Dziennik Urzędowy L 151
Unii Europejskiej

Wydanie polskie **Legislacja**

Rocznik 62

7 czerwca 2019

Spis treści

[1] Tekst mający znaczenie dla EOG.

PL

Akty, których tytuły wydrukowano zwykłą czcionką, odnoszą się do bieżącego zarządzania sprawami rolnictwa i generalnie zachowują ważność przez określony czas.

Tytuły wszystkich innych aktów poprzedza gwiazdka, a drukuje się je czcionką pogrubioną.

I

(Akty ustawodawcze)

ROZPORZĄDZENIA

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/880

z dnia 17 kwietnia 2019 r.

w sprawie wprowadzania i przywozu dóbr kultury

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 207 ust. 2,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([1]),

a także mając na uwadze, co następuje:

(1) W świetle konkluzji Rady z dnia 12 lutego 2016 r. w sprawie zwalczania finansowania terroryzmu, komunikatu Komisji do Parlamentu Europejskiego i Rady z dnia 2 lutego 2016 r. w sprawie planu działania na rzecz skuteczniejszego zwalczania finansowania terroryzmu, a także dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 ([2]), należy przyjąć wspólne przepisy dotyczące handlu z państwami trzecimi, aby zapewnić skuteczną ochronę przed nielegalnym handlem dobrami kultury oraz przed ich utratą lub zniszczeniem, ochronę dziedzictwa kulturowego ludzkości, a także zapobieganie finansowaniu terroryzmu oraz praniu pieniędzy ze sprzedaży zagrabionych dóbr kultury nabywcom w Unii.

(2) Wyzysk ludności i eksploatacja terytoriów może prowadzić do nielegalnego handlu dobrami kultury, w szczególności gdy taki nielegalny handel pojawia się w kontekście konfliktów zbrojnych. W związku z tym, w niniejszym rozporządzeniu należy w większym stopniu uwzględnić specyfikę regionalną i lokalną ludności i terytoriów niż wartość rynkową dóbr kultury.

(3) Dobra kultury są częścią dziedzictwa kulturowego i często mają duże znaczenie kulturalne, artystyczne, historyczne i naukowe. Dziedzictwo kulturowe jest jednym z podstawowych elementów cywilizacji, który ma między innymi wartość symboliczną i tworzy kulturową pamięć ludzkości. Wzbogaca ono życie kulturowe wszystkich ludzi i łączy ich przez wspólną pamięć, wiedzę i rozwój cywilizacji. Z tego względu powinno być chronione przed bezprawnym przywłaszczeniem i grabieżą. Grabież stanowisk archeologicznych zawsze miała miejsce, jednak obecnie osiągnęła skalę przemysłową i wraz z handlem nielegalnie wydobytymi dobrami kultury stanowi poważne przestępstwo, które powoduje znaczące cierpienie tych bezpośrednio lub pośrednio nim dotkniętych. Nielegalny handel dobrami kultury w wielu przypadkach przyczynia się do wymuszonej jednolitości kulturowej lub utraty tożsamości kulturowej, natomiast grabież dóbr kultury przyczynia się między innymi do dezintegracji kultur Dopóki możliwy jest udział w lukratywnym handlu nielegalnie wydobytymi dobrami kultury i korzystanie z niego bez jakiegokolwiek większego ryzyka, takie wydobywanie i taka grabież będą trwać. Z uwagi na wartość ekonomiczną i artystyczną dóbr kultury, na rynku międzynarodowym tworzy się na nie silny popyt. Brak zdecydowanych międzynarodowych środków prawnych oraz nieskuteczne egzekwowanie wszelkich istniejących środków prowadzą do przeniesienia takich dóbr do szarej strefy. Unia powinna odpowiednio zabronić wprowadzania na obszar celny Unii dóbr kultury nielegalnie wywożonych z państw trzecich, ze szczególnym naciskiem na dobra

([1]) Stanowisko Parlamentu Europejskiego z dnia 12 marca 2019 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 9 kwietnia 2019 r.

([2]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. L 88 z 31.3.2017, s. 6).

kultury z państw trzecich dotkniętych konfliktem zbrojnym, w szczególności gdy takie dobra kultury zostały nielegalnie sprzedane przez terrorystów lub inne organizacje przestępcze. Chociaż ten ogólny zakaz nie powinien pociągać za sobą systematycznych kontroli, państwa członkowskie powinny móc interweniować po otrzymaniu informacji dotyczących podejrzanych ładunków oraz podejmować wszelkie odpowiednie środki w celu przejęcia nielegalnie wywiezionych dóbr kultury.

(4) Ze względu na różne przepisy stosowane w państwach członkowskich w odniesieniu do przywozu dóbr kultury na obszar celny Unii, należy podjąć środki, w szczególności w celu zapewnienia, aby przywóz niektórych dóbr kultury podlegał jednolitym kontrolom w momencie ich wprowadzania na obszar celny Unii, na podstawie istniejących procesów, procedur i narzędzi administracyjnych mających na celu osiągnięcie jednolitego wykonania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 952/2013 ([3]).

(5) Ochrona dóbr kultury uznanych za narodowe dobra kultury państw członkowskich jest już objęta zakresem rozporządzenia Rady (WE) nr 116/2009 ([4]) i dyrektywy Parlamentu Europejskiego i Rady 2014/60/UE ([5]). W związku z tym niniejsze rozporządzenie nie ma zastosowania do dóbr kultury, które powstały lub zostały odkryte na obszarze celnym Unii. Wspólne przepisy wprowadzone niniejszym rozporządzeniem powinny obejmować odprawę celną dóbr kultury spoza Unii wprowadzanych na obszar celny Unii. Do celów niniejszego rozporządzenia właściwym obszarem celnym powinien być obszar celny Unii w momencie przywozu.

(6) Środki kontroli, które mają być wprowadzone w odniesieniu do wolnych obszarów celnych i tzw. „wolnych portów", powinny mieć jak najszerszy zakres pod względem danych procedur celnych, aby zapobiec obchodzeniu niniejszego rozporządzenia poprzez korzystanie z tych wolnych obszarów celnych, które potencjalnie mogą być wykorzystywane do dalszego rozprzestrzeniania się nielegalnego handlu. Te środki kontroli powinny zatem dotyczyć nie tylko dóbr kultury dopuszczanych do obrotu, ale również dóbr kultury objętych specjalną procedurą celną. Jednakże zakres nie powinien wykraczać poza cel, jakim jest zapobieganie wprowadzaniu na obszar celny Unii nielegalnie wywiezionych dóbr kultury. W związku z tym systematyczne środki kontroli powinny obejmować dopuszczenie do obrotu i niektóre specjalne procedury celne, którymi mogą być obejmowane towary wprowadzane na obszar celny Unii, lecz z wyłączeniem tranzytu.

(7) W wielu państwach trzecich oraz w większości państw członkowskich znane są definicje stosowane w konwencji Unesco dotyczącej środków zmierzających do zakazu i zapobiegania nielegalnemu przywozowi, wywozowi i przenoszeniu własności dóbr kultury, podpisanej w Paryżu w dniu 14 listopada 1970 r. (zwanej dalej „konwencją Unesco z 1970 r."), których stroną jest znacząca liczba państw członkowskich, oraz w Konwencji UNIDROIT dotyczącej skradzionych lub nielegalnie wywiezionych dóbr kultury, podpisanej w Rzymie w dniu 24 czerwca 1995 r. Z tego powodu definicje użyte w niniejszym rozporządzeniu oparte są na tych definicjach.

(8) Legalność wywozu dóbr kultury powinna być badana przede wszystkim w oparciu o przepisy ustawowe i wykonawcze kraju, w którym te dobra kultury powstały lub zostały odkryte. Aby jednak nie utrudniać nadmiernie legalnego handlu należy zamiast tego, w niektórych przypadkach, zezwolić w drodze wyjątku osobie, która zamierza dokonać przywozu dóbr kultury na obszar celny Unii, na wykazanie, że zostały one legalnie wywiezione z innego państwa trzeciego, w którym znajdowały się przed ich wysyłką do Unii. Ten wyjątek powinien mieć zastosowanie w przypadku gdy nie można wiarygodnie ustalić, w którym kraju dobra kultury powstały lub zostały odkryte, lub jeżeli wywóz danych dóbr kultury miał miejsce przed wejściem w życie konwencji Unesco z 1970 r., tj. przed dniem 24 kwietnia 1972 r. Aby zapobiec obchodzeniu niniejszego rozporządzenia poprzez wysyłanie nielegalnie wywożonych dóbr kultury do innego państwa trzeciego przed ich przywozem do Unii, wyjątki powinny mieć zastosowanie w przypadku gdy dobra kultury znajdowały się w państwie trzecim przez okres dłuższy niż pięć lat do celów innych niż do użytku tymczasowego, tranzytu, powrotnego wywozu lub przeładunku. W przypadku gdy warunki te są spełnione w odniesieniu do więcej niż jednego kraju, za właściwy uznaje się ostatni z tych krajów przed wprowadzeniem dóbr kultury na obszar celny Unii.

(9) Art. 5 konwencji Unesco z 1970 r. wzywa Państwa Strony do ustanowienia jednej lub większej liczby krajowych służb odpowiedzialnych za ochronę dóbr kultury przed nielegalnym przywozem, wywozem i przenoszeniem własności. Takie służby krajowe powinny dysponować wykwalifikowanym personelem w liczbie wystarczającej do zapewnienia tej ochrony zgodnie z tą konwencją, a także powinny umożliwić niezbędną aktywną współpracę między właściwymi organami państw członkowskich będących Stronami tej konwencji w dziedzinie bezpieczeństwa oraz w ramach walki z nielegalnym przywozem dóbr kultury, zwłaszcza z obszarów dotkniętych konfliktem zbrojnym.

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 952/2013 z dnia 9 października 2013 r. ustanawiające unijny kodeks celny (Dz.U. L 269 z 10.10.2013, s. 1).

([4]) Rozporządzenie Rady (WE) nr 116/2009 z dnia 18 grudnia 2008 r. w sprawie wywozu dóbr kultury (Dz.U. L 39 z 10.2.2009, s. 1).

([5]) Dyrektywa Parlamentu Europejskiego i Rady 2014/60/UE z dnia 15 maja 2014 r. w sprawie zwrotu dóbr kultury wyprowadzonych niezgodnie z prawem z terytorium państwa członkowskiego, zmieniająca rozporządzenie (UE) nr 1024/2012 (Dz.U. L 159 z 28.5.2014, s. 1).

(10) Aby nie utrudniać niewspółmiernie handlu dobrami kultury przez zewnętrzne granice Unii, niniejsze rozporządzenie powinno mieć zastosowanie wyłącznie do dóbr kultury powyżej określonej granicy wieku, która jest ustanowiona niniejszym rozporządzeniem. Właściwe wydaje się także ustalenie progu finansowego, aby wyłączyć ze stosowania warunków i procedur dotyczących przywozu na obszar celny Unii dobra kultury o niższej wartości. Progi te zapewnią, aby środki przewidziane w niniejszym rozporządzeniu koncentrowały się na tych dobrach kultury, w przypadku których istnieje największe prawdopodobieństwo, że mogą paść łupem grabieżców na obszarach dotkniętych konfliktem, nie wyłączając innych dóbr, których kontrola jest niezbędna do zapewnienia ochrony dziedzictwa kulturowego.

(11) Nielegalny handel zagrabionymi dobrami kultury został uznany, w ramach ponadnarodowej oceny ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu mającego wpływ na rynek wewnętrzny, za możliwe źródło finansowania terroryzmu i prania pieniędzy.

(12) Z uwagi na fakt, że niektóre kategorie dóbr kultury, mianowicie obiekty archeologiczne i elementy zabytków, są szczególnie narażone na grabież i zniszczenie, wydaje się niezbędne wprowadzenie systemu wzmożonej kontroli przed uzyskaniem pozwolenia na ich wprowadzenie na obszar celny Unii. W takim systemie powinien istnieć wymóg przedstawienia pozwolenia na przywóz wydanego przez właściwy organ państwa członkowskiego Unii przed dopuszczeniem takich dóbr kultury do obrotu w Unii lub objęciem ich specjalną procedurą celną inną niż tranzyt. Osoby, które starają się uzyskać takie pozwolenie, powinny być w stanie udowodnić legalny wywóz z kraju, w którym te dobra kultury powstały lub zostały odkryte, za pomocą odpowiednich dokumentów i dowodów, takich jak świadectwa wywozowe, tytuły własności, faktury, umowy sprzedaży, dokumenty ubezpieczeniowe, dokumenty przewozowe i ekspertyzy. Na podstawie kompletnych i dokładnie wypełnionych wniosków właściwe organy państw członkowskich powinny bez zbędnej zwłoki podjąć decyzję w sprawie wydania pozwolenia. Wszystkie pozwolenia na przywóz powinny być przechowywane w systemie elektronicznym.

(13) Ikona stanowi każde przedstawienie postaci istotnej w danej religii lub wydarzenia religijnego. Może być tworzona różnymi środkami i w różnych rozmiarach, w formie monumentalnej lub przenośnej. W przypadkach gdy ikona była niegdyś integralną częścią, przykładowo, wnętrza kościoła, klasztoru, kaplicy, samodzielnie lub jako część wyposażenia architektonicznego, na przykład ikonostasu lub ekspozycji na specjalnych podstawach, stanowi ona niezwykle istotną i nieodłączną część kultu religijnego i życia liturgicznego i powinna być uznawana za integralną część zabytku religijnego, który został rozczłonkowany. Nawet w przypadkach gdy nie wiadomo do którego konkretnego zabytku ikona należała, ale istnieje dowód, że stanowiła kiedyś integralną część zabytku, w szczególności gdy obecne są znaki lub elementy wskazujące, że była kiedyś częścią ikonostasu lub była eksponowana na specjalnych podstawach, ikona powinna być nadal objęta kategorią „elementy zabytków artystycznych lub historycznych, lub stanowisk archeologicznych, które zostały rozczłonkowane" wymienionych w załączniku.

(14) Z uwagi na szczególny charakter dóbr kultury, niezwykle istotna jest rola organów celnych, które powinny mieć możliwość, w razie konieczności, żądania dodatkowych informacji od zgłaszającego oraz dokonywania fizycznej kontroli dóbr kultury.

(15) W odniesieniu do kategorii dóbr kultury, których przywóz nie wymaga pozwolenia na przywóz, osoby, które zamierzają przywieźć takie dobra na obszar celny Unii, powinny, w drodze oświadczenia, poświadczyć i przyjąć na siebie odpowiedzialność za ich legalny wywóz z państwa trzeciego oraz powinny przedstawić wystarczające informacje na temat tych dóbr kultury, umożliwiające ich identyfikację przez organy celne. W celu ułatwienia procedury oraz ze względu na pewność prawa informacje na temat dóbr kultury powinny być przekazywane przy użyciu zestandaryzowanego dokumentu. Do opisu dóbr kultury mógłby być stosowany *Object ID standard*, zalecany przez Unesco. Posiadacz dóbr powinien rejestrować te informacje w systemie elektronicznym, w celu ułatwienia identyfikacji przez organy celne, umożliwienia analizy ryzyka i ukierunkowanych kontroli, a także aby zapewnienia możliwości śledzenia dóbr kultury po ich wprowadzeniu na rynek wewnętrzny.

(16) W kontekście środowiska Single Window w obszarze celnym, Komisja powinna być odpowiedzialna za ustanowienie scentralizowanego systemu elektronicznego składania wniosków o pozwolenia na przywóz oraz oświadczeń importerów, a także przechowywania i wymiany informacji między organami państw członkowskich, w szczególności w odniesieniu do oświadczeń importerów i pozwoleń na przywóz.

(17) Przetwarzanie danych w ramach niniejszego rozporządzenia powinno móc obejmować także dane osobowe i powinno być prowadzone zgodnie z prawem Unii. Państwa członkowskie i Komisja powinny przetwarzać dane osobowe jedynie do celów niniejszego rozporządzenia lub w należycie uzasadnionych okolicznościach do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania sankcji karnych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego oraz zapobiegania takim zagrożeniom. Wszelkie gromadzenie, ujawnianie, przekazywanie, komunikowanie

oraz inne przetwarzanie danych osobowych w ramach niniejszego rozporządzenia powinno podlegać wymogom rozporządzeń Parlamentu Europejskiego i Rady (UE) 2016/679 ([6]) oraz (UE) 2018/1725 ([7]). Przetwarzanie danych osobowych do celów niniejszego rozporządzenia powinno odbywać się również zgodnie z prawami do poszanowania życia prywatnego i rodzinnego uznanymi w art. 8 Konwencji Rady Europy o ochronie praw człowieka i podstawowych wolności, a także zgodnie z prawem do poszanowania życia prywatnego i rodzinnego oraz prawem do ochrony danych osobowych, uznanymi, odpowiednio, w art. 7 i 8 Karty praw podstawowych Unii Europejskiej.

(18) Dobra kultury, które nie powstały ani nie zostały odkryte na obszarze celnym Unii, ale które zostały wywiezione jako towary unijne, nie powinny być objęte wymogiem przedstawienia pozwolenia na przywóz lub oświadczenia importera, gdy są wwożone na ten obszar jako towary powracające w rozumieniu rozporządzenia (UE) nr 952/2013.

(19) Odprawa czasowa dóbr kultury do celów edukacyjnych, naukowych, konserwacji, restauracji, wystawienniczych, digitalizacji, przedstawień artystycznych, badań prowadzonych przez instytucje naukowe lub do współpracy pomiędzy muzeami lub podobnymi instytucjami również nie powinna podlegać wymogowi przedstawienia pozwolenia na przywóz lub oświadczenia importera.

(20) Składowanie dóbr kultury pochodzących z krajów dotkniętych konfliktami zbrojnymi lub klęskami żywiołowymi, w wyłącznym celu zapewnienia ich bezpiecznego przechowywania i ochrony przez organ publiczny lub pod nadzorem takiego organu nie powinno podlegać wymogowi przedstawienia pozwolenia na przywóz lub oświadczenia importera.

(21) W celu ułatwienia prezentacji dóbr kultury na komercyjnych targach sztuki, pozwolenie na przywóz nie powinno być konieczne w przypadku gdy dobra kultury są przywożone w ramach odprawy czasowej, w rozumieniu art. 250 rozporządzenia (UE) nr 952/2013, oraz gdy zamiast pozwolenia na przywóz przedstawiono oświadczenie importera. Jednakże przedstawienie pozwolenia na przywóz powinno być wymagane w przypadku gdy takie dobra kultury mają pozostać w Unii po targach sztuki.

(22) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze do przyjmowania szczegółowych zasad dotyczących: dóbr kultury, które są towarami powracającymi, lub odprawy czasowej dóbr kultury na obszarze celnym Unii oraz ich bezpiecznego przechowywania, wzorów wniosków o pozwolenia na przywóz oraz formularzy pozwolenia na przywóz, wzorów oświadczeń importera i dokumentów towarzyszących, a także dalszych przepisów proceduralnych w odniesieniu do ich składania i rozpatrywania. Komisji należy także powierzyć uprawnienia wykonawcze do podejmowania działań w celu utworzenia elektronicznego systemu składania wniosków o pozwolenia na przywóz oraz oświadczeń importerów, a także przechowywania i wymiany informacji między państwami członkowskimi. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([8]).

(23) W celu zapewnienia skutecznej koordynacji oraz unikania powielania wysiłków podczas organizacji szkoleń, budowania zdolności oraz prowadzenia kampanii informacyjnych, a także zlecania odpowiednich badań oraz opracowywania norm, Komisja i państwa członkowskie powinny, w stosownych przypadkach, współpracować z organizacjami i organami międzynarodowymi, takimi jak Unesco, Interpol, Europol, Światowa Organizacja Celna, Międzynarodowy Ośrodek Studiów nad Ochroną i Restauracją Dóbr Kultury oraz Międzynarodowa Rada Muzeów (ICOM).

(24) Odnośne informacje na temat przepływów handlowych dóbr kultury powinny być gromadzone w formie elektronicznej i wymieniane między państwami członkowskimi i Komisją, aby wspierać skuteczne wykonywanie niniejszego rozporządzenia oraz zapewnić podstawę jego przyszłej oceny. W interesie przejrzystości i kontroli publicznej jak najwięcej informacji powinno być podawane do wiadomości publicznej. Przepływów handlowych dóbr kultury nie można skutecznie monitorować jedynie na podstawie ich wartości lub masy. Istotne jest elektroniczne gromadzenie informacji dotyczących liczby zgłaszanych przedmiotów. Ponieważ w Nomenklaturze scalonej nie określono żadnej uzupełniającej jednostki miary dla dóbr kultury, konieczne jest nałożenie wymogu zgłaszania liczby przedmiotów.

([6]) 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).

([7]) 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).

([8]) 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).

(25) Strategia UE i plan działania w zakresie zarządzania ryzykiem celnym mają na celu między innymi wzmocnienie zdolności organów celnych w zakresie reagowania na ryzyko w dziedzinie dóbr kultury. Należy wykorzystywać ramy wspólnego zarządzania ryzykiem określone w rozporządzeniu (UE) nr 952/2013, a organy celne powinny wymieniać między sobą odpowiednie informacje o ryzyku.

(26) W celu skorzystania z wiedzy fachowej organizacji i organów międzynarodowych działających w sferze kultury oraz ich doświadczenia związanego z nielegalnym handlem dobrami kultury, zalecenia i wytyczne wydawane przez te organizacje i organy powinny być uwzględniane w ramach wspólnego zarządzania ryzykiem przy określaniu ryzyka związanego z dobrami kultury. W szczególności czerwone listy publikowane przez ICOM powinny służyć jako wytyczne do identyfikacji tych państw trzecich, których dziedzictwo jest najbardziej zagrożone oraz wywożonych z nich obiektów, które mogłyby częściej stawać się przedmiotem nielegalnego handlu.

(27) Konieczne jest przygotowanie kampanii informacyjnych skierowanych do nabywców dóbr kultury, dotyczących ryzyka nielegalnego handlu oraz wspieranie podmiotów działających na rynku w zakresie zrozumienia i stosowania przez nie niniejszego rozporządzenia. Państwa członkowskie powinny angażować w rozpowszechnianie tych informacji odpowiednie krajowe punkty kontaktowe oraz inne służby informacyjne.

(28) Komisja powinna zapewnić, aby mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa (zwane dalej „MŚP") korzystały z odpowiedniej pomocy technicznej oraz powinna ułatwiać dostarczanie im informacji w celu skutecznego wykonywania niniejszego rozporządzenia. MŚP z siedzibą w Unii, które dokonują przywozu dóbr kultury, powinny zatem korzystać z obecnych i przyszłych programów Unii mających na celu wspieranie konkurencyjności małych i średnich przedsiębiorstw.

(29) Aby zachęcić do przestrzegania przepisów oraz zniechęcać do ich obchodzenia, państwa członkowskie powinny wprowadzić skuteczne, proporcjonalne i odstraszające sankcje w przypadku nieprzestrzegania przepisów niniejszego rozporządzenia oraz przekazać informacje o tych sankcjach Komisji. Sankcje wprowadzane przez państwa członkowskie w przypadku naruszeń niniejszego rozporządzenia powinny mieć równoważny skutek odstraszający w całej Unii.

(30) Państwa członkowskie powinny zapewnić, aby organy celne i właściwe organy uzgadniały środki podejmowane na mocy art. 198 rozporządzenia (UE) nr 952/2013. Szczegóły dotyczące tych środków powinny podlegać prawu krajowemu.

(31) Komisja powinna niezwłocznie przyjąć przepisy wykonawcze do niniejszego rozporządzenia, w szczególności przepisy dotyczące zestandaryzowanych formularzy elektronicznych, z których należy korzystać przy składaniu wniosku o pozwolenie na przywóz lub przygotowywaniu oświadczenie importera, a także jak najszybciej ustanowić system elektroniczny. Stosowanie przepisów dotyczących pozwoleń na przywóz i oświadczeń importerów należy odpowiednio odroczyć.

(32) Zgodnie z zasadą proporcjonalności, konieczne i stosowne jest przyjęcie przepisów dotyczących wprowadzania oraz warunków i procedur przywozu dóbr kultury na obszar celny Unii, aby osiągnąć podstawowe cele niniejszego rozporządzenia. Niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów, zgodnie z art. 5 ust. 4 Traktatu o Unii Europejskiej,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot i zakres stosowania

1. Niniejsze rozporządzenie określa warunki wprowadzania dóbr kultury oraz warunki i procedury przywozu dóbr kultury w celu ochrony dziedzictwa kulturowego ludzkości oraz zapobiegania nielegalnemu handlowi dobrami kultury, w szczególności w przypadku gdy taki nielegalny handel mógłby przyczynić się do finansowania terroryzmu.

2. Niniejsze rozporządzenie nie ma zastosowania do dóbr kultury, które powstały lub zostały odkryte na obszarze celnym Unii.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „dobra kultury" oznacza każdy przedmiot, który ma znaczenie dla archeologii, prehistorii, historii, literatury, sztuki lub nauki, wymieniony w załączniku;

2) „wprowadzenie dóbr kultury" oznacza każde wprowadzenie na obszar celny Unii dóbr kultury, które podlegają dozorowi celnemu lub kontroli celnej na obszarze celnym Unii, zgodnie z rozporządzeniem (UE) nr 952/2013;

3) „przywóz dóbr kultury" oznacza:

a) dopuszczenie dóbr kultury do obrotu, o którym mowa w art. 201 rozporządzenia (UE) nr 952/2013; lub

b) objęcie dóbr kultury jedną z następujących kategorii procedur specjalnych, o których mowa w art. 210 rozporządzenia (UE) nr 952/2013:

(i) składowaniem, które obejmuje składowanie celne i wolne obszary celne;

(ii) szczególnym przeznaczeniem, które obejmuje odprawę czasową i końcowe przeznaczenie;

(iii) uszlachetnianiem czynnym;

4) „posiadacz towarów" oznacza posiadacza towarów zgodnie z definicją w art. 5 pkt 34 rozporządzenia (UE) nr 952/2013;

5) „właściwe organy" oznacza organy publiczne wyznaczone przez państwa członkowskie do wydawania pozwoleń na przywóz.

Artykuł 3

Wprowadzanie i przywóz dóbr kultury

1. Wprowadzanie dóbr kultury, o których mowa w części A załącznika, które zostały wyprowadzone z terytorium kraju, w którym powstały lub zostały odkryte, z naruszeniem przepisów ustawowych i wykonawczych tego kraju jest zabronione.

Organy celne i właściwe organy podejmują wszelkie odpowiednie środki w przypadku próby wprowadzenia dóbr kultury, o których mowa w akapicie pierwszym.

2. Przywóz dóbr kultury wymienionych w częściach B i C załącznika jest dozwolony jedynie po przedstawieniu:

a) pozwolenia na przywóz wydanego zgodnie z art. 4; albo

b) oświadczenia importera przedłożonego zgodnie z art. 5.

3. Pozwolenie na przywóz lub oświadczenie importera, o którym mowa w ust. 2 niniejszego artykułu, przedstawia się organom celnym zgodnie z art. 163 rozporządzenia (UE) nr 952/2013. W przypadku obejmowania dóbr kultury procedurą wolnego obszaru celnego, posiadacz dóbr przedstawia pozwolenie na przywóz lub oświadczenie importera przy przedstawianiu towarów zgodnie z art. 245 ust. 1 lit. a) i b) rozporządzenia (UE) nr 952/2013.

4. Ust. 2 niniejszego artykułu nie ma zastosowania do:

a) dóbr kultury, które są towarami powracającymi w rozumieniu art. 203 rozporządzenia (UE) nr 952/2013;

b) przywozu dóbr kultury w wyłącznym celu zapewnienia ich bezpiecznego przechowywania przez organ publiczny lub pod nadzorem takiego organu, z zamiarem dokonania zwrotu tych dóbr kultury, gdy sytuacja na to pozwoli;

c) odprawy czasowej dóbr kultury, w rozumieniu art. 250 rozporządzenia (UE) nr 952/2013, na obszarze celnym Unii do celów edukacyjnych, naukowych, konserwacji, restauracji, wystawienniczych, digitalizacji, przedstawień artystycznych, badań prowadzonych przez instytucje naukowe lub współpracy pomiędzy muzeami lub podobnymi instytucjami.

5. Pozwolenie na przywóz nie jest wymagane w przypadku dóbr kultury objętych procedurą odprawy czasowej w rozumieniu art. 250 rozporządzenia (UE) nr 952/2013, w przypadku gdy takie dobra mają być wystawione na komercyjnych targach sztuki. W takich przypadkach przedstawia się oświadczenie importera zgodnie z procedurą określoną w art. 5 niniejszego rozporządzenia.

Jeżeli jednak te dobra kultury są następnie obejmowane inną procedurą celną, o której mowa w art. 2 pkt 3 niniejszego rozporządzenia, wymagane jest pozwolenie na przywóz wydane zgodnie z art. 4 niniejszego rozporządzenia.

6. Komisja określa, w drodze aktów wykonawczych, szczegółowe zasady dotyczące dóbr kultury, które są towarami powracającymi, przywozu dóbr kultury w celu ich bezpiecznego przechowywania oraz odprawy czasowej dóbr kultury, o których mowa w ust. 4 i 5 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 13 ust. 2.

7. Ust. 2 niniejszego artykułu pozostaje bez uszczerbku dla innych środków przyjętych przez Unię zgodnie z art. 215 Traktatu o funkcjonowaniu Unii Europejskiej.

8. W przywozowym zgłoszeniu celnym dóbr kultury wymienionych w częściach B i C załącznika podaje się liczbę towarów za pomocą jednostki uzupełniającej określonej w niniejszym załączniku. W przypadku obejmowania dóbr kultury procedurą wolnego obszaru celnego, posiadacz dóbr podaje liczbę przedmiotów przy przedstawianiu dóbr zgodnie z art. 245 ust. 1 lit. a) i b) rozporządzenia (UE) nr 952/2013.

Artykuł 4

Pozwolenie na przywóz

1. Na przywóz dóbr kultury wymienionych w części B załącznika, innych niż te, o których mowa w art. 3 ust. 4 i 5, wymagane jest pozwolenie. Pozwolenie na przywóz wydaje właściwy organ państwa członkowskiego, w którym dobra kultury obejmowane są po raz pierwszy jedną z procedur celnych, o których mowa w art. 2 ust. 3.

2. Pozwolenia na przywóz wydane przez właściwe organy państwa członkowskiego zgodnie z niniejszym artykułem są ważne w całej Unii.

3. Pozwolenia na przywóz wydanego zgodnie z niniejszym artykułem nie traktuje się jako dowodu legalnego pochodzenia lub własności danych dóbr kultury.

4. Posiadacz dóbr składa wniosek o pozwolenie na przywóz do właściwego organu państwa członkowskiego, o którym mowa w ust. 1 niniejszego artykułu, za pomocą systemu elektronicznego, o którym mowa w art. 8. Do wniosku dołącza się wszelkie dokumenty i informacje będące dowodem, że dane dobra kultury zostały wywiezione z kraju, w którym powstały lub zostały odkryte zgodnie z przepisami ustawowymi i wykonawczymi tego kraju lub będące dowodem braku takich przepisów ustawowych i wykonawczych w okresie, w którym zostały wywiezione z jego terytorium.

Na zasadzie odstępstwa od akapitu pierwszego wnioskowi mogą zamiast tego towarzyszyć wszelkie dokumenty i informacje będące dowodem, że dane dobra kultury zostały wywiezione zgodnie z przepisami ustawowymi i wykonawczymi ostatniego kraju, w którym znajdowały się przez okres dłuższy niż pięć lat w celach innych niż do użytku tymczasowego, tranzytu, powrotnego wywozu lub przeładunku, w następujących przypadkach:

a) nie można wiarygodnie ustalić, w jakim kraju dobra kultury powstały lub zostały odkryte; lub

b) dobra kultury zostały wywiezione z kraju, w którym powstały lub zostały odkryte, przed dniem 24 kwietnia 1972 r.

5. Dowód, że dane dobra kultury zostały wywiezione zgodnie z ust. 4 przedstawia się w postaci świadectw wywozowych lub pozwoleń na wywóz w przypadku gdy dane państwo ustanowiło takie dokumenty dla wywozu dóbr kultury w czasie ich wywozu.

6. Właściwy organ sprawdza, czy wniosek jest kompletny. Zwraca się do wnioskodawcy o wszelkie brakujące lub dodatkowe informacje lub dokumenty w terminie 21 dni od dnia otrzymania wniosku.

7. W terminie 90 dni od otrzymania kompletnego wniosku właściwy organ bada go i podejmuje decyzję o wydaniu pozwolenia na przywóz lub odrzuca wniosek.

Właściwy organ odrzuca wniosek w przypadku gdy:

a) posiada informacje lub ma uzasadnione powody, aby sądzić, że dobra kultury zostały wyprowadzone z terytorium kraju, w którym powstały lub zostały odkryte, z naruszeniem przepisów ustawowych i wykonawczych tego kraju;

b) nie został przedstawiony dowód wymagany na mocy ust. 4;

c) posiada informacje lub ma uzasadnione podstawy, aby sądzić, że posiadacz towarów nie nabył ich legalnie; lub

d) został poinformowany, że istnieją nierozpatrzone wnioski o zwrot tych dóbr kultury złożone przez organy kraju, w którym powstały lub zostały odkryte.

8. W przypadku odrzucenia wniosku, wnioskodawcy przekazuje się niezwłocznie decyzję administracyjną, o której mowa w ust. 7, wraz z uzasadnieniem oraz informacją o procedurze odwoławczej.

9. W przypadku gdy wniosek dotyczy pozwolenia na przywóz dóbr kultury, w odniesieniu do których wcześniej odrzucono taki wniosek, wnioskodawca informuje właściwy organ, do którego składany jest wniosek, o poprzednim odrzuceniu.

10. W przypadku gdy państwo członkowskie odrzuca wniosek, informuje o tym odrzuceniu, a także o powodach tego odrzucenia pozostałe państwa członkowskie i Komisję za pomocą systemu elektronicznego, o którym mowa w art. 8.

11. Państwa członkowskie wyznaczają niezwłocznie właściwe organy do celów wydawania pozwoleń na przywóz zgodnie z niniejszym artykułem. Państwa członkowskie przekazują Komisji informacje o właściwych organach, a także o wszelkich zmianach w tym zakresie.

Komisja publikuje informacje o właściwych organach oraz wszelkie zmiany w tym zakresie w serii C *Dziennika Urzędowego Unii Europejskiej*.

12. Komisja określa, w drodze aktów wykonawczych, wzór i format wniosku o pozwolenie na przywóz oraz wskazuje dopuszczalne dokumenty do celów udowodnienia legalnego pochodzenia danych dóbr kultury, a także przepisy proceduralne dotyczące składania i rozpatrywania takiego wniosku. Ustanawiając te elementy, Komisja dąży do osiągnięcia jednolitego stosowania przez właściwe organy procedur wydawania pozwoleń na przywóz. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 13 ust. 2.

Artykuł 5

Oświadczenie importera

1. Na przywóz dóbr kultury wymienionych w części C załącznika wymagane jest oświadczenie importera, które posiadacz towarów składa za pomocą systemu elektronicznego, o którym mowa w art. 8.

2. Oświadczenie importera zawiera:

a) deklarację podpisaną przez posiadacza towarów, stwierdzającą, że zostały one wywiezione z kraju, w którym powstały lub zostały odkryte, zgodnie z przepisami ustawowymi i wykonawczymi tego kraju obowiązującymi w czasie, w którym zostały one wywiezione z jego terytorium; oraz

b) zestandaryzowany dokument opisujący dane dobra kultury w sposób wystarczająco szczegółowy i umożliwiający ich identyfikację przez organy oraz przeprowadzenie analizy ryzyka i ukierunkowanych kontroli.

Na zasadzie odstępstwa od akapitu pierwszego lit. a) deklaracja może zamiast tego stwierdzać, że dane dobra kultury zostały wywiezione zgodnie z przepisami ustawowymi i wykonawczymi ostatniego kraju, w którym znajdowały się przez okres dłuższy niż pięć lat w celach innych niż do użytku tymczasowego, tranzytu, powrotnego wywozu lub przeładunku, w następujących przypadkach:

a) nie można wiarygodnie ustalić, w jakim kraju dobra kultury powstały lub zostały odkryte; lub

b) dobra kultury zostały wywiezione z kraju, w którym powstały lub zostały odkryte, przed dniem 24 kwietnia 1972 r.

3. Komisja określa, w drodze aktów wykonawczych, zestandaryzowany wzór i format oświadczenia importera, a także przepisy proceduralne dotyczące jego składania oraz wskazuje dopuszczalne dokumenty do celów udowodnienia legalnego pochodzenia danych dóbr kultury, które powinien mieć posiadacz towarów, oraz przepisy dotyczące przetwarzania takiego oświadczenia importera. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 13 ust. 2.

Artykuł 6

Właściwe urzędy celne

Państwa członkowskie mogą ograniczyć liczbę urzędów celnych właściwych do przywozu dóbr kultury objętych niniejszym rozporządzeniem. W przypadku gdy państwa członkowskie zastosują takie ograniczenie, przekazują Komisji informacje o tych urzędach celnych, a także o wszelkich zmianach w tym zakresie.

Komisja publikuje szczegółowe dane właściwych urzędów celnych oraz wszelkie zmiany w tym zakresie w serii C *Dziennika Urzędowego Unii Europejskiej*.

Artykuł 7

Współpraca administracyjna

Do celów wykonywania niniejszego rozporządzenia państwa członkowskie zapewniają współpracę między swoimi organami celnymi oraz z właściwymi organami, o których mowa w art. 4.

Artykuł 8

Stosowanie systemu elektronicznego

1. Przechowywanie i wymiana informacji między organami państw członkowskich, w szczególności w odniesieniu do pozwoleń na przywóz i oświadczeń importerów, odbywa się za pomocą centralnego systemu elektronicznego.

W przypadku czasowej awarii systemu elektronicznego mogą być stosowane czasowo inne sposoby przechowywania i wymiany informacji.

2. Komisja określa w drodze aktów wykonawczych:

a) zasady dotyczące wdrożenia, funkcjonowania i utrzymywania systemu elektronicznego, o którym mowa w ust. 1;

b) szczegółowe przepisy dotyczące przedstawiania, przetwarzania, przechowywania i wymiany informacji między organami państw członkowskich za pomocą systemu elektronicznego lub innych sposobów, o których mowa w ust. 1.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 13 ust. 2, do dnia 28 czerwca 2021 r.

Artykuł 9

Ustanowienie systemu elektronicznego

Komisja ustanawia system elektroniczny, o którym mowa w art. 8. System elektroniczny musi stać się operacyjny najpóźniej cztery lata po wejściu w życie pierwszego z aktów wykonawczych, o których mowa w art. 8 ust. 2.

Artykuł 10

Ochrona danych osobowych i okresy przechowywania danych

1. Organy celne i właściwe organy państw członkowskich działają jako administratorzy danych osobowych uzyskanych zgodnie z art. 4, 5 i 8.

2. Przetwarzanie danych osobowych na podstawie niniejszego rozporządzenia odbywa się wyłącznie w celu określonym w art. 1 ust. 1.

3. Dostęp do danych osobowych uzyskanych zgodnie z art. 4, 5 i 8 mają wyłącznie należycie uprawnieni pracownicy organów, a dane te muszą być odpowiednio chronione przed nieuprawnionym dostępem lub przekazaniem. Dane nie mogą być ujawniane ani przekazywane bez wyraźnej pisemnej zgody organu, który pierwotnie je uzyskał. Zgoda ta nie jest jednak konieczna, jeżeli organy mają obowiązek ujawnić lub przekazać dane na mocy przepisów obowiązujących w danym państwie członkowskim, w szczególności w związku z postępowaniem sądowym.

4. Organy przechowują dane osobowe uzyskane zgodnie z art. 4, 5 i 8 przez okres 20 lat od dnia ich uzyskania. Po upływie tego okresu takie dane osobowe usuwa się.

Artykuł 11

Sankcje

Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia i podejmują wszelkie niezbędne środki w celu zapewnienia ich wykonywania. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające.

Do dnia 28 grudnia 2020 r. państwa członkowskie powiadamiają Komisję o przepisach dotyczących sankcji mających zastosowanie w przypadku wprowadzania dóbr kultury z naruszeniem art. 3 ust. 1 oraz o związanych z nimi środkach.

Do dnia 28 czerwca 2025 r. państwa członkowskie powiadamiają Komisję o przepisach dotyczących sankcji za inne naruszenia niniejszego rozporządzenia, a w szczególności składania fałszywych oświadczeń i przekazywania fałszywych informacji, oraz o związanych z nimi środkach.

Państwa członkowskie niezwłocznie powiadamiają Komisję o wszelkich późniejszych zmianach dotyczących tych przepisów.

Artykuł 12

Współpraca z państwami trzecimi

Komisja, w kwestiach objętych jej działaniami oraz w zakresie wymaganym do wypełniania jej zadań wynikających z niniejszego rozporządzenia, może zorganizować dla państw trzecich, we współpracy z państwami członkowskimi, szkolenia oraz działania związane z budowaniem zdolności.

Artykuł 13

Procedura komitetowa

1. Komisję wspomaga komitet ustanowiony na mocy art. 8 rozporządzenia Rady (WE) nr 116/2009. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 14

Sprawozdawczość i ocena

1. Państwa członkowskie przekazują Komisji informacje na temat wykonania niniejszego rozporządzenia.

W tym celu Komisja przesyła odpowiednie kwestionariusze do państw członkowskich. Państwa członkowskie mają sześć miesięcy od otrzymania kwestionariusza na przekazanie Komisji żądanych informacji.

2. W terminie trzech lat od dnia rozpoczęcia stosowania niniejszego rozporządzenia w całości, a następnie co pięć lat Komisja przedstawi Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące wykonania niniejszego rozporządzenia. Sprawozdanie będzie podawane do wiadomości publicznej i będzie zawierać istotne informacje statystyczne, zarówno na poziomie unijnym, jak i krajowym, takie jak liczba wydanych pozwoleń na przywóz, odrzuconych wniosków oraz złożonych oświadczeń importerów. Będzie zawierać uwagi na temat praktycznego wykonania, w tym wpływu na unijne podmioty gospodarcze, w szczególności MŚP.

3. Do dnia 28 czerwca 2020 r., a następnie co dwanaście miesięcy, do momentu ustanowienia systemu elektronicznego określonego w art. 9, Komisja będzie przedkładać Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące postępów w zakresie przyjmowania aktów wykonawczych zgodnie z art. 8 ust. 2 oraz postępów w zakresie ustanowienia systemu elektronicznego określonego w art. 9.

Artykuł 15

Wejście w życie

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

Artykuł 16

Stosowanie

1. Niniejsze rozporządzenie stosuje się od dnia jego wejścia w życie.

2. Niezależnie od ust. 1:

a) art. 3 ust. 1 stosuje się od dnia 28 grudnia 2020 r.;

b) art. 3 ust. 2–5 oraz ust. 7 i 8, art. 4 ust. 1–10, art. 5 ust. 1 i 2 oraz art. 8 ust. 1 stosuje się od dnia rozpoczęcia funkcjonowania systemu elektronicznego, o którym mowa w art. 8, lub najpóźniej od dnia 28 czerwca 2025 r. Komisja opublikuje w serii C *Dziennika Urzędowego Unii Europejskiej* datę spełnienia wszystkich warunków określonych w niniejszym ustępie.

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

Część A. Dobra kultury objęte zakresem art. 3 ust. 1

a) rzadkie kolekcje i okazy zoologiczne, botaniczne, mineralogiczne i anatomiczne oraz przedmioty o wartości paleontologicznej;

b) dobra związane z historią, w tym historią nauki i techniki, historią wojskowości i historią społeczną, z życiem krajowych przywódców, myślicieli, naukowców i artystów oraz z ważnymi dla danego kraju wydarzeniami;

c) przedmioty pochodzące z wykopalisk archeologicznych (w tym legalnych i nielegalnych) lub z odkryć archeologicznych na lądzie lub pod wodą;

d) elementy zabytków artystycznych lub historycznych, lub stanowisk archeologicznych, które zostały rozczłonkowane ([1]);

e) antyki mające ponad sto lat, takie jak inskrypcje, monety i grawerowane pieczęci;

f) przedmioty o wartości etnograficznej;

g) przedmioty o wartości artystycznej, takie jak:

(i) obrazy, malarstwo i rysunki wykonane wyłącznie ręcznie na dowolnym podłożu i przy użyciu dowolnych materiałów (z wyjątkiem wzorów przemysłowych i artykułów przemysłowych zdobionych ręcznie);

(ii) oryginalne posągi i rzeźby z dowolnych materiałów;

(iii) oryginalne ryciny, druki i litografie;

(iv) oryginalne asamblaże i kompozycje z dowolnych materiałów;

h) rzadkie manuskrypty i inkunabuły;

i) stare książki, dokumenty i publikacje o szczególnym znaczeniu (historycznym, artystycznym, naukowym, literackim itp.), pojedynczo lub w zbiorach;

j) znaczki pocztowe, skarbowe i podobne znaczki, pojedynczo lub w zbiorach;

k) archiwa, w tym fonograficzne, fotograficzne i kinematograficzne;

l) artykuły meblarskie mające ponad sto lat i dawne instrumenty muzyczne.

([1]) Liturgiczne ikony i posągi, nawet wolnostojące, są uważane za należące do tej kategorii dóbr kultury.

Część B. Dobra kultury objęte zakresem art. 4

Kategorie dóbr kultury zgodnie z częścią A	Nomenklatura scalona (CN), dział, pozycja lub podpozycja	Próg minimalnego wieku	Próg minimalnej wartości (wartość celna)	Jednostki uzupełniające
c) przedmioty pochodzące z wykopalisk archeologicznych (w tym legalnych i nielegalnych), lub z odkryć archeologicznych na lądzie lub pod wodą;	ex 9705; ex 9706	Starsze niż 250 lat	Niezależnie od wartości	Liczba sztuk (p/st)
d) elementy zabytków artystycznych lub historycznych, lub stanowisk archeologicznych, które zostały rozczłonkowane ([1]);	ex 9705; ex 9706	Starsze niż 250 lat	Niezależnie od wartości	Liczba sztuk (p/st)

([1]) Liturgiczne ikony i posągi, nawet wolnostojące, są uważane za należące do tej kategorii dóbr kultury.

Część C. Dobra kultury objęte zakresem art. 5

Kategorie dóbr kultury zgodnie z częścią A	Nomenklatura scalona (CN), dział, pozycja lub podpozycja	Próg minimalnego wieku	Próg minimalnej wartości (wartość celna)	Jednostki uzupełniające
a) rzadkie kolekcje i okazy zoologiczne, botaniczne, mineralogiczne i anatomiczne oraz przedmioty o wartości paleontologicznej;	ex 9705	Starsze niż 200 lat	18 000 EUR lub więcej za sztukę	Liczba sztuk (p/st)
b) dobra związane z historią, w tym historią nauki i techniki, historią wojskowości i historią społeczną, życiem krajowych przywódców, myślicieli, naukowców i artystów oraz ważnymi dla danego kraju wydarzeniami;	ex 9705	Starsze niż 200 lat	18 000 EUR lub więcej za sztukę	Liczba sztuk (p/st)
e) antyki, takie jak inskrypcje, monety i grawerowane pieczęci;	ex 9706	Starsze niż 200 lat	18 000 EUR lub więcej za sztukę	Liczba sztuk (p/st)
f) przedmioty o wartości etnograficznej;	ex 9705	Starsze niż 200 lat	18 000 EUR lub więcej za sztukę	Liczba sztuk (p/st)
g) przedmioty o wartości artystycznej, takie jak:				
(i) obrazy, malarstwo i rysunki wykonane wyłącznie ręcznie na dowolnym podłożu przy użyciu dowolnych materiałów (z wyjątkiem wzorów przemysłowych i artykułów przemysłowych zdobionych ręcznie);	ex 9701	Starsze niż 200 lat	18 000 EUR lub więcej za sztukę	Liczba sztuk (p/st)

Kategorie dóbr kultury zgodnie z częścią A	Nomenklatura scalona (CN), dział, pozycja lub podpozycja	Próg minimalnego wieku	Próg minimalnej wartości (wartość celna)	Jednostki uzupełniające
(ii) oryginalne posągi i rzeźby z dowolnych materiałów;	ex 9703	Starsze niż 200 lat	18 000 EUR lub więcej za sztukę	Liczba sztuk (p/st)
(iii) oryginalne ryciny, druki i litografie;	ex 9702;	Starsze niż 200 lat	18 000 EUR lub więcej za sztukę	Liczba sztuk (p/st)
(iv) oryginalne asamblaże i kompozycje z dowolnych materiałów;	ex 9701	Starsze niż 200 lat	18 000 EUR lub więcej za sztukę	Liczba sztuk (p/st)
h) rzadkie manuskrypty i inkunabuły;	ex 9702; ex 9706	Starsze niż 200 lat	18 000 EUR lub więcej za sztukę	Liczba sztuk (p/st)
i) stare książki, dokumenty i publikacje o szczególnym znaczeniu (historycznym, artystycznym, naukowym, literackim itp.), pojedynczo lub w zbiorach;	ex 9705; ex 9706	Starsze niż 200 lat	18 000 EUR lub więcej za sztukę	Liczba sztuk (p/st)

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.

DYREKTYWY

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/882

z dnia 17 kwietnia 2019 r.

w sprawie wymogów dostępności produktów i usług

(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]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

a także mając na uwadze, co następuje:

(1) Celem niniejszej dyrektywy jest przyczynienie się do właściwego funkcjonowania rynku wewnętrznego w drodze zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich w odniesieniu do wymogów dostępności niektórych produktów i usług, w szczególności poprzez wyeliminowanie i zapobieganie powstawaniu barier dla swobodnego przepływu niektórych dostępnych produktów i usług, które wynikają z rozbieżnych wymogów dostępności w poszczególnych państwach członkowskich. Zwiększyłoby to podaż na rynku wewnętrznym dostępnych produktów i usług, a także poprawiło dostępność stosownych informacji.

(2) Popyt na dostępne produkty i usługi jest wysoki, a przewiduje się, że liczba osób z niepełnosprawnościami znacznie wzrośnie. Środowisko, w którym produkty i usługi są bardziej dostępne, umożliwia większe włączenie społeczne i ułatwia osobom z niepełnosprawnościami prowadzenie niezależnego życia. W tym kontekście należy pamiętać, że w Unii niepełnosprawność częściej występuje wśród kobiet niż mężczyzn.

(3) Niniejsza dyrektywa definiuje osoby z niepełnosprawnościami zgodnie z Konwencją ONZ o prawach osób niepełnosprawnych przyjętą w dniu 13 grudnia 2006 r. (zwaną dalej „Konwencją"), której Unia jest stroną od dnia 21 stycznia 2011 r. i którą ratyfikowały wszystkie państwa członkowskie. Konwencja stwierdza, że „do »osób niepełnosprawnych« zalicza się te osoby, które mają długotrwale naruszoną sprawność fizyczną, psychiczną, intelektualną lub w zakresie zmysłów co może, w oddziaływaniu z różnymi barierami, utrudniać im pełny i skuteczny udział w życiu społecznym na zasadzie równości z innymi osobami". Niniejsza dyrektywa promuje pełny i skuteczny udział w życiu społecznym na równych prawach poprzez poprawę dostępu do powszechnie używanych produktów i usług, które z uwagi na swój pierwotny projekt lub późniejsze dostosowanie zaspokajają szczególne potrzeby osób z niepełnosprawnościami.

(4) Niniejsza dyrektywa przyniesie korzyść również innym osobom, które doświadczają ograniczeń funkcjonalnych, takim jak osoby starsze, kobiety w ciąży czy osoby podróżujące z bagażem. Pojęcie „osób z ograniczeniami funkcjonalnymi", o których mowa w niniejszej dyrektywie, obejmuje osoby, które mają naruszoną sprawność fizyczną, psychiczną, intelektualną lub w zakresie zmysłów, osoby, które doświadczają naruszenia sprawności wynikającego z wieku lub z innych przyczyn związanych z niepełną sprawnością fizyczną, w sposób trwały lub czasowy, które to naruszenia sprawności mogą, w oddziaływaniu z różnymi barierami, zmniejszać dostęp takich osób do produktów i usług, co z kolei prowadzi do sytuacji wymagającej dostosowań tych produktów i usług do szczególnych potrzeb takich osób.

(5) Rozbieżności pomiędzy przepisami prawnymi i środkami administracyjnymi państw członkowskich w zakresie dostępności produktów i usług dla osób z niepełnosprawnościami stwarzają bariery dla swobodnego przepływu produktów i usług oraz zakłócają skuteczną konkurencję na rynku wewnętrznym. W przypadku niektórych produktów i usług rozbieżności te prawdopodobnie będą się pogłębiać w Unii w związku z wejściem w życie Konwencji. Bariery te mają szczególny wpływ na podmioty gospodarcze, w szczególności na małe i średnie przedsiębiorstwa (MŚP).

([1]) Dz.U. C 303 z 19.8.2016, s. 103.

([2]) Stanowisko Parlamentu Europejskiego z dnia 13 marca 2019 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 9 kwietnia 2019 r.

(6) Z uwagi na różnice pomiędzy krajowymi wymogami dostępności indywidualni przedsiębiorcy, MŚP i mikroprzedsiębiorstwa w szczególności zniechęcani są do podejmowania przedsięwzięć biznesowych poza swoim rynkiem krajowym. Ustanowione przez państwa członkowskie krajowe, a nawet regionalne czy lokalne wymogi dostępności różnią się obecnie zarówno pod względem zakresu, jak i poziomu szczegółowości. Te różnice wywierają negatywny wpływ na konkurencyjność i wzrost gospodarczy ze względu na dodatkowe koszty ponoszone w związku z tworzeniem i wprowadzaniem na każdy rynek krajowy dostępnych produktów i usług.

(7) Konsumenci dostępnych produktów i usług oraz technologii wspomagających muszą płacić wysokie ceny ze względu na ograniczoną konkurencję wśród dostawców. Rozdrobnienie regulacji krajowych ogranicza ewentualne korzyści pochodzące z wymiany z partnerami krajowymi i międzynarodowymi doświadczeń w kwestii reagowania na zmiany społeczne i technologiczne.

(8) Zbliżenie środków krajowych na poziomie Unii jest zatem niezbędne dla prawidłowego funkcjonowania rynku wewnętrznego, aby położyć kres rozdrobnieniu rynku dostępnych produktów i usług, uzyskać korzyści skali, ułatwić handel transgraniczny i transgraniczną mobilność, a także pomóc podmiotom gospodarczym w koncentrowaniu zasobów na innowacjach, zamiast wykorzystywania ich na wydatki wynikające z rozdrobnienia przepisów w Unii.

(9) Korzyści wynikające z harmonizacji wymogów dotyczących dostępności na rynku wewnętrznym zostały potwierdzone poprzez stosowanie dyrektywy Parlamentu Europejskiego i Rady 2014/33/UE ([3]) w odniesieniu do dźwigów oraz rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 661/2009 ([4]) w dziedzinie transportu.

(10) W załączonej do Traktatu z Amsterdamu deklaracji nr 22 w sprawie osób niepełnosprawnych przyjętej na konferencji przedstawicieli rządów państw członkowskich zawarto uzgodnienie, że przy opracowywaniu środków na mocy art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) instytucje Unii mają brać pod uwagę potrzeby osób z niepełnosprawnościami.

(11) Ogólnym celem komunikatu Komisji z dnia 6 maja 2015 r. pt. „Strategia jednolitego rynku cyfrowego dla Europy" jest uzyskanie z połączonego jednolitego rynku cyfrowego trwałych korzyści ekonomicznych i społecznych, co ułatwi handel i będzie wspierać zatrudnienie w Unii. Unijni konsumenci wciąż nie mogą w pełni korzystać z niższych cen i z większego wyboru, które może zapewnić jednolity rynek, ponieważ transakcje transgraniczne on-line nadal są bardzo ograniczone. Fragmentacja ogranicza też popyt na transgraniczne transakcje handlu elektronicznego. Potrzebne są również wspólne działania, aby osobom z niepełnosprawnościami zapewnić pełny dostęp do treści elektronicznych, usług łączności elektronicznej i audiowizualnych usług medialnych. Należy zatem zharmonizować wymogi dostępności na całym jednolitym rynku cyfrowym oraz zapewnić, by wszyscy obywatele Unii, bez względu na stopień sprawności, mogli czerpać z niego korzyści.

(12) Ponieważ Unia została stroną Konwencji, postanowienia Konwencji stały się integralną częścią porządku prawnego Unii i są wiążące dla instytucji Unii i dla państw członkowskich.

(13) Konwencja zobowiązuje swoje strony do wprowadzenia odpowiednich środków w celu zapewnienia osobom z niepełnosprawnościami, na równi z innymi, dostępu do środowiska fizycznego, środków transportu, informacji i komunikacji, w tym technologii i systemów informacyjno-komunikacyjnych, a także do innych urządzeń i usług, powszechnie dostępnych lub powszechnie zapewnianych, zarówno na obszarach miejskich, jak i wiejskich. Komitet ONZ ds. praw osób z niepełnosprawnościami wskazał na potrzebę stworzenia ram prawnych z konkretnymi, wykonalnymi i określonymi w czasie poziomami odniesienia w celu monitorowania stopniowego tworzenia warunków dostępności.

(14) Konwencja wzywa swoje strony do podejmowania lub wspierania badań naukowych i rozwoju nowych technologii odpowiednich dla osób z niepełnosprawnościami, w tym technologii informacyjno-komunikacyjnych, przyrządów ułatwiających poruszanie się, urządzeń i technologii wspomagających, a także do wspierania podaży i wykorzystywania takich nowych technologii. Konwencja apeluje także o priorytetowe traktowanie technologii przystępnych cenowo.

([3]) Dyrektywa Parlamentu Europejskiego i Rady 2014/33/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących dźwigów i elementów bezpieczeństwa do dźwigów (Dz.U. L 96 z 29.3.2014, s. 251).

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 661/2009 z dnia 13 lipca 2009 r. w sprawie wymagań technicznych w zakresie homologacji typu pojazdów silnikowych dotyczących ich bezpieczeństwa ogólnego, ich przyczep oraz przeznaczonych dla nich układów, części i oddzielnych zespołów technicznych (Dz.U. L 200 z 31.7.2009, s. 1).

(15) Wejście w życie Konwencji w porządkach prawnych państw członkowskich oznacza potrzebę przyjęcia dodatkowych przepisów krajowych dotyczących dostępności produktów i usług. Przy braku działań ze strony Unii przepisy te mogłyby doprowadzić do dalszego zwiększenia rozbieżności w przepisach ustawowych, wykonawczych i administracyjnych państw członkowskich.

(16) Konieczne jest zatem ułatwienie wdrażania Konwencji w Unii poprzez ustanowienie wspólnych unijnych przepisów. Niniejsza dyrektywa wspiera również działania państw członkowskich mające na celu zharmonizowaną realizację ich krajowych zobowiązań, jak również wynikających z Konwencji obowiązków dotyczących dostępności.

(17) W komunikacie Komisji z dnia 15 listopada 2010 r. pt. „Europejska strategia w sprawie niepełnosprawności 2010–2020: Odnowione zobowiązanie do budowania Europy bez barier" wskazano zgodnie z Konwencją dostępność jako jeden z ośmiu obszarów działań, stwierdzono, że stanowi ona jeden z podstawowych warunków uczestnictwa w życiu społecznym, oraz postawiono za cel zapewnienie dostępności produktów i usług.

(18) Produkty i usługi objęte zakresem stosowania niniejszej dyrektywy wskazano na podstawie badania przeprowadzonego w trakcie przygotowywania oceny skutków; badanie to pozwoliło zidentyfikować produkty i usługi, które są istotne dla osób z niepełnosprawnościami oraz w odniesieniu do których państwa członkowskie przyjęły lub mogą przyjąć rozbieżne krajowe wymogi dostępności, co zakłócałoby funkcjonowanie rynku wewnętrznego.

(19) Aby zapewnić dostępność usług, które są objęte zakresem stosowania niniejszej dyrektywy, wykorzystane do świadczenia takich usług produkty, z którymi konsument wchodzi w interakcję, również powinny spełniać odpowiednie wymogi dostępności określone w niniejszej dyrektywie.

(20) Nawet jeżeli usługa lub część usługi jest świadczona przez podwykonawcę, nie powinno to ograniczać dostępności tej usługi, a usługodawcy powinni wywiązywać się z obowiązków wynikających z niniejszej dyrektywy. Usługodawcy powinni także zapewnić właściwe i ustawiczne szkolenie swoich pracowników w celu zapewnienia, by wiedzieli oni, jak korzystać z dostępnych produktów i usług. Szkolenie to powinno obejmować kwestie, takie jak udzielanie informacji i porad oraz reklamę.

(21) Wymogi dostępności należy wprowadzić w sposób jak najmniej uciążliwy dla podmiotów gospodarczych i państw członkowskich.

(22) Istnieje potrzeba określenia wymogów dostępności dotyczących wprowadzania na rynek produktów i usług, które objęte są zakresem stosowania niniejszej dyrektywy, tak aby zapewnić ich swobodny przepływ na rynku wewnętrznym.

(23) Niniejsza dyrektywa powinna wprowadzić obowiązek stosowania funkcjonalnych wymogów dostępności, które powinny być wyrażane jako ogólne cele. Te wymogi powinny być wystarczająco precyzyjne, aby stwarzać prawnie wiążące zobowiązania, i wystarczająco szczegółowe, aby umożliwić ocenę zgodności w celu zapewnienia właściwego funkcjonowania wewnętrznego rynku produktów i usług objętych niniejszą dyrektywą, a także powinny pozostawiać pewien stopień elastyczności, by umożliwiać innowacje.

(24) Niniejsza dyrektywa zawiera szereg kryteriów funkcjonalnych dotyczących sposobów działania produktów i usług. Kryteriów tych nie należy uważać za ogólną alternatywę dla wymogów dostępności określonych w niniejszej dyrektywie, lecz powinny one być stosowane wyłącznie w szczególnych okolicznościach. Te kryteria powinny mieć zastosowanie do określonych funkcji lub cech produktów lub usług, tak aby stały się dostępne, w przypadkach gdy wymogi dostępności wynikające z niniejszej dyrektywy nie obejmują jednej lub kilku określonych funkcji lub cech. Ponadto, w sytuacji gdy jeden z wymogów dostępności zawiera konkretne wymogi techniczne, a dany produkt lub dana usługa obejmuje alternatywne rozwiązanie techniczne dla tych wymogów technicznych, to alternatywne rozwiązanie techniczne nadal powinno spełniać odnośne wymogi dostępności i powinno zapewniać równoważną lub większą dostępność poprzez zastosowanie odpowiednich kryteriów funkcjonalnych.

(25) Niniejsza dyrektywa powinna obejmować systemy sprzętu komputerowego ogólnego przeznaczenia. Aby systemy te funkcjonowały w sposób dostępny, ich systemy operacyjne również powinny być dostępne dla takich osób. Takie systemy sprzętu komputerowego cechują się wielofunkcyjnym charakterem oraz zdolnością do wykonywania, z odpowiednim oprogramowaniem, najczęstszych zadań informatycznych na żądanie konsumentów, i są przeznaczone do obsługi przez konsumentów. Przykładami takich systemów sprzętu komputerowego są komputery osobiste, w tym komputery stacjonarne, laptopy, smartfony i tablety. Specjalistyczne komputery wbudowane

w produkty elektroniki użytkowej nie są systemami sprzętu komputerowego ogólnego przeznaczenia. Niniejsza dyrektywa nie powinna obejmować, w poszczególnych przypadkach, pojedynczych komponentów mających specyficzne funkcje, takich jak płyta główna lub układ pamięci, które są wykorzystywane lub mogą być wykorzystywane w ramach takiego systemu.

(26) Niniejsza dyrektywa powinna również obejmować terminale płatnicze – w tym zarówno urządzenia, jak i oprogramowanie – i niektóre interaktywne terminale samoobsługowe, w tym zarówno urządzenia, jak i oprogramowanie, przeznaczone do świadczenia usług objętych zakresem stosowania niniejszej dyrektywy – np. bankomaty, automaty biletowe wydające fizyczne bilety zapewniające dostęp do usług, takie jak automaty wydające bilety komunikacyjne, urządzenia wydające bilety kolejkowe w placówkach bankowych, urządzenia do odprawy samoobsługowej i interaktywne terminale samoobsługowe udzielające informacji, w tym interaktywne ekrany informacyjne.

(27) Z zakresu stosowania niniejszej dyrektywy powinny jednak zostać wyłączone niektóre interaktywne terminale samoobsługowe udzielające informacji, instalowane jako zintegrowane części pojazdów, statków powietrznych, statków wodnych lub taboru kolejowego, ponieważ terminale te są częścią tych pojazdów, statków powietrznych, statków wodnych lub taboru kolejowego, które nie są objęte niniejszą dyrektywą.

(28) Niniejsza dyrektywa powinna również obejmować usługi łączności elektronicznej, w tym zgłoszenia alarmowe w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 ([5]). Obecnie w celu zapewnienia dostępu osobom z niepełnosprawnościami państwa członkowskie stosują różnorodne środki, które nie są zharmonizowane w obrębie rynku wewnętrznego. Zapewnienie, aby te same wymogi dostępności miały zastosowanie w całej Unii, prowadzić będzie do osiągnięcia przez podmioty gospodarcze działające w więcej niż jednym państwie członkowskim korzyści skali oraz ułatwi skuteczny dostęp osobom z niepełnosprawnościami zarówno przebywającym w swoich państwach członkowskich, jak i podróżującym po innych państwach członkowskich. Aby usługi łączności elektronicznej, w tym zgłoszenia alarmowe, były dostępne, usługodawcy oprócz głosu powinni zapewniać usługi tekstu w czasie rzeczywistym i – gdy oferują wideo – pełnej konwersacji wideo i tekstowej, zapewniając synchronizację wszystkich tych środków łączności. Poza wymogami niniejszej dyrektywy, zgodnie z dyrektywą (UE) 2018/1972, państwa członkowskie powinny być w stanie wskazać podmiot świadczący usługi przekazu, z których to usług mogłyby korzystać osoby z niepełnosprawnościami.

(29) Niniejsza dyrektywa harmonizuje wymogi dostępności w odniesieniu do usług łączności elektronicznej oraz do związanych z nimi produktów oraz jest uzupełnieniem dyrektywy (UE) 2018/1972, która ustanawia wymogi dotyczące równorzędnego dostępu i wyboru dla użytkowników końcowych z niepełnosprawnościami. Dyrektywa (UE) 2018/1972 ustanawia także – w ramach ogólnych obowiązków dotyczących usług – wymogi w zakresie przystępności cenowej dostępu do internetu i komunikacji głosowej oraz przystępności cenowej i dostępności związanych z nimi urządzeń końcowych oraz specjalnych urządzeń i usług dla konsumentów z niepełnosprawnościami.

(30) Niniejsza dyrektywa powinna także obejmować konsumenckie urządzenia końcowe mające interaktywne zdolności obliczeniowe przewidziane do wykorzystywania głównie przy uzyskiwaniu dostępu do usług łączności elektronicznej. Na potrzeby niniejszej dyrektywy należy uznać, że urządzenia te obejmującą urządzenia wykorzystywane jako część struktury zapewniającej dostęp do usług łączności elektronicznej, takie jak router lub modem.

(31) Na potrzeby niniejszej dyrektywy dostęp do audiowizualnych usług medialnych powinien oznaczać, że istnieje dostęp do treści audiowizualnych i mechanizmów, które umożliwiają użytkownikom z niepełnosprawnościami korzystanie z potrzebnych im technologii wspomagających. Usługi umożliwiające dostęp do audiowizualnych usług medialnych mogą obejmować strony internetowe, aplikacje internetowe, aplikacje oparte na urządzeniach typu set-top box, aplikacje do pobrania, usługi oparte na urządzeniach mobilnych, w tym aplikacje mobilne oraz powiązane odtwarzacze multimedialne, jak również usługi w zakresie telewizji hybrydowej. Dostępność audiowizualnych usług medialnych uregulowana jest dyrektywą Parlamentu Europejskiego i Rady 2010/13/UE ([6]), z wyjątkiem dostępności elektronicznych przewodników po programach, które są objęte definicją usług umożliwiających dostęp do audiowizualnych usług medialnych, do których zastosowanie ma niniejsza dyrektywa.

(32) W kontekście usług lotniczego, autobusowego, kolejowego i wodnego transportu pasażerskiego niniejsza dyrektywa powinna obejmować między innymi udzielanie informacji o usługach transportowych, w tym informacji o podróży udzielanych w czasie rzeczywistym za pośrednictwem stron internetowych, usług opartych na urządzeniach mobilnych, interaktywnych ekranów informacyjnych i interaktywnych terminali samoobsługowych, które

([5]) 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).

([6]) Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (Dz.U. L 95 z 15.4.2010, s. 1).

to informacje są potrzebne do podróżowania pasażerom z niepełnosprawnościami. Informacje te mogłyby obejmować informacje o oferowanych przez danego usługodawcę produktach i usługach transportu pasażerskiego, informacje udzielane przed podróżą, informacje udzielane w trakcie podróży i informacje o odwołaniu danej usługi lub o opóźnieniu rozpoczęcia podróży. Inne elementy informacji mogłyby również obejmować informacje o cenach i promocjach.

(33) Niniejsza dyrektywa powinna również obejmować strony internetowe, usługi oparte na urządzeniach mobilnych, w tym aplikacje mobilne opracowane lub udostępnione przez operatorów usług transportu pasażerskiego w ramach zakresu stosowania niniejszej dyrektywy lub z ich inicjatywy, usługi elektronicznej sprzedaży biletów, bilety elektroniczne oraz interaktywne terminale samoobsługowe.

(34) Określenie zakresu stosowania niniejszej dyrektywy w odniesieniu do usług lotniczego, autobusowego, kolejowego i wodnego transportu pasażerskiego powinno być oparte na obowiązujących sektorowych przepisach dotyczących praw pasażerów. W przypadku gdy niniejsza dyrektywa nie ma zastosowania do niektórych rodzajów usług transportowych, państwa członkowskie powinny zachęcać usługodawców do stosowania odpowiednich wymogów dostępności wynikających z niniejszej dyrektywy.

(35) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 ([7]) nakłada już na organy sektora publicznego świadczące usługi transportowe, w tym przewozy miejskie i podmiejskie oraz przewozy regionalne, obowiązek zapewnienia dostępności swoich stron internetowych. Niniejsza dyrektywa zawiera odstępstwa dla mikroprzedsiębiorstw świadczących usługi, w tym przewozy miejskie i podmiejskie oraz przewozy regionalne. Niniejsza dyrektywa wprowadza też obowiązki w zakresie zapewnienia, by strony internetowe, poprzez które prowadzony jest handel elektroniczny, były dostępne. Ponieważ niniejsza dyrektywa zawiera obowiązek dla znacznej większości prywatnych podmiotów świadczących usługi transportowe do zapewnienia dostępności swoich stron internetowych przy sprzedaży biletów w internecie, wprowadzenie w niniejszej dyrektywie dalszych wymogów co do stron internetowych podmiotów świadczących przewozy miejskie i podmiejskie oraz przewozy regionalne nie jest konieczne.

(36) Niektóre elementy wymogów dostępności, w szczególności wymogi dotyczące udzielania informacji określone w niniejszej dyrektywie, są już objęte obowiązującymi unijnymi aktami prawnymi w dziedzinie przewozów pasażerskich. Obejmuje to elementy rozporządzeń Parlamentu Europejskiego i Rady (WE) nr 261/2004 ([8]), (WE) nr 1107/2006 ([9]), (WE) nr 1371/2007 ([10]), (UE) nr 1177/2010 ([11]) oraz (UE) nr 181/2011 ([12]). Obejmuje to także odpowiednie akty prawne przyjęte na podstawie dyrektywy Parlamentu Europejskiego i Rady 2008/57/WE ([13]). Z uwagi na potrzebę zapewnienia spójności regulacyjnej wymogi dostępności określone w tych rozporządzeniach oraz te akty prawne powinny mieć zastosowanie nadal bez zmian. Niemniej jednak wynikające z niniejszej dyrektywy wymogi dodatkowe będą stanowić uzupełnienie wymogów już obowiązujących, poprawiając funkcjonowanie rynku wewnętrznego w dziedzinie transportu i przynosząc korzyści osobom z niepełnosprawnościami.

(37) Niektóre elementy usług transportowych nie powinny zostać objęte niniejszą dyrektywą, gdy są świadczone poza terytorium państw członkowskich, nawet jeżeli dana usługa została skierowana na rynek unijny. W odniesieniu do tych elementów podmiot świadczący usługi transportu pasażerskiego powinien być zobowiązany wyłącznie do zapewnienia, aby wymogi określone w niniejszej dyrektywie zostały spełnione w odniesieniu do tej części usługi, która jest oferowana na terytorium Unii. W przypadku transportu lotniczego unijni przewoźnicy lotniczy powinni jednak zapewnić, aby odpowiednie wymogi określone w niniejszej dyrektywie zostały również spełnione w odniesieniu do lotów rozpoczynających się w porcie lotniczym znajdującym się w państwie trzecim i kończących się

([7]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (Dz.U. L 327 z 2.12.2016, s. 1).

([8]) Rozporządzenie (WE) nr 261/2004 Parlamentu Europejskiego i Rady z dnia 11 lutego 2004 r. ustanawiające wspólne zasady odszkodowania i pomocy dla pasażerów w przypadku odmowy przyjęcia na pokład albo odwołania lub dużego opóźnienia lotów, uchylające rozporządzenie (EWG) nr 295/91 (Dz.U. L 46 z 17.2.2004, s. 1).

([9]) Rozporządzenie (WE) nr 1107/2006 Parlamentu Europejskiego i Rady z dnia 5 lipca 2006 r. w sprawie praw osób niepełnosprawnych oraz osób o ograniczonej sprawności ruchowej podróżujących drogą lotniczą (Dz.U. L 204 z 26.7.2006, s. 1).

([10]) Rozporządzenie (WE) nr 1371/2007 Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. dotyczące praw i obowiązków pasażerów w ruchu kolejowym (Dz.U. L 315 z 3.12.2007, s. 14).

([11]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1177/2010 z dnia 24 listopada 2010 r. o prawach pasażerów podróżujących drogą morską i drogą wodną śródlądową oraz zmieniające rozporządzenie (WE) nr 2006/2004 (Dz.U. L 334 z 17.12.2010, s. 1).

([12]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 181/2011 z dnia 16 lutego 2011 r. dotyczące praw pasażerów w transporcie autobusowym i autokarowym oraz zmieniające rozporządzenie (WE) nr 2006/2004 (Dz.U. L 55 z 28.2.2011, s. 1).

([13]) Dyrektywa Parlamentu Europejskiego i Rady 2008/57/WE z dnia 17 czerwca 2008 r. w sprawie interoperacyjności systemu kolei we Wspólnocie (Dz.U. L 191 z 18.7.2008, s. 1).

w porcie lotniczym znajdującym się na terytorium jednego z państw członkowskich. Ponadto wszyscy przewoźnicy lotniczy, w tym przewoźnicy niezarejestrowani w Unii, powinni zapewniać, aby odpowiednie wymogi określone w niniejszej dyrektywie zostały spełnione w przypadkach, w których loty rozpoczynają się na terytorium Unii i kończą na terytorium państwa trzeciego.

(38) Władze miejskie należy zachęcać, by w swoich planach zrównoważonej mobilności miejskiej uwzględniały pozbawioną barier dostępność do miejskich usług transportowych, a także by regularnie publikowały wykazy najlepszych praktyk w zakresie pozbawionej barier dostępności miejskiego transportu publicznego i miejskiej mobilności.

(39) Prawo Unii obowiązujące w zakresie usług bankowych i finansowych ma na celu ochronę i informowanie konsumentów tych usług w całej Unii, ale nie obejmuje wymogów dostępności. Aby osoby z niepełnosprawnościami miały możliwość korzystania z tych usług w całej Unii, w tym, w stosownych przypadkach, poprzez strony internetowe i usługi oparte na urządzeniach mobilnych, w tym aplikacje mobilne, aby mogły podejmować świadome decyzje i były pewne, że są odpowiednio chronione na równi z innymi konsumentami, a także aby zapewnić usługodawcom równe szanse, niniejsza dyrektywa powinna ustanowić wspólne wymogi dostępności dla niektórych usług bankowych i finansowych świadczonych konsumentom.

(40) Odpowiednie wymogi dostępności powinny również mieć zastosowanie do metod identyfikacji, podpisu elektronicznego i usług płatniczych, ponieważ są to elementy niezbędne do zawarcia transakcji w bankowości detalicznej.

(41) Pliki zawierające książki elektroniczne tworzone są przy użyciu elektronicznego kodowania komputerowego, które umożliwia rozpowszechnianie i przeglądanie utworów intelektualnych najczęściej przybierających formę tekstową i graficzną. Stopień precyzji tego kodowania rozstrzyga o dostępności plików zawierających książki elektroniczne, w szczególności w odniesieniu do kwalifikacji poszczególnych zasadniczych elementów dzieła i znormalizowanego opisu jego struktury. Interoperacyjność w kontekście dostępności powinna pomóc zoptymalizować kompatybilność tych plików z aplikacjami klienckimi i z obecnymi oraz przyszłymi technologiami wspomagającymi. Szczególne cechy specyficznych publikacji, takich jak komiksy, książki dla dzieci i książki o sztuce, powinny być analizowane pod kątem wszystkich mających zastosowanie wymogów dostępności. Rozbieżne wymogi dostępności w poszczególnych państwach członkowskich mogą utrudniać wydawcom i innym podmiotom gospodarczym korzystanie z zalet rynku wewnętrznego, mogą prowadzić do problemów w zakresie interoperacyjności czytników książek elektronicznych oraz mogą ograniczać dostęp klientów z niepełnosprawnościami do produktów i usług. W kontekście książek elektronicznych pojęcie usługodawcy może obejmować wydawców i inne podmioty gospodarcze uczestniczące w ich dystrybucji.

Uznaje się, że osoby z niepełnosprawnościami nadal napotykają przeszkody, które utrudniają dostęp do treści chronionych przez prawo autorskie i prawa pokrewne, jak i że podjęto już pewne środki w celu zaradzenia tej sytuacji – na przykład poprzez przyjęcie dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/1564 ([14]) oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/1563 ([15]) – oraz uznaje się, że w przyszłości możliwe jest podjęcie dalszych środków unijnych w tym zakresie.

(42) Niniejsza dyrektywa definiuje usługi handlu elektronicznego jako usługę na odległość za pośrednictwem stron internetowych i usług opartych na urządzeniach mobilnych, świadczoną drogą elektroniczną i na indywidualne żądanie konsumenta w celu zawarcia umowy konsumenckiej. Na potrzeby tej definicji określenie „na odległość" oznacza, że usługa świadczona jest bez równoczesnej obecności stron; „drogą elektroniczną" oznacza, że usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (z uwzględnieniem kompresji cyfrowej) oraz przechowywania danych, i jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych; „na indywidualne żądanie konsumenta" oznacza, że usługa świadczona jest na indywidualne żądanie. Zważywszy na rosnące znaczenie usług handlu elektronicznego i ich wysoki stan zaawansowania technologicznego, istotne jest zharmonizowanie wymogów ich dostępności.

([14]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1564 z dnia 13 września 2017 r. w sprawie niektórych dozwolonych sposobów korzystania z utworów i innych przedmiotów chronionych prawem autorskim i prawami pokrewnymi z korzyścią dla osób niewidomych, osób słabowidzących i osób z niepełnosprawnościami uniemożliwiającymi zapoznawanie się z drukiem oraz w sprawie zmiany dyrektywy 2001/29/WE w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. L 242 z 20.9.2017, s. 6).

([15]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1563 z dnia 13 września 2017 r. w sprawie transgranicznej wymiany między Unią a państwami trzecimi kopii w dostępnych formatach określonych utworów i innych przedmiotów chronionych prawem autorskim i prawami pokrewnymi z korzyścią dla osób niewidomych, osób słabowidzących lub osób z niepełnosprawnościami uniemożliwiającymi zapoznawanie się z drukiem (Dz.U. L 242 z 20.9.2017, s. 1).

(43) Wynikające z niniejszej dyrektywy wymogi dostępności usług handlu elektronicznego powinny mieć zastosowanie do internetowej sprzedaży wszelkich produktów lub usług i powinny w związku z tym mieć zastosowanie również do sprzedaży produktów lub usług, które same są objęte zakresem stosowania niniejszej dyrektywy.

(44) Środki dotyczące dostępności odbioru zgłoszeń alarmowych powinny być przyjmowane bez uszczerbku dla organizacji służb ratunkowych i nie powinny one wywierać wpływu na tę organizację, która pozostaje w wyłącznej kompetencji państw członkowskich.

(45) Zgodnie z dyrektywą (UE) 2018/1972 państwa członkowskie mają zapewnić, by użytkownicy końcowi z niepełnosprawnościami mieli dostęp do służb ratunkowych za pośrednictwem zgłoszeń alarmowych na równi z innymi użytkownikami końcowymi zgodnie z prawem Unii harmonizującym wymogi dostępności produktów i usług. Komisja oraz krajowe organy regulacyjne oraz inne właściwe organy mają przyjąć odpowiednie środki w celu zapewnienia, aby użytkownicy końcowi z niepełnosprawnościami, gdy podróżują do innego państwa członkowskiego, mogli mieć dostęp do służb ratunkowych na równi z pozostałymi użytkownikami końcowymi, w miarę możliwości bez wcześniejszej rejestracji. Środki te dążą do zapewnienia interoperacyjności między państwami członkowskimi i mają być w jak największym stopniu oparte na europejskich normach lub specyfikacjach określonych zgodnie z art. 39 dyrektywy (UE) 2018/1972. Takie środki nie uniemożliwiają państwom członkowskim przyjmowania dodatkowych wymogów służących osiągnięciu celów określonych w tej dyrektywie. W ramach alternatywy do spełnienia określonych w niniejszej dyrektywie wymogów dostępności w odniesieniu do skierowanych do użytkowników z niepełnosprawnościami usług odbioru zgłoszeń alarmowych państwa członkowskie powinny mieć możliwość wskazania będącego stroną trzecią podmiotu świadczącego usługi przekazu, z których to usług mogłyby korzystać osoby z niepełnosprawnościami w celu komunikowania się z publicznym punktem przyjmowania zgłoszeń, dopóki te publiczne punkty przyjmowania zgłoszeń nie będą w stanie wykorzystywać – do zapewnienia dostępności odbioru zgłoszeń alarmowych – usług łączności elektronicznej poprzez protokoły internetowe. W żadnym przypadku obowiązków wynikających z niniejszej dyrektywy nie należy rozumieć jako ograniczających ani łagodzących jakiekolwiek obowiązki na rzecz użytkowników końcowych z niepełnosprawnościami, w tym równoważne obowiązki dotyczące dostępu do usług łączności elektronicznej i do służb ratunkowych, a także obowiązki dotyczące dostępności określone w dyrektywie (UE) 2018/1972.

(46) Dyrektywa (UE) 2016/2102 określa wymogi dostępności dla stron internetowych i aplikacji mobilnych instytucji sektora publicznego oraz inne powiązane aspekty, w szczególności wymogi odnoszące się do zgodności z przepisami przedmiotowych stron internetowych i aplikacji mobilnych. Niemniej jednak dyrektywa ta zawiera szczegółowy wykaz wyjątków. Podobne wyjątki są odpowiednie w przypadku niniejszej dyrektywy. Niektóre rodzaje działalności, które odbywają się poprzez strony internetowe i aplikacje mobilne instytucji sektora publicznego, takie jak usługi transportu pasażerskiego czy usługi handlu elektronicznego, które są objęte zakresem stosowania niniejszej dyrektywy, powinny ponadto spełniać mające zastosowanie wymogi dostępności określone w niniejszej dyrektywie, tak aby zapewnić osobom z niepełnosprawnościami dostęp do internetowej sprzedaży produktów i usług, niezależnie od tego, czy sprzedawca jest publicznym czy prywatnym podmiotem gospodarczym. Wymogi dostępności określone w niniejszej dyrektywie powinny być dostosowane do wymogów dyrektywy (UE) 2016/2102 pomimo różnic dotyczących np. monitorowania, sprawozdawczości i egzekwowania przepisów.

(47) Cztery zasady dostępności stron internetowych i aplikacji mobilnych, do których odwołuje się dyrektywa (UE) 2016/2102 to: postrzegalność – która oznacza, że informacje i elementy interfejsu użytkownika muszą być przedstawiane użytkownikom w sposób, który potrafią oni odebrać; funkcjonalność – która oznacza, że elementy interfejsu użytkownika i nawigacja muszą być funkcjonalne; zrozumiałość – która oznacza, że informacje i obsługa interfejsu użytkownika muszą być zrozumiałe; oraz integralność – która oznacza, że treści muszą być wystarczająco integralne, by mogły być skutecznie interpretowane przez różnego rodzaju aplikacje klienckie, w tym technologie wspomagające. Zasady te są też istotne dla niniejszej dyrektywy.

(48) Państwa członkowskie powinny przyjąć wszelkie odpowiednie środki w celu zapewnienia, aby – w przypadku gdy produkty i usługi objęte niniejszą dyrektywą są zgodne z odpowiednimi wymogami dostępności – ich swobodny przepływ w Unii nie był utrudniony z powodów związanych z wymogami dostępności.

(49) W niektórych sytuacjach wspólne wymogi dostępności do środowiska zbudowanego ułatwiłyby swobodny przepływ powiązanych usług oraz osób z niepełnosprawnościami. Dlatego też niniejsza dyrektywa powinna dać państwom członkowskim możliwość uwzględnienia środowiska zbudowanego wykorzystywanego do świadczenia usług objętych zakresem stosowania niniejszej dyrektywy, co zapewni spełnienie wymogów dostępności określonych w załączniku III.

(50) Dostępność powinna zostać osiągnięta poprzez systematyczne usuwanie barier i zapobieganie ich powstawaniu, w miarę możliwości poprzez zastosowanie podejścia „projektowania uniwersalnego", co przyczyni się do zapewnienia osobom z niepełnosprawnościami dostępu do produktów i usług na równi z innymi. Jak wynika z Konwencji, podejście to „oznacza projektowanie produktów, środowiska, programów i usług, w taki sposób, by były użyteczne dla wszystkich, w możliwie największym stopniu, bez potrzeby adaptacji lub specjalistycznego projektowania". Zgodnie z Konwencją projektowanie uniwersalne „nie wyklucza pomocy technicznych dla szczególnych

grup osób niepełnosprawnych, jeżeli jest to potrzebne". Ponadto dostępność nie powinna wykluczać dokonywania racjonalnych usprawnień, gdy wymaga tego prawo Unii lub prawo krajowe. Dostępność i projektowanie uniwersalne należy interpretować zgodnie z Komentarzem ogólnym nr 2(2014) - art. 9: Dostępność, sporządzonym przez Komitet ds. Praw Osób z Niepełnosprawnościami.

(51) Produkty i usługi objęte zakresem stosowania niniejszej dyrektywy nie zostają automatycznie objęte zakresem stosowania dyrektywy Rady 93/42/EWG ([16]). Jednakże zakresem stosowania tej dyrektywy mogłyby być objęte niektóre technologie wspomagające będące wyrobami medycznymi.

(52) Większość miejsc pracy w UE powstaje w MŚP i w mikroprzedsiębiorstwach. Przedsiębiorstwa takie mają kluczowe znaczenie dla przyszłego wzrostu gospodarczego, jednak bardzo często napotykają na przeszkody i utrudnienia przy opracowywaniu swoich produktów lub usług, zwłaszcza w kontekście transgranicznym. Konieczne jest zatem ułatwienie działalności MŚP i mikroprzedsiębiorstw poprzez harmonizację krajowych przepisów w zakresie dostępności przy jednoczesnym zachowaniu koniecznych gwarancji.

(53) Aby mikroprzedsiębiorstwa i MŚP mogły korzystać z niniejszej dyrektywy, muszą faktycznie spełniać wymogi zalecenia Komisji 2003/361/WE ([17]) i stosownego orzecznictwa, mające na celu zapobieganie obchodzeniu tych przepisów.

(54) Aby zapewnić spójność prawa Unii niniejsza dyrektywa powinna być oparta na decyzji Parlamentu Europejskiego i Rady nr 768/2008/WE ([18]), ponieważ dotyczy produktów już objętych innymi aktami unijnymi, a jednocześnie powinna uwzględnić szczególne cechy wymogów dostępności określonych w niniejszej dyrektywie.

(55) Wszystkie podmioty gospodarcze objęte zakresem stosowania niniejszej dyrektywy i uczestniczące w łańcuchu dostaw i dystrybucji powinny zapewnić, by na rynku udostępniane były wyłącznie produkty zgodne z niniejszą dyrektywą. Ta sama zasada powinna mieć zastosowanie do podmiotów gospodarczych świadczących usługi. Konieczne jest określenie wyraźnego i proporcjonalnego podziału obowiązków stosownie do ról odgrywanych przez poszczególne podmioty gospodarcze w procesie dostaw i dystrybucji.

(56) Podmioty gospodarcze powinny być odpowiedzialne za zgodność produktów i usług, stosownie do roli odgrywanej przez nie w łańcuchu dostaw, tak aby zapewnić wysoki poziom ochrony dostępności, a także zagwarantować uczciwą konkurencję na rynku unijnym.

(57) Obowiązki określone w niniejszej dyrektywie powinny mieć zastosowanie w takim samym stopniu do podmiotów gospodarczych w sektorze publicznym i do podmiotów gospodarczych w sektorze prywatnym.

(58) Zważywszy na fakt, że producent posiada szczegółową wiedzę o procesie projektowania i produkcji, jest on najbardziej kompetentny do przeprowadzenia kompletnej oceny zgodności. Mimo że odpowiedzialność za zgodność produktów spoczywa na producencie, organy nadzoru rynku powinny odgrywać kluczową rolę w sprawdzaniu, czy produkty udostępniane w Unii są produkowane zgodnie z prawem Unii.

(59) Importerzy i dystrybutorzy powinni być zaangażowani w zadania związane z nadzorem rynku, realizowane przez organy krajowe, oraz brać aktywny udział w wykonywaniu tych zadań poprzez przedstawianie właściwym organom wszystkich koniecznych informacji dotyczących danego produktu.

(60) Importerzy powinni zapewniać, by wprowadzane na rynek Unii produkty z państw trzecich były zgodne z niniejszą dyrektywą, a w szczególności zapewniać, aby były one poddawane przez producentów odpowiednim procedurom oceny.

(61) Wprowadzając produkt do obrotu, importerzy powinni umieścić na nim swoją nazwę, zarejestrowaną nazwę handlową lub zarejestrowany znak towarowy i swoje adresy kontaktowe.

([16]) Dyrektywa Rady 93/42/EWG z dnia 14 czerwca 1993 r. dotycząca wyrobów medycznych (Dz.U. L 169 z 12.7.1993, s. 1).

([17]) Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

([18]) Decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu i uchylająca decyzję Rady 93/465/EWG (Dz.U. L 218 z 13.8.2008, s. 82).

(62) Dystrybutorzy powinni zapewnić, aby wykonywane przez nich czynności, którym poddawany jest produkt, nie miały negatywnego wpływu na jego zgodność z wymogami dostępności określonymi w niniejszej dyrektywie.

(63) Podmiot gospodarczy wprowadzający produkt do obrotu pod własną nazwą lub znakiem towarowym lub modyfikujący produkt już znajdujący się w obrocie w sposób, który może wpłynąć na zgodność produktu z mającymi zastosowanie wymogami, powinien być uznany za producenta i przejąć jego obowiązki z tego tytułu.

(64) Ze względu na zasadę proporcjonalności wymogi dostępności powinny mieć zastosowanie jedynie w zakresie, w jakim nie stanowią nieproporcjonalnego obciążenia dla danego podmiotu gospodarczego lub w zakresie, w którym nie wymagają znaczących zmian w produktach i usługach w związku z niniejszą dyrektywą. Niemniej jednak należy ustanowić mechanizmy kontroli w celu weryfikowania, czy dany podmiot jest uprawniony do odstępstwa od stosowania wymogów dostępności.

(65) Niniejsza dyrektywa powinna opierać się na zasadzie „najpierw myśl na małą skalę" i uwzględniać obciążenia administracyjne, z którymi borykają się MŚP. Zamiast ustanawiać ogólne wyjątki i odstępstwa dla podmiotów gospodarczych powinna ona zawierać proste zasady w zakresie oceny zgodności i klauzule ochronne dla tych przedsiębiorstw. W związku z tym przy ustanawianiu zasad doboru i wdrażania najodpowiedniejszych procedur oceny zgodności należy uwzględnić sytuację MŚP, a obowiązki przeprowadzania oceny zgodności z wymogami dostępności należy ograniczyć w takim zakresie, by nie stanowiły one nieproporcjonalnego obciążenia dla MŚP. Ponadto organy nadzoru rynku powinny działać w sposób proporcjonalny do rozmiaru przedsiębiorstw oraz do produkcji w małych seriach lub produkcji nieseryjnej, bez tworzenia zbędnych utrudnień dla MŚP i bez szkody dla ochrony interesu publicznego.

(66) W wyjątkowych przypadkach, gdy zgodność z wymogami dostępności określonymi w niniejszej dyrektywie wiązałaby się z nieproporcjonalnym obciążeniem dla podmiotów gospodarczych, należy wymagać od tych podmiotów, by przestrzegały ich jedynie w zakresie, w jakim wymogi te nie stanowią nieproporcjonalnego obciążenia. W takich odpowiednio uzasadnionych przypadkach podmiot gospodarczy nie miałby racjonalnej możliwości pełnego stosowania jednego lub większej liczby wymogów dostępności określonych w niniejszej dyrektywie. Podmiot gospodarczy powinien jednak zapewnić, by dana usługa lub dany produkt, objęte zakresem stosowania niniejszej dyrektywy, były jak najbardziej dostępne, stosując te wymogi w takim zakresie, w jakim nie stanowią one nieproporcjonalnego obciążenia. Te wymogi dostępności, które nie zostały przez podmiot gospodarczy uznane za stanowiące nieproporcjonalne obciążenie, powinny być stosowane w pełni. Wyjątki od obowiązku przestrzegania jednego lub więcej wymogów dostępności wynikające z nieproporcjonalnego obciążenia związanego ze stosowaniem tych wymogów nie powinny wykraczać poza to, co jest ściśle konieczne do ograniczenia tego obciążenia w odniesieniu do danego produktu lub danej usługi w konkretnym przypadku. Środki, które stanowiłyby nieproporcjonalne obciążenie, należy rozumieć jako środki, które – zgodnie z kryteriami określonymi w niniejszej dyrektywie – nakładałyby na podmiot gospodarczy dodatkowe nadmierne obciążenie organizacyjne lub finansowe, przy uwzględnieniu prawdopodobnych związanych z nimi korzyści dla osób z niepełnosprawnościami. Należy ustalić oparte na tych rozważaniach kryteria, aby zarówno podmiotom gospodarczym, jak i właściwym organom umożliwić systematyczne porównywanie poszczególnych sytuacji i ocenę, czy występuje nieproporcjonalne obciążenie. Dokonując oceny zakresu, w jakim wymogi dostępności nie mogą zostać spełnione ze względu na wiążące się z nimi nieproporcjonalne obciążenie, należy uwzględniać wyłącznie uzasadnione przyczyny. Za uzasadnione przyczyny nie należy uznawać braku priorytetowego traktowania, braku czasu ani braku wiedzy.

(67) Ogólnej oceny nieproporcjonalnego obciążenia należy dokonywać stosując kryteria określone w załączniku VI. Ocena nieproporcjonalnego obciążenia powinna zostać przez podmiot gospodarczy udokumentowana z uwzględnieniem odpowiednich kryteriów. Usługodawcy powinni ponownie przeprowadzać ocenę nieproporcjonalnego obciążenia nie rzadziej niż co pięć lat.

(68) Dany podmiot gospodarczy powinien poinformować odpowiednie organy, że zastosował przepisy niniejszej dyrektywy dotyczące zasadniczej zmiany lub nieproporcjonalnego obciążenia. Wyłącznie na wniosek właściwych organów podmioty gospodarcze powinny przedstawić kopię oceny wyjaśniającej, dlaczego ich produkt lub usługa nie są w pełni dostępne, i wykazującą istnienie nieproporcjonalnego obciążenia lub zasadniczej zmiany, lub obu tych powodów.

(69) Jeśli na podstawie wymaganej oceny usługodawca stwierdzi, że obowiązek zapewnienia, by wszystkie terminale samoobsługowe wykorzystywane do celów świadczenia usług objętych niniejszą dyrektywą spełniały wymogi dostępności określone w niniejszej dyrektywie, stanowiłby nieproporcjonalne obciążenie, usługodawca powinien w dalszym ciągu stosować te wymogi w zakresie, w jakim nie powodują one dla niego takiego nieproporcjonalnego obciążenia. Usługodawcy powinni zatem ocenić, w jakim zakresie ograniczony stopień dostępności wszystkich terminali samoobsługowych lub ograniczona liczba terminali samoobsługowych w pełni spełniających kryteria dostępności umożliwiają im uniknięcie nieproporcjonalnego obciążenia, które w innym przypadku byłoby na nich nałożone, i powinni być zobowiązani do spełniania określonych w niniejszej dyrektywie wymogów dostępności tylko w tym zakresie.

(70) Mikroprzedsiębiorstwa wyróżniają się spośród wszystkich innych przedsiębiorstw swoimi ograniczonymi zasobami ludzkimi, niewielkim rocznym obrotem lub niewielkim bilansem rocznym. W przypadku mikroprzedsiębiorstw obciążenie związane ze spełnieniem wymogów dostępności pochłania zatem, ogólnie rzecz biorąc, większą część zasobów finansowych i ludzkich niż w przypadku innych przedsiębiorstw i istnieje większe prawdopodobieństwo, że będzie to stanowić nieproporcjonalną część ich kosztów. Znaczny udział kosztów ponoszonych przez mikroprzedsiębiorstwa wiąże się z uzupełnianiem lub prowadzeniem dokumentacji i rejestrów potwierdzających, że przestrzegają one poszczególnych wymogów określonych w prawie Unii. Wszystkie podmioty gospodarcze objęte zakresem stosowania niniejszej dyrektywy powinny móc oceniać proporcjonalność obciążenia, jakim jest dla nich spełnienie wymogów dostępności określonych w niniejszej dyrektywie, i powinny spełniać te wymogi wyłącznie w zakresie, w jakim obciążenie to nie jest nieproporcjonalne, jednak wymaganie takiej oceny od mikroprzedsiębiorstw świadczących usługi samo w sobie stanowi nieproporcjonalne obciążenie. Wymogi i obowiązki określone w niniejszej dyrektywie nie powinny zatem mieć zastosowania do mikroprzedsiębiorstw świadczących usługi objęte zakresem stosowania niniejszej dyrektywy.

(71) W odniesieniu do mikroprzedsiębiorstw mających do czynienia z produktami objętymi zakresem stosowania niniejszej dyrektywy wymogi i obowiązki określone w niniejszej dyrektywie powinny być złagodzone, tak by ograniczyć obciążenie administracyjne.

(72) Mimo że niektóre mikroprzedsiębiorstwa są zwolnione z obowiązków przewidzianych w niniejszej dyrektywie, wszystkie mikroprzedsiębiorstwa powinny być zachęcane do produkowania, przywozu lub dystrybucji produktów oraz świadczenia usług, które spełniają wymogi dostępności określone w niniejszej dyrektywie, tak by zwiększyć ich konkurencyjność oraz ich potencjał wzrostu na rynku wewnętrznym. Dlatego też państwa członkowskie powinny zapewnić mikroprzedsiębiorstwom wytyczne i narzędzia, aby ułatwić stosowanie krajowych środków transponujących niniejszą dyrektywę.

(73) Wszystkie podmioty gospodarcze powinny przy udostępnianiu na rynku lub wprowadzaniu produktów do obrotu lub świadczeniu usług na rynku postępować odpowiedzialnie i w pełnej zgodności z mającymi zastosowanie wymogami prawnymi.

(74) W celu ułatwienia oceny zgodności z mającymi zastosowanie wymogami dostępności należy przewidzieć domniemanie zgodności produktów i usług zgodnych z dobrowolnymi normami zharmonizowanymi przyjmowanymi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012 ([19]), w celu sporządzenia szczegółowych specyfikacji technicznych związanych z tymi wymogami. Komisja opublikowała już szereg skierowanych do europejskich organizacji normalizacyjnych wniosków o normalizację w dziedzinie dostępności, takich jak zlecenia normalizacji M/376, M/473 i M/420, które byłyby istotne dla przygotowania norm zharmonizowanych.

(75) Rozporządzenie (UE) nr 1025/2012 ustanawia procedurę formalnych zastrzeżeń do norm zharmonizowanych uznanych za niespełniające wymogów określonych w niniejszej dyrektywie.

(76) Europejskie normy powinny być oparte na zasadach rynkowych, uwzględniać interes publiczny, a także cele polityki jasno określone we wnioskach o opracowanie norm zharmonizowanych kierowanych przez Komisję do jednej lub kilku europejskich organizacji normalizacyjnych, a także powinny opierać się na konsensusie. W przypadku braku norm zharmonizowanych lub gdy jest to konieczne do celów harmonizacji rynku wewnętrznego Komisja powinna mieć możliwość przyjmowania w niektórych przypadkach aktów wykonawczych ustanawiających specyfikacje techniczne dotyczące określonych w niniejszej dyrektywie wymogów dostępności. Do specyfikacji technicznych należy odwoływać się wyłącznie w takich przypadkach. Komisja powinna mieć możliwość przyjmowania specyfikacji technicznych, na przykład jeżeli proces normalizacji jest zablokowany z powodu braku konsensusu pomiędzy interesariuszami lub występują nieuzasadnione opóźnienia w ustanawianiu normy zharmonizowanej, przykładowo z powodu nieosiągnięcia wymaganej jakości. Komisja powinna przewidzieć wystarczająco dużo czasu między przyjęciem skierowanego do jednej lub kilku europejskich organizacji normalizacyjnych wniosku o opracowanie norm zharmonizowanych a przyjęciem specyfikacji technicznej związanej z tym samym wymogiem dostępności. Komisja nie powinna mieć możliwości przyjęcia specyfikacji technicznej, jeżeli uprzednio nie podjęła próby objęcia wymogów dostępności europejskim systemem normalizacji, chyba że może wykazać, iż specyfikacje techniczne spełniają wymagania określone w załączniku II do rozporządzenia (UE) nr 1025/2012.

(77) W celu ustanowienia norm zharmonizowanych i specyfikacji technicznych, które najskuteczniej spełniają określone w niniejszej dyrektywie wymogi dostępności produktów i usług, Komisja powinna w miarę możliwości angażować w ten proces europejskie organizacje patronackie reprezentujące osoby z niepełnosprawnościami oraz wszystkich pozostałych interesariuszy.

([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).

(78) Aby zapewnić skuteczny dostęp do informacji do celów nadzoru rynku, informacje niezbędne do zadeklarowania zgodności ze wszystkimi mającymi zastosowanie aktami prawnymi Unii powinny zostać udostępnione w pojedynczej deklaracji zgodności UE. W celu zmniejszenia obciążenia administracyjnego podmiotów gospodarczych, podmioty te powinny mieć możliwość uwzględnienia wszystkich odpowiednich poszczególnych deklaracji zgodności w jednej unijnej deklaracji zgodności.

(79) Aby umożliwić ocenę zgodności produktów, w niniejszej dyrektywie powinna być przewidziana wewnętrzna kontrola produkcji (moduł A), określona w załączniku II do decyzji nr 768/2008/WE, ponieważ daje ona podmiotom gospodarczym możliwość wykazania że, a właściwym organom zapewnienia, aby produkty udostępniane na rynku spełniały wymogi dostępności, nie nakładając jednocześnie nieuzasadnionego obciążenia.

(80) Prowadząc nadzór rynku produktów i sprawdzając zgodność usług, organy powinny również kontrolować, czy oceny zgodności, w tym, w stosownych przypadkach, ocena dotycząca zasadniczej zmiany lub nieproporcjonalnego obciążenia zostały przeprowadzone prawidłowo. Wykonując swoje zadania, organy te powinny również współpracować z osobami z niepełnosprawnościami i organizacjami, które reprezentują takie osoby i ich interesy.

(81) W przypadku usług informacje niezbędne do oceny zgodności z wymogami dostępności określonymi w niniejszej dyrektywie powinny zostać zawarte w ogólnych warunkach lub w równoważnym dokumencie, bez uszczerbku dla dyrektywy Parlamentu Europejskiego i Rady 2011/83/UE ([20]).

(82) Oznakowanie CE, wskazujące na zgodność produktu z określonymi w niniejszej dyrektywie wymogami dostępności, jest widoczną konsekwencją całego procesu obejmującego ocenę zgodności w szerokim znaczeniu. Niniejsza dyrektywa powinna być zgodna z ogólnymi zasadami regulującymi oznakowanie CE, określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 765/2008 ([21]) ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu. Oprócz sporządzenia deklaracji zgodności UE producent powinien w sposób racjonalny pod względem kosztów informować konsumentów o spełnianiu wymogów dostępności przez swoje produkty.

(83) Zgodnie z rozporządzeniem (WE) nr 765/2008 przez umieszczenie na produkcie oznakowania CE producent deklaruje zgodność danego produktu z wszystkimi mającymi zastosowanie wymogami dostępności, biorąc tym samym na siebie pełną odpowiedzialność za tę zgodność.

(84) Zgodnie z decyzją nr 768/2008/WE państwa członkowskie są odpowiedzialne za zapewnienie dla produktów na swoim terytorium zdecydowanego i skutecznego nadzoru rynku i powinny przyznać organom nadzoru rynku wystarczające uprawnienia i środki.

(85) Państwa członkowskie powinny sprawdzać zgodność usług z obowiązkami określonymi w niniejszej dyrektywie i rozpatrywać skargi oraz zapoznawać się ze sprawozdaniami opisującymi przypadki niezgodności w celu zapewnienia działań naprawczych.

(86) W stosownych przypadkach Komisja mogłaby przyjąć w porozumieniu z interesariuszami niewiążące wytyczne, aby wspierać koordynację między organami nadzoru rynku a organami odpowiedzialnymi za sprawdzanie zgodności usług. Komisja i państwa członkowskie powinny móc ustanowić inicjatywy w celu dzielenia zasobów i wiedzy fachowej organów.

(87) Państwa członkowskie powinny zapewnić, aby organy nadzoru rynku i organy odpowiedzialne za sprawdzanie zgodności usług kontrolowały spełnianie przez podmioty gospodarcze kryteriów określonych w załączniku VI, zgodnie z rozdziałami VIII i IX. Do wypełniania przewidzianych w niniejszej dyrektywie obowiązków organów nadzoru rynku lub organów odpowiedzialnych za kontrolę zgodności usług państwa członkowskie powinny móc wyznaczyć wyspecjalizowany organ. Państwa członkowskie powinny móc zdecydować, że kompetencje takiego wyspecjalizowanego organu powinny ograniczać się do zakresu stosowania niniejszej dyrektywy lub niektórych jej części, bez uszczerbku dla zobowiązań państw członkowskich wynikających z rozporządzenia (WE) nr 765/2008.

([20]) Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady (Dz.U. L 304 z 22.11.2011, s. 64).

([21]) 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).

(88) Należy ustanowić procedurę ochronną, która powinna mieć zastosowanie w przypadku braku między państwami członkowskimi zgody co do środków wprowadzanych przez jedno z nich, w ramach której to procedury zainteresowane strony będą informowane o środkach, które mają zostać wprowadzone w odniesieniu do dostępności produktów niespełniających wymogów dostępności określonych w niniejszej dyrektywie. Procedura ochronna powinna umożliwiać organom nadzoru rynku podejmowanie w odniesieniu do takich produktów – we współpracy z odpowiednimi podmiotami gospodarczymi – działań na wcześniejszym etapie.

(89) W przypadku gdy państwa członkowskie i Komisja osiągną porozumienie co do zasadności określonego środka wprowadzonego przez dane państwo członkowskie, dalsze zaangażowanie Komisji nie powinno być wymagane z wyjątkiem przypadków, w których niezgodność można przypisać niedociągnięciom w normach zharmonizowanych lub specyfikacjach technicznych.

(90) Dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE ([22]) i 2014/25/UE ([23]) w sprawie zamówień publicznych, określające procedury udzielania zamówień publicznych i konkursów odnośnie do niektórych dostaw (produktów), usług i robót budowlanych, stanowią, że w przypadku wszystkich zamówień, które przeznaczone są do użytku osób fizycznych – zarówno ogółu społeczeństwa, jak i pracowników instytucji zamawiającej lub podmiotu zamawiającego – przedmiotowe specyfikacje techniczne sporządza się, z wyjątkiem przypadków należycie uzasadnionych, w taki sposób, aby uwzględnić kryteria dostępności dla osób niepełnosprawnych lub projektowanie dla wszystkich użytkowników. Co więcej, dyrektywy te wymagają, by w przypadku gdy obowiązkowe wymogi w zakresie dostępności są przyjmowane w formie aktu prawnego Unii, specyfikacje techniczne określano – jeżeli chodzi o kryteria dostępności dla osób z niepełnosprawnościami lub projektowanie dla wszystkich – przez odesłanie do tego aktu. Niniejsza dyrektywa powinna ustanowić obowiązkowe wymogi dostępności produktów i usług, które są nią objęte. Wymogi dostępności określone w niniejszej dyrektywie nie są wiążące w odniesieniu do produktów i usług nieobjętych jej zakresem stosowania. Niemniej jednak stosowanie tych wymogów dostępności w celu wywiązania się z odpowiednich obowiązków określonych w aktach Unii innych niż niniejsza dyrektywa ułatwiłoby tworzenie warunków dostępności i przyczyniłoby się do pewności prawa oraz do zbliżenia wymogów dostępności w obrębie Unii. Organom nie należy uniemożliwiać ustanawiania wymogów dostępności wykraczających poza wymogi dostępności określone w załączniku I do niniejszej dyrektywy.

(91) Niniejsza dyrektywa nie powinna zmieniać obowiązkowego lub dobrowolnego charakteru przepisów dotyczących dostępności przewidzianych innymi aktami Unii.

(92) Niniejsza dyrektywa powinna mieć zastosowanie wyłącznie do procedur zamówień, w przypadku których zaproszenie zostało wysłane lub – gdy nie przewiduje się zaproszeń – w przypadku których instytucja zamawiająca lub podmiot zamawiający rozpoczęli procedurę udzielania zamówienia po dacie rozpoczęcia stosowania niniejszej dyrektywy.

(93) Aby zapewnić odpowiednie stosowanie niniejszej dyrektywy, należy przekazać Komisji uprawnienia do przyjmowania zgodnie z art. 290 TFUE aktów w celu: sprecyzowania wymogów dostępności, które ze względu na swój charakter nie mogą przynieść zamierzonego skutku, o ile nie zostaną sprecyzowane w wiążących aktach prawnych Unii; zmiany okresu, w którym podmiot gospodarczy musi mieć możliwość zidentyfikowania innego podmiotu gospodarczego, który dostarczył mu produkt lub któremu on dostarczył produkt; oraz dalszego sprecyzowania odpowiednich kryteriów, które powinny być brane pod uwagę przez podmiot gospodarczy do oceny, czy spełnienie wymogów dostępności stanowiłoby nieproporcjonalne obciążenie. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa ([24]). W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(94) W celu zapewnienia jednolitych warunków wykonywania niniejszej dyrektywy należy powierzyć Komisji uprawnienia wykonawcze w odniesieniu do ustanowienia specyfikacji technicznych. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([25]).

([22]) 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).

([23]) Dyrektywa Parlamentu Europejskiego i Rady 2014/25/UE z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylająca dyrektywę 2004/17/WE (Dz.U. L 94 z 28.3.2014, s. 243).

([24]) Dz.U. L 123 z 12.5.2016, s. 1.

([25]) 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).

(95) Państwa członkowskie powinny zapewnić istnienie właściwych i skutecznych środków służących zapewnieniu zgodności z niniejszą dyrektywą i w związku z tym powinny ustanowić odpowiednie mechanizmy kontroli, takie jak kontrola a posteriori przez organy nadzoru rynku, w celu sprawdzenia, czy zwolnienie ze stosowania wymogów dostępności jest uzasadnione. Podczas rozpatrywania skarg dotyczących dostępności państwa członkowskie powinny przestrzegać ogólnej zasady dobrej administracji, a w szczególności obowiązku zapewnienia przez urzędników, by decyzja w każdej sprawie zapadała w rozsądnym terminie.

(96) W celu ułatwienia jednolitego wykonania niniejszej dyrektywy Komisja powinna ustanowić grupę roboczą składającą się z odpowiednich organów i interesariuszy, tak by usprawnić wymianę informacji i najlepszych praktyk oraz zapewnić doradztwo. Należy rozwijać współpracę między organami i odpowiednimi interesariuszami, w tym z osobami z niepełnosprawnościami i organizacjami reprezentującymi takie osoby, między innymi w celu zwiększenia spójności w stosowaniu niniejszej dyrektywy w odniesieniu do wymogów dostępności oraz monitorowania wdrażania jej przepisów dotyczących zasadniczych zmian i nieproporcjonalnego obciążenia.

(97) Biorąc pod uwagę obowiązujące ramy prawne dotyczące środków odwoławczych w obszarach objętych zakresem stosowania dyrektyw 2014/24/UE i 2014/25/UE, przepisy niniejszej dyrektywy dotyczące egzekwowania przepisów i dotyczące sankcji nie powinny mieć zastosowania do procedur udzielania zamówień podlegających obowiązkom przewidzianym w niniejszej dyrektywie. Wyłączenie takie pozostaje bez uszczerbku dla wynikających z Traktatów obowiązków podejmowania przez państwa członkowskie wszelkich środków niezbędnych do zagwarantowania stosowania i skuteczności prawa Unii.

(98) Sankcje powinny być odpowiednie do charakteru naruszeń, jak i do okoliczności, tak by nie stały się alternatywą dla spełnienia przez podmioty gospodarcze obowiązku zapewnienia dostępności ich produktów lub usług.

(99) Państwa członkowskie powinny zapewnić, by zgodnie z obowiązującymi przepisami prawa Unii istniała możliwość skorzystania z alternatywnych mechanizmów rozstrzygania sporów w celu rozstrzygnięcia każdego domniemanego przypadku niezgodności z niniejszą dyrektywą, zanim wszczęte zostanie postępowanie przed sądem lub właściwym organem administracyjnym.

(100) Zgodnie ze wspólną deklaracją polityczną państw członkowskich i Komisji z dnia 28 września 2011 r. dotyczącą dokumentów wyjaśniających ([26]) państwa członkowskie zobowiązały się do zapewnienia, w uzasadnionych przypadkach, by powiadomieniu o środkach transpozycji towarzyszył co najmniej jeden dokument wyjaśniający związki między elementami dyrektywy a odpowiadającymi im częściami krajowych instrumentów transpozycyjnych. W odniesieniu do niniejszej dyrektywy prawodawca uznaje, że przekazanie takich dokumentów jest uzasadnione.

(101) W celu zapewnienia usługodawcom wystarczającego czasu na dostosowanie się do wymogów określonych w niniejszej dyrektywie niezbędne jest wprowadzenie okresu przejściowego wynoszącego pięć lat od daty rozpoczęcia stosowania niniejszej dyrektywy, w którym to okresie produkty wykorzystywane do świadczenia usług wprowadzone do obrotu przed tą datą nie będą musiały spełniać wymogów dostępności określonych w niniejszej dyrektywie, chyba że zostaną one zastąpione przez usługodawców w okresie przejściowym. Biorąc pod uwagę koszt i długi cykl życia terminali samoobsługowych, należy przewidzieć możliwość, by – o ile są one wykorzystywane do świadczenia usług – można je było wykorzystywać do końca okresu ich użyteczności, o ile nie zostaną one w tym okresie zastąpione, ale nie dłużej niż przez 20 lat.

(102) Wymogi dostępności określone w niniejszej dyrektywie powinny mieć zastosowanie do produktów wprowadzanych do obrotu i usług świadczonych po dacie rozpoczęcia stosowania krajowych środków transponujących niniejszą dyrektywę, w tym także do produktów używanych i z drugiej ręki importowanych z państwa trzeciego i wprowadzanych do obrotu po tej dacie.

(103) Niniejsza dyrektywa nie narusza praw podstawowych i jest zgodna z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej (zwanej dalej „Kartą"). W szczególności niniejsza dyrektywa ma na celu zapewnienie pełnego przestrzegania prawa osób z niepełnosprawnościami do korzystania ze środków mających zapewnić im niezależność, integrację społeczną i zawodową oraz udział w życiu społeczności; ma ona również na celu zachęcenie do stosowania art. 21, 25 i 26 Karty.

(104) Z racji tego, że cel niniejszej dyrektywy, jakim jest wyeliminowanie barier dla swobodnego przepływu niektórych dostępnych produktów i usług w celu przyczynienia się do właściwego funkcjonowania rynku wewnętrznego, nie może zostać osiągnięty w wystarczający sposób przez państwa członkowskie, ponieważ wymaga harmonizacji różnych przepisów istniejących obecnie w ich systemach prawnych, ale przez określenie wspólnych wymogów dostępności i zasad funkcjonowania rynku wewnętrznego cel ten można lepiej osiągnąć na poziomie unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,

([26]) Dz.U. C 369 z 17.12.2011, s. 14.

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

Postanowienia ogólne

Artykuł 1

Przedmiot

Celem niniejszej dyrektywy jest przyczynienie się do właściwego funkcjonowania rynku wewnętrznego w drodze zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich w odniesieniu do wymogów dostępności niektórych produktów i usług, w szczególności poprzez wyeliminowanie i zapobieganie powstawaniu barier, które utrudniają swobodny przepływ produktów i usług objętych zakresem stosowania niniejszej dyrektywy i wynikają z rozbieżnych wymogów dostępności w poszczególnych państwach członkowskich.

Artykuł 2

Zakres stosowania

1. Niniejsza dyrektywa ma zastosowanie do następujących produktów wprowadzanych do obrotu po dniu 28 czerwca 2025 r.:

a) systemy sprzętu komputerowego ogólnego przeznaczenia i systemy operacyjne do nich;

b) następujące terminale samoobsługowe:

(i) terminale płatnicze;

(ii) następujące terminale samoobsługowe przeznaczone do świadczenia usług objętych zakresem stosowania niniejszej dyrektywy:

— bankomaty,

— automaty biletowe,

— urządzenia do odprawy samoobsługowej,

— interaktywne terminale samoobsługowe udzielające informacji, z wyjątkiem terminali instalowanych jako zintegrowane części pojazdów, statków powietrznych, statków wodnych lub taboru kolejowego;

c) konsumenckie urządzenia końcowe z interaktywnymi zdolnościami obliczeniowymi wykorzystywane na potrzeby usług łączności elektronicznej;

d) konsumenckie urządzenia końcowe mające interaktywne zdolności obliczeniowe, służące do korzystania z audiowizualnych usług medialnych; oraz

e) czytniki książek elektronicznych.

2. Bez uszczerbku dla art. 32 niniejsza dyrektywa ma zastosowanie do następujących usług świadczonych na rzecz konsumentów po dniu 28 czerwca 2025 r.:

a) usługi łączności elektronicznej, z wyjątkiem usług transmisji wykorzystywanych do świadczenia usług łączności maszyna–maszyna;

b) usługi umożliwiające dostęp do audiowizualnych usług medialnych;

c) następujące elementy usług lotniczego, autobusowego, kolejowego i wodnego transportu pasażerskiego, z wyjątkiem przewozów miejskich i podmiejskich i przewozów regionalnych, do których zastosowanie mają wyłącznie elementy ujęte w ppkt (v):

(i) strony internetowe;

(ii) usługi oparte na urządzeniach mobilnych, w tym aplikacje mobilne;

(iii) bilety elektroniczne i usługi elektronicznych systemów sprzedaży biletów;

(iv) dostarczanie informacji o usługach transportu, w tym informacji o podróży w czasie rzeczywistym; w odniesieniu do ekranów informacyjnych ograniczone jest ono do interaktywnych ekranów znajdujących się na terytorium Unii; oraz

(v) interaktywne terminale samoobsługowe znajdujące się na terytorium Unii, z wyjątkiem tych instalowanych jako zintegrowane części pojazdów, statków powietrznych, statków wodnych i taboru, wykorzystywane do świadczenia wszelkich części takich usług transportu pasażerskiego;

d) usługi bankowości detalicznej;

e) książki elektroniczne i ich specjalistyczne oprogramowanie; oraz

f) usługi handlu elektronicznego.

3. Niniejsza dyrektywa ma zastosowanie do odbioru zgłoszeń alarmowych, które są kierowane pod jednolity europejski numer alarmowy 112.

4. Niniejsza dyrektywa nie ma zastosowania do następujących treści w odniesieniu do stron internetowych i aplikacji mobilnych:

a) zarejestrowane z wyprzedzeniem media zmienne w czasie opublikowane przed dniem 28 czerwca 2025 r.;

b) formaty plików dokumentów biurowych opublikowane przed dniem 28 czerwca 2025 r.;

c) mapy internetowe i internetowe usługi mapowania, jeżeli w przypadku map przeznaczonych do zastosowań nawigacyjnych podstawowe informacje są dostarczane w sposób dostępny w formie cyfrowej;

d) pochodzące od stron trzecich treści, które nie są finansowane ani tworzone przez dany podmiot gospodarczy ani nie znajdują się pod jego kontrolą;

e) treści stron internetowych i aplikacji mobilnych uznawanych za zarchiwizowane, co oznacza, że zawierają one wyłącznie treści, które nie były aktualizowane ani edytowane po dniu 28 czerwca 2025 r.

5. Niniejsza dyrektywa pozostaje bez uszczerbku dla dyrektywy (UE) 2017/1564 i rozporządzenia (UE) 2017/1563.

Artykuł 3

Definicje

Na użytek niniejszej dyrektywy stosuje się następujące definicje:

1) „osoby z niepełnosprawnościami” oznaczają osoby, które mają długotrwale naruszoną sprawność fizyczną, psychiczną, intelektualną lub w zakresie zmysłów, co może, w oddziaływaniu z różnymi barierami, utrudniać im pełny i skuteczny udział w życiu społecznym na równi z innymi;

2) „produkt” oznacza substancję, preparat lub wyrób wytworzony w procesie produkcji, niebędący produktem żywnościowym, paszą, żywą rośliną ani zwierzęciem, produktem pochodzenia ludzkiego ani produktem uzyskanym z roślin lub zwierząt związanym bezpośrednio z ich przyszłą reprodukcją;

3) „usługa” oznacza usługę w rozumieniu art. 4 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2006/123/WE ([27]);

4) „usługodawca” oznacza osobę fizyczną lub prawną, która świadczy usługę na rynku unijnym lub oferuje świadczenie takiej usługi konsumentom w Unii;

5) „audiowizualne usługi medialne” oznaczają usługi zdefiniowane w art. 1 ust. 1 lit. a) dyrektywy 2010/13/UE;

6) „usługi umożliwiające dostęp do audiowizualnych usług medialnych” oznaczają usługi przekazywane przez sieć łączności elektronicznej, wykorzystywane do identyfikacji audiowizualnych usług medialnych, do wyboru takich usług i odbierania informacji o nich oraz do wyświetlania ich oraz jakiekolwiek inne przewidziane cechy – takie jak napisy dla osób niesłyszących i niedosłyszących, audiodeskrypcja, napisy czytane i tłumaczenie na język migowy – wynikające z wdrożenia środków mających zapewnić, by takie usługi stały się dostępne, o czym mowa w art. 7 dyrektywy 2010/13/UE; niniejsza definicja obejmuje też elektroniczne przewodniki po programach;

7) „konsumenckie urządzenie końcowe mające interaktywne zdolności obliczeniowe, służące do korzystania z audiowizualnych usług medialnych” oznacza urządzenie, którego głównym przeznaczeniem jest zapewnianie dostępu do audiowizualnych usług medialnych;

([27]) Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym (Dz.U. L 376 z 27.12.2006, s. 36).

8) „usługa łączności elektronicznej” oznacza usługę łączności elektronicznej zdefiniowaną w art. 2 pkt 4 dyrektywy (UE) 2018/1972;

9) „usługa pełnej konwersacji wideo i tekstowej” oznacza usługę pełnej konwersacji wideo i tekstowej zdefiniowaną w art. 2 pkt 35 dyrektywy (UE) 2018/1972;

10) „publiczny punkt przyjmowania zgłoszeń” lub „PSAP” oznacza publiczny punkt przyjmowania zgłoszeń o wypadkach lub PSAP zdefiniowany w art. 2 pkt 36 dyrektywy (UE) 2018/1972;

11) „najwłaściwszy publiczny punkt przyjmowania zgłoszeń” oznacza najwłaściwszy publiczny punkt przyjmowania zgłoszeń o wypadkach zdefiniowany w art. 2 pkt 37 dyrektywy (UE) 2018/1972;

12) „zgłoszenie alarmowe” oznacza zgłoszenie alarmowe zdefiniowane w art. 2 pkt 38 dyrektywy (UE) 2018/1972;

13) „służba ratunkowa” oznacza służbę ratunkową zdefiniowaną w art. 2 pkt 39 dyrektywy (UE) 2018/1972;

14) „komunikacja tekstowa w czasie rzeczywistym” oznacza rodzaj konwersacji tekstowej w sytuacjach punkt–punkt lub w konferencjach wielopunktowych, gdy wprowadzany tekst jest przesyłany w taki sposób, że komunikacja jest postrzegana przez użytkowników jako ciągła w trybie znak po znaku;

15) „udostępnianie na rynku” oznacza dostarczenie produktu do celów dystrybucji, konsumpcji lub używania na rynku Unii w ramach działalności o charakterze komercyjnym, odpłatnie lub nieodpłatnie;

16) „wprowadzenie do obrotu” oznacza pierwsze udostępnienie produktu na rynku Unii;

17) „producent” oznacza osobę fizyczną lub prawną, która wytwarza produkt lub która zleca zaprojektowanie lub wytworzenie produktu i prowadzi obrót tym produktem pod własną nazwą lub znakiem towarowym;

18) „upoważniony przedstawiciel” oznacza osobę fizyczną lub prawną mającą siedzibę w Unii, posiadającą pisemne pełnomocnictwo od producenta do działania w jego imieniu w odniesieniu do określonych zadań;

19) „importer” oznacza osobę fizyczną lub prawną mającą siedzibę w Unii, która wprowadza do obrotu w Unii produkt pochodzący z państwa trzeciego;

20) „dystrybutor” oznacza osobę fizyczną lub prawną w łańcuchu dostaw, niebędącą producentem ani importerem, która udostępnia produkt na rynku;

21) „podmiot gospodarczy” oznacza producenta, upoważnionego przedstawiciela, importera, dystrybutora lub usługodawcę;

22) „konsument” oznacza osobę fizyczną, która kupuje dany produkt lub korzysta z danych usług w celach niezwiązanych z jej działalnością handlową, gospodarczą, rzemieślniczą lub z wykonywaniem wolnego zawodu;

23) „mikroprzedsiębiorstwo” oznacza przedsiębiorstwo zatrudniające mniej niż 10 osób z rocznym obrotem nieprzekraczającym 2 mln EUR lub bilansem rocznym nieprzekraczającym 2 mln EUR;

24) „małe i średnie przedsiębiorstwa” lub „MŚP” oznaczają przedsiębiorstwa, które zatrudniają mniej niż 250 pracowników i których roczny obrót nie przekracza 50 mln EUR lub których bilans roczny nie przekracza 43 mln EUR, z wyłączeniem mikroprzedsiębiorstw;

25) „norma zharmonizowana” oznacza normę zharmonizowaną zdefiniowaną w art. 2 ust. 1 lit. c) rozporządzenia (UE) nr 1025/2012;

26) „specyfikacja techniczna” oznacza specyfikację techniczną zdefiniowaną w art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012, która zawiera środki umożliwiające spełnienie wymogów dostępności dla danego produktu lub usługi;

27) „wycofanie z obrotu” oznacza dowolny środek, którego celem jest zapobieżenie udostępnianiu na rynku produktu znajdującego się w łańcuchu dostaw;

28) „usługi bankowości detalicznej" oznaczają świadczenie na rzecz konsumentów następujących usług bankowych i finansowych:

a) umów o kredyt objętych dyrektywą Parlamentu Europejskiego i Rady 2008/48/WE ([28]) lub dyrektywą Parlamentu Europejskiego i Rady 2014/17/UE ([29]);

b) usług zdefiniowanych w sekcji A pkt 1, 2, 4 i 5 oraz w sekcji B pkt 1, 2, 4 i 5 załącznika I do dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE ([30]);

c) usług płatniczych zdefiniowanych w art. 4 pkt 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 ([31]);

d) usług powiązanych z rachunkiem płatniczym zdefiniowanych w art. 2 pkt 6 dyrektywy Parlamentu Europejskiego i Rady 2014/92/UE ([32]); oraz

e) usług w zakresie pieniądza elektronicznego zdefiniowanego w art. 2 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE ([33]);

29) „terminal płatniczy" oznacza urządzenie, którego głównym przeznaczeniem jest umożliwianie dokonywania płatności z użyciem instrumentów płatniczych zdefiniowanych w art. 4 pkt 14 dyrektywy (UE) 2015/2366 w fizycznym punkcie sprzedaży, ale nie w środowisku wirtualnym;

30) „usługi handlu elektronicznego" oznaczają usługi świadczone na odległość poprzez strony internetowe i usługi oparte na urządzeniach mobilnych, drogą elektroniczną i na indywidualne żądanie konsumenta w celu zawarcia umowy konsumenckiej;

31) „usługi lotniczego transportu pasażerskiego" oznaczają handlowe przewozy pasażerskie zdefiniowane w art. 2 lit. l) rozporządzenia (WE) nr 1107/2006, rozpoczynające się, kończące się lub z przesiadką w porcie lotniczym znajdującym się na terytorium państwa członkowskiego, w tym loty rozpoczynające się w porcie lotniczym znajdującym się w państwie trzecim i kończące się w porcie lotniczym znajdującym się na terytorium państwa członkowskiego, w przypadku gdy usługi takie są świadczone przez unijnych przewoźników lotniczych;

32) „usługi autobusowego transportu pasażerskiego" oznaczają usługi objęte art. 2 ust. 1 i 2 rozporządzenia (UE) nr 181/2011;

33) „usługi kolejowego transportu pasażerskiego" oznaczają wszystkie kolejowe usługi pasażerskie, o których mowa w art. 2 ust. 1 rozporządzenia (WE) nr 1371/2007, z wyłączeniem usług, o których mowa w jego art. 2 ust. 2;

34) „usługi wodnego transportu pasażerskiego" oznaczają usługi przewozu pasażerskiego objęte art. 2 ust. 1 rozporządzenia (UE) nr 1177/2010 z wyjątkiem usług, o których mowa w art. 2 ust. 2 tego rozporządzenia;

35) „przewozy miejskie i podmiejskie" oznaczają przewozy miejskie i podmiejskie zdefiniowane w art. 3 pkt 6 dyrektywy Parlamentu Europejskiego 2012/34/UE ([34]); jednak na potrzeby niniejszej dyrektywy pojęcie to obejmuje wyłącznie następujące środki transportu: kolej, autobusy i autokary, metro, tramwaje i trolejbusy;

([28]) Dyrektywa Parlamentu Europejskiego i Rady 2008/48/WE z dnia 23 kwietnia 2008 r. w sprawie umów o kredyt konsumencki oraz uchylająca dyrektywę Rady 87/102/EWG (Dz.U. L 133 z 22.5.2008, s. 66).

([29]) Dyrektywa Parlamentu Europejskiego i Rady 2014/17/UE z dnia 4 lutego 2014 r. w sprawie konsumenckich umów o kredyt związanych z nieruchomościami mieszkalnymi i zmieniająca dyrektywy 2008/48/WE i 2013/36/UE oraz rozporządzenie (UE) nr 1093/2010 (Dz.U. L 60 z 28.2.2014, s. 34).

([30]) Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.U. L 173 z 12.6.2014, s. 349).

([31]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. L 337 z 23.12.2015, s. 35).

([32]) Dyrektywa Parlamentu Europejskiego i Rady 2014/92/UE z dnia 23 lipca 2014 r. w sprawie porównywalności opłat związanych z rachunkami płatniczymi, przenoszenia rachunku płatniczego oraz dostępu do podstawowego rachunku płatniczego (Dz.U. L 257 z 28.8.2014, s. 214).

([33]) Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE (Dz.U. L 267 z 10.10.2009, s. 7).

([34]) Dyrektywa Parlamentu Europejskiego i Rady 2012/34/UE z dnia 21 listopada 2012 r. w sprawie utworzenia jednolitego europejskiego obszaru kolejowego (Dz.U. L 343 z 14.12.2012, s. 32).

36) „przewozy regionalne" oznaczają przewozy regionalne zdefiniowane w art. 3 pkt 7 dyrektywy 2012/34/UE; jednak na potrzeby niniejszej dyrektywy pojęcie to obejmuje wyłącznie następujące środki transportu: kolej, autobusy i autokary, metro, tramwaje i trolejbusy;

37) „technologia wspomagająca" oznacza dowolny element, część wyposażenia lub system usług lub produktów, w tym oprogramowanie, wykorzystywane w celu zwiększenia, utrzymania, zastąpienia lub poprawy możliwości funkcjonalnych osób z niepełnosprawnościami lub w celu łagodzenia i kompensowania upośledzeń, ograniczeń aktywności lub ograniczeń możliwości uczestnictwa;

38) „system operacyjny" oznacza oprogramowanie, które, między innymi, obsługuje interfejs sprzętu peryferyjnego, planuje zadania, przydziela pamięć i stanowi domyślny interfejs dla użytkownika, gdy żaden program aplikacyjny, w tym graficzny interfejs użytkownika, nie jest aktywny, niezależnie od tego, czy takie oprogramowanie jest integralną częścią sprzętu komputerowego ogólnego przeznaczenia, czy jest samodzielnym oprogramowaniem przeznaczonym do stosowania w sprzęcie komputerowym ogólnego przeznaczenia, z wyłączeniem modułu ładującego system operacyjny, podstawowego systemu wejścia-wyjścia oraz innego oprogramowania układowego niezbędnego przy uruchamianiu lub instalowaniu systemu operacyjnego;

39) „system sprzętu komputerowego ogólnego przeznaczenia" oznacza stanowiące kompletny komputer połączenie sprzętu komputerowego, które cechuje wielofunkcyjny charakter oraz zdolność do wykonywania, z odpowiednim oprogramowaniem, najczęstszych zadań informatycznych, z których korzystają konsumenci, oraz które jest przeznaczone do obsługi przez konsumentów; obejmuje to komputery osobiste, w szczególności komputery stacjonarne, laptopy, smartfony i tablety;

40) „interaktywne zdolności obliczeniowe" oznaczają funkcję obsługi interakcji między człowiekiem a urządzeniem umożliwiającą przetwarzanie i transmisję danych, głosu lub wideo, lub ich kombinacji;

41) „książka elektroniczna i jej oprogramowanie" oznacza usługę polegającą na dostarczaniu plików cyfrowych stanowiących elektroniczną wersję książki, do których to plików można uzyskać dostęp, po których można nawigować, które można czytać i wykorzystywać, oraz oprogramowanie obejmujące usługi oparte na urządzeniach mobilnych, w tym aplikacje mobilne, przeznaczone do uzyskiwania dostępu do tych plików cyfrowych, nawigowania po nich, czytania i korzystania z nich, z wyłączeniem oprogramowania objętego definicją zawartą w pkt 42;

42) „czytnik książek elektronicznych" oznacza specjalne urządzenie, obejmujące zarówno sprzęt, jak i oprogramowanie, wykorzystywane do uzyskiwania dostępu do plików książek elektronicznych, nawigowania po nich, czytania ich i korzystania z nich;

43) „bilety elektroniczne" oznaczają system, w którym uprawnienie do podróżowania, w postaci biletu uprawniającego do pojedynczego lub wielokrotnego podróżowania, abonamentu na podróżowanie lub kredytu na podróżowanie jest przechowywane elektronicznie na fizycznej karcie transportowej lub na innym urządzeniu, zamiast w postaci wydrukowanych biletów papierowych;

44) „usługi elektronicznych systemów sprzedaży biletów" oznaczają system, w którym bilety w transporcie pasażerskim są kupowane, w tym przez internet, za pomocą urządzenia mającego interaktywne zdolności obliczeniowe, i dostarczane do nabywcy w formie elektronicznej, tak aby umożliwić mu wydrukowanie w formie papierowej lub okazane – w czasie podróży – przy użyciu urządzeń mobilnych z interaktywnymi zdolnościami obliczeniowymi.

ROZDZIAŁ II

Wymogi dostępności a swoboda przemieszczania się

Artykuł 4

Wymogi dostępności

1. Państwa członkowskie zapewniają, zgodnie z ust. 2, 3 i 5 niniejszego artykułu i z zastrzeżeniem art. 14, aby podmioty gospodarcze wprowadzały do obrotu wyłącznie produkty i świadczyły wyłącznie usługi, które spełniają wymogi dostępności określone w załączniku I.

2. Wszystkie produkty muszą spełniać wymogi dostępności określone w sekcji I załącznika I.

Wszystkie produkty, z wyjątkiem terminali samoobsługowych, muszą spełniać wymogi dostępności określone w sekcji II załącznika I.

3. Bez uszczerbku dla ust. 5 niniejszego artykułu, wszystkie usługi, z wyjątkiem przewozów miejskich i podmiejskich oraz przewozów regionalnych, muszą spełniać wymogi dostępności określone w sekcji III załącznika I.

Bez uszczerbku dla ust. 5 niniejszego artykułu, wszystkie usługi muszą spełniać wymogi dostępności określone w sekcji IV załącznika I.

4. Uwzględniając warunki krajowe, państwa członkowskie mogą zdecydować, że środowisko zbudowane wykorzystywane przez klientów korzystających z usług objętych niniejszą dyrektywą musi spełniać wymogi dostępności określone w załączniku III, tak by zmaksymalizować korzystanie z nich przez osoby z niepełnosprawnościami.

5. Mikroprzedsiębiorstwa świadczące usługi są zwolnione z obowiązku spełnienia wymogów dostępności, o których mowa w ust. 3 niniejszego artykułu, i wszelkich obowiązków odnoszących się do zgodności z tymi wymogami.

6. Państwa członkowskie zapewniają mikroprzedsiębiorstwom wytyczne i narzędzia, aby ułatwić stosowanie krajowych środków transponujących niniejszą dyrektywę. Państwa członkowskie opracowują te narzędzia w porozumieniu z odpowiednimi interesariuszami.

7. Państwa członkowskie mogą poinformować podmioty gospodarcze o zawartych w załączniku II orientacyjnych przykładach możliwych rozwiązaniach przyczyniających się do spełnienia wymogów dostępności określonych w załączniku I.

8. Państwa członkowskie zapewniają, by odbieranie zgłoszeń alarmowych kierowanych pod jednolity europejski numer alarmowy 112 przez najwłaściwszy publiczny punkt przyjmowania zgłoszeń spełniał szczegółowe wymogi dostępności określone w sekcji V załącznika I w sposób najlepiej odpowiadający krajowej organizacji systemów alarmowych.

9. Komisja jest uprawniona do przyjmowania zgodnie z art. 26 aktów delegowanych w celu uzupełnienia załącznika I, poprzez sprecyzowanie wymogów dostępności, które ze względu na swój charakter nie mogą przynieść zamierzonego skutku, o ile nie zostaną sprecyzowane w wiążących aktach prawnych Unii, np. wymogów związanych z interoperacyjnością.

Artykuł 5

Obowiązujące prawo Unii w dziedzinie transportu pasażerskiego

Usługi spełniające wymogi dotyczące zapewnienia dostępnych informacji oraz informowania o dostępności określone w rozporządzeniach (WE) nr 261/2004, (WE) nr 1107/2006, (WE) nr 1371/2007, (UE) nr 1177/2010 oraz (UE) nr 181/2011 oraz w odpowiednich aktach przyjętych na podstawie dyrektywy 2008/57/WE uznaje się za spełniające odnośne wymogi określone w niniejszej dyrektywie. W przypadku gdy niniejsza dyrektywa przewiduje wymogi dodatkowe względem tych przewidzianych we wspomnianych rozporządzeniach oraz aktach, te dodatkowe wymogi mają w pełni zastosowanie.

Artykuł 6

Swobodny przepływ

Państwa członkowskie nie utrudniają na swoim terytorium – z powodów związanych z wymogami dostępności – udostępniania na rynku produktów ani świadczenia na swoim terytorium usług, które spełniają wymogi niniejszej dyrektywy.

ROZDZIAŁ III

Obowiązki podmiotów gospodarczych mających do czynienia z produktami

Artykuł 7

Obowiązki producentów

1. Wprowadzając swoje produkty do obrotu, producenci zapewniają, aby zostały one zaprojektowane i wyprodukowane zgodnie z odpowiednimi wymogami dostępności określonymi w niniejszej dyrektywie.

2. Producenci sporządzają dokumentację techniczną zgodnie z załącznikiem IV oraz przeprowadzają procedurę oceny zgodności, o której mowa w tym załączniku, lub zlecają jej przeprowadzenie.

W przypadku wykazania – w wyniku przeprowadzenia tej procedury – zgodności takiego produktu z mającymi zastosowanie wymogami dostępności producenci sporządzają deklarację zgodności UE i umieszczają oznakowanie CE.

3. Producenci przechowują dokumentację techniczną oraz deklarację zgodności UE przez pięć lat po wprowadzeniu produktu do obrotu.

4. Producenci zapewniają, by istniały procedury pozwalające na utrzymanie zgodności produkcji seryjnej z niniejszą dyrektywą. Odpowiednio uwzględniane muszą być zmiany w projekcie lub właściwościach produktu oraz zmiany w normach zharmonizowanych lub w specyfikacjach technicznych, na podstawie których zadeklarowano zgodność produktu.

5. Producenci zapewniają, aby ich produkty były opatrzone nazwą typu, numerem partii lub serii lub inną informacją umożliwiającą ich identyfikację, lub w przypadku gdy wielkość lub charakter produktu to uniemożliwiają, aby wymagane informacje były umieszczone na opakowaniu lub w dokumencie dołączonym do produktu.

6. Producenci opatrują produkt swoim nazwiskiem lub swoją nazwą, zarejestrowaną nazwą towarową lub zarejestrowanym znakiem towarowym i umieszczają swój adres kontaktowy na produkcie, a jeżeli nie jest to możliwe – na opakowaniu lub w dokumencie dołączonym do produktu. Adres musi wskazywać pojedynczy punkt, w którym można skontaktować się z producentem. Dane kontaktowe są podawane w języku łatwo zrozumiałym dla użytkowników końcowych i organów nadzoru rynku.

7. Producenci zapewniają dołączenie do produktu instrukcji obsługi oraz dostarczenie informacji na temat bezpieczeństwa w języku łatwo zrozumiałym dla konsumentów i innych użytkowników końcowych, wskazanym przez zainteresowane państwo członkowskie. Takie instrukcje i informacje, jak również wszelkie etykiety, muszą być jasne, zrozumiałe i czytelne.

8. Producenci, którzy uznają lub mają powody, by uważać, że wprowadzony przez nich do obrotu wyrób jest niezgodny z niniejszą dyrektywą, niezwłocznie podejmują środki naprawcze niezbędne do zapewnienia zgodności wyrobu lub – w stosownych przypadkach – wycofania go z obrotu. Ponadto, w przypadku gdy dany produkt nie spełnia wymogów dostępności określonych w niniejszej dyrektywie, producenci niezwłocznie informują o tym właściwe organy krajowe państw członkowskich, w których produkt został udostępniony, podając szczegółowe informacje, zwłaszcza na temat niezgodności oraz wszelkich przyjętych środków naprawczych. W takich przypadkach producenci prowadzą ewidencję produktów niezgodnych z mającymi zastosowanie wymogami dostępności i związanych z tym skarg.

9. Na uzasadnione żądanie właściwego organu krajowego producenci przekazują mu wszelkie informacje i dokumentację, które są konieczne do wykazania zgodności danego produktu, w języku łatwo zrozumiałym dla tego organu. Na żądanie tego organu współpracują z nim w działaniach podejmowanych w celu wyeliminowania niezgodności wprowadzonych przez nich do obrotu produktów z mającymi zastosowanie wymogami dostępności, w szczególności poprzez doprowadzenie do zgodności produktów z mającymi zastosowanie wymogami dostępności.

Artykuł 8

Upoważnieni przedstawiciele

1. Na podstawie pisemnego pełnomocnictwa producent może wyznaczyć upoważnionego przedstawiciela.

Zakres pełnomocnictwa udzielonego upoważnionemu przedstawicielowi nie może obejmować realizacji obowiązków określonych w art. 7 ust. 1 ani sporządzania dokumentacji technicznej.

2. Upoważniony przedstawiciel wykonuje zadania określone w pełnomocnictwie udzielonym przez producenta. Pełnomocnictwo musi pozwalać upoważnionemu przedstawicielowi co najmniej na:

a) przechowywanie deklaracji zgodności UE oraz dokumentacji technicznej do dyspozycji organów nadzoru rynku przez pięć lat;

b) przekazywanie właściwemu krajowemu organowi, na jego uzasadnione żądanie, wszelkich informacji i dokumentacji koniecznej do wykazania zgodności produktu;

c) współpracę z właściwym krajowym organem, na jego żądanie, w działaniach podejmowanych w celu wyeliminowania niezgodności objętych pełnomocnictwem produktów z mającymi zastosowanie wymogami dostępności.

Artykuł 9

Obowiązki importerów

1. Importerzy wprowadzają do obrotu wyłącznie produkty zgodne z wymogami.

2. Przed wprowadzeniem produktu do obrotu importerzy zapewniają, aby producent przeprowadził procedurę oceny zgodności określoną w załączniku IV. Importerzy zapewniają sporządzenie przez producenta dokumentacji technicznej, zgodnie z zawartymi w tym załączniku wymogami, opatrzenie produktu oznakowaniem CE, dołączenie wymaganych dokumentów oraz spełnienie przez producenta wymogów określonych w art. 7 ust. 5 i 6.

3. W przypadku gdy importer uznaje lub ma powody, by uważać, że produkt nie spełnia mających zastosowanie wymogów dostępności określonych w niniejszej dyrektywie, nie wprowadza tego produktu do obrotu, dopóki nie zostanie zapewniona zgodność. Ponadto w przypadku gdy produkt nie spełnia mających zastosowanie wymogów dostępności, importer informuje o tym producenta oraz organy nadzoru rynku.

4. Importerzy są obowiązani opatrzyć produkt swoim nazwiskiem lub swoją nazwą, zarejestrowaną nazwą towarową lub zarejestrowanym znakiem towarowym i umieścić swój adres kontaktowy na produkcie, a jeżeli nie jest to możliwe – na opakowaniu lub w dokumencie dołączonym do produktu. Dane kontaktowe podaje się w języku łatwo zrozumiałym dla użytkowników końcowych i organów nadzoru rynku.

5. Importerzy zapewniają, by do produktu została dołączona była instrukcja obsługi oraz informacje na temat bezpieczeństwa w języku łatwo zrozumiałym dla konsumentów i innych użytkowników końcowych, wskazanym przez zainteresowane państwo członkowskie.

6. Importerzy zapewniają, aby w czasie, gdy to oni ponoszą odpowiedzialność za produkt, warunki jego przechowywania ani przewożenia nie wpływały negatywnie na jego zgodność z mającymi zastosowanie wymogami dostępności.

7. Importerzy przechowują kopię deklaracji zgodności UE do dyspozycji organów nadzoru rynku przez pięć lat i zapewniają, by dokumentacja techniczna mogła być udostępniana tym organom na ich żądanie.

8. Importerzy, którzy uznają lub mają powody, by uważać, że wprowadzony przez nich do obrotu produkt jest niezgodny z niniejszą dyrektywą, niezwłocznie podejmują środki naprawcze niezbędne do zapewnienia zgodności produktu lub – w stosownych przypadkach – wycofania go z obrotu. Ponadto, w przypadku gdy dany produkt nie spełnia mających zastosowanie wymogów dostępności, importerzy niezwłocznie informują o tym właściwe organy krajowe państw członkowskich, w których produkt został udostępniony, podając informacje, w szczególności na temat niezgodności oraz wszelkich przyjętych środków naprawczych. W takich przypadkach importerzy są zobowiązani do prowadzenia ewidencji produktów niezgodnych z mającymi zastosowanie wymogami dostępności i związanych z tym skarg.

9. Na uzasadnione żądanie właściwego organu krajowego importerzy przekazują mu wszelkie informacje i dokumentację konieczne do wykazania zgodności produktu, w języku łatwo zrozumiałym dla tego organu. Na żądanie tego organu podejmują z nim współpracę w działaniach podejmowanych w celu wyeliminowania niezgodności wprowadzonych przez nich do obrotu produktów z mającymi zastosowanie wymogami dostępności.

Artykuł 10

Obowiązki dystrybutorów

1. Przy udostępnianiu produktu na rynku dystrybutorzy działają z należytą starannością w odniesieniu do wymogów niniejszej dyrektywy.

2. Przed udostępnieniem produktu na rynku dystrybutorzy sprawdzają, czy produkt jest opatrzony oznakowaniem CE i czy dołączone do niego są wymagane dokumenty oraz instrukcje i informacje na temat bezpieczeństwa w języku łatwo zrozumiałym dla konsumentów i innych użytkowników końcowych w państwie członkowskim, w którym produkt ma zostać udostępniony na rynku, a także czy producent i importer spełnili wymogi określone odpowiednio w art. 7 ust. 5 i 6 oraz art. 9 ust. 4.

3. W przypadku gdy dystrybutor uznaje lub ma powody, by uważać, że produkt nie jest zgodny z odpowiednimi wymogami dostępności określonymi w niniejszej dyrektywie, nie udostępnia tego produktu na rynku, dopóki nie zostanie zapewniona zgodność. Ponadto jeżeli produkt nie spełnia mających zastosowanie wymogów dostępności, dystrybutor informuje o tym producenta lub importera oraz organy nadzoru rynku.

4. Dystrybutorzy zapewniają, aby w czasie, gdy to oni są odpowiedzialni za produkt, warunki jego przechowywania ani przewożenia nie wpływały negatywnie na jego zgodność z mającymi zastosowanie wymogami dostępności.

5. Dystrybutorzy, którzy uznają lub mają powody, by uważać, że udostępniany przez nich na rynku produkt nie jest zgodny z niniejszą dyrektywą, zapewniają w stosownych przypadkach zastosowanie środków naprawczych koniecznych do zapewnienia zgodności tego produktu, lub – w stosownych przypadkach – wycofania go z obrotu. Ponadto, w przypadku gdy dany produkt nie spełnia mających zastosowanie wymogów dostępności, dystrybutorzy niezwłocznie informują o tym właściwe organy krajowe państw członkowskich, w których produkt został udostępniony, podając informacje, w szczególności na temat niezgodności oraz zastosowanych środków naprawczych.

6. Na uzasadnione żądanie właściwego organu krajowego dystrybutorzy przekazują mu wszelkie informacje i dokumentację konieczne do wykazania zgodności produktu. Na żądanie tego organu podejmują z nim współpracę w działaniach podejmowanych w celu wyeliminowania niezgodności udostępnionych przez nich na rynku produktów z mającymi zastosowanie wymogami dostępności.

Artykuł 11

Przypadki, w których obowiązki producentów mają zastosowanie do importerów i dystrybutorów

Na użytek niniejszej dyrektywy importera lub dystrybutora uznaje się za producenta i nakłada na niego obowiązki producenta określone w art. 7, w przypadku gdy wprowadza on dany produkt do obrotu pod swoim nazwiskiem, swoją nazwą lub znakiem towarowym lub modyfikuje produkt już wprowadzony do obrotu w taki sposób, że może to mieć wpływ na jego zgodność z wymogami niniejszej dyrektywy.

Artykuł 12

Identyfikacja podmiotów gospodarczych mających do czynienia z produktami

1. Na żądanie organów nadzoru rynku podmioty gospodarcze, o których mowa w art. 7–10, wskazują:

a) każdy inny podmiot gospodarczy, który dostarczył im produkt;

b) każdy inny podmiot gospodarczy, któremu dostarczyły produkt.

2. Podmioty gospodarcze, o których mowa w art. 7–10, muszą być w stanie podać informacje, o których mowa w ust. 1 niniejszego artykułu, przez pięć lat od momentu dostarczenia im produktu i przez pięć lat od momentu dostarczenia przez nie produktu.

3. Komisja jest uprawniona do przyjmowania zgodnie z art. 26 aktów delegowanych dotyczących zmiany niniejszej dyrektywy poprzez zmianę długości okresu, o którym mowa w ust. 2 niniejszego artykułu, w odniesieniu do niektórych produktów. Ten zmieniony okres musi być dłuższy niż 5 lat i być proporcjonalny do okresu ekonomicznej użyteczności danego produktu.

ROZDZIAŁ IV

Obowiązki usługodawców

Artykuł 13

Obowiązki usługodawców

1. Usługodawcy zapewniają, aby ich usługi były projektowane i świadczone zgodnie z wymogami dostępności określonymi w niniejszej dyrektywie.

2. Usługodawcy przygotowują niezbędne informacje zgodnie z załącznikiem V i wyjaśniają, w jaki sposób usługi spełniają mające zastosowanie wymogi dostępności. Informacje podawane są do wiadomości publicznej w formie pisemnej i ustnej, w tym w sposób dostępny dla osób z niepełnosprawnościami. Usługodawcy przechowują te informacje przez cały okres świadczenia danej usługi.

3. Bez uszczerbku dla art. 32 usługodawcy zapewniają, by istniały procedury służące zachowaniu zgodności świadczenia usług z mającymi zastosowanie wymogami dostępności. Usługodawcy należycie uwzględniają zmiany dotyczące okoliczności świadczenia usługi, zmiany mających zastosowanie wymogów dostępności oraz zmiany w normach zharmonizowanych lub specyfikacjach technicznych, na podstawie których deklaruje się zgodność usługi z wymogami dostępności.

4. W przypadku niezgodności usługodawcy przyjmują środki naprawcze niezbędne do doprowadzenia do zgodności danej usługi z mającymi zastosowanie wymogami dostępności. Ponadto, w przypadku gdy dana usługa nie spełnia mających zastosowanie wymogów dostępności, usługodawcy niezwłocznie informują o tym właściwe organy krajowe państw członkowskich, w których usługa ta jest świadczona, podając szczegółowe informacje, zwłaszcza na temat niezgodności oraz zastosowanych środków naprawczych.

5. Na uzasadnione żądanie właściwego organu usługodawcy udzielają mu wszelkich informacji koniecznych do wykazania zgodności danej usługi z mającymi zastosowanie wymogami dostępności. Na żądanie tego organu współpracują oni z nim w zakresie działań podejmowanych w celu zapewnienia zgodności z tymi wymogami.

ROZDZIAŁ V

Zasadnicza zmiana produktów lub usług oraz nieproporcjonalne obciążenie podmiotów gospodarczych

Artykuł 14

Zasadnicza zmiana i nieproporcjonalne obciążenie

1. Wymogi dostępności, o których mowa w art. 4, mają zastosowanie wyłącznie w zakresie, w jakim zapewnienie zgodności:

a) nie wymaga dokonania znaczących zmian produktu lub usługi, które stanowiłyby zasadniczą zmianę podstawowych właściwości danego produktu lub danej usługi; oraz

b) nie stanowi dla odnośnych podmiotów gospodarczych nieproporcjonalnego obciążenia.

2. Podmioty gospodarcze przeprowadzają ocenę w celu stwierdzenia, czy spełnienie wymogów dostępności, o których mowa w art. 4, łączyłoby się z koniecznością wprowadzenia zasadniczej zmiany lub czy stanowiłoby ono – w oparciu o kryteria określone w załączniku VI – nieproporcjonalne obciążenie, o czym mowa w ust. 1 niniejszego artykułu.

3. Podmioty gospodarcze dokumentują ocenę, o której mowa w ust. 2. Podmioty gospodarcze przechowują wszystkie odpowiednie wyniki oceny przez pięć lat od, odpowiednio, ostatniego udostępnienia na rynku produktu lub od zakończenia świadczenia usługi. Na żądanie, stosowanie do przypadku, organów nadzoru rynku lub organów odpowiedzialnych za kontrolę zgodności usług podmioty gospodarcze udostępniają im kopię oceny, o której mowa w ust. 2.

4. W drodze odstępstwa od ust. 3 mikroprzedsiębiorstwa mające do czynienia z produktami są zwolnione z wymogu dokumentowania swojej oceny. Niemniej jednak na żądanie organu nadzoru rynku mikroprzedsiębiorstwa mające do czynienia z produktami, które zdecydowały się skorzystać z ust. 1, przedstawiają temu organowi fakty mające znaczenie dla dokonania oceny, o której mowa w ust. 2.

5. Usługodawcy korzystający z ust. 1 lit. b) ponownie przeprowadzają ocenę ewentualnego nieproporcjonalnego obciążenia w odniesieniu do każdej kategorii lub każdego rodzaju usług:

a) gdy świadczona usługa ulega zmianie; lub

b) na żądanie organu odpowiedzialnego za kontrolę zgodności usług; oraz

c) w każdym przypadku, nie rzadziej niż co 5 lat.

6. Podmioty gospodarcze nie mogą korzystać z ust. 1 lit. b), w przypadku gdy w celu poprawy dostępności otrzymują finansowanie z innych źródeł niż zasoby własne podmiotu gospodarczego, zarówno publicznych, jak i prywatnych.

7. Komisja jest uprawniona do przyjmowania zgodnie z art. 26 aktów delegowanych w celu uzupełnienia załącznika VI poprzez sprecyzowanie odpowiednich kryteriów, które podmiot gospodarczy musi uwzględnić przy ocenie, o której mowa w ust. 2 niniejszego artykułu. Precyzując te kryteria, Komisja bierze pod uwagę potencjalne korzyści nie tylko dla osób z niepełnosprawnościami, ale także dla osób z ograniczeniami funkcjonalnymi.

W razie potrzeby Komisja przyjmie pierwszy taki akt delegowany do dnia 28 czerwca 2020 r. Akt taki zacznie obowiązywać najwcześniej w dniu 28 czerwca 2025 r.

8. W przypadku gdy w odniesieniu do danego produktu lub danej usługi podmioty gospodarcze korzystają z ust. 1, informują o tym właściwe organy nadzoru rynku lub odpowiedzialne za kontrolę zgodności usług organy państwa członkowskiego, w którym dany produkt jest wprowadzany do obrotu lub w którym dana usługa jest świadczona.

Akapit pierwszy nie ma zastosowania do mikroprzedsiębiorstw.

ROZDZIAŁ VI

Normy zharmonizowane oraz specyfikacje techniczne produktów i usług

Artykuł 15

Domniemanie zgodności

1. W przypadku produktów i usług spełniających normy zharmonizowane lub ich części, do których to norm odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, domniemywa się, że dane produkty i usługi spełniają wymogi dostępności określone w niniejszej dyrektywie, w zakresie, w jakim wymogi te są objęte takimi normami lub ich częściami.

2. Komisja, zgodnie z art. 10 rozporządzenia (UE) nr 1025/2012, zwraca się do jednej lub kilku europejskich organizacji normalizacyjnych z wnioskiem o opracowanie norm zharmonizowanych dla wymogów dostępności produktów określonych w załączniku I. Pierwszy taki wniosek Komisja przedstawi zainteresowanemu komitetowi do dnia 28 czerwca 2021 r.

3. Komisja może przyjąć akty wykonawcze ustanawiające specyfikacje techniczne, które spełniają wymogi dostępności określone w niniejszej dyrektywie, w przypadku gdy zostały spełnione następujące warunki:

a) w *Dzienniku Urzędowym Unii Europejskiej* nie opublikowano odniesienia do norm zharmonizowanych zgodnie z rozporządzeniem (UE) nr 1025/2012; oraz

b) albo:

(i) Komisja zwróciła się do co najmniej jednej z europejskich organizacji normalizacyjnych z wnioskiem o opracowanie normy zharmonizowanej, a w procedurze normalizacyjnej wystąpiły nieuzasadnione opóźnienia lub wniosek nie został przyjęty przez żadną z europejskich organizacji normalizacyjnych; albo

(ii) Komisja może wykazać, że specyfikacja techniczna spełnia wymagania określone w załączniku II do rozporządzenia (UE) nr 1025/2012, z wyjątkiem wymagania, by specyfikacje techniczne zostały opracowane przez organizację o charakterze niekomercyjnym.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 27 ust. 2.

4. Produkty i usługi, które są zgodne ze specyfikacjami technicznymi lub ich częściami, uznaje się za spełniające wymogi dostępności określone w niniejszej dyrektywie, w zakresie, w jakim te specyfikacje techniczne lub ich części obejmują te wymogi.

ROZDZIAŁ VII

Zgodność produktów i oznakowanie CE

Artykuł 16

Unijna deklaracja zgodności produktów

1. W deklaracji zgodności UE stwierdza się, że wykazano spełnienie mających zastosowanie wymogów dostępności. Jeżeli w drodze wyjątku zastosowano art. 14, deklaracja zgodności UE zawiera informację, które wymogi dostępności są objęte tym wyjątkiem.

2. Deklaracja zgodności UE musi być zgodna z szablonem określonym w załączniku III do decyzji nr 768/2008/WE. Zawiera ona elementy określone w załączniku IV do niniejszej dyrektywy oraz jest systematycznie aktualizowana. W wymogach dotyczących dokumentacji technicznej unika się nakładania nieuzasadnionych obciążeń na mikroprzedsiębiorstwa oraz MŚP. Deklaracja zgodności jest tłumaczona na język lub języki wymagane przez państwo członkowskie, w którym wprowadza się do obrotu lub udostępnia dany produkt na rynku.

3. W przypadku gdy dany produkt podlega więcej niż jednemu aktowi prawa Unii wymagającemu deklaracji zgodności UE, sporządzana jest jedna deklaracja zgodności UE odnosząca się do wszystkich takich aktów prawa Unii. Deklaracja wskazuje odpowiednie akty prawne, łącznie z ich odniesieniami publikacyjnymi.

4. Poprzez sporządzenie deklaracji zgodności UE producent bierze na siebie odpowiedzialność za zgodność produktu z wymogami określonymi w niniejszej dyrektywie.

Artykuł 17

Ogólne zasady dotyczące oznakowania CE dla produktów

Oznakowanie CE podlega ogólnym zasadom określonym w art. 30 rozporządzenia (WE) nr 765/2008.

Artykuł 18

Przepisy i warunki dotyczące umieszczania oznakowania CE

1. Oznakowanie CE umieszcza się w sposób widoczny, czytelny i trwały na produkcie lub jego tabliczce znamionowej. W przypadku gdy jest to niemożliwe lub nieuzasadnione ze względu na charakter produktu, oznakowanie CE umieszcza się na opakowaniu i w dołączonych dokumentach.

2. Oznakowanie CE umieszcza się przed wprowadzeniem produktu do obrotu.

3. Państwa członkowskie korzystają z istniejących mechanizmów w celu zapewnienia prawidłowego stosowania systemu regulującego oznakowanie CE oraz podejmują odpowiednie działania w przypadku nieprawidłowego stosowania tego oznakowania.

ROZDZIAŁ VIII

Nadzór rynku produktów oraz unijna procedura ochronna

Artykuł 19

Nadzór rynku produktów

1. Do produktów zastosowanie mają art. 15 ust. 3 i art. 16–19, art. 21, art. 23–28 i art. 29 ust. 2 i 3 rozporządzenia (WE) nr 765/2008.

2. Prowadząc nadzór rynku produktów, odpowiednie organy nadzoru rynku – w przypadkach gdy podmiot gospodarczy skorzystał z art. 14 niniejszej dyrektywy:

a) sprawdzają, czy podmiot gospodarczy przeprowadził ocenę, o której mowa w art. 14;

b) dokonują analizy tej oceny i jej wyników, w tym prawidłowego stosowania kryteriów określonych w załączniku VI; oraz

c) sprawdzają, czy spełnione są mające zastosowanie wymogi dostępności.

3. Państwa członkowskie zapewniają, aby informacje posiadane przez organy nadzoru rynku dotyczące spełniania przez podmioty gospodarcze mających zastosowanie wymogów dostępności określonych w niniejszej dyrektywie oraz ocena przewidziana w art. 14 dostępne były dla konsumentów na żądanie oraz w formacie dostępnym, chyba że informacje te nie mogą być udostępniane ze względu na ich poufny charakter, jak przewidziano w art. 19 ust. 5 rozporządzenia (WE) nr 765/2008.

Artykuł 20

Procedura postępowania na szczeblu krajowym w przypadku produktów niespełniających mających zastosowanie wymogów dostępności

1. W przypadku gdy organy nadzoru rynku jednego państwa członkowskiego mają wystarczające powody, by uważać, że dany produkt objęty zakresem stosowania niniejszej dyrektywy nie spełnia mających zastosowanie wymogów dostępności, dokonują one oceny tego produktu pod kątem spełnienia wszystkich mających zastosowanie wymogów określonych w niniejszej dyrektywie. W tym celu odpowiednie podmioty gospodarcze w pełni współpracują z organami nadzoru rynku.

W przypadku gdy w toku oceny, o której mowa w akapicie pierwszym, organy nadzoru rynku stwierdzą, że dany produkt nie spełnia wymogów określonych w niniejszej dyrektywie, niezwłocznie zobowiązują odpowiedni podmiot gospodarczy do podjęcia wszystkich określonych przez te ograny stosownych działań naprawczych w celu zapewnienia zgodności produktu z tymi wymogami w rozsądnym terminie, współmiernie do charakteru niezgodności.

Organy nadzoru rynku zobowiązują odpowiednie podmioty gospodarcze do wycofania danego produktu z obrotu w dodatkowym rozsądnym terminie, jedynie jeżeli odpowiedni podmiot gospodarczy nie podejmie adekwatnych działań naprawczych w terminie, o którym mowa w akapicie drugim.

Art. 21 rozporządzenia (WE) nr 765/2008 ma zastosowanie do środków, o których mowa w akapitach drugim i trzecim niniejszego ustępu.

2. W przypadku gdy organy nadzoru rynku uznają, że niezgodność nie ogranicza się wyłącznie do terytorium państwa, w którym prowadzą nadzór, informują one Komisję oraz pozostałe państwa członkowskie o wynikach oceny oraz działaniach, których podjęcia zażądały od podmiotu gospodarczego.

3. Dany podmiot gospodarczy zapewnia podjęcie wszelkich odpowiednich działań naprawczych w odniesieniu do wszystkich odnośnych produktów, które ten podmiot udostępnił na rynku w Unii.

4. W przypadku gdy odpowiedni podmiot gospodarczy nie podejmie odpowiednich działań naprawczych w terminie, o którym mowa w ust. 1 akapit trzeci, organy nadzoru rynku wprowadzają wszelkie odpowiednie środki tymczasowe w celu zakazania lub ograniczenia udostępniania produktów na rynku krajowym lub wycofania danego produktu z obrotu.

Organy nadzoru rynku niezwłocznie przekazują Komisji i pozostałym państwom członkowskim informacje na temat tych środków.

5. Informacje, o których mowa w ust. 4 akapit drugi, obejmują wszelkie dostępne szczegóły, przede wszystkim dane konieczne do identyfikacji produktu niezgodnego, informacje na temat pochodzenia produktu, charakteru występującej domniemanej niezgodności i wymogów dostępności niespełnianych przez dany produkt, rodzaju i okresu obowiązywania wprowadzonych środków krajowych, a także stanowisko przedstawione przez odpowiedni podmiot gospodarczy. W szczególności organy nadzoru rynku są zobowiązane wskazać, czy brak zgodności wynika z którejkolwiek z następujących przyczyn:

a) niespełniania przez produkt mających zastosowanie wymogów dostępności; lub

b) niedociągnięć w normach zharmonizowanych lub specyfikacjach technicznych, o których mowa w art. 15, będących podstawą domniemania zgodności.

6. Państwa członkowskie inne niż państwo członkowskie, które wszczęło postępowanie na podstawie niniejszego artykułu, niezwłocznie informują Komisję i pozostałe państwa członkowskie o wszystkich wprowadzonych środkach i przekazują wszystkie będące w ich posiadaniu dodatkowe informacje dotyczące niezgodności danego produktu, a w przypadku gdy wyrażają sprzeciw wobec notyfikowanego środka krajowego, przedstawiają swoje zastrzeżenia.

7. W przypadku gdy w ciągu trzech miesięcy od otrzymania informacji, o których mowa w ust. 4 akapit drugi, żadne państwo członkowskie ani Komisja nie zgłoszą sprzeciwu wobec środka tymczasowego podjętego przez państwo członkowskie, środek ten uznaje się za uzasadniony.

8. Państwa członkowskie zapewniają niezwłoczne przyjęcie w odniesieniu do danego produktu właściwych środków ograniczających, takich jak wycofanie z obrotu.

Artykuł 21

Procedura ochronna na poziomie Unii

1. W przypadku gdy po ukończeniu postępowania określonego w art. 20 ust. 3 i 4 zgłaszane są sprzeciwy wobec środka podjętego przez państwo członkowskie lub w przypadku gdy Komisja dysponuje racjonalnymi dowodami sugerującymi, że środek krajowy jest sprzeczny z prawem Unii, Komisja niezwłocznie rozpoczyna konsultacje z państwami członkowskimi i odpowiednim podmiotem gospodarczym lub odpowiednimi podmiotami gospodarczymi oraz dokonuje oceny tego środka krajowego. Na podstawie wyników tej oceny Komisja rozstrzyga, czy dany środek krajowy jest uzasadniony.

Komisja kieruje swoją decyzję do wszystkich państw członkowskich i niezwłocznie informuje o niej państwa członkowskie i odpowiedni podmiot gospodarczy lub odpowiednie podmioty gospodarcze.

2. Jeżeli środek krajowy, o którym mowa w ust. 1, zostanie uznany za uzasadniony, wszystkie państwa członkowskie podejmują środki konieczne do zapewnienia, by wyrób niezgodny z wymogami został wycofany z ich rynku, i informują o nich Komisję. Jeżeli środek krajowy zostaje uznany za nieuzasadniony, dane państwo członkowskie wycofuje ten środek.

3. W przypadku gdy środek krajowy, o którym mowa w ust. 1 niniejszego artykułu, zostanie uznany za uzasadniony, a niezgodność produktu zostanie uznana za wynikającą z niedociągnięć w normach zharmonizowanych, o których mowa w art. 20 ust. 5 lit. b), Komisja stosuje procedurę określoną w art. 11 rozporządzenia (UE) nr 1025/2012.

4. W przypadku gdy środek krajowy, o którym mowa w ust. 1 niniejszego artykułu, zostanie uznany za uzasadniony, a niezgodność produktu zostanie uznana za wynikającą z niedociągnięć w specyfikacjach technicznych, o których mowa w art. 20 ust. 5 lit. b), Komisja niezwłocznie przyjmuje akt wykonawczy zmieniający lub uchylający daną specyfikację techniczną. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 27 ust. 2.

Artykuł 22

Niezgodność pod względem formalnym

1. Bez uszczerbku dla art. 20, w przypadku gdy państwo członkowskie dokona jednego z poniższych ustaleń, zobowiązuje ono odpowiedni podmiot gospodarczy do usunięcia przedmiotowych niezgodności:

a) oznakowanie CE zostało umieszczone z naruszeniem art. 30 rozporządzenia (WE) nr 765/2008 lub art. 18 niniejszej dyrektywy;

b) oznakowanie CE nie zostało umieszczone;

c) nie została sporządzona deklaracja zgodności UE;

d) deklaracja zgodności UE nie została sporządzona w prawidłowy sposób;

e) dokumentacja techniczna jest niedostępna lub niekompletna;

f) brak jest informacji, o których mowa w art. 7 ust. 6 lub art. 9 ust. 4, lub są one nieprawdziwe lub niekompletne;

g) nie zostały spełnione inne wymogi administracyjne, o których mowa w art. 7 lub 9.

2. W przypadku utrzymywania się niezgodności, o której mowa w ust. 1, dane państwo członkowskie podejmuje wszelkie odpowiednie środki w celu ograniczenia lub zakazania udostępniania na rynku danego produktu lub w celu zapewnienia jego wycofania z obrotu.

ROZDZIAŁ IX

Zgodność usług

Artykuł 23

Zgodność usług

1. Państwa członkowskie ustanawiają, wdrażają i okresowo aktualizują odpowiednie procedury w celu:

a) sprawdzania zgodności usług z wymogami określonymi w niniejszej dyrektywie, w tym oceny, o której mowa w art. 14, do których stosuje się odpowiednio art. 19 ust. 2;

b) rozpatrywania skarg lub sprawozdań dotyczących kwestii odnoszących się do niezgodności usług z wymogami dostępności określonymi w niniejszej dyrektywie;

c) sprawdzania, czy dany podmiot gospodarczy podjął niezbędne działania naprawcze.

2. Państwa członkowskie wyznaczają organy odpowiedzialne za wdrożenie procedur, o których mowa w ust. 1, w odniesieniu do zgodności usług.

Państwa członkowskie zapewniają, aby społeczeństwo było informowane o istnieniu, obowiązkach, nazwie, pracach i decyzjach organów, o których mowa w akapicie pierwszym. Organy te udostępniają na żądanie te informacje w formatach dostępnych.

ROZDZIAŁ X

Wymogi dostępności w innych aktach prawnych Unii

Artykuł 24

Dostępność na podstawie innych aktów prawnych Unii

1. W odniesieniu do produktów i usług, o których mowa w art. 2 niniejszej dyrektywy, wymogi dostępności określone w załączniku I do niej są obowiązkowymi wymogami w zakresie dostępności w rozumieniu art. 42 ust. 1 dyrektywy 2014/24/UE i art. 60 ust. 1 dyrektywy 2014/25/UE.

2. Produkty lub usługi, których cechy, elementy lub funkcje spełniają wymogi dostępności określone w załączniku I do niniejszej dyrektywy zgodnie z jego sekcją VI, uznaje się za wypełniające – odnośnie do tych cech, elementów lub funkcji – odpowiednie obowiązki w zakresie dostępności określone w aktach unijnych innych niż niniejsza dyrektywa, chyba że w tych innych aktach przewidziano inaczej.

Artykuł 25

Normy zharmonizowane i specyfikacje techniczne odnośnie do innych aktów unijnych

Zgodność z normami zharmonizowanymi i specyfikacjami technicznymi lub ich częściami, które są przyjmowane zgodnie z art. 15, stanowi podstawę domniemania zgodności z art. 24, w zakresie, w jakim te normy i specyfikacje techniczne lub ich części spełniają wymogi dostępności określone w niniejszej dyrektywie.

ROZDZIAŁ XI

Akty delegowane, uprawnienia wykonawcze i przepisy końcowe

Artykuł 26

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 4 ust. 9, powierza się Komisji na czas nieokreślony od dnia 27 czerwca 2019 r.

Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 12 ust. 3 i art. 14 ust. 7, powierza się Komisji na okres pięciu lat od dnia dnia 27 czerwca 2019 r. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem okresu pięciu lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem danego okresu.

3. Przekazanie uprawnień, o którym mowa w art. 4 ust. 9, art. 12 ust. 3 i art. 14 ust. 7, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 4 ust. 9, art. 12 ust. 3 i art. 14 ust. 7 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 27

Procedura komitetowa

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 28

Grupa robocza

Komisja powołuje grupę roboczą składającą się z przedstawicieli organów nadzoru rynku, organów odpowiedzialnych za zgodność usług oraz odpowiednich interesariuszy, w tym przedstawicieli organizacji reprezentujących osoby z niepełnosprawnością.

Grupa robocza:

a) ułatwia wymianę informacji i najlepszych praktyk między organami nadzoru rynku i odpowiednimi interesariuszami;

b) wzmacnia współpracę między organami a odpowiednimi interesariuszami w kwestiach odnoszących się do wdrażania niniejszej dyrektywy, tak by zwiększyć spójność stosowania wymogów dostępności określonych w niniejszej dyrektywie i ściśle monitorować wdrażanie art. 14; oraz

c) udziela porad, w szczególności Komisji, zwłaszcza w odniesieniu do wdrażania art. 4 i 14.

Artykuł 29

Egzekwowanie przepisów

1. Państwa członkowskie zapewniają istnienie odpowiednich i skutecznych środków zapewniających przestrzeganie niniejszej dyrektywy.

2. Środki, o których mowa w ust. 1, obejmują:

a) przepisy, na podstawie których konsument może wnieść skargę na mocy prawa krajowego do sądu lub właściwego organu administracyjnego, aby zapewnić stosowanie krajowych przepisów transponujących przepisy niniejszej dyrektywy;

b) przepisy, na podstawie których organy publiczne lub prywatne stowarzyszenia, organizacje lub inne podmioty prawne, które mają uzasadniony interes w zapewnieniu zgodności z niniejszą dyrektywą, mogą występować na mocy prawa krajowego do sądu lub właściwego organu administracyjnego w imieniu skarżącego, albo dla wsparcia go, za jego zgodą, w ramach dowolnego postępowania sądowego lub administracyjnego dotyczącego egzekwowania obowiązków określonych w niniejszej dyrektywie.

3. Niniejszy artykuł nie ma zastosowania do procedur udzielania zamówień objętych dyrektywą 2014/24/UE lub dyrektywą 2014/25/UE.

Artykuł 30

Sankcje

1. Państwa członkowskie ustanawiają przepisy dotyczące sankcji nakładanych w przypadku naruszenia przepisów krajowych przyjętych na podstawie niniejszej dyrektywy i podejmują wszelkie niezbędne środki w celu zapewnienia ich wdrożenia.

2. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające. Muszą im też towarzyszyć skuteczne działania zaradcze w przypadku niezapewnienia zgodności przez podmiot gospodarczy.

3. Państwa członkowskie bezzwłocznie powiadamiają Komisję o tych przepisach i środkach oraz niezwłocznie powiadamiają ją o każdej późniejszej zmianie, która ich dotyczy.

4. Sankcje uwzględniają zakres niezgodności, w tym jej wagę oraz liczbę niezgodnych z przepisami produktów lub usług, jak również liczbę dotkniętych nimi osób.

5. Niniejszy artykuł nie ma zastosowania do procedur udzielania zamówień objętych dyrektywą 2014/24/UE lub dyrektywą 2014/25/UE.

Artykuł 31

Transpozycja

1. Państwa członkowskie przyjmują i publikują, do dnia 28 czerwca 2022 r., przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie przekazują Komisji tekst tych przepisów.

2. Państwa członkowskie stosują te przepisy od dnia 28 czerwca 2025 r.

3. W drodze odstępstwa od ust. 2 niniejszego artykułu państwa członkowskie mogą podjąć decyzję o stosowaniu środków w odniesieniu do obowiązków określonych w art. 4 ust. 8 najpóźniej od dnia 28 czerwca 2027 r.

4. Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.

5. Państwa członkowskie przekazują Komisji tekst podstawowych przepisów prawa krajowego, przyjętych w dziedzinie objętej niniejszą dyrektywą.

6. Państwa członkowskie korzystające z możliwości przewidzianej w art. 4 ust. 4 przekazują Komisji teksty przyjętych w tym celu podstawowych przepisów prawa krajowego i składają Komisji sprawozdanie z postępów w ich wdrażaniu.

Artykuł 32

Środki przejściowe

1. Bez uszczerbku dla ust. 2 niniejszego artykułu państwa członkowskie ustanawiają okres przejściowy trwający do dnia 28 czerwca 2030 r., w trakcie którego usługodawca może nadal świadczyć usługi, wykorzystując produkty, które zgodnie z prawem wykorzystywał w celu świadczenia podobnych usług przed tą datą.

Umowy o świadczenie usług zawarte przed dniem 28 czerwca 2025 r., mogą nadal obowiązywać w niezmienionej formie do momentu ich wygaśnięcia, lecz nie dłużej niż przez pięć lat od tej daty.

2. Państwa członkowskie mogą postanowić, że terminale samoobsługowe stosowane zgodnie z prawem przez usługodawców w związku ze świadczeniem usług przed dniem 28 czerwca 2025 r. mogą w dalszym ciągu być stosowane do świadczenia podobnych usług aż do upływu okresu ich ekonomicznej użyteczności, nie dłużej jednak niż 20 lat od daty rozpoczęcia ich stosowania.

Artykuł 33

Sprawozdanie i przegląd

1. Do dnia 28 czerwca 2030 r., a następnie co pięć lat, Komisja przedkłada Parlamentowi Europejskiemu, Radzie, Europejskiemu Komitetowi Ekonomiczno-Społecznemu i Komitetowi Regionów sprawozdanie ze stosowania niniejszej dyrektywy.

2. Sprawozdania te dotyczą między innymi – w świetle rozwoju sytuacji społecznej, gospodarczej i technologicznej – zmian w dostępności produktów i usług, ewentualnych blokad technologicznych lub barier dla innowacji oraz skutków niniejszej dyrektywy dla podmiotów gospodarczych i dla osób z niepełnosprawnościami. Sprawozdanie zawiera również ocenę tego, czy stosowanie art. 4 ust. 4 przyczyniło się do zbliżenia rozbieżnych wymogów dostępności środowiska zbudowanego odnośnie do usług przewozów pasażerskich, usług bankowości detalicznej oraz centrów obsługi klienta w sklepach dostawców usług łączności elektronicznej, w miarę możliwości, aby umożliwić ich stopniowe dostosowywanie do wymogów dostępności określonych w załączniku III.

W sprawozdaniach ocenia się także, czy stosowanie niniejszej dyrektywy, w szczególności jej przepisów o charakterze dobrowolnym, przyczyniło się do zbliżenia wymogów dostępności środowiska zbudowanego stanowiącego roboty budowlane objęte zakresem stosowania dyrektywy Parlamentu Europejskiego i Rady 2014/23/UE ([35]), dyrektywy 2014/24/UE i dyrektywy 2014/25/UE.

Sprawozdania obejmują również skutki, jakie dla funkcjonowania rynku wewnętrznego mają stosowanie art. 14 niniejszej dyrektywy, w tym – w stosownych przypadkach – na podstawie informacji otrzymanych zgodnie z art. 14 ust. 8, oraz wyłączenie mikroprzedsiębiorstw. Z myślą o ewentualnym przeglądzie niniejszej dyrektywy w sprawozdaniu stwierdzone zostanie, czy niniejsza dyrektywa osiągnęła swoje cele i czy wskazane byłoby objęcie zakresem stosowania niniejszej dyrektywy nowych produktów i usług lub wykluczenie z niego niektórych produktów lub usług; określone zostaną także, w miarę możliwości, dziedziny, w których należy zmniejszyć obciążenia.

Komisja, w razie potrzeby, proponuje odpowiednie środki, które mogą obejmować środki ustawodawcze.

([35]) Dyrektywa Parlamentu Europejskiego i Rady 2014/23/UE z dnia 26 lutego 2014 r. w sprawie udzielania koncesji (Dz.U. L 94 z 28.3.2014, s. 1).

3. Państwa członkowskie przekazują Komisji w odpowiednim terminie wszystkie informacje, które są dla niej niezbędne do sporządzenia takich sprawozdań.

4. Sprawozdania Komisji uwzględniają opinie zainteresowanych podmiotów gospodarczych i odpowiednich organizacji pozarządowych, w tym organizacji reprezentujących osoby z niepełnosprawnościami.

Artykuł 34

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 35

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w Strasburgu dnia 17 kwietnia 2019 r.

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

ZAŁĄCZNIK I

WYMOGI DOSTĘPNOŚCI PRODUKTÓW I USŁUG

Sekcja I

Ogólne wymogi dostępności dotyczące wszystkich produktów objętych niniejszą dyrektywą zgodnie z art. 2 ust. 1

Produkty muszą być projektowane i wytwarzane w taki sposób, aby zmaksymalizować ich przewidywalne wykorzystywanie przez osoby z niepełnosprawnościami; do produktów muszą być dołączane, w miarę możliwości w produkcie lub na nim, dostępne informacje o ich działaniu oraz o cechach decydujących o ich dostępności.

1. Wymogi dotyczące udzielania informacji:

   a) informacje na temat użytkowania produktu zamieszczone na samym produkcie (etykietowanie, instrukcje i ostrzeżenia) muszą być:

      (i) udostępniane za pomocą więcej niż jednego kanału sensorycznego;

      (ii) przedstawione w sposób zrozumiały;

      (iii) przedstawione użytkownikom w formie umożliwiającej ich odbiór;

      (iv) przedstawione za pomocą czcionki o odpowiednim rozmiarze i kształcie, z uwzględnieniem przewidywalnych warunków użytkowania oraz z zastosowaniem wystarczającego kontrastu i regulowanych odstępów między literami, wierszami i akapitami;

   b) instrukcje użytkowania produktu niezamieszczone na samym produkcie, ale udostępniane podczas jego użytkowania lub w inny sposób (na przykład za pośrednictwem strony internetowej) – w tym instrukcje dotyczące funkcji produktu ułatwiających dostęp, sposobu ich aktywacji i ich interoperacyjności z rozwiązaniami wspomagającymi – muszą być dostępne publicznie w momencie wprowadzania produktu do obrotu i muszą:

      (i) być udostępniane za pomocą więcej niż jednego kanału sensorycznego;

      (ii) być przedstawione w sposób zrozumiały;

      (iii) być przedstawione użytkownikom w formie umożliwiającej ich odbiór;

      (iv) być przedstawione za pomocą czcionki o odpowiednim rozmiarze i kształcie, z uwzględnieniem przewidywalnych warunków użytkowania oraz z zastosowaniem wystarczającego kontrastu i regulowanych odstępów między literami, wierszami i akapitami;

      (v) jeżeli chodzi o treść, instrukcje muszą być udostępniane w formatach tekstowych umożliwiających tworzenie alternatywnych formatów wspomagających, które mogą być przedstawiane na różne sposoby i za pomocą więcej niż jednego kanału sensorycznego;

      (vi) obejmować alternatywną prezentację treści nietekstowych;

      (vii) obejmować opis interfejsu użytkownika produktu (obsługa, sterowanie i informacje zwrotne, dane wejściowe i wyjściowe), który jest przedstawiany zgodnie z pkt 2; opis ten powinien wskazywać – dla każdej z liter w pkt 2 – czy produkt posiada te cechy;

      (viii) obejmować opis funkcjonowania produktu, który jest zapewniany poprzez funkcje mające na celu uwzględnienie potrzeb osób z niepełnosprawnościami zgodnie z pkt 2; opis ten powinien wskazywać – dla każdej z liter w pkt 2 – czy produkt posiada te cechy;

      (ix) obejmować opis oprogramowania i sprzętu łączących produkt z urządzeniami wspomagającymi; opis ten powinien obejmować wykaz tych urządzeń wspomagających, które były testowane wraz z danym produktem.

2. Interfejs użytkownika i projektowanie uwzględniające potrzebę funkcjonalności:

   Produkt, w tym jego interfejs użytkownika, musi zawierać cechy, elementy i funkcje, które umożliwiają osobom z niepełnosprawnościami dostęp do produktu, jego postrzeganie, obsługę, zrozumienie sposobu jego działania i sterowanie nim:

   a) jeżeli produkt umożliwia komunikowanie się, w tym komunikację interpersonalną, obsługę, informację, sterowanie i orientację, musi to być możliwe przez więcej niż jeden kanał sensoryczny; musi to obejmować rozwiązania alternatywne dla elementów wizualnych i dźwiękowych, elementów mowy i elementów dotykowych;

   b) jeżeli produkt wykorzystuje mowę, musi zapewniać alternatywne rozwiązania dla mowy i wprowadzania danych głosowych na potrzeby komunikacji, obsługi, sterowania i orientacji;

c) jeżeli produkt wykorzystuje elementy wizualne, musi zapewniać elastyczne rozwiązania dotyczące powiększania obrazu, zwiększania jasności i kontrastu dla komunikacji, informacji i obsługi, a także zapewniać interoperacyjność z urządzeniami wspomagającymi i programami umożliwiającymi nawigację po interfejsie;

d) jeżeli produkt wykorzystuje kolor do przekazywania informacji, wskazania działania, które należy wykonać, wskazania konieczności reakcji ze strony użytkownika lub zaznaczenia pewnych elementów, musi zapewnić rozwiązanie alternatywne do stosowania kolorów;

e) jeżeli produkt wykorzystuje sygnały dźwiękowe do przekazywania informacji, wskazania działania, które należy wykonać, wskazania konieczności reakcji ze strony użytkownika lub zaznaczenia pewnych elementów, musi zapewnić rozwiązanie alternatywne do stosowania sygnałów dźwiękowych;

f) jeżeli produkt wykorzystuje elementy wizualne, musi zapewniać elastyczne sposoby poprawy wyrazistości wizji;

g) jeżeli produkt wykorzystuje elementy dźwiękowe, musi zapewniać użytkownikowi możliwość sterowania głośnością i szybkością odtwarzania oraz zaawansowane funkcje dźwiękowe, w tym redukcję zakłóceń ze strony sygnałów dźwiękowych pochodzących od okolicznych produktów i wyrazistość dźwięku;

h) jeżeli produkt wymaga ręcznej obsługi i sterowania, musi umożliwiać sterowanie sekwencyjne i alternatywne rozwiązania z zakresu motoryki małej; należy unikać konieczności jednoczesnego manipulowania więcej niż jednym przełącznikiem, które muszą być możliwe do rozróżnienia za pomocą dotyku;

i) w produkcie nie stosuje się trybów pracy wymagających dużego zasięgu i dużej siły fizycznej;

j) produkt nie może wywoływać ataków padaczki fotogennej;

k) przy korzystaniu z cech decydujących o dostępności produktu musi chronić prywatność użytkownika;

l) produkt musi zapewnić alternatywę dla identyfikacji biometrycznej i kontroli danych biometrycznych;

m) produkt musi zapewniać spójność funkcji i zapewnić wystarczająco długi czas na interakcję oraz możliwość elastycznego dostosowywania czasu;

n) produkt musi zapewniać oprogramowanie i sprzęt służące do łączenia się z technologiami wspomagającymi;

o) produkt musi spełniać następujące wymogi sektorowe:

(i) terminale samoobsługowe:

— muszą oferować technologię syntezy mowy,

— muszą umożliwiać stosowanie własnych słuchawek,

— jeżeli wymagana jest reakcja w określonym czasie – muszą informować użytkownika o tym za pośrednictwem więcej niż jednego kanału sensorycznego,

— muszą zapewniać możliwość wydłużenia danego czasu,

— muszą zapewniać odpowiedni kontrast oraz możliwość dotykowego rozpoznania klawiszy i przełączników, o ile występują,

— nie mogą wymagać, by dana cecha decydująca o dostępności musiała zostać aktywowana, aby użytkownik mógł z niej korzystać,

— jeżeli produkt wykorzystuje sygnały lub elementy dźwiękowe, musi być kompatybilny z dostępnymi na poziomie Unii urządzeniami i technologiami wspomagającymi, w tym technologiami wzmacniającymi słuch, takimi jak aparaty słuchowe, cewki indukcyjne, implanty ślimakowe i urządzenia wspomagające słyszenie;

(ii) czytniki książek elektronicznych muszą oferować technologię syntezy mowy;

(iii) konsumenckie urządzenie końcowe mające interaktywne zdolności obliczeniowe wykorzystywane do usług łączności elektronicznej:

— gdy poza porozumiewaniem głosowym oferuje możliwości porozumiewania się za pomocą tekstu, musi umożliwiać przetwarzanie tekstu w czasie rzeczywistym i obsługiwać dźwięk jakości hi-fi,

— gdy poza porozumiewaniem głosowym i za pomocą tekstu lub w połączeniu z takimi sposobami porozumiewania się oferuje możliwości porozumiewania się za pomocą transmisji wideo, musi umożliwiać przeprowadzenie pełnej konwersacji, obejmującej komunikację głosową zsynchronizowaną z tekstem przekazywanym w czasie rzeczywistym i transmisją wideo o rozdzielczości umożliwiającej komunikację w języku migowym,

— musi umożliwiać skuteczne bezprzewodowe połączenie z technologiami wzmacniającymi słuch,

— musi unikać zakłóceń ze strony urządzeń wspomagających;

(iv) konsumenckie urządzenie końcowe mające interaktywne zdolności obliczeniowe, służące do korzystania z audiowizualnych usług medialnych musi oferować osobom z niepełnosprawnościami elementy dostępności zapewniane przez dostawcę usług audiowizualnych dotyczące dostępu użytkownika, wyboru, sterowania i personalizacji oraz transmisji do urządzeń wspomagających.

3. Usługi wsparcia:

W przypadku gdy udostępniane są usługi wsparcia (działy pomocy technicznej, centra obsługi telefonicznej, wsparcie techniczne, usługi przekazu i usługi szkoleniowe), udzielają one informacji na temat dostępności produktu i jego kompatybilności z technologiami wspomagającymi, za pośrednictwem dostępnych sposobów komunikacji.

Sekcja II

Wymogi dostępności dotyczące produktów objętych art. 2 ust. 1, z wyjątkiem terminali samoobsługowych, o których mowa w art. 2 ust. 1 lit. b)

W uzupełnieniu wymogów sekcji I opakowaniom i instrukcjom produktów, których dotyczy niniejsza sekcja, należy nadać dostępny charakter, aby zmaksymalizować ich przewidywalne wykorzystywanie przez osoby z niepełnosprawnościami. Oznacza to, że:

a) opakowanie produktu oraz zamieszczone na nim informacje (dotyczące np. otwierania, zamykania, stosowania, usuwania), w tym, o ile są podawane, informacje dotyczące cech produktu decydujących o jego dostępności, muszą mieć dostępny charakter i w miarę możliwości być umieszczone na opakowaniu;

b) instrukcje dotyczące instalacji, konserwacji, przechowywania i usuwania produktu, niezamieszczone na samym produkcie, ale udostępniane w inny sposób (np. za pośrednictwem strony internetowej), muszą być udostępniane publicznie w momencie wprowadzania produktu do obrotu i spełniać przedstawione poniżej wymogi:

(i) być dostępne za pomocą więcej niż jednego kanału sensorycznego;

(ii) być przedstawione w sposób zrozumiały;

(iii) być przedstawione użytkownikom w formie umożliwiającej ich odbiór;

(iv) być przedstawione za pomocą czcionki o odpowiednim rozmiarze i kształcie, z uwzględnieniem przewidywalnych warunków użytkowania oraz z zastosowaniem wystarczającego kontrastu i regulowanych odstępów między literami, wierszami i akapitami;

(v) treść instrukcji musi być udostępniana w formatach tekstowych umożliwiających tworzenie alternatywnych formatów wspomagających, które mogą być przedstawiane na różne sposoby i za pośrednictwem więcej niż jednego kanału sensorycznego; oraz

(vi) instrukcjom zawierającym treści nietekstowe powinny towarzyszyć alternatywne prezentacje tych treści.

Sekcja III

Ogólne wymogi dostępności dotyczące wszystkich usług objętych niniejszą dyrektywą zgodnie z art. 2 ust. 2

Świadczenie usług w taki sposób, aby zmaksymalizować ich przewidywalne wykorzystywanie przez osoby z niepełnosprawnościami odbywa się poprzez:

a) zapewnienie dostępności produktów wykorzystywanych do świadczenia danej usługi, zgodnie z sekcją I niniejszego załącznika, oraz – w stosownych przypadkach – z sekcją II;

b) udzielanie informacji o funkcjonowaniu usługi oraz, w przypadku produktów wykorzystywanych w ramach świadczenia usług, udzielanie informacji o ich związku z usługą, ich właściwościach dotyczących dostępności oraz ich interoperacyjności z urządzeniami i funkcjami wspomagającymi:

(i) udostępnianie informacji za pomocą więcej niż jednego kanału sensorycznego;

(ii) przedstawianie informacji w sposób zrozumiały;

(iii) przedstawianie użytkownikom informacji w formie umożliwiającej ich odbiór;

(iv) udostępnianie treści informacji w formatach tekstowych umożliwiających tworzenie alternatywnych formatów wspomagających, które mogą być przedstawiane przez użytkowników na różne sposoby i za pośrednictwem więcej niż jednego kanału sensorycznego;

(v) przedstawianie za pomocą czcionki o odpowiednim rozmiarze i kształcie, z uwzględnieniem przewidywalnych warunków użytkowania oraz z zastosowaniem wystarczającego kontrastu i regulowanych odstępów między literami, wierszami i akapitami;

(vi) uzupełnianie treści nietekstowych alternatywnymi prezentacjami tych treści; oraz

(vii) udzielanie informacji elektronicznych potrzebnych do świadczenia usługi w sposób spójny i adekwatny poprzez uczynienie ich zauważalnymi, funkcjonalnymi, zrozumiałymi i solidnymi;

c) zapewnianie dostępności stron internetowych – w tym powiązanych aplikacji internetowych, usług świadczonych za pomocą urządzeń mobilnych, w tym aplikacji mobilnych – w sposób spójny i adekwatny, poprzez uczynienie ich zauważalnymi, funkcjonalnymi, zrozumiałymi i solidnymi;

d) w przypadku gdy udostępniane są usługi wsparcia (działy pomocy technicznej, centra obsługi telefonicznej, wsparcie techniczne, usługi przekazu i usługi szkoleniowe) – udzielanie przez nie informacji na temat dostępności usługi i jej kompatybilności z technologiami wspomagającymi, za pośrednictwem dostępnych sposobów komunikacji.

Sekcja IV

Dodatkowe wymogi dostępności usług szczególnych

Świadczenie usług musi odbywać się w taki sposób, aby zmaksymalizować ich przewidywalne wykorzystywanie przez osoby z niepełnosprawnościami; w tym celu uwzględnia się następujące funkcje, praktyki, strategie i procedury oraz zmiany w świadczeniu usług ukierunkowane na zaspokajanie potrzeb osób z niepełnosprawnościami oraz zapewnianie interoperacyjności z technologiami wspomagającymi:

a) Usługi łączności elektronicznej, w tym zgłoszenia alarmowe, o których mowa w art. 109 ust. 2 dyrektywy (UE) 2018/1972:

(i) przekazywanie tekstu w czasie rzeczywistym w uzupełnieniu komunikacji głosowej;

(ii) zapewnianie pełnej konwersacji, w przypadku gdy poza komunikacją głosową dostępna jest transmisja wideo;

(iii) zapewnianie, by zgłoszenia alarmowe z wykorzystaniem głosu, tekstu (w tym tekstu w czasie rzeczywistym) były synchronizowane i – gdy oferowane jest wideo – by były także synchronizowane jako pełna konwersacja i przekazywane przez dostawców usług łączności elektronicznej najwłaściwszemu publicznemu punktowi przyjmowania zgłoszeń.

b) Usługi umożliwiające dostęp do audiowizualnych usług medialnych:

(i) udostępnianie zauważalnych, funkcjonalnych, zrozumiałych i solidnych elektronicznych przewodników po programach oraz informacji o oferowanej dostępności;

(ii) upewnianie, by elementy dostępności (usługi dostępu) audiowizualnych usług medialnych, takie jak napisy dla osób niesłyszących i niedosłyszących, audiodeskrypcja, napisy czytane i tłumaczenie na język migowy, były w pełni przekazywane z odpowiednią jakością umożliwiającą ich właściwe wyświetlenie oraz zsynchronizowane z dźwiękiem i wideo, a jednocześnie by umożliwiały sterowanie ich wyświetlaniem i wykorzystywaniem przez użytkownika.

c) Usługi lotniczego, autobusowego, kolejowego i wodnego transportu pasażerskiego, z wyjątkiem przewozów miejskich i podmiejskich oraz przewozów regionalnych:

(i) zapewnianie udzielania informacji na temat dostępności pojazdów, otaczającej infrastruktury oraz środowiska zbudowanego oraz na temat pomocy dla osób z niepełnosprawnościami;

(ii) zapewnianie udzielania informacji o systemach inteligentnej sprzedaży biletów (rezerwacja elektroniczna, rezerwacja biletów itd.), informacji dla pasażerów w czasie rzeczywistym (rozkłady jazdy, informacje o zakłóceniach ruchu, połączeniach, dalszej podróży innym środkiem transportu itd.), a także dodatkowych informacji o usługach (np. personel na stacjach, niedziałające windy lub usługi czasowo niedostępne).

d) Przewozy miejskie i podmiejskie oraz przewozy regionalne: zapewnianie dostępności terminali samoobsługowych wykorzystywanych w ramach świadczenia usług, zgodnie z sekcją I niniejszego załącznika.

e) Usługi bankowości detalicznej:

(i) zapewnianie zauważalnych, funkcjonalnych, zrozumiałych i solidnych metod identyfikacji, podpisów elektronicznych, bezpieczeństwa i usług płatniczych.

(ii) zapewnianie, by informacje były zrozumiałe, a ich stopień złożoności nie przekraczał poziomu B2 (wyższy średnio zaawansowany) według Europejskiego Systemu Opisu Kształcenia Językowego Rady Europy.

f) Książki elektroniczne:

(i) zapewnianie – w sytuacji gdy książka elektroniczna zawiera oprócz tekstu także dźwięk – synchronizacji tekstu i dźwięku;

(ii) zapewnianie, by cyfrowe pliki książki elektronicznej nie uniemożliwiały prawidłowego funkcjonowania technologii wspomagających;

(iii) zapewnianie dostępu do treści, nawigacji po treści pliku i jego układzie graficznym (również w dynamicznym układzie graficznym), struktury, elastyczności i możliwości wyboru sposobu prezentacji treści;

(iv) umożliwienie alternatywnego przedstawienia treści i jej interoperacyjności z różnorodnymi technologiami wspomagającymi w taki sposób, by było ono zauważalne, funkcjonalne, zrozumiałe i solidne;

(v) zapewnianie, by były one wykrywalne, poprzez oferowanie informacji za pośrednictwem metadanych dotyczących ich cech decydujących o dostępności;

(vi) zapewnianie, by środki w zakresie zarządzania prawami cyfrowymi nie blokowały cech decydujących o dostępności.

g) Usługi handlu elektronicznego:

(i) udzielanie informacji o dostępności sprzedawanych produktów i usług, jeżeli informacje te zostały podane przez odpowiedzialny podmiot gospodarczy;

(ii) zapewnianie, by funkcje służące identyfikacji, zachowaniu bezpieczeństwa i płatności, gdy stanowią one część dostarczanej usługi (a nie produktu) charakteryzowały się dostępnością, tak by były one zauważalne, funkcjonalne, zrozumiałe i solidne;

(iii) zapewnianie zauważalnych, funkcjonalnych, zrozumiałych i solidnych metod identyfikacji, podpisów elektronicznych i usług płatniczych.

Sekcja V

Szczegółowe wymogi dostępności dotyczące odbioru zgłoszeń alarmowych kierowanych pod jednolity europejski numer alarmowy 112 przez najwłaściwszy publiczny punkt przyjmowania zgłoszeń

Odbiór zgłoszeń alarmowych przez najwłaściwszy publiczny punkt przyjmowania zgłoszeń kierowanych pod jednolity europejski numer alarmowy 112 należy – aby zmaksymalizować ich przewidywalne wykorzystywanie przez osoby z niepełnosprawnościami – zapewnić poprzez uwzględnienie funkcji, praktyk, strategii i procedur oraz zmian ukierunkowanych na zaspokajanie potrzeb osób z niepełnosprawnościami.

Zgłoszenia alarmowe kierowane pod jednolity europejski numer alarmowy 112 muszą być odbierane w adekwatny sposób najlepiej odpowiadający krajowej organizacji systemów alarmowych, w najwłaściwszym publicznym punkcie przyjmowania zgłoszeń z wykorzystaniem tego samego środka łączności, za pośrednictwem którego zgłoszenie odebrano, mianowicie poprzez wykorzystywanie synchronizowanego głosu i tekstu (w tym tekstu w czasie rzeczywistym) lub – gdy oferowane jest wideo – głosu, tekstu (w tym tekstu w czasie rzeczywistym) i wideo zsynchronizowanych jako pełna konwersacja.

Sekcja VI

Wymogi dostępności cech, elementów lub funkcji produktów i usług, zgodnie z art. 24 ust. 2

Domniemanie spełnienia odpowiednich obowiązków określonych w innych aktach unijnych dotyczących cech, elementów lub funkcji produktów i usług wymaga, by spełnione były następujące warunki:

1. Produkty:

a) dostępny charakter informacji dotyczących działania produktów oraz cech decydujących o dostępności produktów musi być zgodny z odpowiednimi elementami określonymi w pkt 1 sekcji I niniejszego załącznika; chodzi mianowicie o informacje dotyczące użytkowania produktu zamieszczone na samym produkcie oraz instrukcje użytkowania produktu niezamieszczone w samym produkcie, lecz udostępniane w trakcie użytkowania produktu lub w inny sposób, na przykład za pośrednictwem strony internetowej;

b) dostępny charakter cech, elementów i funkcji interfejsu użytkownika oraz projektowanie produktów uwzględniające potrzebę funkcjonalności musi spełniać odpowiednie wymogi dostępności, które odnoszą się do takiego interfejsu użytkownika lub projektowania uwzględniającego potrzebę funkcjonalności i które określono w pkt 2 sekcji I niniejszego załącznika;

c) dostępny charakter opakowania, w tym informacje udostępnione w nim oraz instrukcje dotyczące instalacji, konserwacji, przechowywania i usuwania produktu, niezamieszczone w samym produkcie, ale udostępniane w inny sposób (np. za pośrednictwem strony internetowej), z wyjątkiem terminali samoobsługowych, muszą spełniać odpowiednie wymogi dostępności określone w sekcji II niniejszego załącznika.

2. Usługi:

Dostępny charakter cech, elementów i funkcji usług musi spełniać odpowiednie wymogi dostępności tych cech, elementów i funkcji, które to wymogi określono w sekcjach niniejszego załącznika dotyczących usług.

Sekcja VII

Kryteria funkcjonalne

Jeżeli wymogi dostępności określone w sekcjach I–VI niniejszego załącznika nie uwzględniają jednej lub większej liczby funkcji projektowania i wytwarzania produktów lub świadczenia usług, te funkcje lub środki muszą być dostępne, tak by – poprzez spełnienie odnośnych kryteriów funkcjonalnych – zapewnione było ich jak najlepsze przewidywalne wykorzystanie przez osoby z niepełnosprawnościami.

Te kryteria funkcjonalne mogą być wykorzystywane wyłącznie jako alternatywa dla jednego specyficznego wymogu technicznego lub większej ich liczby, gdy wymogi te są wskazane w wymogach dostępności, jedynie w przypadku gdy stosowanie odpowiednich kryteriów funkcjonalnych spełnia wymogi dostępności i powoduje, że projektowanie i wytwarzanie produktów oraz świadczenie usług prowadzi do równoważnej lub większej dostępności w przewidywalnym wykorzystaniu przez osoby z niepełnosprawnościami.

a) Użytkowanie przez osoby niewidome

Jeżeli produkt lub usługa obsługiwane są w sposób angażujący wzrok, należy zapewnić co najmniej jeden tryb obsługi, który nie wymaga zaangażowania wzroku.

b) Użytkowanie w przypadku ograniczonej zdolności widzenia

Jeżeli produkt lub usługa obsługiwane są w sposób angażujący wzrok, należy zapewnić co najmniej jeden tryb obsługi, który umożliwia użytkownikom obsługę produktu przy ograniczonej zdolności widzenia.

c) Użytkowanie w przypadku zaburzenia widzenia barw

Jeżeli produkt lub usługa obsługiwane są w sposób angażujący wzrok, należy zapewnić co najmniej jeden tryb obsługi, który nie wymaga od użytkownika zdolności widzenia barw.

d) Użytkowanie przez osoby niesłyszące

Jeżeli produkt lub usługa obsługiwane są w sposób angażujący słuch, należy zapewnić co najmniej jeden tryb obsługi, który nie wymaga zaangażowania słuchu.

e) Użytkowanie w przypadku ograniczonej zdolności słyszenia

Jeżeli produkt lub usługa obsługiwane są w sposób angażujący słuch, należy zapewnić co najmniej jeden tryb obsługi, który wykorzystuje zaawansowane funkcje dźwiękowe i umożliwia obsługę użytkownikom o ograniczonej zdolności słyszenia.

f) Użytkowanie przez osoby nieme

Jeżeli produkt lub usługa wymagają od użytkowników użycia głosu, należy zapewnić co najmniej jeden tryb obsługi, który nie wymaga używania głosu. Używanie głosu oznacza wydawanie za pomocą ust. wszelkiego rodzaju dźwięków, np. mowy, gwizdów lub mlasków.

g) Użytkowanie w przypadku ograniczonej sprawności manualnej lub siły fizycznej

Jeżeli produkt lub usługa wymagają obsługi manualnej, należy zapewnić co najmniej jeden tryb obsługi, który umożliwia użytkownikom korzystanie z tego produktu za pomocą alternatywnych trybów obsługi niewymagających czynności z zakresu motoryki małej, sprawności manualnej ani siły fizycznej w rękach ani też jednoczesnego manipulowania więcej niż jednym przełącznikiem.

h) Użytkowanie przez osoby o ograniczonym zasięgu

Elementy umożliwiające obsługę produktów muszą znajdować się w zasięgu wszystkich użytkowników. Jeżeli produkt lub usługa obsługiwane są w sposób manualny, należy zapewnić co najmniej jeden tryb obsługi pozwalający na użytkowanie przez osoby o ograniczonym zasięgu i ograniczonej sile fizycznej.

i) Minimalizacja ryzyka wywołania napadów padaczki fotogennej

Jeżeli produkt obsługiwany jest w sposób angażujący wzrok, należy unikać trybów obsługi, które wywołują napady padaczki fotogennej.

j) Użytkowanie w przypadku ograniczonych zdolności poznawczych

Należy zapewnić co najmniej jeden tryb obsługi produktu lub usługi obejmujący cechy upraszczające i ułatwiające obsługę.

k) Ochrona prywatności

Jeżeli produkt lub usługa posiadają cechy wprowadzone w celu zapewnienia dostępności, należy zapewnić co najmniej jeden tryb obsługi, który zachowuje prywatność przy korzystaniu z tych cech wprowadzonych w celu zapewnienia dostępności.

ZAŁĄCZNIK II

ORIENTACYJNE NIEWIĄŻĄCE PRZYKŁADY ROZWIĄZAŃ, KTÓRE PRZYCZYNIAJĄ SIĘ DO SPEŁNIENIA WYMOGÓW DOSTĘPNOŚCI OKREŚLONYCH W ZAŁĄCZNIKU I

SEKCJA I:

PRZYKŁADY DOTYCZĄCE OGÓLNYCH WYMOGÓW DOSTĘPNOŚCI W ODNIESIENIU DO WSZYSTKICH PRODUKTÓW OBJĘTYCH NINIEJSZĄ DYREKTYWĄ ZGODNIE Z ART. 2 UST. 1

WYMOGI SEKCJI I ZAŁĄCZNIKA I	PRZYKŁADY
1. Udzielanie informacji	
a)	
(i)	Zapewnienie informacji wizualnej i dotykowej lub wizualnej i dźwiękowej wskazującej miejsce, w które należy wprowadzić kartę w terminalu samoobsługowym, tak by z terminala mogły skorzystać osoby niewidome i niesłyszące.
(ii)	Stosowanie tego samego słownictwa w sposób spójny lub zgodnie z jasną i logiczną strukturą, tak by osoby z niepełnosprawnościami intelektualnymi mogły je lepiej zrozumieć.
(iii)	Zapewnienie wypukłych oznaczeń dotykowych lub dźwięków wraz z ostrzeżeniem tekstowym, tak by osoby niewidome mogły to ostrzeżenie odebrać.
(iv)	Zapewnienie, by tekst mogły odczytać osoby słabowidzące.
b)	
(i)	Dostarczanie plików elektronicznych, które mogą być odczytane przez komputer z czytnikiem ekranu, tak by osoby niewidome mogły wykorzystać te informacje.
(ii)	Stosowanie tego samego słownictwa w sposób spójny lub zgodnie z jasną i logiczną strukturą, tak by osoby z niepełnosprawnościami intelektualnymi mogły je lepiej zrozumieć.
(iii)	Zapewnianie napisów przy wyświetlaniu wideo z instrukcjami.
(iv)	Zapewnienie, by tekst mogły odczytać osoby słabowidzące.
(v)	Drukowanie alfabetem Braille'a, tak by osoby niewidome mogły wykorzystać udzielane informacje.
(vi)	Dołączanie do diagramu opisu tekstowego określającego jego główne elementy lub opisującego najważniejsze działania.
(vii)	Brak przykładów
(viii)	Brak przykładów
(ix)	Uwzględnienie w bankomacie gniazdka i oprogramowania, które umożliwią podłączenie słuchawek odbierających wyświetlony na ekranie tekst w formie dźwiękowej.

2. Interfejs użytkownika i projektowanie uwzględniające potrzebę funkcjonalności	
a)	Dostarczanie instrukcji w formie głosowej i tekstowej lub umieszczenie oznakowania dotykowego na klawiaturze, tak by osoby niewidome lub niedosłyszące mogły korzystać z produktu.
b)	Zapewnienie, by terminal samoobsługowy wydający instrukcje głosowe wyświetlał je np. także w formie tekstu lub obrazów, tak by wymagane działanie mogły wykonać także osoby niesłyszące.
c)	Umożliwienie użytkownikom powiększenia tekstu, powiększenia konkretnego piktogramu lub zwiększenia kontrastu, tak by osoby słabowidzące mogły zapoznać się z przedstawionymi informacjami.
d)	Zapewnienie – oprócz możliwości wciśnięcia zielonego lub czerwonego przycisku w celu wyboru jednej z opcji – opisowego oznaczenia przycisków, tak by wyboru mogły dokonać osoby z zaburzeniem widzenia barw.
e)	Zapewnienie, by komputer, wydając sygnał błędu, wyświetlał tekst lub obraz informujący o błędzie, tak by komunikat o błędzie był zrozumiały dla osób niesłyszących.
f)	Umożliwienie dodatkowego kontrastu w obrazach pierwszego planu, tak by mogły je zobaczyć osoby niedowidzące.
g)	Umożliwienie użytkownikowi telefonu wyboru poziomu głośności i zmniejszenie interferencji z aparatem słuchowym, tak by z telefonu mogły korzystać osoby niedosłyszące.
h)	Zwiększenie rozmiaru przycisków na ekranie dotykowym i odległości między nimi, tak by można je było wcisnąć drżącą dłonią.
i)	Zapewnienie, by wciskanie przycisków nie wymagało dużej siły fizycznej, tak by mogły z nich korzystać osoby o mniejszej sprawności motorycznej.
j)	Unikanie migoczących obrazów, tak by nie powodować zagrożenia dla osób, u których może wystąpić atak.
k)	Umożliwienie korzystania ze słuchawek, gdy bankomat udziela informacji głosowych.
l)	Umożliwienie osobom, które nie mogą używać rąk – jako alternatywę dla stosowania odcisków palca – ustawienia hasła blokującego i odblokowującego telefon.
m)	Zapewnienie, by przy wykonywaniu konkretnego działania oprogramowanie reagowało w sposób przewidywalny, oraz zapewnienie odpowiedniego czasu na wprowadzenie hasła, tak by osoby z niepełnosprawnościami intelektualnymi nie miały problemów z korzystaniem z danego oprogramowania.
n)	Umożliwienie połączenia z odświeżalnym monitorem brajlowskim, tak by osoba niewidoma mogła korzystać z komputera.
o)	Przykłady wymogów sektorowych
(i)	Brak przykładów
(ii)	Brak przykładów
(iii) tiret pierwsze	Zapewnienie, by telefon komórkowy mógł obsługiwać konwersacje tekstowe w czasie rzeczywistym, tak by osoby niedosłyszące mogły aktywnie uczestniczyć w wymianie informacji.
(iii) tiret czwarte	Umożliwienie jednoczesnego korzystania z transmisji wideo do wyświetlania komunikatów w języku migowym oraz tekstu do wpisywania komunikatów, tak by umożliwić komunikację dwóch osób niesłyszących lub osoby niesłyszącej z osobą słyszącą.

(iv)	Zapewnienie, by napisy były przekazywane przez urządzenia typu set-top box umożliwiające korzystanie z nich przez osoby niesłyszące.

3. Usługi wsparcia: Brak przykładów

SEKCJA II:

PRZYKŁADY DOTYCZĄCE WYMOGÓW DOSTĘPNOŚCI W ODNIESIENIU DO PRODUKTÓW OBJĘTYCH ART. 2 UST. 1, Z WYJĄTKIEM TERMINALI SAMOOBSŁUGOWYCH, O KTÓRYCH MOWA W ART. 2 UST. 1 LIT. b)

WYMOGI SEKCJI II ZAŁĄCZNIKA I	PRZYKŁADY
Opakowania i instrukcje produktów	
a)	Wskazanie na opakowaniu, że telefon posiada cechy ułatwiające dostęp osobom z niepełnosprawnościami.
b)	
(i)	Dostarczanie plików elektronicznych, które mogą być odczytane przez komputer z czytnikiem ekranu, tak by osoby niewidome mogły wykorzystać te informacje.
(ii)	Stosowanie tego samego słownictwa w sposób spójny lub zgodnie z jasną i logiczną strukturą, tak by osoby z niepełnosprawnościami intelektualnymi mogły je lepiej zrozumieć.
(iii)	Zapewnienie wypukłych oznaczeń dotykowych lub dźwięków wraz z ostrzeżeniem tekstowym, tak by osoby niewidome mogły to ostrzeżenie odebrać.
(iv)	Zapewnienie, by tekst mogły odczytać osoby słabowidzące.
(v)	Drukowanie alfabetem Braille'a, tak by osoby niewidome mogły przeczytać opakowanie lub instrukcję.
(vi)	Dołączanie do diagramu opisu tekstowego określającego jego główne elementy lub opisującego najważniejsze działania.

SEKCJA III:

PRZYKŁADY DOTYCZĄCE OGÓLNYCH WYMOGÓW DOSTĘPNOŚCI W ODNIESIENIU DO WSZYSTKICH USŁUG OBJĘTYCH NINIEJSZĄ DYREKTYWĄ ZGODNIE Z ART. 2 UST. 2

WYMOGI SEKCJI III ZAŁĄCZNIKA I	PRZYKŁADY
Świadczenie usług	
a)	Brak przykładów
b)	
(i)	Dostarczanie plików elektronicznych, które mogą być odczytane przez komputer z czytnikiem ekranu, tak by osoby niewidome mogły wykorzystać te informacje.
(ii)	Stosowanie tego samego słownictwa w sposób spójny lub zgodnie z jasną i logiczną strukturą, tak by osoby z niepełnosprawnościami intelektualnymi mogły je lepiej zrozumieć.
(iii)	Uwzględnianie napisów przy wyświetlaniu wideo z instrukcjami.

(iv)	Umożliwienie osobom niewidomym korzystania z danego pliku poprzez drukowanie alfabetem Braille'a.
(v)	Zapewnienie, by tekst mogły odczytać osoby słabowidzące.
(vi)	Dołączanie do diagramu opisu tekstowego określającego jego główne elementy lub opisującego najważniejsze działania.
(vii)	Gdy dostawca usługi oferuje klucz USB zawierający informacje o danej usłudze, zapewnienie, by informacje takie miały dostępny charakter.
c)	Zapewnianie tekstowego opisu obrazów, umożliwienie uruchomienia wszystkich funkcji za pośrednictwem klawiatury, zapewnienie odpowiedniego czasu na przeczytanie, zapewnienie, by treść pojawiała się i działała w sposób przewidywalny, oraz zapewnienie kompatybilności z technologiami wspomagającymi, tak by osoby z różnymi rodzajami niepełnosprawności mogły czytać daną stronę internetową i z niej korzystać.
d)	Brak przykładów

SEKCJA IV:

PRZYKŁADY DOTYCZĄCE DODATKOWYCH WYMOGÓW DOSTĘPNOŚCI W ODNIESIENIU DO USŁUG SZCZEGÓLNYCH

WYMOGI SEKCJI IV ZAŁĄCZNIKA I	PRZYKŁADY
Usługi szczególne	
a)	
(i)	Zapewnienie, by osoba niedosłysząca mogła pisać i odczytywać tekst w sposób interaktywny i w czasie rzeczywistym.
(ii)	Zapewnienie, by osoby niesłyszące mogły stosować język migowy do komunikacji między sobą.
(iii)	Zapewnienie, by osoba z zaburzeniami mowy i słuchu, chcąca wykorzystać połączenie tekstu, głosu i wideo, wiedziała, że jej zgłoszenie jest przekazywane przez sieć do służb ratunkowych.
b)	
(i)	Umożliwienie osobie niewidomej wyboru programów telewizyjnych.
(ii)	Wspieranie możliwości wyboru, personalizacji i wyświetlania usług dostępu, takich jak napisy dla osób niesłyszących i niedosłyszących, audiodeskrypcja, napisy czytane i tłumaczenie na język migowy, poprzez zapewnienie skutecznego połączenia bezprzewodowego z technologiami wzmacniającymi słuch lub poprzez zapewnienie przełączników do aktywacji usług dostępu do audiowizualnych usług medialnych na takim samym poziomie widoczności jak w przypadku głównych przełączników sterujących danym medium.
c)	
(i)	Brak przykładów
(ii)	Brak przykładów
d)	Brak przykładów
e)	
(i)	Zapewnienie, by okna dialogowe dotyczące identyfikacji mogły być odczytywane przez czytniki ekranu, tak by mogły z nich korzystać osoby niewidome.

(ii)	Brak przykładów
f)	
(i)	Zapewnienie, by osoba z dysleksją mogła jednocześnie czytać tekst i go słuchać.
(ii)	Umożliwienie synchronizacji tekstowych i dźwiękowych danych wyjściowych lub umożliwienie dokonywania zapisu przy użyciu odświeżalnego monitora brajlowskiego.
(iii)	Zapewnienie, by osoba niewidząca mogła skorzystać ze spisu treści lub przejść do innego rozdziału.
(iv)	Brak przykładów
(v)	Zapewnienie, by informacje o ich cechach ułatwiających dostęp były możliwe do odbioru w pliku elektronicznym, tak by docierały do osób z niepełnosprawnościami.
(vi)	Zapewnienie braku blokowania, na przykład by techniczne środki ochrony, informacje o zarządzaniu prawami lub kwestie interoperacyjności nie uniemożliwiały czytania tekstu na głos przez urządzenia wspomagające, tak by osoby niewidome mogły przeczytać daną książkę.
g)	
(i)	Zapewnienie, by oferowane informacje o cechach decydujących o dostępności produktu nie były usuwane.
(ii)	Zapewnienie głosowego dostępu do interfejsu użytkownika usługi płatniczej, by osoby niewidome mogły samodzielnie dokonywać zakupów przez internet.
(iii)	Zapewnienie, by okna dialogowe dotyczące identyfikacji mogły być odczytywane przez czytniki ekranu, tak by mogły z nich korzystać osoby niewidome.

ZAŁĄCZNIK III

WYMOGI DOSTĘPNOŚCI DLA CELÓW ART. 4 UST. 4 DOTYCZĄCE ŚRODOWISKA ZBUDOWANEGO, W KTÓRYM ŚWIADCZONE SĄ USŁUGI OBJĘTE ZAKRESEM NINIEJSZEJ DYREKTYWY

Aby zmaksymalizować przewidywalne wykorzystywanie w sposób samodzielny przez osoby z niepełnosprawnościami środowiska zbudowanego, w którym świadczona jest usługa i za które odpowiedzialny jest usługodawca, o czym mowa w art. 4 ust. 4, dostępność przestrzeni przeznaczonej do publicznego dostępu musi obejmować następujące aspekty:

a) korzystanie z powiązanych obszarów i pomieszczeń znajdujących się na zewnątrz;

b) dostęp do budynków;

c) korzystanie z wejść;

d) poruszanie się w przestrzeni poziomej;

e) poruszanie się w przestrzeni pionowej;

f) publiczne korzystanie z pomieszczeń;

g) korzystanie ze sprzętu i urządzeń wykorzystywanych w świadczeniu usług;

h) korzystanie z toalet i pomieszczeń sanitarnych;

i) korzystanie z wyjść, dróg ewakuacyjnych i koncepcje dotyczące planowania działań w sytuacjach wyjątkowych;

j) komunikacja i orientacja przez więcej niż jeden kanał sensoryczny;

k) korzystanie z pomieszczeń i budynków do ich przewidywanego celu;

l) ochrona przed zagrożeniami wewnątrz i na zewnątrz budynków.

ZAŁĄCZNIK IV

PROCEDURA OCENY ZGODNOŚCI – PRODUKTY

1. Wewnętrzna kontrola produkcji

Wewnętrzna kontrola produkcji to procedura oceny zgodności, poprzez którą producent wypełnia obowiązki określone w pkt 2, 3 i 4 niniejszego załącznika oraz zapewnia i deklaruje, na swoją wyłączną odpowiedzialność, spełnienie przez dany produkt odpowiednich wymogów określonych w niniejszej dyrektywie.

2. Dokumentacja techniczna

Producent sporządza dokumentację techniczną. Dokumentacja techniczna umożliwia ocenę zgodności produktu z odpowiednimi wymogami dostępności, o których mowa w art. 4, a także – w przypadku gdy producent powołuje się na art. 14 – wykazanie, że spełnienie wymogów dostępności łączyłoby się z koniecznością wprowadzenia zasadniczej zmiany lub powodowałoby nałożenie nieproporcjonalnego obciążenia. Dokumentacja techniczna określa jedynie mające zastosowanie wymagania i obejmuje – w stopniu odpowiednim dla takiej oceny – projekt, produkcję i działanie produktu.

Dokumentacja techniczna zawiera, w stosownych przypadkach, przynajmniej następujące elementy:

a) ogólny opis produktu;

b) wykaz norm zharmonizowanych oraz specyfikacji technicznych, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, stosowanych w całości lub częściowo, oraz opisy rozwiązań przyjętych w celu spełnienia odpowiednich wymogów dostępności, o których mowa w art. 4, w przypadku gdy takie normy zharmonizowane lub specyfikacje techniczne nie zostały zastosowane; w przypadku częściowego zastosowania norm zharmonizowanych lub specyfikacji technicznych w dokumentacji technicznej określa się, które części zostały zastosowane.

3. Produkcja

Producent wprowadza wszelkie niezbędne środki, aby proces wytwórczy i jego monitorowanie zapewniały zgodność produktów z dokumentacją techniczną, o której mowa w pkt 2 niniejszego załącznika, oraz z wymogami dostępności określonymi w niniejszej dyrektywie.

4. Oznakowanie CE i deklaracja zgodności UE

4.1. Producent umieszcza oznakowanie CE, o którym mowa w niniejszej dyrektywie, na każdym egzemplarzu produktu spełniającym mające zastosowanie wymogi określone w niniejszej dyrektywie.

4.2. Producent sporządza pisemną deklarację zgodności UE dla modelu produktu. W deklaracji zgodności UE wskazuje się produkt, dla którego została ona sporządzona.

Kopia deklaracji zgodności UE zostaje udostępniona na żądanie właściwych organów.

5. Upoważniony przedstawiciel

Obowiązki producenta określone w pkt 4 mogą być, w jego imieniu i na jego odpowiedzialność, wypełniane przez upoważnionego przedstawiciela, pod warunkiem że zostały one wyszczególnione w pełnomocnictwie.

ZAŁĄCZNIK V

INFORMACJE DOTYCZĄCE USŁUG SPEŁNIAJĄCYCH WYMOGI DOSTĘPNOŚCI

1. Usługodawca uwzględnia w ogólnych zasadach i warunkach lub w równoważnym dokumencie informacje zawierające ocenę sposobu, w jaki dana usługa spełnia wymogi dostępności, o których mowa w art. 4. Informacje te opisują mające zastosowanie wymogi i obejmują – w stopniu odpowiednim dla danej oceny – projekt i warunki świadczenia danej usługi. Oprócz informacji dla konsumentów określonych w dyrektywie 2011/83/UE informacje te zawierają w stosownych przypadkach następujące elementy:

   a) ogólny opis usługi w formatach, które mają dostępny charakter;

   b) opisy i wyjaśnienia niezbędne do zrozumienia sposobu działania usługi;

   c) opis, w jaki sposób dana usługa spełnia odpowiednie wymogi dostępności określone w załączniku I.

2. Aby zapewnić zgodność z pkt 1 niniejszego załącznika, usługodawca może stosować w całości lub częściowo normy zharmonizowane oraz specyfikacje techniczne, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*.

3. Usługodawca udziela informacji wskazujących, że proces świadczenia usługi i jego monitorowanie zapewniają zgodność z pkt 1 niniejszego załącznika oraz z mającymi zastosowanie wymogami określonymi w niniejszej dyrektywie.

ZAŁĄCZNIK VI

KRYTERIA OCENY NIEPROPORCJONALNEGO OBCIĄŻENIA

Kryteria stosowane przy przeprowadzaniu i dokumentowaniu oceny:

1. Stosunek kosztów netto związanych ze spełnieniem wymogów dostępności do ogólnych kosztów (wydatków operacyjnych i kapitałowych) produkcji, dystrybucji lub przywozu produktu lub świadczenia usługi, ponoszonych przez podmioty gospodarcze.

   Elementy stosowane przy ocenie kosztów netto związanych ze spełnieniem wymogów dostępności:

   a) kryteria dotyczące jednorazowych kosztów organizacyjnych, które uwzględnia się w ocenie:

      (i) koszty dodatkowego personelu dysponującego wiedzą fachową w zakresie dostępności;

      (ii) koszty szkolenia personelu i nabywania kompetencji w zakresie dostępności;

      (iii) koszty opracowania nowych procesów w celu uwzględnienia kwestii dostępności w rozwoju produktu lub w świadczeniu usługi;

      (iv) koszty opracowania materiałów z wytycznymi dotyczącymi dostępności;

      (v) jednorazowe koszty zapoznania się z przepisami w zakresie dostępności;

   b) kryteria dotyczące bieżących kosztów produkcji i rozwoju, które uwzględnia się w ocenie:

      (i) koszty projektowania cech decydujących o dostępności produktu lub usługi;

      (ii) koszty ponoszone w procesach wytwórczych;

      (iii) koszty testowania produktu lub usługi pod kątem dostępności;

      (iv) koszty opracowania dokumentacji.

2. Szacowane koszty i korzyści dla podmiotów gospodarczych, w tym w odniesieniu do procesów wytwórczych i inwestycji, w stosunku do szacowanej korzyści dla osób z niepełnosprawnościami, z uwzględnieniem liczby przypadków i częstotliwości korzystania z konkretnego produktu lub usługi.

3. Stosunek kosztów netto związanych ze spełnieniem wymogów dostępności do przychodów netto danego podmiotu gospodarczego ze sprzedaży.

   Elementy stosowane do oceny kosztów netto związanych ze spełnieniem wymogów dostępności:

   a) kryteria dotyczące jednorazowych kosztów organizacyjnych, które uwzględnia się w ocenie:

      (i) koszty dodatkowego personelu dysponującego wiedzą fachową w zakresie dostępności;

      (ii) koszty szkolenia personelu i nabywania kompetencji w zakresie dostępności;

      (iii) koszty opracowania nowych procesów w celu uwzględnienia kwestii dostępności w rozwoju produktu lub w świadczeniu usługi;

      (iv) koszty opracowania materiałów z wytycznymi dotyczącymi dostępności;

      (v) jednorazowe koszty zapoznania się z przepisami w zakresie dostępności;

   b) kryteria dotyczące bieżących kosztów produkcji i rozwoju do uwzględnienia w ocenie:

      (i) koszty projektowania cech decydujących o dostępności produktu lub usługi;

      (ii) koszty ponoszone w procesach wytwórczych;

      (iii) koszty testowania produktu lub usługi pod kątem dostępności;

      (iv) koszty opracowania dokumentacji.

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/883

z dnia 17 kwietnia 2019 r.

w sprawie portowych urządzeń do odbioru odpadów ze statków, zmieniająca dyrektywę 2010/65/UE i uchylająca dyrektywę 2000/59/WE

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 100 ust. 2,

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) Polityka morska Unii ma na celu zapewnienie wysokiego poziomu bezpieczeństwa i ochrony środowiska. Cele te można osiągnąć przez spełnienie wymogów określonych w konwencjach, kodeksach oraz rezolucjach międzynarodowych przy jednoczesnym zachowaniu swobody żeglugi, określonej w Konwencji Narodów Zjednoczonych o prawie morza (zwanej dalej „konwencją UNCLOS").

(2) Cel zrównoważonego rozwoju nr 14 określony przez organizację Narodów Zjednoczonych zwraca uwagę na zagrożenia wynikające z zanieczyszczenia morza i zanieczyszczenia związkami biogennymi, ze zmniejszenia zasobów i zmiany klimatu, których przyczyną jest przede wszystkim działalność człowieka. Zagrożenia te dodatkowo obciążają systemy środowiskowe, takie jak różnorodność biologiczna i infrastruktura przyrodnicza, a jednocześnie powodują globalne problemy społeczno-ekonomiczne, w tym zagrożenia dla zdrowia i bezpieczeństwa oraz zagrożenia finansowe. Unia musi podejmować działania na rzecz ochrony gatunków morskich i wspierać wszystkich, których byt uzależniony jest od oceanów, pod względem zatrudnienia, zasobów czy też wypoczynku.

(3) Międzynarodowa Konwencja o zapobieganiu zanieczyszczaniu morza przez statki (zwana dalej „konwencją MARPOL") zawiera ogólny zakaz zrzutu odpadów ze statków do morza, reguluje jednak również warunki, na jakich niektóre rodzaje odpadów mogą być zrzucane ze statków do środowiska morskiego. Konwencja MARPOL zobowiązuje umawiające się strony do zapewnienia odpowiednich portowych urządzeń do odbioru odpadów.

(4) Unia wdrożyła część konwencji MARPOL za pośrednictwem dyrektywy Parlamentu Europejskiego i Rady 2000/59/WE ([4]), stosując podejście oparte na sektorze portowym. Dyrektywa 2000/59/WE ma na celu pogodzenie potrzeb niezakłóconego prowadzenia działalności w transporcie morskim z wymogami ochrony środowiska morskiego.

(5) W ciągu ostatnich dwudziestu lat konwencja MARPOL i załączniki do niej uległy istotnym zmianom, które wprowadziły surowsze normy i zakazy dotyczące zrzutów odpadów ze statków do morza.

(6) W załączniku VI do konwencji MARPOL wprowadzono normy dotyczące zrzutów ze statków w odniesieniu do nowych kategorii odpadów, w szczególności pozostałości pochodzących z systemów oczyszczania spalin, składających się ze szlamu i upuszczonej wody. Te kategorie odpadów należy włączyć do zakresu stosowania niniejszej dyrektywy.

([1]) Dz.U. C 283 z 10.8.2018, s. 61.
([2]) Dz.U. C 461 z 21.12.2018, s. 220.
([3]) Stanowisko Parlamentu Europejskiego i Rady z dnia 13 marca 2019 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 9 kwietnia 2019 r.
([4]) Dyrektywa 2000/59/WE Parlamentu Europejskiego i Rady z dnia 27 listopada 2000 r. w sprawie portowych urządzeń do odbioru odpadów wytwarzanych przez statki i pozostałości ładunku (Dz.U. L 332 z 28.12.2000, s. 81).

(7) Państwa członkowskie powinny nadal prowadzić prace na szczeblu Międzynarodowej Organizacji Morskiej (IMO) w celu wszechstronnego uwzględnienia wpływu zrzutu wody ze skruberów w układzie otwartym na środowisko, w tym środków mających zaradzić ewentualnym negatywnym skutkom.

(8) Należy zachęcać państwa członkowskie do przyjmowania stosownych środków zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2000/60/WE ([5]), w tym zakazu zrzutu wody przepłukującej ze skruberów w układzie otwartym i niektórych pozostałości ładunku na ich wodach terytorialnych.

(9) W dniu 1 marca 2018 r. IMO przyjęła zmienione skonsolidowane wytyczne dla dostawców i użytkowników portowych urządzeń do odbioru odpadów (MEPC.1/okólnik 834/Rev.1) (zwane dalej „skonsolidowanymi wytycznymi IMO"), które zawierają standardowe formaty powiadamiania o odpadach, pokwitowania odprowadzenia odpadów i zgłaszania informacji o nieprawidłowościach w zakresie portowych urządzeń do odbioru odpadów, a także wymogi w zakresie sprawozdawczości dotyczącej urządzeń do odbioru odpadów.

(10) Pomimo tych zmian w przepisach nadal dochodzi do zrzutów odpadów do morza, co powoduje znaczne koszty środowiskowe, społeczne i ekonomiczne. Wynika to z połączenia różnych czynników, a mianowicie odpowiednie portowe urządzenia do odbioru odpadów nie zawsze są dostępne w portach, egzekwowanie przepisów jest często niewystarczające i brakuje zachęt do odprowadzania odpadów na lądzie.

(11) Dyrektywa 2000/59/WE przyczyniła się do zwiększenia ilości odpadów odprowadzanych do portowych urządzeń do odbioru odpadów, między innymi poprzez zapewnienie częściowego pokrywanie kosztów tych urządzeń przez statki niezależnie od faktycznego wykorzystywania tych urządzeń, i w ten sposób walnie przyczyniła się do zmniejszenia zrzutów odpadów do morza, jak stwierdzono w ocenie tej dyrektywy przeprowadzonej w ramach programu sprawności i wydajności regulacyjnej (zwanej dalej „oceną REFIT").

(12) Ocena REFIT wykazała również, że dyrektywa 2000/59/WE nie była w pełni skuteczna ze względu na brak spójności z konwencją MARPOL. Ponadto państwa członkowskie opracowały różne interpretacje kluczowych pojęć tej dyrektywy, takich jak odpowiedniość portowych urządzeń, wcześniejsze powiadamianie o odpadach, obowiązek odprowadzania odpadów do portowych urządzeń do odbioru odpadów oraz zwolnień dla statków włączonych w ustalony harmonogram podróży. W ocenie REFIT wezwano do większej harmonizacji tych pojęć i pełnego dostosowania przepisów do konwencji MARPOL, aby uniknąć niepotrzebnych obciążeń administracyjnych zarówno dla portów, jak i użytkowników portów.

(13) Aby dostosować dyrektywę Parlamentu Europejskiego i Rady 2005/35/WE ([6]) do stosownych postanowień konwencji MARPOL odnoszących się do norm dotyczących zrzutów, Komisja powinna ocenić potrzebę przeglądu tej dyrektywy, w szczególności poprzez rozszerzenie jej zakresu stosowania.

(14) Unijna polityka morska powinna mieć na celu wysoki poziom ochrony środowiska morskiego przy uwzględnieniu różnorodności obszarów morskich w Unii. Powinna być oparta na zasadach podejmowania działania zapobiegawczego, naprawiania szkody dla środowiska morskiego w pierwszym rzędzie u źródła oraz zasadzie „zanieczyszczający płaci".

(15) Niniejsza dyrektywa powinna mieć również zasadnicze znaczenie dla stosowania podstawowych przepisów i zasad dotyczących ochrony środowiska w odniesieniu do portów i gospodarowania odpadami ze statków. W szczególności dyrektywy Parlamentu Europejskiego i Rady 2008/56/WE ([7]) oraz 2008/98/WE ([8]) stanowią odpowiednie narzędzia w tym zakresie

(16) W dyrektywie 2008/98/WE określono główne zasady gospodarowania odpadami, w tym zasadę „zanieczyszczający płaci" i hierarchię postępowania z odpadami, która określa ponowne użycie i recykling odpadów jako preferowane formy odzysku i unieszkodliwiania odpadów oraz zawiera wymóg stworzenia systemów selektywnej zbiórki odpadów. Ponadto koncepcja rozszerzonej odpowiedzialności producenta stanowi zasadę przewodnią prawodawstwa Unii dotyczącego odpadów, zgodnie z którą producenci odpowiedzialni są za wpływ swoich produktów na środowisko w całym cyklu życia tych produktów. Obowiązki te mają również zastosowanie do gospodarowania odpadami ze statków.

([5]) Dyrektywa Parlamentu Europejskiego i Rady 2000/60/WE z dnia 23 października 2000 r. ustanawiająca ramy wspólnotowego działania w dziedzinie polityki wodnej (Dz.U. L 327 z 22.12.2000, s. 1).

([6]) Dyrektywa 2005/35/WE Parlamentu Europejskiego i Rady z dnia 7 września 2005 r. w sprawie zanieczyszczeń pochodzących ze statków oraz wprowadzenia sankcji, w tym sankcji karnych, za przestępstwa związane z zanieczyszczeniami (Dz.U. L 255 z 30.9.2005, s. 11).

([7]) Dyrektywa Parlamentu Europejskiego i Rady 2008/56/WE z dnia 17 czerwca 2008 r. ustanawiająca ramy działań Wspólnoty w dziedzinie polityki środowiska morskiego (dyrektywa ramowa w sprawie strategii morskiej) (Dz.U. L 164 z 25.6.2008, s. 19).

([8]) Dyrektywa Parlamentu Europejskiego i Rady 2008/98/WE z dnia 19 listopada 2008 r. w sprawie odpadów oraz uchylająca niektóre dyrektywy (Dz.U. L 312 z 22.11.2008, s. 3).

(17) Selektywne zbieranie odpadów ze statków, w tym porzuconych narzędzi połowowych, jest konieczne, aby zapewnić ich późniejszy odzysk, umożliwić ich przygotowanie do ponownego użycia lub recyklingu w kolejnych ogniwach łańcucha gospodarowania odpadami oraz aby zapobiegać szkodom, jakie mogą wyrządzić dzikiej faunie i florze morskiej i środowisku morskiemu. Odpady są często segregowane już na statku, zgodnie z międzynarodowymi normami i standardami, a prawo Unii powinno zapewniać, aby wysiłki związane z selektywną zbiórką odpadów na statku nie zostały zniweczone przez brak uzgodnień dotyczących selektywnej zbiórki na lądzie.

(18) Każdego roku znacząca ilość tworzyw sztucznych wpada do wód mórz i oceanów w Unii. Mimo że w większości obszarów morskich większość odpadów w środowisku morskim pochodzi z działalności lądowej, ważnym czynnikiem generującym odpady jest również żegluga, w tym sektor rybołówstwa i branża rekreacyjna, ze względu na zrzuty odpadów, w tym tworzyw sztucznych i porzuconych narzędzi połowowych, które trafiają bezpośrednio do morza.

(19) Dyrektywa 2008/98/WE wzywa państwa członkowskie do zaprzestania powstrzymania wprowadzania odpadów do morza, aby przyczynić się do realizacji ustalonego przez Organizację Narodów Zjednoczonych celu zrównoważonego rozwoju polegającego na zapobieganiu zanieczyszczeniu mórz i znacznym zmniejszeniu wszelkiego rodzaju zanieczyszczeń mórz.

(20) W komunikacie Komisji z dnia 2 grudnia 2015 r. zatytułowanym „Zamknięcie obiegu – plan działania UE dotyczący gospodarki o obiegu zamkniętym" uznano szczególną rolę, jaką dyrektywa 2000/59/WE ma do odegrania w tym zakresie, zapewniając dostępność odpowiednich urządzeń do odbioru odpadów oraz odpowiedni poziom zachęt i egzekwowania wymogu odprowadzania odpadów do urządzeń na lądzie.

(21) Jednym z umiejscowionych na morzu źródeł odpadów w środowisku morskim są instalacje przybrzeżne. Z tego względu państwa członkowskie powinny w stosownych przypadkach przyjąć środki dotyczące odprowadzania odpadów z instalacji przybrzeżnych pod ich banderą lub działających na ich wodach lub w obu tych przypadkach, a także zapewnić zgodność z najostrzejszymi normami dotyczącymi zrzutów określonymi w konwencji MARPOL i mającymi zastosowanie do instalacji przybrzeżnych.

(22) Jedną z głównych źródeł zanieczyszczenia morza odpadami, w szczególności odpadami z tworzyw sztucznych, są rzeki, w tym zrzuty ze statków żeglugi śródlądowej. Statki te powinny zatem podlegać rygorystycznym normom dotyczącym zrzutów i odprowadzania odpadów. Aktualnie zasady te są określane przez właściwą komisję rzeczną. Porty śródlądowe są jednak objęte przepisami prawa Unii dotyczącymi odpadów. Aby kontynuować wysiłki prowadzące do harmonizacji ram prawnych dotyczących unijnych śródlądowych dróg wodnych, wzywa się Komisję do przeprowadzenia oceny unijnego systemu norm dotyczących zrzutów i odprowadzania odpadów ze statków śródlądowych, uwzględniając Konwencję o zbieraniu, składowaniu i odbiorze odpadów wytwarzanych podczas żeglugi po Renie i śródlądowych drogach wodnych z dnia 9 września 1996 r. (CDNI).

(23) Rozporządzenie Rady (WE) nr 1224/2009 ([9]) nakłada na unijne statki rybackie wymóg posiadania na pokładzie sprzętu do odzyskiwania utraconych narzędzi. W przypadku utracenia narzędzi kapitan statku ma podjąć próbę jak najszybszego ich odzyskania. Jeżeli utraconych narzędzi nie można odzyskać, od kapitana statku rybackiego wymaga się zgłoszenia tego w przeciągu 24 godzin organom swojego państwa członkowskiego bandery. Państwo członkowskie bandery musi następnie poinformować właściwy organ nadbrzeżnego państwa członkowskiego. Zgłoszenie obejmuje oznakę rybacką i nazwę statku rybackiego, rodzaj i położenie utraconych narzędzi połowowych oraz działania podjęte w celu ich odzyskania. Statki rybackie o długości mniejszej niż 12 metrów mogą być zwolnione z tego wymogu. Zgodnie z wnioskiem dotyczącym rozporządzenia Parlamentu Europejskiego i Rady w sprawie zmiany rozporządzenia (WE) nr 1224/2009 statek rybacki ma dokonać zgłoszenia w dzienniku elektronicznym, a od państw członkowskich wymaga się gromadzenia i zachowywania informacji o utraconych narzędziach połowowych oraz przekazywania ich Komisji na jej wniosek. W ten sam sposób również mogłyby być zgłaszane informacje o biernie poławianych odpadach gromadzone i dostępne zgodnie z niniejszą dyrektywą w pokwitowaniach odbioru odpadów.

(24) Zgodnie z Międzynarodową konwencją o kontroli i postępowaniu ze statkowymi wodami balastowymi i osadami, która została przyjęta przez IMO w dniu 13 lutego 2004 r. i weszła w życie w dniu 8 września 2017 r., wszystkie statki są zobowiązane do przestrzegania procedur dotyczących postępowania z wodami balastowymi zgodnych z normami IMO, a porty i terminale wyznaczone do czyszczenia i naprawy zbiorników balastowych muszą posiadać odpowiednie urządzenia do odbioru osadów.

([9]) Rozporządzenie Rady (WE) nr 1224/2009 z dnia 20 listopada 2009 r. ustanawiające unijny system kontroli w celu zapewnienia przestrzegania przepisów wspólnej polityki rybołówstwa, zmieniające rozporządzenia (WE) nr 847/96, (WE) nr 2371/2002, (WE) Rozporządzenie Radynr 811/2004, (WE) nr 768/2005, (WE) nr 2115/2005, (WE) nr 2166/2005, (WE) nr 388/2006, (WE) nr 509/2007, (WE) nr 676/2007, (WE) nr 1098/2007, (WE) nr 1300/2008, (WE) nr 1342/2008 i uchylające rozporządzenia (EWG) nr 2847/93, (WE) nr 1627/94 oraz (WE) nr 1966/2006 (Dz.U. L 343 z 22.12.2009, s. 1).

(25) Portowe urządzenie do odbioru odpadów uważa się za odpowiednie, jeżeli jest w stanie sprostać potrzebom statków normalnie korzystających z portu bez powodowania nieuzasadnionych opóźnień, jak również określono w skonsolidowanych wytycznych IMO oraz w wytycznych IMO dotyczących zapewnienia prawidłowego działania portowych urządzeń do odbioru odpadów (rezolucja MEPC.83(44)). Odpowiedniość odnosi się zarówno do warunków operacyjnych urządzenia w związku z potrzebami użytkowników, jak i do zarządzania środowiskowego urządzeniami zgodnie z przepisami prawa Unii dotyczącymi odpadów. W niektórych przypadkach przeprowadzenie oceny, czy dane portowe urządzenie do odbioru odpadów usytuowane poza Unią spełnia taką normę, może być trudne.

(26) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1069/2009 ([10]) wymaga, aby odpady gastronomiczne ze środków transportu międzynarodowego były spalane lub unieszkodliwiane w drodze grzebania na zatwierdzonym składowisku odpadów; dotyczy to również odpadów ze statków zawijających do portów Unii, które to odpady potencjalnie miały kontakt z produktami ubocznymi pochodzenia zwierzęcego na statku. Aby ten wymóg nie ograniczał przygotowania do ponownego użycia i recyklingu odpadów ze statków, należy podjąć starania zgodne ze skonsolidowanymi wytycznymi IMO w celu zapewnienia lepszego segregowania odpadów, tak aby unikać potencjalnego zanieczyszczenia odpadów, np. odpadów opakowaniowych.

(27) Zgodnie z rozporządzeniem (WE) nr 1069/2009 w związku z rozporządzeniem Komisji (UE) nr 142/2011 ([11]) rejsów w obrębie Unii nie uważa się za przewóz międzynarodowy i odpady gastronomiczne pochodzące z tych rejsów nie muszą być spalane. Takie rejsy w obrębie Unii są jednak uznawane za podróże międzynarodowe na mocy międzynarodowego prawa morskiego (konwencja MARPOL i Międzynarodowa konwencja o bezpieczeństwie życia na morzu SOLAS). Aby zagwarantować spójność prawa Unii, podczas określania zakresu i sposobu postępowania z odpadami gastronomicznymi z międzynarodowych środków transportu na mocy niniejszej dyrektywy w związku z rozporządzeniem (UE) nr 142/2011 należy stosować definicje z rozporządzenia (WE) nr 1069/2009.

(28) Aby zapewnić odpowiedniość portowych urządzeń do odbioru odpadów, należy opracować plan odbioru i zagospodarowania odpadów, wprowadzić go w życie i dokonać jego ponownej oceny, w oparciu o konsultacje ze wszystkimi odpowiednimi stronami. Ze względów praktycznych i organizacyjnych sąsiednie porty w tym samym regionie geograficznym mogą chcieć opracować wspólny plan, uwzględniający dostępność portowych urządzeń do odbioru odpadów w każdym z portów objętych planem, zapewniając jednocześnie wspólne ramy administracyjne.

(29) Wyzwanie może stanowić przyjęcie i monitorowanie wykonania planów odbioru i zagospodarowania odpadów w niewielkich niehandlowych portach, takich jak cumowiska i mariny, w których występuje niewielki ruch jednostek pływających, wyłącznie rekreacyjnych, lub które są eksploatowane tylko przez część roku. Odpady z tych niewielkich portów są zwykle zagospodarowywane w ramach systemu gospodarowania odpadami komunalnymi zgodnie z zasadami określonymi w dyrektywie 2008/98/WE. Aby nie obciążać nadmiernie władz lokalnych i ułatwić gospodarowanie odpadami w takich niewielkich portach, powinno wystarczyć włączenie odpadów z takich portów do strumienia odpadów komunalnych i stosowne gospodarowanie nimi, udostępnianie przez port jego użytkownikom informacji o odbiorze odpadów oraz zgłoszenie portów objętych takim wyłączeniem w systemie elektronicznym, by umożliwić minimalny poziom monitorowania.

(30) Zasadnicze znaczenie dla skutecznego rozwiązania problemu odpadów w środowisku morskim ma zapewnienie odpowiednich zachęt do odprowadzania odpadów do portowych urządzeń do odbioru odpadów, w szczególności odpadów w rozumieniu definicji zawartej w załączniku V do konwencji MARPOL (zwanych dalej „odpadami z załącznika V do konwencji MARPOL"). Można to osiągnąć przez system pokrywania kosztów wymagający zastosowania pośredniej opłaty. Taka pośrednia opłata powinna być należna niezależnie od odprowadzenia odpadów oraz dawać prawo do odprowadzenia odpadów bez żadnych dodatkowych opłat bezpośrednich. Sektor rybołówstwa i branża rekreacyjna, z uwagi na ich udział w powstawaniu odpadów w środowisku morskim, powinny również zostać objęte taką pośrednią opłatą. Jednak w przypadku, gdy statek odprowadza wyjątkowo dużą ilość odpadów z załącznika V do konwencji MARPOL, w szczególności odpadów eksploatacyjnych, przekraczającą maksymalną pojemność magazynowania przeznaczoną na odpady, określoną w standardowym formularzu wcześniejszego powiadomienia o odpadach, powinna istnieć możliwość naliczenia dodatkowej opłaty bezpośredniej w celu zapewnienia, by koszty związane z odbiorem tej wyjątkowo dużej ilości odpadów nie spowodowały nieproporcjonalnego obciążenia systemu pokrywania kosztów w danym porcie. Podobny przypadek może mieć miejsce, gdy deklarowana pojemność magazynowania przeznaczona na odpady jest nadmierna lub nieracjonalnie duża.

([10]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1069/2009 z dnia 21 października 2009 r. określające przepisy sanitarne dotyczące produktów ubocznych pochodzenia zwierzęcego, nieprzeznaczonych do spożycia przez ludzi, i uchylające rozporządzenie (WE) nr 1774/2002 (rozporządzenie o produktach ubocznych pochodzenia zwierzęcego) (Dz.U. L 300 z 14.11.2009, s. 1).

([11]) Rozporządzenie Komisji (UE) nr 142/2011 z dnia 25 lutego 2011 r. w sprawie wykonania rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1069/2009 określającego przepisy sanitarne dotyczące produktów ubocznych pochodzenia zwierzęcego, nieprzeznaczonych do spożycia przez ludzi, oraz w sprawie wykonania dyrektywy Rady 97/78/WE w odniesieniu do niektórych próbek i przedmiotów zwolnionych z kontroli weterynaryjnych na granicach w myśl tej dyrektywy (Dz.U. L 54 z 26.2.2011, s. 1).

(31) W niektórych państwach członkowskich utworzono programy zapewniające alternatywne sposoby finansowania zbierania porzuconych narzędzi połowowych i biernie poławianych odpadów oraz zarządzania nimi na lądzie, w tym programy „poławiania odpadów". Takie inicjatywy powinny być przyjmowanie z zadowoleniem, a państwa członkowskie należy zachęcać do uzupełniania systemów pokrywania kosztów ustanowionych zgodnie z niniejszą dyrektywą programami „poławiania odpadów", by pokryć koszty biernie poławianych odpadów. Te systemy pokrywania kosztów, oparte na zastosowaniu 100 % opłaty pośredniej za odpady z załącznika V do konwencji MARPOL, z wyłączeniem pozostałości ładunku, nie powinny zniechęcać społeczności związanych z danym portem rybackim do uczestnictwa w istniejących programach przekazywania biernie poławianych odpadów.

(32) Opłaty nakładane na statek powinny zostać obniżone w stosunku do statków zaprojektowanych, wyposażonych lub eksploatowanych w sposób minimalizujący odpady, zgodnie z określonymi kryteriami, które mają zostać opracowane w ramach przekazanych Komisji uprawnień wykonawczych, na podstawie wytycznych IMO dotyczących wdrożenia załącznika V do konwencji MARPOL i norm opracowanych przez Międzynarodową Organizację Normalizacyjną. Ograniczenie ilości i skuteczny recykling odpadów można osiągnąć przede wszystkim dzięki skutecznej selektywnej zbiórce odpadów na statku zgodnie z tymi wytycznymi i normami.

(33) Ze względu na rodzaj handlu obejmujący częste zawijanie do portów żegluga morska bliskiego zasięgu w obecnym systemie ponosi znaczne koszty odprowadzania odpadów do portowych urządzeń do odbioru odpadów, gdyż uiszczanie opłaty jest konieczne przy każdym wejściu do portu. Ruch nie jest zarazem wystarczająco planowy i regularny, by z tego powodu kwalifikować się do zwolnień z uiszczania opłaty i odprowadzania odpadów. Aby ograniczyć obciążenie finansowe tego sektora, pobierane powinny być obniżone opłaty od statków w zależności od rodzaju ruchu, w jakim uczestniczą.

(34) Pozostałości ładunku stanowią własność właściciela ładunku po rozładowaniu ładunku w terminalu i mogą mieć wartość ekonomiczną. Z tego powodu pozostałości ładunku nie należy uwzględniać w systemach pokrywania kosztów ani przy stosowaniu opłaty pośredniej. Koszty odprowadzenia pozostałości ładunku powinny być pokrywane przez użytkownika portowego urządzenia do odbioru odpadów, zgodnie z postanowieniami umów między zaangażowanymi stronami lub innych ustaleń lokalnych. Pozostałości ładunku obejmują także resztki oleistych lub szkodliwych ładunków ciekłych pozostałych po operacji czyszczenia, do których zastosowanie mają normy dotyczące zrzutów ze statków określone w załącznikach I i II do konwencji MARPOL i które pod pewnymi warunkami określonymi w tych załącznikach nie muszą być dostarczane do portu, by uniknąć zbędnych kosztów eksploatacji statków oraz zatorów w portach.

(35) Państwa członkowskie powinny zachęcać do odprowadzania pozostałości po myciu zbiorników zawierających substancje o dużej lepkości trwale unoszące się na wodzie, ewentualnie poprzez stosowanie odpowiednich zachęt finansowych.

(36) Zakres stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/352 ([12]) obejmuje zapewnianie portowych urządzeń do odbioru odpadów jako usługi. W rozporządzeniu tym określono zasady dotyczące przejrzystości struktur pobierania opłat mających zastosowanie do usług portowych, zasady konsultacji z użytkownikami portu i procedury rozpatrywania skarg. Niniejsza dyrektywa wykracza poza ramy przewidziane w tym rozporządzeniu, zapewniając bardziej szczegółowe wymogi dotyczące projektowania i funkcjonowania systemów pokrywania kosztów portowych urządzeń do odbioru odpadów ze statków oraz przejrzystość struktury kosztów.

(37) Poza zachęceniem do odprowadzania odpadów, skuteczne egzekwowanie obowiązku odprowadzania odpadów ma ogromne znaczenie i powinno wpisywać się w podejście oparte na analizie ryzyka, dla którego należy ustanowić unijny ukierunkowany mechanizm oparty na analizie ryzyka.

(38) Jedną z głównych przeszkód utrudniających skuteczne egzekwowanie obowiązku odprowadzania odpadów stanowi odmienna interpretacja i wdrażanie przez państwa członkowskie wyjątku opartego na dostatecznej pojemności magazynowania. Aby uniknąć sytuacji, w której zastosowanie tego wyjątku osłabiłoby główny cel niniejszej dyrektywy, należy sprecyzować powyższą kwestię, w szczególności w odniesieniu do następnego portu zawinięcia, a kwestię dostatecznej pojemności magazynowania należy ustalić w zharmonizowany sposób, w oparciu o wspólną metodykę i kryteria. W przypadkach, w których trudno jest ustalić, czy w portach poza Unią dostępne są odpowiednie portowe urządzenia do odbioru odpadów, zasadnicze znaczenie ma, aby właściwy organ szczegółowo rozważył zastosowanie wyłączenia.

([12]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/352 z dnia 15 lutego 2017 r. ustanawiające ramy w zakresie świadczenia usług portowych oraz wspólne zasady dotyczące przejrzystości finansowej portów (Dz.U. L 57 z 3.3.2017, s. 1).

(39) Istnieje potrzeba dalszej harmonizacji systemu zwolnień dla statków włączonych w ustalony harmonogram podróży, z częstymi i regularnymi zawinięciami do portów, w szczególności potrzeba wyjaśnienia stosowanych terminów i warunków regulujących te zwolnienia. Ocena REFIT i ocena skutków wykazały, że brak harmonizacji warunków i stosowania zwolnień spowodował niepotrzebne obciążenia administracyjne dla statków i portów.

(40) Monitorowanie i egzekwowanie przepisów powinno być ułatwione przez system oparty na elektronicznym raportowaniu i wymianie informacji. W tym celu istniejący system informacji i monitorowania ustanowiony dyrektywą 2000/59/WE powinien być dalej rozwijany i nadal funkcjonować w oparciu o istniejące elektroniczne systemy danych, w szczególności unijny system wymiany informacji morskiej (SafeSeaNet) utworzony dyrektywą Parlamentu Europejskiego i Rady 2002/59/WE ([13]) oraz bazę danych o inspekcji (THETIS) utworzoną dyrektywą Parlamentu Europejskiego i Rady 2009/16/WE ([14]). Taki system powinien również zawierać informacje o portowych urządzeniach do odbioru odpadów dostępnych w różnych portach.

(41) Dyrektywa Parlamentu Europejskiego i Rady 2010/65/UE ([15]) upraszcza i harmonizuje procedury administracyjne mające zastosowanie do transportu morskiego poprzez upowszechnienie przekazywania informacji drogą elektroniczną i usprawnienie formalności sprawozdawczych. W oświadczeniu z Valletty, w sprawie priorytetów w zakresie unijnej polityki transportu morskiego do 2020 r. zatwierdzonym przez Radę w konkluzjach z dnia 8 czerwca 2017 r., wezwano Komisję do zaproponowania odpowiednich działań następczych po przeglądzie tej dyrektywy. W okresie od dnia 25 października 2017 r. do dnia 18 stycznia 2018 r. Komisja przeprowadziła konsultacje społeczne dotyczące formalności sprawozdawczych dotyczących statków. W dniu 17 maja 2018 r. Komisja przedłożyła Parlamentowi Europejskiemu i Radzie wniosek dotyczący rozporządzenia ustanawiającego system europejskich morskich pojedynczych punktów kontaktowych i uchylającego dyrektywę 2010/65/UE.

(42) Konwencja MARPOL wymaga od umawiających się stron, aby aktualizowały informacje na temat swoich portowych urządzeń do odbioru odpadów i przekazywały te informacje do IMO. W tym celu IMO utworzyła bazę danych w zakresie portowych urządzeń do odbioru odpadów w ramach Światowego Zintegrowanego Systemu Informacji Żeglugowej („GISIS").

(43) W skonsolidowanych wytycznych IMO, IMO przewiduje zgłaszanie stwierdzonych nieprawidłowości w zakresie portowych urządzeń do odbioru odpadów. W ramach tej procedury statek powinien zgłaszać takie nieprawidłowości administracji państwa bandery, która z kolei powiadamia IMO oraz państwo portu, w którym nieprawidłowości wystąpiły. Państwo portu powinno przeanalizować zgłoszenie i odpowiednio się do niego ustosunkować, informując IMO i zgłaszające państwo bandery. Wpisanie informacji o stwierdzonych nieprawidłowościach bezpośrednio do systemu informacji, monitorowania i egzekwowania przepisów przewidzianego niniejszą dyrektywą umożliwiłoby dalsze przekazanie informacji do GISIS, zdejmując z państw członkowskich – jako państw bandery i portu – obowiązek zgłaszania IMO nieprawidłowości.

(44) Prace podgrupy ds. portowych urządzeń do odbioru odpadów utworzonej w ramach Europejskiego Forum Zrównoważonej Żeglugi i skupiającej szerokie grono ekspertów w zakresie zanieczyszczeń pochodzących ze statków i gospodarowania odpadami ze statków zostały zawieszone w grudniu 2017 r. ze względu na rozpoczęcie negocjacji między instytucjami. Podgrupa ta służyła Komisji cennymi wskazówkami i specjalistyczną wiedzą; byłoby zatem pożądane utworzenie podobnej grupy eksperckiej, której mandat polegałby na wymianie doświadczeń w zakresie wdrażania niniejszej dyrektywy.

(45) Ważne jest, aby wszelkie sankcje wprowadzane przez państwa członkowskie były właściwie stosowane oraz aby były one skuteczne, proporcjonalne i odstraszające.

(46) Dobre warunki pracy personelu portowego obsługującego portowe urządzenia do odbioru odpadów mają zasadnicze znaczenie dla stworzenia bezpiecznego, wydajnego i społecznie odpowiedzialnego sektora morskiego, który będzie przyciągać wykwalifikowanych pracowników i zapewni równe warunki działania w całej Europie. Początkowe i okresowe szkolenia personelu są niezbędne do zapewnienia jakości usług i ochrony pracowników. Organy portowe i zarządzające portowymi urządzeniami do odbioru odpadów powinny zapewniać, aby wszyscy pracownicy przechodzili szkolenie niezbędne do zdobycia wiedzy, która ma podstawowe znaczenie dla ich pracy, ze szczególnym naciskiem na aspekty dotyczące zdrowia i bezpieczeństwa w postępowaniu z materiałami niebezpiecznymi, oraz aby wymogi szkoleniowe były regularnie aktualizowane w celu sprostania wyzwaniom związanym z innowacjami technologicznymi.

([13]) Dyrektywa 2002/59/WE Parlamentu Europejskiego i Rady z dnia 27 czerwca 2002 r. ustanawiająca wspólnotowy system monitorowania i informacji o ruchu statków i uchylająca dyrektywę Rady 93/75/EWG (Dz.U. L 208 z 5.8.2002, s. 10).

([14]) Dyrektywa Parlamentu Europejskiego i Rady 2009/16/WE z dnia 23 kwietnia 2009 r. w sprawie kontroli przeprowadzanej przez państwo portu (Dz.U. L 131 z 28.5.2009, s. 57).

([15]) Dyrektywa Parlamentu Europejskiego i Rady 2010/65/UE z dnia 20 października 2010 r. w sprawie formalności sprawozdawczych dla statków wchodzących do lub wychodzących z portów państw członkowskich i uchylająca dyrektywę 2002/6/WE (Dz.U. L 283 z 29.10.2010, s. 1).

(47) Uprawnienia powierzone Komisji w celu wdrożenia dyrektywy 2000/59/WE należy zaktualizować zgodnie z Traktatem o funkcjonowaniu Unii Europejskiej (TFUE).

(48) Komisji należy przekazać uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w odniesieniu do wprowadzenia zmian w załącznikach do niniejszej dyrektywy oraz do aktualizacji odniesień do instrumentów międzynarodowych w zakresie niezbędnym do dostosowania ich do prawa Unii lub w celu uwzględnienia postępów na poziomie międzynarodowym, w szczególności w odniesieniu do IMO; wprowadzania zmian w załącznikach do niniejszej dyrektywy, jeżeli jest to konieczne do poprawy uzgodnień dotyczących wdrażania i monitorowania ustanowionych niniejszą dyrektywą, w szczególności w odniesieniu do skutecznego powiadamiania i odprowadzania odpadów, a także właściwego stosowania zwolnień; a także w wyjątkowych okolicznościach, w przypadku gdy jest to należycie uzasadnione odpowiednią analizą przeprowadzoną przez Komisję oraz w celu uniknięcia poważnego i niedopuszczalnego zagrożenia dla środowiska morskiego wprowadzania zmian w niniejszej dyrektywie w zakresie niezbędnym do uniknięcia takiego zagrożenia, aby zapobiec, w razie konieczności, stosowaniu zmian w tych instrumentach międzynarodowych na potrzeby niniejszej dyrektywy. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz by prowadziła te konsultacje zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa ([16]). W szczególności, aby zapewnić udział Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych na równych zasadach, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(49) W celu określenia metod obliczania dostatecznej pojemności magazynowania przeznaczonej na odpady; w celu opracowania wspólnych kryteriów uznawania projektu, wyposażenia i eksploatacji statku, które wykazują, że na statku powstaje zmniejszona ilość odpadów, a odpadami gospodaruje się w sposób zrównoważony i przyjazny dla środowiska, na potrzeby przyznania statkom obniżonej opłaty za odpady; w celu określenia metodologii gromadzenia danych dotyczących objętości i ilości biernie poławianych odpadów oraz formatu sprawozdań; w celu określenia szczegółowych elementów unijnego ukierunkowanego mechanizmu opartego na analizie ryzyka, należy przyznać Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([17]).

(50) Z uwagi na fakt, że cel niniejszej dyrektywy, jakim jest ochrona środowiska morskiego przed zrzutami odpadów do morza, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, a ze względu na skalę działania możliwe jest lepsze jego osiągnięcie na poziomie Unii, Unia może podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(51) Unia charakteryzuje się regionalnymi różnicami na poziomie portów, co wykazano również w ocenie oddziaływania terytorialnego przeprowadzonej przez Komisję. Porty różnią się od siebie w zależności od położenia geograficznego, wielkości, struktury administracyjnej oraz struktury ich własności oraz charakteryzują się rodzajem statków, które zwykle wpływają do danych portów. Ponadto systemy gospodarowania odpadami odzwierciedlają różnice na szczeblu lokalnym i infrastrukturę gospodarowania odpadami niższego szczebla.

(52) Art. 349 TFUE wymaga uwzględnienia szczególnych cech charakterystycznych regionów najbardziej oddalonych Unii, a mianowicie Gwadelupy, Gujany Francuskiej, Martyniki, Majotty, Reunionu, Saint-Martin, Azorów, Madery i Wysp Kanaryjskich. Aby zapewnić odpowiedniość i dostępność portowych urządzeń do odbioru odpadów, wskazane może być udostępnienie przez państwa członkowskie operatorom portowych urządzeń do odbioru odpadów lub organom portowym w tych regionach Unii regionalnej pomocy operacyjnej w celu skompensowania wpływu stałych utrudnień, o których mowa w art. 349 TFUE. Regionalna pomoc operacyjna udostępniona przez państwa członkowskie podlega zwolnieniu z obowiązku notyfikacji określonego w art. 108 ust. 3 TFUE, jeżeli w momencie jej udzielenia spełnia ona warunki określone w rozporządzeniu Komisji (UE) nr 651/2014 ([18]) przyjętym na mocy rozporządzenia Rady (WE) nr 994/98 ([19]).

(53) W związku z powyższym należy uchylić dyrektywę 2000/59/WE,

([16]) Dz.U. L 123 z 12.5.2016, s. 1.

([17]) 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).

([18]) Rozporządzenie Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznające niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz.U. L 187 z 26.6.2014, s. 1).

([19]) Rozporządzenie Rady (WE) nr 994/98 z dnia 7 maja 1998 r. dotyczące stosowania art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej do niektórych kategorii horyzontalnej pomocy państwa (Dz.U. L 142 z 14.5.1998, s. 1).

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

Sekcja 1

Przepisy ogólne

Artykuł 1

Przedmiot

Niniejsza dyrektywa ma na celu ochronę środowiska morskiego przed negatywnymi skutkami zrzutów odpadów ze statków korzystających z portów znajdujących się na terenie Unii, przy jednoczesnym zapewnieniu niezakłóconego prowadzenia działalności w transporcie morskim, poprzez poprawę dostępności i wykorzystania odpowiednich portowych urządzeń do odbioru odpadów oraz odprowadzanie odpadów do tych urządzeń.

Artykuł 2

Definicje

Na użytek niniejszej dyrektywy stosuje się następujące definicje:

1) „statek" oznacza jakiegokolwiek typu jednostkę używaną w środowisku morskim, w tym statki rybackie, rekreacyjne jednostki pływające, wodoloty, poduszkowce, statki podwodne i urządzenia pływające;

2) „konwencja MARPOL" oznacza Międzynarodową konwencję o zapobieganiu zanieczyszczaniu morza przez statki, w aktualnej wersji;

3) „odpady ze statków" oznaczają wszelkie odpady, włączając w to pozostałości ładunku, które wytwarzane są podczas użytkowania statku lub załadunku i rozładunku oraz czyszczenia, i które objęte są zakresem stosowania załączników I, II, IV, V i VI do konwencji MARPOL, a także biernie poławiane odpady;

4) „biernie poławiane odpady" oznaczają odpady zebrane w sieci podczas operacji połowowych;

5) „pozostałości ładunku" oznaczają pozostałości jakichkolwiek ładunków na pokładzie lub w ładowniach czy zbiornikach, które pozostają po zakończonych operacjach załadunku i rozładunku, wraz z nadwyżkami po ładowaniu i rozładowaniu oraz resztkami, zarówno w stanie mokrym, jak i suchym, lub zawiesiny w wodzie przepłukującej, z wyłączeniem pyłu ładunku pozostającego na pokładzie po zamiataniu oraz pyłów na powierzchniach zewnętrznych statku;

6) „portowe urządzenie do odbioru odpadów" oznacza dowolne stałe, pływające lub ruchome urządzenie zdolne do świadczenia usługi odbioru odpadów ze statków;

7) „statek rybacki" oznacza jakikolwiek statek wyposażony lub wykorzystywany komercyjnie do połowu ryb lub innych żywych zasobów morza;

8) „rekreacyjna jednostka pływająca" oznacza jakiegokolwiek typu statek, o długości kadłuba wynoszącej 2,5 m lub większej, bez względu na jego napęd, wykorzystywany w celach sportowych lub rekreacyjnych i niewykorzystywany w handlu;

9) „port" oznacza miejsce lub obszar geograficzny uzbrojony w udogodnienia i urządzenia przeznaczone przede wszystkim do przyjmowania statków, w tym obszar kotwicowiska podlegający jurysdykcji portu;

10) „dostateczna pojemność magazynowania" oznacza wystarczającą ilość miejsca do przechowywania odpadów na statku od momentu wypłynięcia z portu do zawinięcia do następnego portu, z uwzględnieniem odpadów, które prawdopodobnie zostaną wytworzone podczas rejsu;

11) „ustalony harmonogram podróży" oznacza ruch oparty o opublikowany lub planowany rozkład wypłynięć i wpłynięć do określonych portów lub powtarzające się odcinki podróży pozwalające rozpoznać ich cykliczny charakter;

12) „regularne zawinięcia do portów" oznaczają powtarzające się podróże tego samego statku, tworzące stały wzór pomiędzy określonymi portami lub serię rejsów z i do tego samego portu bez pośrednich zawinięć;

13) „częste zawinięcia do portów" oznaczają wizyty statku w tym samym porcie co najmniej raz na dwa tygodnie;

14) „GISIS" oznacza Światowy Zintegrowany System Informacji Żeglugowej ustanowiony przez IMO;

15) „przetwarzanie" oznacza procesy odzysku lub unieszkodliwiania, w tym przygotowanie poprzedzające odzysk lub unieszkodliwianie;

16) „opłata pośrednia" oznacza opłatę za świadczenie usług portowych w zakresie urządzeń do odbioru odpadów, niezależnie od faktycznego odprowadzania odpadów ze statków.

„Odpady ze statków", o których mowa w pkt 3, uważa się za odpady w rozumieniu art. 3 pkt 1 dyrektywy 2008/98/WE.

Artykuł 3

Zakres stosowania

1. Niniejsza dyrektywa ma zastosowanie do:

a) wszystkich statków, bez względu na banderę, pod jaką pływają, wpływających lub eksploatowanych w porcie państwa członkowskiego, z wyjątkiem statków uczestniczących w usługach portowych w rozumieniu art. 1 ust. 2 rozporządzenia (UE) 2017/352, i z wyjątkiem wszelkich okrętów wojennych, okrętów pomocniczych marynarki wojennej lub innych statków pozostających własnością państwa lub przez nie chwilowo wykorzystywanych jedynie w rządowej służbie niehandlowej;

b) wszystkich portów państw członkowskich zwykle przyjmujących statki objęte zakresem stosowania lit. a).

Na potrzeby niniejszej dyrektywy i aby nie powodować nieuzasadnionych opóźnień statków, państwa członkowskie mogą zadecydować o wyłączeniu obszaru kotwicowisk ze swoich portów na potrzeby stosowania art. 6, 7 i 8.

2. Państwa członkowskie podejmują środki w celu zapewnienia, na ile to możliwe, aby statki, które nie są objęte zakresem stosowania niniejszej dyrektywy, odprowadzały odpady w sposób zgodny z niniejszą dyrektywą.

3. Państwa członkowskie, które nie mają portów ani statków pływających pod ich banderą, objętych zakresem stosowania niniejszej dyrektywy, mogą, z wyjątkiem zobowiązania określonego w akapicie trzecim niniejszego ustępu, odstąpić od stosowania przepisów niniejszej dyrektywy.

Państwa członkowskie, które nie mają portów objętych zakresem stosowania niniejszej dyrektywy, mogą zastosować odstępstwo od tych przepisów niniejszej dyrektywy, które odnoszą się wyłącznie do portów.

Te państwa członkowskie, które zamierzają skorzystać z odstępstw określonych w niniejszym ustępie, powiadamiają Komisję do dnia 28 czerwca 2021 r., czy odpowiednie warunki są spełnione, a następnie corocznie informują Komisję o wszelkich późniejszych zmianach. Dopóki te państwa członkowskie nie transponują i nie wdrożą niniejszej dyrektywy, nie mogą posiadać portów objętych zakresem stosowania niniejszej dyrektywy ani nie mogą zezwalać statkom, w tym jednostkom objętym zakresem stosowania niniejszej dyrektywy na podnoszenie ich bandery.

Sekcja 2

Zapewnienie odpowiednich portowych urządzeń do odbioru odpadów

Artykuł 4

Portowe urządzenia do odbioru odpadów

1. Państwa członkowskie zapewniają dostępność portowych urządzeń do odbioru odpadów odpowiednich do zaspokojenia potrzeb statków zwykle korzystających z portu bez powodowania nieuzasadnionych opóźnień dla statków.

2. Państwa członkowskie zapewniają, aby:

a) portowe urządzenia do odbioru odpadów były w stanie odebrać rodzaje oraz ilości odpadów ze statków zwykle korzystających z portu biorąc pod uwagę:

(i) potrzeby operacyjne użytkowników portu;

(ii) wielkość oraz położenie geograficzne portu;

(iii) rodzaj statków zawijających do portu; oraz

(iv) zwolnienia przewidziane w art. 9;

b) formalności i rozwiązania praktyczne związane z korzystaniem z portowych urządzeń do odbioru odpadów były proste i szybkie, tak by nie powodowały nieuzasadnionych opóźnień dla statków;

c) opłaty pobierane za odprowadzanie odpadów nie zniechęcały statków do korzystania z tych urządzeń; oraz

d) portowe urządzenia do odbioru odpadów umożliwiały gospodarowanie odpadami ze statków w sposób bezpieczny dla środowiska zgodnie z dyrektywą 2008/98/WE i innymi stosownymi przepisami prawa Unii i prawa krajowego dotyczącymi odpadów.

Na użytek akapitu pierwszego lit. d) państwa członkowskie zapewniają selektywną zbiórkę, by ułatwić ponowne użycie i recykling odpadów ze statków w portach zgodnie z wymogami przepisów prawa Unii dotyczących odpadów, w szczególności zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2006/66/WE ([20]), dyrektywą 2008/98/WE oraz dyrektywą Parlamentu Europejskiego i Rady 2012/19/UE ([21]). Aby ułatwić ten proces, portowe urządzenia do odbioru odpadów mogą odbierać odrębne frakcje odpadów zgodnie z kategoriami odpadów określonymi w konwencji MARPOL, z uwzględnieniem zawartych w niej wytycznych.

Akapit pierwszy lit. d) ma zastosowanie bez uszczerbku dla bardziej rygorystycznych wymogów nałożonych rozporządzeniem (WE) nr 1069/2009 w zakresie gospodarowania odpadami gastronomicznymi z międzynarodowych środków transportu.

3. Państwa członkowskie, działając w charakterze państw bandery, stosują formularze i procedury określone przez IMO w celu powiadamiania IMO oraz organów państwa portu oraz zgłaszania nieprawidłowości w zakresie portowych urządzeń do odbioru odpadów.

Państwa członkowskie, działając w charakterze państw portu, analizują wszystkie zgłoszone przypadki stwierdzonych nieprawidłowości i stosują formularze oraz procedury określone przez IMO w celu informowania IMO oraz zgłaszającego państwa bandery o wynikach analiz.

4. Właściwe władze portowe lub – w przypadku ich braku – inne odpowiednie organy zapewniają, by odprowadzanie i odbiór odpadów odbywały się z zachowaniem dostatecznych środków ostrożności, aby uniknąć potencjalnego zagrożenia dla człowieka i środowiska w portach objętych niniejszą dyrektywą.

5. Państwa członkowskie zapewniają, aby każda strona zaangażowana w odprowadzanie lub odbiór odpadów ze statków mogła domagać się odszkodowania za szkodę powstałą wskutek nieuzasadnionego opóźnienia.

([20]) Dyrektywa 2006/66/WE Parlamentu Europejskiego i Rady z dnia 6 września 2006 r. w sprawie baterii i akumulatorów oraz zużytych baterii i akumulatorów oraz uchylająca dyrektywę 91/157/EWG (Tekst mający znaczenie dla EOG) (Dz.U. L 266 z 26.9.2006, s. 1).

([21]) Dyrektywa Parlamentu Europejskiego i Rady 2012/19/UE z dnia 4 lipca 2012 r. w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE) (Dz.U. L 197 z 24.7.2012, s. 38).

Artykuł 5

Plany odbioru i zagospodarowania odpadów

1. Państwa członkowskie zapewniają, by w każdym porcie został wdrożony odpowiedni plan odbioru i zagospodarowania odpadów opracowany po przeprowadzeniu konsultacji z odpowiednimi stronami, w tym w szczególności z użytkownikami portu lub ich przedstawicielami, oraz, w stosownych przypadkach, właściwymi organami lokalnymi, operatorami portowych urządzeń do odbioru odpadów, z organizacjami realizującymi obowiązki wynikające z rozszerzonej odpowiedzialności producenta oraz z przedstawicielami społeczeństwa obywatelskiego. Konsultacje te powinny odbywać się zarówno podczas wstępnego opracowywania planu odbioru i zagospodarowania odpadów, jak i po jego przyjęciu, w szczególności gdy wprowadzono znaczące zmiany, w odniesieniu do wymogów zawartych w art. 4, 6 i 7.

Szczegółowe wymogi dotyczące przygotowania planu odbioru i zagospodarowania odpadów określone są w załączniku 1.

2. Państwa członkowskie zapewniają, aby następujące informacje zawarte w planie odbioru i zagospodarowania odpadów, dotyczące dostępności odpowiednich portowych urządzeń do odbioru odpadów w ich portach oraz struktury kosztów, były jednoznacznie przekazywane operatorom statków, podawane do wiadomości publicznej oraz były łatwo dostępne w języku urzędowym państwa członkowskiego, w którym znajduje się port, oraz – w stosownych przypadkach – w języku wykorzystywanym w kontaktach międzynarodowych:

a) lokalizacja portowych urządzeń do odbioru odpadów odpowiednio dla każdego miejsca postoju, oraz – w stosownych przypadkach – ich godziny otwarcia;

b) wykaz odpadów ze statków normalnie zarządzanych przez port;

c) wykaz punktów kontaktowych, operatorów portowych urządzeń do odbioru odpadów i oferowanych usług;

d) opis procedur dotyczących odprowadzania odpadów;

e) opis systemów pokrywania kosztów, w tym – w stosownych przypadkach – programów gospodarowania odpadami oraz finansowania, o których mowa w załączniku 4.

Informacje, o których mowa w akapicie pierwszym niniejszego ustępu, są również udostępniane i aktualizowane drogą elektroniczną w części systemu informacji, monitorowania i egzekwowania przepisów, o którym mowa w art. 13.

3. Tam gdzie to konieczne ze względu na efektywność, plany odbioru i zagospodarowania odpadów mogą być przygotowywane wspólnie przez dwa lub kilka sąsiednich portów w tym samym regionie geograficznym, przy odpowiednim zaangażowaniu każdego z portów, pod warunkiem że potrzeby oraz dostępność portowych urządzeń do odbioru odpadów określane są oddzielnie dla każdego portu.

4. Państwa członkowskie oceniają oraz zatwierdzają plan odbioru i zagospodarowania odpadów, a także zapewniają jego ponowne zatwierdzanie nie rzadziej niż raz na pięć lat po jego zatwierdzeniu lub ponownym zatwierdzeniu oraz po każdorazowym wprowadzeniu znaczących zmian w funkcjonowaniu portu. Zmiany te mogą obejmować zmiany strukturalne w ruchu do portu, rozwój nowej infrastruktury, zmiany popytu i zapewnienia portowych urządzeń do odbioru odpadów oraz nowe technologie obróbki na statku.

Państwa członkowskie monitorują wdrażanie przez port planu odbioru i zagospodarowania odpadów. Jeżeli w pięcioletnim okresie, o którym mowa w akapicie pierwszym, nie zaszły istotne zmiany, ponowne zatwierdzenie może polegać na walidacji istniejących planów.

5. Małe porty niehandlowe o nieczęstym lub niewielkim ruchu wyłącznie rekreacyjnych jednostek pływających mogą zostać wyłączone ze stosowania ust. 1–4, jeżeli posiadane przez nie portowe urządzenia do odbioru odpadów są zintegrowane z systemem gospodarowania odpadami zarządzanym przez odpowiednią gminę lub w jej imieniu, a państwa członkowskie, na których terytorium znajdują się te porty, zapewniają, by informacje dotyczące systemu gospodarowania odpadami były udostępniane użytkownikom tych portów.

Państwa członkowskie, na których terytorium znajdują się takie porty, przekazują informację o ich nazwach i lokalizacji drogą elektroniczną do części systemu informacji, monitorowania i egzekwowania przepisów, o którym mowa w art. 13.

Sekcja 3

Odprowadzanie odpadów ze statków

Artykuł 6

Wcześniejsze powiadomienie o odpadach

1. Operator, agent lub kapitan statku objętego zakresem stosowania dyrektywy 2002/59/WE, który zmierza do portu w Unii, wypełnia zgodnie z prawdą i dokładnie formularz określony w załączniku 2 do niniejszej dyrektywy (zwane dalej „wcześniejszym powiadomieniem o odpadach") i przekazuje wszystkie informacje w nim zawarte organowi lub podmiotowi wyznaczonemu do tego celu przez państwo członkowskie, w którym znajduje się ten port:

a) co najmniej 24 godziny przed przybyciem, jeśli port zawinięcia jest znany;

b) gdy tylko będzie znany port zawinięcia, jeśli ta informacja jest dostępna w okresie krótszym niż 24 godziny przed przybyciem do portu; lub

c) najpóźniej w momencie wyjścia z poprzedniego portu, jeśli czas podróży jest krótszy niż 24 godziny.

2. Informacje zawarte we wcześniejszym powiadomieniu o odpadach są przekazywane drogą elektroniczną do części systemu informacji, monitorowania i egzekwowania przepisów, o którym mowa w art. 13 niniejszej dyrektywy, zgodnie z dyrektywami 2002/59/WE i 2010/65/UE.

3. Informacje zawarte we wcześniejszym powiadomieniu o odpadach muszą być dostępne na statku, najlepiej w formie elektronicznej, co najmniej do czasu zawinięcia do następnego portu oraz są udostępniane na żądanie właściwym organom państw członkowskich.

4. Państwa członkowskie zapewniają, aby informacje przekazywane zgodnie z niniejszym artykułem były analizowane i bezzwłocznie udostępniane właściwym organom odpowiedzialnym za egzekwowanie przepisów.

Artykuł 7

Odprowadzanie odpadów ze statków

1. Kapitan statku zawijającego do portu Unii przed opuszczeniem tego portu odprowadza wszelkie odpady znajdujące się na statku do portowego urządzenia do odbioru odpadów zgodnie z odpowiednimi normami dotyczącymi zrzutów określonymi w konwencji MARPOL.

2. Po odprowadzeniu odpadów operator portowego urządzenia do odbioru odpadów lub władze portu, w którym odpady zostały odprowadzone, zgodnie z prawdą i dokładnie wypełniają formularz określony w załączniku 3 (zwany dalej „pokwitowaniem odbioru odpadów") i niezwłocznie wydają i przekazują pokwitowanie odbioru odpadów kapitanowi statku.

Wymogi określone w akapicie pierwszym nie mają zastosowania w przypadku małych portów o bezzałogowych urządzeniach lub portów znajdujących się w odległych miejscach, pod warunkiem że państwo członkowskie, w którym znajdują się takie porty, poinformowało o nazwach i lokalizacji tych portów drogą elektroniczną w części systemu informacji, monitorowania i egzekwowania przepisów, o którym mowa w art. 13.

3. Operator, agent lub kapitan statku objętego zakresem stosowania dyrektywy 2002/59/WE przed wypłynięciem z portu lub niezwłocznie po otrzymaniu pokwitowania odbioru odpadów przesyła drogą elektroniczną zawarte w nim informacje do części systemu informacji, monitorowania i egzekwowania przepisów, o którym mowa w art. 13 niniejszej dyrektywy, zgodnie z dyrektywami 2002/59/WE i 2010/65/UE.

Informacje zawarte w pokwitowaniu odbioru odpadów muszą być dostępne na statku przez co najmniej dwa lata, w stosownych przypadkach z odpowiednią książką zapisów olejowych, książką zapisów ładunkowych, książką zapisów o postępowaniu z odpadami lub planem postępowania z odpadami oraz są udostępniane na żądanie właściwym organom państw członkowskich.

4. Bez uszczerbku dla ust. 1, statek może udać się do następnego portu zawinięcia bez odprowadzenia odpadów, jeżeli:

a) informacje przekazane zgodnie z załącznikami 2 i 3 wskazują, że istnieje dostateczna pojemność magazynowania przeznaczona na wszystkie odpady, które zostały zgromadzone i które powstaną podczas planowanego rejsu statku do następnego portu zawinięcia;

b) informacje dostępne na pokładzie statków, które nie są objęte zakresem stosowania dyrektywy 2002/59/WE, wskazują, że istnieje dostateczna pojemność magazynowania przeznaczona na wszystkie odpady, które zostały zgromadzone i które powstaną podczas planowanego rejsu statku do następnego portu zawinięcia; lub

c) statek zawija na kotwicowisko jedynie na czas krótszy niż 24 godziny lub w niesprzyjających warunkach pogodowych, chyba że obszar ten został wyłączony zgodnie z art. 3 ust. 1 akapit drugi.

Aby zapewnić jednolite warunki stosowania wyłączenia, o którym mowa w pierwszym akapicie lit a) i b), Komisja przyjmuje akty wykonawcze w celu określenia metod, które należy stosować do obliczania dostatecznej pojemności magazynowania. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 20 ust. 2.

5. Państwo członkowskie wymaga, aby statek odprowadził wszystkie swoje odpady przed wypłynięciem z portu, jeżeli:

a) na podstawie dostępnych informacji, w tym informacji dostępnych drogą elektroniczną w części systemu informacji, monitorowania i egzekwowania przepisów, o którym mowa w art. 13, lub w GISIS, nie można ustalić, czy w następnym porcie zawinięcia są dostępne odpowiednie portowe urządzenia do odbioru odpadów; lub

b) następny port zawinięcia jest nieznany.

6. Ust. 4 stosuje się bez uszczerbku dla bardziej rygorystycznych wymogów dla statków, przyjętych zgodnie z prawem międzynarodowym.

Artykuł 8

Systemy pokrywania kosztów

1. Państwa członkowskie zapewniają pokrycie kosztów funkcjonowania portowych urządzeń do odbioru i przetwarzania odpadów ze statków, innych niż pozostałości ładunku, poprzez pobieranie opłat od statków. Koszty te obejmują elementy wymienione w załączniku 4.

2. Systemy pokrywania kosztów nie mogą tworzyć zachęt dla statków do dokonywania zrzutów odpadów do morza. W tym celu państwa członkowskie przy projektowaniu i wdrażaniu systemów pokrywania kosztów stosują wszystkie poniższe zasady:

a) statki uiszczają opłatę pośrednią, niezależnie od odprowadzenia odpadów do portowego urządzenia do odbioru odpadów;

b) opłata pośrednia obejmuje:

   (i) pośrednie koszty administracyjne;

   (ii) znaczną część bezpośrednich kosztów operacyjnych wskazanych w załączniku 4, która stanowi co najmniej 30 % całkowitych bezpośrednich kosztów rzeczywistego odprowadzania odpadów w roku poprzedzającym, z możliwością uwzględnienia również kosztów związanych z przewidywanym natężeniem ruchu w roku następnym;

c) w celu zapewnienia maksymalnej zachęty dla statków do odprowadzania odpadów z załącznika V do konwencji MARPOL, innych niż pozostałości ładunku, za takie odpady nie pobiera się opłaty bezpośredniej, aby zapewnić prawo do odprowadzenia bez żadnych dodatkowych opłat uzależnionych od ilości odpadów, z wyjątkiem przypadków, w których ilość odprowadzonych odpadów przekracza maksymalną pojemność magazynowania, o której mowa w formularzu zawartym w załączniku 2 do niniejszej dyrektywy; system ten obejmuje również biernie poławiane odpady, w tym prawo do ich odprowadzenia;

d) aby uniknąć sytuacji, w której koszty odbierania i przetwarzania biernie poławianych odpadów są ponoszone wyłącznie przez użytkowników portów, państwa członkowskie pokrywają te koszty – w stosownych przypadkach – z przychodów pochodzących z alternatywnych systemów finansowania, w tym z programów gospodarowania odpadami oraz z dostępnego finansowania unijnego, krajowego lub regionalnego;

e) aby zachęcić do odprowadzania pozostałości po myciu zbiorników zawierających substancje o dużej lepkości trwale unoszące się na wodzie, państwa członkowskie mogą przewidzieć odpowiednie zachęty finansowe do ich odprowadzania;

f) opłata pośrednia nie obejmuje odpadów pochodzących z systemów oczyszczania gazów spalinowych, których koszty są pokrywane na podstawie rodzajów i ilości odprowadzonych odpadów.

3. Część kosztów nieobjętych pośrednią opłatą, jeśli takie występują, pokrywana jest na podstawie rodzajów oraz ilości odpadów faktycznie odprowadzonych przez statek.

4. Opłaty mogą być zróżnicowane na podstawie:

a) kategorii, rodzaju i wielkości statku;

b) świadczenia usług na rzecz statków poza normalnymi godzinami pracy w porcie; lub

c) niebezpiecznego charakteru odpadów.

5. Opłaty obniża się na następującej podstawie:

a) rodzaj handlu, w który statek jest zaangażowany, w szczególności gdy zaangażowany jest w żeglugę morską bliskiego zasięgu;

b) projekt, wyposażenie i działalność statku, które wykazują, że na statku powstaje zmniejszona ilość odpadów, a odpadami gospodaruje się w sposób zrównoważony i bezpieczny dla środowiska.

Do dnia 28 czerwca 2020 r. Komisja przyjmie akty wykonawcze w celu określenia kryteriów wskazujących, że dany statek spełnia wymogi określone w akapicie pierwszym lit. b) w odniesieniu do gospodarowania odpadami na statku. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 20 ust. 2.

6. W celu zapewnienia, że opłaty są sprawiedliwe, przejrzyste, łatwe do zidentyfikowania, niedyskryminujące oraz odzwierciedlają koszty urządzeń oraz dostępnych usług i, w stosownych przypadkach, wykorzystywanych, wysokość opłat oraz podstawy ich wyliczania należy udostępnić w języku urzędowym państwa członkowskiego, w którym znajduje się port, oraz – w stosownych przypadkach – w języku wykorzystywanym w kontaktach międzynarodowych użytkownikom portu w planie odbioru i zagospodarowania odpadów.

7. Państwa członkowskie zapewniają gromadzenie danych dotyczących objętości i ilości biernie poławianych odpadów oraz przekazują te dane Komisji. Komisja, na podstawie tych danych publikuje sprawozdanie do dnia 31 grudnia 2022 r., a następnie co dwa lata.

Komisja przyjmuje akty wykonawcze w celu określenia metod gromadzenia danych oraz formatu raportowania. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 20 ust. 2.

Artykuł 9

Zwolnienia

1. Państwa członkowskie mogą zwolnić statek zawijający do ich portu z obowiązków określonych w art. 6, art. 7 ust. 1 i art. 8 („zwolnienie"), jeżeli istnieją wystarczające dowody na to, że spełniono następujące warunki:

a) statek włączony jest w ustalony harmonogram podróży, z częstymi i regularnymi zawinięciami do portów;

b) istnieje uzgodnienie zapewniające odprowadzanie odpadów i uiszczanie opłat w porcie wzdłuż trasy statku, które:

(i) jest potwierdzone podpisaną umową z portem lub odbiorcą odpadów oraz pokwitowaniami odbioru odpadów;

(ii) o tym uzgodnieniu poinformowano wszystkie porty położone na trasie statku; oraz

(iii) zostało ono zaakceptowane przez port, gdzie następuje odprowadzenie i uiszczenie opłaty, co może mieć miejsce w porcie Unii lub w innym porcie, w którym dostępne są odpowiednie portowe urządzenia do odbioru odpadów, co ustalono na podstawie informacji przekazanych drogą elektroniczną do części systemu informacji, monitorowania i egzekwowania przepisów, o którym mowa w art. 13, i w GISIS;

c) zwolnienie nie powoduje negatywnego wpływu na bezpieczeństwo morskie, zdrowie, warunki życia lub warunki pracy na statku ani na środowisko morskie.

2. W przypadku przyznania zwolnienia państwo członkowskie, na obszarze którego położony jest port, wystawia świadectwo zwolnienia zgodnie z wzorem określonym w załączniku 5, potwierdzające, że statek spełnia niezbędne warunki i wymogi dotyczące stosowania zwolnień i wskazujące czas obowiązywania zwolnienia.

3. Państwa członkowskie przekazują informacje zawarte w świadectwie zwolnienia drogą elektroniczną do części systemu informacji, monitorowania i egzekwowania przepisów, o którym mowa w art. 13.

4. Państwa członkowskie zapewniają skuteczne monitorowanie i egzekwowanie uzgodnień dotyczących odprowadzania odpadów i płatności obowiązujących statki, którym przyznano zwolnienie, odwiedzające ich porty.

5. Niezależnie od przyznanego zwolnienia statek nie może udać się do następnego portu zawinięcia, jeżeli nie ma dostatecznej pojemności magazynowania przeznaczonej na wszystkie odpady, które zostały zgromadzone i które powstaną podczas planowanego rejsu statku do następnego portu zawinięcia.

Sekcja 4

Egzekwowanie

Artykuł 10

Inspekcje

Państwa członkowskie zapewniają, aby inspekcjom, w tym inspekcjom wyrywkowym mógł zostać poddany każdy statek, w celu sprawdzenia zgodności z niniejszą dyrektywą.

Artykuł 11

Zobowiązania inspekcyjne

1. Każde państwo członkowskie przeprowadza inspekcje statków zawijających do jego portów w liczbie odpowiadającej co najmniej 15 % ogólnej liczby pojedynczych statków zawijających rocznie do jego portów.

Ogólną liczbę pojedynczych statków zawijających do portów danego państwa członkowskiego oblicza się jako średnią liczbę pojedynczych statków w trzech poprzednich latach, zgodnie z danymi wprowadzonymi do części systemu informacji, monitorowania i egzekwowania przepisów, o którym mowa w art. 13.

2. Państwa członkowskie realizują wymóg określony w ust. 1 niniejszego artykułu wybierając statki na podstawie unijnego ukierunkowanego mechanizmu opartego na analizie ryzyka.

Aby zapewnić harmonizację inspekcji i jednolite warunki wyboru statków do inspekcji, Komisja przyjmuje akty wykonawcze w celu określenia szczegółowych elementów unijnego ukierunkowanego mechanizmu opartego na analizie ryzyka. Te akty wykonawcze przyjmowane są zgodnie z procedurą sprawdzającą, o której mowa w art. 20 ust. 2.

3. Państwa członkowskie ustanawiają procedury dotyczące inspekcji statków, które nie są objęte zakresem dyrektywy 2002/59/WE, aby zapewnić, w miarę możliwości, zgodność z przepisami niniejszej dyrektywy.

Ustanawiając te procedury, państwa członkowskie mogą uwzględnić unijny ukierunkowany mechanizm oparty na analizie ryzyka, o którym mowa w ustępie 2.

4. Jeżeli odpowiedni organ państwa członkowskiego nie jest usatysfakcjonowany wynikami inspekcji, to bez uszczerbku dla zastosowania sankcji, o których mowa w art. 16, zapewnia, aby statek nie opuścił portu, dopóki nie odprowadzi odpadów do portowego urządzenia do odbioru odpadów, zgodnie z art. 7.

Artykuł 12

System informowania, monitorowania i egzekwowania przepisów

Wdrażanie i egzekwowanie przepisów niniejszej dyrektywy ułatwi system elektronicznego raportowania i wymiany informacji pomiędzy państwami członkowskimi zgodnie z art. 13 i 14.

Artykuł 13

Raportowanie i wymiana informacji

1. Raportowanie i wymiana informacji powinny być oparte na unijnym systemie wymiany informacji morskich (SafeSeaNet), o którym mowa w art. 22a ust. 3 oraz w załączniku III do dyrektywy 2002/59/WE.

2. Państwa członkowskie zapewniają, aby drogą elektroniczną i w rozsądnym terminie zgodnie z dyrektywą 2010/65/UE przekazywane były następujące informacje:

a) dotyczące rzeczywistego czasu przybycia do portu i czasu wyjścia z portu każdego statku, objętego zakresem dyrektywy 2002/59/WE, który zawija do portu na terenie Unii, wraz z identyfikatorem danego portu;

b) pochodzące z wcześniejszego powiadomienia o odpadach określonego w załączniku 2;

c) pochodzące z pokwitowania odprowadzenia odpadów określonego w załączniku 3;

d) widniejące na świadectwie zwolnienia określonym w załączniku 5.

3. Państwa członkowskie zapewniają, aby informacje wymienione w art. 5 ust. 2 były udostępniane poprzez SafeSeaNet drogą elektroniczną.

Artykuł 14

Rejestrowanie inspekcji

1. Komisja opracowuje, utrzymuje i aktualizuje bazę danych wyników inspekcji, do której podłączone są wszystkie państwa członkowskie i która zawiera wszystkie informacje wymagane do wdrożenia systemu inspekcji określonego w niniejszej dyrektywie (zwaną dalej „bazą danych wyników inspekcji"). Baza danych wyników inspekcji jest oparta na bazie danych wyników inspekcji, o której mowa w art. 24 dyrektywy 2009/16/WE, oraz posiada podobne funkcje.

2. Państwa członkowskie zapewniają, aby informacje dotyczące inspekcji przeprowadzonych zgodnie z niniejszą dyrektywą, w tym informacje dotyczące niezgodności z przepisami i wydanych zakazów wyjścia w morze, były przekazywane do bazy danych wyników inspekcji niezwłocznie po:

a) zakończeniu sporządzania protokołu inspekcji,

b) uchyleniu zakazu wyjścia w morze; lub

c) przyznaniu zwolnienia.

3. Komisja zapewnia, aby baza danych wyników inspekcji umożliwiała pobieranie wszelkich istotnych danych zgłoszonych przez państwa członkowskie w celu monitorowania wdrażania niniejszej dyrektywy.

Komisja zapewnia, by baza danych wyników inspekcji zawierała informacje użyteczne dla unijnego ukierunkowanego mechanizmu opartego na analizie ryzyka, o którym mowa w art. 11 ust. 2.

Komisja dokonuje regularnego przeglądu bazy danych wyników inspekcji w celu monitorowania wdrażania niniejszej dyrektywy i zwraca uwagę na wszelkie wątpliwości dotyczące całościowego wdrażania w celu zastosowania działań naprawczych.

4. Państwa członkowskie muszą mieć zawsze dostęp do informacji zarejestrowanych w bazie danych wyników inspekcji.

Artykuł 15

Szkolenie personelu

Organy portowe i zarządzające portowymi urządzeniami do odbioru odpadów zapewniają, aby wszyscy pracownicy przechodzili szkolenie niezbędne do zdobycia wiedzy, która ma podstawowe znaczenie dla ich pracy w zakresie postępowania z odpadami, ze szczególnym naciskiem na aspekty dotyczące zdrowia i bezpieczeństwa podczas postępowania z odpadami niebezpiecznymi, oraz aby wymogi szkoleniowe były regularnie aktualizowane w celu sprostania wyzwaniom związanym z innowacjami technologicznymi.

Artykuł 16

Sankcje

Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszenia przepisów krajowych przyjętych na podstawie niniejszej dyrektywy oraz podejmują wszelkie niezbędne środki w celu zapewnienia ich wdrożenia. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające.

Sekcja 5

Przepisy końcowe

Artykuł 17

Wymiana doświadczeń

Komisja zapewnia zorganizowanie wymiany doświadczeń między organami państw członkowskich i ekspertami, w tym z sektora prywatnego, społeczeństwa obywatelskiego i związków zawodowych, na temat stosowania niniejszej dyrektywy w portach na terenie Unii.

Artykuł 18

Procedura wprowadzania zmian

1. Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 19 do wprowadzenia zmian do załączników do niniejszej dyrektywy i odniesień do instrumentów IMO w niniejszej dyrektywie w zakresie niezbędnym do dostosowania ich do prawa Unii lub w celu uwzględnienia postępów na poziomie międzynarodowym, w szczególności w odniesieniu do IMO.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 19 w celu zmiany załączników, jeżeli jest to konieczne do poprawy rozwiązań dotyczących wdrażania i monitorowania ustanowionych niniejszą dyrektywą, w szczególności określonych w art. 6, 7 i 9, w celu zapewnienia skutecznego powiadamiania i odprowadzania odpadów, a także właściwego stosowania zwolnień.

3. W wyjątkowych okolicznościach, w przypadku gdy jest to należycie uzasadnione odpowiednią analizą przeprowadzoną przez Komisję oraz w celu uniknięcia poważnego i niedopuszczalnego zagrożenia dla środowiska morskiego, Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 19 w celu zmiany niniejszej dyrektywy w zakresie koniecznym do uniknięcia takiego zagrożenia, tak aby do celów niniejszej dyrektywy nie stosować zmiany wprowadzonej do konwencji MARPOL.

4. Akty delegowane przewidziane w niniejszym artykule przyjmuje się co najmniej trzy miesiące przed upływem terminu ustalonego na szczeblu międzynarodowym dla dorozumianego przyjęcia danej zmiany do konwencji MARPOL lub przed przewidzianą datą wejścia w życie tej zmiany.

W okresie poprzedzającym wejście w życie takich aktów delegowanych państwa członkowskie powstrzymują się od wszelkich inicjatyw zmierzających do włączenia tej zmiany do przepisów krajowych lub od stosowania zmiany do danego instrumentu międzynarodowego.

Artykuł 19

Wykonanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 18 ust. 1, 2 i 3, powierza się Komisji na czas pięciu lat od dnia 27 czerwca 2019 r. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem pięcioletniego okresu. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.

3. Przekazanie uprawnień, o którym mowa w art. 18 ust. 1, 2 i 3, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go jednocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 18 ust. 1, 2 i 3 wchodzi w życie, tylko jeśli Parlament Europejski albo Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie lub jeśli, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 20

Procedura komitetowa

1. Komisja jest wspierana przez Komitet ds. Bezpiecznych Mórz i Zapobiegania Zanieczyszczeniom Morza przez Statki (COSS) ustanowiony na mocy rozporządzenia (WE) nr 2099/2002 Parlamentu Europejskiego i Rady ([22]). Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 21

Zmiany w dyrektywie 2010/65/UE

W pkt A załącznika do dyrektywy 2010/65/UE pkt 4 otrzymuje brzmienie:

„4. Powiadomienie o odpadach ze statków, w tym pozostałości

Art. 6, 7 i 9 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/883 z dnia 17 kwietnia 2019 r. w sprawie portowych urządzeń do odbioru odpadów ze statków, zmieniającej dyrektywę 2010/65/UE i uchylającej dyrektywę 2000/59/WE (Dz.U. L 151 z 7.6.2019, s. 116).”.

Artykuł 22

Uchylenie

Dyrektywa 2000/59/WE traci moc.

Odniesienia do uchylonej dyrektywy traktuje się jako odniesienia do niniejszej dyrektywy.

Artykuł 23

Przegląd

1. Komisja oceni niniejszą dyrektywę i przekaże wyniki oceny Parlamentowi Europejskiemu i Radzie do dnia 28 czerwca 2026 r. Ocena ta obejmuje także szczegółowe sprawozdanie na temat najlepszych praktyk dotyczących zapobiegania powstawaniu odpadów i gospodarowania nimi na statkach.

2. W świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/1625 ([23]), gdy nadejdzie termin kolejnego przeglądu mandatu Europejskiej Agencji Bezpieczeństwa Morskiego (EMSA), Komisja oceni również, czy agencji tej należy przyznać dodatkowe kompetencje w celu wdrażania niniejszej dyrektywy.

([22]) Rozporządzenie (WE) nr 2099/2002 Parlamentu Europejskiego i Rady z dnia 5 listopada 2002 r. ustanawiające Komitet ds. Bezpiecznych Mórz i Zapobiegania Zanieczyszczeniu Morza przez Statki (COSS) i zmieniające rozporządzenia dotyczące bezpieczeństwa na morzu i zapobiegania zanieczyszczeniom morza przez statki (Dz.U. L 324 z 29.11.2002, s. 1).

([23]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1625 z dnia 14 września 2016 r. zmieniające rozporządzenie (WE) nr 1406/2002 ustanawiające Europejską Agencję Bezpieczeństwa Morskiego (Dz.U. L 251 z 16.9.2016, s. 77).

Artykuł 24

Transpozycja

1. Państwa członkowskie wprowadzają w życie, środki ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy do dnia 28 czerwca 2021 r. Niezwłocznie informują one o tym Komisję.

Środki przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.

2. Państwa członkowskie przekazują Komisji tekst podstawowych przepisów prawa krajowego przyjętych w dziedzinie objętej niniejszą dyrektywą.

Artykuł 25

Wejście w życie

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 26

Adresaci

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w Strasburgu dnia 17 kwietnia 2019 r.

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

ZAŁĄCZNIK 1

WYMOGI DOTYCZĄCE PLANÓW ODBIORU I ZAGOSPODAROWANIA ODPADÓW

Plany odbioru i zagospodarowania odpadów obejmują wszystkie rodzaje odpadów ze statków zwykle odwiedzających dany port, i są opracowywane stosownie do wielkości portu i rodzaju statków zawijających do tego portu.

W planach odbioru i zagospodarowania odpadów uwzględnia się następujące elementy:

a) ocenę zapotrzebowania na portowe urządzenia do odbioru odpadów, w świetle zapotrzebowania statków zwykle odwiedzających dany port;

b) opis rodzaju i pojemności portowych urządzeń do odbioru odpadów;

c) opis procedur odbierania i gromadzenia odpadów ze statków;

d) opis systemu pokrywania kosztów;

e) opis procedury zgłaszania nieprawidłowości w zakresie portowych urządzeń do odbioru odpadów;

f) opis procedury konsultacji prowadzonych z użytkownikami portów, odbiorcami odpadów, operatorami terminali i innymi zainteresowanymi stronami; oraz

g) przegląd rodzajów i ilości odpadów odbieranych ze statków i przetwarzanych w portowych urządzeniach do odbioru odpadów.

Plany odbioru i zagospodarowania odpadów mogą obejmować:

a) streszczenie odpowiednich przepisów krajowych oraz procedur i formalności związanych z odprowadzaniem odpadów do portowych urządzeń do odbioru odpadów;

b) wskazanie punktu kontaktowego w porcie;

c) opis sprzętu do wstępnej obróbki i procesów w odniesieniu do określonych strumieni odpadów w porcie, jeżeli istnieją;

d) opis metod rejestrowania bieżącego wykorzystania portowych urządzeń do odbioru odpadów;

e) opis metod rejestrowania ilości odpadów odprowadzanych przez statki;

f) opis metod postępowania z różnymi strumieniami odpadów w porcie.

Procedury dotyczące odbierania, gromadzenia, składowania, przetwarzania i unieszkodliwiania są zgodne pod każdym względem z systemem zarządzania środowiskiem, odpowiednim do stopniowej redukcji oddziaływania tych działań na środowisko. Domniemywa się, że taka zgodność ma miejsce, jeżeli procedury są zgodne z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 1221/2009 ([1]).

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1221/2009 z dnia 25 listopada 2009 r. w sprawie dobrowolnego udziału organizacji w systemie ekozarządzania i audytu we Wspólnocie (EMAS), uchylające rozporządzenie (WE) nr 761/2001 oraz decyzje Komisji 2001/681/WE i 2006/193/WE (Dz.U. L 342 z 22.12.2009, s. 1).

ZAŁĄCZNIK 2

STANDARDOWY FORMAT WCZEŚNIEJSZEGO POWIADOMIENIA O ODPROWADZANIU ODPADÓW DO PORTOWYCH URZĄDZEŃ DO ODBIORU ODPADÓW

Powiadomienie o odprowadzaniu odpadów do: *(podać nazwę portu zawinięcia, jak określono w art. 6 dyrektywy (UE) 2019/883)*

Niniejszy formularz należy przechowywać na statku wraz z odpowiednią książką zapisów olejowych, książką zapisów ładunkowych, książką zapisów o postępowaniu z odpadami lub planem postępowania z odpadami zgodnie z wymogami konwencji MARPOL.

1. DANE DOTYCZĄCE STATKU

1.1. Nazwa statku:	1.5. Właściciel lub operator:
1.2. Numer IMO:	1.6. Numer lub litery identyfikacyjne:
	Numer MMSI (Identyfikator morskiej służby ruchomej):
1.3. Pojemność brutto:	1.7. Państwo bandery:
1.4. Rodzaj statku: ☐ Tankowiec ☐ Chemikaliowiec ☐ Masowiec ☐ Kontenerowiec ☐ Inny statek towarowy ☐ Statek pasażerski ☐ Statek ro-ro ☐ Inny (należy określić)	

2. DANE DOTYCZĄCE PORTU I REJSU

2.1. Lokalizacja/nazwa terminalu:	2.6. Ostatni port, w którym odprowadzono odpady:
2.2. Data i godzina przybycia do portu:	2.7. Data ostatniego odprowadzenia odpadów:
2.3. Data i godzina wypłynięcia z portu:	2.8. Następny port odprowadzenia odpadów:
2.4. Ostatni port i kraj:	2.9. Następny port odprowadzenia odpadów:
2.5. Następny port i kraj (jeśli są znane):	

3. RODZAJ I ILOŚĆ ODPADÓW ORAZ POJEMNOŚĆ MAGAZYNOWANIA

Rodzaj	Ilość odpadów do odprowadzenia (m^3)	Maksymalna pojemność magazynowania przeznaczona na odpady (m^3)	Ilość odpadów zatrzymanych na statku (m^3)	Port, w którym pozostałe odpady zostaną odprowadzone	Szacowana ilość odpadów wytworzonych między powiadomieniem a następnym portem zawinięcia (m^3)
Konwencja MARPOL Załącznik I – Oleje					
Zaolejone wody zęzowe					
Pozostałości olejowe (szlam)					
Zaolejone wody po myciu zbiorników					
Brudny balast					

Rodzaj	Ilość odpadów do odprowadzenia (m^3)	Maksymalna pojemność magazynowania przeznaczona na odpady (m^3)	Ilość odpadów zatrzymanych na statku (m^3)	Port, w którym pozostałe odpady zostaną odprowadzone	Szacowana ilość odpadów wytworzonych między powiadomieniem a następnym portem zawinięcia (m^3)
Kamień i szlam po czyszczeniu zbiorników					
Inne (proszę określić)					
Konwencja MARPOL Załącznik II – SZKODLIWE SUBSTANCJE CIEKŁE (1)					
Substancja kategorii X					
Substancja kategorii Y					
Substancja kategorii Z					
IS – Inne substancje					
Konwencja MARPOL Załącznik IV – Ścieki					
Konwencja MARPOL Załącznik V – Odpady					
A. Tworzywa sztuczne					
B. Odpady produktów spożywczych					
C. Odpady komunalne (np. wyroby z papieru, szmaty, szkło, metal, butelki, porcelana stołowa itp.)					
D. Zużyty olej spożywczy					
E. Popiół ze spalarek					
F. Odpady eksploatacyjne					
G. Zwłoki zwierzęce					
H. Narzędzia połowowe					
I. Zużyty sprzęt elektryczny i elektroniczny					

(1) Należy podać prawidłową nazwę przewozową przedmiotowej szkodliwej substancji ciekłej.

(1) Należy podać prawidłową nazwę przewozową przedmiotowej szkodliwej substancji ciekłej.

Rodzaj	Ilość odpadów do odprowadzenia (m^3)	Maksymalna pojemność magazynowania przeznaczona na odpady (m^3)	Ilość odpadów zatrzymanych na statku (m^3)	Port, w którym pozostałe odpady zostaną odprowadzone	Szacowana ilość odpadów wytworzonych między powiadomieniem a następnym portem zawinięcia (m^3)
J. Pozostałości ładunku (1) (szkodliwe dla środowiska morskiego)					
K. Pozostałości ładunku (2) (nieszkodliwe dla środowiska morskiego)					
Konwencja MARPOL Załącznik VI – Związane z zanieczyszczeniem powietrza					
Substancje zubożające warstwę ozonową i urządzenia zawierające takie substancje (3)					
Pozostałości z oczyszczania spalin					

Inne odpady nieujęte w konwencji MARPOL					
Biernie poławiane odpady					

Uwagi

1. Powyższe informacje mogą być wykorzystywane w ramach inspekcji przeprowadzanej przez państwo portu oraz innych inspekcji.
2. Niniejszy formularz należy wypełnić, chyba że statek podlega wyłączeniu zgodnie z art. 9 dyrektywy (UE) 2019/883

(1) Wartości mogą być szacunkowe. Należy podać prawidłową nazwę przewozową suchego ładunku.
(2) Wartości mogą być szacunkowe. Należy podać prawidłową nazwę przewozową suchego ładunku.
(3) Wynikające z normalnych czynności konserwacyjnych na pokładzie.

ZAŁĄCZNIK 3

STANDARDOWY FORMAT POKWITOWANIA ODPROWADZENIA ODPADÓW

Wyznaczony przedstawiciel podmiotu zarządzającego portowym urządzeniem do odbioru odpadów przekazuje poniższy formularz kapitanowi statku, który odprowadził odpady zgodnie z art. 7 dyrektywy (UE) 2019/883.

Formularz ten należy zachować na statku wraz z odpowiednią książką zapisów olejowych, książką zapisów ładunkowych, książką zapisów postępowania z odpadami lub planem postępowania z odpadami zgodnie z wymogami konwencji MARPOL.

1. PORTOWE URZĄDZENIE DO ODBIORU ODPADÓW I SZCZEGÓŁY DOT. PORTU

1.1. Lokalizacja/nazwa terminalu:
1.2. Dostawca (dostawcy) portowych urządzeń do odbioru odpadów:
1.3. Podmiot świadczący (podmioty świadczące) usługi przetwarzania odpadów – jeżeli inne niż powyżej:
1.4. Data i czas odprowadzenia odpadów od: do:

2. DANE DOTYCZĄCE STATKU

2.1. Nazwa statku:					2.5. Właściciel lub operator:				
2.2. Numer IMO:					2.6. Numer lub litery identyfikacyjne: Numer MMSI (Identyfikator morskiej służby ruchomej):::				
2.3. Pojemność brutto:					2.7. Państwo bandery:				
2.4. Rodzaj statku:	☐	Tankowiec	☐	Chemikaliowiec	☐	Masowiec	☐	Kontenerowiec	
	☐	Inny statek towarowy	☐	Statek pasażerski	☐	Statek ro-ro	☐	Inne (proszę określić)	

3. RODZAJ I ILOŚĆ ODPROWADZONYCH ODPADÓW

Konwencja MARPOL Załącznik I – Oleje	Ilość (m^3)
Zaolejone wody zęzowe	
Pozostałości olejowe (szlam)	
Zaolejone wody po myciu zbiorników	
Brudny balast	
Kamień i szlam po czyszczeniu zbiorników	
Inne (proszę określić)	
Konwencja MARPOL Załącznik II – Szkodliwe substancje ciekłe	Ilość (m^3)/ Nazwa (1)
Substancja kategorii X	

Konwencja MARPOL Załącznik V – Śmieci	Ilość (m^3)
A. Tworzywa sztuczne	
B. Odpady produktów spożywczych	
C. Odpady komunalne (np. wyroby z papieru, szmaty, szkło, metal, butelki, porcelana stołowa itp.)	
D. Zużyty olej spożywczy	
E. Popioły ze spalarek	
F. Odpady eksploatacyjne	
G. Zwłoki zwierzęce	
H. Narzędzia połowowe	

Substancja kategorii Y	
Substancja kategorii Z	
IS – Inne substancje	
Konwencja MARPOL Załącznik IV – Ścieki	Ilość (m^3)

I. Zużyty sprzęt elektryczny i elektroniczny	
J. Pozostałości ładunku (2) (szkodliwe dla środowiska morskiego)	
K. Pozostałości ładunku (2) (nieszkodliwe dla środowiska morskiego)	
Konwencja MARPOL Załącznik VI – Związane z zanieczyszczeniem powietrza	Ilość (m^3)
Substancje zubożające warstwę ozonową i urządzenia zawierające takie substancje	
Pozostałości z oczyszczania spalin	
Inne odpady nieujęte w konwencji MARPOL	Ilość (m^3)
Biernie poławiane odpady	

(1) Należy podać prawidłową nazwę przewozową przedmiotowej szkodliwej substancji ciekłej.
(2) Należy podać prawidłową nazwę przewozową suchego ładunku.

ZAŁĄCZNIK 4

KATEGORIE KOSZTÓW I PRZYCHODÓW NETTO ZWIĄZANYCH Z FUNKCJONOWANIEM PORTOWYCH URZĄDZEŃ DO ODBIORU ODPADÓW I ZARZĄDZANIEM NIMI

Koszty bezpośrednie	Koszty pośrednie	Przychody netto
Bezpośrednie koszty operacyjne wynikające z faktycznego odprowadzania odpadów ze statków, w tym pozycje kosztów wymienione poniżej.	Pośrednie koszty administracyjne wynikające z zarządzania systemem w porcie, w tym pozycje kosztów wymienione poniżej.	Przychody netto z programów gospodarowania odpadami oraz dostępnego finansowania na szczeblu krajowym/regionalnym, w tym składniki przychodów wymienione poniżej.
— Udostępnianie infrastruktury portowych urządzeń do odbioru odpadów, w tym pojemników, zbiorników, narzędzi do obróbki, barek, ciężarówek, urządzeń do odbioru odpadów, instalacji do obróbki odpadów; — Koncesje z tytułu dzierżawy terenu, jeśli dotyczy, lub leasingu sprzętu niezbędnego do funkcjonowania portowych urządzeń do odbioru odpadów; — Rzeczywista eksploatacja portowych urządzeń do odbioru odpadów: odbieranie odpadów ze statku, transport odpadów z portowych urządzeń do odbioru odpadów do końcowego zakładu przetwarzania, konserwacja i czyszczenie portowych urządzeń do odbioru odpadów, koszty personelu, w tym nadgodzin, dostawa energii elektrycznej, analiza odpadów i ubezpieczenie; — Przygotowanie do ponownego użycia, recykling lub unieszkodliwianie odpadów ze statków, w tym selektywna zbiórka odpadów; — Administracja: fakturowanie, wystawianie pokwitowań odbioru odpadów ze statku, raportowanie.	— Opracowanie i zatwierdzenie planu odbioru i zagospodarowania odpadów, w tym wszelkich audytów planu i jego realizacji; — Aktualizacja planu odbioru i zagospodarowania odpadów, w tym kosztów pracy i kosztów doradztwa, w stosownych przypadkach; — Organizowanie procedur konsultacyjnych dotyczących (ponownej) oceny planu odbioru i zagospodarowania odpadów; — Zarządzanie systemami powiadamiania i pokrywania kosztów, w tym stosowanie obniżonych opłat dla „zielonych statków”, zapewnianie systemów informatycznych na poziomie portu, analiza statystyczna i związane z powyższym koszty pracy; — Organizowanie procedur zamówień publicznych na dostarczanie portowych urządzeń do odbioru odpadów, a także wydawanie niezbędnych zezwoleń na dostarczanie portowych urządzeń do odbioru odpadów; — Przekazywanie informacji użytkownikom portu poprzez dystrybucję ulotek, wystawianie znaków i plakatów w porcie lub publikowanie informacji na stronie internetowej portu oraz elektroniczne przekazywanie informacji zgodnie z wymogami art. 5; — Zarządzanie programami gospodarowania odpadami: Systemy rozszerzonej odpowiedzialności producenta, recykling oraz ubieganie się o fundusze krajowe/regionalne i korzystanie z nich; — Inne koszty administracyjne: koszt monitorowania i elektronicznego zgłaszania zwolnień zgodnie z art. 9.	— Korzyści finansowe netto wynikające z systemów rozszerzonej odpowiedzialności producenta; — Inne przychody netto z gospodarowania odpadami, np. z programów recyklingu; — Finansowanie w ramach Europejskiego Funduszu Morskiego i Rybackiego (EFMR); — inne rodzaje finansowania lub dotacje dla portów przeznaczone na gospodarowanie odpadami i rybołówstwo.

ZAŁĄCZNIK 5

ŚWIADECTWO ZWOLNIENIA NA MOCY ART. 9 W ZWIĄZKU Z WYMOGAMI ART. 6, ART. 7 UST. 1 I ART. 8 DYREKTYWY (UE) 2019/883 W PORCIE/PORTACH *[WPISAĆ NAZWĘ PORTU]* W *[WPISAĆ NAZWĘ PAŃSTWA CZŁONKOWSKIEGO]* [1]

Nazwa statku	Numer lub litery identyfikacyjne	Państwo bandery
[*wpisać nazwę statku*]	[*wpisać numer IMO*]	[*wpisać nazwę państwa bandery*]

statek włączony jest w ustalony harmonogram podróży, z częstymi i regularnymi zawinięciami do portu (portów) w *[wpisać nazwę państwa członkowskiego]* zgodnie z harmonogramem lub wcześniej ustaloną trasą:

[ ]

i zawija co najmniej raz na dwa tygodnie do portów:

[ ]

i zawarta została umowa w celu zapewnienia uiszczania opłat i odprowadzania odpadów do portu lub stronie trzeciej w porcie:

[ ]

i jest w związku z tym zwolniony, zgodnie z [*wpisać odpowiedni przepis prawa krajowego obowiązującego w danym kraju*], [*z wymogów dotyczących:*

☐ *obowiązku odprowadzania odpadów ze statków*,

☐ *wcześniejszego powiadamiania o odpadach, oraz*

☐ *uiszczania obowiązkowej opłaty, w następującym porcie (następujących portach):*]

Niniejsze świadectwo jest ważne do [*wstawić datę*], chyba że podstawy wydania niniejszego świadectwa zostaną zmienione przed tą datą.

Miejsce i data

.....

Nazwisko
Tytuł

(1) Niepotrzebne skreślić.

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/884

z dnia 17 kwietnia 2019 r.

zmieniająca decyzję ramową Rady 2009/315/WSiSW w odniesieniu do wymiany informacji dotyczących obywateli państw trzecich oraz w odniesieniu do europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS) i zastępująca decyzję Rady 2009/316/WSiSW

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 82 ust. 1 akapit drugi lit. d),

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([1]),

a także mając na uwadze, co następuje:

(1) Unia wyznaczyła sobie cel polegający na zapewnieniu swoim obywatelom przestrzeni wolności, bezpieczeństwa i sprawiedliwości bez granic wewnętrznych, w której zapewniony jest swobodny przepływ osób. Cel ten należy osiągnąć, między innymi, za pomocą odpowiednich środków służących zapobieganiu przestępczości – w tym przestępczości zorganizowanej i terroryzmowi – i jej zwalczaniu.

(2) Osiągnięcie tego celu wymaga, by informacje dotyczące wyroków skazujących zapadłych w państwach członkowskich m były uwzględniane poza skazującym państwem członkowskim w toku nowego postępowania karnego, jak określono w decyzji ramowej Rady 2008/675/WSiSW ([2]), jak i w celu zapobiegania kolejnym przestępstwom.

(3) Realizacja tego celu wymaga prowadzenia między właściwymi organami państw członkowskich wymiany informacji pochodzących z rejestrów karnych. Tego rodzaju wymianę informacji organizują i ułatwiają zasady określone w decyzji ramowej Rady 2009/315/WSiSW ([3]) oraz europejski system przekazywania informacji z rejestrów karnych (ECRIS), ustanowiony zgodnie z decyzją Rady 2009/316/WSiSW ([4]).

(4) Obowiązujące ramy prawne ECRIS nie uwzględniają jednak w sposób wystarczający specyfiki wniosków dotyczących obywateli państw trzecich. Pomimo że wymiana informacji dotyczących obywateli państw trzecich za pośrednictwem ECRIS jest już możliwa, nie istnieje żadna wspólna unijna procedura ani mechanizm, które pozwalałyby na efektywną, szybką i prawidłową wymianę takich informacji.

(5) W Unii informacje dotyczące obywateli państw trzecich nie są gromadzone tak jak ma to miejsce w przypadku obywateli państw członkowskich – w państwach członkowskich ich obywatelstwa, lecz są jedynie przechowywane w państwach członkowskich, w których wydano wyroki skazujące. Pełną informację na temat wcześniejszej karalności danego obywatela państwa trzeciego można zatem uzyskać jedynie wtedy, gdy wniosek o udzielenie takich informacji zostanie skierowany do wszystkich państw członkowskich.

(6) Tego rodzaju „wnioski ogólne" stanowią nieproporcjonalne obciążenie administracyjne dla wszystkich państw członkowskich, w tym dla państw członkowskich nieposiadających informacji dotyczących danego obywatela państwa trzeciego. W praktyce obciążenie to zniechęca państwa członkowskie do występowania do innych państw członkowskich z wnioskami o udzielenie informacji dotyczących obywateli państw trzecich, co poważnie utrudnia wymianę tych informacji między państwami członkowskimi, ograniczając ich dostęp do informacji z rejestrów karnych do informacji przechowywanych w ich rejestrach krajowych. W konsekwencji wzrasta ryzyko, że wymiana informacji między państwami członkowskimi będzie nieskuteczna i niepełna

([1]) Stanowisko Parlamentu Europejskiego z dnia 12 marca 2019 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 9 kwietnia 2019 r.

([2]) Decyzja ramowa Rady 2008/675/WSiSW z dnia 24 lipca 2008 r. w sprawie uwzględniania w nowym postępowaniu karnym wyroków skazujących zapadłych w państwach członkowskich Unii Europejskiej (Dz.U. L 220 z 15.8.2008, s. 32).

([3]) Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji (Dz.U. L 93 z 7.4.2009, s. 23).

([4]) Decyzja Rady 2009/316/WSiSW z dnia 6 kwietnia 2009 r. w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), zgodnie z art. 11 decyzji ramowej 2009/315/WSiSW (Dz.U. L 93 z 7.4.2009, s. 33).

(7) Aby poprawić tę sytuację, Komisja przedłożyła wniosek, który doprowadził do przyjęcia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/816 ([5]) ustanawiającego na poziomie Unii scentralizowany system zawierającego dane osobowe skazanych obywateli państw trzecich, umożliwiający ustalenie które państwa członkowskie posiadają informacje dotyczące uprzednich wyroków skazujących wydanych wobec obywateli państw trzecich (zwany dalej „ECRIS-TCN").

(8) ECRIS-TCN umożliwi organowi centralnemu państwa członkowskiego szybkie i efektywne ustalenie, jakie inne państwa członkowskie przechowują informacje z rejestrów karnych dotyczące danego obywatela państwa trzeciego tak, aby możliwe było skorzystanie z istniejących ram ECRIS po to, by zwrócić się do tych państw członkowskich z wnioskiem o udzielenie informacji z rejestrów karnych zgodnie z decyzją ramową 2009/315/WSiSW.

(9) Wymiana informacji dotyczących wyroków skazujących jest istotna w każdej strategii zwalczania przestępczości i terroryzmu. Wykorzystanie przez państwa członkowskie pełnego potencjału ECRIS umożliwiłoby wymiarowi sprawiedliwości w sprawach karnych lepsze reagowanie na radykalizację postaw prowadzącą do terroryzmu i brutalnego ekstremizmu.

(10) Aby zwiększyć przydatność informacji dotyczących wyroków skazujących i pozbawienia praw na podstawie wyroku skazującego za przestępstwa seksualne popełnione wobec dzieci, dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE ([6]) nałożyła na państwa członkowskie obowiązek podjęcia środków niezbędnych do zapewnienia, by – do celu rekrutowania osób na stanowiska wiążące się z bezpośrednimi i regularnymi kontaktami z dziećmi – informacje o wyrokach skazujących za przestępstwa seksualne popełnione wobec dzieci odnotowanych w rejestrze karnym lub o jakimkolwiek pozbawieniu praw wynikającym z tych wyroków skazujących były przekazywane zgodnie z procedurami określonymi w decyzji ramowej 2009/315/WSiSW. Celem tego mechanizmu jest zapewnienie, by osoba skazana za przestępstwo seksualne wobec dzieci nie mogła zataić takiego wyroku skazującego ani takiego pozbawienia praw z myślą o podjęciu w innym państwie członkowskim działalności zawodowej związanej z bezpośrednimi i regularnymi kontaktami z dziećmi.

(11) Niniejsza dyrektywa ma na celu dokonanie w decyzji ramowej 2009/315/WSiSW niezbędnych zmian, które umożliwią skuteczną wymianę informacji za pośrednictwem ECRIS dotyczących wyroków skazujących wydanych wobec obywateli państw trzecich. Zobowiązuje ona państwa członkowskie do podjęcia środków niezbędnych do zapewnienia, by wyrokom skazującym towarzyszyły informacje dotyczące obywatelstwa lub obywatelstw osoby skazanej, o ile państwa członkowskie takimi informacjami dysponują. Wprowadza ona również procedury odpowiadania na wnioski o udzielenie informacji, zapewnia, by wypis z rejestru karnego stanowiący przedmiot wniosku obywatela państwa trzeciego został uzupełniony informacjami z innych państw członkowskich, oraz przewiduje niezbędne zmiany techniczne w celu zapewnienia funkcjonowania systemu wymiany informacji.

(12) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 ([7]) powinna być stosowana do przetwarzania danych osobowych przez właściwe organy krajowe do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([8]) powinno być stosowane do przetwarzania danych osobowych przez organy krajowe, gdy przetwarzanie takie nie jest objęte zakresem stosowania dyrektywy (UE) 2016/680.

(13) W celu zapewnienia jednolitych warunków wykonywania decyzji ramowej 2009/315/WSiSW zasady określone w decyzji 2009/316/WSiSW należy włączyć do tej decyzji ramowej oraz należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([9]).

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiające scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniające rozporządzenie (UE) 2018/1726 (Dz.U. L 135, 22.5.2019, s. 1).

([6]) Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.U. L 335 z 17.12.2011, s. 1).

([7]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

([8]) 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).

([9]) 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).

(14) Wspólną infrastrukturę komunikacyjną wykorzystywaną do celów wymiany informacji z rejestrów karnych powinna stanowić zabezpieczona transeuropejska telematyczna sieć komunikacyjna między administracjami (S-TESTA) lub każda kolejna jej wersja bądź jakakolwiek alternatywna zabezpieczona sieć.

(15) Niezależnie od możliwości korzystania, zgodnie z mającymi zastosowanie przepisami, z unijnych programów finansowych każde państwo członkowskie powinno ponosić własne koszty wynikające z wdrożenia, użytkowania i utrzymywania swojej bazy danych rejestru karnego oraz zarządzania tą bazą danych, a także z wdrożenia, użytkowania i utrzymywania dostosowań technicznych potrzebnych do umożliwienia korzystania z ECRIS oraz zarządzania tymi dostosowaniami.

(16) Niniejsza dyrektywa respektuje podstawowe prawa i wolności zapisane, w szczególności, w Karcie praw podstawowych Unii Europejskiej, w tym prawo do ochrony danych osobowych, prawo do sądowego i administracyjnego środka zaskarżenia, zasadę równości wobec prawa, prawo do dostępu do bezstronnego sądu, domniemanie niewinności oraz ogólny zakaz dyskryminacji. Niniejszą dyrektywę należy wykonywać zgodnie z tymi prawami i zasadami.

(17) Ponieważ cel niniejszej dyrektywy, a mianowicie umożliwienie szybkiej i skutecznej wymiany prawidłowych informacji z rejestrów karnych dotyczących obywateli państw trzecich, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast możliwe jest – poprzez wprowadzenie wspólnych zasad – jego lepsze 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, niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(18) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do TUE i do Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), Dania nie uczestniczy w przyjęciu niniejszej dyrektywy i nie jest nią związana ani jej nie stosuje.

(19) Zgodnie z art. 1 i 2 oraz art. 4a ust. 1 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do TUE i do TFUE, bez uszczerbku dla art. 4 tego protokołu, Irlandia nie uczestniczy w przyjęciu niniejszej dyrektywy i nie jest nią związana ani jej nie stosuje.

(20) Zgodnie z art. 3 i art. 4a ust. 1 Protokołu nr 21 Zjednoczone Królestwo powiadomiło o chęci uczestniczenia w przyjęciu i stosowaniu niniejszej dyrektywy.

(21) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady ([10]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię dnia 13 kwietnia 2016 r. ([11]).

(22) Należy zatem odpowiednio zmienić decyzję ramową 2009/315/WSiSW,

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

Artykuł 1

Zmiany decyzji ramowej 2009/315/WSiSW

W decyzji ramowej 2009/315/WSiSW wprowadza się następujące zmiany:

1) art. 1 otrzymuje brzmienie:

„*Artykuł 1*

Przedmiot

W niniejszej decyzji ramowej:

a) określa się warunki, zgodnie z którymi skazujące państwo członkowskie dzieli się informacjami dotyczącymi wyroków skazujących z innymi państwami członkowskimi;

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

([11]) Dz.U. C 186 z 25.5.2016, s. 7.

b) określa się obowiązki spoczywające na skazującym państwie członkowskim i na państwie członkowskim, którego obywatelem jest osoba skazana (zwanym dalej »państwem członkowskim, którego obywatelem jest dana osoba«) oraz metody, które należy stosować, odpowiadając na wniosek o udzielenie informacji pochodzących z rejestrów karnych;

c) ustanawia się zdecentralizowany system informatyczny służący wymianie informacji dotyczących wyroków skazujących, oparty na bazach danych rejestrów karnych poszczególnych państw członkowskich, tj. europejski system przekazywania informacji z rejestrów karnych (ECRIS).";

2) w art. 2 dodaje się litery w brzmieniu:

„d) »skazujące państwo członkowskie« oznacza państwo członkowskie, w którym wydano wyrok skazujący;

e) »obywatel państwa trzeciego« oznacza osobę niebędącą obywatelem Unii w rozumieniu art. 20 ust. 1 TFUE, osobę, która jest bezpaństwowcem lub osobę, której obywatelstwo jest nieznane;

f) »dane daktyloskopijne« oznaczają dane odnoszące się do odcisków wszystkich palców danej osoby w formie odbitek płaskich i przetoczonych;

g) »wizerunek twarzy« oznacza cyfrowy wizerunek twarzy danej osoby;

h) »oprogramowanie wzorcowe ECRIS« oznacza oprogramowanie opracowane przez Komisję i udostępnione państwom członkowskim do celów wymiany informacji z rejestrów karnych za pośrednictwem ECRIS.";

3) art. 4 ust. 1 otrzymuje brzmienie:

„1. Każde skazujące państwo członkowskie podejmuje wszelkie środki konieczne do zapewnienia, by wyrokom skazującym wydanym na jego terytorium towarzyszyły informacje dotyczące obywatelstwa lub obywatelstw osoby skazanej, jeżeli jest ona obywatelem innego państwa członkowskiego lub obywatelem państwa trzeciego. W przypadku gdy obywatelstwo osoby skazane nie jest znane albo gdy jest ona bezpaństwowcem, należy to odnotować w rejestrze karnym.";

4) w art. 6 wprowadza się następujące zmiany:

a) ust. 3 otrzymuje brzmienie:

„3. W przypadku gdy obywatel jednego państwa członkowskiego zwraca się z wnioskiem do organu centralnego innego państwa członkowskiego o udzielenie mu informacji zawartych w rejestrze karnym na jego temat, organ ten składa wniosek do organu centralnego państwa członkowskiego, którego obywatelem jest dana osoba, o przekazanie informacji i związanych z nimi danych pochodzących z rejestru karnego oraz uwzględnia takie informacje i związane z nimi dane w wypisie przekazywanym danej osobie.";

b) dodaje się ustęp w brzmieniu:

„3a. W przypadku gdy obywatel państwa trzeciego zwraca się z wnioskiem do organu centralnego państwa członkowskiego o udzielenie mu informacji zawartych w rejestrze karnym na jego temat, organ ten składa wniosek wyłącznie do tych organów centralnych państw członkowskich, które posiadają informacje zawarte w rejestrach karnych na temat tej osoby, o przekazanie informacji i związanych z nimi danych pochodzących z rejestrów karnych oraz uwzględnia takie informacje i związane z nimi dane w wypisie przekazywanym danej osobie.";

5) w art. 7 wprowadza się następujące zmiany:

a) ust. 4 otrzymuje brzmienie:

„4. W przypadku złożenia na podstawie art. 6 do organu centralnego państwa członkowskiego innego niż państwo członkowskie, którego obywatelem jest dana osoba, wniosku o udzielenie informacji pochodzących z rejestru karnego dotyczących wyroków skazujących wydanych wobec obywatela państwa członkowskiego, państwo członkowskie, do którego skierowano wniosek, przekazuje takie informacje w takim samym zakresie, jaki przewidziano w art. 13 Europejskiej konwencji o pomocy prawnej w sprawach karnych.";

b) dodaje się ustęp w brzmieniu:

„4a. W przypadku złożenia na podstawie art. 6 wniosku o udzielenie do celów postępowania karnego informacji pochodzących z rejestru karnego dotyczących wyroków skazujących wydanych wobec obywatela państwa trzeciego państwo członkowskie, do którego skierowano wniosek, przekazuje informacje o wszelkich wyrokach skazujących wydanych w państwie członkowskim, do którego skierowano wniosek, i wpisanych do rejestru karnego oraz o wszelkich wyrokach skazujących, które zostały wydane w państwach trzecich, a następnie przekazane temu państwu i wpisane do rejestru karnego.

W przypadku złożenia wniosku o udzielenie takich informacji do celów innych niż postępowanie karne stosuje się odpowiednio ust. 2 niniejszego artykułu.";

6) art. 8 ust. 2 otrzymuje brzmienie:

„2. Odpowiedzi na wnioski, o których mowa w art. 6 ust. 2, 3 i 3a, udziela się w terminie dwudziestu dni roboczych od daty otrzymania wniosku.";

7) w art. 9 wprowadza się następujące zmiany:

a) w ust. 1 wyrazy „art. 7 ust. 1 i 4" zastępuje się wyrazami „art. 7 ust. 1, 4 i 4a";

b) w ust. 2 wyrazy „art. 7 ust. 2 i 4" zastępuje się wyrazami „art. 7 ust. 2, 4 i 4a";

c) w ust. 3 wyrazy „art. 7 ust. 1, 2 i 4" zastępuje się wyrazami „art. 7 ust. 1, 2, 4 i 4a";

8) w art. 11 wprowadza się następujące zmiany:

a) w ust. 1 akapit pierwszy lit. c) dodaje się podpunkt w brzmieniu:

„(iv) wizerunek twarzy.";

b) ust. 3–7 otrzymują brzmienie:

„3. Organy centralne państw członkowskich przekazują drogą elektroniczną za pośrednictwem ECRIS oraz przy zastosowaniu znormalizowanego formatu zgodnie z normami określonymi w aktach wykonawczych następujące informacje:

a) informacje, o których mowa w art. 4;

b) wnioski, o których mowa w art. 6;

c) odpowiedzi, o których mowa w art. 7; oraz

d) inne istotne informacje.

4. Jeżeli sposób przekazywania informacji, o którym mowa w ust. 3, jest niedostępny, organy centralne państw członkowskich przekazują, uwzględniając bezpieczeństwo tego procesu, wszystkie informacje, o których mowa w ust. 3, wykorzystując do tego celu wszelkie środki pozwalające na wytworzenie pisemnego potwierdzenia i umożliwiające organowi centralnemu państwa członkowskiego otrzymującego informacje stwierdzenie autentyczności tych informacji.

Jeżeli sposób przekazywania informacji, o którym mowa w ust. 3, jest niedostępny przez długi czas, dane państwo członkowskie informuje pozostałe państwa członkowskie oraz Komisję.

5. Każde państwo członkowskie dokonuje dostosowań technicznych niezbędnych do stosowania przez nie znormalizowanego formatu w celu przekazywania innym państwom członkowskim wszelkich informacji, o których mowa w ust. 3, drogą elektroniczną za pośrednictwem ECRIS. Każde państwo członkowskie powiadamia Komisję o dacie, od której będzie w stanie przekazywać informacje w taki sposób.";

9) dodaje się artykuły w brzmieniu:

„Artykuł 11a

Europejski system przekazywania informacji z rejestrów karnych (ECRIS)

1. W celu prowadzenia wymiany informacji pochodzących z rejestrów karnych drogą elektroniczną zgodnie z niniejszą decyzją ramową ustanawia się zdecentralizowany system informatyczny oparty na bazach danych rejestrów karnych poszczególnych państw członkowskich, tj. europejski system przekazywania informacji z rejestrów karnych (ECRIS). System ten składa się z następujących elementów:

a) oprogramowanie wzorcowe ECRIS;

b) wspólna infrastruktura komunikacyjna między organami centralnymi zapewniająca szyfrowaną sieć.

W celu zapewnienia poufności i integralności informacji z rejestrów karnych przekazywanych innym państwom członkowskim wykorzystuje się odpowiednie środki techniczne i organizacyjne, z uwzględnieniem stanu wiedzy technicznej, kosztów wdrożenia i ryzyka wiążącego się z przetwarzaniem informacji.

2. Wszystkie dane z rejestrów karnych są przechowywane wyłącznie w bazach danych prowadzonych przez państwa członkowskie.

3. Organy centralne państw członkowskich nie mogą mieć bezpośredniego dostępu do baz danych rejestrów karnych innych państw członkowskich.

4. Odpowiedzialność za obsługę oprogramowania wzorcowego ECRIS i baz danych służących do przechowywania, wysyłania i odbierania informacji pochodzących z rejestrów karnych spoczywa na danym państwie członkowskim. Państwa członkowskie wspiera Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), ustanowiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1726 (*), zgodnie z jej zadaniami określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/816 (**).

5. Odpowiedzialność za obsługę wspólnej infrastruktury komunikacyjnej spoczywa na Komisji. Infrastruktura ta musi spełniać niezbędne wymogi w zakresie bezpieczeństwa oraz w pełni odpowiadać potrzebom ECRIS.

6. eu-LISA zapewnia, rozwija i utrzymuje oprogramowanie wzorcowe ECRIS,

7. Każde państwo członkowskie ponosi własne koszty wynikające z wdrożenia, użytkowania i utrzymywania swojej bazy danych rejestru karnego oraz zarządzania tą bazą danych, a także instalacji i użytkowania oprogramowania wzorcowego ECRIS.

Komisja ponosi koszty wynikające z wdrożenia, użytkowania, utrzymywania i dalszego rozwijania wspólnej infrastruktury komunikacyjnej oraz zarządzania nią.

8. Państwa członkowskie, które korzystają ze swojego krajowego oprogramowania ECRIS zgodnie z art. 4 ust. 4–8 rozporządzenia (UE) 2019/816 mogą nadal korzystać ze swojego krajowego oprogramowania ECRIS zamiast oprogramowania wzorcowego ECRIS, o ile spełnione są wszystkie warunki określone w tych ustępach.

Artykuł 11b

Akty wykonawcze

1. Komisja przyjmuje akty wykonawcze, w których określa:

a) znormalizowany format, o którym mowa w art. 11 ust. 3, w tym w odniesieniu do informacji o przestępstwie będącym podstawą wyroku skazującego oraz informacji dotyczących treści wyroku skazującego;

b) zasady dotyczące wdrożenia technicznego ECRIS oraz wymiany danych daktyloskopijnych;

c) inne sposoby techniczne organizowania i ułatwiania wymiany informacji dotyczących wyroków skazujących między organami centralnymi państw członkowskich, w tym:

(i) sposoby ułatwiania zrozumienia i automatycznego tłumaczenia przekazywanych informacji;

(ii) sposoby wymiany informacji drogą elektroniczną, w szczególności w odniesieniu do specyfikacji technicznych, które należy stosować oraz, w razie potrzeby, wszelkich stosownych procedur wymiany.

2. Akty wykonawcze, o których mowa w ust. 1 niniejszego artykułu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 12a ust. 2.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1726 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), zmiany rozporządzenia (WE) nr 1987/2006 i decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia (UE) nr 1077/2011 (Dz.U. L 295 z 21.11.2018, s. 99).

(**) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiające scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniające rozporządzenie (UE) 2018/1726 (Dz.U. L 135, 22.5.2019, s. 1).";

10) dodaje się artykuł w brzmieniu:

„Artykuł 12a

Procedura komitetowa

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

W przypadku, gdy komitet nie wyda żadnej opinii, Komisja nie przyjmuje projektu aktu wykonawczego i stosuje się art. 5 ust. 4 akapit trzeci rozporządzenia (UE) nr 182/2011.";

11) dodaje się artykuł w brzmieniu:

„Artykuł 13a

Sprawozdania Komisji i przegląd

1. Do dnia 29 czerwca 2023 r. Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie ze stosowania niniejszej decyzji ramowej. W sprawozdaniu ocenia się, w jakim stopniu państwa członkowskie podjęły środki niezbędne do wykonania niniejszej decyzji ramowej, z uwzględnieniem jej wdrożenia technicznego.

2. W stosownych przypadkach do sprawozdania dołącza się odpowiednie wnioski ustawodawcze.

3. Komisja regularnie publikuje sprawozdanie dotyczące wymiany, za pośrednictwem ECRIS, informacji pochodzących z rejestrów karnych i dotyczące stosowania ECRIS-TCN, oparte w szczególności na statystykach dostarczonych przez eu-LIS-ę i państwa członkowskie zgodnie z rozporządzeniem (UE) 2019/816. Sprawozdanie to po raz pierwszy publikuje się po upływie roku od przedłożenia sprawozdania, o którym mowa w ust. 1.

4. Sprawozdanie Komisji, o którym mowa w ust. 3, przedstawia w szczególności poziom wymiany informacji między państwami członkowskimi, w tym informacji dotyczących obywateli państw trzecich, a także wskazuje cele wniosków i odpowiednio ich liczbę, w tym wniosków do celów innych niż postępowanie karne, takich jak kontrole przeszłości oraz wnioski zainteresowanych osób o udzielenie im informacji zawartych w rejestrach karnych na ich temat.".

Artykuł 2

Zastąpienie decyzji 2009/316/WSiSW

Decyzja 2009/316/WSiSW zostaje zastąpiona w odniesieniu do państw członkowskich związanych niniejszą dyrektywą, bez uszczerbku dla zobowiązań państw członkowskich dotyczących terminu wykonania tej decyzji.

Artykuł 3

Transpozycja

1. Państwa członkowskie wprowadzą w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy do dnia 28 czerwca 2022 r. Niezwłocznie przekazują one Komisji tekst tych przepisów.

Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Przepisy te zawierają także wskazanie, że w istniejących przepisach ustawowych, wykonawczych i administracyjnych odniesienia do decyzji zastąpionej niniejszą dyrektywą traktuje się jak odniesienia do niniejszej dyrektywy. Sposób dokonywania takiego odniesienia i formułowania takiego wskazania określany jest przez państwa członkowskie.

2. Państwa członkowskie przekazują Komisji teksty najważniejszych przepisów prawa krajowego w dziedzinie objętej zakresem niniejszej dyrektywy.

3. Państwa członkowskie dokonują dostosowań technicznych, o których mowa w art. 11 ust. 5 decyzji ramowej 2009/315/WSiSW, w brzmieniu określonym niniejszą dyrektywą, do dnia 28 czerwca 2022 r.

Artykuł 4

Wejście w życie i stosowanie

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Art. 2 stosuje się od dnia 28 czerwca 2022 r.

Artykuł 5

Adresaci

Niniejsza dyrektywa skierowana jest do państw członkowskich zgodnie z Traktatami.

Sporządzono w Strasburgu dnia 17 kwietnia 2019 r.

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

ISSN 1977-0766 (wydanie elektroniczne)
ISSN 1725-5139 (wydanie papierowe)

Urząd Publikacji Unii Europejskiej
2985 Luksemburg
LUKSEMBURG

PL