja powinna również angażować sektor prywatny, działając w ramach wyznaczonych przez dyrektywę w sprawie bezpieczeństwa sieci i informacji, w której położono podstawy pod dobrowolną wymianę informacji technicznych na poziomie operacyjnym **[...] w ramach** sieci CSIRT.

(19) Agencja powinna wnosić wkład w reakcję na szczeblu UE w przypadku transgranicznych cyberincydentów na dużą skalę i cyberkryzysów. Zadanie to **powinno być wykonywane zgodnie z jej mandatem na mocy niniejszego rozporządzenia i podejściem uzgodnionym przez państwa członkowskie w kontekście Zalecenia Komisji w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę. Mogłoby to** 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 [...] **regularnych** ćwiczeń w dziedzinie cyberbezpieczeństwa.

(20) [...] **Wspierając współpracę** operacyjną [...], Agencja powinna korzystać z dostępnej **technicznej i operacyjnej** wiedzy fachowej CERT-UE w ramach współpracy strukturalnej [...]. […] W stosownych przypadkach należy poczynić specjalne ustalenia między obiema tymi organizacjami, aby określić sposób praktycznej realizacji takiej współpracy i **uniknąć powielania działań**.

(21) Zgodnie ze swoimi zadaniami [...] **polegającymi na wspieraniu współpracy operacyjnej w ramach sieci CSIRT** Agencja powinna być w stanie zapewniać wsparcie **na wniosek** państw członkowskich, na przykład oferując doradztwo **dotyczące zwiększenia ich możliwości w zakresie zapobiegania incydentom, ich wykrywania oraz reagowanie na nie, […] ułatwiając działania** [...] techniczne w **obliczu incydentów o znacznych lub istotnych skutkach** [...] lub zapewniając analizy zagrożeń i incydentów. **Ułatwianie technicznych działań w obliczu incydentów o znacznych lub istotnych skutkach powinno w szczególności obejmować wsparcie udzielane przez agencję ENISA w zakresie dobrowolnego dzielenia się rozwiązaniami technicznymi między państwami członkowskimi lub opracowywanie zbiorczych informacji technicznych – na przykład na temat rozwiązań technicznych, które dobrowolnie udostępniły państwa członkowskie. 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 we [...] **wspieraniu współpracy operacyjnej**.

(22) Jako element regularnej współpracy na poziomie technicznym służącej wzmocnieniu unijnej orientacji sytuacyjnej Agencja powinna regularnie przygotowywać w **ścisłej współpracy z państwami członkowskimi** unijny raport techniczny o stanie cyberbezpieczeństwa w UE dotyczący incydentów i zagrożeń, oparty na publicznie dostępnych informacjach, swojej własnej analizie i sprawozdaniach przekazanych przez zespoły CSIRT państw członkowskich [...] lub pojedyncze punkty kontaktowe powołane zgodnie z dyrektywą w sprawie bezpieczeństwa sieci i informacji **(oba rodzaje przekazywane na zasadzie dobrowolności)**, Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu oraz przez 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) **Wsparcie Agencji udzielane** – na wniosek **zainteresowanych** państw członkowskich – w przypadku technicznych postępowań wyjaśniających **e**x-post dotyczących incydentów o istotnych skutkach powinno koncentrować się na zapobieganiu przyszłym incydentom [...]. **Zainteresowane państwa członkowskie powinny dostarczyć niezbędnych informacji, by umożliwić Agencji skuteczne wsparcie technicznego postępowania wyjaśniającego.**

(24) [...]

(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 **publicznie dostępne lub dobrowolnie udostępniane** 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 cyberbezpieczeństwo. 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 [...] **cyberincydentom**.

(27) W celu wzmocnienia odporności Unii Agencja powinna przyczyniać się do osiągnięcia doskonałości w dziedzinie **cyber**bezpieczeństwa **infrastruktur wspierających zwłaszcza sektory wymienione w załączniku II dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz infrastruktur wykorzystywanych przez dostawców usług cyfrowych, które to usługi wymieniono w załączniku III tej dyrektywy** [...], 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, [...] agencjami i **organami** 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), **Agencją Europejskiego Globalnego Systemu Nawigacji Satelitarnej (Agencja Europejskiego GNSS)** 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, w **swojej roli** [...] sekretariatu sieci CSIRT, powinna wspierać zespoły CSIRT państw członkowskich i CERT-UE we współpracy operacyjnej dotyczącej wszystkich odpowiednich zadań sieci CSIRT określonych w dyrektywie w sprawie bezpieczeństwa sieci i informacji. 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 [...] **regularne** ćwiczenia w dziedzinie cyberbezpieczeństwa na szczeblu unijnym i wspierać – na wniosek – państwa członkowskie oraz instytucje, agencje i organy UE 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, [...] agencjom i **organom** Unii, a także – w stosownych przypadkach i na ich wniosek – państwom członkowskim w kwestii potrzeb badawczych w dziedzinie [...] cyberbezpieczeństwa. **W celu określenia potrzeb i priorytetów badawczych Agencja powinna prowadzić konsultacje z odpowiednimi grupami użytkowników.**

(37) **Zagrożenia** [...] dla cyberbezpieczeństwa mają charakter globalny. Istnieje potrzeba zacieśnienia współpracy międzynarodowej w celu poprawy norm **cyber**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, [...] agencjom i **organom** 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 przedkładane zarządowi sprawozdanie roczne, w **tym informacje na temat wykonania rocznego programu prac Agencji**, 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 […] **p**rogramu […] **p**rac, 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[12]. 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[13]. 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.

---

[12] 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).

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

(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) […]

(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 uzasadnienia 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 bezpieczeństwa sieci i informacji 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 **procesów**, 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 uzasadnienia 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, [...] 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 główne wymogi horyzontalne dotyczące europejskich systemów certyfikacji cyberbezpieczeństwa, które mają zostać opracowane, oraz umożliwiających uznawanie i stosowanie we wszystkich państwach członkowskich certyfikatów **i unijnych oświadczeń o zgodności** 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 **europejskich**, o ile normy te nie są nieskuteczne lub nieodpowiednie na potrzeby realizacji uzasadnionych celów UE w tym zakresie.

(53) Komisja powinna być uprawniona do przyjmowania europejskich systemów certyfikacji cyberbezpieczeństwa dotyczących określonych grup **procesów**, produktów i usług ICT. Systemy te powinny być wprowadzane i nadzorowane przez krajowe organy ds. [...] certyfikacji **cyberbezpieczeństwa**, 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 europejskiego systemu certyfikacji cyberbezpieczeństwa powinno być zapewnienie, by **procesy**, produkty i usługi ICT certyfikowane zgodnie z takim systemem, spełniają określone wymogi **[...] w** celu **[...] zabezpieczenia** dostępności, autentyczności, integralności i poufności przechowywanych lub przekazywanych lub przetwarzanych danych, lub też funkcji bądź usług oferowanych lub dostępnych za pośrednictwem tych produktów, procesów, usług i systemów w **trakcie ich całego cyklu życia** – w rozumieniu niniejszego rozporządzenia. Nie jest możliwe szczegółowe określenie w niniejszym rozporządzeniu wymogów w zakresie cyberbezpieczeństwa odnoszących się do wszystkich **procesów**, produktów i usług ICT. **Procesy**, 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 **procesów**, produktów i usług ICT należy następnie doprecyzować na poziomie poszczególnych systemów certyfikacji przyjmowanych przez Komisję, na przykład poprzez odniesienie do norm lub specyfikacji technicznych w **przypadku gdy nie istnieją odpowiednie normy**.

(55a) Specyfikacje techniczne, które mają być wykorzystywane w europejskim systemie certyfikacji cyberbezpieczeństwa, powinny być identyfikowane przy poszanowaniu zasad określonych w załączniku II do rozporządzenia (UE) 1025/2012. Pewne odstępstwa od tych zasad mogą się jednak okazać konieczne w należycie uzasadnionych przypadkach, gdy te specyfikacje techniczne mają być wykorzystywane w europejskim systemie certyfikacji cyberbezpieczeństwa o poziomie uzasadnienia pewności „wysoki". Uzasadnienie takich odstępstw musi być podane od wiadomości publicznej.

(55b) Certyfikowana ocena zgodności to proces, w którym ocenia się czy zostały spełnione konkretne wymogi dotyczące procesu, produktu lub usługi ICT. Proces ten przeprowadza niezależna strona trzecia, inna niż wytwórca produktu lub dostawca usług. Proces wydania certyfikatu następuje w wyniku pozytywnej oceny procesu, produktu lub usługi ICT. Należy uznać go za potwierdzenie, że dana ocena została przeprowadzona prawidłowo. Zależnie od poziomu uzasadnienia pewności, europejski system certyfikacji cyberbezpieczeństwa powinien określać, czy certyfikat wydaje podmiot prywatny czy publiczny. Ocena zgodności i certyfikacja same w sobie nie są w stanie 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.

(55c) Dokonywany przez użytkowników certyfikatów wybór odpowiedniego poziomu certyfikacji i powiązanych wymogów bezpieczeństwa powinien być oparty na analizie ryzyka dotyczącej korzystania z danego procesu, produktu lub usługi ICT. Poziom uzasadnienia pewności powinien zatem być współmierny do poziomu ryzyka związanego z przewidzianym zastosowaniem procesu, produktu lub usługi ICT.

(55d) Europejski system certyfikacji cyberbezpieczeństwa mógłby przewidywać, że ocenę zgodności przeprowadza się na wyłączną odpowiedzialność wytwórcy lub dostawcy produktów lub usług ICT (samoocena zgodności). W takich przypadkach wystarczy, by wytwórca lub dostawca przeprowadził we własnym zakresie wszelkie kontrole w celu zapewnienia zgodności procesu, produktu lub usługi ICT z systemem certyfikacji. Ten rodzaj oceny zgodności powinien być uznawany za odpowiedni dla produktów i usług ICT o niewielkiej złożoności (np. mechanizm o prostej konstrukcji i prostym wytwarzaniu), które stwarzają niskie ryzyko dla interesu publicznego. Ponadto przedmiotem samooceny zgodności mogłyby być jedynie produkty i usługi ICT o poziomie uzasadnienia pewności „podstawowy".

(55e) Europejski system certyfikacji cyberbezpieczeństwa mógłby zezwalać zarówno na certyfikację, jak i samoocenę zgodności produktów i usług ICT. W takim przypadku system powinien przewidywać jasne i zrozumiałe dla konsumentów lub innych użytkowników środki rozróżniania między produktami i usługami ocenianymi na odpowiedzialność wytwórcy lub dostawcy a produktami i usługami, które certyfikuje strona trzecia.

(55f) Wytwórca lub dostawca produktów i usług ICT przeprowadzający samoocenę zgodności powinien sporządzić i podpisać unijne oświadczenie o zgodności, jako element procedury oceny zgodności. Unijne oświadczenie o zgodności to dokument, w którym stwierdza się, że dany produkt lub usługa ICT są zgodne z wymogami systemu. Sporządzając i podpisując unijne oświadczenie o zgodności, wytwórca lub dostawca przyjmują odpowiedzialność za zgodność produktu lub usługi ICT z prawnymi wymogami danego systemu. Kopia unijnego oświadczenia o zgodności powinna być przedkładana krajowemu organowi ds. certyfikacji cyberbezpieczeństwa i agencji ENISA.

(55g) Wytwórcy lub dostawcy produktów i usług ICT powinni – przez okres zdefiniowany w danym europejskim systemie certyfikacji cyberbezpieczeństwa – przechowywać do dyspozycji właściwego krajowego organu ds. certyfikacji cyberbezpieczeństwa unijne oświadczenie o zgodności i dokumentację techniczną wszystkich istotnych informacji związanych ze zgodnością produktów lub usług ICT z systemem certyfikacji. Dokumentacja techniczna powinna określać mające zastosowane wymogi i obejmować, w stopniu, w jakim ma to znaczenie dla oceny, projekt, produkcję i działanie produktu lub usługi ICT. Dokumentacja techniczna powinna być opracowana tak, by umożliwiać ocenę zgodności produktu lub usługi ICT z odpowiednimi wymogami.

(55h) Państwa członkowskie i zainteresowane organizacje interesariuszy powinny być uprawione do zwracania się do Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa z propozycją dotyczącą przygotowania kandydującego systemu. Zainteresowane organizacje interesariuszy to organizacje branżowe lub organizacje przedstawicieli konsumentów, w tym przedstawiciele organizacji MŚP, mające istotny interes w stworzeniu konkretnego europejskiego systemu certyfikacji cyberbezpieczeństwa. Propozycje takie powinny zostać następnie przeanalizowane w świetle kryteriów opracowanych przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa na podstawie wytycznych opartych na zasadach przejrzystości, otwartości, bezstronności, konsensusu, skuteczności, istotności i spójności.

(56) Komisja **i Grupa** powinny zostać uprawnione do zwracania się do agencji ENISA z wnioskiem o przygotowanie **bez zbędnej zwłoki** kandydujących systemów dla określonych **procesów**, 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 **procesów**, 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 uzasadnienia pewności: podstawowy, istotny lub wysoki, a **w stosownych przypadkach poziomy oceny.**

(56a) Pewność, jaką daje europejski system certyfikacji, buduje zaufanie, że proces, produkt lub usługa ICT spełniają wymogi bezpieczeństwa danego europejskiego systemu certyfikacji cyberbezpieczeństwa. By zapewnić spójność ram certyfikowanych procesów, produktów i usług ICT, poszczególne systemy certyfikacji cyberbezpieczeństwa mogłyby określać poziomy uzasadnienia pewności wydawanych w swoich ramach europejskich certyfikatów cyberbezpieczeństwa i unijnych oświadczeń o zgodności. Każdy certyfikat mógłby wskazywać jeden z poziomów uzasadnienia pewności: podstawowy, istotny bądź wysoki, natomiast unijne oświadczenie o zgodności mogłoby jedynie wskazywać poziom uzasadnienia pewności „podstawowy". Poziomy uzasadnienia pewności odpowiadają poziomowi nakładów wymaganych do oceny […] i ustala się je podając odniesienia do powiązanych z nimi specyfikacji technicznych, norm i procedur, w tym kontroli technicznych, których celem jest zapobieganie cyberincydentom lub łagodzenie ich skutków. Poszczególne poziomy uzasadnienia pewności powinny być spójne dla poszczególnych dziedzin sektorów, w których stosuje się certyfikację.

(56b) Europejski system certyfikacji cyberbezpieczeństwa może przewidywać kilka poziomów oceny zależnie od tego, jak rygorystyczny i dogłębny charakter ma zastosowana metodologia oceny; poziomy te powinny odpowiadać poziomom uzasadnienia pewności i być powiązane z odpowiednim zestawem elementów określania poziomu uzasadnienia pewności. Dla wszystkich poziomów uzasadnienia pewności, produkt lub usługa ICT powinny zawierać pewne funkcje zabezpieczeń określone przez dany system certyfikacji. Takimi funkcjami mogą być: konfiguracja ustawień fabrycznych służąca bezpieczeństwu, podpisany kod, mechanizmy bezpiecznej aktualizacji i chroniące przed programami wykorzystującymi błędy w oprogramowaniu (exploit), pełna ochrona pamięci stosu (stack) / sterty (heap). Funkcje te powinny zostać zaprogramowane i być utrzymywane przy wykorzystaniu metod rozwoju zorientowanych na bezpieczeństwo i odpowiednich narzędzi w celu zagwarantowania, że zostały wdrożone skuteczne mechanizmy (zarówno w odniesieniu do oprogramowania jak i sprzętu). na których można polegać. W przypadku poziomu uzasadnienia pewności „podstawowy" ocena powinna być dokonana w oparciu o co najmniej następujące elementy określania poziomu uzasadnienia pewności: zawierać co najmniej przegląd dokumentacji technicznej produktu lub usługi ICT przeprowadzany przez jednostkę oceniającą zgodność. Jeśli certyfikacja obejmuje również procesy ICT, przeglądowi technicznemu powinny również podlegać procesy wykorzystane do zaprojektowania, stworzenia i utrzymania produktu lub usługi ICT. Jeśli europejski system certyfikacji cyberbezpieczeństwa przewiduje samoocenę zgodności, wystarczy, że wytwórca lub dostawca przeprowadzili samoocenę zgodności procesu, produktów lub usług ICT z systemem certyfikacji. W przypadku poziomu uzasadnienia pewności „istotny" ocena – oprócz elementów oceny dla poziomu uzasadnienia pewności „podstawowy" – powinna obejmować co najmniej weryfikację zgodności funkcji bezpieczeństwa produktów lub usług ICT z ich dokumentacją techniczną. W przypadku poziomu uzasadnienia pewności „wysoki" ocena – oprócz elementów oceny dla poziomu uzasadnienia pewności „istotny" – powinna obejmować co najmniej testy sprawności, w których ocenia się odporność funkcji bezpieczeństwa produktów lub usług ICT na zaawansowane cyberataki przeprowadzane przez osoby o wysokich umiejętnościach i dysponujące znacznymi zasobami.

(56c) Przygotowując system kandydujący, agencja ENISA powinna konsultować się ze wszystkimi zainteresowanymi stronami, takimi jak europejskie organizacje normalizacyjne, odpowiednie organy krajowe, organizacje działające w oparciu o umowy o wzajemnym uznawaniu takie jak SOG-IS, MŚP, organizacje konsumenckie, a także interesariusze z dziedziny środowiska i spraw społecznych.

(56d) Agencja ENISA powinna utrzymywać stronę internetową zawierającą informacje na temat europejskich systemów certyfikacji cyberbezpieczeństwa i popularyzującą te systemy, która powinna między innymi zawierać wnioski o przygotowanie kandydującego europejskiego systemu certyfikacji cyberbezpieczeństwa oraz informacje zwrotne otrzymane w wyniku konsultacji przeprowadzonych przez Agencję w fazie przygotowawczej. Taka strona powinna również zawierać informacje na temat certyfikatów i unijnych oświadczeń o zgodności wydanych na mocy niniejszego rozporządzenia.

(57) Korzystanie z europejskiej certyfikacji cyberbezpieczeństwa i **unijnego oświadczenia o zgodności** powinno pozostać dobrowolne, chyba że przepisy unijne lub przepisy krajowe **przyjęte zgodnie z prawem Unii** stanowią inaczej. **W przypadku braku zharmonizowanych przepisów państwa członkowskie mogą zgodnie z dyrektywą (UE) 2015/1535 przyjąć krajowe przepisy techniczne przewidujące obowiązkową certyfikację w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa. Państwa członkowskie mogłyby również stosować europejską certyfikację cyberbezpieczeństwa w kontekście zamówień publicznych oraz dyrektywy 2014/214/UE.** […]

(57a) Z myślą o osiągnięciu celów niniejszego rozporządzenia i uniknięciu rozdrobnienia rynku wewnętrznego krajowe systemy lub procedury certyfikacji cyberbezpieczeństwa dotyczące produktów i usług ICT objętych europejskim systemem certyfikacji cyberbezpieczeństwa powinny przestać być skuteczne z dniem ustalonym przez Komisję w drodze 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. Niemniej państwa członkowskie powinny mieć możliwość przyjmowania lub utrzymywania krajowych systemów certyfikacji do celów bezpieczeństwa narodowego.

(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 **ograniczyć, zawiesić lub** cofać akredytację danej jednostki oceniającej zgodność, jeżeli warunki akredytacji nie są lub przestały być spełniane, bądź w przypadku gdy działania podejmowane przez jednostkę oceniającą zgodność naruszają niniejsze rozporządzenie.

(59) [...] Państwa członkowskie **[...] powinny** wyznaczyć **co najmniej jeden organ** ds. [...] certyfikacji cyberbezpieczeństwa odpowiedzialny za nadzorowanie zgodności z **obowiązkami wynikającymi z niniejszego rozporządzenia**. **Jeśli dane państwo członkowskie uzna to za właściwe, zadania te mogą zostać przydzielone już istniejącym organom. Państwa członkowskie powinny także mieć możliwość podjęcia decyzji, za obopólnym porozumieniem z innym państwem członkowskim, w sprawie wyznaczenia organu nadzoru lub organów nadzoru na terytorium tego innego państwa członkowskiego. Organ nadzoru powinien w szczególności: monitorować i egzekwować wypełnianie przez mających siedzibę na ich terytorium wytwórców lub dostawców produktów i usług ICT obowiązków związanych z unijnym oświadczeniem o zgodności; wspierać, poprzez udostępnianie wiedzy fachowej i odpowiednich informacji, krajowe jednostki akredytacyjne w monitorowaniu i nadzorowaniu działalności jednostek oceniających zgodność; zezwalać jednostkom oceniającym zgodność na wykonywanie ich zadań pod warunkiem spełnienia przez nie dodatkowych wymogów przewidzianych w danym systemie; oraz monitorować rozwój sytuacji w dziedzinie certyfikacji cyberbezpieczeństwa.** […] Krajowe organy [...] ds. certyfikacji **cyberbezpieczeństwa** powinny rozpatrywać skargi składane przez osoby fizyczne lub prawne w związku z wydanymi **przez te organy certyfikatami lub certyfikatami wydanymi przez jednostki oceniające zgodność i dotyczącymi poziomu uzasadnienia pewności „wysoki”** [...], 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 [...] ds. certyfikacji **cyberbezpieczeństwa** 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 [...] ds. certyfikacji **cyberbezpieczeństwa lub innych odpowiednich organów krajowych**. 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 Agencji opinii na temat systemów kandydujących oraz** skierowanych do Komisji opinii dotyczących utrzymania i przeglądu istniejących europejskich systemów certyfikacji cyberbezpieczeństwa;

(60a) Grupa powinna ułatwiać wymianę dobrych praktyk i wiedzy fachowej między krajowymi organami ds. certyfikacji cyberbezpieczeństwa odpowiedzialnymi za jednostki oceniające zgodność i wydawanie certyfikatów. Grupa powinna wspierać rozwijanie mechanizmu wzajemnej oceny w kontekście przygotowywania kandydującego systemu i wdrażanie tego mechanizmu – na rzecz organów wydających europejskie certyfikaty cyberbezpieczeństwa o poziomie uzasadnienia pewności „wysoki”. Takie wzajemne oceny powinny w szczególności sprawdzać, czy dane organy dysponują odpowiednią wiedzą fachową i wykonują swoje obowiązki w zharmonizowany sposób. Wyniki wzajemnych ocen powinny być podane od wiadomości publicznej. Organy te mogą przyjmować odpowiednie środki w celu dostosowania swoich praktyk i wiedzy fachowej.

(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.

(61a) W celu dalszego ułatwiania handlu i uznając, że łańcuchy dostaw w dziedzinie ICT maja charakter globalny, Unia może zgodnie z art. 218 TFUE zawierać umowy o wzajemnym uznawaniu dotyczące certyfikatów wydanych w ramach systemów stanowiących część europejskich ram certyfikacji cyberbezpieczeństwa. Komisja, uwzględniając opinię agencji ENISA i Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa, może zalecić rozpoczęcie stosownych negocjacji. Każdy system powinien przewidywać szczegółowe warunki wzajemnego uznawania z państwami trzecimi.

(62) […]

(63) […]

(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 przez krajowe organy [...] ds. certyfikacji **cyberbezpieczeństwa** akredytowanych jednostek oceniających zgodność.

(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 stosowania

1. 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 [...] Unii Europejskiej ds. **Cyberbezpieczeństwa**" ENISA, zwanej dalej „Agencją"; oraz

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

2. **Niniejsze rozporządzenie pozostaje 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 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „cyberbezpieczeństwo” obejmuje wszystkie działania niezbędne do ochrony przed zagrożeniami dla cyberbezpieczeństwa 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) „zagrożenie dla cyberbezpieczeństwa” oznacza wszelkie potencjalne okoliczności lub zdarzenia, które mogą **uszkodzić lub zakłócić** sieci i systemy informatyczne, ich użytkowników oraz osoby, których zagrożenie to dotyczy, **albo w inny sposób niekorzystnie wpływać** na te sieci i systemy informatyczne, użytkowników i osoby, których zagrożenie to dotyczy.

9) „europejski system certyfikacji cyberbezpieczeństwa” oznacza kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur określonych na szczeblu Unii i mających zastosowanie do certyfikacji **lub oceny zgodności** objętych zakresem danego systemu **procesów**, produktów i usług z dziedziny technologii informacyjno-komunikacyjnych (ICT) ;

9a) „krajowy system certyfikacji cyberbezpieczeństwa” oznacza kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur określonych i przyjętych przez krajowy organ publiczny i mających zastosowanie do certyfikacji lub oceny zgodności objętych zakresem danego systemu procesów, produktów i usług z dziedziny ICT;

10) „europejski certyfikat cyberbezpieczeństwa” oznacza dokument [...] poświadczający, że dany **proces**, produkt lub dana usługa ICT [...] **zostały ocenione pod kątem zgodności** ze szczegółowymi wymogami **bezpieczeństwa** określonymi w europejskim systemie certyfikacji cyberbezpieczeństwa;

11) „produkt [...] ICT” oznacza każdy element lub każdą grupę elementów sieci i systemów informatycznych;

11a) „usługa ICT” oznacza każdą usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych;

11b) „proces ICT” oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, utrzymywania i dostarczania produktów lub usług ICT;

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;

16a) „specyfikacja techniczna” oznacza dokument określający wymogi techniczne, które powinny zostać spełnione przez proces, produkt lub usługę ICT;

16b) „poziom uzasadnienia pewności” daje podstawy uznania, że proces, produkt lub usługa ICT spełniają wymogi bezpieczeństwa konkretnego europejskiego systemu certyfikacji cyberbezpieczeństwa i wskazuje na jakim poziomie została dokonana ich ocena; poziom uzasadnienia pewności nie stanowi pomiaru bezpieczeństwa samych procesów, produktów lub usług ICT.

TYTUŁ II

ENISA – „*Agencja [...] Unii Europejskiej ds. Cyberbezpieczeństwa*”

ROZDZIAŁ I

MANDAT I CELE *[...]*

Artykuł 3

Mandat

1. Agencja podejmuje zadania przypisane jej na mocy niniejszego rozporządzenia w celu przyczyniania się do wysokiego poziomu cyberbezpieczeństwa [...] **na terytorium** Unii, **szczególnie poprzez wspieranie państw członkowskich i instytucji, agencji i organów Unii w w poprawie cyberbezpieczeństwa. Agencja działa jako punkt odniesienia w zakresie doradztwa i wiedzy fachowej z zakresu cyberbezpieczeństwa – na rzecz instytucji, agencji i organów 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.

2a. Wykonując swoje zadania, Agencja działa niezależnie i w możliwie największym stopniu uwzględnia krajową wiedzę fachową, którą dysponują odpowiednie organy państw członkowskich, a jednocześnie unika powielania działań.

3. [...]

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 **unijnych** polityk dotyczących cyberbezpieczeństwa**, w tym polityk sektorowych dotyczących cyberbezpieczeństwa**.

3. Agencja wspiera budowanie potencjału i gotowości w całej Unii, pomagając **instytucjom, agencjom i organom** Unii, a **także** państwom członkowskim oraz zainteresowanym stronom z sektora publicznego i prywatnego w zwiększeniu ochrony ich sieci i systemów informatycznych, rozwijaniu i **polepszaniu cyberodporności i zdolności reagowania oraz w rozwijaniu** umiejętności i kompetencji z dziedziny cyberbezpieczeństwa [...].

4. Agencja propaguje współpracę i koordynację na szczeblu unijnym pomiędzy państwami członkowskimi, instytucjami, agencjami i organami Unii oraz właściwymi zainteresowanymi stronami z **sektora publicznego i prywatnego** [...] w kwestiach związanych z cyberbezpieczeństwem.

5. Agencja **przyczynia się do zwiększania** [...] zdolności w zakresie cyberbezpieczeństwa na poziomie unijnym w celu [...] **wspomagania** państw członkowskich w zapobieganiu zagrożeniom dla cyberbezpieczeństwa i reagowaniu na nie, zwłaszcza w przypadku incydentów transgranicznych.

6. Agencja propaguje stosowanie certyfikacji z **myślą o unikaniu rozdrobnienia systemów certyfikacji w UE**. **Agencja przyczynia się szczególnie** [...] 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 cyberbezpieczeństwem.

ROZDZIAŁ IA

ZADANIA

Artykuł 5

[...] ***Opracowywanie i wdrażanie 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 [...] **incydentach w zakresie** 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

[...] ***Budowanie zdolności***

1. Agencja pomaga:

a) państwom członkowskim w ich staraniach na rzecz poprawy w zakresie zapobiegania [...] cyberincydentom i **zagrożeniom** dla cyberbezpieczeństwa, wykrywania i analizowania tych zagrożeń i incydentów oraz zdolności reagowania na nie – poprzez zapewnianie państwom członkowskim niezbędnej wiedzy fachowej;

b) instytucjom, agencjom i **organom** [...] Unii w ich staraniach na rzecz poprawy zapobiegania [...] cyberincydentom i **zagrożeniom** dla cyberbezpieczeństwa, ich wykrywania i analizowania oraz zdolności reagowania na nie – **szczególnie** poprzez odpowiednie wsparcie zespołu CERT na rzecz unijnych instytucji, organów i agencji (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 i [...] **śledzi ich wdrażanie** w całej Unii 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 **regularne** [...] ćwiczenia w dziedzinie cyberbezpieczeństwa na szczeblu unijnym, 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, w [...] wymianie 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 **wspiera wymianę informacji w ramach sektorów i między sektorami** [...], 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

*[...] **Współpraca operacyjna na szczeblu unijnym***

1. Agencja wspiera współpracę operacyjną między **państwami członkowskimi, instytucjami, agencjami i** [...] organami Unii, oraz między zainteresowanymi stronami.

2. Agencja współpracuje na poziomie operacyjnym i tworzy synergię z instytucjami, agencjami i [...] **organami** 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 i w **ramach tych obowiązków** [...] ułatwia wymianę informacji i współpracę między jej członkami.

4. Agencja **wspiera** [...] współpracę operacyjną w ramach sieci CSIRT, zapewniając państwom członkowskim, **na ich wniosek**, wsparcie poprzez:

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

   b) [...] **ułatwianie** technicznych **działań w obliczu** incydentów o znacznych lub istotnych skutkach, w **tym zwłaszcza poprzez wspieranie dobrowolnego dzielenia się rozwiązaniami technicznymi przez państwa członkowskie**;

   c) analizę podatności na zagrożenia [...] i incydentów**;**

   ca) dostarczanie wsparcia w zakresie technicznych postępowań wyjaśniających ex post dotyczących incydentów o znacznych lub istotnych skutkach zgodnie z dyrektywą (UE) 2016/1148.

Realizując te zadania, Agencja i CERT-UE angażują się we współpracę strukturalną w celu czerpania korzyści z efektów synergii i **unikania powielania działań** [...].

5. [...]

[...]

6. Agencja organizuje **regularne** [...] 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. **Takie ćwiczenia na szczeblu unijnym mogą obejmować elementy techniczne, operacyjne i strategiczne.** [...] **Raz na dwa lata należy organizować ćwiczenia na wielką skalę, które będą obejmować wszystkie te elementy. W** stosownych przypadkach Agencja wnosi również wkład w sektorowe ćwiczenia w dziedzinie cyberbezpieczeństwa i pomaga w ich organizacji wspólnie z odpowiednimi [...] **organizacjami, które mogą również brać** udział w ćwiczeniach w dziedzinie cyberbezpieczeństwa na szczeblu unijnym.

7. Agencja, w **ścisłej współpracy z państwami członkowskimi**, przygotowuje regularnie unijny raport techniczny o stanie cyberbezpieczeństwa w UE dotyczący incydentów i zagrożeń, w oparciu o informacje ze źródeł otwartych, własne analizy oraz sprawozdania udostępniane przez, między innymi: zespoły CSIRT państw członkowskich [...] lub pojedyncze punkty kontaktowe powołane zgodnie z dyrektywą w sprawie bezpieczeństwa sieci i informacji (**oba rodzaje sprawozdań przekazywane na zasadzie dobrowolności** [...]) Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu, zespół 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) zestawianie **udostępnionych dobrowolnie** 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) [...] **na wniosek państw członkowskich, ułatwianie** technicznych działań w obliczu incydentu lub kryzysu, w **tym zwłaszcza** [...] **poprzez wspieranie dobrowolnego** dzielenia się przez państwa członkowskie rozwiązaniami technicznymi;

d) wspieranie **instytucji, agencji i organów UE oraz, na wniosek, państw członkowskich** w zakresie komunikacji publicznej w związku z incydentem lub kryzysem;

e) **wspieranie państw członkowskich na ich wniosek w** testowaniu planów współpracy w zakresie reagowania na takie incydenty lub kryzysy.

Artykuł 8

[...] ***Rynek, certyfikacja cyberbezpieczeństwa i normalizacja***

Agencja:

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

1) przygotowywanie kandydujących europejskich systemów certyfikacji cyberbezpieczeństwa w odniesieniu do **procesów**, produktów i usług ICT **we współpracy z sektorem oraz 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 [...] ds. certyfikacji **cyberbezpieczeństwa** oraz z przemysłem;

3a) zalecanie odpowiednich specyfikacji technicznych do zastosowania przy tworzeniu europejskich systemów certyfikacji cyberbezpieczeństwa, o których to specyfikacjach mowa w art. 47 ust. 1 lit. b), w przypadkach gdy nie istnieją odpowiednie normy;

3b) przyczynianie się do budowania wystarczających zdolności związanych z procesami oceny i certyfikacji – w drodze opracowywania i publikowania wytycznych, a także udzielania wsparcia państwom członkowskim na ich wniosek;

b) ułatwia ustanowienie i upowszechnienie europejskich i międzynarodowych norm dotyczących zarządzania ryzykiem i bezpieczeństwa **procesów**, produktów i usług ICT [...]**;**

ba) 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

[...] ***Wiedza i informacje*** [...]

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 dla cyberbezpieczeństwa i cyberincydentów w celu określenia powstających tendencji i pomocy w zapobieganiu [...] **cyberincydentom**;

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 [...] infrastruktur, które stanowią wsparcie sektorów wymienionych w załączniku II do dyrektywy (UE) 2016/1148 **oraz infrastruktur wykorzystywanych przez dostawców usług cyfrowych, które to usługi wymieniono w załączniku III tej dyrektywy**;

d) gromadzi, systematyzuje i podaje do wiadomości publicznej za pośrednictwem specjalnego portalu informacje na temat cyberbezpieczeństwa przekazane przez instytucje, agencje i organy Unii oraz udostępnione, **na zasadzie dobrowolności, przez państwa członkowskie i zainteresowane strony z sektora publicznego i prywatnego;**

e) […]

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

g) [...].

Artykuł 9a

Podnoszenie świadomości i edukowanie

Agencja:

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

b) organizuje, we współpracy z państwami członkowskimi oraz instytucjami, agencjami i organami Unii, regularne kampanie informacyjne na rzecz zwiększenia cyberbezpieczeństwa i jego wyeksponowania w Unii;

c) wspiera państwa członkowskie w ich staraniach mających na celu podniesienie świadomości na temat cyberbezpieczeństwa i propagowanie edukacji na ten temat;

d) wspiera bliższą współpracę i wymianę najlepszych praktyk między państwami członkowskimi odnośnie do edukacji i wiedzy na temat cyberbezpieczeństwa poprzez ułatwianie tworzenia i utrzymywania sieci krajowych punktów kontaktowych ds. edukacji.

Artykuł 10

*[...] **Badania i innowacje***

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

[...] ***Współpraca międzynarodowa***

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, poprzez:

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, [...] w **kontekście odpowiednich międzynarodowych ram współpracy**, wymiany najlepszych praktyk [...];

c) zapewnianie Komisji, na wniosek, wiedzy fachowej**;**

ca) zapewnianie doradztwa i wsparcia na rzecz Komisji, we współpracy z Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa ustanowioną na mocy art. 53, w kwestiach związanych z zawieranymi z państwami trzecimi umowami o wzajemnym uznawaniu certyfikatów cyberbezpieczeństwa.

ROZDZIAŁ II

STRUKTURA ORGANIZACYJNA 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; […]

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

da) sieć krajowych oficerów łącznikowych, która pełni funkcje określone w art. 20a.

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;

ca) nadzoruje realizację programowania wieloletniego i rocznego zawartego w jednolitym dokumencie programowym;

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. [...]

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, w **tym z realizacji rocznego programu prac**, 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;

la) regularne kontakty z instytucjami, agencjami i organami Unii w odniesieniu do ich działalności w dziedzinie cyberbezpieczeństwa w celu zapewnienia spójności w zakresie opracowywania i wdrażania polityki UE;

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. **W razie potrzeby, do celów wykonywania zadań Agencji w skuteczny i wydajny sposób i w oparciu o odpowiednią analizę kosztów i korzyści,** dyrektor wykonawczy **może** podjąć decyzję [...] o **ustanowieniu jednego lub kilku lokalnych biur w jednym lub kilku państwach członkowskich**. Przed podjęciem decyzji o utworzeniu biura lokalnego dyrektor wykonawczy **zasięga opinii państwa członkowskiego (państw członkowskich), którego (których) to dotyczy, w tym państwa członkowskiego, w którym Agencja ma siedzibę oraz** uzyskuje wcześniejszą zgodę Komisji i zarządu [...]. **Jeśli w procesie konsultacji dyrektor wykonawczy i państwa członkowskie, których to dotyczy, nie mogą osiągnąć porozumienia, kwestia ta zostaje poddana pod obrady Rady. W** decyzji określa się zakres działań prowadzonych w biurze lokalnym w sposób pozwalający uniknąć niepotrzebnych kosztów i powielania administracyjnych funkcji Agencji. [...]**Liczba personelu we wszystkich biurach lokalnych będzie utrzymywana na minimalnym poziomie, a <u>całkowita</u> liczba takich pracowników nie może przekraczać 40 % liczby personelu <u>pracującego w państwie członkowskim, w którym Agencja ma siedzibę</u>. Liczba personelu w każdym poszczególnym biurze lokalnym nie może przekraczać 10 % <u>[…]</u> liczby personelu <u>[…]</u> <u>pracującego w państwie członkowskim, w którym Agencja ma siedzibę.</u>**

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, **operatorzy usług kluczowych**, 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.

5a. Stała Grupa Przedstawicieli Zainteresowanych Stron regularnie informuje zarząd o swoich działaniach.

SEKCJA 4A
SIEĆ KRAJOWYCH OFICERÓW ŁĄCZNIKOWYCH

Artykuł 20a

Sieć krajowych oficerów łącznikowych

1. Zarząd, działając na wniosek dyrektora wykonawczego, powołuje sieć krajowych oficerów łącznikowych, w której uczestniczą przedstawiciele państw członkowskich.

2. Sieć krajowych oficerów łącznikowych składa się z przedstawicieli wszystkich państw członkowskich. Każde państwo członkowskie wyznacza jednego przedstawiciela. Posiedzenia sieci mogą być organizowane w różnych konfiguracjach eksperckich.

3. Sieć krajowych oficerów łącznikowych ma w szczególności ułatwiać wymianę informacji między agencją ENISA a państwami członkowskimi. Wspiera agencję ENISA zwłaszcza w rozpowszechnianiu jej działalności, ustaleń i zaleceń w całej UE wśród odpowiednich zainteresowanych stron.

4. Sieć krajowych oficerów łącznikowych pełni funkcję krajowego centralnego punktu kontaktowego, by ułatwiać współpracę agencji ENISA i ekspertów krajowych w kontekście realizacji programu prac tej agencji.

5. Podczas gdy krajowi oficerowie łącznikowi powinni ściśle współpracować z pochodzącymi z ich państwa przedstawicielami zarządu, sama sieć nie powiela działań zarządu ani działań prowadzonych na innych forach UE.

6. Zadania i procedury sieci krajowych oficerów łącznikowych określa się w wewnętrznych zasadach działania Agencji i upublicznia je.

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[14] 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.

---

14 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[15] i 2015/444[16]. Zasady te obejmują przepisy dotyczące wymiany, przetwarzania i przechowywania informacji niejawnych.

---

[15] 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).

[16] 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).

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.

TYTUŁ 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[17] 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.

---

[17] 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).

3. OLAF może przeprowadzać dochodzenia, w tym kontrole na miejscu i inspekcje, zgodnie z przepisami i procedurami określonymi w rozporządzeniu Parlamentu Europejskiego i Rady nr 883/2013 oraz w rozporządzeniu Rady (Euratom, WE) nr 2185/96[18] 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, 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.

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.

[18] 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).

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 **cztery** [...] lata. 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 **cztery** [...] lata.

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 decyzją zarządu [...].

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 oraz może być stroną w postępowaniach sądowych [...].

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[19]. 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[20].

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.

---

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

[20] 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 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.

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 [...] warunki umożliwiające właściwe funkcjonowanie 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 ramy certyfikacji **cyberbezpieczeństwa [...]**

1. **Ustanawia się europejskie ramy certyfikacji cyberbezpieczeństwa w celu poprawienia warunków funkcjonowania rynku wewnętrznego poprzez zwiększenie poziomu cyberbezpieczeństwa w Unii. Określają one struktury zarządzania, które umożliwiają zharmonizowane podejście na szczeblu UE do europejskich systemów certyfikacji cyberbezpieczeństwa z myślą o stworzeniu jednolitego rynku cyfrowego w zakresie procesów, produktów i usług ICT.**

2. **Europejskie ramy certyfikacji cyberbezpieczeństwa określają mechanizm ustanawiania** europejskich system**ów** [...] certyfikacji cyberbezpieczeństwa i potwierdzania, że **procesy**, produkty i usługi ICT, które [...] **oceniono** zgodnie z tymi systemami są zgodne z określonymi wymogami w zakresie **bezpieczeństwa [...] w celu zabezpieczenia** 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 [...] w **trakcie ich całego cyklu życia**.

Artykuł 44

Przygotowanie i przyjęcie europejskiego systemu certyfikacji cyberbezpieczeństwa

1. Po otrzymaniu wniosku Komisji **lub Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa (zwanej dalej „Grupą") ustanowionej na mocy art. 53**, agencja ENISA przygotowuje kandydujący europejski system certyfikacji cyberbezpieczeństwa, który spełnia wymogi określone w art. 45, 46 i 47 niniejszego rozporządzenia. […]

1a. Państwa członkowskie lub zainteresowane organizacje interesariuszy mogą proponować Grupie przygotowanie kandydującego europejskiego systemu certyfikacji cyberbezpieczeństwa. Grupa dokonuje oceny tych propozycji w oparciu o kryteria określone przez nią za pomocą wytycznych zgodnie z art. 53 ust. 3 lit. ca) i może zwrócić się do agencji ENISA o przygotowanie kandydującego europejskiego systemu certyfikacji cyberbezpieczeństwa.

2. Przygotowując kandydujące systemy, o których mowa w ust. 1 niniejszego artykułu, agencja ENISA konsultuje się ze wszystkimi odpowiednimi zainteresowanymi stronami w przejrzystych procesach konsultacji i ściśle współpracuje z Grupą. Grupa zapewnia Agencji pomoc i fachowe doradztwo [...] w związku z przygotowywaniem kandydującego systemu oraz **przyjmuje opinię na temat takiego kandydującego systemu przed przedstawieniem go Komisji.** [...] **Agencja ENISA zapewnia spójność kandydujących systemów z mającą zastosowanie zharmonizowaną normą stosowaną do akredytacji jednostki oceniającej zgodność.**

3. **Agencja ENISA w jak największym stopniu uwzględnia opinię Grupy przed przekazaniem** [...] Komisji kandydującego [...] systemu przygotowanego 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 **procesów**, produktów i usług ICT spełniające wymogi art. 45, 46 i 47 niniejszego rozporządzenia.

5. [...]

Artykuł 44a

Utrzymanie europejskiego systemu certyfikacji cyberbezpieczeństwa

1. Agencja prowadzi specjalną stronę internetową zawierającą informacje na temat europejskich systemów certyfikacji cyberbezpieczeństwa, certyfikatów i unijnych oświadczeń o zgodności wydanych zgodnie z art. 47a i popularyzującą te systemy, certyfikaty i oświadczenia.

2. Agencja, w ścisłej współpracy z Grupą, przynajmniej raz na 5 lat dokonuje przeglądu wprowadzonych europejskich systemów certyfikacji cyberbezpieczeństwa, biorąc pod uwagę informacje zwrotne otrzymane od zainteresowanych stron. Jeżeli zostanie to uznane za konieczne, Komisja lub Grupa mogą zwrócić się do Agencji o rozpoczęcie procesu opracowania zmienionego kandydującego systemu zgodnie z art. 44 ust. 2 i 3.

Artykuł 45

Cele w zakresie bezpieczeństwa europejskich systemów certyfikacji cyberbezpieczeństwa

Europejski system certyfikacji cyberbezpieczeństwa musi być tak zaprojektowany, aby [...] **osiągać**, w zależności od przypadku, **co najmniej** następujące cele w zakresie bezpieczeństwa:

a) ochrona przechowywanych, przekazywanych lub w inny sposób przetwarzanych danych przed przypadkowym lub nieuprawnionym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem **podczas całego cyklu życia procesu, produktu lub usługi**;

b) ochrona przechowywanych, przekazywanych lub w inny sposób przetwarzanych danych przed przypadkowym lub nieuprawnionym zniszczeniem, [...] takąż utratą lub zmianą **lub brakiem dostępności podczas całego cyklu życia procesu, produktu lub usługi**;

c) [...] dostęp uprawnionych osób, programów lub maszyn wyłącznie do tych danych, usług lub funkcji, do których odnoszą się ich prawa dostępu;

d) rejestracja tego, do których danych, funkcji lub usług [...] **uzyskano dostęp, które dane, funkcje lub usługi wykorzystano lub przetwarzano w innych sposób**, kiedy to miało miejsce i kto tego dokonał;

e) [...] możliwa jest kontrola, do których danych, usług lub funkcji uzyskano dostęp, [...] które dane, usługi lub funkcje wykorzystano **lub przetwarzano w innych sposób**, 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) [...] **procesy**, produkty i usług ICT oferowane są wraz z aktualnym oprogramowaniem i **sprzętem** niezawierającym **publicznie** znanych luk w zabezpieczeniach oraz mechanizmami na rzecz dokonywania bezpiecznych aktualizacji [...]**;**

ga) procesy, produkty i usługi ICT są rozwijane, produkowane, dostarczane zgodnie z wymogami w zakresie bezpieczeństwa określonymi w danym systemie.

Artykuł 46

Poziomy uzasadnienia pewności europejskich systemów certyfikacji cyberbezpieczeństwa

1. W odniesieniu do **procesów**, produktów i usług ICT poszczególne europejskie systemy certyfikacji cyberbezpieczeństwa mogą wskazać jeden lub więcej z następujących poziomów uzasadnienia pewności: podstawowy, istotny lub wysoki […]. **Poziom uzasadnienia pewności musi zatem być proporcjonalny do poziomu ryzyka związanego z przewidzianym zastosowaniem procesu, produktu lub usługi ICT.**

2. Poziomy uzasadnienia pewności: podstawowy, istotny i wysoki […] **odnoszą się do certyfikatu lub unijnego oświadczenia o zgodności wydanych w kontekście europejskiego systemu certyfikacji cyberbezpieczeństwa, który dla każdego poziomu uzasadnienia pewności przewiduje odpowiednie wymogi bezpieczeństwa, w tym funkcje bezpieczeństwa oraz odpowiadający im poziom nakładów wymaganych do oceny procesu, produktu lub usługi ICT. Certyfikat lub unijne oświadczenie o zgodności pod względem związanych z nimi specyfikacji technicznych, norm i procedur, w tym kontroli technicznych mających na celu zmniejszenie ryzyka wystąpienia cyberincydentów lub zapobieganie takim incydentom, mają następujące właściwości:**

a) **europejski certyfikat cyberbezpieczeństwa lub unijne oświadczenie o zgodności, które określają** poziom uzasadnienia pewności „podstawowy”, **dają gwarancję, że procesy, produkty lub usługi ICT spełniają odpowiednie wymogi bezpieczeństwa, w tym w zakresie funkcji bezpieczeństwa, i że zostały one ocenione na poziomie, który ma na celu zminimalizowanie znanych podstawowych ryzyk w zakresie cyberincydentów i cyberataków. Działania w zakresie oceny obejmują przynajmniej przegląd dokumentacji technicznej lub, w przypadku gdy nie ma to zastosowania, alternatywne działania o równoważnym skutku** […].

b) **europejski certyfikat cyberbezpieczeństwa, który określa** poziom uzasadnienia pewności jako **„**istotny**”**, daje **gwarancję, że procesy, produkty lub usługi ICT spełniają odpowiednie wymogi bezpieczeństwa, w tym w zakresie funkcji bezpieczeństwa, i że zostały one ocenione na poziomie, który ma na celu zminimalizowanie znanych cyberryzyk, cyberincydentów i cyberataków przeprowadzanych przez osoby o ograniczonych umiejętnościach i dysponujących niewielkimi zasobami. Działania w zakresie oceny obejmują co najmniej: sprawdzenie, czy nie występują publicznie znane luki w zabezpieczeniach oraz testy w zakresie tego, czy procesy, produkty lub usługi ICT mają prawidłowo zaimplementowaną niezbędną funkcję bezpieczeństwa; lub w przypadku gdy nie ma to zastosowania, przeprowadzane są alternatywne działania o równoważnym skutku** […];

c) **europejski certyfikat cyberbezpieczeństwa, który określa** poziom uzasadnienia pewności jako **„**wysoki**”**, daje **gwarancję, że procesy, produkty lub usługi ICT spełniają odpowiednie wymogi bezpieczeństwa, w tym w zakresie funkcji bezpieczeństwa, i że zostały one ocenione na poziomie, który ma na celu zminimalizowanie ryzyka wystąpienia zaawansowanych cyberataków przeprowadzanych przez osoby o znacznych umiejętnościach i dysponujących znaczącymi zasobami. Działania w zakresie oceny obejmują co najmniej: sprawdzenie, czy nie występują publicznie znane luki w zabezpieczeniach oraz testy w zakresie tego, czy procesy, produkty lub usługi ICT mają prawidłowo zaimplementowaną niezbędną, nowoczesną funkcję bezpieczeństwa, oraz ocenę sprawdzającą za pomocą testów penetracyjnych odporność na zaawansowane ataki. w przypadku gdy nie ma to zastosowania, przeprowadzane są alternatywne działania o równoważnym skutku** […].

2a. Europejski system certyfikacji cyberbezpieczeństwa może przewidywać kilka poziomów oceny zależnie od tego, jak rygorystyczny i dogłębny charakter ma zastosowana metodologia oceny. Każdy z poziomów oceny odpowiada jednemu z poziomów uzasadnienia pewności i jest definiowany poprzez odpowiedni zestaw elementów służących zapewnieniu danego poziomu uzasadnienia pewności.

Artykuł 47

Elementy europejskich systemów certyfikacji cyberbezpieczeństwa

1. Europejski system certyfikacji cyberbezpieczeństwa obejmuje **co najmniej** następujące elementy:

a) przedmiot i zakres **sytemu** certyfikacji, w tym rodzaj lub kategorie objętych systemem **procesów**, produktów i usług ICT, a **także objaśnienie, w jaki sposób system certyfikacji odpowiada potrzebom zakładanej grupy docelowej**;

b) [...] odniesienie do [...] międzynarodowych, **europejskich [...] lub krajowych** norm **[...] wykorzystywanych podczas oceny. W przypadku gdy nie ma takich norm, podaje się odniesienie do** […] specyfikacji technicznych **spełniających wymogi określone w załączniku II do rozporządzenia 1025/2012, lub w przypadku braku takich specyfikacji, do innych wymogów w zakresie cyberbezpieczeństwa określonych w tym systemie**;

c) w stosownych przypadkach jeden lub więcej poziomów uzasadnienia pewności;

ca) w stosownych przypadkach szczególne lub dodatkowe wymogi mające zastosowanie do jednostek oceniających zgodność w celu zagwarantowania ich kompetencji technicznych odnośnie do oceny wymogów w zakresie cyberbezpieczeństwa;

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) **w stosownych przypadkach** informacje, które wnioskodawca ma dostarczać, **lub udostępniać w inny sposób,** 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) zasady monitorowania zgodności z wymogami certyfikatów **lub unijnymi oświadczeniami o zgodności**, w tym mechanizmy wykazywania ciągłej zgodności z określonymi wymogami w zakresie cyberbezpieczeństwa;

h) **w stosownych przypadkach** warunki przyznawania i **odnawiania certyfikatu**, a **także** utrzymania, kontynuowania, rozszerzania **lub** zmniejszania zakresu certyfikacji;

i) zasady dotyczące konsekwencji niezgodności certyfikowanych **lub podlegających samoocenie** produktów i usług ICT z wymogami [...] **systemu**;

j) zasady dotyczące sposobu zgłaszania uprzednio niewykrytych, a wpływających na cyberbezpieczeństwo, luk w zabezpieczeniach **procesów**, produktów i usług ICT oraz sposobu postępowania z takimi lukami;

k) **w stosownych przypadkach** zasady dotyczące przechowywania zapisów przez jednostki oceniające zgodność;

l) identyfikacja krajowych **lub międzynarodowych** systemów certyfikacji cyberbezpieczeństwa, obejmujących ten sam rodzaj lub kategorie **procesów**, produktów i usług ICT, **wymogów w zakresie bezpieczeństwa oraz kryteriów i metod oceny;**

m) treść wydanego certyfikatu **lub unijnego oświadczenia o zgodności;**

ma) okres przechowywania przez wytwórcę lub dostawcę produktów i usług ICT unijnego oświadczenia o zgodności i dokumentacji technicznej dotyczącej wszystkich istotnych informacji;

mb[...]) maksymalny okres ważności certyfikatów;

mc[...]) polityka dotycząca ujawniania informacji na temat certyfikatów, które zostały przyznane, zmienione lub wycofane;

md[...]) warunki wzajemnego uznawania systemów certyfikacji z państwami trzecimi;

me[...]) w stosownych przypadkach, zasady dotyczące mechanizmu wzajemnej oceny dla organów wydających europejskie certyfikaty cyberbezpieczeństwa o poziomie uzasadnienia pewności „wysoki" [...] zgodnie z art. 48 ust. 4a.

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

3. Jeżeli zostanie to przewidziane w konkretnym akcie unijnym, certyfikacja **lub unijne oświadczenie o zgodności** w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa mogą być stosowane 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 47a

Samoocena zgodności

1. Europejski system certyfikacji cyberbezpieczeństwa może zezwalać na ocenę zgodności przeprowadzaną na wyłączną odpowiedzialność wytwórcy lub dostawcy produktów lub usług ICT. Taka ocena zgodności ma zastosowanie jedynie do produktów lub usług ICT o niskim ryzyku i odpowiada poziomowi uzasadnienia pewności „podstawowy”.

2. Wytwórca lub dostawca produktów i usług ICT może wydać unijne oświadczenie o zgodności stwierdzające, że wykazano spełnienie wymogów określonych w systemie. Wydając takie oświadczenie, wytwórca lub dostawca produktów i usług ICT przyjmuje na siebie odpowiedzialność za zgodność produktu lub usługi ICT z wymogami określonymi w systemie.

3. Wytwórcy lub dostawcy produktów i usług ICT przechowują – przez okres zdefiniowany w odpowiednim europejskim systemie certyfikacji cyberbezpieczeństwa – do dyspozycji krajowego organu ds. certyfikacji cyberbezpieczeństwa, o którym mowa w art. 50 ust. 1, unijne oświadczenie o zgodności i dokumentację techniczną dotyczącą wszystkich istotnych informacji związanych ze zgodnością produktów lub usług ICT z systemem certyfikacji. Kopia unijnego oświadczenia o zgodności musi zostać przedłożona krajowemu organowi ds. certyfikacji cyberbezpieczeństwa i agencji ENISA.

4. Wydanie unijnego oświadczenia o zgodności jest dobrowolne, o ile prawo Unii lub prawo państw członkowskich nie stanowi inaczej.

5. Unijne oświadczenie o zgodności wydane na podstawie niniejszego artykułu jest uznawane we wszystkich państwach członkowskich.

Artykuł 48

Certyfikacja cyberbezpieczeństwa

1. Przyjmuje się, że **procesy**, 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 **lub prawo państw członkowskich** nie stanowi inaczej.

3. Europejski certyfikat cyberbezpieczeństwa na podstawie niniejszego artykułu **odnoszący się do poziomu uzasadnienia pewności „podstawowy" lub „istotny"** 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 otrzymywany na podstawie tego systemu może być wydawany jedynie przez podmiot publiczny. Takim podmiotem [...] musi być jeden z wymienionych poniżej podmiotów:

a) krajowy organ [...] ds. certyfikacji **cyberbezpieczeństwa**, o którym mowa w art. 50 ust. 1;

b) podmiot **publiczny** akredytowany jako jednostka oceniająca zgodność na podstawie art. 51 ust. 1 [...];

c) [...].

4a. W przypadku gdy europejski system certyfikacji cyberbezpieczeństwa zgodny z art. 44 wymaga poziomu uzasadnienia pewności „wysoki", certyfikat może wydać jedynie krajowy organ ds. certyfikacji cyberbezpieczeństwa, o którym mowa w art. 50 ust. 1, lub – po spełnieniu następujących warunków – jednostka oceniająca zgodność, o której mowa w art. 51:

a) po uprzednim zatwierdzeniu przez krajowy organ ds. certyfikacji cyberbezpieczeństwa każdego certyfikatu wydanego przez jednostkę oceniającą zgodność; lub

b) po uprzednim, całościowym powierzeniu wykonywania tego zadania jednostce oceniającej zgodność przez krajowy organ ds. certyfikacji cyberbezpieczeństwa.

5. Osoba fizyczna lub prawna, która poddaje swoje **procesy**, produkty lub usługi ICT mechanizmowi certyfikacji, **udostępnia** jednostce oceniającej zgodność, o której mowa w art. 51, **lub krajowemu organowi ds. certyfikacji cyberbezpieczeństwa, o którym mowa w art. 50 – w przypadku gdy organ ten jest podmiotem wydającym certyfikat,** [...] wszystkie informacje niezbędne do przeprowadzenia procedury certyfikacji.

5a. Posiadacz certyfikatu informuje jednostkę, która wydała certyfikat, o wszelkich wykrytych później lukach lub nieprawidłowościach, związanych z bezpieczeństwem certyfikowanych procesów, produktów lub usług ICT, które to luki lub nieprawidłowości mogą mieć wpływ na wymogi z zakresu certyfikacji. Jednostka przekazuje bez zbędnej zwłoki te informacje krajowemu organowi ds. certyfikacji cyberbezpieczeństwa.

6. Certyfikaty są wydawane na [...] **okres zdefiniowany w danym systemie certyfikacji** i mogą być odnawiane [...], 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. Bez uszczerbku dla przepisów ust. 3 krajowe systemy certyfikacji cyberbezpieczeństwa i powiązane procedury dotyczące **procesów**, 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. Nadal funkcjonują krajowe systemy certyfikacji cyberbezpieczeństwa i powiązane procedury dotyczące **procesów**, produktów i usług ICT nieobjętych europejskim systemem certyfikacji cyberbezpieczeństwa.

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

3. Istniejące certyfikaty wydane w ramach krajowych systemów certyfikacji cyberbezpieczeństwa i objęte zakresem europejskiego systemu certyfikacji cyberbezpieczeństwa pozostają ważne aż do upływu ich terminu ważności.

Artykuł 50

Krajowe organy** [...] **ds. certyfikacji** **cyberbezpieczeństwa

1. Każde państwo członkowskie [...] **wyznacza na swoim terytorium co najmniej jeden** krajowy organ [...] ds. certyfikacji **cyberbezpieczeństwa lub za obopólnym porozumieniem z innym państwem członkowskim, wyznacza co najmniej jeden organ ustanowiony na terytorium tego innego państwa członkowskiego jako organ odpowiedzialny za zadania związane z nadzorem w wyznaczającym państwie członkowskim.**

2. Każde państwo członkowskie podaje Komisji nazwę **[...] wyznaczonych organów i informuje o przypisanych im zadaniach**.

3. **Bez uszczerbku dla art. 48. ust. 4 lit. a) i art. 48 ust. 4a** […] **k**ażdy krajowy organ [...] ds. certyfikacji **cyberbezpieczeństwa** pozostaje – w zakresie swojej organizacji, decyzji w sprawie finansowania, struktury prawnej i procesu podejmowania decyzji – niezależny od jednostek, nad którymi sprawuje nadzór.

3a. Państwa członkowskie zapewniają, by działalność krajowych organów ds. certyfikacji cyberbezpieczeństwa – związana z wydawaniem certyfikatów zgodnie z art. 48 ust. 4 lit. a) i art. 48 ust. 4a – była wykonywana z zachowaniem ścisłego podziału ról i obowiązków w stosunku do działań nadzorczych opisanych w niniejszym artykule i by oba rodzaje działalności były wykonywane niezależnie od siebie.

4. Państwa członkowskie zapewniają, aby krajowe organy [...] ds. certyfikacji **cyberbezpieczeństwa** 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 [...] ds. certyfikacji **cyberbezpieczeństwa**:

a) [...]

aa) monitorują i egzekwują ustanowione w art. 47a ust. 2 i 3 i w odpowiednich europejskich systemach certyfikacji cyberbezpieczeństwa obowiązki mających siedzibę na ich terytoriach wytwórców lub dostawców produktów lub usług ICT;

b) [...] **bez uszczerbku dla art. 51 ust. 1b wspierają krajowe jednostki akredytacyjne w monitorowaniu i nadzorowaniu** działalności jednostek oceniających zgodność do celów niniejszego rozporządzenia [...].

ba) monitorują i nadzorują działania podmiotów, o których mowa w art. 48 ust. 4;

bb) zezwalają na działalność jednostek oceniających zgodność, o których mowa w art. 51 ust. 1b, oraz ograniczają, zawieszają lub wycofują istniejące zezwolenia w przypadkach nieprzestrzegania wymogów niniejszego rozporządzenia;

c) rozpatrują skargi złożone przez osoby fizyczne lub prawne w związku z certyfikatami wydanymi przez [...] **krajowe organy ds, certyfikacji cyberbezpieczeństwa, lub, zgodnie z art. 48 ust 4a, przez jednostki oceniające zgodność**, badają w odpowiednim zakresie przedmiot skarg oraz informują skarżących w rozsądnym terminie o postępach i wynikach badania;

d) współpracują z innymi krajowymi organami [...] ds. certyfikacji **cyberbezpieczeństwa** lub innymi organami publicznymi, w tym poprzez wymianę informacji na temat ewentualnej niezgodności **procesów**, 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 [...] ds. certyfikacji **cyberbezpieczeństwa** posiada co najmniej następujące uprawnienia:

a) prawo żądania od jednostek oceniających zgodność**,**[...] posiadaczy europejskich certyfikatów cyberbezpieczeństwa oraz **podmiotów, które wydały unijne oświadczenie o zgodności** przekazania wszelkich informacji, których organ ten potrzebuje do wykonania swojego zadania;

b) prawo przeprowadzania dochodzeń, w trybie kontroli, w stosunku do jednostek oceniających zgodność**,** [...] posiadaczy europejskich certyfikatów cyberbezpieczeństwa i **podmiotów, które wydały unijne oświadczenie o zgodności**, 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**,** [...] posiadaczy certyfikatów i **podmiotów, które wydały unijne oświadczenie o zgodności**;

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 wycofania, zgodnie z prawem krajowym, certyfikatów – **wydanych przez krajowy organ ds. certyfikacji cyberbezpieczeństwa lub zgodnie z art. 48 ust. 4a przez jednostki oceniające zgodność** – które to certyfikaty 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 [...] ds. certyfikacji **cyberbezpieczeństwa** 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 **procesów**, 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.

1a. W przypadkach gdy europejski certyfikat cyberbezpieczeństwa wydawany jest przez krajowy organ ds. certyfikacji cyberbezpieczeństwa zgodnie z art. 48 ust. 4 lit. a) i art. 48 ust. 4a, jednostka certyfikująca krajowego organu ds. certyfikacji cyberbezpieczeństwa zostaje akredytowana jako jednostka oceniająca zgodność na podstawie ustępu 1 niniejszego artykułu.

1b. W stosownych przypadkach jednostki oceniające zgodność zostają upoważnione przez krajowy organ ds. certyfikacji cyberbezpieczeństwa do wykonywania jego obowiązków, jeśli spełniają szczególne lub dodatkowe wymogi określone w europejskim systemie certyfikacji cyberbezpieczeństwa na podstawie art. 47 ust. 1 lit. ca).

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 **podejmują w odpowiednim czasie wszelkie stosowne środki w celu ograniczenia, zawieszenia lub** cofnięcia akredytacji jednostki oceniającej zgodność udzielonej 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 [...] ds. certyfikacji **cyberbezpieczeństwa** notyfikują Komisji [...] jednostki oceniające zgodność akredytowane, a **w stosownych przypadkach upoważnione – na podstawie art. 51 ust. 1b,** do wydawania certyfikatów poświadczających określone poziomy uzasadnienia 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 [...] ds. certyfikacji **cyberbezpieczeństwa** może wystąpić do Komisji z wnioskiem o usunięcie jednostki oceniającej zgodność notyfikowanej przez dane państwo członkowskie z wykazu, o którym mowa w ust. 2 niniejszego artykułu. W ciągu miesiąca od daty otrzymania wniosku krajowego organu [...] ds. certyfikacji **cyberbezpieczeństwa** 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 **przedstawiciele** krajowych organów [...] ds. certyfikacji **cyberbezpieczeństwa lub przedstawiciele innych odpowiednich organów krajowych**. [...] **Każdy członek Grupy może reprezentować nie więcej niż jedno inne państwo członkowskie**.

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;

ba) przyjmowanie opinii na temat kandydującego systemu zgodnie z art. 44 niniejszego rozporządzenia;

c) [...] **zwracanie się** do Agencji o przygotowanie kandydującego europejskiego systemu certyfikacji cyberbezpieczeństwa zgodnie z art. 44 niniejszego rozporządzenia;

ca) opracowywanie i przyjmowanie wytycznych na temat kryteriów oceny wniosków w sprawie przygotowania kandydującego systemu, przedłożonych [...] Grupie zgodnie z art. 44 ust. 1a.

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 [...] ds. certyfikacji **cyberbezpieczeństwa** na mocy przepisów niniejszego tytułu poprzez **budowanie zdolności**, wymianę informacji, a w szczególności poprzez ustanowienie metod efektywnej wymiany informacji związanych z wszystkimi kwestiami dotyczącymi certyfikacji cyberbezpieczeństwa;

fa) dostarczanie wsparcia w zakresie wdrażania mechanizmu wzajemnej oceny zgodnie z zasadami ustanowionymi w danym europejskim systemie certyfikacji cyberbezpieczeństwa na postawie art. 47 ust. 1 lit. md).

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

Artykuł 53a

Prawo do wnoszenia skarg do krajowego organu [...] ds. certyfikacji cyberbezpieczeństwa

1. Osoby fizyczne lub prawne mają prawo do wnoszenia skarg do krajowego organu ds. certyfikacji cyberbezpieczeństwa w odniesieniu do certyfikatów wydanych przez ten organ, lub – zgodnie z art. 48 ust 4a – przez jednostki oceniające zgodność.

2. Krajowy organ ds. certyfikacji cyberbezpieczeństwa, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania ze środka zaskarżenia na mocy art. 53b.

Artykuł 53b

Prawo do skutecznego środka zaskarżenia

1. Osoby fizyczne lub prawne mają prawo do skutecznego środka zaskarżenia odnośnie do dotyczącej ich prawnie wiążącej decyzji krajowego organu ds. certyfikacji cyberbezpieczeństwa.

2. Osoby fizyczne lub prawne mają prawo do skutecznego środka zaskarżenia, w przypadku gdy krajowy organ ds. certyfikacji cyberbezpieczeństwa nie rozpatrzy skargi.

3. Postępowanie przeciwko krajowemu organowi ds. certyfikacji cyberbezpieczeństwa wszczyna się przed sądem państwa członkowskiego, w którym ma siedzibę ten organ.

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 **ust. 4 lit. b)** 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*.

1a. Niniejsze rozporządzenie stosuje się od dnia [...], z wyjątkiem art. 50, 51, 52, 53a, 53b i 54, które stosuje się od dnia [24 miesiące od daty publikacji 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*

ZAŁĄCZNIK

WYMAGANIA, KTÓRE MUSZĄ BYĆ SPEŁNIONE PRZEZ JEDNOSTKI OCENIAJĄCE ZGODNOŚĆ

Jednostki oceniające zgodność, które chcą być akredytowane, muszą spełniać następujące wymagania:

1. Jednostka oceniająca zgodność musi być powołana na podstawie prawa krajowego i posiadać osobowość prawną.

2. Jednostka oceniająca zgodność musi być stroną trzecią, niezależną od organizacji lub produktów bądź usług ICT, które ocenia.

3. Jednostkę należącą do organizacji przedsiębiorców lub zrzeszenia zawodowego, reprezentującego przedsiębiorstwa zaangażowane w projektowanie, produkcję, dostarczanie, montowanie, użytkowanie lub utrzymywanie ocenianych produktów bądź usług ICT, można uważać za jednostkę oceniającą zgodność, pod warunkiem że wykazano jej niezależność i brak konfliktu interesów.

4. Jednostka oceniająca zgodność, jej ścisłe kierownictwo oraz pracownicy odpowiedzialni za realizację zadań związanych z oceną zgodności nie mogą być projektantami, producentami, dostawcami, instalatorami, nabywcami, właścicielami, użytkownikami ani osobami odpowiedzialnymi za utrzymanie produktów bądź usług ICT, które są przedmiotem oceny, ani upoważnionymi przedstawicielami żadnej z wymienionych stron. Nie wyklucza to wykorzystywania ocenianych produktów, które są niezbędne do prowadzenia działalności jednostki oceniającej zgodność, lub wykorzystywania tych produktów do celów osobistych.

5. Jednostka oceniająca zgodność, jej ścisłe kierownictwo oraz pracownicy odpowiedzialni za wykonywanie zadań związanych z oceną zgodności nie mogą być bezpośrednio zaangażowani w projektowanie, wytwarzanie ani konstruowanie, wprowadzanie do obrotu, instalację lub użytkowanie ani być osobami odpowiedzialnymi za utrzymanie tych produktów bądź usług ICT, ani też reprezentować stron zaangażowanych w taką działalność. Nie mogą oni angażować się w żadną działalność, która może zagrozić niezależności ich osądów lub uczciwości w związku z działalnością w zakresie oceny zgodności, której dotyczy notyfikacja. Dotyczy to w szczególności usług konsultingowych.

6. Jednostki oceniające zgodność zapewniają, aby działalność ich jednostek zależnych lub podwykonawców nie wpływała na poufność, obiektywizm lub bezstronność działalności związanej z oceną zgodności.

7. Jednostki oceniające zgodność i ich pracownicy spełniają w toku realizacji zadań związanych z oceną zgodności najwyższe standardy zawodowe, posiadają konieczne kwalifikacje techniczne w danej dziedzinie oraz nie są poddawani żadnym naciskom ani zachętom, w tym także finansowym, mogącym wpływać na ich opinię lub wyniki oceny zgodności, szczególnie ze strony osób lub grup osób, których interesy związane są z rezultatami tych działań.

8. Jednostka oceniająca zgodność musi być w stanie wykonywać wszelkie zadania dotyczące oceny zgodności wyznaczone jej na podstawie niniejszego rozporządzeniu, bez względu na to, czy zadania te wykonuje sama jednostka oceniająca zgodność, czy też są one wykonywane w jej imieniu i na jej odpowiedzialność.

9. Przez cały czas i w odniesieniu do każdej procedury oceny zgodności oraz każdego rodzaju, każdej kategorii lub podkategorii produktów bądź usług ICT jednostka oceniająca zgodność musi dysponować niezbędnymi:

a) pracownikami posiadającymi wiedzę techniczną oraz wystarczające i odpowiednie doświadczenie do realizacji zadań związanych z oceną zgodności;

b) opisami procedur, zgodnie z którymi przeprowadza się ocenę zgodności, zapewniającymi przejrzystość tych procedur i możliwość ich powtarzania. Jednostka prowadzi odpowiednią politykę i posiada stosowne procedury, dzięki którym możliwe jest odróżnienie zadań wykonywanych w charakterze jednostki notyfikowanej od innej działalności;

c) procedurami służącymi prowadzeniu działalności przy należytym uwzględnieniu wielkości przedsiębiorstwa, sektora, w którym ono działa, struktury przedsiębiorstwa, stopnia złożoności technologii danego produktu lub danej usługi ICT oraz masowego lub seryjnego charakteru procesu produkcyjnego.

10. Jednostka oceniająca zgodność posiada środki niezbędne do prawidłowej realizacji czynności o charakterze technicznym i administracyjnym z zakresu oceny zgodności oraz ma dostęp do wszelkiego niezbędnego wyposażenia i obiektów.

11. Pracownicy odpowiedzialni za realizację zadań związanych z oceną zgodności posiadają:

a) solidne kwalifikacje techniczne i zawodowe, obejmujące wszystkie czynności w ramach oceny zgodności;

b) wystarczającą znajomość wymagań dotyczących ocen, które przeprowadzają, oraz odpowiednie uprawnienia do przeprowadzania takich ocen;

c) stosowną wiedzę i zrozumienie mających zastosowanie wymogów i norm badania;

d) umiejętności wymagane do sporządzania certyfikatów, zapisów i sprawozdań dokumentujących przeprowadzenie ocen.

12. Należy zagwarantować bezstronność jednostek oceniających zgodność, ich ścisłego kierownictwa i pracowników wykonujących ocenę.

13. Wynagrodzenie ścisłego kierownictwa jednostki oceniającej zgodność oraz jej pracowników wykonujących ocenę nie może zależeć od liczby przeprowadzonych ocen ani od wyników tych ocen.

14. Jednostki oceniające zgodność muszą posiadać ubezpieczenie od odpowiedzialności, chyba że na mocy prawa krajowego odpowiedzialność spoczywa na państwie lub za ocenę zgodności odpowiada bezpośrednio samo państwo członkowskie.

15. Pracownicy jednostki oceniającej zgodność dochowują tajemnicy służbowej w odniesieniu do wszystkich informacji, które uzyskują w trakcie wykonywania swoich zadań zgodnie z niniejszym rozporządzeniem lub z wszelkimi przepisami prawa krajowego nadającymi mu skuteczność, są jednak zwolnieni z tego obowiązku w stosunku do właściwych organów państwa członkowskiego, w którym realizowane są zadania.

16. Jednostki oceniające zgodność spełniają wymogi **odpowiedniej** normy, **zharmonizowanej na podstawie rozporządzenia (WE) 765/2008, w zakresie akredytacji jednostek oceniających zgodność dokonujących certyfikacji procesów, produktów lub usług [...].**

17. Jednostki oceniające zgodność zapewniają, aby laboratoria badawcze wykorzystywane do celów oceny zgodności spełniały wymogi **odpowiedniej normy**, **zharmonizowanej na podstawie rozporządzenia (WE) 765/2008, w zakresie akredytacji laboratoriów przeprowadzających badania** [...].