Rada
Unii Europejskiej

Bruksela, 18 grudnia 2020 r.
(OR. en)

14262/20

Międzyinstytucjonalny numer referencyjny:
2020/0365 (COD)

PROCIV 105	**ECOFIN 1182**
JAI 1132	**ENV 832**
COSI 258	**SAN 490**
ENFOPOL 354	**CHIMIE 69**
CT 121	**RECH 539**
COTER 120	**DENLEG 90**
ENER 512	**RELEX 1037**
TRANS 621	**HYBRID 49**
TELECOM 277	**CYBER 283**
ATO 91	**ESPACE 85**

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	16 grudnia 2020 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2020) 829 final
Dotyczy:	Wniosek dotyczący DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY w sprawie odporności podmiotów krytycznych

Delegacje otrzymują w załączeniu dokument COM(2020) 829 final.

Zał.: COM(2020) 829 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 16.12.2020 r.
COM(2020) 829 final

2020/0365 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie odporności podmiotów krytycznych

{SEC(2020) 433 final} - {SWD(2020) 358 final} - {SWD(2020) 359 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Aby skutecznie chronić Europejczyków, Unia Europejska musi nadal ograniczać podatność na zagrożenia między innymi infrastruktury krytycznej, która ma zasadnicze znaczenie dla funkcjonowania naszych społeczeństw i gospodarki. Źródła utrzymania obywateli Unii oraz dobre funkcjonowanie rynku wewnętrznego zależą od różnych rodzajów infrastruktury zapewniającej niezawodne świadczenie usług niezbędnych do utrzymania krytycznej działalności społecznej i gospodarczej. Usługi te – o kluczowym znaczeniu w normalnych warunkach – są tym bardziej istotne w sytuacji, gdy Europa zmaga się ze skutkami pandemii COVID-19 i myśli o odbudowie po jej zakończeniu. Podmioty świadczące usługi kluczowe muszą być zatem odporne, tj. muszą być w stanie stawić opór w przypadku incydentów, które mogą prowadzić do poważnych, potencjalnie międzysektorowych i transgranicznych zakłóceń, a także stłumić te incydenty, dostosować się do nich oraz usunąć ich skutki.

Celem niniejszego wniosku jest wzmocnienie świadczenia na rynku wewnętrznym usług o kluczowym znaczeniu dla utrzymania niezbędnych funkcji społecznych lub działalności gospodarczej poprzez zwiększenie odporności podmiotów krytycznych świadczących takie usługi. Niniejszy wniosek odzwierciedla niedawne wezwania do podjęcia działań ze strony Rady[1] i Parlamentu Europejskiego[2], które zachęciły Komisję do przeglądu obecnego podejścia, aby lepiej odzwierciedlić rosnące wyzwania stojące przed podmiotami krytycznymi oraz zapewnić lepsze dostosowanie do dyrektywy w sprawie bezpieczeństwa sieci i informacji (NIS)[3]. Niniejszy wniosek jest spójny i tworzy ścisłą synergię z proponowaną dyrektywą w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii („dyrektywa NIS 2”), która zastąpi dyrektywę w sprawie bezpieczeństwa sieci i informacji („dyrektywa NIS”), aby uwzględnić kwestię coraz silniejszych wzajemnych powiązań między światem fizycznym a cyfrowym dzięki ramom legislacyjnym obejmującym zdecydowane środki na rzecz zwiększania odporności zarówno w odniesieniu do aspektów cybernetycznych, jak fizycznych, określonych w strategii UE w zakresie unii bezpieczeństwa[4].

Ponadto we wniosku uwzględniono podejścia krajowe w coraz większej liczbie państw członkowskich, które kładą nacisk na międzysektorowe i transgraniczne współzależności i coraz bardziej świadomie uwzględniają kwestię odporności, w której ochrona jest tylko jednym z elementów obok zapobiegania ryzyku i jego ograniczania, ciągłości działania i odbudowy. Biorąc pod uwagę fakt, że infrastruktura krytyczna jest również zagrożona jako potencjalny cel ataków terrorystycznych, przewidziane w niniejszym wniosku środki mające

---

1 Konkluzje Rady z dnia 10 grudnia 2019 r. w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych (14972/19).

2 Sprawozdanie w sprawie ustaleń i zaleceń Komisji Specjalnej Parlamentu Europejskiego ds. Terroryzmu (2018/2044(INI)).

3 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.

4 COM(2020) 605.

na celu zapewnienie odporności podmiotów krytycznych przyczyniają się do realizacji celów niedawno przyjętego Planu dla UE w dziedzinie zwalczania terroryzmu[5].

Unia Europejska (UE) od dawna uznaje paneuropejskie znaczenie infrastruktur krytycznych. Na przykład w 2006 r. UE ustanowiła europejski program ochrony infrastruktury krytycznej[6], a w 2008 r. przyjęła dyrektywę w sprawie europejskiej infrastruktury krytycznej[7]. W dyrektywie w sprawie europejskiej infrastruktury krytycznej, mającej zastosowanie wyłącznie do sektorów energii i transportu, przewidziano procedurę rozpoznawania i wyznaczania europejskich infrastruktur krytycznych, których zakłócenie lub zniszczenie miałoby istotne transgraniczne skutki w co najmniej dwóch państwach członkowskich. Określono w niej również szczegółowe wymogi w zakresie ochrony dla operatorów europejskiej infrastruktury krytycznej i właściwych organów państw członkowskich. Dotychczas wyznaczono 94 europejskie infrastruktury krytyczne, z których dwie trzecie są zlokalizowane w trzech państwach członkowskich w Europie Środkowo-Wschodniej. Zakres unijnego działania na rzecz zwiększenia odporności infrastruktury krytycznej wykracza jednak poza te środki i obejmuje środki sektorowe oraz międzysektorowe między innymi w zakresie uodparniania na klimat, ochrony ludności, bezpośrednich inwestycji zagranicznych i cyberbezpieczeństwa[8]. Tymczasem państwa członkowskie we własnym zakresie wprowadzały w tej dziedzinie środki, które różnią się między sobą.

Oczywiste jest zatem, że obecne ramy ochrony infrastruktury krytycznej nie są wystarczające, aby odpowiadać na wyzwania, przed którymi stają obecnie infrastruktury krytyczne oraz obsługujące je podmioty. Biorąc pod uwagę coraz silniejsze wzajemne połączenia między infrastrukturami, sieciami i operatorami świadczącymi usługi kluczowe na rynku wewnętrznym, konieczna jest zasadnicza zmiana obecnego podejścia z ochrony konkretnych składników infrastruktury na wzmacnianie odporności podmiotów krytycznych, które je obsługują.

W ostatnich latach środowisko operacyjne, w którym działają podmioty krytyczne, znacząco się zmieniło. Po pierwsze, krajobraz ryzyka jest bardziej złożony niż w 2008 r. i obejmuje obecnie zagrożenia naturalne[9] (w wielu przypadkach spotęgowane przez zmianę klimatu), działania hybrydowe finansowane przez państwo, terroryzm, zagrożenia wewnętrzne, pandemie i wypadki (takie jak awarie przemysłowe). Po drugie, operatorzy stają przed wyzwaniami związanymi z wprowadzaniem do swoich operacji nowych technologii, takich jak sieć 5G oraz pojazdy bezzałogowe, borykając się jednocześnie z podatnością na zagrożenia, jaką technologie te mogą powodować. Po trzecie, technologie te oraz inne tendencje sprawiają, że operatorzy w coraz większym stopniu są zależni od siebie nawzajem. Skutki takiej sytuacji są oczywiste – zakłócenie świadczenia usług przez jednego operatora

5 COM(2020) 795.

6 Komunikat Komisji w sprawie europejskiego programu ochrony infrastruktury krytycznej. COM(2006) 786.

7 Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony.

8 Komunikat Komisji „Strategia UE w zakresie przystosowania się do zmiany klimatu". COM(2013) 216; decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności; rozporządzenie 2019/452 ustanawiające ramy monitorowania bezpośrednich inwestycji zagranicznych w Unii; dyrektywa 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

9 Overview of natural and man-made disaster risks the European Union may face [Przegląd zagrożeń związanych z klęskami żywiołowymi i katastrofami spowodowanymi przez człowieka, wobec jakich może stanąć Unia Europejska]. SWD(2020) 330.

w jednym sektorze może wywołać efekt kaskadowy mający wpływ na świadczenie usług w innych sektorach, a także potencjalnie w innych państwach członkowskich lub w całej Unii.

Jak wynika z opublikowanej w 2019 r. oceny dyrektywy w sprawie europejskiej infrastruktury krytycznej[10], istniejące środki europejskie i krajowe mają ograniczenia, jeżeli chodzi o pomoc operatorom w stawieniu czoła wyzwaniom operacyjnym, przed którymi obecnie stoją, oraz podatności na zagrożenia wynikającej z ich współzależnego charakteru.

Istnieje kilka powodów ku temu, przedstawionych w ocenie skutków, która stanowiła podstawę do opracowania wniosku. Po pierwsze, operatorzy nie są w pełni świadomi lub nie rozumieją w pełni skutków dynamicznego krajobrazu ryzyka, w ramach którego działają. Po drugie, istnieją znaczące rozbieżności między działaniami na rzecz zwiększania odporności w poszczególnych państwach członkowskich i sektorach. Po trzecie, podobne rodzaje podmiotów są uznawane za krytyczne przez niektóre państwa członkowskie, ale przez inne – nie, co oznacza, że porównywalne podmioty otrzymują różny poziom oficjalnego wsparcia w zakresie budowania zdolności (np. w formie wytycznych, organizacji szkoleń i ćwiczeń) w zależności od tego, w którym miejscu w Unii prowadzą działalność, i podlegają różnym wymogom. Fakt, że wymogi i wsparcie rządowe dla operatorów różnią się w poszczególnych państwach członkowskich, tworzy przeszkody dla operatorów prowadzących działania transgraniczne, w szczególności w przypadku tych podmiotów krytycznych, które działają w państwach o bardziej rygorystycznych ramach prawnych. Biorąc pod uwagę coraz bardziej współzależny charakter świadczenia usług i sektorów w państwach członkowskich i w UE, niewystarczający poziom odporności u jednego operatora stwarza poważne ryzyko dla podmiotów w innych miejscach w obrębie rynku wewnętrznego.

Zakłócenia – w szczególności te o skutkach transgranicznych i potencjalnych paneuropejskich – oprócz tego, że zagrażają sprawnemu funkcjonowaniu rynku wewnętrznego, mogą mieć poważne negatywne skutki dla obywateli, przedsiębiorstw, rządów i środowiska. Na poziomie jednostki zakłócenia mogą mieć bowiem wpływ na zdolność Europejczyków do swobodnego podróżowania, pracy i korzystania z kluczowych usług publicznych, takich jak opieka zdrowotna. W wielu przypadkach świadczenie tych i innych usług podstawowych, które stanowią podstawę codziennego życia, odbywa się za pośrednictwem ściśle powiązanych ze sobą sieci europejskich przedsiębiorstw; zakłócenia dotyczące jednego przedsiębiorstwa w jednym sektorze mogą mieć kaskadowe skutki w wielu innych sektorach gospodarki. Ponadto zakłócenia, takie jak na przykład przerwy w dostawie energii elektrycznej na dużą skalę i poważne wypadki transportowe, mogą przyczynić się do osłabienia ochrony i bezpieczeństwa publicznego, wywołując niepewność i podważając zaufanie do podmiotów krytycznych, a także do organów odpowiedzialnych za ich nadzór oraz za zapewnienie bezpieczeństwa społeczeństwa.

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

Niniejszy wniosek odzwierciedla priorytety opracowanej przez Komisję strategii UE w zakresie unii bezpieczeństwa[11]. Wzywa się w niej do zmiany podejścia do odporności infrastruktury krytycznej, które lepiej odzwierciedla obecny i przewidywany w przyszłości krajobraz ryzyka, coraz ściślejszą współzależność między różnymi sektorami, jak również coraz bardziej współzależne relacje między infrastrukturą fizyczną i cyfrową.

10 SWD(2019) 308.

11 Komunikat Komisji w sprawie strategii UE w zakresie unii bezpieczeństwa. COM(2020) 605.

Proponowana dyrektywa zastępuje dyrektywę w sprawie europejskiej infrastruktury krytycznej, a także opiera się na innych istniejących i planowanych instrumentach oraz je uwzględnia. Proponowana dyrektywa stanowi znaczącą zmianę w stosunku do dyrektywy w sprawie europejskiej infrastruktury krytycznej, która ma zastosowanie wyłącznie do sektorów energii i transportu, koncentruje się wyłącznie na środkach ochrony i przewiduje procedurę rozpoznawania i wyznaczania europejskich infrastruktur krytycznych w drodze dialogu transgranicznego. Po pierwsze, proponowana dyrektywa miałaby znacznie szerszy zakres sektorowy obejmujący dziesięć sektorów, a mianowicie sektory energii, transportu, bankowości, infrastruktury rynku finansowego, zdrowia, wody pitnej, ścieków, infrastruktury cyfrowej, administracji publicznej i przestrzeni kosmicznej. Po drugie, w dyrektywie przewidziano procedurę umożliwiającą państwom członkowskim wskazanie podmiotów krytycznych na podstawie wspólnych kryteriów w oparciu o krajową ocenę ryzyka. Po trzecie, we wniosku określono obowiązki państw członkowskich i wskazanych przez nie podmiotów krytycznych, w tym podmiotów o szczególnym znaczeniu europejskim, tj. podmiotów krytycznych, które świadczą usługi kluczowe na rzecz ponad jednej trzeciej lub w ponad jednej trzeciej państw członkowskich i które podlegałyby szczególnemu nadzorowi.

W stosownych przypadkach Komisja zapewniłaby właściwym organom i podmiotom krytycznym wsparcie w wypełnianiu ich obowiązków wynikających z dyrektywy. Ponadto Grupa ds. Odporności Podmiotów Krytycznych, która jest grupą ekspertów Komisji podlegającą horyzontalnym ramom mającym zastosowanie do takich grup, doradzałaby Komisji i wspierałaby strategiczną współpracę i wymianę informacji. Ponieważ współzależności wykraczają poza granice zewnętrzne UE, konieczna jest również współpraca z krajami partnerskimi. Proponowana dyrektywa przewiduje możliwość takiej współpracy, na przykład w dziedzinie oceny ryzyka.

Spójność z innymi politykami Unii

Proponowana dyrektywa jest wyraźnie powiązana oraz spójna z innymi sektorowymi i międzysektorowymi inicjatywami UE dotyczącymi m.in. uodparniania na klimat, ochrony ludności, bezpośrednich inwestycji zagranicznych (BIZ), cyberbezpieczeństwa i dorobku prawnego UE w dziedzinie usług finansowych. W szczególności wniosek jest ściśle dostosowany do proponowanej dyrektywy NIS 2, która ma na celu zwiększenie odporności „podmiotów niezbędnych" i „podmiotów istotnych" osiągających określone progi w wielu sektorach na wszelkie zagrożenia związane z technologiami informacyjno-komunikacyjnymi (ICT), oraz tworzy z nią ścisłą synergię. Niniejszy wniosek dotyczący dyrektywy w sprawie odporności podmiotów krytycznych ma na celu zapewnienie, aby właściwe organy wyznaczone na podstawie niniejszej dyrektywy oraz organy wyznaczone na podstawie proponowanej dyrektywy NIS 2 stosowały wzajemnie się uzupełniające środki i w razie potrzeby wymieniały się informacjami dotyczącymi cyberodporności i odporności niezwiązanej z cyberbezpieczeństwem, a także aby najważniejsze podmioty krytyczne w sektorach uznawanych za „niezbędne" zgodnie z proponowaną dyrektywą NIS 2 podlegały również ogólniejszym obowiązkom w zakresie zwiększania odporności w celu uwzględnienia ryzyka poza cyberprzestrzenią. Do fizycznego bezpieczeństwa sieci i systemów informatycznych podmiotów sektora infrastruktury cyfrowej odniesiono się szczegółowo w proponowanej dyrektywie NIS 2 w ramach obowiązków tych podmiotów w zakresie zarządzania ryzykiem w cyberprzestrzeni i sprawozdawczości. Ponadto wniosek opiera się na istniejącym dorobku prawnym UE w dziedzinie usług finansowych, w którym ustanowiono kompleksowe wymagania względem podmiotów finansowych odnoszące się do zarządzania ryzykiem operacyjnym oraz zapewnienia ciągłości działania. W związku z tym podmioty związane z sektorami infrastruktury cyfrowej, bankowości i infrastruktury finansowej należy traktować

jak podmioty równoważne z podmiotami krytycznymi zgodnie z niniejszą dyrektywą na potrzeby obowiązków i działań państw członkowskich, a niniejsza dyrektywa nie wiązałaby się w takim przypadku z dodatkowymi obowiązkami dla tych podmiotów.

We wniosku uwzględniono również inne inicjatywy sektorowe i międzysektorowe dotyczące np. ochrony ludności, zmniejszania ryzyka związanego z klęskami żywiołowymi i przystosowania się do zmiany klimatu. Ponadto we wniosku uznaje się, że w niektórych przypadkach istniejące przepisy UE nakładają na podmioty obowiązek reagowania na określone ryzyko za pomocą środków ochronnych. W takich przypadkach, np. w odniesieniu do ochrony lotnictwa lub bezpieczeństwa morskiego, podmioty krytyczne powinny opisać te środki w swoich planach zwiększania odporności. Ponadto proponowana dyrektywa pozostaje bez uszczerbku dla zastosowania reguł konkurencji ustanowionych w Traktacie o funkcjonowaniu Unii Europejskiej (TFUE).

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

W przeciwieństwie do dyrektywy 2008/114/WE, którą oparto na art. 308 Traktatu ustanawiającego Wspólnotę Europejską (który odpowiada obecnemu art. 352 Traktatu o funkcjonowaniu Unii Europejskiej), niniejszy wniosek dotyczący dyrektywy opiera się na art. 114 TFUE, który dotyczy zbliżenia przepisów w celu usprawnienia rynku wewnętrznego. Jest to uzasadnione zmianą celu, zakresu i treści dyrektywy, rosnącymi współzależnościami i potrzebą zapewnienia podmiotom krytycznym równiejszych szans. Zamiast ochrony ograniczonej liczby elementów infrastruktury fizycznej, w przypadku których zakłócenie działania lub zniszczenie miałoby istotne skutki transgraniczne, celem jest zwiększenie odporności podmiotów w państwach członkowskich, które mają kluczowe znaczenie dla świadczenia usług koniecznych do utrzymania niezbędnych funkcji społecznych lub prowadzenia działalności gospodarczej na rynku wewnętrznym w szeregu sektorów stanowiących podstawę funkcjonowania wielu innych sektorów gospodarki Unii. Ze względu na rosnące współzależności transgraniczne między usługami świadczonymi z wykorzystaniem infrastruktury krytycznej w tych sektorach zakłócenie w jednym państwie członkowskim może wywołać skutki w innych państwach członkowskich lub w całej Unii.

Obecne ramy prawne ustanowione na szczeblu państw członkowskich, regulujące przedmiotowe usługi wiążą się z istotnie rozbieżnymi obowiązkami, które prawdopodobnie jeszcze się rozwiną. Rozbieżne przepisy krajowe, którym podlegają podmioty krytyczne, nie tylko zagrażają niezawodnemu świadczeniu usług na całym rynku wewnętrznym, ale także mogą mieć negatywny wpływ na konkurencję. Wynika to głównie z faktu, że w niektórych państwach członkowskich, lecz nie we wszystkich, za krytyczne uznaje się podobne rodzaje podmiotów świadczące podobne rodzaje usług. Oznacza to, że podmioty, które prowadzą lub chcą prowadzić działalność w więcej niż jednym państwie członkowskim, podlegają różnym obowiązkom, gdy działają na rynku wewnętrznym, oraz że podmioty prowadzące działalność w państwach członkowskich, w których obowiązują bardziej rygorystyczne wymogi, mogą napotykać trudności w porównaniu z podmiotami w państwach członkowskich o łagodniejszych ramach prawnych. Rozbieżności te są tak duże, że mają bezpośredni negatywny wpływ na funkcjonowanie rynku wewnętrznego.

- **Pomocniczość**

Wspólne ramy legislacyjne na szczeblu europejskim w tej dziedzinie uzasadnia współzależny, transgraniczny charakter relacji między działaniami w zakresie infrastruktury krytycznej a ich

wynikami, tj. usługami kluczowymi. Operator znajdujący się w jednym państwie członkowskim może bowiem świadczyć usługi w szeregu innych państw członkowskich lub w całej UE za pośrednictwem ściśle ze sobą powiązanych sieci. W związku z tym zakłócenie dotyczące tego operatora może mieć daleko idące skutki dla innych sektorów i ponad granicami państwowymi. Potencjalne ogólnoeuropejskie skutki zakłóceń wymagają podjęcia działań na szczeblu UE. Ponadto rozbieżne przepisy krajowe mają bezpośredni negatywny wpływ na funkcjonowanie rynku wewnętrznego. Jak wykazano w ocenie skutków, wiele państw członkowskich i zainteresowanych stron z branży dostrzega potrzebę zastosowania bardziej ujednoliconego i skoordynowanego podejścia europejskiego mającego na celu zapewnienie podmiotom wystarczającej odporności na poszczególne rodzaje ryzyka, które, choć nieco różne w poszczególnych państwach członkowskich, stwarzają wiele wspólnych wyzwań, którym nie można sprostać za pomocą środków krajowych lub na poziomie poszczególnych operatorów.

- **Proporcjonalność**

Wniosek jest proporcjonalny w stosunku do określonego celu nadrzędnego inicjatywy. Chociaż obowiązki państw członkowskich i podmiotów krytycznych mogą w niektórych przypadkach wiązać się z dodatkowymi obciążeniami administracyjnymi, np. jeżeli państwa członkowskie muszą opracować strategię krajową lub jeżeli podmioty krytyczne muszą wdrożyć pewne środki techniczne i organizacyjne, przewiduje się, że będą one zasadniczo ograniczone. W związku z tym należy zauważyć, że wiele podmiotów wprowadziło już pewne środki bezpieczeństwa w celu ochrony swojej infrastruktury i zapewnienia ciągłości działania.

W niektórych przypadkach osiągnięcie zgodności z dyrektywą może jednak wymagać większych inwestycji. Nawet w takich przypadkach inwestycje te mają jednak uzasadnienie, ponieważ przyczyniłyby się do zwiększenia odporności na poziomie operatora i odporności systemowej, a także do stosowania spójniejszego podejścia i zwiększenia zdolności do świadczenia niezawodnych usług w całej Unii. Ponadto jakiekolwiek dodatkowe obciążenia wynikające z dyrektywy będą najprawdopodobniej dużo mniejsze niż koszty związane z koniecznością zarządzania poważnymi zakłóceniami, które zagrażają nieprzerwanemu świadczeniu usług związanych z niezbędnymi funkcjami społecznymi i dobrobytem gospodarczym operatorów, poszczególnych państw członkowskich, Unii i, ogólniej rzecz ujmując, jej obywateli, oraz usuwania ich skutków.

- **Wybór instrumentu**

Wniosek ma formę dyrektywy w celu zapewnienia stosowania bardziej ujednoliconego podejścia do kwestii odporności podmiotów krytycznych w szeregu sektorów w całej Unii. We wniosku określono szczegółowe obowiązki właściwych organów w zakresie wskazywania podmiotów krytycznych w oparciu o wspólne kryteria i wyniki oceny ryzyka. W drodze dyrektywy można zapewnić, aby państwa członkowskie stosowały jednolite podejście do wskazywania podmiotów krytycznych, jednocześnie uwzględniając krajową specyfikę, w tym różne poziomy ekspozycji na ryzyko i współzależności między sektorami i ponad granicami.

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

- **Oceny ex post/oceny adekwatności obowiązującego prawodawstwa**

W 2019 r. przeprowadzono ewaluację dyrektywy w sprawie europejskiej infrastruktury krytycznej w celu oceny jej wdrożenia pod kątem adekwatności, spójności, skuteczności, efektywności, europejskiej wartości dodanej i trwałości[12].

W ocenie stwierdzono, że od czasu wejścia w życie dyrektywy kontekst uległ znacznej zmianie. W świetle tych zmian uznano, że dyrektywa jest jedynie częściowo adekwatna. Chociaż w ocenie przyznano, że dyrektywa jest zasadniczo zgodna z odpowiednimi europejskimi przepisami sektorowymi i polityką na szczeblu międzynarodowym, stwierdzono, że jest jedynie częściowo skuteczna ze względu na ogólny charakter niektórych jej przepisów. Stwierdzono, że dyrektywa wytworzyła europejską wartość dodaną, ponieważ przyniosła rezultaty (tj. wspólne ramy ochrony europejskiej infrastruktury krytycznej), których nie można by osiągnąć ani za pomocą krajowych, ani innych europejskich inicjatyw bez rozpoczęcia znacznie dłuższych, bardziej kosztownych i mniej wyraźnie określonych procesów. Stwierdzono jednak, że niektóre przepisy przyniosły wielu państwom członkowskim niewielką wartość dodaną.

Jeśli chodzi o trwałość, zakładano, że niektóre skutki dyrektywy (np. dyskusje transgraniczne, wymogi dotyczące sprawozdawczości) zanikną, jeśli dyrektywa zostanie uchylona, a nie zastąpiona. W ocenie stwierdzono, że państwa członkowskie nadal popierają zaangażowanie UE w działania na rzecz zwiększenia odporności infrastruktury krytycznej oraz że istnieją pewne obawy, iż całkowite uchylenie dyrektywy może mieć negatywne skutki w tej dziedzinie, a w szczególności dla ochrony wyznaczonych elementów europejskiej infrastruktury krytycznej. Państwom członkowskim zależało na zapewnieniu, aby zaangażowanie Unii w tej dziedzinie nadal było zgodne z zasadą pomocniczości, służyło wspieraniu środków na szczeblu krajowym oraz ułatwiało współpracę transgraniczną, w tym z państwami trzecimi.

- **Konsultacje z zainteresowanymi stronami**

Przy opracowywaniu niniejszego wniosku Komisja przeprowadziła konsultacje z wieloma różnymi zainteresowanymi stronami, w tym z: instytucjami i agencjami Unii Europejskiej; organizacjami międzynarodowymi; organami państw członkowskich; podmiotami prywatnymi, w tym indywidualnymi operatorami oraz krajowymi i europejskimi stowarzyszeniami branżowymi reprezentującymi operatorów z wielu różnych sektorów; ekspertami i sieciami ekspertów, w tym Europejską Siecią Referencyjną ds. Ochrony Infrastruktury Krytycznej (ERNCIP); przedstawicielami środowiska akademickiego; organizacjami pozarządowymi; i zwykłymi obywatelami.

Konsultacje z zainteresowanymi stronami przeprowadzono za pomocą różnych środków, w tym: publicznie dostępnej możliwości wyrażenia opinii na temat wstępnej oceny skutków dotyczącej niniejszego wniosku; seminariów konsultacyjnych; ukierunkowanych kwestionariuszy; dwustronnych dyskusji; oraz konsultacji publicznych (na potrzeby przeprowadzonej w 2019 r. oceny dyrektywy w sprawie europejskiej infrastruktury krytycznej).Ponadto wykonawca zewnętrzny odpowiedzialny za sporządzenie studium wykonalności, które uwzględniono w opracowaniu oceny skutków, przeprowadził konsultacje z wieloma zainteresowanymi stronami, np. za pomocą ankiety internetowej, pisemnego kwestionariusza, wywiadów indywidualnych oraz wirtualnych „wizyt w terenie” w 10 państwach członkowskich.

[12] SWD(2019) 310.

Komisja wykorzystała te konsultacje do zbadania poziomu skuteczności, efektywności, adekwatności, spójności i europejskiej wartości dodanej obowiązujących ram dotyczących odporności infrastruktury krytycznej (tj. sytuacji wyjściowej), problemów z nich wynikających, różnych wariantów strategicznych, które można rozważyć w celu rozwiązania tych problemów, oraz spodziewanych konkretnych skutków tych wariantów. Ogólnie rzecz biorąc, w wyniku konsultacji wskazano szereg obszarów, w których zainteresowane strony były ogólnie zgodne – w szczególności fakt, że ze względu na wzrost współzależności międzysektorowych i zmieniający się krajobraz zagrożeń należy zreorganizować obowiązujące unijne ramy dotyczące odporności infrastruktury krytycznej.

W szczególności zainteresowane strony były zasadniczo zgodne co do tego, że każde nowe podejście powinno być oparte na połączeniu środków wiążących i niewiążących, kłaść nacisk na odporność, a nie skupiać się na ochronie konkretnych składników infrastruktury, oraz w sposób bardziej wyraźny łączyć środki służące zwiększaniu odporności w zakresie cyberbezpieczeństwa ze środkami służącymi zwiększaniu odporności niezwiązanej z cyberbezpieczeństwem. Ponadto zainteresowane strony opowiedziały się za podejściem, które uwzględnia przepisy obowiązującego prawodawstwa sektorowego, obejmuje co najmniej te sektory, które wchodzą w zakres obowiązującej dyrektywy w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS), oraz za nakładaniem na szczeblu krajowym bardziej jednolitych obowiązków na podmioty krytyczne, które z kolei powinny mieć możliwość sprawowania wystarczającej kontroli bezpieczeństwa w odniesieniu do personelu posiadającego dostęp do obiektów o szczególnym znaczeniu/wrażliwych informacji. Ponadto zainteresowane strony zasugerowały, że każde nowe podejście powinno stwarzać państwom członkowskim możliwości sprawowania większego nadzoru nad działalnością podmiotów krytycznych, ale także gwarantować, aby podmioty krytyczne o znaczeniu dla całej Europy zostały wskazane i posiadały wystarczają odporność. Zainteresowane strony opowiedziały się również za zwiększeniem finansowania i wsparcia ze strony UE, np. w zakresie wdrażania jakichkolwiek nowych instrumentów, budowania zdolności na poziomie krajowym oraz koordynacji/współpracy publiczno-prywatnej, a także wymiany dobrych praktyk, wiedzy i know-how na różnych poziomach. Niniejszy wniosek zawiera przepisy, które zasadniczo odpowiadają poglądom i preferencjom wyrażonym przez zainteresowane strony.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Jak wspomniano w poprzedniej sekcji, przy opracowywaniu niniejszego wniosku Komisja korzystała w kontekście konsultacji z pomocy ekspertów zewnętrznych np. niezależnych ekspertów, sieci ekspertów i przedstawicieli środowiska akademickiego.

- **Ocena skutków**

W ocenie skutków, którą wykorzystano do opracowania niniejszej inicjatywy, rozważono różne warianty strategiczne mające na celu rozwiązanie opisanych wcześniej problemów ogólnych i szczegółowych. Poza sytuacją wyjściową, której utrzymanie nie wiązałoby się z żadnymi zmianami, warianty te obejmowały:

– Wariant 1: utrzymanie obowiązującej dyrektywy w sprawie europejskiej infrastruktury krytycznej, której towarzyszyłyby dobrowolne środki w kontekście istniejącego europejskiego programu ochrony infrastruktury krytycznej.

– Wariant 2: rewizja obowiązującej dyrektywy w sprawie europejskiej infrastruktury krytycznej w taki sposób, aby obejmowała te same sektory co obowiązująca dyrektywa w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS) oraz aby

bardziej skupiała się na odporności. Nowa dyrektywa w sprawie europejskiej infrastruktury krytycznej obejmowałaby zmiany w istniejącym transgranicznym procesie wyznaczania europejskiej infrastruktury krytycznej, w tym nowe kryteria wyznaczania, a także nowe wymogi dla państw członkowskich i operatorów.

– Wariant 3: zastąpienie obowiązującej dyrektywy w sprawie europejskiej infrastruktury krytycznej nowym instrumentem mającym na celu zwiększenie odporności podmiotów krytycznych w sektorach uznanych za niezbędne w proponowanej dyrektywie NIS 2. Wariant ten obejmowałby określenie minimalnych wymogów dla państw członkowskich i podmiotów krytycznych wskazanych zgodnie z nowymi ramami. Powstałaby procedura wskazywania podmiotów krytycznych oferujących usługi na rzecz wielu, jeżeli nie wszystkich, państw członkowskich UE lub w wielu, jeżeli nie we wszystkich, państwach członkowskich. We wdrożeniu przepisów pomagałoby specjalne centrum wiedzy działające w strukturach Komisji.

– Wariant 4: zastąpienie obowiązującej dyrektywy w sprawie europejskiej infrastruktury krytycznej nowym instrumentem mającym na celu zwiększenie odporności podmiotów krytycznych w sektorach uznanych za niezbędne w proponowanej dyrektywie NIS 2, a także przyznanie Komisji większej roli we wskazywaniu podmiotów krytycznych oraz utworzenie specjalnej agencji UE odpowiedzialnej za odporność infrastruktury krytycznej (która wypełniałaby role i obowiązki przypisane centrum wiedzy zaproponowanemu w poprzednim wariancie).

Po rozważeniu różnych skutków gospodarczych, społecznych i środowiskowych wynikających z poszczególnych wariantów, ale także wartości wariantów pod względem skuteczności, efektywności i proporcjonalności, w ocenie skutków stwierdzono, że najlepszym wariantem jest wariant 3. Warianty 1 i 2 nie przyniosłyby zmian wymaganych do rozwiązania problemu, a wariant 3 skutkowałby powstaniem zharmonizowanych i bardziej wszechstronnych ram odporności, które byłyby również dostosowane do prawa Unii obowiązującego w powiązanych dziedzinach i to prawo uwzględniały. Uznano również, że wariant 3 jest proporcjonalny i wydaje się, że jest politycznie wykonalny, ponieważ jest zgodny z oświadczeniami Rady i Parlamentu dotyczącymi potrzeby działania Unii w tej dziedzinie. Ponadto uznano, że wariant ten powinien zapewnić elastyczność i stworzyć dostosowane do przyszłych wyzwań ramy, które dadzą podmiotom krytycznym możliwości reagowania na różne rodzaje ryzyka w miarę upływu czasu. W ocenie skutków stwierdzono również, że wariant ten stanowiłby uzupełnienie istniejących ram i instrumentów sektorowych i międzysektorowych. Na przykład wariant ten umożliwia wyznaczonym podmiotom wypełniać określone zobowiązania przewidziane w tym nowym instrumencie poprzez wypełnianie zobowiązań przewidzianych w instrumentach już istniejących – w takim przypadku nie musiałyby one podejmować dalszych działań. Z drugiej strony musiałyby wprowadzić pewne środki, jeżeli zakres istniejących instrumentów nie obejmuje przedmiotowej kwestii lub ogranicza się jedynie do określonych rodzajów ryzyka lub środków.

Rada ds. Kontroli Regulacyjnej poddała kontroli ocenę skutków i w dniu 20 listopada 2020 r. wydała pozytywną opinię z zastrzeżeniami. Rada ds. Kontroli Regulacyjnej wskazała szereg elementów oceny skutków, na które należy zwrócić uwagę. W szczególności zwróciła się o dodatkowe wyjaśnienia na temat ryzyka związanego z infrastrukturą krytyczną i wymiarem transgranicznym, związku między inicjatywą a trwającą rewizją dyrektywy w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS) oraz związku między preferowanym

wariantem strategicznym a innymi aktami prawodawstwa sektorowego. Ponadto Rada ds. Kontroli Regulacyjnej dostrzegła potrzebę dalszego uzasadnienia rozszerzenia zakresu sektorowego instrumentu i zażądała dodatkowych informacji na temat kryteriów wyboru podmiotów krytycznych. Dodatkowo – jeżeli chodzi o proporcjonalność – Rada ds. Kontroli Regulacyjnej wniosła o udzielenie dodatkowych wyjaśnień dotyczących tego, w jaki sposób preferowany wariant miałby prowadzić do skuteczniejszych krajowych reakcji na ryzyko transgraniczne. Do tych oraz innych, bardziej szczegółowych uwag przekazanych przez Radę ds. Kontroli Regulacyjnej odniesiono się w wersji ostatecznej oceny skutków, w której na przykład opisano bardziej szczegółowo ryzyko transgraniczne ponoszone przez infrastruktury krytyczne oraz związek między niniejszym wnioskiem a wnioskiem dotyczącym dyrektywy NIS 2. Uwagi Rady ds. Kontroli Regulacyjnej uwzględniono również w proponowanej poniżej dyrektywie.

- **Sprawność regulacyjna i uproszczenie**

Zgodnie z programem sprawności i wydajności regulacyjnej (REFIT) Komisji wszystkie inicjatywy mające na celu zmianę istniejących przepisów UE powinny przyczyniać się do uproszczenia i skuteczniejszego osiągnięcia określonych celów polityki. Z ustaleń zawartych w ocenie skutków wynika, że wniosek powinien prowadzić do ograniczenia ogólnego obciążenia państw członkowskich. Lepsze dostosowanie do podejścia ukierunkowanego na usługi zastosowanego w obecnej dyrektywie w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS) może prowadzić z czasem do ograniczenia kosztów przestrzegania przepisów. Na przykład obciążający transgraniczny proces rozpoznawania i wyznaczania przewidziany w obecnie obowiązującej dyrektywie w sprawie europejskiej infrastruktury krytycznej zostałby zastąpiony procedurą opartą na analizie ryzyka na poziomie krajowym mającą na celu wyłącznie wskazanie podmiotów krytycznych podlegających różnym obowiązkom. W oparciu o ocenę ryzyka państwa członkowskie wskazywałyby podmioty krytyczne, z których większość jest już wyznaczonymi operatorami usług kluczowych na podstawie obecnej dyrektywy w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS).

Ponadto poprzez wdrażanie środków mających na celu zwiększenie swojej odporności podmioty krytyczne będą w mniejszym stopniu narażone na zakłócenia. W ten sposób ograniczone zostanie prawdopodobieństwo incydentów powodujących zakłócenia negatywnie wpływające na świadczenie usług kluczowych w poszczególnych państwach członkowskich i w całej Europie. Ta kwestia, wraz z pozytywnymi skutkami wynikającymi z harmonizacji rozbieżnych przepisów krajowych na poziomie Unii, miałaby pozytywny wpływ na przedsiębiorstwa, w tym na mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa, ogólną kondycję unijnej gospodarki oraz niezawodne funkcjonowanie rynku wewnętrznego.

- **Prawa podstawowe**

Celem proponowanych przepisów jest zwiększenie odporności podmiotów krytycznych świadczących różne formy usług kluczowych przy jednoczesnym wyeliminowaniu przeszkód regulacyjnych zakłócających ich zdolność do świadczenia swoich usług w całej Unii. Dzięki takim działaniom doszłoby do zmniejszenia ogólnego ryzyka zakłóceń na poziomie społeczeństwa i jednostki oraz do ograniczenia obciążenia. Przyczyniłoby się to do zapewnienia wyższego poziomu bezpieczeństwa publicznego, jednocześnie wywierając pozytywny wpływ na wolność działalności gospodarczej przedsiębiorstw, a także wielu innych podmiotów gospodarczych zależnych od świadczenia usług kluczowych, co w ostatecznym rozrachunku przyniosłoby korzyści konsumentom. Zawarte we wniosku przepisy mające na celu zapewnienie skutecznego zarządzania bezpieczeństwem pracowników będą standardowo obejmować przetwarzanie danych osobowych. Jest to

uzasadnione potrzebą sprawdzenia przeszłości w przypadku szczególnych kategorii personelu. Ponadto wszelkie przetwarzanie danych osobowych tego rodzaju będzie zawsze podlegać unijnym przepisom dotyczącym ochrony danych osobowych, w tym ogólnemu rozporządzeniu o ochronie danych[13].

4. WPŁYW NA BUDŻET

Proponowana dyrektywa ma wpływ finansowy na budżet Unii. Środki finansowe niezbędne do wsparcia wdrożenia niniejszego wniosku szacunkowo wynoszą łącznie 42,9 mln EUR w latach 2021–2027, z czego 5,1 mln EUR stanowią wydatki administracyjne. Koszty te można podzielić w następujący sposób:

– działania wspierające podejmowane przez Komisję,–w-tym rekrutacja, projekty, badania i działania wspierające;

– misje doradcze organizowane przez Komisję;

– regularne posiedzenia Grupy ds. Odporności Podmiotów Krytycznych, komitetu procedury komitetowej oraz inne posiedzenia.

Bardziej szczegółowe informacje są dostępne w ocenie skutków finansowych regulacji towarzyszącej niniejszemu wnioskowi.

5. ELEMENTY FAKULTATYWNE

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

Wdrożenie proponowanej dyrektywy zostanie poddane przeglądowi po upływie czterech i pół roku od dnia jej wejścia w życie, po czym Komisja przedłoży sprawozdanie dla Parlamentu Europejskiego i Rady. W sprawozdaniu tym dokonana zostanie ocena stopnia, w jakim państwa członkowskie przyjęły środki niezbędne do zapewnienia zgodności z dyrektywą. Komisja przedłoży Parlamentowi Europejskiemu i Radzie sprawozdanie oceniające wpływ i wartość dodaną dyrektywy w terminie sześciu lat od dnia wejścia dyrektywy w życie.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Przedmiot, zakres i definicje (art. 1–2)

W art. 1 określono przedmiot i zakres dyrektywy, w której nakłada się na państwa członkowskie obowiązki polegające na przyjmowaniu pewnych środków mających na celu zapewnienie świadczenia na rynku wewnętrznym usług koniecznych do utrzymania niezbędnych funkcji społecznych lub działalności gospodarczej, a w szczególności na wskazywaniu podmiotów krytycznych oraz umożliwianiu im dopełniania konkretnych obowiązków celem zwiększenia ich odporności i poprawy ich zdolności do świadczenia tych usług na rynku wewnętrznym. W dyrektywie ustanawia się również przepisy dotyczące nadzoru nad podmiotami krytycznymi i egzekwowania, aby stosowały one przepisy, a także dotyczące szczególnego nadzoru nad podmiotami krytycznymi uznawanymi za podmioty o szczególnym znaczeniu europejskim. W art. 1 wyjaśniono również związek między dyrektywą a innymi właściwymi aktami prawa Unii, a także określono warunki wymiany

[13] 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.

z Komisją i innymi właściwymi organami informacji, które są poufne zgodnie z przepisami unijnymi i krajowymi. W art. 2 zawarto wykaz obowiązujących definicji.

Krajowe ramy dotyczące odporności podmiotów krytycznych (art. 3–9)

W art. 3 przewidziano, że państwa członkowskie przyjmują strategię służącą wzmocnieniu odporności podmiotów krytycznych, opisano elementy, które taka strategia powinna zawierać, wyjaśniono, że należy ją aktualizować regularnie i w razie potrzeby, oraz określono, że państwa członkowskie przekazują swoje strategie i ich wszelkie aktualizacje Komisji. Art. 4 stanowi, że właściwe organy sporządzają wykaz usług kluczowych i regularnie dokonują oceny wszystkich istotnych czynników ryzyka, które mogą wpływać na świadczenie tych usług kluczowych, celem wskazania podmiotów krytycznych. W ocenie tej uwzględnia się oceny ryzyka przeprowadzone zgodnie z innymi właściwymi aktami prawa Unii, ryzyko wynikające z zależności między poszczególnymi sektorami oraz dostępne informacje na temat incydentów. Państwa członkowskie zapewniają, aby odpowiednie elementy oceny ryzyka zostały udostępnione podmiotom krytycznym, a dane dotyczące rozpoznanych rodzajów ryzyka oraz wyniki ich ocen ryzyka były regularnie udostępniane Komisji.

W art. 5 przewidziano, że państwa członkowskie wskazują podmioty krytyczne w poszczególnych sektorach i podsektorach. W procesie wskazywania należy uwzględnić wyniki oceny ryzyka oraz zastosować konkretne kryteria. Państwa członkowskie sporządzają wykaz podmiotów krytycznych, który podlega aktualizacji w razie potrzeby i regularnie. Podmioty krytyczne są należycie informowane o ich wskazaniu oraz wynikających z tego obowiązkach. Właściwe organy odpowiedzialne za wdrażanie dyrektywy informują właściwe organy odpowiedzialne za wdrażanie dyrektywy NIS 2 o wskazaniu podmiotów krytycznych. Gdy co najmniej dwa państwa członkowskie wskazały dany podmiot jako podmiot krytyczny, państwa członkowskie przystępują do wzajemnych konsultacji w celu ograniczenia obciążenia podmiotu krytycznego. W przypadku gdy podmioty krytyczne świadczą usługi na rzecz ponad jednej trzeciej lub w ponad jednej trzeciej państw członkowskich, odnośne państwo członkowskie przekazuje Komisji dane identyfikacyjne tych podmiotów krytycznych.

W art. 6 zawarto definicję pojęcia „istotnego skutku zakłócającego”, o którym mowa w art. 5 ust. 2, oraz przewidziano wymóg, zgodnie z którym państwa członkowskie przekazują Komisji pewne rodzaje informacji dotyczących wskazanych przez nie podmiotów krytycznych oraz sposobu ich wskazania. Dodatkowo w art. 6 upoważniono Komisję do przyjmowania odpowiednich wytycznych po konsultacji z Grupą ds. Odporności Podmiotów Krytycznych.

Art. 7 stanowi, że państwa członkowskie powinny wskazać podmioty w sektorze bankowym, sektorze infrastruktury rynku finansowego oraz sektorze infrastruktury cyfrowej, które mają być traktowane jako równoważne z podmiotami krytycznymi wyłącznie do celów rozdziału II. Podmioty te należy poinformować o ich wskazaniu.

Zgodnie z art. 8 każde państwo członkowskie wyznacza co najmniej jeden właściwy organ odpowiedzialny za prawidłowe stosowanie dyrektywy na szczeblu krajowym, któremu zapewnia odpowiednie zasoby, oraz pojedynczy punkt kontaktowy odpowiedzialny za zapewnianie współpracy transgranicznej. Pojedynczy punkt kontaktowy regularnie przekazuje Komisji sprawozdanie podsumowujące dotyczące zgłaszania incydentów. W art. 8 zawarto wymóg, zgodnie z którym właściwe organy odpowiedzialne za stosowanie dyrektywy

współpracują z innymi odpowiednimi organami krajowymi, w tym z właściwymi organami wyznaczonymi na podstawie dyrektywy NIS 2. Art. 9 stanowi, że państwa członkowskie wspierają podmioty krytyczne w zapewnianiu ich odporności oraz ułatwiają współpracę i dobrowolną wymianę informacji i dobrych praktyk między właściwymi organami a podmiotami krytycznymi.

Odporność podmiotów krytycznych (art. 10–13)

Zgodnie z art. 10 podmioty krytyczne dokonują regularnej oceny wszystkich istotnych czynników ryzyka w oparciu o krajową ocenę ryzyka i inne odpowiednie źródła informacji. Art. 11 stanowi, że podmioty krytyczne wprowadzają odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zapewnienia swojej odporności, a także zapewniają, aby środki te były opisane w planie zwiększania odporności lub równoważnym dokumencie/równoważnych dokumentach. Państwa członkowskie mogą wnieść o to, aby Komisja zorganizowała misje doradcze celem zapewnienia podmiotom krytycznym doradztwa w zakresie dopełniania ich obowiązków. W art. 11 upoważniono również Komisję do przyjmowania w stosownych przypadkach aktów delegowanych i wykonawczych.

Art. 12 stanowi, że państwa członkowskie zapewniają, aby podmioty krytyczne mogły składać wnioski o sprawdzenie przeszłości osób, które należą lub mogą zacząć należeć do pewnych szczególnych kategorii personelu, a także aby organy odpowiedzialne za sprawdzanie przeszłości dokonywały sprawnej oceny takich wniosków. W artykule tym opisano cel, zakres i elementy składowe sprawdzenia przeszłości, przy czym wszystkie te aspekty muszą być zgodne z ogólnym rozporządzeniem o ochronie danych.

Art. 13 stanowi, że państwa członkowskie zapewniają, aby podmioty krytyczne zgłaszały właściwemu organowi incydenty, które w znacznym stopniu zakłócają lub mogą potencjalnie w znacznym stopniu zakłócać ich funkcjonowanie. Właściwe organy przekazują z kolei zgłaszającym podmiotom krytycznym odpowiednie informacje na temat działań następczych. Za pośrednictwem pojedynczego punktu kontaktowego właściwe organy informują również pojedyncze punkty kontaktowe w innych zainteresowanych państwach członkowskich w przypadku, gdy incydent ma lub może mieć wpływ transgraniczny w co najmniej jednym innym państwie członkowskim.

Szczególny nadzór nad podmiotami krytycznymi o szczególnym znaczeniu europejskim (art. 14–15)

W art. 14 podmioty krytyczne o szczególnym znaczeniu europejskim zdefiniowano jako podmioty, które wskazano jako podmioty krytyczne i które świadczą usługi kluczowe na rzecz ponad jednej trzeciej lub w ponad jednej trzeciej państw członkowskich. Po otrzymaniu zgłoszenia na podstawie art. 5 ust. 6 Komisja informuje podmiot, którego to dotyczy, że uznaje się go za podmiot krytyczny o szczególnym znaczeniu europejskim, o wynikających z tego obowiązkach oraz o dacie, od której obowiązki zaczynają mieć zastosowanie. W art. 15 opisano ustalenia dotyczące szczególnego nadzoru mające zastosowanie do podmiotów krytycznych o szczególnym znaczeniu europejskim, które to ustalenia obejmują przekazywanie Komisji i Grupie ds. Odporności Podmiotów Krytycznych – na wniosek – informacji na temat oceny ryzyka, o której mowa w art. 10, oraz środków wdrożonych zgodnie z art. 11, a także na temat wszelkich działań z zakresu nadzoru lub egzekwowania ze strony państwa członkowskiego, w którym znajduje się infrastruktura. Art. 15 stanowi również, że Komisja może organizować misje doradcze celem dokonania oceny środków wdrożonych przez poszczególne podmioty krytyczne o szczególnym znaczeniu europejskim.

W oparciu o analizę ustaleń misji doradczej przeprowadzoną przez Grupę ds. Odporności Podmiotów Krytycznych Komisja przekazuje państwu członkowskiemu, w którym znajduje się infrastruktura podmiotu, swoje uwagi na temat tego, czy podmiot ten wywiązuje się ze swoich obowiązków, oraz – w stosownych przypadkach – jakie środki można wprowadzić, aby zwiększyć odporność tego podmiotu. W artykule tym opisano skład, organizację i finansowanie misji doradczych. Stanowi on również, że Komisja przyjmuje akt wykonawczy ustanawiający przepisy dotyczące ustaleń proceduralnych na potrzeby prowadzenia misji doradczych i opracowywania sprawozdań z tych misji.

Współpraca i sprawozdawczość (art. 16–17)

W art. 16 opisano rolę i zadania Grupy ds. Odporności Podmiotów Krytycznych, która składa się z przedstawicieli państw członkowskich i Komisji. Grupa wspiera Komisję i ułatwia współpracę strategiczną oraz wymianę informacji. W artykule tym wyjaśniono, że Komisja może przyjmować akty wykonawcze określające ustalenia proceduralne niezbędne do funkcjonowania Grupy ds. Odporności Podmiotów Krytycznych. Art. 17 stanowi, że Komisja w stosownych przypadkach udziela państwom członkowskim i podmiotom krytycznym wsparcia w wywiązywaniu się z ich obowiązków wynikających z niniejszej dyrektywy i uzupełnia działania państw członkowskich, o których mowa w art. 9.

Nadzór i egzekwowanie (art. 18–19)

W art. 18 przewidziano, że państwa członkowskie dysponują pewnymi uprawnieniami i środkami oraz że spoczywają na nich pewne obowiązki w zakresie zapewniania wdrożenia i egzekwowania dyrektywy. Państwa członkowskie zapewniają, aby w przypadku, gdy właściwy organ przeprowadza ocenę zgodności dotyczącą podmiotu krytycznego, informował on właściwe organy odnośnego państwa członkowskiego wyznaczone zgodnie z dyrektywą NIS 2 oraz mógł zwrócić się do tych organów o ocenę cyberbezpieczeństwa takiego podmiotu, a także by współpracował i wymieniał informacje w tym celu. Art. 19 stanowi, że zgodnie z ugruntowaną praktyką państwa członkowskie określają zasady dotyczące sankcji za naruszanie przepisów i podejmują wszystkie konieczne działania w celu zapewnienia ich wdrożenia.

Przepisy końcowe (art. 20–26)

Art. 20 stanowi, że Komisję wspiera komitet w rozumieniu rozporządzenia (UE) nr 182/2011. Jest to standardowy artykuł. W art. 21 nadano Komisji uprawnienie do przyjmowania aktów delegowanych na warunkach określonych w tym artykule. Jest to również standardowy artykuł. W art. 22 określono, że Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie oceniające, w jakim stopniu państwa członkowskie przyjęły środki niezbędne do zapewnienia zgodności z dyrektywą. Sprawozdanie oceniające wpływ i wartość dodaną dyrektywy oraz to, czy zakres dyrektywy należy rozszerzyć o inne sektory lub podsektory, w tym sektor produkcji, przetwarzania i dystrybucji żywności, należy przedkładać regularnie Parlamentowi Europejskiemu i Radzie.

Art. 23 stanowi, że dyrektywa 2008/114/WE traci moc ze skutkiem od dnia rozpoczęcia stosowania niniejszej dyrektywy. Zgodnie z art. 24 państwa członkowskie przyjmują i publikują – w określonym terminie – przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania dyrektywy i informują o tym Komisję. Tekst podstawowych przepisów prawa krajowego przyjętych w dziedzinie objętej niniejszą dyrektywą przekazuje się Komisji. Art. 25 stanowi, że niniejsza dyrektywa wchodzi w życie dwudziestego dnia po

jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*. Art. 26 stanowi, że dyrektywa jest skierowana do państw członkowskich.

2020/0365 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie odporności podmiotów krytycznych

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[14],

uwzględniając opinię Komitetu Regionów[15],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą[16],

a także mając na uwadze, co następuje:

(1) Dyrektywa Rady 2008/114/WE[17] przewiduje procedurę wyznaczania europejskich infrastruktur krytycznych w sektorach energii i transportu, których zakłócenie lub zniszczenie miałoby istotny wpływ transgraniczny w co najmniej dwóch państwach członkowskich. W dyrektywie tej skoncentrowano się wyłącznie na ochronie takich infrastruktur. Ocena dyrektywy 2008/114/WE przeprowadzona w 2019 r.[18] wykazała jednak, że ze względu na w coraz większym stopniu wzajemnie powiązany i transgraniczny charakter operacji wykorzystujących infrastrukturę krytyczną środki ochronne związane wyłącznie z pojedynczymi składnikami infrastruktury są niewystarczające, aby zapobiec wszystkim zakłóceniom. Wobec tego niezbędna jest zmiana podejścia na podejście zapewniające odporność podmiotów krytycznych, a mianowicie ich zdolność do łagodzenia i tłumienia incydentów mogących zakłócić funkcjonowanie podmiotu krytycznego oraz dostosowania się do nich i usunięcia ich skutków.

(2) Mimo istniejących środków na poziomie unijnym[19] i krajowym mających na celu wsparcie ochrony infrastruktur krytycznych w Unii podmioty będące operatorami tych infrastruktur nie są odpowiednio przygotowane do reagowania na obecne i przewidywane ryzyko dla ich funkcjonowania, które może prowadzić do zakłóceń świadczenia usług koniecznych do pełnienia niezbędnych funkcji społecznych lub prowadzenia niezbędnej działalności gospodarczej. Wynika to z dynamicznego krajobrazu zagrożeń charakteryzującego się rozwijającym się zagrożeniem

---

14 Dz.U. C […] z , s. .

15 Dz.U. C […] z […], s. […].

16 Stanowisko Parlamentu Europejskiego [...] i Rady [...].

17 Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.U. L 345 z 23.12.2008, s. 75).

18 SWD(2019) 308.

19 Europejski program ochrony infrastruktury krytycznej.

terrorystycznym i rosnącymi współzależnościami między infrastrukturami i sektorami, a także ze zwiększonego fizycznego ryzyka związanego z klęskami żywiołowymi i zmianą klimatu, które przyczynia się do zwiększenia częstotliwości i skali ekstremalnych zdarzeń pogodowych i wywołuje długoterminowe zmiany średnich warunków klimatycznych, co może ograniczyć zdolność i skuteczność niektórych rodzajów infrastruktury, jeżeli nie zostaną wdrożone środki z zakresu odporności lub przystosowania się do zmiany klimatu. Ponadto odpowiednich sektorów i rodzajów podmiotów nie uznaje się konsekwentnie za krytyczne we wszystkich państwach członkowskich.

(3) Te rosnące współzależności są rezultatem w coraz większym stopniu transgranicznej i współzależnej sieci świadczenia usług wykorzystującej kluczowe infrastruktury w całej Unii w sektorach energii, transportu, bankowości, infrastruktury rynku finansowego, infrastruktury cyfrowej, wody pitnej i ścieków, zdrowia, niektórych aspektów administracji publicznej, a także w sektorze kosmicznym – w zakresie obejmującym świadczenie niektórych usług zależnych od naziemnych infrastruktur, których właścicielami są, którymi zarządzają i które obsługują albo państwa członkowskie, albo podmioty prywatne, czyli z pominięciem infrastruktur, których właścicielem jest, którymi zarządza lub które obsługuje Unia lub odbywa się to w jej imieniu w ramach unijnych programów kosmicznych. Współzależności te oznaczają, że jakiekolwiek zakłócenie – nawet takie, które początkowo ogranicza się do jednego podmiotu lub jednego sektora – może wywołać szerzej zakrojony efekt kaskadowy, potencjalnie prowadzący do daleko idącego i długotrwałego negatywnego wpływu na świadczenie usług na rynku wewnętrznym. Pandemia COVID-19 uwidoczniła podatność naszych w coraz większym stopniu współzależnych społeczeństw w obliczu mało prawdopodobnego ryzyka.

(4) Podmioty zaangażowane w świadczenie usług kluczowych w coraz większym stopniu podlegają zróżnicowanym wymaganiom nakładanym na nie na gruncie prawa państw członkowskich. Fakt, iż niektóre państwa członkowskie mają mniej surowe wymagania w zakresie bezpieczeństwa względem tych podmiotów, może nie tylko negatywnie wpływać na utrzymanie niezbędnych funkcji społecznych lub działalności gospodarczej w Unii, lecz prowadzi również do powstania przeszkód dla prawidłowego funkcjonowania rynku wewnętrznego. W niektórych państwach członkowskich, lecz nie we wszystkich, za krytyczne uznaje się podobne rodzaje podmiotów, a podmioty wskazane jako krytyczne podlegają zróżnicowanym wymaganiom w poszczególnych państwach członkowskich. Prowadzi to do powstania dodatkowego i zbędnego obciążenia administracyjnego dla przedsiębiorstw prowadzących działalność transgraniczną, w szczególności dla przedsiębiorstw działających w państwach członkowskich o surowszych wymaganiach.

(5) Konieczne jest zatem wprowadzenie zharmonizowanych norm minimalnych celem zapewnienia świadczenia usług kluczowych na rynku wewnętrznym oraz zwiększenia odporności podmiotów krytycznych.

(6) Aby osiągnąć ten cel, państwa członkowskie powinny wskazać podmioty krytyczne, które z kolei powinny podlegać szczególnym wymogom i nadzorowi, otrzymując jednak również szczególne wsparcie i wytyczne mające na celu osiągnięcie wysokiego poziomu odporności w obliczu wszystkich istotnych czynników ryzyka.

(7) Niektóre sektory gospodarki, takie jak sektory energii i transportu, są już regulowane lub mogą być w przyszłości regulowane sektorowymi aktami prawa Unii, które zawierają przepisy dotyczące niektórych aspektów odporności podmiotów

prowadzących działalność w tych sektorach. Aby podejść do kwestii odporności tych podmiotów, które są krytyczne dla prawidłowego funkcjonowania rynku wewnętrznego, w sposób kompleksowy, wspomniane środki sektorowe należy uzupełnić środkami przewidzianymi w niniejszej dyrektywie, która tworzy nadrzędne ramy dotyczące odporności podmiotów krytycznych na wszystkie zagrożenia, to znaczy zagrożenia naturalne i spowodowane przez człowieka, przypadkowe i zamierzone.

(8) Biorąc pod uwagę znaczenie cyberbezpieczeństwa z punktu widzenia odporności podmiotów krytycznych oraz mając na względzie spójność, niezbędne jest, aby w miarę możliwości zachować spójne podejście między niniejszą dyrektywą a dyrektywą Parlamentu Europejskiego i Rady (UE) XX/YY[20] [proponowaną dyrektywą w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dalej „dyrektywa NIS 2")]. Ze względu na większą częstotliwość i szczególny charakter ryzyka w cyberprzestrzeni dyrektywą NIS 2 nakłada się kompleksowe wymagania na dużą grupę podmiotów celem zapewnienia ich cyberbezpieczeństwa. Zważywszy że w dyrektywie NIS 2 w wystarczający sposób uregulowano kwestię cyberbezpieczeństwa, aspekty regulowane przez tę dyrektywę należy wykluczyć z zakresu niniejszej dyrektywy, bez uszczerbku dla szczególnych uregulowań dotyczących podmiotów w sektorze infrastruktury cyfrowej.

(9) Jeżeli w przepisach innych aktów prawnych Unii nałożono na podmioty krytyczne obowiązek oceny istotnego ryzyka, zastosowania środków zapewniających ich odporność lub zgłaszania incydentów, a wymagania te są co najmniej równoważne z odpowiadającymi im obowiązkami przewidzianymi w niniejszej dyrektywie, odpowiednie przepisy niniejszej dyrektywy nie powinny mieć zastosowania, co pozwoli uniknąć powielania i zbędnego obciążenia. W takim przypadku należy stosować odpowiednie przepisy wspomnianych aktów. Jeżeli odpowiednie przepisy niniejszej dyrektywy nie mają zastosowania, jej przepisów dotyczących nadzoru i egzekwowania również nie należy stosować. Państwa członkowskie powinny jednak uwzględnić wszystkie sektory umieszczone w zawartym w załączniku wykazie w swojej strategii mającej na celu wzmocnienie odporności podmiotów krytycznych, ocenie ryzyka i działaniach wspierających, o których mowa w rozdziale II, oraz być w stanie wskazać podmioty krytyczne w tych sektorach, w których spełnione zostały obowiązujące warunki, biorąc przy tym pod uwagę szczególne uregulowania dotyczące podmiotów w sektorach bankowości, infrastruktury rynku finansowego i infrastruktury cyfrowej.

(10) W celu zapewnienia kompleksowego podejścia do odporności podmiotów krytycznych każde państwo członkowskie powinno dysponować strategią określającą cele i środki z zakresu polityki, które należy wdrożyć. Aby to osiągnąć, państwa członkowskie powinny zapewnić, aby ich strategie dotyczące cyberbezpieczeństwa przewidywały ramy polityczne umożliwiające zwiększoną koordynację między właściwymi organami, o których mowa w niniejszej dyrektywie i w dyrektywie NIS 2, w zakresie wymiany informacji na temat incydentów i cyberzagrożeń oraz wykonywania zadań nadzorczych.

(11) Podstawą działań państw członkowskich mających na celu wskazanie i przyczynienie się do zapewnienia odporności podmiotów krytycznych powinno być podejście oparte

[20] [Odniesienie do dyrektywy NIS 2, po jej przyjęciu].

na analizie ryzyka, w ramach którego starania skupiają się na podmiotach najważniejszych dla pełnienia niezbędnych funkcji społecznych lub prowadzenia niezbędnej działalności gospodarczej. W celu zapewnienia takiego ukierunkowanego podejścia każde państwo członkowskie powinno przeprowadzić – w zharmonizowanych ramach – ocenę wszystkich istotnych zagrożeń, naturalnych i spowodowanych przez człowieka, które mogą wpływać na świadczenie usług kluczowych, w tym wypadków, klęsk żywiołowych, stanów zagrożenia zdrowia publicznego, takich jak pandemie, oraz zagrożeń związanych z konfliktem, w tym przestępstw terrorystycznych. Dokonując takich ocen ryzyka, państwa członkowskie powinny uwzględnić inne ogólne lub sektorowe oceny ryzyka przeprowadzone na podstawie innych aktów prawa Unii oraz powinny wziąć pod uwagę zależności między sektorami, w tym sektorami z innych państw członkowskich i państw trzecich. Wyniki oceny ryzyka należy wykorzystać w procesie wskazywania podmiotów krytycznych i wspierania tych podmiotów w spełnianiu wymogów dotyczących odporności przewidzianych w niniejszej dyrektywie.

(12) W celu zapewnienia, aby wszystkie odpowiednie podmioty były objęte tymi wymogami, i w celu ograniczenia rozbieżności w tym zakresie należy wprowadzić zharmonizowane przepisy pozwalające na spójne wskazywanie podmiotów krytycznych na terenie Unii, umożliwiając przy tym państwom członkowskim odzwierciedlenie ich krajowej specyfiki. Należy zatem określić kryteria dotyczące wskazywania podmiotów krytycznych. Przez wzgląd na skuteczność, efektywność, spójność oraz pewność prawa należy ustanowić również odpowiednie przepisy dotyczące zgłaszania i współpracy w związku z takim wskazywaniem oraz jego skutki prawne. W celu umożliwienia Komisji oceny prawidłowego stosowania niniejszej dyrektywy państwa członkowskie powinny przekazać Komisji, w sposób jak najbardziej szczegółowy i konkretny, odpowiednie informacje i, w każdym wypadku, wykaz podmiotów krytycznych, liczbę podmiotów krytycznych wskazanych w każdym sektorze i podsektorze, o których mowa w załączniku, oraz usługę kluczową lub usługi kluczowe, które świadczy każdy z tych podmiotów, a także wszelkie zastosowane progi.

(13) Dodatkowo należy ustanowić kryteria umożliwiające określenie znaczenia skutku zakłócającego wywołanego przez takie incydenty. Kryteria te powinny opierać się na kryteriach przewidzianych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148[21] w celu wykorzystania starań, jakie państwa członkowskie włożyły we wskazanie tych operatorów, oraz doświadczenia zdobytego w tym zakresie.

(14) Podmioty związane z sektorem infrastruktury cyfrowej opierają się w istocie na sieci i na systemach informatycznych oraz wchodzą w zakres stosowania dyrektywy NIS 2, która reguluje kwestię bezpieczeństwa fizycznego takich systemów w ramach ich obowiązku zarządzania ryzykiem w cyberprzestrzeni i obowiązku sprawozdawczego. Ponieważ aspekty te reguluje dyrektywa NIS 2, obowiązki przewidziane w niniejszej dyrektywie nie mają zastosowania do takich podmiotów. Niemniej biorąc pod uwagę znaczenie usług świadczonych przez podmioty w sektorze infrastruktury cyfrowej dla świadczenia innych usług kluczowych, państwa członkowskie powinny wskazać – na podstawie kryteriów i z wykorzystaniem procedury przewidzianych odpowiednio w niniejszej dyrektywie – podmioty związane z sektorem infrastruktury cyfrowej,

[21] 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).

które należy traktować jako równoważne z podmiotami krytycznymi wyłącznie do celów rozdziału II, w tym udzielić tym podmiotom wsparcia w zwiększaniu ich odporności. W rezultacie takie podmioty nie powinny podlegać obowiązkom określonym w rozdziałach III–VI. Ponieważ obowiązki podmiotów krytycznych przewidziane w rozdziale II i polegające na przekazywaniu pewnych informacji właściwym organom są związane ze stosowaniem rozdziałów III–IV, wspomniane podmioty nie powinny podlegać również tym obowiązkom.

(15) W dorobku prawnym UE dotyczącym usług finansowych ustanowiono kompleksowe wymagania względem podmiotów finansowych polegające na zarządzaniu wszystkimi czynnikami ryzyka, z jakimi się zmagają, w tym ryzykiem operacyjnym, oraz zapewnieniu ciągłości działania. Obejmuje on rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012[22], dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE[23] i rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014[24], a także rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013[25] i dyrektywę Parlamentu Europejskiego i Rady 2013/36/UE[26]. Niedawno Komisja zaproponowała uzupełnienie tych ram rozporządzeniem Parlamentu Europejskiego i Rady XX/YYYY [proponowane rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego (dalej „rozporządzenie DORA")[27]], w którym określono wymagania względem przedsiębiorstw finansowych dotyczące zarządzania ryzykiem związanym z ICT, w tym ochrony fizycznych infrastruktur ICT. Ponieważ odporność podmiotów wymienionych w załączniku pkt 3 i 4 jest kompleksowo uregulowana w dorobku prawnym UE dotyczącym usług finansowych, podmioty te również należy traktować jako równoważne z podmiotami krytycznymi wyłącznie do celów rozdziału II niniejszej dyrektywy. Aby zapewnić spójne stosowanie przepisów dotyczących ryzyka operacyjnego i odporności cyfrowej w sektorze finansowym, wsparcia ze strony państw członkowskich w zwiększaniu ogólnej odporności podmiotów finansowych równoważnych z podmiotami krytycznymi powinny udzielać organy wyznaczone zgodnie z art. 41 [rozporządzenia DORA] oraz powinno ono podlegać procedurom określonym w tych przepisach w sposób w pełni zharmonizowany.

(16) Państwa członkowskie powinny wyznaczyć organy odpowiedzialne za nadzór nad stosowaniem przepisów niniejszej dyrektywy i, w stosownych przypadkach, za ich

---

22 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz.U. L 201 z 27.7.2012, s. 1).

23 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).

24 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 173 z 12.6.2014, s. 84).

25 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 176 z 27.6.2013, s. 1).

26 Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.U. L 176 z 27.6.2013, s. 338).

27 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014 – COM(2020) 595.

egzekwowanie oraz zapewnić, aby organy te dysponowały odpowiednimi uprawnieniami i zasobami. Z uwagi na różnice w krajowych strukturach zarządzania oraz w celu zabezpieczenia obowiązujących już ustaleń sektorowych lub unijnych organów nadzorczych i regulacyjnych, a także w celu unikania powielania państwa członkowskie powinny móc wyznaczać więcej niż jeden właściwy organ. W takim wypadku powinny one jednak wyraźnie rozgraniczyć odpowiednie zadania tych organów oraz zapewnić, aby organy te współpracowały ze sobą w sposób płynny i skuteczny. Wszystkie właściwe organy powinny również współpracować w ujęciu bardziej ogólnym z innymi właściwymi organami, zarówno na szczeblu krajowym, jak i szczeblu unijnym.

(17) W celu ułatwienia współpracy i komunikacji transgranicznej oraz umożliwienia skutecznego wdrożenia niniejszej dyrektywy każde państwo członkowskie powinno, bez uszczerbku dla unijnych wymogów prawnych dotyczących danego sektora, wyznaczyć – w ramach jednego z organów wskazanych jako właściwe organy na podstawie niniejszej dyrektywy – pojedynczy punkt kontaktowy odpowiedzialny za koordynację kwestii związanych z odpornością podmiotów krytycznych oraz współpracę transgraniczną na poziomie Unii w tym zakresie.

(18) Zważywszy, że zgodnie z dyrektywą NIS 2 podmioty wskazane jako podmioty krytyczne, a także podmioty wskazane w sektorze infrastruktury cyfrowej, które należy traktować jako równoważne na podstawie niniejszej dyrektywy, podlegają wymaganiom dotyczącym cyberbezpieczeństwa przewidzianym w dyrektywie NIS 2, właściwe organy wyznaczone na podstawie obu tych dyrektyw powinny ze sobą współpracować, w szczególności w odniesieniu do ryzyka w cyberprzestrzeni i incydentów mających wpływ na te podmioty.

(19) Państwa członkowskie powinny wspierać podmioty krytyczne we wzmacnianiu ich odporności, zgodnie z ich obowiązkami przewidzianymi w niniejszej dyrektywie, bez uszczerbku dla własnej odpowiedzialności prawnej podmiotów za zapewnienie takiej zgodności. Państwa członkowskie mogłyby w szczególności opracować materiały zawierające wytyczne i metodyki, wspierać organizację działań mających na celu sprawdzenie ich odporności oraz zapewnić szkolenia personelu podmiotów krytycznych. Ponadto biorąc pod uwagę współzależności między podmiotami i sektorami, państwa członkowskie powinny ustanowić narzędzia służące do wymiany informacji, aby wspierać dobrowolną wymianę informacji między podmiotami krytycznymi, bez uszczerbku dla zastosowania reguł konkurencji ustanowionych w Traktacie o funkcjonowaniu Unii Europejskiej.

(20) Aby móc zapewnić swoją odporność, podmioty krytyczne powinny mieć kompleksowe wyobrażenie na temat wszystkich istotnych czynników ryzyka, na które są narażone, oraz je analizować. W tym celu powinny przeprowadzać oceny ryzyka, gdy tylko jest to konieczne ze względu na ich szczególne okoliczności oraz zmianę tych czynników ryzyka, a w każdym wypadku co cztery lata. Oceny ryzyka prowadzone przez podmioty krytyczne powinny opierać się na ocenie ryzyka przeprowadzonej przez państwa członkowskie.

(21) Podmioty krytyczne powinny zastosować środki organizacyjne i techniczne odpowiednie i proporcjonalne do ryzyka, na które są narażone, aby zapobiegać incydentowi, stawiać mu opór, złagodzić i stłumić go oraz dostosować się do niego i usunąć jego skutki. Mimo iż podmioty krytyczne powinny zastosować środki w odniesieniu do wszystkich punktów określonych w niniejszej dyrektywie, szczegóły i zakres tych środków powinny odzwierciedlać poszczególne czynniki ryzyka

rozpoznane przez każdy z podmiotów w ramach jego oceny ryzyka oraz specyfikę takiego podmiotu w sposób odpowiedni i proporcjonalny.

(22) W trosce o skuteczność i odpowiedzialność podmioty krytyczne powinny opisać wspomniane środki – stosując taki poziom szczegółowości, aby wystarczająco osiągnąć te cele, i biorąc pod uwagę rozpoznane czynniki ryzyka – w planie zwiększania odporności lub dokumencie/dokumentach równoważnych z planem zwiększania odporności oraz wprowadzać ten plan w życie. Taki równoważny dokument lub takie równoważne dokumenty można sporządzić zgodnie z wymaganiami i normami opracowanymi w kontekście umów międzynarodowych w sprawie ochrony fizycznej, których państwa członkowskie są stronami, w tym w stosownych przypadkach Konwencji o ochronie fizycznej materiałów jądrowych i obiektów jądrowych.

(23) Rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 300/2008[28], rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 725/2004[29] oraz dyrektywą Parlamentu Europejskiego i Rady 2005/65/WE[30] ustanowiono wymagania mające zastosowanie do podmiotów w sektorach transportu lotniczego i transportu morskiego w celu zapobieżenia incydentom powodowanym bezprawnymi czynami oraz stawienia oporu skutkom takich incydentów i ograniczenia tych skutków. Chociaż środki wymagane zgodnie z niniejszą dyrektywą są ogólniejsze pod kątem czynników ryzyka, których dotyczą, i rodzajów środków, które należy wdrożyć, podmioty krytyczne w tych sektorach powinny odzwierciedlić w swoim planie zwiększania odporności lub równoważnych dokumentach środki wdrożone na podstawie wspomnianych innych aktów Unii. Ponadto podczas wdrażania środków na rzecz zwiększania odporności zgodnie z niniejszą dyrektywą podmioty krytyczne mogą rozważyć odniesienie się do niewiążących dokumentów zawierających wytyczne i dobre praktyki opracowanych w ramach sektorowych grup roboczych, takich jak unijna platforma bezpieczeństwa pasażerów w ruchu kolejowym[31].

(24) Ryzyko, że pracownicy podmiotów krytycznych nadużyją na przykład swoich praw dostępu w ramach organizacji podmiotu w celu wyrządzenia szkody, budzi coraz większe obawy. Ryzyko to zwiększa się wraz z przybierającym na sile zjawiskiem radykalizacji prowadzącym do brutalnego ekstremizmu i terroryzmu. Wobec tego niezbędne jest umożliwienie podmiotom krytycznym wnoszenia o sprawdzenie przeszłości osób należących do szczególnych kategorii ich personelu oraz zapewnienie, aby właściwe organy dokonywały sprawnej oceny takich wniosków, zgodnie z obowiązującymi przepisami unijnymi i krajowymi, w tym dotyczącymi ochrony danych osobowych.

(25) Podmioty krytyczne powinny zgłaszać tak szybko, jak jest to racjonalnie możliwe w danych okolicznościach, właściwym organom państw członkowskich incydenty, które w znacznym stopniu zakłócają lub mogą potencjalnie w znacznym stopniu

---

28 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (Dz.U. L 97 z 9.4.2008, s. 72).

29 Rozporządzenie (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie wzmocnienia ochrony statków i obiektów portowych, Dz.U. L 129 z 29.4.2004, s. 6.

30 Dyrektywa 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów (Dz.U. L 310 z 25.11.2005, s. 28).

31 Decyzja Komisji z dnia 29 czerwca 2018 r. w sprawie utworzenia unijnej platformy bezpieczeństwa pasażerów w ruchu kolejowym, C/2018/4014.

zakłócać ich funkcjonowanie. Zgłoszenie powinno umożliwiać właściwym organom szybką i adekwatną reakcję na incydenty oraz uzyskanie kompleksowego wyobrażenia na temat wszystkich czynników ryzyka, na które podmioty krytyczne są narażone. W tym celu należy ustanowić procedurę zgłaszania określonych incydentów oraz określić parametry umożliwiające ustalenie, kiedy rzeczywiste lub potencjalne zakłócenie jest znaczące, w związku z czym dane incydenty należy zgłosić. Zważywszy na potencjalny wpływ transgraniczny takich zakłóceń, należy ustanowić procedurę, za pomocą której państwa członkowskie będą mogły przekazywać informacje innym zainteresowanym państwom członkowskim za pośrednictwem pojedynczych punktów kontaktowych.

(26) Podczas gdy podmioty krytyczne działają zazwyczaj jako część w coraz większym stopniu połączonej sieci świadczenia usług i infrastruktur oraz często świadczą usługi kluczowe w więcej niż jednym państwie członkowskim, niektóre z tych podmiotów mają szczególne znaczenie dla Unii, ponieważ świadczą usługi kluczowe na rzecz dużej liczby państw członkowskich, i wymagają zatem szczególnego nadzoru na poziomie Unii. Należy zatem ustanowić przepisy dotyczące szczególnego nadzoru w odniesieniu do takich podmiotów krytycznych o szczególnym znaczeniu europejskim. Przepisy te pozostają bez uszczerbku dla przepisów dotyczących nadzoru i egzekwowania przewidzianych w niniejszej dyrektywie.

(27) Jeżeli którekolwiek państwo członkowskie uważa, że do udzielenia pomocy podmiotowi krytycznemu w wypełnianiu jego obowiązków wynikających z rozdziału III lub do oceny wypełnienia tych obowiązków przez podmiot krytyczny o szczególnym znaczeniu europejskim niezbędne są dodatkowe informacje, Komisja organizuje – w porozumieniu z państwem członkowskim, w którym znajduje się infrastruktura tego podmiotu – misję doradczą w celu oceny środków wdrożonych przez ten podmiot. Aby zapewnić prawidłowe powadzenie takich misji doradczych, należy ustanowić dodatkowe przepisy, w szczególności dotyczące organizacji i przebiegu misji, działań następczych oraz obowiązków podmiotów krytycznych o szczególnym znaczeniu europejskim, których dotyczą misje. Misje doradcze należy – bez uszczerbku dla konieczności przestrzegania przepisów niniejszej dyrektywy przez państwo członkowskie, w którym prowadzi się misję doradczą, oraz przez podmiot, którego ona dotyczy – prowadzić zgodnie ze szczegółowymi przepisami prawa tego państwa członkowskiego, na przykład dotyczącymi konkretnych warunków, które należy spełnić, aby uzyskać dostęp do odpowiednich pomieszczeń lub dokumentów, oraz dotyczącymi środka zaskarżenia. O konkretną wiedzę ekspercką wymaganą na potrzeby takich misji można by w stosownych przypadkach wnosić za pośrednictwem Centrum Koordynacji Reagowania Kryzysowego.

(28) W celu wsparcia Komisji i ułatwienia współpracy strategicznej oraz wymiany informacji, w tym najlepszych praktyk, na temat kwestii związanych z niniejszą dyrektywą należy powołać Grupę ds. Odporności Podmiotów Krytycznych, będącą grupą ekspertów Komisji. Państwa członkowskie powinny dokładać starań, aby zapewnić skuteczną i efektywną współpracę wyznaczonych przedstawicieli ich właściwych organów w ramach Grupy ds. Odporności Podmiotów Krytycznych. Grupa powinna rozpocząć wykonywanie zadań sześć miesięcy po wejściu w życie niniejszej dyrektywy, tak aby zapewnić dodatkowe środki na rzecz odpowiedniej współpracy w okresie transpozycji niniejszej dyrektywy.

(29) Aby osiągnąć cele niniejszej dyrektywy i bez uszczerbku dla odpowiedzialności prawnej państw członkowskich i podmiotów krytycznych za wywiązywanie się z ich odpowiednich obowiązków przewidzianych w niniejszej dyrektywie, Komisja

powinna – jeżeli uzna to za stosowne – podjąć pewne działania wspierające mające na celu ułatwienie wypełniania tych obowiązków. Udzielając wsparcia państwom członkowskim i podmiotom krytycznym w wykonywaniu obowiązków na podstawie niniejszej dyrektywy, Komisja powinna korzystać z istniejących struktur i narzędzi, takich jak te dostępne w ramach Unijnego Mechanizmu Ochrony Ludności oraz Europejskiej Sieci Referencyjnej ds. Ochrony Infrastruktury Krytycznej.

(30) Państwa członkowskie powinny zapewnić, aby ich właściwe organy dysponowały pewnymi szczególnymi uprawnieniami umożliwiającymi im prawidłowe stosowanie i egzekwowanie niniejszej dyrektywy względem podmiotów krytycznych, jeżeli zgodnie z niniejszą dyrektywą podmioty te należą do ich jurysdykcji. Takie uprawnienia powinny obejmować w szczególności uprawnienie do prowadzenia inspekcji i audytów oraz sprawowania nadzoru, wymagania, aby podmioty krytyczne przekazały informacje i dowody związane ze środkami, które wdrożyły, aby wywiązać się ze swoich obowiązków, oraz w stosownych przypadkach wydawanie nakazów usunięcia skutków stwierdzonych naruszeń. Wydając takie nakazy, państwa członkowskie nie powinny wymagać środków wykraczających poza środki niezbędne i proporcjonalne do zapewnienia przestrzegania przepisów przez dane podmioty krytyczne, biorąc pod uwagę w szczególności powagę naruszenia oraz zdolność gospodarczą podmiotu krytycznego. Mówiąc ogólniej, uprawnieniom tym powinny towarzyszyć odpowiednie i skuteczne zabezpieczenia przewidziane prawem krajowym i zgodne z wymogami wynikającymi z Karty praw podstawowych Unii Europejskiej. Dokonując oceny wypełnienia obowiązków wynikających z niniejszej dyrektywy przez podmiot krytyczny, właściwe organy wyznaczone na podstawie niniejszej dyrektywy powinny mieć możliwość zwrócenia się do właściwych organów wyznaczonych na podstawie dyrektywy NIS 2 o przeprowadzenie oceny cyberbezpieczeństwa tych podmiotów. W tym celu wyżej wymienione właściwe organy powinny współpracować i wymieniać informacje.

(31) W celu uwzględnienia nowych czynników ryzyka, rozwoju technologii lub specyfiki jednego sektora lub ich większej liczby należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej uzupełniających środki na rzecz zwiększania odporności, które podmioty krytyczne mają obowiązek wdrożyć, poprzez dalsze określenie wszystkich tych środków lub niektórych spośród nich. 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 w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.[32] 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.

(32) W celu zapewnienia jednolitych warunków wykonywania niniejszej dyrektywy należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być

[32] Dz.U. L 123 z 12.5.2016, s. 1.

wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[33].

(33) Ponieważ cele niniejszej dyrektywy – a mianowicie zapewnienie świadczenia na rynku wewnętrznym usług koniecznych do utrzymania niezbędnych funkcji społecznych lub działalności gospodarczej oraz zwiększenie odporności podmiotów krytycznych świadczących takie usługi – nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na skutki działania możliwe jest lepsze ich 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 art. 5 niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(34) Należy zatem uchylić dyrektywę 2008/114/WE,

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I
PRZEDMIOT, ZAKRES I DEFINICJE

Artykuł 1
Przedmiot i zakres stosowania

1. W niniejszej dyrektywie:

   a) nakłada się na państwa członkowskie obowiązki polegające na przyjmowaniu pewnych środków mających na celu zapewnienie świadczenia na rynku wewnętrznym usług koniecznych do utrzymania niezbędnych funkcji społecznych lub działalności gospodarczej, a w szczególności na wskazywaniu podmiotów krytycznych i podmiotów, które w niektórych aspektach należy traktować jako równoważne, oraz umożliwianiu im dopełniania ich obowiązków;

   b) ustanawia się obowiązki podmiotów krytycznych mające na celu zwiększenie ich odporności i poprawę ich zdolności do świadczenia takich usług na rynku wewnętrznym;

   c) ustanawia się przepisy dotyczące nadzoru nad podmiotami krytycznymi i egzekwowania, aby stosowały one przepisy, a także dotyczące szczególnego nadzoru nad podmiotami krytycznymi uznawanymi za podmioty o szczególnym znaczeniu europejskim.

2. Niniejsza dyrektywa nie ma zastosowania do kwestii objętych dyrektywą (UE) XX/YY [proponowaną dyrektywą w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii („dyrektywa NIS 2")], bez uszczerbku dla art. 7.

[33] 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).

3. Jeżeli w przepisach sektorowych aktów prawa Unii nałożono na podmioty krytyczne obowiązek zastosowania środków przewidzianych w rozdziale III i jeżeli wymagania te są co najmniej równoważne z obowiązkami przewidzianymi w niniejszej dyrektywie, odpowiednie przepisy niniejszej dyrektywy nie mają zastosowania, w tym przepisy dotyczące nadzoru i egzekwowania przewidziane w rozdziale VI.

4. Bez uszczerbku dla art. 346 TFUE informacje, które są poufne zgodnie z przepisami unijnymi i krajowymi, takimi jak przepisy dotyczące tajemnicy przedsiębiorstwa, podlegają wymianie z Komisją i innymi odpowiednimi organami tylko wtedy, gdy wymiana taka jest niezbędna do stosowania niniejszej dyrektywy. Informacje podlegające wymianie ogranicza się do tego, co jest istotne dla celów takiej wymiany i proporcjonalne do jej celów. Podczas wymiany informacji zachowuje się poufność tych informacji oraz chroni się bezpieczeństwo i interesy handlowe podmiotów krytycznych.

Artykuł 2
Definicje

Do celów niniejszej dyrektywy stosuje się następujące definicje:

1) „podmiot krytyczny” oznacza podmiot prywatny lub publiczny należący do jednego z rodzajów wymienionych w załączniku, który został wskazany jako taki przez państwo członkowskie zgodnie z art. 5;

2) „odporność” oznacza zdolność do zapobiegania i stawiania oporu incydentowi zakłócającemu lub mogącemu zakłócić funkcjonowanie podmiotu krytycznego, łagodzenia i tłumienia takiego incydentu oraz dostosowania się do niego i usunięcia jego skutków;

3) „incydent” oznacza każde zdarzenie mogące zakłócić lub zakłócające funkcjonowanie podmiotu krytycznego;

4) „infrastruktura” oznacza składnik infrastruktury, system lub jego część niezbędny lub niezbędną do świadczenia usługi kluczowej;

5) „usługa kluczowa” oznacza usługę, która ma kluczowe znaczenie dla utrzymania niezbędnych funkcji społecznych lub działalności gospodarczej;

6) „ryzyko” oznacza każdą okoliczność lub każde zdarzenie, które mają potencjalny niekorzystny wpływ na odporność podmiotów krytycznych;

7) „ocena ryzyka” oznacza metodykę umożliwiającą ustalenie charakteru i zakresu ryzyka poprzez analizę potencjalnych zagrożeń oraz ocenę istniejących uwarunkowań podatności, które mogłyby prowadzić do zakłócenia funkcjonowania podmiotu krytycznego.

ROZDZIAŁ II
KRAJOWE RAMY DOTYCZĄCE ODPORNOŚCI PODMIOTÓW KRYTYCZNYCH

Artykuł 3
Strategia w zakresie odporności podmiotów krytycznych

1. Każde państwo członkowskie przyjmuje w terminie do dnia [trzy lata po wejściu w życie niniejszej dyrektywy] strategię mającą na celu wzmocnienie odporności podmiotów krytycznych. W strategii tej określa się cele strategiczne i środki polityczne służące osiągnięciu i utrzymaniu wysokiego poziomu odporności po

stronie tych podmiotów krytycznych oraz obejmujące co najmniej sektory, o których mowa w załączniku.

2. Strategia zawiera przynajmniej następujące elementy:

a) cele i priorytety strategiczne do celów zwiększenia ogólnej odporności podmiotów krytycznych, biorąc pod uwagę transgraniczne i międzysektorowe współzależności;

b) ramy zarządzania służące osiągnięciu celów i priorytetów strategicznych, w tym opis ról i obowiązków poszczególnych organów, podmiotów krytycznych i innych stron zaangażowanych we wdrażanie strategii;

c) opis środków niezbędnych do zwiększenia ogólnej odporności podmiotów krytycznych, w tym krajowej oceny ryzyka, wskazania podmiotów krytycznych i podmiotów równoważnych z podmiotami krytycznymi, a także środków mających na celu wsparcie podmiotów krytycznych zastosowanych zgodnie z niniejszym rozdziałem;

d) ramy polityczne umożliwiające zwiększoną koordynację między właściwymi organami wyznaczonymi na podstawie art. 8 niniejszej dyrektywy oraz na podstawie [dyrektywy NIS 2] na potrzeby wymiany informacji na temat incydentów i cyberzagrożeń oraz wykonywania zadań nadzorczych.

Strategię tę aktualizuje się w razie potrzeby i co najmniej co cztery lata.

3. Państwa członkowskie przekazują Komisji swoje strategie i wszelkie aktualizacje tych strategii w ciągu trzech miesięcy od ich przyjęcia.

Artykuł 4
Ocena ryzyka przeprowadzana przez państwa członkowskie

1. Właściwe organy wyznaczone na podstawie art. 8 ustanawiają wykaz usług kluczowych w sektorach, o których mowa w załączniku. W terminie do dnia [trzy lata po wejściu w życie niniejszej dyrektywy], a następnie w miarę potrzeby i co najmniej co cztery lata dokonują one oceny wszystkich istotnych czynników ryzyka, które mogą wpływać na świadczenie tych usług kluczowych, w celu wskazania podmiotów krytycznych zgodnie z art. 5 ust. 1 oraz udzielenia pomocy tym podmiotom krytycznym we wdrożeniu środków zgodnie z art. 11.

Ocena ryzyka uwzględnia wszystkie istotne zagrożenia, spowodowane przez człowieka i naturalne, w tym wypadki, klęski żywiołowe, stany zagrożenia zdrowia publicznego, zagrożenia związane z konfliktem, w tym przestępstwa terrorystyczne, o których mowa w dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/541[34].

2. Dokonując oceny ryzyka, państwa członkowskie biorą pod uwagę co najmniej:

a) ogólną ocenę ryzyka przeprowadzoną na podstawie art. 6 ust. 1 decyzji Parlamentu Europejskiego i Rady nr 1313/2013/UE[35];

[34] 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).

[35] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).

b) inne istotne oceny ryzyka przeprowadzone zgodnie z wymogami właściwych sektorowych aktów prawa Unii, w tym rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/941[36] i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/1938[37];

c) wszelkie czynniki ryzyka wynikające ze współzależności między sektorami wymienionymi w załączniku, w tym z innych państw członkowskich i państw trzecich, oraz wpływ, jaki zakłócenie w jednym sektorze może mieć na inne sektory;

d) wszelkie informacje na temat incydentów zgłoszonych zgodnie z art. 13.

Do celów akapitu pierwszego lit. c) państwa członkowskie współpracują w stosownych przypadkach z właściwymi organami innych państw członkowskich i państw trzecich.

3. Państwa członkowskie udostępniają odpowiednie elementy oceny ryzyka, o których mowa w ust. 1, podmiotom krytycznym, które wskazały zgodnie z art. 5, w celu udzielenia tym podmiotom krytycznym wsparcia w przeprowadzaniu oceny ryzyka, zgodnie z art. 10, oraz w stosowaniu środków służących zapewnieniu ich odporności, zgodnie z art. 11.

4. Każde państwo członkowskie przekazuje Komisji dane dotyczące rozpoznanych rodzajów ryzyka oraz wyników oceny ryzyka w odniesieniu do poszczególnych sektorów i podsektorów, o których mowa w załączniku, w terminie do dnia [trzy lata po wejściu w życie niniejszej dyrektywy], a następnie w miarę potrzeby i co najmniej co cztery lata.

5. Komisja może – we współpracy z państwami członkowskimi – opracować dobrowolny wspólny formularz sprawozdawczy do celów wykonania ust. 4.

Artykuł 5
Wskazywanie podmiotów krytycznych

1. W terminie do dnia [trzy lata i trzy miesiące po wejściu w życie niniejszej dyrektywy] państwa członkowskie wskazują podmioty krytyczne w przypadku każdego sektora i podsektora, o których mowa w załączniku, z wyjątkiem jego pkt 3, 4 i 8.

2. Wskazując podmioty krytyczne zgodnie z ust. 1, państwa członkowskie biorą pod uwagę wyniki oceny ryzyka zgodnie z art. 4, oraz stosują następujące kryteria:

a) podmiot świadczy co najmniej jedną usługę kluczową;

b) świadczenie tej usługi zależy od infrastruktury znajdującej się w państwie członkowskim; oraz

[36] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/941 z dnia 5 czerwca 2019 r. w sprawie gotowości na wypadek zagrożeń w sektorze energii elektrycznej i uchylające dyrektywę 2005/89/WE (Dz.U. L 158 z 14.6.2019, s. 1).

[37] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1938 z dnia 25 października 2017 r. dotyczące środków zapewniających bezpieczeństwo dostaw gazu ziemnego i uchylające rozporządzenie (UE) nr 994/2010 (Dz.U. L 280 z 28.10.2017, s. 1).

c) incydent miałby istotne skutki zakłócające dla świadczenia tej usługi lub innych usług kluczowych w sektorach, o których mowa w załączniku, zależnych od tej usługi.

3. Każde państwo członkowskie sporządza wykaz wskazanych podmiotów krytycznych i zapewnia, aby te podmioty krytyczne były powiadamiane o ich wskazaniu jako podmioty krytyczne w terminie jednego miesiąca od takiego wskazania, informując je o ich obowiązkach przewidzianych w rozdziałach II i III oraz o dacie, począwszy od której przepisy tych rozdziałów mają do nich zastosowanie.

W przypadku odnośnych podmiotów krytycznych przepisy niniejszego rozdziału mają zastosowanie od dnia powiadomienia, a przepisy rozdziału III mają zastosowanie po sześciu miesiącach od tego dnia.

4. Państwa członkowskie zapewniają, aby ich właściwe organy wyznaczone na podstawie art. 8 niniejszej dyrektywy przekazywały właściwym organom wyznaczonym przez państwa członkowskie na podstawie art. 8 [dyrektywy NIS 2] dane identyfikacyjne podmiotów krytycznych, które państwa te wskazały na podstawie niniejszego artykułu, w terminie jednego miesiąca od takiego wskazania.

5. Po powiadomieniu, o którym mowa w ust. 3, państwa członkowskie zapewniają, aby podmioty krytyczne przekazały informacje ich właściwym organom wyznaczonym na podstawie art. 8 niniejszej dyrektywy o tym, czy zostały one wskazane jako podmioty krytyczne w co najmniej jednym innym państwie członkowskim. Gdy co najmniej dwa państwa członkowskie wskazały dany podmiot jako podmiot krytyczny, te państwa członkowskie przystępują do wzajemnych konsultacji w celu ograniczenia obciążenia podmiotu krytycznego pod względem obowiązków przewidzianych w rozdziale III.

6. Do celów rozdziału IV państwa członkowskie zapewniają, aby podmioty krytyczne – po powiadomieniu, o którym mowa w ust. 3 – przekazały ich właściwym organom wyznaczonym na podstawie art. 8 niniejszej dyrektywy informacje o tym, czy świadczą one usługi kluczowe na rzecz ponad jednej trzeciej lub w ponad jednej trzeciej państw członkowskich. W takim przypadku odnośne państwo członkowskie niezwłocznie przekazuje Komisji dane identyfikacyjne tych podmiotów krytycznych.

7. W razie potrzeby i w każdym wypadku nie rzadziej niż co cztery lata państwa członkowskie dokonują przeglądu wykazu wskazanych podmiotów krytycznych oraz, w stosownych przypadkach, aktualizują go.

Jeżeli takie aktualizacje prowadzą do wskazania dodatkowych podmiotów krytycznych, stosuje się ust. 3, 4, 5 i 6. Ponadto państwa członkowskie zapewniają, aby podmioty, które wskutek jakiejkolwiek tego rodzaju aktualizacji nie są już wskazane jako podmioty krytyczne, zostały poinformowane, że z chwilą otrzymania takiej informacji nie podlegają już obowiązkom przewidzianym w rozdziale III.

Artykuł 6
Istotny skutek zakłócający

1. Przy określaniu istotności skutku zakłócającego, o którym mowa w art. 5 ust. 2 lit. c), państwa członkowskie uwzględniają następujące kryteria:

a) liczbę użytkowników zależnych od usługi świadczonej przez podmiot;

b) zależność innych sektorów, o których mowa w załączniku, od tej usługi;

c) wpływ, jaki incydenty – jeżeli chodzi o ich skalę i czas trwania – mogłyby mieć na działalność gospodarczą i społeczną, środowisko oraz bezpieczeństwo publiczne;

d) udział podmiotu w rynku takich usług;

e) obszar geograficzny, którego mógłby dotyczyć incydent, z uwzględnieniem wszelkiego wpływu transgranicznego;

f) znaczenie podmiotu w utrzymywaniu wystarczającego poziomu usługi przy uwzględnieniu dostępności alternatywnych sposobów świadczenia tej usługi.

2. W terminie do dnia [trzy lata i trzy miesiące po wejściu w życie niniejszej dyrektywy] państwa członkowskie przekazują Komisji następujące informacje:

a) wykaz usług, o których mowa w art. 4 ust. 1;

b) liczbę podmiotów krytycznych wskazanych w każdym sektorze i podsektorze, o których mowa w załączniku, oraz usługę lub usługi, o których mowa w art. 4 ust. 1, które świadczy każdy z tych podmiotów;

c) wszelkie progi zastosowane celem ustalenia co najmniej jednego spośród kryteriów, o których mowa w ust. 1.

Następnie państwa członkowskie przekazują te informacje w razie potrzeby i co najmniej co cztery lata.

3. Komisja może – po skonsultowaniu się z Grupą ds. Odporności Podmiotów Krytycznych – przyjąć wytyczne mające na celu ułatwienie stosowania kryteriów, o których mowa w ust. 1, biorąc pod uwagę informacje, o których mowa w ust. 2.

Artykuł 7

Podmioty równoważne z podmiotami krytycznymi do celów niniejszego rozdziału

1. Jeżeli chodzi o sektory, o których mowa w pkt 3, 4 i 8 załącznika, w terminie do dnia [trzy lata i trzy miesiące po wejściu w życie niniejszej dyrektywy] państwa członkowskie wskazują podmioty, które należy traktować jako równoważne z podmiotami krytycznymi do celów niniejszego rozdziału. W odniesieniu do tych podmiotów państwa członkowskie stosują przepisy art. 3, 4, art. 5 ust. 1–4 i 7 oraz art. 9.

2. W odniesieniu do podmiotów w sektorach, o których mowa w pkt 3 i 4 załącznika, wskazanych zgodnie z ust. 1, państwa członkowskie zapewniają, aby do celów stosowania art. 8 ust. 1 organy wyznaczone jako właściwe organy były właściwymi organami wyznaczonymi na podstawie art. 41 [rozporządzenia DORA].

3. Państwa członkowskie zapewniają, aby podmioty, o których mowa w ust. 1, powiadamiano bezzwłocznie o ich wskazaniu jako podmiotów, o których mowa w niniejszym artykule.

Artykuł 8

Właściwe organy i pojedynczy punkt kontaktowy

1. Każde państwo członkowskie wyznacza co najmniej jeden właściwy organ odpowiedzialny za prawidłowe stosowanie – i w stosownych przypadkach wdrażanie – przepisów niniejszej dyrektywy na szczeblu krajowym („właściwy organ”). Państwa członkowskie mogą wyznaczyć istniejący organ lub istniejące organy.

Jeżeli wyznaczą one więcej niż jeden organ, wyraźnie określają odpowiednie zadania przedmiotowych organów oraz zapewniają ich skuteczną współpracę w wypełnianiu

ich zadań na mocy niniejszej dyrektywy, w tym w odniesieniu do wyznaczenia i działań pojedynczego punktu kontaktowego, o którym mowa w ust. 2.

2. Każde państwo członkowskie wyznacza w ramach właściwego organu pojedynczy punkt kontaktowy, aby pełnił on funkcję łącznikową w celu zapewnienia współpracy transgranicznej z właściwymi organami innych państw członkowskich oraz z Grupą ds. Odporności Podmiotów Krytycznych, o której mowa w art. 16 („pojedynczy punkt kontaktowy").

3. W terminie do dnia [trzy lata i sześć miesięcy po wejściu w życie niniejszej dyrektywy], a następnie raz do roku, pojedyncze punkty kontaktowe przekazują Komisji oraz Grupie ds. Odporności Podmiotów Krytycznych sprawozdanie podsumowujące na temat otrzymanych zgłoszeń, w tym liczby zgłoszeń, charakteru zgłoszonych incydentów oraz działań podjętych zgodnie z art. 13 ust. 3.

4. Każde państwo członkowskie zapewnia, aby właściwy organ, w tym pojedynczy punkt kontaktowy wyznaczony w ramach takiego organu, posiadał uprawnienia oraz odpowiednie zasoby finansowe, ludzkie i techniczne, by w sposób skuteczny i wydajny wykonywać przydzielone mu zadania.

5. Państwa członkowskie zapewniają, aby ich właściwe organy – w stosownych przypadkach oraz zgodnie z prawem Unii i prawem krajowym – konsultowały się oraz współpracowały z innymi odpowiednimi organami krajowymi, w szczególności z tymi, które zajmują się ochroną ludności, egzekwowaniem prawa oraz ochroną danych osobowych, a także z odpowiednimi zainteresowanymi stronami, w tym z podmiotami krytycznymi.

6. Państwa członkowskie zapewniają, aby ich właściwe organy wyznaczone zgodnie z niniejszym artykułem współpracowały z właściwymi organami wyznaczonymi zgodnie z [dyrektywą NIS 2] w zakresie ryzyka w cyberprzestrzeni i cyberincydentów wpływających na podmioty krytyczne, a także środków wdrożonych przez właściwe organy wyznaczone na mocy [dyrektywy NIS 2] istotnych dla podmiotów krytycznych.

7. Każde państwo członkowskie powiadamia Komisję o wyznaczeniu właściwego organu i pojedynczego punktu kontaktowego w ciągu trzech miesięcy od tego wyznaczenia, w tym o ich poszczególnych zadaniach i obowiązkach wynikających z niniejszej dyrektywy, o ich danych kontaktowych oraz o wszelkich późniejszych zmianach w tym zakresie. Każde państwo członkowskie podaje do publicznej wiadomości informację o wyznaczeniu właściwego organu i pojedynczego punktu kontaktowego.

8. Komisja publikuje wykaz pojedynczych punktów kontaktowych państw członkowskich.

Artykuł 9

Wsparcie państw członkowskich na rzecz podmiotów krytycznych

1. Państwa członkowskie wspierają podmioty krytyczne w zwiększaniu ich odporności. Wsparcie to może obejmować opracowywanie materiałów zawierających wytyczne i metodyk, wspieranie organizacji działań mających na celu sprawdzenie ich odporności oraz zapewnianie szkoleń dla personelu podmiotów krytycznych.

2. Państwa członkowskie zapewniają, aby właściwe organy współpracowały z podmiotami krytycznymi z sektorów, o których mowa w załączniku, oraz aby prowadziły z nimi wymianę informacji i dobrych praktyk.

3. Państwa członkowskie ustanawiają narzędzia wymiany informacji w celu wspierania dobrowolnej wymiany informacji między podmiotami krytycznymi w odniesieniu do kwestii objętych niniejszą dyrektywą zgodnie z unijnymi i krajowymi przepisami, w szczególności z przepisami dotyczącymi konkurencji i ochrony danych osobowych.

ROZDZIAŁ III
ODPORNOŚĆ PODMIOTÓW KRYTYCZNYCH

Artykuł 10
Ocena ryzyka przeprowadzana przez podmioty krytyczne

Państwa członkowskie zapewniają, aby w ciągu sześciu miesięcy po otrzymaniu powiadomienia, o którym mowa w art. 5 ust. 3, a następnie w stosownych przypadkach i co najmniej raz na cztery lata, podmioty krytyczne dokonywały oceny – na podstawie ocen ryzyka i innych istotnych źródeł informacji – wszystkich istotnych czynników ryzyka, które mogą zakłócać ich funkcjonowanie.

Ocena ryzyka obejmuje wszystkie istotne czynniki ryzyka, o których mowa w art. 4 ust. 1, które mogą prowadzić do zakłócenia świadczenia usług kluczowych. Ocena ta uwzględnia wszelkie zależności innych sektorów, o których mowa w załączniku, od usług kluczowych świadczonych przez podmiot krytyczny, w tym w stosownych przypadkach w sąsiadujących państwach członkowskich i w państwach trzecich, oraz skutki, jakie zakłócenie świadczenia usług kluczowych w co najmniej jednym z tych sektorów może wywierać na usługę kluczową świadczoną przez dany podmiot krytyczny.

Artykuł 11
Środki na rzecz zwiększania odporności podmiotów krytycznych

1. Państwa członkowskie zapewniają, aby podmioty krytyczne wprowadziły odpowiednie i proporcjonalne środki techniczne i organizacyjne służące zapewnieniu ich odporności, w tym środki niezbędne w celu:

   a) zapobiegania incydentom, w tym za pośrednictwem środków zmniejszania ryzyka związanego z klęskami żywiołowymi i przystosowania się do zmiany klimatu;

   b) zapewnienia odpowiedniej fizycznej ochrony wrażliwych obszarów, obiektów i innej infrastruktury, w tym ogrodzeń, barierek, narzędzi i procedur monitorowania granic, a także sprzętu do wykrywania i kontroli dostępu;

   c) przeciwdziałania konsekwencjom incydentów, w tym wdrażania procedur i protokołów zarządzania ryzykiem i zarządzania kryzysowego, a także procedur ostrzegawczych;

   d) zapewnienia działań naprawczych po incydentach, w tym środki na rzecz ciągłości działania oraz identyfikacji alternatywnych łańcuchów dostaw;

e) zapewnienia odpowiedniego zarządzania bezpieczeństwem pracowników, w tym poprzez ustanowienie kategorii personelu wykonującego krytyczne funkcje, ustanowienie praw dostępu do wrażliwych obszarów, obiektów i innej infrastruktury, a także do informacji szczególnie chronionych oraz określenie szczególnych kategorii personelu w kontekście art. 12;

f) zwiększania świadomości odpowiednich pracowników na temat środków, o których mowa w lit. a)–e).

2. Państwa członkowskie zapewniają, aby podmioty krytyczne posiadały i stosowały plan zwiększania odporności lub równoważny dokument lub dokumenty opisujące szczegółowo środki zgodnie z ust. 1. Jeżeli podmioty krytyczne wprowadziły środki na podstawie zobowiązań przewidzianych w innych aktach prawa Unii, które są istotne także dla środków, o których mowa w ust. 1, opisują te środki również w planie zwiększania odporności lub równoważnym dokumencie lub dokumentach.

3. Na wniosek państwa członkowskiego, które wskazało podmiot krytyczny, oraz za zgodą zainteresowanego podmiotu krytycznego Komisja organizuje misje doradcze – zgodnie z ustaleniami określonymi w art. 15 ust. 4, 5, 7 i 8 – w celu zapewnienia zainteresowanemu podmiotowi krytycznemu porady w zakresie wypełniania przez niego obowiązków zgodnie z rozdziałem III. Misja doradcza zgłasza swoje ustalenia Komisji, danemu państwu członkowskiemu oraz zainteresowanemu podmiotowi krytycznemu.

4. Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 21 uzupełniającym ust. 1 poprzez ustanowienie szczegółowych przepisów określających niektóre lub wszystkie środki, które mają zostać wprowadzone zgodnie ze wspomnianym ustępem. Komisja przyjmuje te akty delegowane w zakresie, w jakim jest to konieczne na potrzeby skutecznego i spójnego stosowania wspomnianego ustępu zgodnie z celami niniejszej dyrektywy, uwzględniając wszelkie istotne zmiany ryzyka, technologii lub świadczenia danych usług, a także specyfikę poszczególnych sektorów oraz rodzajów podmiotów.

5. Komisja przyjmuje akty wykonawcze w celu określenia niezbędnych specyfikacji technicznych i metodycznych związanych ze stosowaniem środków, o których mowa w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 20 ust. 2.

Artykuł 12
Sprawdzenie przeszłości

1. Państwa członkowskie zapewniają, aby podmioty krytyczne mogły składać wnioski o sprawdzenie przeszłości osób, które należą do pewnych szczególnych kategorii personelu, w tym osób, które są brane pod uwagę przy rekrutacji na stanowiska należące do tych kategorii, a także aby organy odpowiedzialne za sprawdzanie przeszłości dokonywały sprawnej oceny takich wniosków.

2. Zgodnie z mającymi zastosowanie przepisami unijnymi i krajowymi, w tym zgodnie z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[38], w ramach sprawdzenia przeszłości, o którym mowa w ust. 1:

[38] Dz.U. L 119 z 4.5.2016, s. 1.

a) ustala się tożsamość osoby na podstawie dokumentów potwierdzających tożsamość;

b) sprawdza się rejestry karne obejmujące okres co najmniej pięciu poprzednich lat, a maksymalnie dziesięciu, pod kątem przestępstw istotnych przy rekrutacji na dane stanowisko w państwie członkowskim lub państwach członkowskich obywatelstwa danej osoby oraz w każdym państwie członkowskim lub państwach trzecich miejsca stałego pobytu danej osoby w tym okresie;

c) sprawdza się poprzednie miejsca zatrudnienia, kształcenia oraz wszelkie luki w kształceniu lub zatrudnieniu w życiorysie danej osoby w okresie co najmniej pięciu poprzednich lat, a maksymalnie dziesięciu.

Jeżeli chodzi o akapit pierwszy lit. b), państwa członkowskie zapewniają, aby ich właściwe organy odpowiedzialne za sprawdzenie przeszłości uzyskały od innych państw członkowskich za pośrednictwem ECRIS informacje z rejestrów karnych zgodnie z procedurami określonymi w decyzji ramowej Rady 2009/315/WSiSW oraz, w stosownych przypadkach, w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/816[39]. Organy centralne, o których mowa w art. 3 wspomnianej decyzji ramowej oraz w art. 3 pkt 5 wspomnianego rozporządzenia, udzielają odpowiedzi na wnioski o przekazanie takich informacji w terminie 10 dni roboczych od dnia otrzymania wniosku.

3. Zgodnie z obowiązującym prawem unijnym i krajowym – w tym zgodnie z rozporządzeniem (UE) 2016/679 – każde państwo członkowskie zapewnia również możliwość rozszerzenia zakresu sprawdzenia przeszłości, o którym mowa w ust. 1, na podstawie należycie uzasadnionego wniosku podmiotu krytycznego, aby umożliwić wykorzystanie danych wywiadowczych oraz wszelkich innych dostępnych obiektywnych informacji, które mogą być niezbędne do określenia, czy dana osoba jest odpowiednia do pracy na stanowisku, w odniesieniu do którego podmiot krytyczny zwrócił się o przeprowadzenie rozszerzonego sprawdzenia przeszłości.

Artykuł 13
Zgłaszanie incydentów

1. Państwa członkowskie zapewniają, aby podmioty krytyczne bez zbędnej zwłoki zgłaszały właściwemu organowi incydenty, które w znacznym stopniu zakłócają lub mogą potencjalnie w znacznym stopniu zakłócać ich funkcjonowanie. Zgłoszenia muszą zawierać wszelkie dostępne informacje, których właściwy organ potrzebuje, aby zrozumieć charakter, przyczynę i ewentualne konsekwencje incydentu, jak również aby określić wszelki wpływ transgraniczny danego incydentu. Zgłoszenie takie nie może narażać podmiotów krytycznych na zwiększoną odpowiedzialność.

2. Aby określić stopień zakłócenia lub potencjalnego zakłócenia funkcjonowania podmiotu krytycznego na skutek incydentu, uwzględnia się w szczególności następujące parametry:

a) liczbę użytkowników, których dotyczy zakłócenie lub potencjalne zakłócenie;

b) czas trwania zakłócenia lub oczekiwany czas trwania potencjalnego zakłócenia;

[39] Dz.U. L 135 z 22.5.2019, s. 1.

c) obszar geograficzny, którego dotyczy zakłócenie lub potencjalne zakłócenie.

3. Na podstawie informacji przekazanych w zgłoszeniu przez podmiot krytyczny właściwy organ – za pośrednictwem swojego pojedynczego punktu kontaktowego – informuje pojedynczy punkt kontaktowy innego państwa członkowskiego, którego dotyczy zakłócenie, jeżeli incydent ma lub może mieć istotny wpływ na podmioty krytyczne oraz na ciągłość świadczenia usług kluczowych w co najmniej jednym innym państwie członkowskim.

   W działaniach tych pojedyncze punkty kontaktowe – zgodnie z prawem Unii lub prawodawstwem krajowym zgodnym z prawem Unii – traktują te informacje w sposób zapewniający zachowanie ich poufności oraz chronią bezpieczeństwo i interesy handlowe danego podmiotu krytycznego.

4. Możliwie najszybciej po otrzymaniu zgłoszenia zgodnie z ust. 1 właściwy organ przekazuje podmiotowi krytycznemu, od którego otrzymał zgłoszenie, odpowiednie informacje dotyczące działań następczych podjętych w związku z przekazanym przez niego zgłoszeniem, w tym informacje, które mogą pomóc podmiotowi krytycznemu w skutecznym zareagowaniu na incydent.

ROZDZIAŁ IV
SZCZEGÓLNY NADZÓR NAD PODMIOTAMI KRYTYCZNYMI O SZCZEGÓLNYM ZNACZENIU EUROPEJSKIM

Artykuł 14
Podmioty krytyczne o szczególnym znaczeniu europejskim

1. Podmioty krytyczne o szczególnym znaczeniu europejskim podlegają szczególnemu nadzorowi zgodnie z niniejszym rozdziałem.

2. Podmiot uznaje się za podmiot krytyczny o szczególnym znaczeniu europejskim, gdy wskazano go jako podmiot krytyczny oraz gdy świadczy usługi kluczowe na rzecz co najmniej jednej trzeciej państw członkowskich lub w co najmniej jednej trzeciej państw członkowskich, a także gdy zgłoszono go Komisji jako taki podmiot odpowiednio na podstawie art. 5 ust. 1 i 6.

3. Po otrzymaniu zgłoszenia na podstawie art. 5 ust. 6 Komisja bez zbędnej zwłoki informuje podmiot, którego to dotyczy, że uznaje się go za podmiot krytyczny o szczególnym znaczeniu europejskim, o obowiązkach spoczywających na nim na podstawie niniejszego rozdziału oraz o dacie, od której obowiązki te mają wobec niego zastosowanie.

   Przepisy niniejszego rozdziału mają zastosowanie do podmiotu krytycznego o szczególnym znaczeniu europejskim, którego dotyczy zgłoszenie, począwszy od daty otrzymania przedmiotowego zgłoszenia.

Artykuł 15
Szczególny nadzór

1. Na wniosek co najmniej jednego państwa członkowskiego lub Komisji państwo członkowskie, w którym znajduje się infrastruktura podmiotu krytycznego o szczególnym znaczeniu europejskim, wraz z tym podmiotem przekazuje Komisji oraz Grupie ds. Odporności Podmiotów Krytycznych informacje na temat wyniku

oceny ryzyka przeprowadzonej na podstawie art. 10 oraz środków wprowadzonych zgodnie z art. 11.

Przedmiotowe państwo członkowskie bez zbędnej zwłoki przekazuje również Komisji i Grupie ds. Odporności Podmiotów Krytycznych informacje na temat wszelkich działań nadzorczych lub działań z zakresu egzekwowania przepisów, w tym na temat wszelkich przeprowadzonych ocen zgodności lub wydanych nakazów, podjętych przez właściwy organ na podstawie art. 18 i 19 w odniesieniu do tego podmiotu.

2. Na wniosek co najmniej jednego państwa członkowskiego lub z własnej inicjatywy oraz po uzgodnieniu z państwem członkowskim, w którym znajduje się infrastruktura podmiotu krytycznego o szczególnym znaczeniu europejskim, Komisja organizuje misję doradczą w celu oceny środków wdrożonych przez ten podmiot, aby wywiązać się z obowiązków wynikających z rozdziału III. W stosownych przypadkach misje doradcze mogą zwrócić się o konkretną wiedzę specjalistyczną w obszarze zarządzania ryzykiem związanym z klęskami żywiołowymi za pośrednictwem Centrum Koordynacji Reagowania Kryzysowego.

3. Misja doradcza zgłasza swoje ustalenia Komisji, Grupie ds. Odporności Podmiotów Krytycznych oraz podmiotowi krytycznemu o szczególnym znaczeniu europejskim, którego dotyczy misja, w terminie trzech miesięcy od zakończenia misji doradczej.

Grupa ds. Odporności Podmiotów Krytycznych analizuje sprawozdanie i w stosownych przypadkach doradza Komisji w kwestii tego, czy przedmiotowy podmiot krytyczny o szczególnym znaczeniu europejskim wywiązuje się z obowiązków spoczywających na nim zgodnie z rozdziałem III, oraz – w razie potrzeby – w kwestii tego, jakie środki można wprowadzić, aby zwiększyć odporność tego podmiotu.

Na podstawie tych porad Komisja przekazuje państwu członkowskiemu, w którym znajduje się infrastruktura przedmiotowego podmiotu, Grupie ds. Odporności Podmiotów Krytycznych oraz temu podmiotowi swoje uwagi na temat tego, czy podmiot ten wywiązuje się z obowiązków spoczywających na nim zgodnie z rozdziałem III, oraz – w stosownych przypadkach – jakie środki można wprowadzić, aby zwiększyć odporność tego podmiotu.

Wspomniane państwo członkowskie należycie uwzględnia te uwagi i przekazuje Komisji i Grupie ds. Odporności Podmiotów Krytycznych informacje na temat wszelkich środków, jakie w związku z nimi wdrożyło.

4. W skład każdej misji doradczej wchodzą eksperci z państw członkowskich oraz przedstawiciele Komisji. Państwa członkowskie mogą występować z propozycjami kandydatów, którzy powinni uczestniczyć w misji doradczej. Komisja wybiera i powołuje członków każdej misji doradczej zgodnie z ich kwalifikacjami zawodowymi, zapewniając, aby reprezentowali państwa członkowskie w sposób zrównoważony pod względem geograficznym. Komisja ponosi koszty związane z uczestnictwem w misji doradczej.

Komisja organizuje program misji doradczej po konsultacji z członkami określonej misji doradczej oraz w porozumieniu z państwem członkowskim, w którym znajduje się infrastruktura lub siedziba podmiotu krytycznego o znaczeniu europejskim.

5. Komisja przyjmuje akt wykonawczy, w którym ustanawia przepisy dotyczące ustaleń proceduralnych na potrzeby prowadzenia misji doradczych i opracowywania

sprawozdań z tych misji. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 20 ust. 2.

6. Państwa członkowskie zapewniają, aby podmiot krytyczny o szczególnym znaczeniu europejskim, którego dotyczy misja, zapewnił misji doradczej dostęp do wszelkich informacji, systemów i obiektów związanych ze świadczeniem usług kluczowych, którego misja potrzebuje do realizacji swoich działań.

7. Misja doradcza realizowana jest zgodnie z obowiązującym prawem krajowym państwa członkowskiego, w którym znajduje się przedmiotowa infrastruktura.

8. Organizując misje doradcze, Komisja bierze pod uwagę sprawozdania z inspekcji przeprowadzonych przez Komisję na podstawie rozporządzenia (WE) nr 300/2008 i rozporządzenia (WE) nr 725/2004 oraz sprawozdania z monitorowania przeprowadzonego przez Komisję na podstawie dyrektywy 2005/65/WE w odniesieniu odpowiednio do podmiotu krytycznego lub podmiotu krytycznego o szczególnym znaczeniu europejskim.

ROZDZIAŁ V
WSPÓŁPRACA I SPRAWOZDAWCZOŚĆ

Artykuł 16
Grupa ds. Odporności Podmiotów Krytycznych

1. Grupę ds. Odporności Podmiotów Krytycznych ustanawia się ze skutkiem od dnia [sześć miesięcy po wejściu w życie niniejszej dyrektywy]. Grupa wspiera Komisję i ułatwia współpracę strategiczną oraz wymianę informacji na temat kwestii związanych z niniejszą dyrektywą.

2. Grupa ds. Odporności Podmiotów Krytycznych składa się z przedstawicieli państw członkowskich i Komisji. Jeżeli jest to konieczne do wykonywania powierzonych jej zadań, Grupa ds. Odporności Podmiotów Krytycznych może zaprosić do udziału w swoich pracach przedstawicieli zainteresowanych stron.

   Grupie ds. Odporności Podmiotów Krytycznych przewodniczy przedstawiciel Komisji.

3. Zadania Grupy ds. Odporności Podmiotów Krytycznych są następujące:

   a) wspieranie Komisji w pomocy państwom członkowskim w zwiększaniu ich zdolności do zapewniania odporności podmiotów krytycznych zgodnie z niniejszą dyrektywą;

   b) ocena strategii w zakresie odporności podmiotów krytycznych, o których to strategiach mowa w art. 3, oraz wskazanie najlepszych praktyk w odniesieniu do tych strategii;

   c) ułatwianie wymiany najlepszych praktyk w odniesieniu do wskazywania podmiotów krytycznych przez państwa członkowskie, zgodnie z art. 5, w tym w odniesieniu do transgranicznych zależności oraz ryzyka i incydentów;

   d) wkład w przygotowywanie wytycznych, o których mowa w art. 6 ust. 3, oraz wszelkich aktów delegowanych i wykonawczych na podstawie niniejszej dyrektywy – na wniosek;

e) coroczna analiza sprawozdań podsumowujących, o których mowa w art. 8 ust. 3;

f) wymiana najlepszych praktyk dotyczących wymiany informacji związanej ze zgłaszaniem incydentów, o którym mowa w art. 13;

g) analizowanie sprawozdań misji doradczych i udzielanie porad dotyczących tych sprawozdań zgodnie z art. 15 ust. 3;

h) wymiana informacji i najlepszych praktyk dotyczących badań i rozwoju w zakresie odporności podmiotów krytycznych zgodnie z niniejszą dyrektywą;

i) w stosownych przypadkach, wymiana informacji w sprawach dotyczących odporności podmiotów krytycznych z odpowiednimi instytucjami, organami, biurami i agencjami Unii.

4. W terminie do dnia [24 miesiące po wejściu w życie niniejszej dyrektywy], a następnie co dwa lata, Grupa ds. Odporności Podmiotów Krytycznych opracowuje program prac w odniesieniu do działań, jakie mają zostać podjęte w celu realizacji celów i zadań, które muszą być spójne z wymogami i celami niniejszej dyrektywy.

5. Grupa ds. Odporności Podmiotów Krytycznych spotyka się regularnie co najmniej raz w roku z Grupą ds. Współpracy ustanowioną zgodnie z [dyrektywą NIS 2] w celu propagowania strategicznej współpracy i wymiany informacji.

6. Komisja może przyjmować akty wykonawcze określające ustalenia proceduralne niezbędne do funkcjonowania Grupy ds. Odporności Podmiotów Krytycznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 20 ust. 2.

7. Komisja przekazuje Grupie ds. Odporności Podmiotów Krytycznych sprawozdanie podsumowujące dotyczące informacji przekazanych przez państwa członkowskie zgodnie z art. 3 ust. 3 i art. 4 ust. 4 w terminie do dnia [trzy i pół roku po wejściu w życie niniejszej dyrektywy], a następnie w miarę potrzeby i co najmniej co cztery lata.

Artykuł 17

Wsparcie Komisji na rzecz właściwych organów i podmiotów krytycznych

1. Komisja wspiera w stosownych przypadkach państwa członkowskie i podmioty krytyczne w wypełnianiu ich obowiązków przewidzianych w niniejszej dyrektywie, przygotowując w szczególności przegląd ryzyka transgranicznego i międzysektorowego na szczeblu unijnym związanego ze świadczeniem usług kluczowych, organizując misje doradcze, o których mowa w art. 11 ust. 3 i art. 15 ust. 3, oraz ułatwiając wymianę informacji pomiędzy ekspertami na terytorium Unii.

2. Komisja uzupełnia działania państw członkowskich, o których mowa w art. 9, opracowując najlepsze praktyki i metody oraz organizując transgraniczne działania szkoleniowe i ćwiczenia w celu sprawdzania odporności podmiotów krytycznych.

ROZDZIAŁ VI
NADZÓR I EGZEKWOWANIE

Artykuł 18
Wdrażanie i egzekwowanie

1. W celu przeprowadzania oceny wypełniania obowiązków wynikających z niniejszej dyrektywy przez podmioty wskazane przez państwa członkowskie, zgodnie z art. 5, jako podmioty krytyczne, państwa członkowskie zapewniają właściwym organom uprawnienia i środki do:

   a) przeprowadzania kontroli na miejscu pomieszczeń wykorzystywanych przez podmiot krytyczny do świadczenia usług kluczowych oraz prowadzenia zdalnego nadzoru nad działaniami podmiotów krytycznych, zgodnie z art. 11;

   b) przeprowadzania lub zlecania audytów dotyczących tych podmiotów.

2. Państwa członkowskie zapewniają właściwym organom uprawnienia i środki, gdy jest to konieczne w celu wykonania przez nie swoich zadań określonych w niniejszej dyrektywie, umożliwiające wymaganie od podmiotów wskazanych przez państwa członkowskie, zgodnie z ust. 5, jako podmioty krytyczne, przekazania w rozsądnym terminie ustalonym przez te organy:

   a) informacji koniecznych do oceny, czy działania podjęte przez dany podmiot w celu zapewniania odporności spełniają wymogi art. 11;

   b) dowodów potwierdzających skuteczne wdrożenie tych działań, w tym wyników audytu przeprowadzonego na koszt tego podmiotu przez wybranego przez niego niezależnego i wykwalifikowanego audytora.

   Zwracając się o przekazanie takich informacji, właściwe organy podają cel wymogu i określają, jakie informacje są wymagane.

3. Bez uszczerbku dla możliwości nałożenia kar zgodnie z art. 19 właściwe organy mogą, po przeprowadzeniu działań nadzorczych, o których mowa w ust. 1, lub oceny informacji, o których mowa w ust. 2, nakazać odnośnym podmiotom krytycznym podjęcie koniecznych i proporcjonalnych działań w celu wyeliminowania wszelkiego stwierdzonego naruszenia niniejszej dyrektywy w rozsądnym terminie ustalonym przez te organy oraz poinformowanie organów o podjętych działaniach. Nakazy te uwzględniają w szczególności wagę naruszenia.

4. Państwo członkowskie zapewnia, aby uprawnienia określone w ust. 1, 2 i 3 mogły być wykonywane wyłącznie z zastrzeżeniem odpowiednich gwarancji prawnych. Takie gwarancje zapewniają w szczególności wykonywanie tych uprawnień w sposób obiektywny, przejrzysty i proporcjonalny oraz należyte zabezpieczenie praw i prawnie uzasadnionych interesów podmiotów krytycznych, których to dotyczy, w tym ich prawa do bycia wysłuchanymi, do obrony oraz do skutecznego środka odwoławczego przed niezależnym sądem.

5. Państwa członkowskie zapewniają, aby w przypadku, gdy właściwy organ przeprowadza ocenę spełniania przez podmiot krytyczny wymogów określonych w niniejszym artykule, informował on właściwe organy odnośnego państwa członkowskiego wyznaczone zgodnie z [dyrektywą NIS 2] oraz mógł zwrócić się do tych organów o ocenę cyberbezpieczeństwa takiego podmiotu, a także by współpracował i wymieniał informacje w tym celu.

Artykuł 19
Sankcje

Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń przepisów krajowych przyjętych na podstawie niniejszej dyrektywy i podejmują wszelkie niezbędne środki w celu zapewnienia ich wykonywania. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych przepisach najpóźniej [dwa lata po wejściu w życie niniejszej dyrektywy] i powiadamiają ją niezwłocznie o każdej następnej zmianie mającej na nie wpływ.

ROZDZIAŁ VII
PRZEPISY KOŃCOWE

Artykuł 20
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 21
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. 11 ust. 4, powierza się Komisji na okres pięciu lat od dnia wejścia w życie niniejszej dyrektywy lub każdej innej daty ustalonej przez współprawodawców.
3. Przekazanie uprawnień, o którym mowa w art. 11 ust. 4, 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 w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.
5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.
6. Akt delegowany przyjęty na podstawie art. 11 ust. 4 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 22
Sprawozdawczość i przegląd przepisów

Do dnia [54 miesiące po wejściu w życie niniejszej dyrektywy] Komisja składa Parlamentowi Europejskiemu i Radzie sprawozdanie, w którym ocenia, w jakim zakresie państwa członkowskie przyjęły środki niezbędne do wykonania niniejszej dyrektywy.

Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. Sprawozdanie to zawiera w szczególności ocenę wpływu i wartości dodanej niniejszej dyrektywy, jeżeli chodzi o zapewnienie odporności podmiotów krytycznych, oraz ocenę konieczności rozszerzenia zakresu dyrektywy na inne sektory lub podsektory. Pierwsze sprawozdanie składane jest najpóźniej do dnia [sześć lat po wejściu w życie niniejszej dyrektywy] i zawiera w szczególności ocenę konieczności rozszerzenia zakresu dyrektywy na sektor produkcji, przetwórstwa i dystrybucji żywności.

Artykuł 23
Uchylenie dyrektywy 2008/114/WE

Dyrektywa 2008/114/WE traci moc ze skutkiem od dnia [data wejścia w życie niniejszej dyrektywy].

Artykuł 24
Transpozycja

1. Państwa członkowskie przyjmują i publikują, najpóźniej do dnia [18 miesięcy po wejściu w życie niniejszej dyrektywy], przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie przekazują Komisji tekst tych przepisów.

   Państwa członkowskie stosują te przepisy od dnia [dwa lata po wejściu w życie niniejszej dyrektywy + jeden dzień].

   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.

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 Brukseli dnia […] r.

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

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie odporności podmiotów krytycznych

1.2. Dziedziny polityki, których dotyczy wniosek/inicjatywa

Bezpieczeństwo

1.3. Wniosek/inicjatywa dotyczy:

☐ **nowego działania**

☐ **nowego działania, będącego następstwem projektu pilotażowego/działania przygotowawczego**[40]

☑ **przedłużenia bieżącego działania**

☐ **połączenia lub przekształcenia co najmniej jednego działania pod kątem innego/nowego działania**

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

Operatorzy infrastruktury krytycznej świadczą usługi w wielu sektorach (takich jak transport, energetyka, zdrowie, gospodarka wodna itp.), które to usługi są kluczowe dla zapewnienia niezbędnych funkcji społecznych i działalności gospodarczej. Operatorzy muszą zatem cechować się odpornością, tzn. muszą być odpowiednio chronieni, lecz jednocześnie mieć zdolność do szybkiego wznowienia działania w przypadku zakłócenia.

Ogólnym celem wniosku jest zwiększenie odporności tych operatorów (zwanych w niniejszej dyrektywie „podmiotami krytycznymi") na szereg rodzajów ryzyka – naturalnych i spowodowanych przez człowieka, umyślnie lub nieumyślnie.

1.4.2. Cel(e) szczegółowy(e)

Inicjatywa ta służy realizacji czterech celów szczegółowych:

– zapewnienia głębszego zrozumienia ryzyka i współzależności, z którymi mają do czynienia podmioty krytyczne, oraz środków pozwalających na zmierzenie się z nimi;

– zapewnienia, aby organy państw członkowskich wskazały jako „podmioty krytyczne" wszystkie odpowiednie podmioty;

– zapewnienia włączenia całego spektrum działań na rzecz odporności do polityki publicznej i praktyki operacyjnej;

– zwiększenia zdolności oraz poprawy współpracy i komunikacji między zainteresowanymi stronami.

[40] O którym mowa w art. 58 ust. 2 lit. a) lub b) rozporządzenia finansowego.

Cele te przyczynią się do osiągnięcia celu ogólnego inicjatywy.

1.4.3. Oczekiwane wyniki i wpływ

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

Oczekuje się, że inicjatywa będzie miała pozytywny wpływ na bezpieczeństwo podmiotów krytycznych, które staną się bardziej odporne na ryzyko i zakłócenia. Będą w stanie lepiej ograniczać ryzyko, radzić sobie z potencjalnymi zakłóceniami i minimalizować negatywne skutki w przypadku wystąpienia incydentu.

Większa odporność podmiotów krytycznych oznacza również, że ich działania będą bardziej niezawodne, a ich usługi w wielu kluczowych sektorach będą świadczone w sposób ciągły, co przyczyni się do sprawnego funkcjonowania rynku wewnętrznego. To z kolei wywrze pozytywny wpływ na ogół społeczeństwa oraz na przedsiębiorstwa, gdyż polegają one w swojej codziennej działalności na tych usługach.

Organy publiczne również odniosłyby korzyści ze stabilności wynikającej ze sprawnego funkcjonowania podstawowych rodzajów działalności gospodarczej oraz z ciągłego świadczenia usług kluczowych na rzecz obywateli.

1.4.4. Wskaźniki dotyczące realizacji celów

Należy wskazać wskaźniki stosowane do monitorowania postępów i osiągnięć.

Wskaźniki stosowane do monitorowania postępów i osiągnięć będą powiązane z celami szczegółowymi inicjatywy:

– liczba i zakres ocen ryzyka przeprowadzonych przez organy i podmioty krytyczne będą wskaźnikiem lepszego zrozumienia ryzyka przez główne podmioty;

– liczba „podmiotów krytycznych” wskazanych przez państwa członkowskie będzie odzwierciedlała kompleksowość zakresu polityk dotyczących infrastruktury krytycznej;

– włączenie kwestii odporności do głównego nurtu polityki publicznej i praktyki operacyjnej znajdzie odzwierciedlenie w strategiach krajowych oraz środkach podmiotów krytycznych na rzecz zwiększania odporności;

– poprawa w odniesieniu do zdolności i współpracy będzie oceniana na podstawie podjętych działań w zakresie budowania zdolności i inicjatyw na rzecz współpracy.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

W celu spełnienia wymogów zawartych w inicjatywie państwa członkowskie będą musiały – w perspektywie krótko- lub średnioterminowej – opracować strategię w zakresie odporności podmiotów krytycznych; przeprowadzić krajową ocenę ryzyka; i na podstawie rezultatów oceny ryzyka oraz szczególnych kryteriów wskazać operatorów będących „podmiotami krytycznymi”. Działania te będą przeprowadzane regularnie, w miarę potrzeb, i co najmniej raz na cztery lata. Państwa członkowskie będą również musiały ustanowić mechanizmy współpracy między właściwymi zainteresowanymi stronami.

W perspektywie krótko- lub średnioterminowej wymaga się, aby operatorzy wyznaczeni jako „podmioty krytyczne” przeprowadzili ocenę ryzyka we własnym

zakresie; wprowadzili odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zapewnienia odporności; oraz powiadamiali właściwe organy o incydentach.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii" należy rozumieć jako wartość wynikającą z unijnej interwencji wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

Przyczyny działania na poziomie europejskim (*ex ante*)

Ogólnym celem niniejszej inicjatywy jest zwiększenie odporności podmiotów krytycznych na różne rodzaje ryzyka. Państwa członkowskie nie mogą samodzielnie osiągnąć tego celu w stopniu wystarczającym: działanie UE jest uzasadnione ze względu na wspólny charakter ryzyka, z którym mają do czynienia podmioty krytyczne; transnarodowy charakter świadczonych przez nie usług; oraz współzależności i powiązania pomiędzy nimi (międzysektorowe i wykraczające poza granice poszczególnych państw). Oznacza to, że podatność lub zakłócenie dotyczące jednego obiektu może potencjalnie spowodować zakłócenie w kilku sektorach i poza granicami danego państwa.

Oczekiwana wygenerowana unijna wartość dodana (*ex post*)

W porównaniu z obecną sytuacją proponowana inicjatywa będzie stanowiła wartość dodaną, w szczególności poprzez:

– ustanowienie ogólnych ram promujących ściślejsze dopasowanie polityk państw członkowskich (spójny zakres sektorów, kryteria wyznaczania podmiotów krytycznych, wspólne wymogi w zakresie oceny ryzyka);

– zapewnienie stosowania przez podmioty krytyczne odpowiednich środków na rzecz zwiększania odporności;

– łączenie wiedzy i know-how z całej UE prowadzące do optymalizacji reagowania podmiotów krytycznych i organów;

– zmniejszenie różnic między państwami członkowskimi i podnoszenie poziomu odporności podmiotów krytycznych na terytorium UE.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Wniosek opiera się na doświadczeniu zdobytym przy wdrażaniu dyrektywy w sprawie europejskiej infrastruktury krytycznej (dyrektywa 2008/114/WE) i jej ocenie (SWD(2019) 308).

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

Niniejszy wniosek stanowi jeden z podstawowych elementów nowej strategii UE w zakresie unii bezpieczeństwa, która ma na celu stworzenie środowiska bezpieczeństwa dostosowanego do przyszłych wyzwań.

Możliwe jest wypracowanie synergii z Unijnym Mechanizmem Ochrony Ludności w zakresie zapobiegania klęskom żywiołowym, łagodzenia ich skutków i zarządzania nimi.

1.6. Okres trwania i wpływ finansowy wniosku/inicjatywy

☐ **Ograniczony czas trwania**

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

☐ Okres trwania wpływu finansowego: od RRRR r. do RRRR r. w odniesieniu do środków na zobowiązania oraz od RRRR r. do RRRR r. w odniesieniu do środków na płatności.

☑ **Nieograniczony czas trwania**

- Wprowadzenie w życie z okresem rozruchu od 2021 r. do 2027 r.,
- po którym następuje faza operacyjna.

1.7. Planowane tryby zarządzania[41]

☑ **Bezpośrednie zarządzanie** przez Komisję

☑ w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii;

☐ przez agencje wykonawcze;

☑ **Zarządzanie dzielone** z państwami członkowskimi

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

☐ państwom trzecim lub organom przez nie wyznaczonym;

☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

☐ EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

☐ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego;

☐ organom prawa publicznego;

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

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

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

W przypadku wskazania więcej niż jednego trybu należy podać dodatkowe informacje w części „Uwagi".

Uwagi

Zarządzanie bezpośrednie będzie obejmowało przede wszystkim: koszty administracyjne DG HOME, porozumienie administracyjne z JRC, dotacje zarządzane przez Komisję.

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

Zarządzanie dzielone będzie obejmowało: projekty w ramach zarządzania dzielonego: państwa członkowskie będą musiały opracować strategię i przeprowadzić ocenę ryzyka, przy czym mogą one wykorzystać do tych celów środki przydzielone dla danego państwa.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Określić częstotliwość i warunki

Zgodnie z wnioskiem dotyczącym rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument unijny na rzecz obszaru bezpieczeństwa (COM(2018) 472 final):

Zarządzanie dzielone:

Każde państwo członkowskie ustanowi systemy zarządzania i kontroli dla swojego programu i zapewni jakość i rzetelność systemu monitorowania i danych na temat wskaźników zgodnie z rozporządzeniem w sprawie wspólnych przepisów. Aby ułatwić szybkie rozpoczęcie wdrażania, istnieje możliwość przedłużenia okresu działania istniejących i sprawnych systemów zarządzania i kontroli na kolejny okres programowania.

W tym kontekście państwa członkowskie zostaną poproszone o powołanie komitetu monitorującego, w którym Komisja będzie zasiadać w charakterze doradczym. Komitet monitorujący będzie się zbierał co najmniej raz w roku. Będzie on dokonywał przeglądu wszystkich kwestii mających wpływ na postępy w realizacji celów programu.

Państwa członkowskie będą przesyłać roczne sprawozdanie z realizacji celów, które powinno zawierać informacje na temat postępów w realizacji programu oraz realizacji celów pośrednich i końcowych. Powinno ono także poruszać wszelkie kwestie mające wpływ na wyniki programu i opisywać środki wprowadzone w celu zaradzenia tym kwestiom.

Na koniec okresu każde państwo członkowskie przedłoży końcowe sprawozdanie z realizacji celów. Sprawozdanie końcowe powinno koncentrować się na postępach w realizacji celów programu i zawierać przegląd najważniejszych kwestii, które wpłynęły na wyniki programu, środków wprowadzonych w celu rozwiązania tych kwestii oraz ocenę skuteczności tych środków. Powinno ono ponadto przedstawiać wkład programu w rozwiązanie problemów określonych w odpowiednich zaleceniach UE skierowanych do danego państwa członkowskiego, postępy w osiąganiu celów końcowych wyznaczonych w ramach wykonania, ustalenia wynikające z odpowiednich ocen oraz działania następcze podjęte w związku z tymi ustaleniami i wyniki działań w zakresie komunikacji.

Zgodnie z projektem wniosku dotyczącego rozporządzenia w sprawie wspólnych przepisów państwa członkowskie przesyłają co roku pakiet dokumentów dotyczących poświadczenia wiarygodności, zawierający roczne sprawozdanie finansowe, deklarację zarządczą i opinie instytucji audytowej dotyczące sprawozdania finansowego, rocznego sprawozdania z kontroli zgodnie z art. 92 ust. 1 lit. d) rozporządzenia w sprawie wspólnych przepisów, systemu zarządzania i kontroli oraz legalności i prawidłowości wydatków zadeklarowanych w rocznym sprawozdaniu finansowym. Komisja wykorzysta wspomniany pakiet dokumentów dotyczących poświadczenia wiarygodności do ustalenia kwoty obciążającej Fundusz w danym roku obrachunkowym.

Co dwa lata organizowane będzie posiedzenie w sprawie przeglądu z udziałem Komisji i danego państwa członkowskiego w celu zbadania wyników poszczególnych programów.

Sześć razy w roku państwa członkowskie przekazują dane dotyczące swojego programu, w podziale na cele szczegółowe. Takie dane dotyczą kosztu operacji i wartości wspólnych wskaźników produktu i rezultatu.

Wymogi ogólne:

Komisja przeprowadza śródokresową i retrospektywną ocenę działań realizowanych w ramach omawianego Funduszu zgodnie z rozporządzeniem w sprawie wspólnych przepisów. Ocena śródokresowa powinna opierać się w szczególności na ocenie śródokresowej programów przedłożonych Komisji przez państwa członkowskie do dnia 31 grudnia 2024 r.

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie dla systemu zarządzania, mechanizmów finansowania wykonania, warunków płatności i proponowanej strategii kontroli

Zgodnie z wnioskiem dotyczącym rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument unijny na rzecz obszaru bezpieczeństwa (COM(2018) 472 final):

Zarówno oceny ex post funduszy Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych (DG HOME) w latach 2007–2013, jak i oceny śródokresowe bieżących funduszy DG HOME pokazują, że połączenie różnych metod realizacji w obszarach migracji i spraw wewnętrznych pozwoliło na wypracowanie skutecznego sposobu osiągania celów tych funduszy. Utrzymuje się całościową strukturę mechanizmów realizacji obejmującą zarządzanie dzielone, bezpośrednie i pośrednie.

Państwa członkowskie wdrażają w ramach zarządzania dzielonego programy, które przyczyniają się do realizacji celów polityki Unii i które są dostosowane do kontekstu krajowego państw członkowskich. Zarządzanie dzielone gwarantuje dostępność wsparcia finansowego we wszystkich państwach uczestniczących. Zarządzanie dzielone zapewnia ponadto przewidywalność finansowania, a państwom członkowskim, które są najbardziej świadome wyzwań, przed którymi stoją, umożliwia odpowiednie planowanie długoterminowych zobowiązań finansowych. Nowość polega na tym, że Fundusz może zapewniać pomoc w sytuacjach nadzwyczajnych także w ramach zarządzania dzielonego, w uzupełnieniu zarządzania bezpośredniego i pośredniego.

Metodą zarządzania bezpośredniego Komisja wspiera inne działania, przyczyniające się do realizacji wspólnych celów polityki Unii. Działania te umożliwiają dostosowanie wsparcia na pilne i szczególne potrzeby w poszczególnych państwach członkowskich („pomoc w sytuacjach nadzwyczajnych”), wspieranie ponadnarodowych sieci i działań, testowanie innowacyjnych działań, które można rozszerzyć w ramach programów krajowych, i uwzględnienie badań w interesie Unii jako całości („działania unijne”).

W ramach zarządzania pośredniego Fundusz zachowuje możliwość delegowania zadań związanych z wykonaniem budżetu, między innymi, na organizacje międzynarodowe i agencje ds. spraw wewnętrznych do konkretnych celów.

Mając na uwadze różne cele i potrzeby, w ramach Funduszu proponuje się wprowadzenie instrumentu tematycznego jako sposobu zrównoważenia przewidywalności wieloletniego przydziału środków dla programów krajowych z elastycznością w okresowym uruchamianiu środków finansowych na działania o wysokim poziomie wartości dodanej dla Unii. Instrument tematyczny będzie wykorzystywany do działań szczególnych w państwach członkowskich i między nimi, działań Unii, pomocy w sytuacjach nadzwyczajnych. Dzięki temu możliwe jest przydzielanie i przenoszenie środków pomiędzy różnymi wspomnianymi wyżej sposobami zarządzania na podstawie dwuletniego programowania.

Zasady płatności w ramach zarządzania dzielonego opisano w projekcie wniosku dotyczącego rozporządzenia w sprawie wspólnych przepisów, który przewiduje roczne płatności zaliczkowe, a następnie maksymalnie 4 płatności okresowe na program i rok na podstawie wniosków o płatność przesłanych przez państwa członkowskie w danym roku obrachunkowym. Zgodnie z projektem wniosku dotyczącego rozporządzenia w sprawie wspólnych przepisów płatności zaliczkowe są rozliczane w ostatnim roku obrachunkowym programów.

Strategia kontroli będzie się opierała na nowym rozporządzeniu finansowym i na rozporządzeniu w sprawie wspólnych przepisów. Nowe rozporządzenie finansowe i projekt wniosku dotyczącego rozporządzenia w sprawie wspólnych przepisów powinny przewidywać rozszerzenie wykorzystania uproszczonych form dotacji, takich jak stawki zryczałtowane, płatności ryczałtowe i koszty jednostkowe. Wprowadza ono również nowe formy płatności, oparte na uzyskanych wynikach, a nie na kosztach. Beneficjenci będą mogli otrzymać stałą kwotę pieniężną, jeśli udowodnią, że miały miejsce pewne działania, takie jak szkolenia czy udzielanie pomocy humanitarnej. Oczekuje się, że zmniejszy to obciążenie związane z kontrolą zarówno na poziomie beneficjenta, jak i na poziomie państw członkowskich (np. kontrole rachunków i pokwitowań z tytułu kosztów).

W odniesieniu do zarządzania dzielonego projekt wniosku dotyczący rozporządzenia w sprawie wspólnych przepisów płatności opiera się na strategii zarządzania i kontroli obowiązujących w okresie programowania 2014–2020, ale wprowadza też pewne środki mające na celu uproszczenie wdrażania i zmniejszenie obciążenia związanego z kontrolą zarówno na poziomie beneficjentów, jak i państw członkowskich. Te nowe elementy obejmują:

- zrezygnowanie z procedury wyznaczania (co umożliwi przyspieszenie realizacji programów);

- kontrole zarządcze (administracyjne i na miejscu) przeprowadzane przez instytucję zarządzającą na zasadzie ryzyka (w porównaniu z kontrolami administracyjnymi wymaganymi w 100 % przypadków w okresie programowania 2014–2020); W pewnych warunkach instytucje zarządzające mogą ponadto stosować proporcjonalne ustalenia dotyczące kontroli zgodnie z procedurami krajowymi;

- warunki pozwalające uniknąć wielokrotnych kontroli w odniesieniu do tej samej operacji/tych samych wydatków.

Instytucje programu przedstawią Komisji wnioski o płatność okresową w oparciu o wydatki poniesione przez beneficjentów. Projekt wniosku dotyczącego rozporządzenia w sprawie wspólnych przepisów zezwala instytucjom zarządzającym na dokonywanie kontroli zarządczych na podstawie ryzyka i przewiduje również szczególne kontrole (np. kontrole na miejscu dokonywane przez instytucję

zarządzającą oraz audyty operacji/wydatków dokonywane przez instytucję audytową) po zgłoszeniu Komisji kosztów dodatkowych we wnioskach o płatności okresowe. Aby zminimalizować ryzyko zwrotu wydatków niekwalifikowalnych, w projekcie wniosku dotyczącego rozporządzenia w sprawie wspólnych przepisów przewidziano maksymalny pułap płatności okresowych Komisji wynoszący 90 %, zważywszy że w danym momencie dokonana została tylko część kontroli krajowych. Komisja wypłaci pozostałą kwotę po rocznym rozliczeniu rachunków, kiedy instytucje programu przekażą jej pakiet dokumentów dotyczących poświadczenia wiarygodności. Wszelkie nieprawidłowości wykryte przez Komisję lub Europejski Trybunał Obrachunkowy po przekazaniu rocznego pakietu dokumentów dotyczących poświadczenia wiarygodności mogą prowadzić do korekty finansowej netto.

W przypadku części wdrażanej w drodze **zarządzania bezpośredniego** w ramach instrumentu tematycznego, system zarządzania i kontroli będzie opierał się na doświadczeniach zdobytych w latach 2014–2020 zarówno w odniesieniu do działań Unii, jak i pomocy w sytuacjach nadzwyczajnych. Ustanowiony zostanie uproszczony system umożliwiający szybkie rozpatrywanie wniosków o przyznanie finansowania przy jednoczesnym ograniczeniu ryzyka wystąpienia błędów: kwalifikujący się wnioskodawcy będą się ograniczać do państw członkowskich i organizacji międzynarodowych, finansowanie będzie oparte na uproszczonych formach kosztów, opracowane zostaną standardowe wzory wniosków o przyznanie finansowania, umów o udzielenie dotacji/wkładu oraz sprawozdań, a stały komitet ds. oceny będzie rozpatrywać wnioski niezwłocznie po ich otrzymaniu.

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

DG HOME nie musi mierzyć się z poważnym ryzykiem wystąpienia błędów w swoich programach wydatkowania. Potwierdza to systematyczny brak istotnych ustaleń w sprawozdaniach rocznych Trybunału Obrachunkowego.

W ramach zarządzania dzielonego ogólne ryzyko związane z realizacją bieżących programów dotyczy niedostatecznego wykorzystania Funduszu przez państwa członkowskie i ewentualnych błędów wynikających ze złożonego charakteru przepisów i słabości systemów zarządzania i kontroli. Projekt rozporządzenia w sprawie wspólnych przepisów upraszcza ramy regulacyjne, ujednolicając przepisy oraz systemy zarządzania i kontroli w różnych funduszach objętych zarządzaniem dzielonym. Projekt upraszcza także wymogi dotyczące kontroli (np. kontrole zarządcze oparte na analizie ryzyka, możliwość proporcjonalnych zasad kontroli opartych na procedurach krajowych, ograniczenia prac audytowych pod względem czasu lub operacji szczególnych).

2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)

Komisja przedstawia sprawozdania dotyczące relacji kosztów kontroli do wartości zarządzanych funduszy powiązanych. W rocznym sprawozdaniu z działalności DG HOME za 2019 r. relacja ta wynosi 0,72 % w odniesieniu do zarządzania dzielonego, 1,31 % w odniesieniu do dotacji w ramach zarządzania bezpośredniego i 6,05 % w odniesieniu do zamówień publicznych w ramach zarządzania bezpośredniego. W przypadku zarządzania dzielonego odsetek ten zazwyczaj zmniejsza się

z upływem czasu w miarę przyrostu wydajności w trakcie realizacji programów oraz zwiększenia płatności na rzecz państw członkowskich.

Przy opartym na analizie ryzyka podejściu do zarządzania i kontroli przewidzianym w projekcie wniosku dotyczącym rozporządzenia w sprawie wspólnych przepisów w połączeniu z większą motywacją do przyjęcia uproszczonych form kosztów zakłada się dalsze obniżenie kosztu kontroli po stronie państw członkowskich.

W rocznym sprawozdaniu z działalności za 2019 r. łączny poziom błędu rezydualnego wynosił 1,57 % dla programów krajowych w ramach FAMI/FBW i 4,11 % dla dotacji w ramach zarządzania bezpośredniego niezwiązanych z działalnością badawczą.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony, np. ze strategii zwalczania nadużyć finansowych.

DG HOME będzie w dalszym ciągu stosować swoją strategię w zakresie zwalczania nadużyć finansowych zgodnie ze strategią Komisji w tym zakresie (CAFS) w celu zapewnienia m.in., by jej wewnętrzne kontrole związane ze zwalczaniem nadużyć były w pełni zgodne z CAFS oraz by jej podejście w kwestii zarządzania ryzykiem nadużyć było nastawione na wykrywanie obszarów obciążonych takim ryzykiem oraz na podejmowanie odpowiednich działań.

W odniesieniu do zarządzania dzielonego państwa członkowskie mają obowiązek zapewnić zgodność z prawem i prawidłowość wydatków ujętych w sprawozdaniu finansowym przedłożonym Komisji. W tym kontekście państwa członkowskie są zobowiązane podejmować wszelkie niezbędne działania, aby wykrywać i korygować nieprawidłowości oraz im zapobiegać. Podobnie jak w obecnym cyklu programowania (2014–2020) państwa członkowskie są zobowiązane wprowadzić procedury wykrywania nieprawidłowości i nadużyć finansowych w związku z rozporządzeniem delegowanym Komisji w sprawie zgłaszania nieprawidłowości. Środki zwalczania nadużyć finansowych pozostaną nadrzędną zasadą i obowiązkiem państw członkowskich.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

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

(1) Nowa linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj wydatków	Wkład			
	Dział 5: Odporność, bezpieczeństwo i obrona	Zróżn. / niezróżn.[42]	państw EFTA[43]	krajów kandydujących[44]	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
5	12.02.01 – „Fundusz Bezpieczeństwa Wewnętrznego”	Zróżn.	NIE	NIE	TAK	NIE
5	12 01 01 – Wydatki na wsparcie dotyczące Funduszu Bezpieczeństwa Wewnętrznego	Niezróżn.	NIE	NIE	TAK	NIE

Uwagi:

Należy zauważyć, że środki operacyjne, o które wnosi się w związku z przedstawionym wnioskiem, są pokrywane ze środków już przewidzianych w ocenie skutków finansowych regulacji, na której opiera się rozporządzenie w sprawie FBW.

W związku z niniejszym wnioskiem ustawodawczym występuje się o dodatkowe zasoby ludzkie.

42 Zróżn. = środki zróżnicowane / niezróżn. = środki niezróżnicowane.

43 EFTA: Europejskie Stowarzyszenie Wolnego Handlu

44 Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Podsumowanie szacunkowego wpływu na środki operacyjne

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

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

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	5	Odporność, bezpieczeństwo i obrona

DG: HOME			2021	2022	2023	2024	2025	2026	2027	**po 2027 r.**	**OGÓŁEM**
• Środki operacyjne											
Linia budżetowa 12 02 01 Fundusz Bezpieczeństwa Wewnętrznego	Środki na zobowiązania	(1a)	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Środki na płatności	(2a)	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822
Środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne[45]											
Linia budżetowa		(3)									
OGÓŁEM środki dla DG HOME	Środki na zobowiązania	=1a+1b +3	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Środki na płatności	=2a+2b +3	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

[45] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

• OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)									
	Środki na płatności	(5)									
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne		(6)									
OGÓŁEM środki na DZIAŁ 5 wieloletnich ram finansowych	Środki na zobowiązania	=4 + 6	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Środki na płatności	=5 + 6	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

Jeżeli wpływ wniosku/inicjatywy nie ogranicza się do jednego działu operacyjnego, należy powtórzyć powyższą część:

• OGÓŁEM środki operacyjne (wszystkie działy operacyjne)	Środki na zobowiązania	(4)									
	Środki na płatności	(5)									
OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy (wszystkie działy operacyjne)		(6)									
OGÓŁEM środki na DZIAŁY 1 do 6 wieloletnich ram finansowych (kwota referencyjna)	Środki na zobowiązania	=4 + 6	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Środki na płatności	=5 + 6	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

Dział wieloletnich ram finansowych	**7**	„Wydatki administracyjne”

Niniejszą część uzupełnia się przy użyciu „danych budżetowych o charakterze administracyjnym”, które należy najpierw wprowadzić do załącznika do oceny skutków finansowych regulacji (załącznik V do zasad wewnętrznych), przesyłanego do DECIDE w celu konsultacji między służbami.

w mln EUR (do trzech miejsc po przecinku)

		2021	2022	2023	2024	2025	2026	2027	**OGÓŁEM**
DG: HOME									
• Zasoby ludzkie		0,152	0,228	0,499	0,813	0,932	0,932	0,932	**4,488**
• Pozostałe wydatki administracyjne		0,033	0,085	0,109	0,109	0,109	0,109	0,109	**0,663**
OGÓŁEM DG HOME	Środki	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,151**

OGÓŁEM środki na DZIAŁ 7 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,151**

w mln EUR (do trzech miejsc po przecinku)

		2021	2022	2023	2024	2025	2026	2027	**po 2027 r.**	**OGÓŁEM**
OGÓŁEM środki na DZIAŁY 1 do 7 wieloletnich ram finansowych	Środki na zobowiązania	**0,309**	**4,661**	**6,178**	**7,642**	**8,061**	**8,061**	**8,061**	**-**	**42,973**
	Środki na płatności	**0,725**	**4,636**	**5,965**	**6,325**	**6,444**	**6,444**	**6,444**	**5,989**	**42,973**

3.2.2. Przewidywany produkt finansowany ze środków operacyjnych

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

Określić cele i produkty ⇩			Rok 2021		Rok 2022		Rok 2023		Rok 2024		Rok 2025		Rok 2026		Rok 2027		OGÓŁEM	
	Rodzaj	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt
CEL SZCZEGÓŁOWY nr 1: Wsparcie Komisji na rzecz właściwych organów i podmiotów krytycznych																		
Produkt	Rozwijanie i utrzymanie potencjału wiedzy i wsparcia					2,000		2,000				2,000		2,000		2,000		12,000
Produkt	Wsparcie właściwych organów poprzez ułatwianie wymiany najlepszych praktyk i informacji oraz przeprowadzanie ocen ryzyka (koszty finansowe uwzględnione w badaniach przedstawionych poniżej)																	
Produkt	Wsparcie właściwych organów i podmiotów krytycznych (tj. operatorów) poprzez opracowywanie materiałów zawierających wytyczne oraz metodyki, wspieranie organizacji działań symulujących scenariusze incydentów w czasie rzeczywistym, organizowanie szkoleń					0,500		0,850		1,200		1,500		1,500		1,500		7,050
Produkt	Projekty dotyczące różnych zagadnień związanych ze wsparciem wymienionych wyżej działań (metodyk oceny ryzyka, symulacji scenariuszy incydentów w czasie rzeczywistym, szkoleń...)	**0,400**			3	1,200	5	2,000	7	2,800		2,800	7	2,800	7		36	14,400
Produkt	Badania (oceny ryzyka) i konsultacje (dotyczące wdrażania dyrektywy)	**0,100**			4	0,400	4	0,400	4	0,400	4	0,400	4	0,400	4	0,400	24	2,400
Produkt	Inne spotkania, konferencje	**0,031**	4	0,124	8	0,248	8	0,248	8	0,248	8	0,248	8	0,248	8	0,248	52	1,612
Cel szczegółowy nr 1 – suma cząstkowa				0,124		4,348		5,498		6,648		6,948		6,948		6,948		37,462
CEL SZCZEGÓŁOWY nr 2: Zespoły doradcze ds. zwiększania odporności																		
Produkt	Organizacja zespołów doradczych ds. zwiększania odporności (członkowie: przedstawiciele państw członkowskich), Komisja odpowiedzialna za organizację zaproszenia dla członków (dla uczestników z państw członkowskich)																	
Produkt	Komisja odpowiedzialna za organizację programu i misji doradczych Komisja odpowiedzialna za zapewnienie istotnego wkładu w misje doradcze (doradztwo i nadzór nad podmiotami krytycznymi o znaczeniu europejskim – wraz z państwami członkowskimi) Bieżąca koordynacja zespołów doradczych ds. zwiększania odporności							0,072		0,072		0,072				0,072		0,072		0,360
Cel szczegółowy nr 2 – suma cząstkowa								0,072		0,072		0,072				0,072		0,072		0,360
OGÓŁEM cele 1 i 2				**0,124**		**4,348**		**5,570**		**6,720**		**7,020**				**7,020**		**7,020**		**37,822**

3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne

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

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

w mln EUR (do trzech miejsc po przecinku)

	2021	2022	2023	2024	2025	2026	2027	OGÓŁEM
DZIAŁ 7 wieloletnich ram finansowych								
Zasoby ludzkie	0,152	0,228	0,499	0,813	0,932	0,932	0,932	4,488
Pozostałe wydatki administracyjne	0,033	0,085	0,109	0,109	0,109	0,109	0,109	0,663
Suma cząstkowa DZIAŁU 7 wieloletnich ram finansowych	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,188**

Poza DZIAŁEM 7[46] wieloletnich ram finansowych								
Zasoby ludzkie								
Pozostałe wydatki administracyjne								
Suma cząstkowa poza DZIAŁEM 7 wieloletnich ram finansowych								

OGÓŁEM	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,188**

Potrzeby w zakresie środków na zasoby ludzkie i inne wydatki o charakterze administracyjnym zostaną pokryte z zasobów dyrekcji generalnej już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

[46] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

3.2.3.1. Szacowane zapotrzebowanie na zasoby ludzkie

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

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

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy

		Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	2025	2026	2027
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)								
20 01 02 01 (w centrali i w biurach przedstawicielstw Komisji)		1	2	4	5	5	5	5
XX 01 01 02 (w delegaturach)								
XX 01 05 01/11/21 (pośrednie badania naukowe)								
10 01 05 01/11 (bezpośrednie badania naukowe)								
• Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC)[47]								
20 02 01 03 (CA, SNE, INT z globalnej koperty finansowej)				1	2	2	2	2
XX 01 02 02 (CA, LA, SNE, INT i JED w delegaturach)								
XX 01 04 **yy** [48]	- w centrali							
	- w delegaturach							
XX 01 05 02/12/22 (CA, SNE, INT – pośrednie badania naukowe)								
10 01 05 02/12 (CA, INT, SNE – bezpośrednie badania naukowe)								
Inna linia budżetowa (określić)								
OGÓŁEM		**1**	**2**	**5**	**7**	**7**	**7**	**7**

XX oznacza odpowiednią dziedzinę polityki lub odpowiedni tytuł w budżecie.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów dyrekcji generalnej już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	Wniosek zakłada – po stronie Komisji – zatrudnienie czterech osób z grupy funkcyjnej AD i jednej osoby z grupy funkcyjnej AST w celu pracy nad wdrożeniem dyrektywy, przy czym jedna osoba z grupy funkcyjnej AD jest już zatrudniona, a pozostałe EPC odpowiadają dodatkowym zasobom ludzkim, które należy zatrudnić. Plan naboru przewiduje: 2022: +1 AD: pracownik merytoryczny odpowiedzialny za budowanie potencjału wiedzy i działania wspierające 2023: +1 AD (pracownik merytoryczny odpowiedzialny za zespoły doradcze), 1 AST (asystent zespołów doradczych ds. zwiększania odporności) 2024: +1 AD (pracownik merytoryczny wspierający działania organów i operatorów)
Personel zewnętrzny	Wniosek zakłada – po stronie Komisji – zatrudnienie dwóch oddelegowanych ekspertów krajowych (SNE) w celu pracy nad wdrożeniem dyrektywy. Plan naboru przewiduje: 2023: +1 SNE (ekspert ds. odporności infrastruktury krytycznej/wspierający działania organów

[47] CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JPD = młodszy specjalista w delegaturze.

[48] W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA").

	i operatorów) 2024: +1 SNE (ekspert ds. odporności infrastruktury krytycznej/wspierający działania organów i operatorów)

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

Wniosek/inicjatywa:

☑ może zostać w pełni sfinansowany(a) przez przegrupowanie środków w ramach odpowiedniego działu wieloletnich ram finansowych (WRF).

Wydatki operacyjne pokrywane przez FBW w ramach WRF na lata 2021–2027

☐ wymaga zastosowania nieprzydzielonego marginesu środków w ramach odpowiedniego działu WRF lub zastosowania specjalnych instrumentów zdefiniowanych w rozporządzeniu w sprawie WRF.

Należy wyjaśnić, który wariant jest konieczny, określając działy i linie budżetowe, których ma dotyczyć, odpowiadające im kwoty oraz proponowane instrumenty, które należy zastosować.

☐ wymaga rewizji WRF.

Należy wyjaśnić, który wariant jest konieczny, określając linie budżetowe, których ma on dotyczyć, oraz podając odpowiednie kwoty.

3.2.5. Udział osób trzecich w finansowaniu

Wniosek/inicjatywa:

☑ nie przewiduje współfinansowania ze strony osób trzecich

☐ przewiduje współfinansowanie ze strony osób trzecich szacowane zgodnie z poniższymi szacunkami:

Środki w mln EUR (do trzech miejsc po przecinku)

	Rok **N**[49]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			Ogółem
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

[49] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy. „N” należy zastąpić oczekiwanym pierwszym rokiem realizacji (np.: 2021). Tak samo należy postąpić dla kolejnych lat.

3.3. Szacunkowy wpływ na dochody

☑ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

☐ wpływ na zasoby własne

☐ wpływ na dochody inne

Wskazać, czy dochody są przypisane do linii budżetowej po stronie wydatków☐

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[50]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)		
Artykuł ….....								

W przypadku wpływu na dochody przeznaczone na określony cel należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

[…]

Pozostałe uwagi (np. metoda/wzór użyte do obliczenia wpływu na dochody albo inne informacje).

[…]

[50] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 20 % na poczet kosztów poboru.