ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/881

z dnia 17 kwietnia 2019 r.

w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([1]),

uwzględniając opinię Komitetu Regionów ([2]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([3]),

a także mając na uwadze, co następuje:

(1) Sieci i systemy informatyczne oraz sieci i usługi łączności elektronicznej odgrywają kluczową rolę w społeczeństwie i stały się podstawą wzrostu gospodarczego. Technologie informacyjno-komunikacyjne (ICT) stanowią podstawę złożonych systemów wspierających codzienne 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, organizacje i przedsiębiorstwa w całej Unii jest obecnie bardzo rozpowszechnione. Cyfryzacja i sieć połączeń stają się podstawowymi cechami coraz większej liczby produktów i usług, a wraz z nastaniem internetu rzeczy w następnym dziesięcioleciu spodziewana jest instalacja wyjątkowo dużej liczby połączonych urządzeń cyfrowych w całej Unii. Coraz więcej urządzeń jest połączonych z internetem, jednak w ich projektowaniu w niewystarczającym stopniu uwzględnia się zabezpieczenia i odporność, co prowadzi do nieefektywnego cyberbezpieczeństwa. W tym kontekście ograniczone stosowanie certyfikacji prowadzi do niewystarczającej wiedzy użytkowników indywidualnych, instytucjonalnych i użytkowników biznesowych o właściwościach produktów ICT, usług ICT i procesów ICT w zakresie cyberbezpieczeństwa, co podważa zaufanie do rozwiązań cyfrowych. Sieci i systemy informatyczne mają możliwość wspierania wszystkich aspektów naszego życia i napędzania wzrostu gospodarczego w Unii. Stanowią one podstawowy element potrzebny do osiągnięcia jednolitego rynku cyfrowego.

(3) Rosnąca cyfryzacja i sieć połączeń zwiększają ryzyka w cyberprzestrzeni, zwiększając tym samym podatność ogółu społeczeństwa na cyberzagrożenia i potęgując niebezpieczeństwo dla osób, w tym osób bardziej na nie podatnych, takich jak dzieci. W celu ograniczenia tych ryzyk należy podjąć wszystkie niezbędne działania na rzecz poprawy cyberbezpieczeństwa w Unii, aby lepiej chronić przed cyberzagrożeniami sieci i systemy informatyczne, sieci łączności oraz produkty, usługi i urządzenia cyfrowe używane przez obywateli, organizacje i przedsiębiorstwa – od małych i średnich przedsiębiorstw (MŚP), zgodnie z definicją zawartą w zaleceniu Komisji 2003/361/WE ([4]), aż po operatorów infrastruktury krytycznej.

([1]) Dz.U. C 227 z 28.6.2018, s. 86.
([2]) Dz.U. C 176 z 23.5.2018, s. 29.
([3]) Stanowisko Parlamentu Europejskiego z dnia 12 marca 2019 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 9 kwietnia 2019 r.
([4]) Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

(4) Udostępniając odpowiednie informacje ogółowi społeczeństwa, Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), ustanowiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 526/2013 (UE) ([5]), przyczynia się do rozwijania sektora cyberbezpieczeństwa w Unii, zwłaszcza MŚP i przedsiębiorstw typu start-up. ENISA powinna dążyć do ściślejszej współpracy z uniwersytetami i ośrodkami badawczymi, by przyczyniać się do zmniejszenia zależności od produktów i usług z dziedziny cyberbezpieczeństwa spoza terytorium Unii i do wzmocnienia łańcuchów dostaw wewnątrz Unii.

(5) Cyberataki nasilają się, a połączona gospodarka i społeczeństwo, które jest bardziej podatne na cyberzagrożenia i ataki, wymagają silniejszej ochrony. Tymczasem jednak, mimo że cyberataki mają często charakter transgraniczny, kompetencje i reakcje polityczne organów odpowiedzialnych za cyberbezpieczeństwo i organów ścigania mają w głównej mierze charakter krajowy. Incydenty na dużą skalę mogą zakłócać świadczenie usług kluczowych w całej Unii. Taka sytuacja wymaga skutecznego i skoordynowanego reagowania oraz zarządzania kryzysowego na poziomie unijnym, 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, jak również systematyczne prognozowanie przyszłych zmian, wyzwań i zagrożeń na poziomie unijnym i ogólnoświatowym mają duże znaczenie dla decydentów politycznych, przemysłu oraz użytkowników.

(6) 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 obejmują dodatkowe zwiększenie potencjału i gotowości do reagowania państw członkowskich i przedsiębiorstw oraz poprawę współpracy, wymiany informacji i koordynacji pomiędzy państwami członkowskimi oraz instytucjami, organami i jednostkami organizacyjnymi Unii. Ponadto z uwagi na ponadgraniczny charakter cyberzagrożeń konieczne jest zwiększenie na poziomie Unii tych zdolności, które mogłyby uzupełniać działania państw członkowskich, zwłaszcza w przypadkach transgranicznych incydentów i kryzysów na dużą skalę, biorąc pod uwagę znaczenie utrzymania i dalszego ulepszania krajowych zdolności do reagowania na cyberzagrożenia niezależnie od ich skali.

(7) Potrzebne są również dodatkowe wysiłki na rzecz podnoszenia wiedzy obywateli, organizacji i przedsiębiorstw na temat cyberbezpieczeństwa. Ponadto, z uwagi na fakt, że incydenty osłabiają zaufanie do dostawców usług cyfrowych i do samego jednolitego rynku cyfrowego, zwłaszcza wśród konsumentów, zaufanie to należy zwiększać przez oferowanie w sposób przejrzysty informacji o poziomie bezpieczeństwa produktów ICT, usług ICT i procesów ICT, podkreślają że nawet wysoki poziom certyfikacji cyberbezpieczeństwa nie może zagwarantować, że produkt ICT, usługa ICT lub proces ICT jest całkowicie bezpieczny. Wzrost zaufania może ułatwiać certyfikacja na poziomie unijnym, ustanawiająca wspólne wymogi cyberbezpieczeństwa i kryteria oceny na wszystkich krajowych rynkach i we wszystkich sektorach krajowych.

(8) Cyberbezpieczeństwo to nie tylko kwestia związana z technologią, ale kwestia, w przypadku której równie ważne są ludzkie zachowania. Dlatego też należy usilnie propagować „cyberhigienę", czyli proste, rutynowe czynności, których wdrożenie i regularne wykonywanie przez obywateli, organizacje i przedsiębiorstwa minimalizuje ich narażenie na ryzyka związane z cyberzagrożeniami.

(9) W celu wzmocnienia unijnych struktur cyberbezpieczeństwa, ważne jest by utrzymywać i rozwijać zdolności państw członkowskich do kompleksowego reagowania na cyberzagrożenia, w tym na incydenty transgraniczne.

(10) Przedsiębiorstwa oraz indywidualni konsumenci powinni posiadać dokładne informacje dotyczące poziomu uzasadnienia zaufania, na jakim certyfikowane zostało bezpieczeństwo ich produktów ICT, usług ICT i procesów ICT. Jednocześnie żaden produkt ICT ani usługa ICT nie jest całkowicie bezpieczny, a podstawowe zasady cyberhigieny muszą być propagowane i traktowane priorytetowo. Mając na uwadze rosnącą dostępność urządzeń z kategorii internetu rzeczy, istnieje szereg dobrowolnych środków, które sektor prywatny może podejmować, by wzmacniać zaufanie do bezpieczeństwa produktów ICT, usług ICT i procesów ICT.

(11) Współczesne produkty i systemy ICT często korzystają ze stworzonych przez strony trzecie technologii i komponentów lub funkcjonują w oparciu o nie; są to na przykład moduły oprogramowania, biblioteki lub interfejsy programowania aplikacji. Wykorzystywanie tych elementów, określane mianem „zależności", może stwarzać dodatkowe ryzyka w cyberprzestrzeni, ponieważ podatności zidentyfikowane w komponentach pochodzących od stron trzecich mogą również wpływać na bezpieczeństwo produktów ICT, usług ICT i procesów ICT. W wielu przypadkach identyfikowanie i dokumentowanie tych zależności pozwala użytkownikom końcowym produktów ICT, usług ICT i procesów ICT usprawnić ich działania w zakresie zarządzania ryzykiem w cyberprzestrzeni, na przykład poprzez poprawę stosowanych przez użytkowników procedur zarządzania i procedur zaradczych w przypadku podatności wpływających na cyberbezpieczeństwo.

([5]) 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).

(12) Organizacje, wytwórców lub dostawców uczestniczących w projektowaniu i rozwijaniu produktów ICT, usług ICT lub procesów ICT należy zachęcać do stosowania środków na najwcześniejszych etapach projektowania i rozwijania w celu ochrony bezpieczeństwa tych produktów, usług i procesów w możliwie najwyższym stopniu, zakładając wystąpienie cyberataków, przygotowując się na ich skutki i minimalizując je („uwzględnianie bezpieczeństwa na etapie projektowania"). Bezpieczeństwo powinno być zapewnione w całym cyklu życia produktu ICT, usługi ICT lub procesu ICT poprzez takie procesy projektowania i rozwijania, które nieustannie ewoluują, by ograniczać ryzyko szkody w przypadku ich złośliwego wykorzystywania.

(13) Przedsiębiorstwa, organizacje i sektor publiczny powinny tak konfigurować projektowane przez siebie produkty ICT, usługi ICT i procesy ICT, by zapewniać wyższy poziom bezpieczeństwa, który powinien umożliwić pierwszemu użytkownikowi otrzymanie domyślnej konfiguracji o najwyższym możliwym poziomie ustawień bezpieczeństwa („bezpieczeństwo domyślne"), zmniejszającej tym samym obciążenie użytkowników w zakresie konieczności odpowiedniej konfiguracji produktu ICT, usługi ICT lub procesu ICT. Bezpieczeństwo domyślne nie powinno wymagać od użytkownika dokonywania zaawansowanej konfiguracji, ani specjalistycznej wiedzy technicznej czy nieintuicyjnego postępowania; powinno działać prosto i poprawnie, tam gdzie zostało wdrożone. Jeżeli, w poszczególnych przypadkach, analiza ryzyka i użyteczności wykaże, że domyślne wprowadzenie tego typu ustawień nie jest możliwe, użytkownikom należy sugerować wybór najbezpieczniejszych ustawień.

(14) Rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 460/2004 ([6]) ustanowiono ENISA, aby przyczynić się do realizacji celów w zakresie zapewnienia wysokiego i efektywnego poziomu bezpieczeństwa sieci i informacji w Unii oraz rozwijania kultury bezpieczeństwa sieci i informacji na rzecz obywateli, konsumentów, przedsiębiorstw oraz administracji publicznej. Rozporządzeniem (WE) nr 1007/2008 Parlamentu Europejskiego i Rady ([7]) przedłużono mandat ENISA do marca 2012 r. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 580/2011 ([8]) dodatkowo przedłużono mandat ENISA do dnia 13 września 2013 r. Rozporządzeniem (UE) nr 526/2013 przedłużono mandat ENISA do dnia 19 czerwca 2020 r.

(15) Unia podjęła już istotne kroki w celu zapewnienia cyberbezpieczeństwa i zwiększenia zaufania do technologii cyfrowych. W roku 2013 przyjęto strategię Unii Europejskiej w zakresie cyberbezpieczeństwa, która wskazuje reakcję polityczną Unii na cyberzagrożenia i ryzyka w cyberprzestrzeni. W ramach starań, aby lepiej chronić obywateli w internecie, w 2016 r. przyjęty został pierwszy akt ustawodawczy Unii w dziedzinie cyberbezpieczeństwa w formie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 ([9]).W dyrektywie (UE) 2016/1148 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 istotnych dla gospodarki i społeczeństwa sektorach, takich jak energetyka, transport, zaopatrzenie w wodę pitną i jej dystrybucja, bankowość, infrastruktura rynków finansowych, opieka zdrowotna, infrastruktura cyfrowa, jak też w odniesieniu do dostawców kluczowych usług cyfrowych (wyszukiwarek, usług przetwarzania w chmurze i targu internetowego).

Kluczową rolę we wspieraniu wdrażania tej dyrektywy wyznaczono agencji ENISA. Skuteczna walka z cyberprzestępczością stanowi ponadto jeden z ważnych priorytetów Europejskiej agendy bezpieczeństwa, przyczyniając się tym samym do realizacji ogólnego celu, jakim jest osiągnięcie wysokiego poziomu cyberbezpieczeństwa. Inne akty prawne, takie jak rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([10]) i dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE ([11]) i (UE) 2018/1972 ([12]), również przyczyniają się do wysokiego poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym.

([6]) 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).

([7]) 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).

([8]) 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).

([9]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

([10]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

([11]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

([12]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz.U. L 321 z 17.12.2018, s. 36).

(16) Od czasu przyjęcia strategii Unii Europejskiej w zakresie cyberbezpieczeństwa w 2013 r. oraz ostatniej zmiany mandatu ENISA znacznie zmienił się ogólny kontekst polityczny, ponieważ otoczenie globalne stało się bardziej niepewne i mniej bezpieczne. W tych warunkach i w kontekście pozytywnego rozwoju roli ENISA jako punktu odniesienia w zakresie doradztwa i wiedzy fachowej oraz jako podmiotu ułatwiającego współpracę i budowane zdolności, a także w ramach nowej unijnej polityki w zakresie cyberbezpieczeństwa konieczne jest dokonanie przeglądu mandatu ENISA, aby określić jej rolę w zmienionym ekosystemie cyberbezpieczeństwa i zapewnić jej skuteczny wkład w reakcję Unii na wyzwania w dziedzinie cyberbezpieczeństwa wynikające z radykalnie zmienionego profilu cyberzagrożeń, w odniesieniu do którego, jak uznano w ocenie, której poddano ENISA, obecny mandat nie jest wystarczający.

(17) ENISA ustanowiona niniejszym rozporządzeniem powinna być następcą ENISA ustanowionej rozporządzeniem (UE) nr 526/2013. ENISA powinna wykonywać zadania powierzone jej na mocy niniejszego rozporządzenia oraz innych 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 pomiędzy państwami członkowskimi i interesariuszami z sektora prywatnego, przedstawiać Komisji i państwom członkowskim sugestie dotyczące polityki, działać jako punkt odniesienia dla unijnych sektorowych inicjatyw odnoszących się do kwestii cyberbezpieczeństwa oraz wspierać współpracę operacyjną zarówno pomiędzy państwami członkowskimi, jak i pomiędzy państwami członkowskimi a instytucjami, organami i jednostkami organizacyjnymi Unii.

(18) W decyzji 2004/97/WE, Euratom przyjętej za wspólnym porozumieniem między przedstawicielami państw członkowskich podczas spotkania na szczeblu szefów państw lub rządów ([13]) przedstawiciele państw członkowskich zdecydowali, że ENISA będzie miała siedzibę w Grecji, w mieście, które wskaże rząd grecki. Państwo członkowskie przyjmujące ENISA powinno zapewnić możliwie najlepsze warunki dla sprawnego i skutecznego działania ENISA. Właściwa lokalizacja ENISA ma zasadnicze znaczenie dla prawidłowego i skutecznego wykonywania przez ENISA zadań, a także naboru i zatrzymania członków personelu oraz zwiększenia efektywności sieci współpracy, zapewniając między innymi odpowiednie połączenia transportowe i infrastrukturę dla małżonków i dzieci towarzyszących pracownikom ENISA. Umowa pomiędzy ENISA a przyjmującym państwem członkowskim, zawarta po uzyskaniu zgody Zarządu ENISA, powinna zawierać niezbędne uzgodnienia w tym zakresie.

(19) Ze względu na narastające ryzyka w cyberprzestrzeni i wyzwania w zakresie cyberbezpieczeństwa, z jakimi boryka się Unia, należy zwiększyć przydzielone ENISA zasoby finansowe i ludzkie, aby odzwierciedlić jej rozszerzoną rolę i zadania oraz jej kluczową pozycję w ekosystemie organizacji chroniących unijny ekosystem cyfrowy, pozwalając ENISA na skuteczne wykonywanie zadań powierzonych jej w niniejszym rozporządzeniu.

(20) ENISA powinna rozwijać i utrzymywać wysoki poziom wiedzy fachowej oraz pełnić rolę punktu odniesienia służącego budowie zaufania i wiarygodności na jednolitym rynku z racji swojej niezależności, jakości oferowanego doradztwa, jakości rozpowszechnianych informacji, przejrzystości jej procedur, przejrzystości jej metod działania, a także staranności w realizacji swoich zadań. ENISA powinna aktywnie wspierać działania krajowe i powinna proaktywnie włączać się w działania unijne, a jednocześnie wykonywać swoje zadania w pełnej współpracy z instytucjami, organami i jednostkami organizacyjnymi Unii oraz z państwami członkowskimi, unikając powielania działań i propagując synergie. Ponadto ENISA powinna bazować na wkładzie i współpracy ze strony sektora prywatnego, jak również innych odpowiednich interesariuszy. Zakres zadań powinien określać sposób, w jaki ENISA ma osiągnąć swoje cele, pozwalając jej jednocześnie na elastyczne działanie.

(21) Aby móc zapewnić odpowiednie wsparcie na rzecz współpracy operacyjnej pomiędzy państwami członkowskimi, ENISA powinna dodatkowo wzmocnić swoje zdolności techniczne i zdolności w zakresie zasobów ludzkich oraz umiejętności. Agencja powinna zwiększać swoje know-how i zdolności. ENISA i państwa członkowskie mogłyby na zasadzie dobrowolności tworzyć programy oddelegowywania ekspertów krajowych do ENISA, tworzenia baz ekspertów i wymiany członków personelu.

(22) ENISA powinna wspomagać Komisję poprzez doradztwo, opinie i analizy w odniesieniu do wszystkich kwestii unijnych związanych z opracowywaniem, aktualizacjami i przeglądami polityki i prawa w dziedzinie cyberbezpieczeństwa, a także kwestii sektorowych w celu zwiększenia roli unijnych polityk i przepisów dotyczących cyberbezpieczeństwa i umożliwienia spójności we wdrażaniu tych polityk i przepisów na poziomie krajowym. ENISA powinna pełnić rolę punktu odniesienia w zakresie doradztwa i wiedzy fachowej na rzecz unijnych sektorowych inicjatyw w dziedzinie polityki i prawa, dotyczących kwestii związanych z cyberbezpieczeństwem. ENISA powinna regularnie informować Parlament Europejski o swoich działaniach.

([13]) Decyzja 2004/97/WE, Euratom przyjęta za wspólnym porozumieniem między przedstawicielami państw członkowskich podczas spotkania na szczeblu szefów państw lub rządów, z dnia 13 grudnia 2003 r. w sprawie lokalizacji siedzib niektórych urzędów i agencji Unii Europejskiej (Dz.U. L 29 z 3.2.2004, s. 15).

(23) Publiczny rdzeń otwartego internetu, a mianowicie jego główne protokoły i infrastruktura będące dobrem publicznym, zapewniają zasadniczą funkcjonalność internetu jako całości i stanowią podstawę jego normalnego funkcjonowania. ENISA powinna wspierać bezpieczeństwo publicznego rdzenia otwartego internetu i stabilność jego funkcjonowania, w tym m.in. kluczowe protokoły (zwłaszcza DNS, BGP i IPv6), funkcjonowanie systemu nazw domen (jak funkcjonowanie wszystkich domen najwyższego poziomu) i funkcjonowanie strefy rdzennej.

(24) Podstawowym zadaniem ENISA jest wspieranie spójnego wprowadzania odpowiednich ram prawnych, a w szczególności skutecznego wdrożenia dyrektywy (UE) 2016/1148 i innych stosownych instrumentów prawnych zawierających aspekty dotyczące cyberbezpieczeństwa, co ma kluczowe znaczenie dla zwiększenia cyberodporności. W obliczu szybko ewoluującego profilu cyberzagrożeń jasne jest, że państwa członkowskie muszą mieć wsparcie w postaci bardziej kompleksowego, przekrojowego pod względem politycznym podejścia do budowania cyberodporności.

(25) ENISA powinna wspierać państwa członkowskie oraz instytucje organy i jednostki organizacyjne Unii w ich staraniach na rzecz budowy i umocnienia zdolności i gotowości do zapobiegania cyberzagrożeniom i incydentom, wykrywania ich i reagowania na nie oraz w odniesieniu do bezpieczeństwa sieci i systemów informatycznych. ENISA powinna w szczególności wspierać rozwój i wzmocnienie krajowych i unijnych zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanych dalej „zespołami CSIRT") przewidzianych w dyrektywie (UE) 2016/1148 z myślą o osiągnięciu wysokiego wspólnego poziomu ich zaawansowania w Unii. Prowadzone przez ENISA działania związane ze zdolnościami operacyjnymi państw członkowskich powinny aktywnie wspierać działania podejmowane przez państwa członkowskie w celu wypełniania ich obowiązków wynikających z dyrektywy (UE) 2016/1148, a zatem nie powinny takich działań zastępować.

(26) ENISA powinna również pomagać w opracowaniu i aktualizacji strategii w zakresie bezpieczeństwa sieci i systemów informatycznych na poziomie Unii i – na wniosek – na poziomie państw członkowskich, w szczególności w odniesieniu do cyberbezpieczeństwa, oraz powinna propagować upowszechnianie takich strategii i monitorować postępy w ich realizacji. ENISA powinna również przyczyniać się do zaspokajania potrzeb w zakresie szkoleń i materiałów szkoleniowych, w tym potrzeb organów publicznych, oraz, w stosownych przypadkach, zaspokajać w znacznym stopniu potrzeby szkoleniowe instruktorów, w oparciu o ramy kompetencji cyfrowych dla obywateli, mając na celu pomaganie państwom członkowskim oraz instytucjom, organom i jednostkom organizacyjnym Unii w rozwoju ich własnych zdolności szkoleniowych.

(27) ENISA powinna wspierać państwa członkowskie w dziedzinie podnoszenia wiedzy na temat cyberbezpieczeństwa i edukacji w tym zakresie poprzez ułatwianie ściślejszej koordynacji i wymiany najlepszych praktyk pomiędzy państwami członkowskimi. Takie wsparcie mogłoby polegać na rozwoju sieci krajowych punktów kontaktowych ds. edukacji i na rozwoju platformy szkoleniowej w zakresie cyberbezpieczeństwa. Sieć krajowych punktów kontaktowych ds. edukacji mogłaby funkcjonować w ramach Sieci Krajowych Urzędników Łącznikowych i stanowić punkt wyjścia do przyszłej koordynacji działań pomiędzy państwami członkowskimi.

(28) ENISA powinna wspierać grupę współpracy utworzoną dyrektywą (UE) 2016/1148 w wykonywaniu jej zadań, w szczególności poprzez zapewnianie wiedzy fachowej i doradztwa oraz ułatwianie wymiany najlepszych praktyk, między innymi w odniesieniu do identyfikowania przez państwa członkowskie operatorów usług kluczowych, a także w odniesieniu do transgranicznych zależności, pod względem ryzyk i incydentów.

(29) Z myślą o pobudzaniu współpracy pomiędzy sektorem publicznym a prywatnym oraz w ramach sektora prywatnego, szczególnie w celu wspierania ochrony infrastruktury krytycznej, ENISA powinna wspierać wymianę informacji w ramach samych sektorów i pomiędzy sektorami, szczególnie w przypadku sektorów wymienionych w załączniku II do dyrektywy (UE) 2016/1148, poprzez zapewnianie najlepszych praktyk i porad w zakresie dostępnych narzędzi i procedur oraz porad na temat rozwiązywania kwestii regulacyjnych związanych z wymianą informacji, na przykład dzięki ułatwianiu ustanawiania sektorowych ośrodków wymiany i analizy informacji.

(30) Zważywszy na fakt, że stale rośnie potencjalny negatywny wpływ podatności w produktach ICT, usługach ICT i procesach ICT, identyfikowanie i eliminowanie tych podatności odgrywa ważną rolę w zmniejszaniu ogólnego ryzyka w cyberprzestrzeni. Dowiedziono, że współpraca pomiędzy organizacjami, wytwórcami lub dostawcami produktów ICT, usług ICT i procesów ICT, w których mogą występować podatności, a członkami społeczności badawczej w obszarze cyberbezpieczeństwa i rządami identyfikującymi podatności w istotny sposób zwiększa wskaźniki wykrywania i eliminowania podatności produktów ICT, usług ICT i procesów ICT. Skoordynowane ujawnianie podatności oznacza ustrukturyzowany proces współpracy, w ramach którego podatności zgłaszane są właścicielowi systemu informacyjnego, co pozwala organizacji na zdiagnozowanie i wyeliminowanie podatności zanim szczegółowe informacje dotyczące podatności zostaną ujawnione stronom trzecim lub podane do wiadomości publicznej. Proces ten przewiduje również koordynację działań pomiędzy identyfikującym podatności a daną organizacją w zakresie podania do wiadomości publicznej informacji o tych podatnościach. Polityki skoordynowanego ujawniania podatności mogą odgrywać ważną rolę w wysiłkach państw członkowskich na rzecz zwiększania cyberbezpieczeństwa.

(31) ENISA powinna gromadzić i analizować dobrowolnie udostępniane raporty krajowe przekazywane przez zespoły CSIRT i międzyinstytucjonalny zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach Unii ustanowiony porozumieniem między Parlamentem Europejskim, Radą Europejską, Radą Unii Europejskiej, Komisją Europejską, Trybunałem Sprawiedliwości Unii Europejskiej, Europejskim Bankiem Centralnym, Europejskim Trybunałem Obrachunkowym, Europejską Służbą Działań Zewnętrznych, Europejskim Komitetem Ekonomiczno-Społecznym, Europejskim Komitetem Regionów i Europejskim Bankiem Inwestycyjnym w sprawie organizacji i funkcjonowania zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE) ([14]), by przyczyniać się do ustanawiania wspólnych procedur, języka i terminologii do celów wymiany informacji. W tym kontekście ENISA powinna angażować sektor prywatny w ramach dyrektywy (UE) 2016/1148, w której określono podstawy dobrowolnej wymiany informacji technicznych na poziomie operacyjnym w ramach utworzonej tą dyrektywą sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanej dalej „siecią CSIRT").

(32) ENISA powinna wnosić wkład w reagowanie na poziomie Unii w przypadku transgranicznych incydentów i kryzysów na dużą skalę związanych z cyberbezpieczeństwem. Zadanie to powinno być wykonywane zgodnie z mandatem ENISA na podstawie niniejszego rozporządzenia i podejściem uzgodnionym przez państwa członkowskie w kontekście zalecenia Komisji (UE) 2017/1584 ([15]) i konkluzji Rady z dnia 26 czerwca 2018 r. w sprawie skoordynowanego reagowania na szczeblu unijnym na cyberincydenty i cyberkryzysy na dużą skalę. Zadanie to mogłoby obejmować gromadzenie odpowiednich informacji i działanie w charakterze pośrednika ułatwiającego współpracę sieci CSIRT i środowiska technicznego, jak również pomiędzy decydentami odpowiedzialnymi za zarządzanie kryzysowe. ENISA powinna ponadto wspierać współpracę operacyjną pomiędzy państwami członkowskimi, jeżeli zwróci się o to jedno państwo członkowskie lub większa ich liczba – w ramach postępowania – od strony technicznej – w przypadku incydentów, ułatwianie odpowiedniej wymiany rozwiązań technicznych pomiędzy państwami członkowskimi oraz oferowanie wkładu w komunikację społeczną. ENISA powinna wspierać współpracę operacyjną testując ustalenia dotyczące takiej współpracy poprzez przeprowadzanie regularnych ćwiczeń w dziedzinie cyberbezpieczeństwa.

(33) Wspierając współpracę operacyjną, ENISA powinna korzystać z dostępnej technicznej i operacyjnej wiedzy fachowej CERT-UE w ramach współpracy strukturalnej. Taka współpraca strukturalna mogłaby bazować na wiedzy fachowej ENISA. W stosownych przypadkach należy poczynić specjalne ustalenia pomiędzy oboma podmiotami, aby określić sposób praktycznej realizacji takiej współpracy i uniknąć powielania działań.

(34) Wykonując swoje zadania polegające na wspieraniu współpracy operacyjnej w ramach sieci CSIRT ENISA powinna być w stanie zapewniać wsparcie na wniosek państw członkowskich, na przykład oferując doradztwo dotyczące sposobów zwiększenia ich zdolności w zakresie zapobiegania incydentom, ich wykrywania oraz reagowania na nie, ułatwiając techniczne postępowanie w przypadku incydentów mających istotny wpływ lub zapewniając analizę cyberzagrożeń i incydentów. ENISA powinna ułatwiać techniczne postępowanie w przypadku incydentów mających istotny wpływ, szczególnie poprzez wspieranie dobrowolnego dzielenia się rozwiązaniami technicznymi pomiędzy państwami członkowskimi lub opracowywanie zbiorczych informacji technicznych, na przykład na temat rozwiązań technicznych udostępnionych dobrowolnie przez państwa członkowskie. W zaleceniu (UE) 2017/1584 zaleca się, aby państwa członkowskie współpracowały w dobrej wierze i bez zbędnej zwłoki wymieniały pomiędzy sobą i z ENISA informacje o incydentach i kryzysach na dużą skalę związanych z cyberbezpieczeństwem. Takie informacje pomogłyby dodatkowo ENISA w wykonywaniu jej zadań polegających na wspieraniu współpracy operacyjnej.

(35) Jako element regularnej współpracy na poziomie technicznym służącej wzmocnieniu unijnej orientacji sytuacyjnej ENISA, w ścisłej współpracy z państwami członkowskimi, powinna przygotowywać regularny pogłębiony raport techniczny o stanie cyberbezpieczeństwa w UE dotyczący incydentów i cyberzagrożeń, oparty o publicznie dostępne informacje, własną analizę oraz sprawozdania przekazane przez zespoły CSIRT państw członkowskich lub krajowe pojedyncze punkty kontaktowe ds. bezpieczeństwa sieci i systemów informatycznych (zwane dalej „pojedynczymi punktami kontaktowymi") przewidziane w dyrektywie (UE) 2016/1148, w obu przypadkach przekazywane na zasadzie dobrowolności, przez Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu, CERT-UE oraz – w stosownych przypadkach – Centrum Analiz Wywiadowczych Unii Europejskiej (EU INTCEN) Europejskiej Służby Działań Zewnętrznych. Raport ten należy udostępniać Radzie, Komisji, Wysokiemu Przedstawicielowi Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa oraz sieci CSIRT.

(36) Wsparcie ENISA udzielane – na wniosek zainteresowanych państw członkowskich – w przypadku technicznych postępowań wyjaśniających *ex post* dotyczących incydentów mających istotny wpływ powinno koncentrować się na zapobieganiu przyszłym incydentom. Zainteresowane państwa członkowskie powinny dostarczyć niezbędnych informacji i pomocy, by umożliwić ENISA skuteczne wsparcie technicznego postępowania wyjaśniającego *ex post*.

([14]) Dz.U. C 12 z 13.1.2018, s. 1.

([15]) Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).

(37) Państwa członkowskie mogą zachęcać przedsiębiorstwa, których dotyczy dany incydent, do współpracy, polegającej na dostarczeniu ENISA niezbędnych informacji i pomocy, bez uszczerbku dla ich prawa do ochrony szczególnie chronionych informacji handlowych oraz informacji istotnych dla bezpieczeństwa publicznego.

(38) Aby lepiej rozumieć wyzwania w dziedzinie cyberbezpieczeństwa i z myślą o zapewnianiu strategicznego długoterminowego doradztwa państwom członkowskim oraz instytucjom, organom i jednostkom organizacyjnym Unii, konieczne jest, aby ENISA analizowała bieżące i pojawiające się ryzyka w cyberprzestrzeni. W tym celu ENISA powinna, we współpracy z państwami członkowskimi oraz – w stosownych przypadkach – z urzędami statystycznymi i innymi podmiotami, gromadzić odpowiednie dostępne publicznie 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. ENISA powinna ponadto – poprzez przeprowadzanie analiz cyberzagrożeń, podatności i incydentów – wspierać państwa członkowskie oraz instytucje, organy i jednostki organizacyjne Unii w identyfikowaniu pojawiających się ryzyk w cyberprzestrzeni i zapobieganiu incydentom.

(39) W celu wzmocnienia odporności Unii ENISA powinna rozwinąć wiedzę specjalistyczną w dziedzinie cyberbezpieczeństwa infrastruktur, w szczególności w celu wsparcia sektorów wymienionych w załączniku II do dyrektywy (UE) 2016/1148 oraz infrastruktur wykorzystywanych przez dostawców usług cyfrowych wymienionych w załączniku III do tej dyrektywy, zapewniając doradztwo, wydając wytyczne i wymieniając najlepsze praktyki. Z myślą o zapewnieniu łatwiejszego dostępu do bardziej usystematyzowanych informacji na temat ryzyk w cyberprzestrzeni i ewentualnych środków zaradczych ENISA powinna stworzyć i utrzymywać unijny „węzeł informacyjny" – portal stanowiący punkt kompleksowej obsługi zapewniający ogółowi społeczeństwa informacje na temat cyberbezpieczeństwa pochodzące od unijnych i krajowych instytucji, organów i jednostek organizacyjnych. Łatwiejszy dostęp do lepiej uporządkowanych informacji na temat ryzyk w cyberprzestrzeni i ewentualnych środków zaradczych mógłby również pomóc państwom członkowskim wzmocnić ich zdolności i dostosować ich praktyki, a zatem poprawić ich ogólną odporność na cyberataki.

(40) ENISA powinna działać na rzecz podnoszenia wiedzy ogółu społeczeństwa na temat ryzyk w cyberprzestrzeni – włączając w to ogólnounijną kampanię informacyjną poprzez propagowanie edukacji i zapewniać obywatelom, organizacjom i przedsiębiorstwom porady w zakresie dobrych praktyk dla użytkowników indywidualnych. ENISA powinna również przyczyniać się do propagowania najlepszych praktyk i rozwiązań, w tym w zakresie cyberhigieny i umiejętności cyfrowych, na poziomie i obywateli, organizacji i przedsiębiorstw poprzez gromadzenie i analizowanie publicznie dostępnych informacji dotyczących istotnych incydentów oraz poprzez sporządzanie i publikowanie raportów i porad dla obywateli, organizacji i przedsiębiorstw oraz poprawy ogólnego poziomu ich gotowości i odporności. ENISA powinna również dążyć do zapewnienia konsumentom odpowiednich informacji na temat obowiązujących programów certyfikacji, na przykład poprzez zapewnianie wytycznych i zaleceń. ENISA powinna ponadto organizować, zgodnie z Planem działania w dziedzinie edukacji cyfrowej ustanowionym w komunikacie Komisji z dnia 17 stycznia 2018 r. i we współpracy z państwami członkowskimi oraz instytucjami, organami i jednostkami organizacyjnymi Unii, regularne działania informacyjne i publiczne kampanie edukacyjne skierowane do użytkowników końcowych w celu propagowania bezpieczniejszych zachowań osób w internecie i umiejętności cyfrowych, podnoszenia wiedzy o potencjalnych cyberzagrożeniach, w tym o działalności przestępczej w internecie, takiej jak ataki phishingowe, botnety oraz oszustwa finansowe i bankowe, incydenty fałszerstwa danych, oraz w celu propagowania podstawowego doradztwa w kwestii wielopoziomowego uwierzytelniania, poprawek, szyfrowania, anonimizacji oraz ochrony danych.

(41) ENISA powinna odgrywać centralną rolę w podnoszeniu wiedzy użytkowników końcowych na temat bezpieczeństwa urządzeń i bezpiecznego korzystania z usług oraz powinna propagować uwzględnianie bezpieczeństwa i ochrony prywatności już na etapie projektowania na poziomie Unii. W tym celu ENISA powinna wykorzystać dostępne najlepsze praktyki i doświadczenie, szczególnie najlepsze praktyki i doświadczenie instytucji akademickich i ekspertów w obszarze bezpieczeństwa informatycznego.

(42) W celu wspierania przedsiębiorstw działających w sektorze cyberbezpieczeństwa, jak również użytkowników rozwiązań w zakresie cyberbezpieczeństwa, ENISA powinna stworzyć i utrzymywać „centrum monitorowania rynku" poprzez przeprowadzanie regularnych analiz i upowszechnianie informacji o głównych tendencjach na rynku cyberbezpieczeństwa, zarówno po stronie popytu, jak i podaży.

(43) ENISA powinna przyczyniać się do wysiłków Unii na rzecz współpracy z organizacjami międzynarodowymi oraz w ramach odpowiednich ram współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa. ENISA powinna w szczególności przyczyniać się, w stosownych przypadkach, do współpracy z takimi organizacjami jak OECD, OBWE i NATO. Współpraca taka mogłaby obejmować wspólne ćwiczenia w dziedzinie cyberbezpieczeństwa i wspólną koordynację reagowania na incydenty. Te działania odbywają się przy pełnym poszanowaniu zasad pluralizmu, wzajemności i autonomii decyzyjnej Unii, bez uszczerbku dla szczególnego charakteru polityki bezpieczeństwa i obrony poszczególnych państw członkowskich.

(44) Dla zapewnienia pełnej realizacji jej celów ENISA powinna współpracować z odpowiednimi organami nadzorczymi Unii i z innymi właściwymi organami w Unii, instytucjami, organami i jednostkami organizacyjnymi Unii, w tym z CERT-UE, EC3, Europejską Agencją Obrony (EDA), Europejskim Organem Nadzoru Globalnego Systemu Nawigacji Satelitarnej (Agencją Europejskiego GNSS), Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC), Europejską Agencją ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości (eu-LISA), Europejskim Bankiem Centralnym (EBC), Europejskim Urzędem Nadzoru Bankowego (EUNB), Europejską Radą Ochrony Danych, Agencją Unii Europejskiej ds. Współpracy Organów Regulacji Energetyki (ACER), Europejską Agencją Bezpieczeństwa Lotniczego (EASA) i każdą inną agencją Unii zaangażowaną w kwestie cyberbezpieczeństwa. ENISA powinna również współpracować z organami zajmującymi się ochroną danych, aby wymieniać know-how i najlepsze praktyki oraz powinna zapewniać doradztwo dotyczące tych kwestii cyberbezpieczeństwa, które mogą mieć wpływ na ich pracę. Przedstawiciele krajowych i unijnych organów ścigania oraz ochrony danych powinni być uprawnieni do udziału w Grupie Doradczej ENISA. Współpracując z organami ścigania w kwestiach z zakresu bezpieczeństwa sieci i informacji, które mogłyby mieć wpływ na ich pracę, ENISA powinna respektować istniejące kanały informacji i ustanowione sieci.

(45) Partnerstwo może być nawiązane z instytucjami akademickimi podejmującymi inicjatywy badawcze w odpowiednich dziedzinach, a także powinny istnieć odpowiednie kanały, dzięki którym informacje będą mogły przekazywać organizacje konsumenckie i inne organizacje, które powinny być uwzględniane.

(46) ENISA, w roli sekretariatu sieci CSIRT, powinna wspierać zespoły CSIRT państw członkowskich i CERT-UE we współpracy operacyjnej w związku ze wszystkimi odpowiednimi zadaniami sieci CSIRT, o których mowa w dyrektywie (UE) 2016/1148. ENISA powinna ponadto propagować i wspierać współpracę pomiędzy odpowiednimi zespołami CSIRT w przypadku incydentów, ataków lub zakłóceń dotyczących sieci lub infrastruktury zarządzanej lub chronionej przez zespoły CSIRT i angażujących lub mających możliwość angażowania co najmniej dwóch zespołów CSIRT, z należytym uwzględnieniem standardowych procedur operacyjnych sieci CSIRT.

(47) W celu zwiększenia gotowości Unii do reagowania na incydenty ENISA powinna organizować regularnie ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie unijnym oraz, na wniosek, wspierać państwa członkowskie oraz instytucje, organy i jednostki organizacyjne Unii przy organizacji takich ćwiczeń. Kompleksowe ćwiczenia na dużą skalę, obejmujące elementy techniczne, operacyjne lub strategiczne, powinny być organizowane raz na dwa lata. Ponadto ENISA powinna móc organizować regularnie ćwiczenia o mniej kompleksowym charakterze z myślą o realizacji tego samego celu, zwiększenia gotowości Unii do reagowania na incydenty.

(48) ENISA powinna dalej rozwijać i utrzymywać swoją wiedzę fachową w dziedzinie certyfikacji cyberbezpieczeństwa w celu wspierania polityki Unii w tej dziedzinie. ENISA powinna korzystać z istniejących najlepszych praktyk i powinna propagować wprowadzenie w Unii certyfikacji cyberbezpieczeństwa, w tym poprzez przyczynianie się do utworzenia i utrzymywania ram certyfikacji cyberbezpieczeństwa na poziomie unijnym (europejskich ram certyfikacji cyberbezpieczeństwa), z myślą o zwiększeniu przejrzystości w zakresie zaufania do cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT, zwiększając w ten sposób zaufanie do wewnętrznego rynku cyfrowego i jego konkurencyjność.

(49) Skuteczna polityka cyberbezpieczeństwa powinna opierać się na dobrze opracowanych metodach szacowania ryzyka, zarówno w sektorze publicznym, jak i prywatnym. Metody szacowania ryzyka są używane na różnych poziomach, bez wspólnej praktyki dotyczącej sposobu ich skutecznego stosowania. Propagowanie i rozwój najlepszych praktyk w zakresie szacowania ryzyka oraz interoperacyjnych rozwiązań w zakresie zarządzania ryzykiem w organizacjach sektora publicznego i sektora prywatnego zwiększy poziom cyberbezpieczeństwa w Unii. W tym celu ENISA powinna wspierać współpracę pomiędzy interesariuszami na poziomie Unii oraz ułatwiać im tworzenie i wprowadzanie europejskich i międzynarodowych norm dotyczących zarządzania ryzykiem oraz norm dotyczących mierzalnego bezpieczeństwa produktów, systemów, sieci i usług elektronicznych, które wraz z oprogramowaniem współtworzą sieci i systemy informatyczne.

(50) ENISA powinna zachęcać państwa członkowskie, wytwórców lub dostawców produktów ICT, usług ICT lub procesów ICT do podnoszenia ich ogólnych norm bezpieczeństwa, tak aby wszyscy użytkownicy internetu mogli podejmować kroki niezbędne do zapewnienia sobie własnego cyberbezpieczeństwa oraz powinna do tego zachęcać. Wytwórcy i dostawcy produktów ICT, usług ICT lub procesów ICT powinni w szczególności dostarczać wszelkie niezbędne aktualizacje i powinni wzywać do przekazania, wycofywać z obrotu lub przebudowywać produkty ICT, usługi ICT lub procesy ICT niespełniające norm cyberbezpieczeństwa, natomiast importerzy i dystrybutorzy powinni upewnić się, czy produkty ICT, usługi ICT i procesy ICT, które wprowadzają do obrotu w Unii, są zgodne z mającymi zastosowanie wymogami oraz czy nie stanowią ryzyka dla unijnych konsumentów.

(51) We współpracy z właściwymi organami ENISA powinna móc rozpowszechniać informacje dotyczące poziomu cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT oferowanych na rynku wewnętrznym oraz powinna wydawać ostrzeżenia skierowane do wytwórców i dostawców produktów ICT, usług ICT lub procesów ICT, żądając od nich poprawy bezpieczeństwa ich produktów ICT, usług ICT i procesów ICT, w tym cyberbezpieczeństwa.

(52) ENISA powinna w pełni uwzględniać bieżącą działalność w zakresie badań naukowych, rozwoju i oceny technologii, w szczególności działalność prowadzoną w ramach różnych unijnych inicjatyw badawczych, w celu doradzania instytucjom, organom i jednostkom organizacyjnym Unii, a także – w stosownych przypadkach i na ich wniosek – państwom członkowskim w kwestii potrzeb i priorytetów badawczych w dziedzinie cyberbezpieczeństwa. W celu określenia potrzeb i priorytetów badawczych ENISA powinna również prowadzić konsultacje z odpowiednimi grupami użytkowników. Konkretniej, mogłaby zostać nawiązana współpraca z Europejską Radą ds. Badań Naukowych, Europejskim Instytutem Innowacji i Technologii i z Instytutem Unii Europejskiej Studiów nad Bezpieczeństwem.

(53) W toku przygotowywania europejskich programów certyfikacji cyberbezpieczeństwa ENISA powinna przeprowadzać regularne konsultacje z organizacjami normalizacyjnymi, w szczególności z europejskimi organizacjami normalizacyjnymi.

(54) Cyberzagrożenia mają charakter globalny. Istnieje potrzeba zacieśnienia współpracy międzynarodowej w celu poprawy norm cyberbezpieczeństwa, w tym potrzeba zdefiniowania wspólnych norm zachowania, przyjęcia kodeksu postępowania, stosowania norm międzynarodowych i wymiany informacji, w celu propagowania sprawniejszej współpracy międzynarodowej w odpowiedzi na kwestie bezpieczeństwa sieci i informacji oraz propagowania wspólnego globalnego podejścia do tych kwestii. W tym celu ENISA powinna wspierać dalsze zaangażowanie Unii oraz współpracę z państwami trzecimi i organizacjami międzynarodowymi, udostępniając, w stosownych przypadkach, właściwym instytucjom, organom i jednostkom organizacyjnym Unii niezbędną wiedzę fachową i analizy.

(55) ENISA powinna być w stanie odpowiadać na wnioski *ad hoc* o doradztwo i pomoc ze strony państw członkowskich oraz instytucji, organów i jednostek organizacyjnych Unii w kwestiach wchodzących w zakres mandatu ENISA.

(56) Uznaje się za rozsądne i zalecane, by wdrożyć określone zasady dotyczące zarządzania ENISA, aby spełnić wymogi Wspólnego oświadczenia i Wspólnego podejścia, które zostały uzgodnione w ramach międzyinstytucjonalnej grupy roboczej ds. agencji zdecentralizowanych UE w lipcu 2012 r., a których celem jest usprawnienie działań agencji zdecentralizowanych i zwiększenie ich skuteczności. Zalecenia zawarte we Wspólnym oświadczeniu i Wspólnym podejściu powinny zostać również uwzględnione, odpowiednio, w programach prac ENISA, ocenach ENISA, a także w sprawozdawczości prowadzonej przez ENISA i jej praktyce administracyjnej.

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

(58) Aby ENISA mogła prawidłowo i skutecznie funkcjonować, Komisja i państwa członkowskie powinny zapewnić, aby osoby powoływane na członków Zarządu posiadały odpowiednią zawodową wiedzę fachową i doświadczenie. Komisja i państwa członkowskie powinny również dołożyć starań, aby ograniczyć rotację swoich przedstawicieli w Zarządzie, tak aby zapewnić ciągłość jego pracy.

(59) Sprawne funkcjonowanie ENISA 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. Obowiązki Dyrektora Wykonawczego powinny być wykonywane w sposób całkowicie niezależny. Dyrektor Wykonawczy powinien opracowywać propozycję rocznego programu prac ENISA, po uprzednim zasięgnięciu opinii Komisji, oraz powinien podejmować wszelkie czynności niezbędne do zapewnienia prawidłowego wykonania tego programu prac. Dyrektor Wykonawczy powinien przygotowywać przedkładane Zarządowi sprawozdanie roczne, obejmujące informacje na temat wykonania rocznego programu prac ENISA, sporządzać projekt preliminarza dochodów i wydatków ENISA oraz wykonywać budżet. Dyrektor Wykonawczy powinien mieć ponadto możliwość ustanawiania grup roboczych *ad hoc* w celu zajęcia się określonymi kwestiami, w szczególności kwestiami o charakterze naukowym, technicznym, prawnym lub społeczno-gospodarczym. Ustanowienie grupy roboczej *ad hoc* uznaje się za niezbędne zwłaszcza w przypadku przygotowań dotyczących konkretnej propozycji dotyczącej europejskiego programu certyfikacji cyberbezpieczeństwa (zwanej

dalej „propozycją programu"). Dyrektor Wykonawczy powinien zapewnić, aby członkowie grup roboczych *ad hoc* byli wybierani według najbardziej rygorystycznych kryteriów dotyczących wiedzy fachowej mając na celu zapewnienie równowagi płci i zrównoważonej reprezentacji – w zależności od specyfiki rozpatrywanych kwestii – przedstawicieli administracji publicznej państw członkowskich, instytucji, organów i jednostek organizacyjnych Unii oraz sektora prywatnego, w tym przemysłu, użytkowników oraz ekspertów akademickich w dziedzinie bezpieczeństwa sieci i informacji.

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

(61) ENISA powinna posiadać organ doradczy w postaci Grupy Doradczej ENISA w celu zapewnienia ciągłego dialogu z sektorem prywatnym, organizacjami konsumenckimi i innymi odpowiednimi interesariuszami. Grupa Doradcza ENISA, ustanowiona przez Zarząd na wniosek Dyrektora Wykonawczego, powinna skupiać się na kwestiach istotnych dla interesariuszy i powinna zwracać na nie uwagę ENISA. Grupa Doradcza ENISA powinna być konsultowana zwłaszcza w odniesieniu do projektu rocznego programu prac ENISA. Skład Grupy Doradczej ENISA oraz powierzone jej zadania powinny zapewniać wystarczającą reprezentację interesariuszy w pracach ENISA.

(62) W celu wsparcia ENISA i Komisji w ułatwianiu konsultacji z odpowiednimi interesariuszami należy ustanowić Grupę Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa. Grupa Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa powinna składać się z członków reprezentujących w zrównoważony sposób przemysł, zarówno po stronie popytu, jak i podaży produktów ICT i usług ICT, w tym szczególnie przedstawicieli MŚP, dostawców usług cyfrowych, europejskich i międzynarodowych organów normalizacyjnych, krajowych jednostek akredytujących, organów nadzorczych ds. ochrony danych i jednostek oceniających zgodność zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008 ([16]) oraz przedstawicieli środowiska akademickiego, a także organizacji konsumenckich.

(63) ENISA powinna posiadać przepisy dotyczące zapobiegania konfliktom interesów i zarządzania nimi. ENISA powinna również stosować odpowiednie przepisy unijne dotyczące publicznego dostępu do dokumentów zawarte w rozporządzeniu (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ([17]). Przetwarzanie danych osobowych przez ENISA powinno podlegać rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/1725 ([18]). ENISA powinna przestrzegać przepisów mających zastosowanie do instytucji, organów i jednostek organizacyjnych Unii oraz przepisów krajowych dotyczących postępowania z informacjami, zwłaszcza ze szczególnie chronionymi informacjami jawnymi i informacjami niejawnymi Unii Europejskiej (EUCI).

(64) W celu zagwarantowania pełnej autonomii i niezależności ENISA oraz umożliwienia jej wykonywania dodatkowych zadań, w tym również nieprzewidzianych zadań w sytuacjach nadzwyczajnych, należy przyznać ENISA wystarczający i niezależny budżet, którego dochody pochodziłyby przede wszystkim z wkładu Unii oraz z wkładów państw trzecich uczestniczących w pracach ENISA. Właściwy budżet ma zasadnicze znaczenie dla zapewnienia ENISA wystarczających zdolności do realizacji swoich wszystkich coraz liczniejszych zadań i do osiągnięcia swoich celów. Większość personelu ENISA powinna pracować bezpośrednio przy operacyjnym wykonywaniu mandatu ENISA. Przyjmujące państwo członkowskie oraz każde inne państwo członkowskie powinno mieć możliwość dobrowolnego wnoszenia wkładu na rzecz budżetu ENISA. Procedura budżetowa Unii powinna nadal mieć zastosowanie do wszelkich dotacji pochodzących z budżetu ogólnego Unii. Ponadto Trybunał Obrachunkowy powinien przeprowadzać kontrolę sprawozdań finansowych ENISA w celu zapewnienia przejrzystości i odpowiedzialności.

(65) Certyfikacja cyberbezpieczeństwa odgrywa ważną rolę, jeżeli chodzi o zwiększanie zaufania do produktów ICT, usług ICT i procesów ICT oraz ich bezpieczeństwa. Jednolity rynek cyfrowy, a w szczególności gospodarka oparta na danych i internet rzeczy, mogą się prawidłowo rozwijać jedynie w atmosferze ogólnego publicznego zaufania, że takie produkty, usługi i procesy zapewniają konkretny poziom cyberbezpieczeństwa. Połączone z siecią i zautomatyzowane pojazdy, elektroniczne wyroby medyczne, systemy sterowania automatyki przemysłowej oraz inteligentne sieci stanowią tylko niektóre przykłady sektorów, w których certyfikacja jest już szeroko stosowana lub najprawdopodobniej będzie stosowana w najbliższej przyszłości. Sektory regulowane dyrektywą (UE) 2016/1148 są również sektorami, w których certyfikacja cyberbezpieczeństwa ma decydujące znaczenie.

([16]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30).

([17]) 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).

([18]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

(66) 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 ICT, usług ICT i procesów ICT na jednolitym rynku nadal charakteryzuje się dużym rozdrobnieniem 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 w dziedzinie cyberbezpieczeństwa należy ponadto między innymi brak interoperacyjnych rozwiązań (norm technicznych), praktyk i ogólnounijnych mechanizmów certyfikacji. Sprawia to, że przedsiębiorstwa europejskie mają trudności w konkurowaniu na poziomie krajowym, unijnym i globalnym. Sytuacja ta ogranicza również wybór opłacalnych i nadających się do użytku technologii z dziedziny cyberbezpieczeństwa, do których mają dostęp jednostki i przedsiębiorstwa. Podobnie w komunikacie z roku 2017 w sprawie śródokresowego przeglądu realizacji strategii jednolitego rynku cyfrowego „Połączony jednolity rynek cyfrowy dla wszystkich" 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 wewnętrznego.

(67) Obecnie certyfikacja cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT jest stosowana jedynie w ograniczonym stopniu. Tam, gdzie się ją stosuje, istnieje ona głównie na poziomie państw członkowskich lub w ramach programów inicjowanych przez przemysł. W związku z powyższym certyfikat wydany przez dany krajowy organ ds. certyfikacji cyberbezpieczeństwa nie jest zasadniczo uznawany w innych państwach członkowskich. Przedsiębiorstwa muszą zatem certyfikować swoje produkty ICT, usługi ICT i procesy ICT w poszczególnych państwach członkowskich, w których działają, na przykład z myślą o uczestniczeniu w krajowych postępowaniach o udzielenie zamówień publicznych, co tym samym powoduje zwiększenie kosztów dla tych przedsiębiorstw. Ponadto w sytuacji gdy powstają nowe programy, najwyraźniej brak jest spójnego i całościowego podejścia do horyzontalnych kwestii cyberbezpieczeństwa, na przykład w dziedzinie internetu rzeczy. Istniejące programy mają istotne niedociągnięcia i różnią się pod względem zakresu objętych nimi produktów, poziomów uzasadnienia zaufania, kryteriów merytorycznych i faktycznego stosowania, utrudniając działanie mechanizmów wzajemnego uznawania w Unii.

(68) Poczyniono pewne starania w celu zapewnienia wzajemnego uznawania certyfikatów w Unii. 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 należą jedynie niektóre państwa członkowskie. Ogranicza to skuteczność przyjętej przez SOG-IS umowy o wzajemnym uznawaniu z punktu widzenia rynku wewnętrznego.

(69) Konieczne jest zatem przyjęcie wspólnego podejścia i ustanowienie europejskich ram certyfikacji cyberbezpieczeństwa, określających główne wymogi horyzontalne dotyczące europejskich programów certyfikacji cyberbezpieczeństwa, które mają zostać opracowane, oraz umożliwiających uznawanie i posługiwanie się we wszystkich państwach członkowskich europejskimi certyfikatami cyberbezpieczeństwa i unijnymi deklaracjami zgodności odnoszącymi się do produktów ICT, usług ICT lub procesów ICT. Należy przy tym wykorzystać istniejące programy krajowe i międzynarodowe, a także systemy wzajemnego uznawania, w szczególności SOG-IS, oraz umożliwić płynne przejście od programów istniejących w obecnych ramach do programów podlegających nowym europejskim ramom certyfikacji cyberbezpieczeństwa. Te europejskie ramy certyfikacji cyberbezpieczeństwa powinny mieć dwojaki cel. Po pierwsze powinny one pomóc w zwiększeniu zaufania do produktów ICT, usług ICT i procesów ICT, które uzyskały certyfikację na podstawie europejskich programów certyfikacji cyberbezpieczeństwa. Po drugie powinny one pomagać uniknąć mnożenia się sprzecznych lub nakładających się wzajemnie krajowych programów certyfikacji cyberbezpieczeństwa i ograniczać dzięki temu koszty ponoszone przez przedsiębiorstwa działające na jednolitym rynku cyfrowym. Europejskie programy certyfikacji cyberbezpieczeństwa powinny mieć charakter niedyskryminujący i opierać się na normach europejskich lub międzynarodowych, o ile normy te nie są nieskuteczne lub nieodpowiednie do realizacji uzasadnionych celów Unii w tym zakresie.

(70) Europejskie ramy certyfikacji cyberbezpieczeństwa należy ustanowić w sposób ujednolicony we wszystkich państwach członkowskich, aby zapobiec praktykom poszukiwania krajów, w których najłatwiej uzyskać certyfikat, z uwagi na różnice w poziomach wymagań w różnych państwach członkowskich.

(71) Europejskie programy certyfikacji cyberbezpieczeństwa powinny opierać się o istniejące już na poziomie międzynarodowym i krajowym elementy oraz, w razie potrzeby, na specyfikacjach technicznych tworzonych przez fora i konsorcja, z uwzględnieniem wniosków w zakresie istniejących mocnych stron oraz oceniając i korygując słabości.

(72) Elastyczne rozwiązania w zakresie cyberbezpieczeństwa są konieczne, aby przemysł był w stanie przewidywać cyberzagrożenia, dlatego też każdy program certyfikacji powinien być tworzony w taki sposób, aby unikać ryzyka jego szybkiej dezaktualizacji.

(73) Komisja powinna być uprawniona do przyjmowania europejskich programów certyfikacji cyberbezpieczeństwa dla określonych grup produktów ICT, usług ICT i procesów ICT. Programy te powinny być wprowadzane i nadzorowane przez krajowe organy ds. certyfikacji cyberbezpieczeństwa, a certyfikaty wydawane w ramach tych programów powinny być ważne i uznawane w całej Unii. Programy certyfikacji prowadzone przez przemysł lub inne organizacje prywatne nie powinny być objęte zakresem stosowania niniejszego rozporządzenia. Organy zarządzające takimi programami powinny jednak mieć możliwość wystąpienia do Komisji z wnioskiem o rozważenie zatwierdzenie takich programów jako europejskiego programu certyfikacji cyberbezpieczeństwa.

(74) Przepisy niniejszego rozporządzenia powinny pozostawać bez uszczerbku dla prawa Unii ustanawiającego szczegółowe zasady certyfikacji produktów ICT, usług ICT i procesów ICT. W szczególności w rozporządzeniu (UE) 2016/679 wprowadzono przepisy dotyczące ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych mających świadczyć o zgodności operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające z tym rozporządzeniem. 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 ICT, usługi ICT i procesy ICT. Niniejsze rozporządzenie pozostaje bez uszczerbku dla certyfikacji operacji przetwarzania danych zgodnie z rozporządzeniem (UE) 2016/679, także wówczas, gdy takie operacje są elementami produktów ICT, usług ICT i procesów ICT.

(75) Celem europejskich programów certyfikacji cyberbezpieczeństwa powinno być zapewnienie, by produkty ICT, usługi ICT i procesy ICT certyfikowane zgodnie z takimi programami spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powiązanych funkcji bądź usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia. Nie jest możliwe szczegółowe określenie wymogów cyberbezpieczeństwa odnoszących się do wszystkich produktów ICT, usług ICT i procesów ICT w niniejszym rozporządzeniu. Produkty ICT, usługi ICT i procesy ICT oraz potrzeby w zakresie cyberbezpieczeństwa powiązane z tymi produktami, usługami i procesami są tak zróżnicowane, że opracowanie ogólnych wymogów cyberbezpieczeństwa obowiązujących dla wszystkich przypadków jest bardzo trudne. Konieczne jest zatem przyjęcie szerokiego i ogólnego pojęcia cyberbezpieczeństwa do celów certyfikacji, który powinien zostać uzupełniony zestawem szczegółowych celów cyberbezpieczeństwa, uwzględnianych przy projektowaniu europejskich programów certyfikacji cyberbezpieczeństwa. Metody osiągania tych celów w przypadku określonych produktów ICT, usług ICT i procesów ICT należy następnie doprecyzować na poziomie poszczególnych programów certyfikacji przyjmowanych przez Komisję, na przykład poprzez odesłanie do norm lub specyfikacji technicznych, w przypadku gdy nie istnieją odpowiednie normy.

(76) Specyfikacje techniczne wykorzystywane w europejskich programach certyfikacji cyberbezpieczeństwa powinny respektować wymogi ustanowione w załączniku II do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 ([19]). W należycie uzasadnionych przypadkach pewne odstępstwa od tych wymogów mogą jednak zostać uznane za konieczne, w przypadku gdy te specyfikacje techniczne mają zostać wykorzystane w europejskim programie certyfikacji cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki". Uzasadnienie takich odstępstw powinno być podane od wiadomości publicznej.

(77) Ocena zgodności to procedura, w której ocenia się, czy zostały spełnione konkretne wymogi dotyczące produktu ICT, usługi ICT lub procesu ICT. Procedurę tę przeprowadza niezależna strona trzecia, która nie jest wytwórcą ani dostawcą poddawanych ocenie produktów ICT, usług ICT lub procesów ICT. Europejski certyfikat cyberbezpieczeństwa powinien być wydany po tym, jak produkt ICT, usługa ICT lub proces ICT przejdzie pomyślną ocenę. Europejski certyfikat cyberbezpieczeństwa należy uznać za potwierdzenie, że dana ocena została przeprowadzona prawidłowo. W zależności od poziomu uzasadnienia zaufania europejski program certyfikacji cyberbezpieczeństwa powinien określać, czy europejski certyfikat cyberbezpieczeństwa wydaje podmiot prywatny czy publiczny. Ocena zgodności i certyfikacja same w sobie nie stanowią gwarancji cyberbezpieczeństwa certyfikowanych produkty ICT, usług ICT i procesów ICT. Stanowią one raczej procedury i metodykę techniczną w celu potwierdzenia, że produkty ICT, usługi ICT i procesy ICT zostały przetestowane i że spełniają one określone wymogi cyberbezpieczeństwa ustanowione gdzie indziej, na przykład w normach technicznych.

(78) Dokonywany przez użytkowników europejskich certyfikatów cyberbezpieczeństwa wybór odpowiedniej certyfikacji i powiązanych wymogów bezpieczeństwa powinien być oparty na analizie ryzyk związanych ze stosowaniem danego produktu ICT, usługi ICT lub procesu ICT. Poziom uzasadnienia zaufania powinien zatem być proporcjonalny do poziomu ryzyka związanego z przewidzianym stosowaniem produktu ICT, usługi ICT lub procesu ICT.

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

(79) Europejskie programy certyfikacji cyberbezpieczeństwa mogą przewidywać, że ocenę zgodności przeprowadza się na wyłączną odpowiedzialność wytwórcy lub dostawcy produktów ICT, usług ICT lub procesów ICT (zwaną dalej „oceną zgodności przez stronę pierwszą"). W takich przypadkach powinno wystarczyć, by wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT przeprowadził we własnym zakresie wszystkie kontrole w celu zapewnienia że produkty ICT, usługi ICT lub procesy ICT są zgodne z europejskim programem certyfikacji cyberbezpieczeństwa. Ocena zgodności przez stronę pierwszą powinna być uznawana za odpowiednią dla produktów ICT, usług ICT lub procesów ICT o niewielkiej złożoności, które stwarzają niewielkie ryzyko dla użytkowników, jak np. proste projekty i mechanizmy produkcji. Ponadto ocena zgodności przez stronę pierwszą powinna być dozwolona w odniesieniu do produktów ICT, usług ICT lub procesów ICT, wyłącznie w przypadku gdy odpowiadają one poziomowi uzasadnienia zaufania „podstawowy".

(80) Europejskie programy certyfikacji cyberbezpieczeństwa mogłyby zezwalać zarówno na ocenę zgodności przez stronę pierwszą, jak i certyfikację produktów ICT, usług ICT lub procesów ICT. W takim przypadku program powinien przewidywać jasne i zrozumiałe dla konsumentów lub innych użytkowników środki rozróżniania pomiędzy produktami ICT, usługami ICT lub procesami ICT, w odniesieniu do których wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT ponosi odpowiedzialność za ocenę, a produktami ICT, usługami ICT lub procesami ICT, które certyfikuje strona trzecia.

(81) Wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT, który przeprowadza ocenę zgodności przez stronę pierwszą powinien móc wydać i podpisać unijną deklarację zgodności jako element procedury oceny zgodności. Unijna deklaracja zgodności to dokument, w którym stwierdza się, że określony produkt ICT, usługa ICT lub proces ICT są zgodne z wymogami europejskiego programu certyfikacji cyberbezpieczeństwa. Wydając i podpisując unijną deklarację zgodności, wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT przyjmują odpowiedzialność za zgodność produktu ICT, usługi ICT lub procesu ICT z prawnymi wymogami europejskiego programu certyfikacji cyberbezpieczeństwa. Kopia unijnej deklaracji zgodności powinna być przedkładana krajowemu organowi ds. certyfikacji cyberbezpieczeństwa i ENISA.

(82) Wytwórcy lub dostawcy produktów ICT, usług ICT lub procesów ICT powinni – przez okres przewidziany w odpowiednim europejskim programie certyfikacji cyberbezpieczeństwa – udostępniać właściwemu krajowemu organowi ds. certyfikacji cyberbezpieczeństwa unijną deklarację zgodności, dokumentację techniczną oraz wszelkie inne istotne informacje związane ze zgodnością produktów ICT, usług ICT lub procesów ICT z europejskim programem certyfikacji cyberbezpieczeństwa. Dokumentacja techniczna powinna określać wymogi mające zastosowanie w ramach programu i powinna ona obejmować – w stopniu, w jakim ma to znaczenie dla oceny zgodności przez stronę pierwszą – projekt, wytwarzanie i działanie produktu ICT, usługi ICT lub procesu ICT. Dokumentacja techniczna powinna być opracowana tak, by umożliwiała ocenę tego, czy produkt ICT lub usługa ICT są zgodne z wymogami mającymi zastosowanie w ramach tego programu.

(83) W zarządzaniu europejskimi ramami certyfikacji cyberbezpieczeństwa uwzględnia się udział państw członkowskich, a także odpowiedni udział interesariuszy oraz określa się rolę Komisji w trakcie planowania, proponowania, przedkładania wniosków, przygotowywania, przyjmowania i przeglądu europejskich programów certyfikacji cyberbezpieczeństwa.

(84) Komisja powinna przygotować – przy wsparciu Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa (ECCG) i Grupy Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa i po przeprowadzeniu otwartych i szeroko zakrojonych konsultacji – unijny kroczący program prac na rzecz europejskich programów certyfikacji cyberbezpieczeństwa i powinna opublikować go w formie niewiążącego instrumentu. Unijny kroczący program prac powinien być dokumentem strategicznym pozwalającym przemysłowi, organom krajowym i organom normalizacyjnym na, w szczególności, przygotowanie się z wyprzedzeniem do przyszłych europejskich programów certyfikacji cyberbezpieczeństwa. Unijny kroczący program prac powinien zawierać wieloletnie zestawienie wniosków dotyczących propozycji programów, które Komisja zamierza przedłożyć ENISA w celu przygotowania na podstawie określonych przesłanek. Komisja powinna uwzględnić ten unijny kroczący program prac, przygotowując swój kroczący plan działań na rzecz normalizacji ICT oraz wnioski dotyczące normalizacji kierowane do europejskich organizacji normalizacyjnych. Z uwagi na szybkie wprowadzanie i rozpowszechnianie nowych technologii, pojawianie się nieznanych wcześniej ryzyk w cyberprzestrzeni oraz zmiany w otoczeniu prawnym lub rynkowym Komisja lub ECCG powinny być uprawnione do zwracania się do ENISA o przygotowanie propozycji programów, które nie zostały ujęte w unijnym kroczącym programie prac. W takich przypadkach Komisja i ECCG powinny również ocenić konieczność takiego wniosku, uwzględniając ogólne cele niniejszego rozporządzenia i potrzebę zapewnienia ciągłość w zakresie planów ENISA i wykorzystania zasobów.

Po otrzymaniu takiego wniosku ENISA powinna przygotowywać, bez zbędnej zwłoki, propozycję programu dla określonych produktów ICT, usług ICT lub procesów ICT. Komisja powinna ocenić pozytywne i negatywne skutki swojego wniosku dla danego rynku, szczególnie skutki dla MŚP, dla innowacji, dla barier wejścia na ten rynek i dla kosztów dla użytkowników końcowych. Komisja, w oparciu o propozycję programu przygotowaną przez ENISA, powinna być uprawniona do przyjęcia w drodze aktów wykonawczych europejskiego programu certyfikacji cyberbezpieczeństwa. Ze względu na cel ogólny oraz cele bezpieczeństwa określone w niniejszym rozporządzeniu europejskie programy certyfikacji cyberbezpieczeństwa przyjęte przez Komisję powinny zawierać minimalny zbiór elementów dotyczących przedmiotu, zakresu i funkcjonowania poszczególnych programów. Elementy te to, między innymi, zakres i przedmiot certyfikacji cyberbezpieczeństwa, w tym kategorie objętych nią produktów ICT, usług ICT i procesów ICT, dokładne wyszczególnienie wymogów cyberbezpieczeństwa, na przykład poprzez odesłanie do norm lub specyfikacji technicznych, szczegółowe kryteria oceny i metody oceny, jak również docelowy poziom uzasadnienia zaufania („podstawowy", „istotny" lub „wysoki"), a w stosownych przypadkach poziomy oceny. ENISA powinna móc odrzucić wniosek złożony przez ECCG. Takie decyzje powinien podejmować Zarząd; powinny one być należycie uzasadnione.

(85) ENISA powinna prowadzić stronę internetową zawierającą informacje na temat europejskich programów certyfikacji cyberbezpieczeństwa i popularyzującą te programy, która powinna między innymi zawierać wnioski o przygotowanie propozycji programu oraz informacje zwrotne otrzymane w wyniku konsultacji przeprowadzonych przez ENISA w fazie przygotowawczej. Strona ta powinna również zawierać informacje na temat europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności wydanych na mocy niniejszego rozporządzenia, w tym informacje dotyczące cofnięcia i wygaśnięcia takich europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności. Strona internetowa powinna również podawać informacje o krajowych programach certyfikacji cyberbezpieczeństwa, które zostały zastąpione europejskim programem certyfikacji cyberbezpieczeństwa.

(86) Poziom uzasadnienia zaufania europejskiego programu certyfikacji stanowi podstawę dla pewności, że produkt ICT, usługa ICT lub proces ICT spełniają wymogi bezpieczeństwa danego europejskiego programu certyfikacji cyberbezpieczeństwa. By zapewnić spójność europejskich ram certyfikacji cyberbezpieczeństwa, poszczególne europejskie programy certyfikacji cyberbezpieczeństwa powinny móc wskazywać poziomy uzasadnienia zaufania dla wydawanych na ich podstawie europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności. Każdy europejski certyfikat cyberbezpieczeństwa mógłby wskazywać jeden z poziomów uzasadnienia zaufania: „podstawowy", „istotny" lub „wysoki", natomiast unijne deklaracje zgodności mogłoby jedynie wskazywać poziom uzasadnienia zaufania „podstawowy". Poziomy uzasadnienia zaufania zapewniałyby odpowiadającą im rygorystyczność i wnikliwość oceny produktu ICT, usługi ICT lub procesu ICT oraz byłyby określane przez odesłanie do powiązanych z nimi specyfikacji technicznych, norm i procedur, w tym kontroli technicznych, których celem jest zapobieganie incydentom lub łagodzenie ich skutków. Poszczególne poziomy uzasadnienia zaufania powinny być jednolite w różnych sektorach, w których stosuje się certyfikację.

(87) Europejski program certyfikacji cyberbezpieczeństwa może przewidywać kilka poziomów oceny w zależności od tego, jak rygorystyczna i wnikliwa jest zastosowana metodyka oceny. Poziomy oceny powinny odpowiadać poziomom uzasadnienia zaufania i być powiązane z odpowiednim zestawem komponentów uzasadnienia zaufania. Dla wszystkich poziomów uzasadnienia zaufania, produkt ICT, usługa ICT lub proces ICT powinny zawierać określone funkcje zabezpieczeń określone przez dany program, które mogą obejmować: ustawienia fabryczne w konfiguracji bezpieczeństwa, podpisany kod, mechanizmy bezpiecznej aktualizacji i chroniące przed programami wykorzystującymi błędy w oprogramowaniu (exploit), pełna ochrona pamięci stosu (stack) lub sterty (heap). Funkcje te powinny zostać zaprogramowane i być utrzymywane przy wykorzystaniu metod rozwoju zorientowanych na bezpieczeństwo i odpowiednich narzędzi w celu zapewnienia, aby skuteczne mechanizmy w odniesieniu do oprogramowania, jak i sprzętu zostały wdrożone w sposób niezawodny.

(88) W przypadku poziomu uzasadnienia zaufania „podstawowy" ocena powinna być dokonywana na podstawie przynajmniej następujących komponentów uzasadnienia zaufania: ocena powinna obejmować przynajmniej przegląd dokumentacji technicznej produktu ICT, usługi ICT lub procesu ICT, przeprowadzany przez jednostkę oceniającą zgodność. W przypadku gdy certyfikacja obejmuje procesy ICT, przeglądowi technicznemu powinny również podlegać procesy wykorzystywane na etapie projektowania, tworzenia i utrzymania produktu ICT lub usługi ICT. Jeśli europejski program certyfikacji cyberbezpieczeństwa przewiduje ocenę zgodności przez stronę pierwszą, wystarczy, że wytwórca lub dostawca produktu ICT, usługi ICT lub procesu ICT przeprowadzili ocenę zgodności przez stronę pierwszą dotyczącą zgodności produktu ICT, usługi ICT lub procesu ICT z danym programem certyfikacji.

(89) W przypadku poziomu uzasadnienia zaufania „istotny" ocena – oprócz wymogów dotyczących poziomu uzasadnienia zaufania „podstawowy" – powinna obejmować przynajmniej weryfikację zgodności funkcjonalności bezpieczeństwa produktu ICT, usługi ICT lub procesu ICT z ich dokumentacją techniczną.

(90) W przypadku poziomu uzasadnienia zaufania „wysoki" ocena – oprócz wymogów dotyczących poziomu uzasadnienia zaufania „istotny" – powinna obejmować przynajmniej testy skuteczności, w których ocenia się odporność funkcjonalności bezpieczeństwa produktu ICT, usługi ICT lub procesu ICT na zaawansowane cyberataki dokonywane przez osoby o wysokich umiejętnościach i dysponujące znacznymi zasobami.

(91) Korzystanie z europejskiej certyfikacji cyberbezpieczeństwa i unijnych deklaracji zgodności powinno pozostać dobrowolne, chyba że prawo Unii lub prawo państwa członkowskiego przyjęte zgodnie z prawem Unii stanowią inaczej. W przypadku braku zharmonizowanego prawa Unii państwa członkowskie mogą zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2015/1535 ([20]) przyjąć krajowe przepisy techniczne przewidujące obowiązkową certyfikację w ramach europejskiego programu certyfikacji cyberbezpieczeństwa. Państwa członkowskie korzystają również z europejskiej certyfikacji cyberbezpieczeństwa w kontekście zamówień publicznych oraz dyrektywy Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE ([21]).

(92) W niektórych obszarach, by zwiększyć poziom cyberbezpieczeństwa w Unii, może być w przyszłości konieczne – w odniesieniu do określonych produktów ICT, usług ICT procesów ICT– nałożenie określonych wymogów cyberbezpieczeństwa i uczynienie ich certyfikacji obowiązkową. Komisja powinna monitorować na bieżąco wpływ przyjętych europejskich programów certyfikacji cyberbezpieczeństwa na dostępność bezpiecznych produktów ICT, usług ICT lub procesów ICT na rynku wewnętrznym oraz powinna na bieżąco oceniać skalę wykorzystania programów certyfikacji przez wytwórców lub dostawców produktów ICT, usług ICT lub procesów ICT w Unii. Skuteczność europejskich programów certyfikacji cyberbezpieczeństwa i decyzja o uczynieniu określonych programów obowiązkowymi powinny być rozważane w świetle przepisów Unii dotyczących cyberbezpieczeństwa, w szczególności dyrektywy (UE) 2016/1148, z uwzględnieniem bezpieczeństwa sieci i systemów informacyjnych wykorzystywanych przez operatorów usług kluczowych.

(93) Europejskie certyfikaty cyberbezpieczeństwa i unijne deklaracje zgodności powinny pomóc użytkownikom końcowym w dokonywaniu świadomego wyboru. Dlatego też produktom ICT, usługom ICT i procesom ICT, które uzyskały certyfikację lub w przypadku których wydana została unijne deklaracja zgodności, powinny towarzyszyć ustrukturyzowane informacje dostosowane do zakładanego poziomu wiedzy technicznej przewidywanych użytkowników końcowych. Wszystkie takie informacje powinny być dostępne on-line, a w stosownych przypadkach – w postaci fizycznej. Użytkownik końcowy powinien mieć dostęp do informacji dotyczących numeru referencyjnego programu certyfikacji, poziomu uzasadnienia zaufania, opisu ryzyk w cyberprzestrzeni powiązanych z produktem ICT, usługą ICT lub procesem ICT oraz organu lub podmiotu wydającego lub powinien mieć możliwość uzyskania kopii europejskiego certyfikatu cyberbezpieczeństwa. Ponadto użytkownik końcowy powinien zostać poinformowany o polityce wytwórcy lub dostawcy produktów ICT, usług ICT lub procesów ICT dotyczącej zapewniania wsparcia z zakresu cyberbezpieczeństwa, a mianowicie o tym, jak długo użytkownik końcowy może liczyć na otrzymywanie aktualizacji lub łat w zakresie cyberbezpieczeństwa. W stosownych przypadkach należy zapewnić: porady w zakresie działań lub ustawień, które użytkownik końcowy może zastosować, by utrzymać lub zwiększyć poziom cyberbezpieczeństwa produktu ICT lub usługi ICT oraz dane kontaktowe pojedynczego punktu kontaktowego, do którego można zgłaszać przypadki cyberataków i otrzymywać od niego wsparcie (oprócz automatycznego zgłaszania). Informacje te powinny być regularnie aktualizowane i udostępnione na stronie internetowej zawierającej informacje na temat europejskich programów certyfikacji cyberbezpieczeństwa.

(94) Z myślą o osiągnięciu celów niniejszego rozporządzenia i uniknięciu rozdrobnienia rynku wewnętrznego krajowe programy lub procedury certyfikacji cyberbezpieczeństwa dotyczące produktów ICT, usług ICT lub procesów ICT objętych europejskim programem certyfikacji cyberbezpieczeństwa powinny utracić skuteczność z dniem ustalonym przez Komisję w drodze aktów wykonawczych. Państwa członkowskie nie powinny ponadto wprowadzać nowych krajowych programów certyfikacji cyberbezpieczeństwa dotyczących produktów ICT, usług ICT lub procesów ICT objętych już istniejącym europejskim programem certyfikacji cyberbezpieczeństwa. Niemniej państwa członkowskie powinny mieć możliwość przyjmowania lub utrzymywania krajowych programów certyfikacji cyberbezpieczeństwa do celów bezpieczeństwa narodowego. Państwa członkowskie powinny informować Komisję oraz ECCG o wszelkich zamiarach dotyczących ustanowienia nowych krajowych programów certyfikacji cyberbezpieczeństwa. Komisja i ECCG powinny ocenić wpływ nowych krajowych programów certyfikacji cyberbezpieczeństwa na prawidłowe funkcjonowanie rynku wewnętrznego, mając na uwadze interes strategiczny, by zamiast krajowego programu certyfikacji wnioskować o wprowadzenie europejskiego programu certyfikacji cyberbezpieczeństwa.

(95) Celem europejskich programów certyfikacji cyberbezpieczeństwa jest pomoc w harmonizacji praktyk w zakresie cyberbezpieczeństwa w Unii. Konieczne jest, aby przyczyniały się one do zwiększenia poziomu cyberbezpieczeństwa w Unii. Przy opracowywaniu europejskich programów cyberbezpieczeństwa należy uwzględnić i umożliwić rozwój innowacji w dziedzinie cyberbezpieczeństwa.

([20]) Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1).

([21]) Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).

(96) Europejskie programy certyfikacji cyberbezpieczeństwa powinny uwzględniać aktualne metody rozwoju oprogramowania i sprzętu, a w szczególności wpływ częstych aktualizacji oprogramowania lub oprogramowania układowego na poszczególne europejskie certyfikaty cyberbezpieczeństwa. Europejskie programy certyfikacji cyberbezpieczeństwa powinny określać warunki, w przypadku których aktualizacja może powodować potrzebę ponownej certyfikacji produktu ICT, usługi ICT lub procesu ICT lub potrzebę ograniczenia zakresu danego europejskiego certyfikatu cyberbezpieczeństwa, uwzględniając wszelkie ewentualne negatywne skutki aktualizacji dla zgodności z wymogami bezpieczeństwa tego certyfikatu.

(97) Po przyjęciu europejskiego programu certyfikacji cyberbezpieczeństwa wytwórcy lub dostawcy produktów ICT, usług ICT lub procesów ICT powinni móc składać wnioski o certyfikację swoich produktów ICT lub usług ICT do wybranej jednostki oceniającej zgodność na terytorium całej Unii. Jednostki oceniające zgodność powinny być akredytowane przez krajową jednostkę akredytującą, jeśli spełniają określone szczegółowe wymogi ustanowione w niniejszym rozporządzeniu. Akredytacji powinno się udzielać na maksymalny okres pięciu lat; powinna być ona odnawialna na tych samych warunkach, o ile jednostka oceniająca zgodność nadal spełnia wymogi. Krajowe jednostki akredytujące powinny ograniczyć, zawiesić lub cofnąć akredytację danej jednostki oceniającej zgodność, jeżeli warunki akredytacji nie są lub przestały być spełniane, lub też w przypadku gdy jednostka oceniająca zgodność narusza niniejsze rozporządzenie.

(98) Obecność w przepisach krajowych odesłań do norm krajowych, które przestały być skuteczne ze względu na wejście w życie europejskiego programu certyfikacji cyberbezpieczeństwa, może powodować dezorientację. Dlatego też państwa członkowskie powinny uwzględnić przyjęcie danego europejskiego programu certyfikacji cyberbezpieczeństwa w swoich przepisach krajowych.

(99) W celu wypracowania równoważnych norm w całej Unii, ułatwienia wzajemnego uznawania i propagowania powszechnej akceptacji europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności konieczne jest ustanowienie systemu wzajemnego przeglądu pomiędzy krajowymi organami ds. certyfikacji cyberbezpieczeństwa. Wzajemny przegląd powinien obejmować procedury nadzoru w odniesieniu do zgodności produktów ICT, usług ICT i procesów ICT z europejskimi certyfikatami cyberbezpieczeństwa, procedury monitorowania przestrzegania obowiązków przez wytwórców lub dostawców produktów ICT, usług ICT i procesów ICT, którzy dokonują oceny zgodności przez stronę pierwszą, procedury monitorowania jednostek oceniających zgodność, a także adekwatność wiedzy fachowej personelu organów wydających certyfikaty o poziomie uzasadnienia zaufania „wysoki". Komisja powinna mieć możliwość ustanowienia, w drodze aktów wykonawczych, planu wzajemnego przeglądu obejmującego co najmniej 5 lat, jak również określenia kryteriów i metod funkcjonowania systemu wzajemnego przeglądu.

(100) Bez uszczerbku dla ogólnego systemu wzajemnego przeglądu, który ma zostać wprowadzony dla wszystkich krajowych organów ds. certyfikacji cyberbezpieczeństwa w ramach dotyczących europejskich ram certyfikacji cyberbezpieczeństwa, niektóre europejskie programy certyfikacji cyberbezpieczeństwa mogą obejmować mechanizm wzajemnej oceny dla organów, które w ramach tych programów wydają dla produktów ICT, usług ICT i procesów ICT europejskie certyfikaty cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki". ECCG powinna wspierać wdrażanie takich mechanizmów wzajemnej oceny. Wzajemna ocena powinna w szczególności oceniać, czy dane organy wykonują swoje obowiązki w zharmonizowany sposób i może zawierać mechanizmy odwoławcze. Wyniki wzajemnych ocen powinny być podawane od wiadomości publicznej. Dane organy mogą przyjmować odpowiednie środki w celu dostosowania odpowiednio swoich praktyk i wiedzy fachowej.

(101) Państwa członkowskie powinny wyznaczyć krajowy organ ds. certyfikacji cyberbezpieczeństwa lub większą liczbę takich organów, odpowiedzialne za nadzorowanie wykonywania obowiązków wynikających z niniejszego rozporządzenia. Krajowy organ ds. certyfikacji cyberbezpieczeństwa może być organem istniejącym lub nowo wyznaczonym. Państwo członkowskie powinno także mieć możliwość wyznaczenia, po uzgodnieniu z innym państwem członkowskim, krajowego organu lub krajowych organów ds. certyfikacji cyberbezpieczeństwa na terytorium tego innego państwa członkowskiego.

(102) Krajowe organy cyberbezpieczeństwa powinny w szczególności: monitorować i egzekwować wypełnianie przez mających siedzibę na ich terytorium wytwórców lub dostawców produktów ICT, usług ICT lub procesów ICT obowiązków związanych z unijną deklaracją zgodności; wspierać, poprzez udostępnianie wiedzy fachowej i odpowiednich informacji, krajowe jednostki akredytujące 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 europejskim programie certyfikacji cyberbezpieczeństwa; oraz monitorować zmiany zachodzące w dziedzinie certyfikacji cyberbezpieczeństwa. Krajowe organy ds. certyfikacji cyberbezpieczeństwa powinny również rozpatrywać skargi wnoszone przez osoby fizyczne lub prawne w związku z europejskimi certyfikatami cyberbezpieczeństwa, wydanymi przez te organy lub w związku z europejskimi certyfikatami cyberbezpieczeństwa wydanymi przez jednostki oceniające zgodność, w przypadku gdy takie certyfikaty wskazują poziom uzasadnienia zaufania „wysoki", powinny badać

w odpowiednim zakresie przedmiot skarg oraz powinny informować skarżących w stosownym terminie o postępach i wynikach badania. Ponadto krajowe organy ds. certyfikacji cyberbezpieczeństwa powinny współpracować z innymi krajowymi organami ds. certyfikacji cyberbezpieczeństwa lub innymi organami publicznymi, również poprzez wymianę informacji na temat ewentualnej niezgodności produktów ICT, usług ICT lub procesów ICT z wymogami niniejszego rozporządzenia lub z określonymi europejskimi programami certyfikacji cyberbezpieczeństwa. Komisja powinna ułatwiać wymianę informacji przez udostępnienie ogólnego elektronicznego systemu wspierającego wymianę informacji, na przykład systemu informacyjnego i komunikacyjnego do celów nadzoru rynku (ICSMS) i wspólnotowego systemu szybkiej informacji (RAPEX) dla produktów innych niż spożywcze, które to systemy są już wykorzystywane przez organy nadzoru rynku zgodnie z rozporządzeniem (WE) nr 765/2008.

(103) Z myślą o zapewnieniu spójnego stosowania europejskich ram certyfikacji cyberbezpieczeństwa należy ustanowić ECCG, w której skład wchodzić powinni przedstawiciele krajowych organów ds. certyfikacji cyberbezpieczeństwa lub innych odpowiednich organów krajowych. Głównymi zadaniami ECCG powinny być doradzanie i pomaganie Komisji w pracach nad zapewnieniem spójnego wprowadzania i stosowania europejskich ram certyfikacji cyberbezpieczeństwa, pomoc ENISA i ścisła z nią współpraca przy przygotowywaniu propozycji programów certyfikacji cyberbezpieczeństwa, zwracanie się do ENISA, w należycie uzasadnionych przypadkach, o przygotowanie propozycji programu, wydawanie skierowanych do ENISA opinii na temat propozycji programów oraz przyjmowanie opinii skierowanych do Komisji dotyczących utrzymania i przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa. ECCG powinna ułatwiać wymianę dobrych praktyk i wiedzy fachowej pomiędzy różnymi krajowymi organami ds. certyfikacji cyberbezpieczeństwa, które są odpowiedzialne za udzielanie zezwoleń jednostkom oceniającym zgodność i wydawanie europejskich certyfikatów cyberbezpieczeństwa.

(104) W celu podnoszenia wiedzy na temat przyszłych europejskich programów certyfikacji cyberbezpieczeństwa oraz ułatwienia ich akceptacji Komisja może wydawać ogólne lub sektorowe wytyczne dotyczące cyberbezpieczeństwa, na przykład na temat dobrych praktyk w zakresie cyberbezpieczeństwa lub odpowiedzialnego zachowania w zakresie cyberbezpieczeństwa, podkreślające pozytywne skutki stosowania certyfikowanych produktów ICT, usług ICT i procesów ICT.

(105) W celu dalszego ułatwiania handlu, dostrzegając, że łańcuchy dostaw w dziedzinie ICT mają charakter globalny, Unia może zgodnie z art. 218 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) zawierać umowy o wzajemnym uznawaniu dotyczące europejskich certyfikatów cyberbezpieczeństwa. Komisja, uwzględniając opinię agencji ENISA i Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa, może zalecić rozpoczęcie stosownych negocjacji. Każdy europejski program certyfikacji cyberbezpieczeństwa powinien przewidywać szczegółowe warunki dotyczące takich umów o wzajemnym uznawaniu z państwami trzecimi.

(106) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([22]).

(107) Należy stosować procedurę sprawdzającą w celu: przyjęcia aktów wykonawczych dotyczących europejskich programów certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT lub procesów ICT, przyjęcia aktów wykonawczych dotyczących zasad prowadzenia przez ENISA postępowań wyjaśniających, w celu przyjęcia aktów wykonawczych dotyczących planu wzajemnego przeglądu krajowych organów ds. certyfikacji cyberbezpieczeństwa, a także przyjęcia aktów wykonawczych dotyczących okoliczności, formatów i procedur notyfikowania Komisji przez krajowe organy ds. certyfikacji cyberbezpieczeństwa akredytowanych jednostek oceniających zgodność.

(108) Działalność ENISA powinna być przedmiotem regularnej i niezależnej oceny. Ocena ta powinna dotyczyć realizacji przez ENISA jej celów, jej metod pracy i zasadności jej zadań, a zwłaszcza jej zadań w zakresie współpracy operacyjnej na poziomie Unii. Taka ocena powinna również dotyczyć wpływu, skuteczności i efektywności europejskich ram certyfikacji cyberbezpieczeństwa. W przypadku przeglądu Komisja powinna ocenić, w jaki sposób można wzmocnić pełnioną przez ENISA rolę punktu odniesienia w zakresie doradztwa i wiedzy fachowej, a także powinna ocenić możliwość pełnienia przez ENISA roli we wspieraniu oceniania pochodzących z państw trzecich produktów ICT, usług ICT i procesów ICT wchodzących na unijny rynek, które nie są zgodne z przepisami Unii.

([22]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

(109) Ponieważ cele niniejszego rozporządzenia nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na jego rozmiary i skutki możliwe jest lepsze ich osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej (TUE). Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(110) Należy uchylić rozporządzenie (UE) nr 526/2013,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

TYTUŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i zakres stosowania

1. Z myślą o zapewnieniu prawidłowego funkcjonowania rynku wewnętrznego, a jednocześnie dążąc do osiągnięcia wysokiego poziomu cyberbezpieczeństwa, cyberodporności i zaufania w Unii, w niniejszym rozporządzeniu określa się:

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

b) ramy ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT w Unii oraz w celu uniknięcia rozdrobnienia rynku wewnętrznego w zakresie programów certyfikacji cyberbezpieczeństwa w Unii.

Ramy, o których mowa w akapicie pierwszym lit. b), stosuje się bez uszczerbku dla przepisów szczegółowych dotyczących dobrowolnej lub obowiązkowej certyfikacji zawartych w innych aktach prawnych Unii.

2. Niniejsze rozporządzenie pozostaje bez uszczerbku dla kompetencji państw członkowskich w zakresie 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” oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami;

2) „sieci i systemy informatyczne” oznaczają sieci i systemy informatyczne zgodnie z definicją w art. 4 pkt 1 dyrektywy (UE) 2016/1148;

3) „krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych” oznacza krajową strategię w zakresie bezpieczeństwa sieci i systemów informatycznych zgodnie z definicją w art. 4 pkt 3 dyrektywy (UE) 2016/1148;

4) „operator usług kluczowych” oznacza operatora usług kluczowych zgodnie z definicją w art. 4 pkt 4 dyrektywy (UE) 2016/1148;

5) „dostawca usług cyfrowych” oznacza dostawcę usług cyfrowych zgodnie z definicją w art. 4 pkt 6 dyrektywy (UE) 2016/1148;

6) „incydent” oznacza incydent zgodnie z definicją w art. 4 pkt 7 dyrektywy (UE) 2016/1148;

7) „postępowanie w przypadku incydentu” oznacza postępowanie w przypadku incydentu zgodnie z definicją w art. 4 pkt 8 dyrektywy (UE) 2016/1148;

8) „cyberzagrożenie" oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób;

9) „europejski program certyfikacji cyberbezpieczeństwa" oznacza kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur ustanowionych na poziomie unijnym i mających zastosowanie do certyfikacji lub oceny zgodności określonych produktów ICT, usług ICT i procesów ICT;

10) „krajowy program 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 programu produktów ICT, usług ICT i procesów ICT;

11) „europejski certyfikat cyberbezpieczeństwa" oznacza wydany przez odpowiedni organ dokument poświadczający, że dany produkt ICT, dana usługa ICT lub dany proces ICT zostały ocenione pod względem zgodności ze szczegółowymi wymogami bezpieczeństwa określonymi w europejskim programie certyfikacji cyberbezpieczeństwa;

12) „produkt ICT" oznacza element lub grupę elementów sieci lub systemów informatycznych;

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

14) „proces ICT" oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;

15) „akredytacja" oznacza akredytację zgodnie z definicją w art. 2 pkt 10 rozporządzenia (WE) nr 765/2008;

16) „krajowa jednostka akredytująca" oznacza krajową jednostkę akredytującą zgodnie z definicją w art. 2 pkt 11 rozporządzenia (WE) nr 765/2008;

17) „ocena zgodności" oznacza ocenę zgodności zgodnie z definicją w art. 2 pkt 12 rozporządzenia (WE) nr 765/2008;

18) „jednostka oceniająca zgodność" oznacza jednostkę oceniającą zgodność zgodnie z definicją w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008;

19) „norma" oznacza normę zgodnie z definicją w art. 2 pkt 1 rozporządzenia (UE) nr 1025/2012;

20) „specyfikacja techniczna" oznacza dokument określający wymogi techniczne, które mają być spełnione przez produkt ICT, usługę ICT lub proces ICT lub procedury oceny zgodności w odniesieniu do produktu ICT, usługi ICT lub procesu ICT;

21) „poziom uzasadnienia zaufania" oznacza podstawę dla pewności, że dany produkt ICT, dana usługa ICT lub dany proces ICT spełnia wymogi bezpieczeństwa określonego europejskiego programu certyfikacji cyberbezpieczeństwa; wskazuje on poziom, na jakim została dokonana ocena danego produktu ICT, danej usługi ICT lub danego procesu ICT, ale jako taki nie dokonuje on pomiaru bezpieczeństwa tego produktu ICT, tej usługi ICT lub tego procesu ICT;

22) „ocena zgodności przez stronę pierwszą" oznacza przeprowadzone przez wytwórcę lub dostawcę produktów ICT, usług ICT lub procesów ICT czynności oceniające, czy te produkty ICT, usługi ICT lub procesy ICT spełniają wymogi określonego europejskiego programu certyfikacji cyberbezpieczeństwa.

TYTUŁ II

ENISA (AGENCJA UNII EUROPEJSKIEJ DS. CYBERBEZPIECZEŃSTWA)

ROZDZIAŁ I

Mandat i cele

Artykuł 3

Mandat

1. ENISA wykonuje zadania powierzone jej na mocy niniejszego rozporządzenia w celu osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, w tym poprzez aktywne wspieranie państw członkowskich, instytucji, organów i jednostek organizacyjnych Unii w poprawie cyberbezpieczeństwa. ENISA działa jako punkt odniesienia w zakresie doradztwa i wiedzy fachowej z zakresu cyberbezpieczeństwa na potrzeby instytucji, organów i jednostek organizacyjnych Unii, a także na potrzeby innych odpowiednich unijnych interesariuszy.

ENISA przyczynia się do zmniejszenia rozdrobnienia rynku wewnętrznego wykonując zadania powierzone jej na mocy niniejszego rozporządzenia.

2. ENISA wykonuje zadania powierzone jej na mocy aktów prawnych Unii określających środki zbliżania przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które to przepisy dotyczą cyberbezpieczeństwa.

3. Wykonując swoje zadania, ENISA działa niezależnie, unikając jednocześnie powielania działań państw członkowskich oraz uwzględniając posiadaną przez państwa członkowskie wiedzę fachową.

4. ENISA tworzy własne zasoby, w tym zdolności techniczne i zdolności w zakresie zasobów ludzkich oraz umiejętności, niezbędne do wykonywania zadań powierzonych jej na mocy niniejszego rozporządzenia.

Artykuł 4

Cele

1. ENISA stanowi ośrodek wiedzy fachowej w dziedzinie cyberbezpieczeństwa z racji swojej niezależności, naukowo-technicznej jakości oferowanego doradztwa i pomocy, przekazywanych przez siebie informacji, przejrzystości swoich procedur działania, metod działania oraz staranności w wykonywaniu swoich zadań.

2. ENISA pomaga instytucjom, organom i jednostkom organizacyjnym Unii, jak również państwom członkowskim w opracowywaniu i realizacji unijnych polityk dotyczących cyberbezpieczeństwa, w tym polityk sektorowych dotyczących cyberbezpieczeństwa.

3. ENISA wspiera budowanie potencjału i gotowości w całej Unii, pomagając instytucjom, organom i jednostkom organizacyjnym Unii, jak również państwom członkowskim oraz interesariuszom z sektora publicznego i prywatnego w zwiększeniu ochrony ich sieci i systemów informatycznych, tworzeniu i ulepszaniu cyberodporności i zdolności reagowania oraz w rozwijaniu umiejętności i kompetencji w dziedzinie cyberbezpieczeństwa.

4. ENISA propaguje współpracę, w tym wymianę informacji i koordynację na poziomie unijnym, pomiędzy państwami członkowskimi, instytucjami, organami i jednostkami organizacyjnymi Unii oraz odpowiednimi interesariuszami z sektora publicznego i prywatnego w kwestiach związanych z cyberbezpieczeństwem.

5. ENISA przyczynia się do zwiększania zdolności w zakresie cyberbezpieczeństwa na poziomie unijnym w celu wspierania działań państw członkowskich służących zapobieganiu cyberzagrożeniom i reagowaniu na nie, w szczególności w przypadku incydentów transgranicznych.

6. ENISA propaguje korzystanie z europejskiej certyfikacji cyberbezpieczeństwa z myślą o unikaniu rozdrobnienia rynku wewnętrznego. ENISA przyczynia się do utworzenia i utrzymywania europejskich ram certyfikacji cyberbezpieczeństwa zgodnie z tytułem III niniejszego rozporządzenia, z myślą o zwiększeniu przejrzystości cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT, zwiększając w ten sposób zaufanie do wewnętrznego rynku cyfrowego i jego konkurencyjność.

7. ENISA propaguje wysoki poziom wiedzy na temat cyberbezpieczeństwa, w tym cyberhigienę i umiejętności cyfrowe wśród obywateli, organizacji i przedsiębiorstw.

ROZDZIAŁ II

Zadania

Artykuł 5

Opracowywanie i wdrażanie polityki i prawa Unii

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

1) pomoc i doradztwo w zakresie opracowywania i przeglądu polityki i prawa Unii w dziedzinie cyberbezpieczeństwa oraz w zakresie inicjatyw dotyczących polityki i prawa Unii w poszczególnych sektorach, w których występują kwestie związane z cyberbezpieczeństwem, w szczególności poprzez wydawanie niezależnych opinii i analiz, jak również prowadzenie prac przygotowawczych;

2) pomoc państwom członkowskim przy wdrażaniu polityki i prawa Unii w dziedzinie cyberbezpieczeństwa w sposób jednolity, w szczególności w związku z dyrektywą (UE) 2016/1148, w tym za pomocą wydawania opinii, wytycznych, udzielania porad i najlepszych praktyk dotyczących takich zagadnień jak zarządzanie ryzykiem, zgłaszanie incydentów i wymiana informacji, jak również za pomocą ułatwiania wymiany najlepszych praktyk pomiędzy właściwymi organami w tym zakresie;

3) pomoc państwom członkowskim oraz instytucjom, organom i jednostkom organizacyjnym Unii przy opracowywaniu i propagowaniu polityk cyberbezpieczeństwa dotyczących utrzymywania ogólnej dostępności i integralności publicznego rdzenia otwartego internetu;

4) wkład w prace grupy współpracy na podstawie art. 11 dyrektywy (UE) 2016/1148, przez zapewnianie wiedzy fachowej i pomocy;

5) wsparcie dla:

   a) opracowywania i wdrażania polityki Unii w dziedzinie tożsamości elektronicznej i usług zaufania, w szczególności poprzez zapewnianie doradztwa i wydawanie wytycznych technicznych, jak również poprzez ułatwianie wymiany najlepszych praktyk pomiędzy właściwymi organami;

   b) działania na rzecz podwyższonego poziomu bezpieczeństwa łączności elektronicznej, w tym poprzez zapewnianie doradztwa i wiedzy fachowej, jak również poprzez ułatwianie wymiany najlepszych praktyk pomiędzy właściwymi organami;

   c) państw członkowskich przy wdrażaniu konkretnych, dotyczących cyberbezpieczeństwa, aspektów polityki i prawa Unii związanych z ochroną danych i prywatnością, w tym poprzez zapewnianie doradztwa Europejskiej Radzie Ochrony Danych na jej wniosek;

6) wsparcie dla regularnego przeglądu działań w ramach polityki Unii poprzez przygotowywanie sprawozdania rocznego na temat stanu wdrożenia odpowiednich ram prawnych w odniesieniu do:

   a) informacji w sprawie zgłoszeń incydentów w państwach członkowskich, przekazywanych grupie współpracy przez pojedyncze punkty kontaktowe na podstawie art. 10 ust. 3 dyrektywy (UE) 2016/1148;

   b) zestawień zawiadomień o naruszeniach bezpieczeństwa lub utracie integralności otrzymanych od dostawców usług zaufania, przekazywanych ENISA przez organy nadzoru na podstawie art. 19 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([23]);

   c) zawiadomień o incydentach związanych z bezpieczeństwem przekazanych przez dostawców udostępniających publiczne sieci łączności elektronicznej lub świadczących publicznie dostępne usług łączności elektronicznej, przekazywanych ENISA przez właściwe organy na podstawie art. 40 dyrektywy (UE) 2018/1972.

([23]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).

Artykuł 6

Budowanie zdolności

1. ENISA pomaga:

a) państwom członkowskim w ich staraniach na rzecz poprawy w zakresie zapobiegania cyberzagrożeniom i incydentom, ich wykrywania i analizowania oraz zdolności reagowania na cyberzagrożenia i incydenty – poprzez zapewnianie państwom członkowskim wiedzy fachowej;

b) państwom członkowskim oraz instytucjom, organom i jednostkom organizacyjnym Unii w ustanawianiu i wdrażaniu dobrowolnych polityk w zakresie ujawniania podatności;

c) instytucjom, organom i jednostkom organizacyjnym Unii w ich staraniach na rzecz poprawy w zakresie zapobiegania cyberzagrożeniom i incydentom, ich wykrywania i analizowania oraz na rzecz poprawy ich zdolności reagowania na takie cyberzagrożenia i incydenty, w szczególności poprzez odpowiednie wsparcie CERT-UE;

d) państwom członkowskim, w tworzeniu krajowych zespołów CSIRT, jeżeli zwrócono się o taką pomoc na podstawie art. 9 ust. 5 dyrektywy (UE) 2016/1148;

e) państwom członkowskim w opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, jeżeli zwrócono się o taką pomoc na podstawie art. 7 ust. 2 dyrektywy (UE) 2016/1148, oraz promuje działania na rzecz upowszechniania tych strategii i odnotowuje postępy w ich wdrażaniu w całej Unii w celu propagowania najlepszych praktyk;

f) instytucjom Unii w opracowywaniu unijnych strategii w zakresie cyberbezpieczeństwa, działaniu na rzecz ich upowszechnienia i monitorowaniu postępów w ich realizacji;

g) 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 – przy uwzględnieniu aktualnego stanu wiedzy – posiadał wspólny zestaw minimalnych wymogów dotyczących zdolności oraz działał zgodnie z najlepszymi praktykami;

h) państwom członkowskim, poprzez regularne organizowanie na poziomie unijnym, co najmniej raz na dwa lata, ćwiczeń w dziedzinie cyberbezpieczeństwa, o których mowa w art. 7 ust. 5, oraz wydawanie zaleceń dotyczących polityki w oparciu o proces oceny tych ćwiczeń i zdobyte przy nich doświadczenia;

i) odpowiednim organom publicznym, poprzez oferowanie szkoleń dotyczących cyberbezpieczeństwa, w stosownych przypadkach we współpracy z interesariuszami;

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

2. ENISA wspiera wymianę informacji w ramach sektorów i pomiędzy sektorami, w szczególności w sektorach wymienionych w załączniku II do dyrektywy (UE) 2016/1148, zapewniając najlepsze praktyki i porady dotyczące dostępnych narzędzi, procedur, jak również sposobu postępowania w kwestiach regulacyjnych związanych z wymianą informacji.

Artykuł 7

Współpraca operacyjna na poziomie unijnym

1. ENISA wspiera współpracę operacyjną pomiędzy państwami członkowskimi, instytucjami, organami i jednostkami organizacyjnymi Unii oraz pomiędzy interesariuszami.

2. ENISA współpracuje na poziomie operacyjnym i tworzy synergię z instytucjami, organami i jednostkami organizacyjnymi Unii, w tym z 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, między innymi poprzez:

a) wymianę know-how i najlepszych praktyk;

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

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

3. ENISA zapewnia sekretariat sieci CSIRT na podstawie art. 12 ust. 2 dyrektywy (UE) 2016/1148 i w ramach tych obowiązków aktywnie wspiera wymianę informacji i współpracę pomiędzy jej członkami.

4. ENISA wspiera państwa członkowskie w zakresie współpracy operacyjnej w ramach sieci CSIRT poprzez:

a) doradztwo dotyczące tego, w jaki sposób podnosić ich zdolność zapobiegania incydentom, ich wykrywania i reagowania na nie oraz, na wniosek co najmniej jednego państwa członkowskiego, zapewnianie doradztwa w związku z konkretnym cyberzagrożeniem;

b) pomoc, udzielaną na wniosek co najmniej jednego państwa członkowskiego, przy ocenie incydentów mających istotny wpływ poprzez zapewnienie wiedzy fachowej i ułatwianie technicznego postępowania w przypadku takich incydentów, w tym w szczególności poprzez wspieranie dobrowolnej wymiany stosownych informacji i rozwiązań technicznych pomiędzy państwami członkowskimi;

c) analizę podatności i incydentów na podstawie publicznie dostępnych informacji lub informacji dobrowolnie przekazanych w tym celu przez państwa członkowskie; oraz

d) wsparcie, udzielane na wniosek co najmniej jednego państwa członkowskiego, w zakresie technicznych postępowań wyjaśniających *ex post* dotyczących incydentów mających istotny wpływ w rozumieniu dyrektywy (UE) 2016/1148.

Realizując te zadania, ENISA i CERT-UE angażują się w ustrukturyzowaną współpracę w celu czerpania korzyści z efektów synergii i unikania powielania działań.

5. ENISA organizuje regularnie ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie unijnym i wspiera państwa członkowskie oraz instytucje, organy i jednostki organizacyjne Unii w organizacji ćwiczeń w dziedzinie cyberbezpieczeństwa w odpowiedzi na ich wnioski. Takie ćwiczenia w dziedzinie cyberbezpieczeństwa na poziomie unijnym mogą obejmować elementy techniczne, operacyjne lub strategiczne. Raz na dwa lata ENISA organizuje kompleksowe ćwiczenia na dużą skalę.

W stosownych przypadkach ENISA wnosi również wkład w sektorowe ćwiczenia w dziedzinie cyberbezpieczeństwa i pomaga w ich organizacji wspólnie z odpowiednimi organizacjami, które również uczestniczą w ćwiczeniach w dziedzinie cyberbezpieczeństwa na poziomie unijnym.

6. ENISA, w ścisłej współpracy z państwami członkowskimi, przygotowuje regularny pogłębiony raport techniczny o stanie cyberbezpieczeństwa w UE dotyczący incydentów i cyberzagrożeń, w oparciu o dostępne publicznie informacje, własne analizy oraz sprawozdania udostępniane przez, między innymi, zespoły CSIRT państw członkowskich lub pojedyncze punkty kontaktowe ustanowione dyrektywą (UE) 2016/1148, w obu przypadkach przekazywane na zasadzie dobrowolności, EC3 i CERT-UE.

7. ENISA wnosi wkład w przygotowanie wspólnej reakcji, na poziomie Unii i państw członkowskich, na transgraniczne incydenty lub kryzysy na dużą skalę związane z cyberbezpieczeństwem, głównie poprzez:

a) zestawianie i analizowanie raportów ze źródeł krajowych, dostępnych publicznie lub udostępnionych na zasadzie dobrowolności, w celu przyczynienia się do ustalenia wspólnej orientacji sytuacyjnej;

b) zapewnienie skutecznego przepływu informacji i wprowadzenie mechanizmów kierowania problemów na wyższy poziom pomiędzy siecią CSIRT a decydentami technicznymi i politycznymi na poziomie unijnym;

c) ułatwianie, na wniosek, postępowania technicznego w przypadku takich incydentów lub kryzysów, w tym – w szczególności – poprzez wspieranie dobrowolnego dzielenia się przez państwa członkowskie rozwiązaniami technicznymi;

d) wspieranie instytucji, organów i jednostek organizacyjnych Unii oraz, na wniosek, państw członkowskich w zakresie komunikacji społecznej w związku z takimi incydentami lub kryzysami;

e) testowanie planów współpracy na potrzeby reagowania na takie incydenty lub kryzysy na poziomie unijnym oraz, na wniosek, wspieranie państw członkowskich w testowaniu takich planów na poziomie krajowym.

Artykuł 8

Rynek, certyfikacja cyberbezpieczeństwa i normalizacja

1. ENISA wspiera i propaguje opracowywanie i realizację ustanowionej w tytule III niniejszego rozporządzenia polityki Unii w zakresie certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT poprzez:

a) monitorowanie na bieżąco zmian w powiązanych dziedzinach normalizacji i zalecanie odpowiednich specyfikacji technicznych do zastosowania przy tworzeniu europejskich programów certyfikacji cyberbezpieczeństwa zgodnie z art. 54 ust. 1 lit. c), w przypadkach gdy nie istnieją normy w danym zakresie;

b) przygotowywanie propozycji dotyczących europejskich programów certyfikacji cyberbezpieczeństwa (zwanych dalej „propozycjami programów") dla produktów ICT, usług ICT i procesów ICT zgodnie z art. 49;

c) ocenianie przyjętych europejskich programów certyfikacji cyberbezpieczeństwa zgodnie z art. 49 ust. 8;

d) uczestniczenie we wzajemnych przeglądach na podstawie art. 59 ust. 4;

e) udzielanie pomocy Komisji przy zapewnianiu obsługi sekretariatu dla ECCG zgodnie z art. 62 ust. 5.

2. ENISA zapewnia obsługę sekretariatu Grupy Interesariuszy Ds. Certyfikacji Cyberbezpieczeństwa zgodnie z art. 22 ust. 4.

3. ENISA sporządza i publikuje wytyczne oraz opracowuje dobre praktyki dotyczące wymogów cyberbezpieczeństwa dotyczących produktów ICT, procesów ICT i usług ICT, we współpracy z krajowymi organami ds. certyfikacji cyberbezpieczeństwa oraz z przemysłem prowadzonej w formalny, ustrukturyzowany i przejrzysty sposób.

4. ENISA przyczynia się do budowania zdolności związanych z procesami oceny i certyfikacji poprzez sporządzanie i wydawanie wytycznych, a także udzielania wsparcia państwom członkowskim na ich wniosek.

5. ENISA ułatwia ustanowienie i upowszechnianie europejskich i międzynarodowych norm dotyczących zarządzania ryzykiem oraz dotyczących bezpieczeństwa produktów ICT, usług ICT i procesów ICT.

6. ENISA opracowuje, we współpracy z państwami członkowskimi i przemysłem, porady i wytyczne dotyczące kwestii technicznych związanych z wymogami bezpieczeństwa dla 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.

7. ENISA 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

ENISA:

a) przeprowadza analizy powstających technologii i przedstawia tematyczne oceny dotyczące spodziewanego społecznego, prawnego, gospodarczego i regulacyjnego wpływu innowacji technologicznych na cyberbezpieczeństwo;

b) przeprowadza długoterminowe analizy strategiczne cyberzagrożeń i incydentów w celu rozpoznania pojawiających się tendencji i w celu pomocy w zapobieganiu incydentom;

c) we współpracy z ekspertami z organów państw członkowskich i odpowiednimi interesariuszami – zapewnia doradztwo, porady 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 wymienionych w załączniku III do tej dyrektywy;

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

e) gromadzi i analizuje publicznie dostępne informacje dotyczące istotnych incydentów oraz sporządza sprawozdania w celu zapewnienia porad obywatelom, organizacjom i przedsiębiorstwom w całej Unii.

Artykuł 10

Podnoszenie wiedzy i edukacja

ENISA:

a) działa na rzecz podnoszenia wiedzy ogółu społeczeństwa na temat ryzyk w cyberprzestrzeni i zapewnia porady w zakresie dobrych praktyk dla użytkowników indywidualnych skierowane do obywateli, organizacji i przedsiębiorstw, w tym w zakresie cyberhigieny i umiejętności cyfrowych;

b) we współpracy z państwami członkowskimi, instytucjami, organami i jednostkami organizacyjnymi Unii oraz przemysłem, organizuje regularne kampanie informacyjne na rzecz zwiększenia cyberbezpieczeństwa i jego wyeksponowania w Unii oraz zachęca do szerokiej debaty publicznej;

c) wspiera państwa członkowskie w ich staraniach mających na celu podniesienie wiedzy na temat cyberbezpieczeństwa i propagowanie edukacji w tym zakresie;

d) wspiera ściślejszą koordynację i wymianę najlepszych praktyk pomiędzy państwami członkowskimi w dziedzinie podnoszenia wiedzy na temat cyberbezpieczeństwa i edukacji w tym zakresie.

Artykuł 11

Badania i innowacje

W odniesieniu do badań i innowacji ENISA:

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

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

c) wnosi wkład do programu strategicznych badań i innowacji na poziomie unijnym w dziedzinie cyberbezpieczeństwa.

Artykuł 12

Współpraca międzynarodowa

ENISA wnosi wkład w starania Unii na rzecz współpracy z państwami trzecimi i organizacjami międzynarodowymi, a także na rzecz propagowania – w ramach odpowiednich międzynarodowych ram współpracy – współpracy międzynarodowej w kwestiach związanych z cyberbezpieczeństwem, poprzez:

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

b) na wniosek Komisji, ułatwianie wymiany najlepszych praktyk;

c) na wniosek Komisji, zapewnianie jej wiedzy fachowej;

d) zapewnianie Komisji doradztwa i wsparcia, we współpracy z ECCG ustanowioną na mocy art. 62, w kwestiach związanych z umowami o wzajemnym uznawaniu certyfikatów cyberbezpieczeństwa zawieranymi z państwami trzecimi.

ROZDZIAŁ III

Struktura organizacyjna ENISA

Artykuł 13

Struktura ENISA

Strukturę administracyjną i kierowniczą ENISA tworzą:

a) Zarząd;

b) Rada Wykonawcza;

c) Dyrektor Wykonawczy;

d) Grupa Doradcza ENISA;

e) Sieć Krajowych Urzędników Łącznikowych.

Sekcja 1

Zarząd

Artykuł 14

Skład Zarządu

1. W skład Zarządu wchodzi po jednym członku powoływanym przez każde z państw członkowskich oraz dwóch członków powoływanych przez Komisję. Prawo głosu przysługuje wszystkim członkom Zarządu.

2. Każdy z członków Zarządu ma zastępcę. Zastępca reprezentuje członka Zarządu pod jego nieobecność.

3. Członków Zarządu i ich zastępców powołuje się z uwagi na ich wiedzę w dziedzinie cyberbezpieczeństwa, uwzględniając ich 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 równowagi płci w Zarządzie.

4. Kadencja członków Zarządu i ich zastępców trwa cztery lata. Kadencja ta jest odnawialna.

Artykuł 15

Funkcje Zarządu

1. Zarząd:

a) określa ogólny kierunek działalności ENISA oraz zapewnia, aby ENISA działała zgodnie z przepisami i zasadami ustanowionymi w niniejszym rozporządzeniu; Zarząd zapewnia również spójność pracy ENISA z działaniami prowadzonymi przez państwa członkowskie oraz działaniami na poziomie unijnym;

b) przyjmuje projekt jednolitego dokumentu programowego ENISA, o którym mowa w art. 24, przed przedłożeniem go Komisji do zaopiniowania;

c) przyjmuje jednolity dokument programowy ENISA, uwzględniając opinię Komisji;

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

e) przyjmuje budżet roczny ENISA oraz pełni inne funkcje dotyczące budżetu ENISA zgodnie z rozdziałem IV;

f) ocenia i przyjmuje skonsolidowane sprawozdanie roczne z działalności ENISA, obejmujące sprawozdanie finansowe i opisujące, w jaki sposób ENISA zrealizowała swoje wskaźniki skuteczności działania, przesyła do dnia 1 lipca następnego roku zarówno sprawozdanie roczne, jak i jego ocenę, Parlamentowi Europejskiemu, Radzie, Komisji i Trybunałowi Obrachunkowemu oraz podaje sprawozdanie roczne do wiadomości publicznej;

g) przyjmuje zgodnie z art. 32 przepisy finansowe mające zastosowanie do ENISA;

h) przyjmuje strategię na rzecz przeciwdziałania nadużyciom finansowym, która jest proporcjonalna do ryzyk wystąpienia takich nadużyć, uwzględniając analizę kosztów i korzyści wynikających z wdrażanych środków;

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

j) 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;

k) przyjmuje swój regulamin wewnętrzny, zawierający przepisy dotyczące decyzji tymczasowych w sprawie przekazania uprawnień do wykonywania określonych zadań na podstawie art. 19 ust. 7;

l) wykonuje wobec personelu ENISA, zgodnie z ust. 2 niniejszego artykułu, uprawnienia powierzone w regulaminie pracowniczym urzędników Unii Europejskiej (zwanym dalej „regulaminem pracowniczym urzędników") oraz w warunkach zatrudnienia innych pracowników Unii Europejskiej (zwanych dalej „warunkami zatrudnienia innych pracowników"), ustanowionych w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68) ([24]), organowi powołującemu oraz organowi uprawnionemu do zawierania umów o pracę („uprawnienia organu powołującego");

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

n) powołuje Dyrektora Wykonawczego oraz w stosownych przypadkach podejmuje decyzje o przedłużeniu jego kadencji lub odwołaniu go ze stanowiska zgodnie z art. 36;

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

p) podejmuje wszystkie decyzje dotyczące ustanowienia wewnętrznej struktury ENISA, a w razie potrzeby zmiany takiej wewnętrznej struktury, uwzględniając potrzeby w zakresie działań ENISA i mając na uwadze należyte zarządzanie budżetem;

q) wydaje zgodę na dokonywanie ustaleń roboczych zgodnie z art. 7;

r) wydaje zgodę na dokonywanie lub zawieranie ustaleń roboczych zgodnie z art. 42.

2. Zgodnie z art. 110 regulaminu pracowniczego urzędników Zarząd przyjmuje na podstawie art. 2 ust. 1 regulaminu pracowniczego urzędników i art. 6 warunków zatrudnienia innych pracowników decyzję przekazującą odpowiednie uprawnienia organu powołującego Dyrektorowi Wykonawczemu i określającą warunki, zgodnie z którymi możliwe jest zawieszenie przekazania tych uprawnień. Dyrektor Wykonawczy może przekazać dalej te uprawnienia.

([24]) Dz.U. L 56 z 4.3.1968, s. 1.

3. W przypadku gdy wymagają tego wyjątkowe okoliczności, Zarząd może przyjąć decyzję o tymczasowym zawieszeniu przekazania uprawnień organu powołującego Dyrektorowi Wykonawczemu i wszelkich uprawnień organu powołującego przekazanych dalej przez Dyrektora Wykonawczego oraz zamiast tego wykonywać je samodzielnie lub przekazać je jednemu ze swoich członków lub członkowi personelu innemu niż Dyrektor Wykonawczy.

Artykuł 16

Przewodniczący Zarządu

Większością dwóch trzecich głosów członków Zarząd wybiera spośród swoich członków przewodniczącego i zastępcę przewodniczącego. Ich kadencja trwa trzy lata, 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 17

Posiedzenia Zarządu

1. Posiedzenia Zarządu zwoływane są przez przewodniczącego Zarządu.

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

3. Dyrektor Wykonawczy bierze udział w posiedzeniach Zarządu, ale nie przysługuje mu prawo głosu.

4. Członkowie Grupy Doradczej ENISA mogą na zaproszenie przewodniczącego brać udział w posiedzeniach Zarządu, ale nie przysługuje im prawo głosu.

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

6. ENISA zapewnia Zarządowi obsługę sekretariatu.

Artykuł 18

Zasady głosowania Zarządu

1. Zarząd przyjmuje decyzje większością głosów swoich członków.

2. Do przyjęcia jednolitego dokumentu programowego, budżetu rocznego, powołania Dyrektora Wykonawczego, przedłużenia jego kadencji lub odwołania go ze stanowiska wymagana jest większość dwóch trzecich głosów członków Zarządu.

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

4. Przewodniczący Zarządu bierze udział w głosowaniu.

5. Dyrektor Wykonawczy nie bierze udziału w głosowaniu.

6. W regulaminie wewnętrznym Zarządu ustala się bardziej szczegółowe zasady głosowania, w szczególności okoliczności, w których jeden członek Zarządu może działać w imieniu innego członka.

Sekcja 2

Rada Wykonawcza

Artykuł 19

Rada Wykonawcza

1. Zarząd wspierany jest przez Radę Wykonawczą.

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. 20, wspiera Dyrektora Wykonawczego i doradza mu przy wdrażaniu decyzji Zarządu w sprawach administracyjnych i budżetowych na podstawie art. 20.

3. W skład Rady Wykonawczej wchodzi pięciu członków. Członkowie Rady Wykonawczej powoływani są spośród członków Zarządu. W skład Rady Wykonawczej musi wchodzić przewodniczący Zarządu, który może również przewodniczyć Radzie Wykonawczej, oraz jeden z przedstawicieli Komisji. Powołania członków Rady Wykonawczej mają na celu zapewnienie równowagi płci w Radzie Wykonawczej. Dyrektor Wykonawczy bierze udział w posiedzeniach Rady Wykonawczej, ale nie przysługuje mu prawo głosu.

4. Kadencja członków Rady Wykonawczej trwa cztery lata. Kadencja ta jest odnawialna.

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

6. Zarząd ustanawia regulamin wewnętrzny Rady Wykonawczej.

7. W stosownych przypadkach, ze względu na pilny charakter sprawy, Rada Wykonawcza może przyjmować w imieniu Zarządu określone decyzje tymczasowe, w szczególności w sprawach dotyczących zarządzania administracyjnego, w tym zawieszenia przekazania uprawnień organu powołującego oraz w sprawach budżetowych. Zarząd jest informowany bez zbędnej zwłoki o wszelkich takich decyzjach tymczasowych. Zarząd podejmuje następnie decyzję o zatwierdzeniu lub odrzuceniu danej decyzji tymczasowej w ciągu nie później niż trzy miesiące od daty jej przyjęcia. Rada Wykonawcza nie może przyjmować w imieniu Zarządu decyzji, które wymagają zatwierdzenia przez większość dwóch trzecich głosów członków Zarządu.

Sekcja 3

Dyrektor Wykonawczy

Artykuł 20

Obowiązki Dyrektora Wykonawczego

1. ENISA kieruje Dyrektor Wykonawczy, który zachowuje niezależność podczas wykonywania 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, by złożył sprawozdanie z wykonywania swoich obowiązków.

3. Dyrektor Wykonawczy odpowiada za:

a) bieżące zarządzanie ENISA;

b) wykonanie decyzji przyjętych przez Zarząd;

c) przygotowanie projektu jednolitego dokumentu programowego i przedłożenie go Zarządowi do zatwierdzenia, zanim zostanie on przedłożony Komisji;

d) realizowanie jednolitego dokumentu programowego i składanie sprawozdań Zarządowi w tym zakresie;

e) przygotowanie skonsolidowanego sprawozdania rocznego z działalności ENISA, w tym z realizacji rocznego programu prac ENISA, i przedstawienie go Zarządowi do oceny i przyjęcia;

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

g) przygotowanie planu działania w następstwie wniosków ze sprawozdań z kontroli wewnętrznej lub zewnętrznej, a także dochodzeń przeprowadzanych przez OLAF oraz składanie Komisji dwa razy w roku sprawozdania z postępów prac, a Zarządowi – regularnie;

h) przygotowanie projektu przepisów finansowych mających zastosowanie do ENISA, zgodnie z art. 32;

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

j) chronienie interesów finansowych Unii poprzez stosowanie środków zapobiegających nadużyciom finansowym, korupcji i wszelkim innym niezgodnym z prawem 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 ENISA na rzecz przeciwdziałania nadużyciom finansowym i przedstawienie jej Zarządowi do zatwierdzenia;

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

m) regularne wymienianie poglądów i informacji z instytucjami, organami i jednostkami organizacyjnymi Unii w odniesieniu do ich działalności związanej z cyberbezpieczeństwem w celu zapewnienia spójności w zakresie opracowywania i wdrażania polityki Unii;

n) realizowanie innych zadań powierzonych Dyrektorowi Wykonawczemu na mocy niniejszego rozporządzenia.

4. W razie potrzeby oraz w ramach celów i zadań ENISA Dyrektor Wykonawczy może tworzyć grupy robocze *ad hoc* złożone z ekspertów, w tym ekspertów reprezentujących właściwe organy państw członkowskich. Dyrektor Wykonawczy informuje o tym z wyprzedzeniem Zarząd. Procedury dotyczące w szczególności składu grup roboczych, powoływania ekspertów grup roboczych przez Dyrektora Wykonawczego oraz działania grup roboczych określa się w wewnętrznych zasadach działania ENISA.

5. W razie potrzeby, do celów wykonywania zadań ENISA w skuteczny i wydajny sposób i w oparciu o odpowiednią analizę kosztów i korzyści, Dyrektor Wykonawczy może podjąć decyzję o utworzeniu jednego lub kilku lokalnych biur w jednym lub kilku państwach członkowskich. Przed podjęciem decyzji o utworzeniu biura lokalnego Dyrektor Wykonawczy zasięga opinii zainteresowanych państw członkowskich, w tym państwa członkowskiego, w którym ENISA ma siedzibę oraz uzyskuje wcześniejszą zgodę Komisji i Zarządu. Jeśli w procesie konsultacji pomiędzy Dyrektorem Wykonawczym a zainteresowanymi państwami członkowskimi nie można osiągnąć porozumienia, kwestia ta zostaje poddana pod obrady Rady. Łączna liczba personelu we wszystkich biurach lokalnych jest utrzymywana na minimalnym poziomie i nie może przekraczać 40 % całkowitej liczby personelu ENISA pracującego w państwie członkowskim, w którym ENISA ma siedzibę. Liczba personelu w każdym z biur lokalnych nie może przekraczać 10 % całkowitej liczby personelu ENISA pracującego w państwie członkowskim, w którym ENISA ma siedzibę.

W decyzji ustanawiającej biuro lokalne określa się zakres działalności prowadzonej w tym biurze lokalnym w sposób pozwalający uniknąć niepotrzebnych kosztów i powielania administracyjnych funkcji ENISA.

Sekcja 4

Grupa Doradcza ENISA, Grupa Interesariuszy ds. Certyfikacji Bezpieczeństwa i Sieć Krajowych Urzędników Łącznikowych

Artykuł 21

Grupa Doradcza ENISA

1. Zarząd, działając na wniosek Dyrektora Wykonawczego, ustanawia w przejrzysty sposób Grupę Doradczą ENISA składającą się z uznanych ekspertów reprezentujących odpowiednich interesariuszy z takich obszarów, jak sektor ICT, dostawcy publicznie dostępnych sieci lub usług łączności elektronicznej, MŚP, operatorzy usług kluczowych, grupy konsumenckie, eksperci akademiccy w dziedzinie cyberbezpieczeństwa oraz przedstawiciele właściwych organów będących przedmiotem powiadomienia zgodnie z dyrektywą (UE) 2018/1972, europejskie organizacje normalizacyjne, a także organy ścigania i organy nadzorcze ds. ochrony danych. Zarząd stara się zapewnić odpowiednią równowagę płci i równowagę geograficzną, a także równowagę pomiędzy poszczególnymi grupami interesariuszy.

2. Procedury dotyczące Grupy Doradczej ENISA, w szczególności dotyczące jej składu, wniosku Dyrektora Wykonawczego, o którym mowa w ust. 1, liczby i powoływania jej członków oraz jej działania, określa się w wewnętrznych zasadach działania ENISA i podaje do wiadomości publicznej.

3. Grupie Doradczej ENISA przewodniczy Dyrektor Wykonawczy lub inna osoba wyznaczona w danym przypadku przez Dyrektora Wykonawczego.

4. Kadencja członków Grupy Doradczej ENISA trwa dwa i pół roku. Członkowie Zarządu nie mogą być członkami Grupy Doradczej ENISA. Eksperci z Komisji i z państw członkowskich są uprawnieni do udziału w posiedzeniach i pracach Grupy Doradczej ENISA. Przedstawiciele innych organów uznanych przez Dyrektora Wykonawczego za istotne, którzy nie są członkami Grupy Doradczej ENISA, mogą być zapraszani na posiedzenia Grupy Doradczej ENISA i uczestniczyć w jej pracach.

5. Grupa Doradcza ENISA doradza ENISA w związku z realizacją jej działań, z wyjątkiem stosowania przepisów tytułu III niniejszego rozporządzenia. Grupa doradza w szczególności Dyrektorowi Wykonawczemu w sprawie sporządzenia wniosku dotyczącego programu prac ENISA oraz w sprawie zapewnienia komunikacji z odpowiednimi interesariuszami w kwestiach związanych z rocznym programem prac.

6. Grupa Doradcza ENISA regularnie informuje Zarząd o swoich działaniach.

Artykuł 22

Grupa Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa

1. Ustanawia się Grupę Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa.

2. Grupa Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa składa się z członków wybranych spośród uznanych ekspertów reprezentujących odpowiednich interesariuszy. Komisja po wystosowaniu przejrzystego i otwartego zaproszenia dokonuje wyboru, na podstawie propozycji przedstawionych przez ENISA, członków Grupy Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa, zapewniając równowagę pomiędzy poszczególnymi grupami interesariuszy, a także odpowiednią równowagę płci i równowagę geograficzną.

3. Grupa Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa:

a) doradza Komisji w sprawie strategicznych kwestii związanych z europejskimi ramami certyfikacji cyberbezpieczeństwa;

b) doradza ENISA, na wniosek, w kwestiach ogólnych i strategicznych dotyczących zadań ENISA związanych z rynkiem, certyfikacją cyberbezpieczeństwa i standaryzacją;

c) wspiera Komisję w przygotowywaniu unijnego kroczącego programu prac, o którym mowa w art. 47;

d) wydaje opinie na temat unijnego kroczącego programu prac na podstawie art. 47 ust. 4; oraz

e) doradza, w pilnych przypadkach, Komisji i ECCG w zakresie potrzeby dodatkowych programów certyfikacji nieujętych w unijnym kroczącym programie prac, o czym mowa w art. 47 i 48.

4. Grupie Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa współprzewodniczą przedstawiciele Komisji i ENISA, a obsługę jej sekretariat zapewnia ENISA.

Artykuł 23

Sieć Krajowych Urzędników Łącznikowych

1. Zarząd, działając na wniosek Dyrektora Wykonawczego, tworzy Sieć Krajowych Urzędników Łącznikowych, w skład której wchodzą przedstawiciele wszystkich państw członkowskich (krajowi urzędnicy łącznikowi). Państwa członkowskie powołują do Sieci Krajowych Urzędników Łącznikowych po jednym przedstawicielu. Posiedzenia Sieci Krajowych Urzędników Łącznikowych mogą odbywać się w różnych konfiguracjach eksperckich.

2. Sieć Krajowych Urzędników Łącznikowych ma w szczególności ułatwiać wymianę informacji pomiędzy ENISA a państwami członkowskimi i wspierać ENISA w rozpowszechnianiu działalności, ustaleń i zaleceń ENISA wśród odpowiednich interesariuszy w całej Unii.

3. Sieć Krajowych Urzędników Łącznikowych pełni funkcję punktu kontaktowego na poziomie krajowym, by ułatwiać współpracę ENISA i ekspertów krajowych w kontekście realizacji rocznego programu prac ENISA.

4. O ile krajowi urzędnicy łącznikowi muszą ściśle współpracować z pochodzącymi z ich państwa członkowskich przedstawicielami Zarządu, to sama Sieć Krajowych Urzędników Łącznikowych nie może powielać działań Zarządu ani działań prowadzonych na innych forach Unii.

5. Zadania i procedury Sieci Krajowych Urzędników Łącznikowych określa się w wewnętrznych zasadach działania ENISA i podaje do wiadomości publicznej.

Sekcja 5

Działanie

Artykuł 24

Jednolity dokument programowy

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

2. Każdego roku Dyrektor Wykonawczy sporządza projekt jednolitego dokumentu programowego obejmującego programowanie roczne i wieloletnie wraz z odpowiadającym mu planowaniem zasobów finansowych i ludzkich zgodnie z art. 32 rozporządzenia delegowanego Komisji (UE) nr 1271/2013 ([25]) 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 do dnia 31 stycznia następnego roku przekazuje go, a także wszelkie późniejsze zaktualizowane wersje tego dokumentu, Parlamentowi Europejskiemu, Radzie i Komisji.

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

([25]) 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).

5. Roczny program prac zawiera szczegółowe cele i oczekiwane wyniki, w tym wskaźniki skuteczności działania. Zawiera on również opis działań, które mają być finansowane, oraz wskazanie zasobów finansowych i ludzkich przeznaczonych na każde działanie 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 wskazuje on zadania, które zostały dodane, zmienione lub usunięte w stosunku do poprzedniego roku budżetowego.

6. Zarząd dokonuje zmiany przyjętego rocznego programu prac w przypadku powierzenia ENISA 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 wyniki i wskaźniki skuteczności działania. Określa 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, gdy tylko zachodzi taka potrzeba, w szczególności zaś gdy jest to niezbędne w celu uwzględnienia wyników oceny, o której mowa w art. 67.

Artykuł 25

Deklaracja interesów

1. Członkowie Zarządu, Dyrektor Wykonawczy oraz urzędnicy oddelegowani czasowo przez państwa członkowskie składają deklarację dotyczącą zobowiązań oraz deklarację wskazującą na brak lub istnienie jakichkolwiek bezpośrednich lub pośrednich interesów, które mogłyby zostać uznane za wpływające na ich niezależność. Deklaracje te muszą być prawdziwe i kompletne; składane są co roku na piśmie oraz aktualizowane, gdy tylko zajdzie taka konieczność.

2. Członkowie Zarządu, Dyrektor Wykonawczy i eksperci zewnętrzni uczestniczący w grupach roboczych *ad hoc* zgłaszają w sposób prawidłowy i kompletny, najpóźniej na początku każdego posiedzenia, wszelkie interesy, które mogłyby zostać uznane za szkodzące ich niezależności w odniesieniu do punktów porządku obrad, oraz powstrzymują się od udziału w dyskusjach i głosowaniach dotyczących tych punktów.

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

Artykuł 26

Przejrzystość

1. ENISA prowadzi swoje działania z zachowaniem wysokiego stopnia przejrzystości oraz zgodnie z art. 28.

2. ENISA zapewnia, aby ogół społeczeństwa i wszelkie inne zainteresowane strony otrzymywały odpowiednie, obiektywne, wiarygodne i łatwo dostępne informacje, w szczególności dotyczące wyników jej pracy. ENISA podaje również do wiadomości publicznej deklaracje interesów złożone zgodnie z art. 25.

3. Zarząd, działając na wniosek Dyrektora Wykonawczego, może upoważnić zainteresowane strony do obserwowania przebiegu niektórych działań ENISA.

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

Artykuł 27

Poufność

1. Bez uszczerbku dla art. 28, ENISA nie może ujawniać stronom trzecim przetwarzanych lub otrzymywanych przez siebie informacji, w odniesieniu do których zgłoszono uzasadniony wniosek o zachowanie poufności.

2. Członkowie Zarządu, Dyrektor Wykonawczy, członkowie Grupy Doradczej ENISA, eksperci zewnętrzni uczestniczący w pracach grup roboczych *ad hoc* oraz członkowie personelu ENISA, w tym również urzędnicy oddelegowani czasowo przez państwa członkowskie, podlegają wymogom dotyczącym poufności określonym w art. 339 TFUE, także po zakończeniu pełnienia swoich obowiązków.

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

4. Jeżeli wymaga tego realizacja zadań ENISA, Zarząd zezwala ENISA na korzystanie z informacji niejawnych. W takim przypadku ENISA, w porozumieniu ze służbami Komisji, przyjmuje przepisy bezpieczeństwa, wprowadzając zasady bezpieczeństwa określone w decyzjach Komisji (UE, Euratom) 2015/443 ([26]) i 2015/444 ([27]). Te przepisy bezpieczeństwa obejmują przepisy dotyczące wymiany, przetwarzania i przechowywania informacji niejawnych.

Artykuł 28

Dostęp do dokumentów

1. Do dokumentów pozostających w posiadaniu ENISA stosuje się rozporządzenie (WE) nr 1049/2001.

2. Zarząd przyjmuje ustalenia dotyczące wykonywania rozporządzenia (WE) nr 1049/2001 do dnia 28 grudnia 2019 r.

3. Decyzje przyjęte przez ENISA 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 spraw kierowanych do Trybunału Sprawiedliwości Unii Europejskiej na podstawie art. 263 TFUE.

ROZDZIAŁ IV

Ustanowienie i struktura budżetu ENISA

Artykuł 29

Ustanowienie budżetu ENISA

1. Każdego roku Dyrektor Wykonawczy sporządza projekt preliminarza dochodów i wydatków ENISA na następny rok budżetowy 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, preliminarz dochodów i wydatków ENISA na następny rok budżetowy.

3. Do dnia 31 stycznia każdego roku Zarząd przesyła Komisji oraz państwom trzecim, z którymi Unia zawarła umowy, o których mowa w art. 42 ust. 2, preliminarz, stanowiący część projektu jednolitego dokumentu programowego.

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

5. Parlament Europejski i Rada zatwierdzają środki na wkład Unii na rzecz ENISA.

6. Parlament Europejski i Rada przyjmują plan zatrudnienia ENISA.

([26]) 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).

([27]) 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).

7. Zarząd przyjmuje budżet ENISA wraz z jednolitym dokumentem programowym. Budżet ENISA staje się ostateczny po ostatecznym przyjęciu budżetu ogólnego Unii. W razie potrzeby Zarząd dokonuje korekty budżetu ENISA i jednolitego dokumentu programowego ENISA zgodnie z budżetem ogólnym Unii.

Artykuł 30

Struktura budżetu ENISA

1. Na dochody ENISA – bez uszczerbku dla innych zasobów – składają się:

a) wkład z budżetu ogólnego Unii;

b) dochody przypisane do określonych pozycji wydatków zgodnie z przepisami finansowymi ENISA, o których mowa w art. 32;

c) finansowanie unijne w formie umów o delegowaniu zadań lub dotacji *ad hoc* zgodnie z przepisami finansowymi ENISA, o których mowa w art. 32, oraz postanowieniami odpowiednich instrumentów wspierających politykę Unii;

d) wkłady państw trzecich uczestniczących w pracach ENISA zgodnie z art. 42;

e) wszelkie dobrowolne finansowe lub rzeczowe wkłady państw członkowskich.

Państwa członkowskie dobrowolnie wnoszące wkłady na podstawie akapitu pierwszego lit. e) nie mogą domagać się przyznania im w zamian żadnych specjalnych praw ani usług.

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

Artykuł 31

Wykonanie budżetu ENISA

1. Za wykonanie budżetu ENISA odpowiedzialny jest Dyrektor Wykonawczy.

2. Audytor wewnętrzny Komisji ma te same uprawnienia wobec ENISA co wobec departamentów Komisji.

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

4. Po otrzymaniu uwag Trybunału Obrachunkowego dotyczących wstępnego sprawozdania finansowego ENISA zgodnie z art. 246 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 ([28]) księgowy ENISA sporządza na swoją odpowiedzialność końcowe sprawozdanie finansowe ENISA i przedkłada je Zarządowi do zaopiniowania.

5. Zarząd wydaje opinię na temat końcowego sprawozdania finansowego ENISA.

6. Do dnia 31 marca roku N + 1 Dyrektor Wykonawczy przekazuje sprawozdanie z zarządzania budżetem i finansami Parlamentowi Europejskiemu, Radzie, Komisji i Trybunałowi Obrachunkowemu.

7. Do dnia 1 lipca roku N + 1 księgowy ENISA przekazuje końcowe sprawozdanie finansowe ENISA wraz z opinią Zarządu Parlamentowi Europejskiemu, Radzie, księgowemu Komisji i Trybunałowi Obrachunkowemu.

([28]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012 (Dz.U. L 193 z 30.7.2018, s. 1).

8. Księgowy ENISA, w tym samym dniu, w którym przekazuje końcowe sprawozdanie finansowe ENISA, przesyła Trybunałowi Obrachunkowemu – wraz z kopią dla księgowego Komisji – również oświadczenie dotyczące tego końcowego sprawozdania finansowego.

9. Do dnia 15 listopada roku N+1 Dyrektor Wykonawczy publikuje końcowe sprawozdanie finansowe ENISA w *Dzienniku Urzędowym Unii Europejskiej*.

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 zastosowania procedury udzielania absolutorium za dany rok budżetowy, zgodnie z art. 261 ust. 3 rozporządzenia (UE, Euratom) 2018/1046.

12. Parlament Europejski, stanowiąc na podstawie zalecenia Rady, udziela Dyrektorowi Wykonawczemu, przed dniem 15 maja roku N + 2, absolutorium z wykonania budżetu za rok N.

Artykuł 32

Przepisy finansowe

Przepisy finansowe mające zastosowanie do ENISA przyjmuje Zarząd po konsultacji z Komisją. Przepisy te nie mogą różnić się od rozporządzenia delegowanego (UE) nr 1271/2013, chyba że takie różnice są specjalnie wymagane dla działania ENISA, a Komisja wydała na nie uprzednią zgodę.

Artykuł 33

Zwalczanie nadużyć finansowych

1. W celu ułatwienia zwalczania nadużyć finansowych, korupcji i innych niezgodnych z prawem działań na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 ([29]) ENISA przystąpi, do dnia 28 grudnia 2019 r., do porozumienia międzyinstytucjonalnego z dnia 25 maja 1999 r. między Parlamentem Europejskim, Radą Unii Europejskiej i Komisją Wspólnot Europejskich dotyczącego dochodzeń wewnętrznych prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) ([30]). ENISA przyjmie odpowiednie przepisy mające zastosowanie do wszystkich pracowników ENISA, wykorzystując w tym celu wzór określony w załączniku do tego porozumienia.

2. Trybunał Obrachunkowy jest uprawniony do przeprowadzania audytu – na podstawie dokumentów oraz inspekcji na miejscu – wszystkich beneficjentów dotacji, wykonawców i podwykonawców, którzy otrzymują od ENISA unijne środki finansowe.

3. OLAF może prowadzić dochodzenia, w tym kontrole na miejscu i inspekcje, zgodnie z przepisami i procedurami określonymi w rozporządzeniu (UE, Euratom) nr 883/2013 oraz w rozporządzeniu Rady (Euratom, WE) nr 2185/96 ([31]), aby ustalić, czy miało miejsce nadużycie finansowe, korupcja lub jakakolwiek inna nielegalna działalność ze szkodą dla interesów finansowych Unii w związku z finansowaniem przez ENISA dotacji lub umowy.

4. Bez uszczerbku dla ust. 1, 2 i 3, w zawieranych przez ENISA umowach o współpracy z państwami trzecimi lub 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 kompetencjami.

([29]) 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).
([30]) Dz.U. L 136 z 31.5.1999, s. 15.
([31]) Rozporządzenie Rady (Euratom, WE) nr 2185/96 z dnia 11 listopada 1996 r. w sprawie kontroli na miejscu oraz inspekcji przeprowadzanych przez Komisję w celu ochrony interesów finansowych Wspólnot Europejskich przed nadużyciami finansowymi i innymi nieprawidłowościami (Dz.U. L 292 z 15.11.1996, s. 2).

ROZDZIAŁ V

Personel

Artykuł 34

Przepisy ogólne

Do personelu ENISA stosuje się regulamin pracowniczy urzędników i warunki zatrudnienia innych pracowników, jak również przepisy przyjęte w drodze porozumienia między instytucjami Unii w celu nadania skuteczności regulaminowi pracowniczemu urzędników i warunkom zatrudnienia innych pracowników.

Artykuł 35

Przywileje i immunitety

Do ENISA i jej personelu stosuje się Protokół nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej, załączony do TUE i do TFUE.

Artykuł 36

Dyrektor Wykonawczy

1. Dyrektor Wykonawczy jest zatrudniony w ENISA 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 o pracę z Dyrektorem Wykonawczym ENISA reprezentuje przewodniczący Zarządu.

4. Przed powołaniem kandydat wybrany przez Zarząd jest wzywany do złożenia oświadczenia przed odpowiednią komisją Parlamentu Europejskiego i udzielenia odpowiedzi na pytania posłów.

5. Kadencja Dyrektora Wykonawczego trwa pięć lat. Przed upływem tego okresu Komisja przeprowadza ocenę wykonywania zadań przez Dyrektora Wykonawczego oraz przyszłe zadania i wyzwania ENISA.

6. Zarząd podejmuje decyzje w sprawie powołania, przedłużenia kadencji lub odwołania ze stanowiska Dyrektora Wykonawczego zgodnie z art. 18 ust. 2.

7. Zarząd, działając na wniosek Komisji uwzględniający ocenę, o której mowa w ust. 5, może przedłużyć kadencję Dyrektora Wykonawczego jednokrotnie, na okres pięciu lat.

8. Zarząd informuje Parlament Europejski o swoim zamiarze przedłużenia kadencji Dyrektora Wykonawczego. W ciągu trzech miesięcy poprzedzających takie przedłużenie Dyrektor Wykonawczy, jeżeli zostanie wezwany, składa oświadczenie przed odpowiednią komisją Parlamentu Europejskiego i udziela odpowiedzi na pytania posłów.

9. Dyrektor Wykonawczy, którego kadencję przedłużono, nie może brać udziału w kolejnej procedurze selekcji na to samo stanowisko.

10. Dyrektor Wykonawczy może zostać odwołany ze stanowiska jedynie na mocy decyzji Zarządu działającego na wniosek Komisji.

Artykuł 37

Oddelegowani eksperci krajowi i inni członkowie personelu

1. ENISA może korzystać z pomocy oddelegowanych ekspertów krajowych lub innych członków personelu niezatrudnionych przez ENISA. Do takich członków personelu nie stosuje się regulaminu pracowniczego urzędników ani warunków zatrudnienia innych pracowników.

2. Zarząd przyjmuje decyzję określającą zasady oddelegowania ekspertów krajowych do ENISA.

ROZDZIAŁ VI

Przepisy ogólne dotyczące ENISA

Artykuł 38

Status prawny ENISA

1. ENISA jest organem Unii i ma osobowość prawną.

2. ENISA ma, w każdym państwie członkowskim, najszerszy zakres zdolności prawnej, jaki można nadać osobie prawnej na mocy prawa krajowego. W szczególności ENISA może nabywać lub zbywać ruchomości i nieruchomości oraz być stroną w postępowaniach sądowych.

3. ENISA jest reprezentowana przez Dyrektora Wykonawczego.

Artykuł 39

Odpowiedzialność ENISA

1. Odpowiedzialność umowną ENISA reguluje prawo właściwe dla danej umowy.

2. Sądem właściwym do rozstrzygania sporów na podstawie klauzuli arbitrażowej zamieszczonej w umowie zawartej przez ENISA jest Trybunał Sprawiedliwości Unii Europejskiej.

3. W przypadku odpowiedzialności pozaumownej ENISA naprawia wszelkie szkody wyrządzone przez nią lub członków jej personelu w trakcie wykonywania ich obowiązków, zgodnie z ogólnymi zasadami wspólnymi dla prawa państw członkowskich.

4. Sądem właściwym do orzekania we wszelkich sporach dotyczących odszkodowania za szkody, o czym mowa w ust. 3, jest Trybunał Sprawiedliwości Unii Europejskiej.

5. Odpowiedzialność osobistą członków personelu ENISA wobec ENISA regulują odpowiednie warunki mające zastosowanie do personelu ENISA.

Artykuł 40

System językowy

1. Do ENISA stosuje się rozporządzenie Rady nr 1 ([32]). Państwa członkowskie i inne organy wyznaczone przez państwa członkowskie mogą zwracać się do ENISA i otrzymywać odpowiedzi w wybranym przez nie języku urzędowym instytucji Unii.

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

Artykuł 41

Ochrona danych osobowych

1. Do przetwarzania danych osobowych przez ENISA stosuje się rozporządzenie (UE) 2018/1725.

2. Zarząd przyjmuje dalsze przepisy wykonawcze, o których mowa w art. 45 ust. 3 rozporządzenia (UE) 2018/1725. Zarząd może przyjąć dodatkowe środki niezbędne do stosowania przez ENISA rozporządzenia (UE) 2018/1725.

([32]) Rozporządzenie nr 1 w sprawie określenia systemu językowego Europejskiej Wspólnoty Gospodarczej (Dz.U. 17 z 6.10.1958, s. 385).

Artykuł 42

Współpraca z państwami trzecimi i organizacjami międzynarodowymi

1. W zakresie, w jakim jest to niezbędne do osiągnięcia celów określonych w niniejszym rozporządzeniu, ENISA może współpracować z właściwymi organami państw trzecich lub z organizacjami międzynarodowymi. W tym celu ENISA może, pod warunkiem uzyskania uprzedniej zgody Komisji, dokonywać ustaleń roboczych z organami państw trzecich i organizacjami międzynarodowymi. Takie ustalenia robocze nie mogą tworzyć zobowiązań prawnych dla Unii ani jej państw członkowskich.

2. ENISA jest otwarta na udział państw trzecich, które zawarły w tym celu umowy z Unią. Na podstawie odpowiednich postanowień takich umów dokonuje się ustaleń roboczych określających w szczególności charakter, zakres i sposób uczestniczenia tych państw trzecich w pracach ENISA, które zawierają postanowienia dotyczące udziału w inicjatywach podejmowanych przez ENISA, wkładów finansowych oraz członków personelu. W odniesieniu do kwestii dotyczących personelu ustalenia robocze muszą być w każdym przypadku zgodne z regulaminem pracowniczym urzędników oraz warunkami zatrudnienia innych pracowników.

3. Zarząd przyjmuje strategię dotyczącą stosunków z państwami trzecimi i organizacjami międzynarodowymi dotyczącą spraw pozostających w kompetencji ENISA. Komisja zapewnia działanie ENISA w ramach jej mandatu i istniejących ram instytucjonalnych, zawierając odpowiednie ustalenia robocze z Dyrektorem Wykonawczym ENISA.

Artykuł 43

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

Po konsultacji z Komisją ENISA przyjmuje przepisy bezpieczeństwa wprowadzające zasady bezpieczeństwa zawarte w przepisach bezpieczeństwa Komisji dotyczących ochrony szczególnie chronionych informacji jawnych i EUCI, określonych w decyzjach (UE, Euratom) 2015/443 i 2015/444. Przepisy bezpieczeństwa ENISA zawierają przepisy dotyczące wymiany, przetwarzania i przechowywania takich informacji.

Artykuł 44

Umowa w sprawie siedziby i warunki działania

1. Niezbędne ustalenia dotyczące pomieszczeń, które przyjmujące państwo członkowskie ma przeznaczyć dla ENISA, 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, personelu ENISA i członków ich rodzin określa się w umowie w sprawie siedziby pomiędzy ENISA a przyjmującym państwem członkowskim, zawartej po uzyskaniu zgody Zarządu.

2. Państwo członkowskie przyjmujące ENISA zapewnia możliwie najlepsze warunki dla zapewnienia właściwego funkcjonowania ENISA, biorąc pod uwagę 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 członków personelu.

Artykuł 45

Kontrola administracyjna

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

TYTUŁ III

RAMY CERTYFIKACJI CYBERBEZPIECZEŃSTWA

Artykuł 46

Europejskie ramy certyfikacji cyberbezpieczeństwa

1. Ustanawia się europejskie ramy certyfikacji cyberbezpieczeństwa w celu poprawy warunków funkcjonowania rynku wewnętrznego poprzez zwiększenie poziomu cyberbezpieczeństwa w Unii oraz umożliwienia zharmonizowanego podejścia na poziomie unijnym do europejskich programów certyfikacji cyberbezpieczeństwa z myślą o stworzeniu jednolitego rynku cyfrowego w zakresie produktów ICT, usług ICT i procesów ICT.

2. Europejskie ramy certyfikacji cyberbezpieczeństwa określają mechanizm ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa i potwierdzania, że produkty ICT, usługi ICT i procesy ICT, które oceniono zgodnie z tymi programami, są zgodne z określonymi wymogami bezpieczeństwa mającymi na celu zabezpieczenia dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych bądź funkcji lub usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia.

Artykuł 47

Unijny kroczący program prac na rzecz europejskich programów certyfikacji cyberbezpieczeństwa

1. Komisja publikuje unijny kroczący program prac na rzecz europejskich programów certyfikacji cyberbezpieczeństwa (zwany dalej „unijnym kroczącym programem prac") wskazujący strategiczne priorytety przyszłych europejskich programów certyfikacji cyberbezpieczeństwa.

2. Unijny kroczący program prac zawiera w szczególności wykaz produktów ICT, usług ICT i procesów ICT lub ich kategorie, które mają możliwość korzystania z włączenia w zakres stosowania danego europejskiego programu certyfikacji cyberbezpieczeństwa.

3. Objęcie określonych produktów ICT, usług ICT i procesów ICT lub ich kategorii unijnym kroczącym programem prac musi być uzasadnione jedną z poniższych przesłanek:

a) obecność i rozwój krajowych programów certyfikacji cyberbezpieczeństwa obejmujących określoną kategorię produktów ICT, usług ICT lub procesów ICT, w szczególności w odniesieniu do ryzyka rozdrobnienia;

b) odpowiednie przepisy lub polityki Unii lub państwa członkowskiego;

c) popyt na rynku;

d) zmiany w zakresie profilu cyberzagrożeń; lub

e) wniosek ECCG o przygotowanie konkretnej propozycji programu.

4. Komisja należycie uwzględnia opinie wydane przez ECCG i Grupę Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa na temat projektu unijnego kroczącego programu prac.

5. Pierwszy unijny kroczący program prac publikuje się do dnia 28 czerwca 2020 r. Unijny kroczący program prac jest aktualizowany co najmniej raz na trzy lata, a w razie konieczności częściej.

Artykuł 48

Wniosek o europejski program certyfikacji cyberbezpieczeństwa

1. Komisja może zwrócić się do ENISA z wnioskiem o przygotowanie propozycji programu lub o przegląd istniejącego europejskiego programu cyberbezpieczeństwa, na podstawie unijnego kroczącego programu prac.

2. W należycie uzasadnionych przypadkach Komisja lub ECCG mogą zwrócić się do ENISA z wnioskiem o przygotowanie propozycji programu lub o przegląd istniejącego europejskiego programu certyfikacji cyberbezpieczeństwa nieobjętego unijnym kroczącym programem prac. Unijny kroczący program prac jest odpowiednio aktualizowany.

Artykuł 49

Przygotowanie, przyjęcie i przegląd europejskiego programu certyfikacji cyberbezpieczeństwa

1. Po otrzymaniu wniosku Komisji na podstawie art. 48 ENISA przygotowuje propozycję programu spełniającego wymogi określone w art. 51, 52 i 54.

2. Po otrzymaniu wniosku ECCG na podstawie art. 48 ust. 2 ENISA może przygotować propozycję programu spełniającego wymogi określone w art. 51, 52 i 54. Jeżeli ENISA odmawia uwzględnienia takiego wniosku, uzasadnia ona swoją odmowę. Każda decyzja o odmowie uwzględnienia wniosku jest przyjmowana przez Zarząd.

3. Przygotowując propozycję programu, ENISA konsultuje się ze wszystkimi odpowiednimi interesariuszami w drodze formalnego, otwartego, przejrzystego i integracyjnego procesu konsultacji.

4. Dla każdej propozycji programu ENISA ustanawia grupę roboczą *ad hoc* zgodnie z art. 20 ust. 4, której celem jest służenie ENISA doradztwem i wiedzą fachową.

5. ENISA ściśle współpracuje z ECCG. ECCG zapewnia ENISA pomoc i fachowe doradztwo w związku z przygotowywaniem propozycji programu oraz przyjmuje opinię na temat takiej propozycji programu.

6. ENISA w możliwie największym stopniu uwzględnia opinię ECCG przed przekazaniem Komisji propozycji programu przygotowanej zgodnie z ust. 3, 4 i 5. Opinia ECCG nie jest wiążąca dla ENISA, a jej brak nie uniemożliwia ENISA przekazania Komisji propozycji programu.

7. Komisja, w oparciu o propozycję programu przygotowaną przez ENISA, może przyjmować akty wykonawcze ustanawiające europejski program certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT spełniający wymogi określone w art. 51, 52 i 54. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 66 ust. 2.

8. ENISA przynajmniej raz na 5 lat dokonuje oceny każdego przyjętego europejskiego programu certyfikacji cyberbezpieczeństwa, biorąc pod uwagę informacje zwrotne otrzymane od zainteresowanych stron. W razie potrzeby, Komisja lub ECCG mogą zwrócić się do ENISA z wnioskiem o rozpoczęcie procesu opracowania zmienionej propozycji programu zgodnie z art. 48 i niniejszym artykułem.

Artykuł 50

Strona internetowa dotycząca europejskich programów certyfikacji cyberbezpieczeństwa

1. ENISA prowadzi specjalną stronę internetową, na której znajdują się informacje na temat europejskich programów certyfikacji cyberbezpieczeństwa, europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności, w tym informacje dotyczące nieważnych europejskich programów certyfikacji cyberbezpieczeństwa oraz europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności, które zostały cofnięte lub wygasły, a także repozytorium linków do informacji o cyberbezpieczeństwie przekazanych zgodnie z art. 55; strona ta popularyzuje również te programy, certyfikaty i deklaracje.

2. W stosownych przypadkach strona internetowa, o której mowa w ust. 1, wskazuje również krajowe programy certyfikacji cyberbezpieczeństwa, które zostały zastąpione europejskim programem certyfikacji cyberbezpieczeństwa.

Artykuł 51

Cele bezpieczeństwa europejskich programów certyfikacji cyberbezpieczeństwa

Europejski program certyfikacji cyberbezpieczeństwa musi być zaprojektowany tak, aby – w stosownych przypadkach – osiągać co najmniej następujące cele bezpieczeństwa:

a) chronić – podczas całego cyklu życia produktu ICT, usługi ICT lub procesu ICT – przechowywane, przekazywane lub w inny sposób przetwarzane dane przed przypadkowym lub nieuprawnionym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem;

b) chronić – podczas całego cyklu życia produktu ICT, usługi ICT lub procesu ICT – przechowywane, przekazywane lub w inny sposób przetwarzane dane przed przypadkowym lub nieuprawnionym zniszczeniem, utratą, zmianą lub brakiem dostępności;

c) aby uprawnione osoby, programy lub maszyny miały dostęp tylko do tych danych, usług lub funkcji, do których odnoszą się ich prawa dostępu;

d) aby znane zależności i podatności zostały zidentyfikowane i udokumentowane;

e) rejestrować, 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) umożliwiać kontrolę, 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;

g) sprawdzać, czy produkty ICT, usługi ICT i procesy ICT nie zawierają znanych podatności;

h) przywracać w odpowiednim czasie dostępność danych, usług i funkcji oraz dostęp do nich w przypadku incydentu fizycznego lub technicznego;

i) aby bezpieczeństwo produktów ICT, usług ICT i procesów ICT było bezpieczeństwem domyślnym i było uwzględniane już na etapie projektowania;

j) aby produkty ICT, usługi ICT i procesy ICT były oferowane wraz z aktualnym oprogramowaniem i sprzętem niezawierającym powszechnie znanych podatności oraz wraz z mechanizmami do dokonywania bezpiecznych aktualizacji.

Artykuł 52

Poziomy uzasadnienia zaufania europejskich programów certyfikacji cyberbezpieczeństwa

1. Europejski program certyfikacji cyberbezpieczeństwa może przewidywać jeden lub więcej z następujących poziomów uzasadnienia zaufania produktów ICT, usług ICT i procesów ICT: „podstawowy", „istotny" lub „wysoki". Poziom uzasadnienia zaufania musi być proporcjonalny do poziomu ryzyka związanego z przewidzianym stosowaniem produktu ICT, usługi ICT lub procesu ICT pod względem prawdopodobieństwa wystąpienia i skutków incydentu.

2. Europejskie certyfikaty cyberbezpieczeństwa i unijne deklaracje zgodności muszą odwoływać się do poziomu uzasadnienia zaufania określonego w europejskim programie certyfikacji cyberbezpieczeństwa, w ramach którego wydany został europejski certyfikat cyberbezpieczeństwa lub unijna deklaracja zgodności.

3. Wymogi bezpieczeństwa, które odpowiadają poszczególnym poziomom uzasadnienia zaufania, muszą być określone w odpowiednich europejskich programach certyfikacji bezpieczeństwa, w tym odpowiadające im funkcjonalności bezpieczeństwa oraz odpowiadająca im rygorystyczność i wnikliwość oceny, której ma zostać poddany produkt ICT, usługa ICT lub proces ICT.

4. Certyfikat lub unijna deklaracja zgodności musi odwoływać się do związanych z nimi specyfikacji technicznych, norm i procedur, w tym kontroli technicznych mających na celu zmniejszenie ryzyka wystąpienia incydentów cyberbezpieczeństwa lub zapobieganie takim incydentom.

5. Europejski certyfikat cyberbezpieczeństwa lub unijna deklaracja zgodności, które odnoszą się do poziomu uzasadnienia zaufania „podstawowy", dają uzasadnione zaufanie, że produkty ICT, usługi ICT i procesy ICT, dla których wydany został ten certyfikat lub wydana została ta unijna deklaracji zgodności, spełniają odpowiadające im wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych podstawowych ryzyk w zakresie incydentów i cyberataków. Działania w zakresie oceny, jakie mają zostać podjęte, obejmują przynajmniej przegląd dokumentacji technicznej. W przypadku gdy taki przegląd nie jest odpowiedni, podejmuje się alternatywne działania w zakresie oceny, które mają równoważny skutek.

6. Europejski certyfikat cyberbezpieczeństwa, który odnosi się do poziomu uzasadnienia zaufania „istotny", daje uzasadnione zaufanie, że produkty ICT, usługi ICT i procesy ICT, dla których wydany został ten certyfikat, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych ryzyk w cyberprzestrzeni oraz ryzyka wystąpienia incydentów i cyberataków przeprowadzanych przez osoby o ograniczonych umiejętnościach i dysponujących niewielkimi zasobami. Działania w zakresie oceny, jakie mają zostać podjęte, obejmują co najmniej: sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności oraz testowanie w celu wykazania, że w produktach ICT, usługach ICT lub procesach ICT prawidłowo zaimplementowane zostały niezbędne funkcjonalności bezpieczeństwa. W przypadku gdy takie działania w zakresie oceny nie są odpowiednie podejmuje się alternatywne działania w zakresie oceny, które mają równoważny skutek.

7. Europejski certyfikat cyberbezpieczeństwa, który odnosi się do poziomu uzasadnienia zaufania „wysoki", daje uzasadnione zaufanie, że produkty ICT, usługi ICT i procesy ICT, dla których wydany został ten certyfikat, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały 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, jakie mają zostać podjęte, obejmują co najmniej: sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności; testowanie w celu wykazania, że w produktach ICT, usługach ICT lub procesach ICT prawidłowo zaimplementowane zostały niezbędne, nowoczesne funkcjonalności bezpieczeństwa; ocenę sprawdzającą za pomocą testów penetracyjnych ich odporność na zaawansowane ataki. W przypadku gdy takie działania w zakresie oceny nie są odpowiednie, podejmuje się alternatywne działania w zakresie oceny, które mają równoważny skutek.

8. Europejski program certyfikacji cyberbezpieczeństwa może przewidywać kilka poziomów oceny zależnie od tego, jak rygorystyczna i wnikliwa jest zastosowana metodyka oceny. Każdy z poziomów oceny odpowiada jednemu z poziomów uzasadnienia zaufania i jest określany poprzez odpowiedni zestaw komponentów uzasadnienia zaufania.

Artykuł 53

Ocena zgodności przez stronę pierwszą

1. Europejski program certyfikacji cyberbezpieczeństwa może zezwalać na ocenę zgodności przez stronę pierwszą przeprowadzaną na wyłączną odpowiedzialność wytwórcy lub dostawcy produktów ICT, usług ICT lub procesów ICT. Na ocenę zgodności przez stronę pierwszą zezwala się jedynie w przypadku produktów ICT, usług ICT lub procesów ICT, które stwarzają niewielkie ryzyko odpowiadające poziomowi uzasadnienia zaufania „podstawowy".

2. Wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT może wydać unijną deklarację zgodności stwierdzającą, że wykazano spełnienie wymogów określonych w programie. Wydając taką deklarację, wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT przyjmuje na siebie odpowiedzialność za zgodność produktu ICT, usługi ICT lub procesu ICT z wymogami określonymi w tym programie.

3. Wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT udostępnia – przez okres przewidziany w odpowiednim europejskim programie certyfikacji cyberbezpieczeństwa – krajowemu organowi ds. certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 ust. 1, unijną deklarację zgodności, dokumentację techniczną oraz wszelkie inne istotne informacje związane ze zgodnością produktów ICT lub usług ICT z programem. Kopię unijnej deklaracji zgodności przedkłada się krajowemu organowi ds. certyfikacji cyberbezpieczeństwa i ENISA.

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

5. Unijne deklaracje zgodności są uznawane we wszystkich państwach członkowskich.

Artykuł 54

Elementy europejskich programów certyfikacji cyberbezpieczeństwa

1. Europejski program certyfikacji cyberbezpieczeństwa obejmuje co najmniej następujące elementy:

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

b) jasny opis celu programu i tego, jak wybrane normy, metody oceny i poziomy uzasadnienia zaufania odpowiadają potrzebom przewidywanych użytkowników programu;

c) odesłanie do międzynarodowych, europejskich lub krajowych norm stosowanych podczas oceny lub, w przypadku braku takich norm lub gdy nie są one odpowiednie, odesłanie do specyfikacji technicznych spełniających wymogi określone w załączniku II do rozporządzenia (UE) nr 1025/2012 lub w przypadku braku takich specyfikacji odesłanie do specyfikacji technicznych lub innych wymogów cyberbezpieczeństwa określonych w tym europejskim programie certyfikacji cyberbezpieczeństwa;

d) w stosownych przypadkach jeden lub więcej poziomów uzasadnienia zaufania;

e) wskazanie, czy w ramach sytemu dozwolona jest ocena zgodności przez stronę pierwszą;

f) w stosownych przypadkach szczegółowe lub dodatkowe wymogi, którym podlegają jednostki oceniające zgodność w celu zagwarantowania ich kwalifikacji technicznych odnośnie do oceny wymogów cyberbezpieczeństwa;

g) szczegółowe kryteria oceny i metody, w tym rodzaje oceny, stosowane w celu wykazania, że zostały osiągnięte cele w zakresie bezpieczeństwa, o których mowa w art. 51;

h) w stosownych przypadkach niezbędne do celów certyfikacji informacje, które wnioskodawca ma dostarczyć lub udostępnić w inny sposób jednostkom oceniającym zgodność;

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

j) zasady monitorowania zgodności produktów ICT, usług ICT i procesów ICT z wymogami europejskich certyfikatów cyberbezpieczeństwa lub unijnymi deklaracjami zgodności, w tym mechanizmy służące wykazaniu ciągłej zgodności z określonymi wymogami cyberbezpieczeństwa;

k) w stosownych przypadkach warunki wydawania, utrzymywania, kontynuowania i odnawiania europejskich certyfikatów cyberbezpieczeństwa, a także warunki rozszerzania lub ograniczenia zakresu certyfikacji;

l) zasady dotyczące skutków dla produktów ICT, usług ICT i procesów ICT, które uzyskały certyfikację lub w przypadku których wydana została unijna deklaracja zgodności, które jednak nie spełniają wymogów programu;

m) zasady dotyczące sposobu zgłaszania uprzednio niewykrytych, a wpływających na cyberbezpieczeństwo podatności produktów ICT, usług ICT i procesów ICT oraz sposobu postępowania z nimi;

n) w stosownych przypadkach zasady dotyczące przechowywania dokumentów przez jednostki oceniające zgodność;

o) identyfikacja krajowych lub międzynarodowych programów certyfikacji cyberbezpieczeństwa, obejmujących ten sam rodzaj lub te same kategorie produktów ICT, usług ICT i procesów ICT, wymogów bezpieczeństwa, kryteriów i metod oceny oraz poziomów uzasadnienia zaufania;

p) treść i format wydawanych europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności;

q) okres dostępności unijnej deklaracji zgodności, dokumentacji technicznej oraz wszelkich innych istotnych informacji, przez jaki mają je udostępniać wytwórcy lub dostawcy produktów ICT, usług ICT lub procesów ICT;

r) maksymalny okres ważności europejskich certyfikatów cyberbezpieczeństwa wydawanych w ramach programu;

s) polityka dotycząca ujawniania informacji na temat europejskich certyfikatów cyberbezpieczeństwa, które zostały wydane, zmienione lub cofnięte w ramach programów;

t) warunki wzajemnego uznawania programów certyfikacji z państwami trzecimi;

u) w stosownych przypadkach zasady dotyczące ustanowionego w danym programie mechanizmu wzajemnej oceny dla organów lub jednostek wydających europejskie certyfikaty cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki" zgodnie z art. 56 ust. 6. Mechanizm taki pozostaje bez uszczerbku dla wzajemnego przeglądu, o którym mowa w art. 59;

v) format i procedury, jakie mają stosować wytwórcy lub dostawcy produktów ICT, usług ICT lub procesów ICT przy dostarczaniu i aktualizowaniu dodatkowych informacji na temat cyberbezpieczeństwa zgodnie z art. 55.

2. Określone wymogi europejskiego programu certyfikacji cyberbezpieczeństwa muszą być zgodne z obowiązującymi wymogami prawnymi, w szczególności z wymogami wynikającymi ze zharmonizowanego prawa Unii.

3. W przypadku gdy przewiduje to dany akt prawny Unii, certyfikat lub unijna deklaracja zgodności wydane w ramach europejskiego programu certyfikacji cyberbezpieczeństwa mogą być stosowane do wykazania domniemania zgodności z wymogami tego aktu prawnego.

4. W przypadku braku zharmonizowanego prawa Unii prawo państwa członkowskiego może również stanowić, że europejski programy certyfikacji cyberbezpieczeństwa może być stosowany do ustanowienia domniemania zgodności z wymogami prawnymi.

Artykuł 55

Dodatkowe informacje na temat cyberbezpieczeństwa certyfikowanych produktów ICT, usług ICT i procesów ICT

1. Wytwórca lub dostawca certyfikowanych produktów ICT, usług ICT lub procesów ICT lub wytwórca lub dostawca produktów ICT, usług ICT i procesów ICT, w przypadku których wydana została unijna deklaracja zgodności, udostępnia publicznie następujące dodatkowe informacje na temat cyberbezpieczeństwa:

a) porady i zalecenia mające pomóc użytkownikom końcowym w bezpiecznych: konfiguracji, instalacji, uruchomieniu, obsłudze i utrzymaniu produktów ICT lub usług ICT;

b) okres, w którym użytkownikom końcowym oferowane jest wsparcie w zakresie bezpieczeństwa, w szczególności pod względem dostępności aktualizacji związanych z cyberbezpieczeństwem;

c) informacje kontaktowe wytwórcy lub dostawcy oraz akceptowane sposoby otrzymywania informacji o podatnościach pochodzących od użytkowników końcowych i ekspertów w obszarze bezpieczeństwa;

d) odesłanie do repozytoriów internetowych zawierających wykaz podanych do wiadomości publicznej podatności związanych z produktami ICT, usługami ICT lub procesami ICT oraz wszelkich odnośnych poradników dotyczących cyberbezpieczeństwa.

2. Informacje, o których mowa w ust. 1, są dostępne w formie elektronicznej oraz pozostają dostępne i są w razie konieczności aktualizowane co najmniej do czasu wygaśnięcia przedmiotowego europejskiego certyfikatu cyberbezpieczeństwa lub unijnej deklaracji zgodności.

Artykuł 56

Certyfikacja cyberbezpieczeństwa

1. Przyjmuje się, że produkty ICT, usługi ICT i procesy ICT, które uzyskały certyfikację w ramach przyjętego na podstawie art. 49 europejskiego programu certyfikacji cyberbezpieczeństwa, są zgodne z wymogami takiego programu.

2. Certyfikacja cyberbezpieczeństwa jest dobrowolna, o ile prawo Unii lub prawo państwa członkowskiego nie stanowi inaczej.

3. Komisja ocenia regularnie wydajność i użyteczność przyjętych europejskich programów certyfikacji cyberbezpieczeństwa oraz to, czy określony europejski program certyfikacji cyberbezpieczeństwa należy uczynić obowiązkowym za pomocą odpowiedniego prawa Unii w celu zapewnienia w Unii odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, procesów ICT i usług ICT oraz w celu poprawy funkcjonowania rynku wewnętrznego. Pierwszą taką ocenę przeprowadza się nie później niż 31 grudnia 2023 r., a kolejne oceny przeprowadza się co najmniej raz na 2 lata. W oparciu o wynik tych ocen Komisja zidentyfikuje te produkty ICT, usługi ICT i procesy ICT objęte jednym z istniejących programów certyfikacji, które należy objąć obowiązkowym programem certyfikacji.

W pierwszej kolejności Komisja skoncentruje się na sektorach wymienionych w załączniku II do dyrektywy (UE) 2016/1148, które zostaną ocenione najpóźniej dwa lata po przyjęciu pierwszego europejskiego programu certyfikacji cyberbezpieczeństwa.

Przygotowując ocenę, Komisja:

a) bierze pod uwagę wpływ danych środków na wytwórców lub dostawców takich produktów ICT, usług ICT lub procesów ICT oraz na użytkowników pod względem kosztów tych środków oraz korzyści społecznych lub gospodarczych wynikających z przewidywanego zwiększonego poziomu bezpieczeństwa wskazanych produktów ICT, usług ICT lub procesów ICT;

b) bierze pod uwagę istnienie i wdrożenie odpowiednich przepisów państwa członkowskiego i państwa trzeciego;

c) prowadzi otwarty, przejrzysty i integracyjny proces konsultacji ze wszystkimi odpowiednimi interesariuszami i państwami członkowskimi;

d) bierze pod uwagę terminy wdrożenia, środki i okresy przejściowe, w szczególności pod względem ewentualnego wpływu danego środka na wytwórców lub dostawców produktów ICT, usług ICT lub procesów ICT, w tym na MŚP;

e) proponuje najszybszy i najbardziej skuteczny sposób przejścia z dobrowolnego programu certyfikacji na program obowiązkowy.

4. Jednostki oceniające zgodność, o których mowa w art. 60, wydają europejskie certyfikaty cyberbezpieczeństwa na podstawie niniejszego artykułu, wskazując na poziom uzasadnienia zaufania „podstawowy" lub „istotny" w oparciu o kryteria zawarte w danym europejskim programie certyfikacji cyberbezpieczeństwa przyjętym przez Komisję na podstawie art. 49.

5. Na zasadzie odstępstwa od ust. 4, w należycie uzasadnionych przypadkach, europejski program certyfikacji cyberbezpieczeństwa może przewidywać, że europejskie certyfikaty cyberbezpieczeństwa otrzymywane na podstawie tego programu są wydawane jedynie przez podmiot publiczny. Takim podmiotem musi być jeden z wymienionych poniżej podmiotów:

a) krajowy organ ds. certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 ust. 1; lub

b) podmiot publiczny akredytowany jako jednostka oceniająca zgodność na podstawie art. 60 ust. 1.

6. W przypadku gdy europejski program certyfikacji cyberbezpieczeństwa przyjęty na podstawie art. 49 wymaga poziomu uzasadnienia zaufania „wysoki", europejski certyfikat cyberbezpieczeństwa wydawany w ramach tego programu może być wydany wyłącznie przez krajowy organ ds. certyfikacji cyberbezpieczeństwa lub – w następujących przypadkach – przez jednostkę oceniającą zgodność:

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

b) na podstawie ogólnego powierzenia przez krajowy organ ds. certyfikacji cyberbezpieczeństwa zadania polegającego na wydawaniu takich europejskich certyfikatów cyberbezpieczeństwa jednostce oceniającej zgodność.

7. Osoba fizyczna lub prawna, która poddaje produkty ICT, usługi ICT lub procesy ICT certyfikacji, udostępnia krajowemu organowi ds. certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 – w przypadku gdy organ ten jest podmiotem wydającym europejski certyfikat cyberbezpieczeństwa – lub jednostce oceniającej zgodność, o której mowa w art. 60, wszelkie informacje niezbędne to przeprowadzenia certyfikacji.

8. Posiadacz europejskiego certyfikatu cyberbezpieczeństwa informuje organ lub jednostkę, o których mowa w ust. 7, o wszelkich wykrytych następnie podatnościach lub nieprawidłowościach związanych z bezpieczeństwem certyfikowanych produktów ICT, usług ICT lub procesów ICT, które mogą mieć wpływ na zgodność z wymogami z zakresu certyfikacji. Organ lub jednostka przekazuje bez zbędnej zwłoki te informacje zainteresowanemu krajowemu organowi ds. certyfikacji cyberbezpieczeństwa.

9. Europejski certyfikat cyberbezpieczeństwa wydaje się na okres przewidziany w europejskim programie certyfikacji cyberbezpieczeństwa i może być on odnowiony, o ile nadal są spełnione odpowiednie wymogi.

10. Europejski certyfikat cyberbezpieczeństwa wydany na podstawie niniejszego artykułu jest uznawany we wszystkich państwach członkowskich.

Artykuł 57

Krajowe programy certyfikacji cyberbezpieczeństwa i krajowe certyfikaty cyberbezpieczeństwa

1. Bez uszczerbku dla ust. 3 niniejszego artykułu krajowe programy certyfikacji cyberbezpieczeństwa i powiązane z nimi procedury dotyczące produktów ICT, usług ICT i procesów ICT, które są objęte europejskim programem certyfikacji cyberbezpieczeństwa przestają być skuteczne z dniem określonym w akcie wykonawczym przyjętym na podstawie art. 49 ust. 7. Krajowe programy certyfikacji cyberbezpieczeństwa i powiązane z nimi procedury dotyczące produktów ICT, usług ICT i procesów ICT, które nie są objęte europejskim programem certyfikacji cyberbezpieczeństwa, funkcjonują nadal.

2. Państwa członkowskie nie mogą wprowadzać nowych krajowych programów certyfikacji cyberbezpieczeństwa dotyczących produktów ICT, usług ICT i procesów ICT, które są już objęte obowiązującym europejskim programem certyfikacji cyberbezpieczeństwa.

3. Istniejące certyfikaty wydane w ramach krajowych programów certyfikacji cyberbezpieczeństwa i objęte zakresem europejskiego programu certyfikacji cyberbezpieczeństwa pozostają ważne do końca ich terminu ważności.

4. Z myślą o unikaniu rozdrobnienia rynku wewnętrznego, państwa członkowskie informują Komisję i ECCG o wszelkich zamiarach dotyczących opracowania nowych krajowych programów certyfikacji cyberbezpieczeństwa.

Artykuł 58

Krajowe organy ds. certyfikacji cyberbezpieczeństwa

1. Każde państwo członkowskie wyznacza na swoim terytorium przynajmniej jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa lub – za zgodą innego państwa członkowskiego – wyznacza przynajmniej jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa ustanowiony na terytorium tego innego państwa członkowskiego jako organ odpowiedzialny za zadania związane z nadzorem w wyznaczającym państwie członkowskim.

2. Każde państwo członkowskie informuje Komisję o wyznaczonych krajowych organach ds. certyfikacji cyberbezpieczeństwa, a w przypadku gdy państwo członkowskie wyznacza więcej niż jeden organ, informuje ono również Komisję o zadaniach powierzonych każdemu z tych organów.

3. Bez uszczerbku dla art. 56 ust. 5 lit. a) i art. 56 ust. 6 każdy krajowy organ ds. certyfikacji cyberbezpieczeństwa pozostaje niezależny od jednostek, nad którymi sprawuje nadzór, w zakresie swojej organizacji, decyzji w sprawie finansowania, struktury prawnej i procesu podejmowania decyzji.

4. Państwa członkowskie zapewniają, by działalność krajowych organów ds. certyfikacji cyberbezpieczeństwa związana z wydawaniem europejskich certyfikatów cyberbezpieczeństwa, o których mowa w art. 56 ust. 5 lit. a) i art. 56 ust. 6, była ściśle oddzielona od ich działalności związanej z nadzorem określonej w niniejszym artykule i by oba rodzaje tej działalności były wykonywane niezależnie od siebie.

5. Państwa członkowskie zapewniają, aby krajowe organy ds. certyfikacji cyberbezpieczeństwa posiadały odpowiednie zasoby na potrzeby wykonywania swoich uprawnień i wywiązywania się ze swoich zadań w skuteczny i wydajny sposób.

6. W celu skutecznego wdrożenia niniejszego rozporządzenia zasadnym jest, aby organy te uczestniczyły w pracach ECCG w aktywny, skuteczny, wydajny i bezpieczny sposób.

7. Krajowe organy ds. certyfikacji cyberbezpieczeństwa:

a) nadzorują i egzekwują stosowanie zawartych w europejskich programach certyfikacji bezpieczeństwa na podstawie art. 54 ust. 1 lit. j) zasad monitorowania zgodności produktów ICT, usług ICT i procesów ICT z wymogami europejskich certyfikatów cyberbezpieczeństwa wydanych na ich terytoriach, we współpracy z innymi odpowiednimi organami nadzoru rynku;

b) monitorują wykonywanie obowiązków wytwórców lub dostawców produktów ICT, usług ICT lub procesów ICT, którzy mają siedzibę na ich terytorium i którzy przeprowadzają ocenę zgodności przez stronę pierwszą, oraz egzekwują takie obowiązki, w szczególności monitorują wykonywanie obowiązków takich wytwórców lub dostawców, które określono w art. 53 ust. 2 i 3 i w odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa, oraz egzekwują takie obwiązki;

c) bez uszczerbku dla art. 60 ust. 3 aktywnie wspomagają i wspierają krajowe jednostki akredytujące w monitorowaniu i nadzorowaniu działalności jednostek oceniających zgodność do celów niniejszego rozporządzenia;

d) monitorują i nadzorują działalność podmiotów publicznych, o których mowa w art. 56 ust. 5;

e) w stosownych przypadkach zezwalają na działalność jednostek oceniających zgodność, zgodnie z art. 60 ust. 3, oraz ograniczają, zawieszają lub cofają istniejące zezwolenia, jeżeli jednostki oceniające zgodność naruszają wymogi niniejszego rozporządzenia;

f) rozpatrują skargi osób fizycznych lub prawnych dotyczące europejskich certyfikatów cyberbezpieczeństwa wydanych przez krajowe organy ds. certyfikacji cyberbezpieczeństwa, europejskich certyfikatów cyberbezpieczeństwa wydanych przez jednostki oceniające zgodność zgodnie z art. 56 ust. 6 lub unijnych deklaracji zgodności wydanych na podstawie art. 53 oraz badają w odpowiednim zakresie przedmiot takich skarg i informują skarżącego w rozsądnym terminie o postępach i wynikach badania;

g) przedkładają ENISA i ECCG roczne sprawozdanie z działań przeprowadzonych na podstawie lit. b), c) i d) niniejszego ustępu lub na podstawie ust. 8;

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

i) monitorują odpowiednie zmiany w dziedzinie certyfikacji cyberbezpieczeństwa.

8. Każdy krajowy organ ds. certyfikacji cyberbezpieczeństwa ma co najmniej następujące uprawnienia do:

a) żądania od jednostek oceniających zgodność, posiadaczy europejskich certyfikatów cyberbezpieczeństwa oraz podmiotów, które wydały unijne deklaracje zgodności przekazania wszelkich informacji, których organ ten potrzebuje do wykonywania swoich zadań;

b) prowadzenia postępowań, w formie audytów, w stosunku do jednostek oceniających zgodność, posiadaczy europejskich certyfikatów cyberbezpieczeństwa i podmiotów, które wydały unijne deklaracje zgodności, w celu weryfikacji przestrzegania przez nie niniejszego tytułu;

c) stosowania odpowiednich środków, zgodnie z prawem krajowym, w celu zapewnienia, by jednostki oceniające zgodność, posiadacze europejskich certyfikatów cyberbezpieczeństwa i podmioty, które wydały unijne deklaracje zgodności przestrzegali niniejszego rozporządzenia lub zachowywali zgodność z danym europejskim programem certyfikacji cyberbezpieczeństwa;

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

e) cofnięcia, zgodnie z prawem krajowym, europejskich certyfikatów cyberbezpieczeństwa wydanych przez krajowe organy ds. certyfikacji cyberbezpieczeństwa lub europejskich certyfikatów cyberbezpieczeństwa wydanych przez jednostki oceniające zgodność zgodnie z art. 56 ust. 6, jeżeli certyfikaty te nie są zgodne z niniejszym rozporządzeniem lub z europejskim programem certyfikacji cyberbezpieczeństwa;

f) nakładania kar zgodnie z prawem krajowym, jak przewidziano w art. 65, oraz żądania natychmiastowego zaprzestania naruszeń obowiązków określonych w niniejszym rozporządzeniu.

9. Krajowe organy ds. certyfikacji cyberbezpieczeństwa współpracują ze sobą i z Komisją, w szczególności wymieniając informacje, doświadczenie i dobre praktyki odnoszące się do certyfikacji cyberbezpieczeństwa i kwestii technicznych dotyczących cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT.

Artykuł 59

Wzajemny przegląd

1. W celu uzyskania równoważnych norm w całej Unii w odniesieniu do europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności krajowe organy ds. certyfikacji cyberbezpieczeństwa podlegają wzajemnemu przeglądowi.

2. Wzajemny przegląd przeprowadza się w oparciu o rzetelne i przejrzyste kryteria i procedury oceny, w szczególności w odniesieniu do wymagań dotyczących struktury, zasobów ludzkich i procedur, poufności i skarg.

3. W ramach wzajemnego przeglądu ocenia się:

a) w stosownych przypadkach – czy działalność krajowych organów ds. certyfikacji cyberbezpieczeństwa związana z wydawaniem europejskich certyfikatów cyberbezpieczeństwa, o których mowa w art. 56 ust. 5 lit. a) i art. 56 ust. 6, jest ściśle oddzielona od działalności związanej z nadzorem określonej w art. 58 i czy te działalności są wykonywane niezależnie od siebie;

b) procedury nadzorowania i egzekwowania zasad monitorowania zgodności produktów ICT, usług ICT i procesów ICT z europejskimi certyfikatami cyberbezpieczeństwa na podstawie art. 58 ust. 7 lit. a);

c) procedury nadzorowania i egzekwowania obowiązków wytwórców lub dostawców produktów ICT, usług ICT lub procesów ICT na podstawie art. 58 ust. 7 lit. b);

d) procedury monitorowania, wydawania zezwoleń na działalność i nadzorowania działalności jednostek oceniających zgodność;

e) w stosownych przypadkach – czy członkowie personelu organów i jednostek wydających certyfikaty o poziomie uzasadnienia zaufania „wysoki" zgodnie z art. 56 ust. 6 mają odpowiednią wiedzę fachową.

4. Wzajemny przegląd musi być przeprowadzany przez co najmniej dwa krajowe organy ds. certyfikacji cyberbezpieczeństwa z innych państw członkowskich oraz Komisję i musi być przeprowadzany co najmniej raz na pięć lat. ENISA może uczestniczyć we wzajemnym przeglądzie.

5. Komisja może przyjmować akty wykonawcze ustanawiające plan wzajemnego przeglądu obejmujący okres co najmniej pięciu lat, ustanawiające kryteria dotyczące składu zespołu ds. wzajemnego przeglądu, metodykę wykorzystywaną do wzajemnego przeglądu, harmonogram, częstotliwość oraz inne zadania związane z wzajemnym przeglądem. Przyjmując te akty wykonawcze, Komisja należycie uwzględnia stanowisko ECCG. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 66 ust. 2.

6. Wyniki wzajemnych przeglądów analizuje ECCG, która sporządza podsumowania, które można podawać do wiadomości publicznej, i która, w razie potrzeby, wydaje wytyczne lub zalecenia dotyczące działań lub środków, jakie mają podjąć zainteresowane podmioty.

Artykuł 60

Jednostki oceniające zgodność

1. Jednostki oceniające zgodność są akredytowane przez krajowe jednostki akredytujące wyznaczone na podstawie rozporządzenia (WE) nr 765/2008. Akredytacji takiej udziela się jedynie wtedy, gdy jednostki oceniające zgodność spełniają wymagania określone w załączniku do niniejszego rozporządzenia.

2. W przypadku gdy europejski certyfikat cyberbezpieczeństwa wydawany jest przez krajowy organ ds. certyfikacji cyberbezpieczeństwa na podstawie art. 56 ust. 5 lit. a) i art. 56 ust. 6, jednostkę certyfikującą krajowego organu ds. certyfikacji cyberbezpieczeństwa akredytuje się jako jednostkę oceniającą zgodność na podstawie ust. 1 niniejszego artykułu.

3. W przypadku gdy europejskie programy certyfikacji cyberbezpieczeństwa określają szczególne lub dodatkowe wymogi zgodnie z art. 54 ust. 1 lit. f), krajowy organ ds. certyfikacji cyberbezpieczeństwa może zezwolić na wykonywanie zadań w ramach takich programów wyłącznie takim jednostkom oceniającym zgodność, które spełniają te wymogi.

4. Akredytacji, o której mowa w ust. 1, udziela się jednostkom oceniającym zgodność na maksymalnie pięć lat i można ją odnowić na tych samych warunkach, o ile jednostka oceniająca zgodność nadal spełnia wymogi określone w niniejszym artykule. Krajowe jednostki akredytujące podejmują, w odpowiednich ramach czasowych, wszelkie stosowne środki w celu ograniczenia, zawieszenia lub cofnięcia akredytacji jednostki oceniającej zgodność udzielonej na podstawie ust. 1, w przypadku gdy warunki udzielenia akredytacji nie zostały spełnione, przestały być spełnione lub gdy jednostka oceniająca zgodność narusza niniejsze rozporządzenie.

Artykuł 61

Notyfikacja

1. W odniesieniu do każdego europejskiego programu certyfikacji cyberbezpieczeństwa krajowe organy ds. certyfikacji cyberbezpieczeństwa notyfikują Komisji jednostki oceniające zgodność, które zostały akredytowane i którym, w stosownych przypadkach, udzielono zezwolenia na podstawie art. 60 ust. 3 na wydawanie europejskich certyfikatów cyberbezpieczeństwa na określonych poziomach uzasadnienia zaufania, o których mowa w art. 52. Krajowe organy ds. certyfikacji cyberbezpieczeństwa powiadamiają bez zbędnej zwłoki o wszelkich późniejszych zmianach w tym zakresie.

2. Po upływie roku od wejścia w życie europejskiego programu certyfikacji cyberbezpieczeństwa Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* wykaz jednostek oceniających zgodność notyfikowanych w odniesieniu do tego programu.

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

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

5. Komisja może przyjmować akty wykonawcze w celu określenia okoliczności, formatów i procedur dotyczących notyfikacji, o których mowa w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 66 ust. 2.

Artykuł 62

Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa

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

2. W skład ECCG wchodzą przedstawiciele krajowych organów ds. certyfikacji cyberbezpieczeństwa lub przedstawiciele innych odpowiednich organów krajowych. Członek ECCG nie może reprezentować więcej niż dwóch państw członkowskich.

3. Interesariusze i odpowiednie strony trzecie mogą być zapraszani na posiedzenia ECCG i do udziału w jej pracach.

4. ECCG ma następujące zadania:

a) doradzanie i pomaganie Komisji przy pracach nad zapewnieniem spójnego wprowadzania i stosowania niniejszego tytułu, w szczególności w odniesieniu do unijnego kroczącego programu prac, kwestii związanych z polityką certyfikacji cyberbezpieczeństwa, koordynacji koncepcji politycznych oraz przygotowywania europejskich programów certyfikacji cyberbezpieczeństwa;

b) pomaganie, doradzanie i współpracowanie z ENISA w związku z przygotowywaniem propozycji programu na podstawie art. 49;

c) wydawanie opinii na temat propozycji programu przygotowanej przez ENISA na podstawie art. 49 niniejszego rozporządzenia;

d) zwracanie się do ENISA z wnioskiem o przygotowanie propozycji programu na podstawie art. 48 ust. 2;

e) wydawanie skierowanych do Komisji opinii dotyczących utrzymania i przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa;

f) monitorowanie odpowiednich zmian w dziedzinie certyfikacji cyberbezpieczeństwa oraz wymiana informacji i dobrych praktyk odnoszących się do programów certyfikacji cyberbezpieczeństwa;

g) ułatwianie współpracy pomiędzy krajowymi organami ds. certyfikacji cyberbezpieczeństwa w ramach niniejszego tytułu poprzez budowanie zdolności, wymianę informacji, a w szczególności poprzez ustanowienie metod efektywnej wymiany informacji związanych z kwestiami dotyczącymi certyfikacji cyberbezpieczeństwa;

h) wspieranie w zakresie wdrażania mechanizmów wzajemnej oceny zgodnie z zasadami ustanowionymi w danym europejskim programie certyfikacji cyberbezpieczeństwa na podstawie art. 54 ust. 1 lit. u);

i) ułatwianie dostosowywania europejskich programów cyberbezpieczeństwa do międzynarodowo uznanych norm, w tym przez dokonywanie przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa i, w stosownych przypadkach, wydawanie skierowanych do ENISA zaleceń dotyczących podjęcia współpracy z odpowiednimi międzynarodowymi organizacjami normalizacyjnymi w celu wyeliminowania braków lub luk w istniejących międzynarodowo uznanych normach.

5. Komisja, z pomocą ENISA, przewodniczy ECCG i zapewnia ECCG obsługę sekretariatu, zgodnie z art. 8 ust. 1 lit. e).

Artykuł 63

Prawo do wniesienia skargi

1. Osoby fizyczne i prawne mają prawo do wniesienia skargi do podmiotu, który wydał europejski certyfikat cyberbezpieczeństwa lub, w przypadku gdy skarga dotyczy europejskiego certyfikatu cyberbezpieczeństwa wydanego przez jednostkę oceniającą zgodność, działającą zgodnie z art. 56 ust. 6 – do odpowiedniego krajowego organu ds. certyfikacji cyberbezpieczeństwa.

2. Organ lub jednostka, do których wniesiono skargę, informuje skarżącego o stanie postępowania i podjętej decyzji, a także informuje skarżącego o prawie do skutecznego środka prawnego przed sądem, o którym mowa w art. 64.

Artykuł 64

Prawo do skutecznego środka prawnego przed sądem

1. Niezależnie od wszelkich administracyjnych lub innych pozasądowych środków ochrony prawnej, osoby fizyczne i prawne mają prawo do skutecznego środka prawnego przed sądem odnośnie do:

a) decyzji podjętych przez organ lub jednostkę, o których mowa w art. 63 ust. 1, w tym, w stosownych przypadkach, w związku z nieprawidłowym wydaniem, niewydaniem lub uznaniem europejskiego certyfikatu cyberbezpieczeństwa, którego posiadaczami są te osoby fizyczne lub prawne;

b) bezczynnością w sprawie skargi wniesionej do organu lub jednostki, o których mowa w art. 63 ust. 1.

2. Postępowania na podstawie niniejszego artykułu wnosi się do sądów państwa członkowskiego, w którym znajduje się organ lub jednostka, przeciwko którym wnoszony jest środek prawny przed sądem.

Artykuł 65

Kary

Państwa członkowskie ustanawiają przepisy o karach nakładanych w przypadku naruszenia niniejszego tytułu i naruszenia europejskich programów certyfikacji cyberbezpieczeństwa oraz stosują wszelkie niezbędne środki, aby zapewnić ich wykonanie. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie 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 66

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 67

Ocena i przegląd

1. Do dnia 28 czerwca 2024 r., a następnie co pięć lat, Komisja ocenia wpływ, skuteczność i efektywność ENISA oraz jej metod pracy, ewentualną potrzebę zmiany mandatu ENISA oraz skutki finansowe wszelkich takich zmian. W ocenie tej uwzględnia się wszelkie informacje zwrotne przekazane ENISA w odpowiedzi na jej działalność. Jeżeli Komisja uzna, że dalsze działanie ENISA w kontekście powierzonych jej celów, mandatu i zadań nie jest już uzasadnione, może wystąpić z wnioskiem o zmianę niniejszego rozporządzenia w zakresie przepisów dotyczących ENISA.

2. Ocena dotyczy również wpływu, skuteczności i efektywności przepisów tytułu III niniejszego rozporządzenia w odniesieniu do celów, którymi są zapewnienie odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT w Unii oraz poprawa funkcjonowania rynku wewnętrznego.

3. Ocena obejmuje również ustalenie, czy w celu zapobieżenia wprowadzaniu na rynek unijny produktów ICT, usług ICT i procesów ICT niespełniających podstawowych wymogów cyberbezpieczeństwa konieczne są zasadnicze wymogi cyberbezpieczeństwa dotyczące dostępu do rynku wewnętrznego.

4. Do dnia 28 czerwca 2024 r., a następnie co pięć lat, Komisja przekazuje sprawozdanie z oceny wraz z wnioskami Parlamentowi Europejskiemu, Radzie i Zarządowi. Ustalenia zawarte w tym sprawozdaniu podaje się do wiadomości publicznej.

Artykuł 68

Uchylenie oraz następstwo prawne

1. Rozporządzenie (UE) nr 526/2013 traci moc ze skutkiem od dnia 27 czerwca 2019 r.

2. Odesłania do rozporządzenia (UE) nr 526/2013 i do ENISA ustanowionej tym rozporządzeniem odczytuje się jako odesłania do niniejszego rozporządzenia i do ENISA ustanowionej niniejszym rozporządzeniem.

3. ENISA ustanowiona niniejszym rozporządzeniem jest następcą prawnym ENISA ustanowionej rozporządzeniem (UE) nr 526/2013, w odniesieniu do wszystkich praw własności, umów, obowiązków prawnych, umów o pracę, zobowiązań finansowych i odpowiedzialności. Wszystkie decyzje Zarządu i Rady Wykonawczej przyjęte zgodnie z rozporządzeniem (UE) nr 526/2013 pozostają ważne, pod warunkiem że są one zgodne z niniejszym rozporządzeniem.

4. ENISA ustanawia się na czas nieokreślony od dnia 27 czerwca 2019 r.

5. Dyrektor Wykonawczy powołany na podstawie art. 24 ust. 4 rozporządzenia (UE) nr 526/2013 pozostaje na swoim stanowisku i pełni obowiązki Dyrektora Wykonawczego określone w art. 20 niniejszego rozporządzenia przez pozostałą część kadencji Dyrektora Wykonawczego. Pozostałe warunki jego umowy pozostają bez zmian.

6. Członkowie Zarządu i ich zastępcy powołani na podstawie art. 6 rozporządzenia (UE) nr 526/2013 pozostają na swoich stanowiskach i pełnią funkcje Zarządu określone w art. 15 niniejszego rozporządzenia przez pozostałą część swoich kadencji.

Artykuł 69

Wejście w życie

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

2. Art. 58, 60, 61, 63, 64 i 65 stosuje się od dnia 28 czerwca 2021 r.

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

Sporządzono w Strasburgu dnia 17 kwietnia 2019 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
A. TAJANI	G. CIAMBA
Przewodniczący	*Przewodniczący*

ZAŁĄCZNIK

WYMOGI, KTÓRE MUSZĄ BYĆ SPEŁNIONE PRZEZ JEDNOSTKI OCENIAJĄCE ZGODNOŚĆ

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

1. Jednostka oceniająca zgodność musi być ustanowiona na podstawie prawa krajowego i mieć osobowość prawną.

2. Jednostka oceniająca zgodność musi być stroną trzecią, niezależną od ocenianych przez nią organizacji lub produktów ICT, usług ICT lub procesów ICT.

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

4. Jednostki oceniające zgodność, ich ścisłe kierownictwo oraz pracownicy odpowiedzialni za realizację zadań z zakresu oceny zgodności nie mogą być projektantami, wytwórcami, dostawcami, instalatorami, nabywcami, właścicielami, użytkownikami ani osobami odpowiedzialnymi za utrzymanie produktu ICT, usługi ICT lub procesu ICT będących przedmiotem oceny, ani upoważnionymi przedstawicielami żadnej z wymienionych stron. Zakaz ten nie wyklucza wykorzystywania ocenianych produktów ICT, które są niezbędne do prowadzenia działalności jednostki oceniającej zgodność, lub wykorzystywania takich produktów ICT do celów osobistych.

5. Jednostki oceniające zgodność, ich ścisłe kierownictwo oraz pracownicy odpowiedzialni za wykonywanie zadań z zakresu oceny zgodności nie mogą być bezpośrednio zaangażowani w projektowanie, wytwarzanie ani konstruowanie, wprowadzanie do obrotu, instalację lub użytkowanie ani być osobami odpowiedzialnymi za utrzymanie produktów ICT, usług ICT lub procesów ICT będących przedmiotem oceny, nie mogą one również reprezentować stron zaangażowanych w taką działalność. Jednostki oceniające zgodność, ich ścisłe kierownictwo oraz pracownicy odpowiedzialni za realizację zadań z zakresu oceny zgodności nie mogą angażować się w żadną działalność, która może zagrozić niezależności ich osądów lub uczciwości w odniesieniu do podejmowanych przez nich czynności z zakresu oceny zgodności. Zakaz ten dotyczy w szczególności usług konsultingowych.

6. Jeżeli jednostka oceniająca zgodność jest własnością podmiotu publicznego lub instytucji publicznej bądź jest przez nie zarządzana, należy zapewnić i udokumentować brak zależności pomiędzy krajowym organem ds. certyfikacji cyberbezpieczeństwa oraz jednostką oceniającą zgodność, a także brak konfliktu interesów pomiędzy nimi.

7. Jednostki oceniające zgodność zapewniają, aby działalność ich jednostek zależnych i podwykonawców nie wpływała na poufność, obiektywizm lub bezstronność czynności z zakresu oceny zgodności.

8. Jednostki oceniające zgodność i ich personel zachowują w toku realizacji czynności z zakresu oceny zgodności najwyższe standardy zawodowe, mają konieczne kwalifikacje techniczne w danej dziedzinie oraz nie są poddawani żadnym naciskom ani zachętom, mogącym wpływać na ich opinię lub rezultaty czynności z zakresu oceny zgodności, w tym naciskom i zachętom o charakterze finansowym, szczególnie ze strony osób lub grup osób, których interesy związane są z rezultatami tych czynności.

9. Jednostka oceniająca zgodność musi mieć możliwość wykonywania wszelkich zadań z zakresu oceny zgodności powierzonych jej na podstawie niniejszego rozporządzenia, bez względu na to, czy zadania te wykonuje sama jednostka oceniająca zgodność, czy też są one wykonywane w jej imieniu i na jej odpowiedzialność. Zlecanie podwykonawstwa lub konsultacje z personelem zewnętrznym są odpowiednio udokumentowane, nie uczestniczą w nich żadni pośrednicy i są one przedmiotem pisemnej umowy obejmującej między innymi kwestie poufności i konfliktu interesów. Jednostka oceniająca zgodność ponosi pełną odpowiedzialność za wykonywane zadania.

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

    a) członkami personelu mającymi wiedzę techniczną oraz wystarczające i odpowiednie doświadczenie do realizacji zadań z zakresu oceny zgodności;

    b) opisami procedur, zgodnie z którymi ma być przeprowadzana ocena zgodności, w celu zapewnienia przejrzystości tych procedur i możliwość ich powtarzania. Jednostka ma odpowiednią politykę i stosowne procedury, dzięki którym możliwe jest odróżnienie zadań wykonywanych w charakterze jednostki notyfikowanej na podstawie art. 61 od pozostałych jej czynności;

c) procedurami dotyczącymi prowadzenia działalności, które w należytym stopniu uwzględniają wielkość przedsiębiorstwa, sektor, w którym ono działa, struktury przedsiębiorstwa, stopień złożoności technologii danego produktu ICT, danej usługi ICT lub danego procesu ICT oraz masowy lub seryjny charakter procesu produkcyjnego.

11. Jednostka oceniająca zgodność dysponuje środkami niezbędnymi do prawidłowej realizacji zadań o charakterze technicznym i administracyjnym związanych z czynnościami z zakresu oceny zgodności oraz ma dostęp do wszelkiego niezbędnego wyposażenia i obiektów.

12. Personel odpowiedzialny za realizację czynności z zakresu oceny zgodności musi mieć:

a) solidne kwalifikacje techniczne i zawodowe, obejmujące wszystkie czynności z zakresu oceny zgodności;

b) wystarczającą znajomość wymagań dotyczących przeprowadzanych przez nich ocen zgodności oraz odpowiednie uprawnienia do przeprowadzania takich ocen;

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

d) umiejętności wymagane do sporządzania certyfikatów, zapisów i sprawozdań potwierdzających, że oceny zgodności zostały przeprowadzone.

13. Należy zagwarantować bezstronność jednostek oceniających zgodność, ich ścisłego kierownictwa, osób odpowiedzialnych za realizację czynności z zakresu oceny zgodności oraz wszelkich podwykonawców.

14. Wynagrodzenie ścisłego kierownictwa jednostki oceniającej zgodność oraz osób odpowiedzialnych za realizację czynności z zakresu oceny zgodności nie może zależeć od liczby przeprowadzonych ocen zgodności ani od wyników tych ocen.

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

16. Jednostka oceniająca zgodność, jej personel, jej komisje, jej jednostki zależne, jej podwykonawcy oraz wszelkie podmioty powiązane i personel jednostek zewnętrznych zachowują poufność i dochowują tajemnicy służbowej w odniesieniu do wszystkich informacji, które uzyskują w trakcie wykonywania swoich zadań z zakresu oceny zgodności zgodnie z niniejszym rozporządzeniem lub z wszelkimi przepisami prawa krajowego nadającymi skuteczność niniejszemu rozporządzeniu; wyjątkiem są sytuacje, kiedy ujawnienie jest wymagane na podstawie prawa Unii lub prawa państwa członkowskiego, któremu takie osoby podlegają oraz w relacjach z właściwymi organami państw członkowskich, w których jednostka oceniająca zgodność prowadzi działalność. Prawo własności intelektualnej podlega ochronie. Jednostka oceniająca musi mieć udokumentowane procedury dotyczące wymogów niniejszego punktu.

17. Z wyjątkiem punktu 16 wymogi niniejszego załącznika nie mogą wykluczać wymiany informacji technicznych i porad regulacyjnych pomiędzy jednostką oceniającą zgodność a osobą ubiegającą się o certyfikację lub rozważającą ubieganie się o nią.

18. Jednostki oceniające zgodność prowadzą działalność na spójnych, uczciwych i rozsądnych warunkach, biorąc pod uwagę interesy MŚP w odniesieniu do opłat.

19. Jednostki oceniające zgodność spełniają wymogi odpowiedniej normy dotyczącej akredytacji jednostek oceniających zgodność dokonujących certyfikacji produktów ICT, usług ICT lub procesów ICT, będącej normą zharmonizowaną zgodnie z rozporządzeniem (WE) nr 765/2008.

20. Jednostki oceniające zgodność zapewniają, aby wykorzystywane do celów oceny zgodności laboratoria przeprowadzające testy spełniały wymogi odpowiedniej normy dotyczące akredytacji laboratoriów przeprowadzających testy, będącej normą zharmonizowaną zgodnie z rozporządzeniem (WE) nr 765/2008.