KOMISJA
EUROPEJSKA

Bruksela, dnia 16.12.2020 r.
COM(2020) 823 final

2020/0359 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148

(Tekst mający znaczenie dla EOG)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Niniejszy wniosek jest częścią pakietu środków służących dalszemu wzmacnianiu zdolności podmiotów publicznych i prywatnych, właściwych organów oraz Unii jako całości w zakresie odporności i reagowania na incydenty w dziedzinach cyberbezpieczeństwa oraz ochrony infrastruktury krytycznej. Jest on zgodny z priorytetami Komisji dotyczącymi stworzenia Europy na miarę ery cyfrowej i zbudowania gospodarki gotowej na przyszłość, która będzie przynosić korzyści obywatelom. Cyberbezpieczeństwo jest priorytetem reakcji Komisji na kryzys związany z COVID-19. Niniejszy pakiet obejmuje nową strategię w zakresie cyberbezpieczeństwa, której celem jest wzmocnienie strategicznej autonomii Unii, aby poprawić jej odporność i wspólną reakcję oraz budować otwarty i globalny internet. Ponadto pakiet obejmuje wniosek dotyczący dyrektywy w sprawie odporności krytycznych operatorów usług kluczowych, którego celem jest ograniczenie fizycznych zagrożeń dla takich operatorów.

Niniejszy wniosek opiera się na dyrektywie (UE) 2016/1148 w sprawie bezpieczeństwa sieci i systemów informatycznych (dyrektywa w sprawie bezpieczeństwa sieci i informacji), która jest pierwszym aktem prawnym w ogólnounijnych przepisach dotyczących cyberbezpieczeństwa zapewniającym środki prawne służące podniesieniu ogólnego poziomu cyberbezpieczeństwa w Unii, oraz uchyla tę dyrektywę. Dyrektywa w sprawie bezpieczeństwa sieci i informacji: 1) przyczyniła się do zwiększenia zdolności w zakresie cyberbezpieczeństwa na szczeblu krajowym przez zobowiązanie państw członkowskich do przyjęcia krajowych strategii cyberbezpieczeństwa oraz do wyznaczenia organów ds. cyberbezpieczeństwa; 2) przyczyniła się do zacieśnienia współpracy między państwami członkowskimi na szczeblu unijnym przez utworzenie różnych forów ułatwiających wymianę strategicznych i operacyjnych informacji; oraz 3) przyczyniła się do poprawy cyberodporności podmiotów publicznych i prywatnych w siedmiu sektorach (energetyki, transportu, bankowości, infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną i jej dystrybucji oraz infrastruktury cyfrowej) oraz w trzech rodzajach usług cyfrowych (internetowe platformy handlowe, wyszukiwarki internetowe i usługi w chmurze) przez nałożenie na państwa członkowskie wymogu zapewnienia, aby operatorzy usług kluczowych i dostawcy usług cyfrowych wdrażali wymogi w zakresie cyberbezpieczeństwa i zgłaszali incydenty.

We wniosku uaktualniono istniejące ramy prawne z uwzględnieniem pogłębionej w ostatnich latach cyfryzacji rynku wewnętrznego oraz zmieniającego się krajobrazu zagrożeń cyberbezpieczeństwa. Oba te zjawiska nasiliły się jeszcze wyraźniej od początku kryzysu związanego z COVID-19. We wniosku usunięto także kilka niedociągnięć, które uniemożliwiły osiągnięcie pełnego potencjału dyrektywy w sprawie bezpieczeństwa sieci i informacji.

Pomimo zauważalnych osiągnięć okazało się, że dyrektywa w sprawie bezpieczeństwa sieci i informacji, która w wielu państwach członkowskich utorowała drogę do znaczącej zmiany w sposobie myślenia w odniesieniu do instytucjonalnego i regulacyjnego podejścia do cyberbezpieczeństwa, ma także pewne ograniczenia. Transformacja cyfrowa społeczeństwa (zintensyfikowana przez kryzys związany z COVID-19) spowodowała ewolucję krajobrazu zagrożeń i pojawianie się nowych wyzwań, które wymagają dostosowanych i innowacyjnych reakcji. Liczba cyberataków w dalszym ciągu rośnie; są one coraz bardziej wyrafinowane i pochodzą z wielu różnych źródeł w UE i poza jej granicami.

Na podstawie oceny funkcjonowania dyrektywy w sprawie bezpieczeństwa sieci i informacji przeprowadzonej na potrzeby oceny skutków zidentyfikowano następujące problemy: 1) niski poziom cyberodporności przedsiębiorstw działających w UE; 2) zróżnicowana odporność w poszczególnych państwach członkowskich i sektorach oraz 3) niski poziom wspólnej orientacji sytuacyjnej i brak wspólnego reagowania kryzysowego. Na przykład w jednym państwie członkowskim dyrektywa w sprawie bezpieczeństwa sieci i informacji nie obejmuje niektórych większych szpitali, w związku z czym nie są one zobowiązane do wdrożenia wynikających z niej środków w zakresie bezpieczeństwa, natomiast w innym państwie członkowskim niemal wszyscy świadczeniodawcy opieki zdrowotnej w tym państwie są objęci wymogami w zakresie bezpieczeństwa sieci i systemów informatycznych.

Ponieważ wniosek jest inicjatywą podjętą w ramach programu sprawności i wydajności regulacyjnej (REFIT), jego celem jest ograniczenie obciążenia regulacyjnego dla właściwych organów oraz kosztów przestrzegania przepisów dla podmiotów publicznych i prywatnych. Osiągnięciu tego celu służy w szczególności zniesienie spoczywającego na właściwych organach obowiązku identyfikacji operatorów usług kluczowych oraz podniesienie poziomu harmonizacji wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, aby ułatwić przestrzeganie przepisów podmiotom świadczącym usługi transgraniczne. Jednocześnie właściwe organy otrzymają także szereg nowych zadań, w tym nadzór nad podmiotami w sektorach dotychczas nieobjętych dyrektywą w sprawie bezpieczeństwa sieci i informacji.

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

Niniejszy wniosek stanowi element szerzej zakrojonego zestawu obowiązujących aktów prawnych i przyszłych inicjatyw na szczeblu unijnym, których celem jest zwiększenie odporności podmiotów publicznych i prywatnych na zagrożenia.

W dziedzinie cyberbezpieczeństwa są to zwłaszcza dyrektywa (UE) 2018/1972 ustanawiająca Europejski kodeks łączności elektronicznej (której przepisy dotyczące cyberbezpieczeństwa zostaną zastąpione przepisami niniejszego wniosku) oraz wniosek dotyczący rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (COM(2020) 595 final), które to przepisy – po wejściu w życie obu aktów – będą uznawane za *lex specialis* do dyrektywy, której dotyczy niniejszy wniosek.

W dziedzinie bezpieczeństwa fizycznego wniosek stanowi uzupełnienie wniosku dotyczącego dyrektywy w sprawie odporności podmiotów krytycznych, w którym zmieniono dyrektywę 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (dyrektywa w sprawie EIK) ustanawiającą unijny proces rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz określono podejście dotyczące poprawy ochrony takiej infrastruktury. W lipcu 2020 r. Komisja przyjęła strategię UE w zakresie unii bezpieczeństwa[1], w której uznano fakt coraz ściślejszego wzajemnego połączenia i współzależności między infrastrukturą fizyczną i cyfrową. Podkreślono w niej konieczność uspójnienia i ujednolicenia podejścia przyjętego w dyrektywie w sprawie EIK oraz w dyrektywie (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

Niniejszy wniosek jest zatem ściśle powiązany z wnioskiem dotyczącym dyrektywy w sprawie odporności podmiotów krytycznych, którego celem jest poprawa odporności

[1] COM(2020) 605 final.

podmiotów krytycznych na fizyczne zagrożenia w dużej liczbie sektorów. Wniosek ma na celu zapewnienie, aby na podstawie obu aktów prawnych właściwe organy przyjmowały środki uzupełniające i w razie potrzeby wymieniały informacje dotyczące cyberodporności i odporności w innych dziedzinach, a także aby szczególnie krytyczni operatorzy w sektorach uznanych w niniejszym wniosku za „niezbędne" również podlegali bardziej ogólnym obowiązkom w zakresie zwiększenia odporności, z naciskiem na ryzyko innego rodzaju niż ryzyko w cyberprzestrzeni.

- **Spójność z innymi politykami Unii**

Jak określono w komunikacie zatytułowanym „Kształtowanie cyfrowej przyszłości Europy"[2], Europa musi wykorzystać wszystkie możliwości, jakie daje epoka cyfrowa, a także wzmocnić swoje zdolności przemysłowe i innowacyjne, w granicach bezpieczeństwa i norm etycznych. W europejskiej strategii w zakresie danych wskazano cztery filary – ochronę danych, prawa podstawowe, bezpieczeństwo i cyberbezpieczeństwo – jako podstawowe warunki wstępne istnienia społeczeństwa posiadającego mocną pozycję dzięki korzystaniu z danych.

W rezolucji z dnia 12 marca 2019 r. Parlament Europejski wezwał „Komisję, by przeanalizowała potrzebę dalszego rozszerzania zakresu dyrektywy w sprawie bezpieczeństwa sieci i informacji na inne sektory i usługi krytyczne nieobjęte szczegółowymi przepisami sektorowymi"[3]. W konkluzjach z dnia 9 czerwca 2020 r. Rada z zadowoleniem przyjęła „plany Komisji dotyczące zapewnienia spójnych zasad dla podmiotów gospodarczych oraz ułatwienia bezpiecznej, rzetelnej i odpowiedniej wymiany informacji na temat zagrożeń i incydentów, w tym przez przegląd dyrektywy w sprawie bezpieczeństwa sieci i informacji, w celu zbadania możliwości zwiększenia cyberodporności i skuteczniejszego reagowania na cyberataki, w szczególności w odniesieniu do zasadniczej działalności gospodarczej i społecznej, przy jednoczesnym poszanowaniu kompetencji państw członkowskich, w tym ich odpowiedzialności za bezpieczeństwo narodowe"[4]. Ponadto proponowany akt prawny pozostaje bez uszczerbku dla stosowania reguł konkurencji określonych w Traktacie o funkcjonowaniu Unii Europejskiej (TFUE).

Zważywszy, że znacząca część zagrożeń dla cyberbezpieczeństwa ma swoje źródło poza UE, niezbędne jest przyjęcie spójnego podejścia do współpracy międzynarodowej. Niniejsza dyrektywa stanowi model odniesienia, który należy propagować w kontekście unijnej współpracy z państwami trzecimi, zwłaszcza jeżeli chodzi o zapewnianie zewnętrznej pomocy technicznej.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

Podstawę prawną dyrektywy w sprawie bezpieczeństwa sieci i informacji stanowi art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, którego celem jest ustanowienie i funkcjonowanie rynku wewnętrznego przez usprawnienie środków służących zbliżeniu przepisów krajowych. Jak orzekł Trybunał Sprawiedliwości Unii Europejskiej w wyroku w sprawie C-58/08 Vodafone i in., skorzystanie z art. 114 TFUE jest uzasadnione

[2] COM(2020) 67 final.
[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_PL.html
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/pl/pdf

w przypadku rozbieżności między przepisami krajowymi, jeśli mogą one wywierać bezpośredni wpływ na funkcjonowanie rynku wewnętrznego. Podobnie Trybunał orzekł, że gdy akt wydany na podstawie art. 114 TFUE doprowadził do usunięcia wszelkich przeszkód w wymianie handlowej w dziedzinie, która została przez ten akt zharmonizowana, prawodawca unijny nie może zostać pozbawiony możliwości dostosowania tego aktu do wszelkich zmian w okolicznościach lub do rozwoju wiedzy, mając na uwadze ciążące na nim zadanie dbania o ochronę uznanych przez traktat ogólnych interesów. Ponadto Trybunał stwierdził, że środki dotyczące zbliżenia objęte art. 114 TFUE mają na celu zapewnienie, w zależności od sytuacji ogólnej i okoliczności konkretnego przypadku w ramach harmonizowanej dziedziny, pewnego zakresu swobodnej oceny co do techniki zbliżania prawodawstwa, najwłaściwszej dla uzyskania zamierzonego rezultatu. Proponowany akt prawny usunie przeszkody w ustanowieniu i funkcjonowaniu rynku wewnętrznego dla podmiotów niezbędnych i istotnych, a także usprawniłby ustanowienie i funkcjonowanie tego rynku przez: ustanowienie jasnych powszechnie stosowanych przepisów dotyczących zakresu stosowania dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz harmonizację przepisów mających zastosowanie w dziedzinie zarządzania ryzykiem w cyberprzestrzeni oraz zgłaszania incydentów. Obecne rozbieżności w tej dziedzinie, zarówno na szczeblu legislacyjnym, jak i nadzorczym, a także na szczeblu krajowym i unijnym, stanowią przeszkodę dla rynku wewnętrznego, ponieważ podmioty prowadzące działalność transgraniczną muszą sprostać różnym, niekiedy nakładającym się na siebie, wymogom regulacyjnym lub ich rozbieżnemu stosowaniu, ze szkodą dla korzystania przez te podmioty ze swobody przedsiębiorczości oraz ze swobody świadczenia usług. Różne przepisy mają także negatywny wpływ na warunki konkurencji na rynku wewnętrznym, jeżeli chodzi o podmioty tego samego rodzaju w różnych państwach członkowskich.

- **Pomocniczość (w przypadku kompetencji niewyłącznych)**

Nie można osiągnąć skutecznej odporności pod względem cyberbezpieczeństwa w całej Unii, jeżeli podchodzi się do niej w zróżnicowany sposób za pomocą rozwiązań krajowych lub regionalnych. W dyrektywie w sprawie bezpieczeństwa sieci i informacji częściowo usunięto to niedociągnięcie przez ustanowienie ram dotyczących bezpieczeństwa sieci i systemów informatycznych na szczeblu krajowym i unijnym. Transpozycja i wdrażanie wspomnianej dyrektywy ujawniły jednak również niedociągnięcia i ograniczenia nieodłącznie związane z niektórymi przepisami lub podejściami, np. niejasne określenie zakresu dyrektywy prowadzące do znaczących różnic w zakresie i skali faktycznej interwencji UE na poziomie państw członkowskich. Ponadto od rozpoczęcia kryzysu związanego z COVID-19 europejska gospodarka stała się jeszcze bardziej zależna od sieci i systemów informatycznych niż kiedykolwiek wcześniej, a sektory i usługi są ze sobą coraz bardziej powiązane. Główne uzasadnienie interwencji UE wykraczającej poza obecne środki określone w dyrektywie w sprawie bezpieczeństwa sieci i informacji stanowią: (i) coraz bardziej transgraniczny charakter zagrożeń i wyzwań związanych z bezpieczeństwem sieci i systemów informatycznych; (ii) potencjał unijnych działań mających na celu usprawnienie i ułatwienie wprowadzania skutecznych i skoordynowanych polityk krajowych; oraz (iii) wpływ uzgodnionych i opierających się na współpracy działań z zakresu polityki na skuteczną ochronę danych i prywatności.

- **Proporcjonalność**

Przepisy proponowane w niniejszej dyrektywie nie wykraczają poza zakres niezbędny do osiągnięcia określonych celów w zadowalający sposób. Przewidziane dostosowanie i uproszczenie środków w zakresie bezpieczeństwa i obowiązków w zakresie zgłaszania

incydentów jest związane z wnioskami państw członkowskich i przedsiębiorstw o udoskonalenie obowiązujących ram.

W niniejszym wniosku uwzględniono praktyki już stosowane w państwach członkowskich. Wyższy poziom ochrony osiągnięty za pośrednictwem takich uproszczonych i skoordynowanych wymogów jest proporcjonalny do coraz poważniejszych zagrożeń, w tym zagrożeń o charakterze transgranicznym; wymogi te są racjonalne i zasadniczo odpowiadają interesowi podmiotów zaangażowanych w zapewnienie ciągłości i jakości swoich usług. Koszty zapewnienia systematycznej współpracy między państwami członkowskimi byłyby niskie w porównaniu z gospodarczymi i społecznymi startami i szkodami spowodowanymi przez cyberincydenty. Ponadto konsultacje z zainteresowanymi stronami przeprowadzone w kontekście przeglądu dyrektywy w sprawie bezpieczeństwa sieci i informacji, w tym wyniki otwartych konsultacji publicznych i ankiet skierowanych do określonych grup docelowych, świadczą o poparciu dla zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji zgodnie z określonymi wyżej kierunkami.

- **Wybór instrumentu**

W niniejszym wniosku wprowadza się dalsze uproszczenie obowiązków nałożonych na przedsiębiorstwa oraz zapewnia się wyższy poziom ich harmonizacji. Jednocześnie celem wniosku jest zapewnienie państwom członkowskim elastyczności niezbędnej do uwzględnienia specyfiki krajowej (np. możliwość określenia dodatkowych podmiotów niezbędnych lub podmiotów istotnych, która wykracza poza poziom bazowy określony w akcie prawnym). Przyszłym aktem prawnym powinna zatem być dyrektywa, ponieważ instrument ten umożliwia ukierunkowaną, lepszą harmonizację, a także zapewnia właściwym organom pewien stopień elastyczności.

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

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

Komisja przeprowadziła ocenę funkcjonowania dyrektywy w sprawie bezpieczeństwa sieci i informacji[5]. W ocenie tej przeanalizowano znaczenie dyrektywy, jej unijną wartość dodaną, spójność, skuteczność i efektywność. Główne ustalenia wynikające z analizy są następujące:

- Zakres dyrektywy w sprawie bezpieczeństwa sieci i informacji jest zbyt ograniczony pod względem sektorów, które dyrektywa ta obejmuje, głównie ze względu na: (i) pogłębioną cyfryzację, która nastąpiła w ostatnich latach, oraz rosnące wzajemne powiązania, (ii) zakres dyrektywy w sprawie bezpieczeństwa sieci i informacji, który nie obejmuje już wszystkich sektorów cyfrowych świadczących kluczowe usługi na rzecz gospodarki i całego społeczeństwa.
- Dyrektywa w sprawie bezpieczeństwa sieci i informacji nie jest wystarczająco jasna, jeżeli chodzi o jej zakres w odniesieniu do operatorów usług kluczowych, a jej przepisy nie są wystarczająco precyzyjne odnośnie do kompetencji krajowych względem dostawców usług cyfrowych. Doprowadziło to do sytuacji, w której nie we wszystkich państwach członkowskich zidentyfikowano niektóre rodzaje podmiotów, w związku z czym nie były one zobowiązane do wdrożenia środków bezpieczeństwa i zgłaszania incydentów.

[5] [Załącznik 5 do oceny skutków.]

- W dyrektywie w sprawie bezpieczeństwa sieci i informacji zapewniono państwom członkowskim duży margines swobody, jeżeli chodzi o ustanawianie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów dla operatorów usług kluczowych. Z oceny wynika, że w niektórych przypadkach państwa członkowskie wdrożyły te wymogi w bardzo różny sposób, co spowodowało dodatkowe obciążenie dla przedsiębiorstw działających w więcej niż jednym państwie członkowskim.
- System nadzoru i egzekwowania przepisów określony w dyrektywie w sprawie bezpieczeństwa sieci i informacji jest nieskuteczny. Na przykład państwa członkowskie bardzo niechętnie stosują kary względem podmiotów, które nie wdrożyły wymogów w zakresie bezpieczeństwa lub które nie zgłaszają incydentów. Może to mieć negatywny wpływ na cyberodporność poszczególnych podmiotów.
- Zasoby finansowe i ludzkie przeznaczone przez państwa członkowskie na wypełnienie ich zadań (takich jak identyfikacja operatorów usług kluczowych lub nadzór nad takimi operatorami) są bardzo różne, a w konsekwencji znacznie różnią się także poszczególne poziomy dojrzałości w postępowaniu z ryzykiem w cyberprzestrzeni. Pogłębia to jeszcze bardziej różnice w zakresie cyberodporności występujące między państwami członkowskimi.
- Państwa członkowskie nie prowadzą między sobą systematycznej wymiany informacji, co ma negatywny wpływ w szczególności na skuteczność środków w zakresie cyberbezpieczeństwa oraz na poziom wspólnej orientacji sytuacyjnej na szczeblu UE. Dotyczy to także informacji wymienianych między sobą przez podmioty prywatne oraz współdziałania między strukturami współpracy na szczeblu unijnym a podmiotami prywatnymi.

- **Konsultacje z zainteresowanymi stronami**

Komisja przeprowadziła konsultacje z wieloma zainteresowanymi stronami. Zaproszono państwa członkowskie i zainteresowane strony do udziału w otwartych konsultacjach publicznych oraz w ankietach i warsztatach organizowanych przez przedsiębiorstwo Wavestone, instytut CEPS oraz ICF, którym Komisja zleciła przeprowadzenie badania mającego na celu wsparcie przeglądu dyrektywy w sprawie bezpieczeństwa sieci i informacji. Wśród zainteresowanych stron, które wzięły udział w konsultacjach, znalazły się właściwe organy, organy Unii ds. cyberbezpieczeństwa, operatorzy usług kluczowych, dostawcy usług cyfrowych, podmioty świadczące usługi nieobjęte zakresem obowiązującej dyrektywy w sprawie bezpieczeństwa sieci i informacji, stowarzyszenia branżowe oraz organizacje konsumenckie i obywatele.

Ponadto Komisja jest w stałym kontakcie z właściwymi organami zajmującymi się wdrażaniem dyrektywy w sprawie bezpieczeństwa sieci i informacji. Grupa Współpracy prowadzi szeroko zakrojone prace dotyczące różnych przekrojowych i sektorowych aspektów wdrażania. Poza tym podczas wizyt krajowych dotyczących bezpieczeństwa sieci i systemów informatycznych, które odbyły się w latach 2019 i 2020, Komisja przeprowadziła wywiady ze 154 podmiotami publicznymi i prywatnymi, a także ze 117 właściwymi organami.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Komisja zleciła konsorcjum Wavestone, CEPS i ICF przeprowadzenie badania mającego na celu wsparcie Komisji w przeglądzie dyrektywy w sprawie bezpieczeństwa sieci i informacji[6]. Wykonawca nie tylko dotarł do zainteresowanych stron, na które dyrektywa w sprawie bezpieczeństwa sieci i informacji miała bezpośredni wpływ, za pośrednictwem ankiet skierowanych do określonych grup docelowych i warsztatów, ale także przeprowadził konsultacje z szerokim gronem ekspertów w dziedzinie cyberbezpieczeństwa, takich jak naukowcy zajmujący się kwestią cyberbezpieczeństwa oraz specjaliści z branży cyberbezpieczeństwa.

- **Ocena skutków**

Niniejszemu wnioskowi towarzyszy ocena skutków[7], która została przedłożona Radzie ds. Kontroli Regulacyjnej dnia 23 października 2020 r. i dnia 20 listopada 2020 r. otrzymała jej pozytywną opinię z uwagami. Rada ds. Kontroli Regulacyjnej zaleciła wprowadzenie usprawnień w niektórych obszarach w celu: 1) lepszego odzwierciedlenia roli transgranicznych efektów zewnętrznych w analizie problemu; 2) lepszego wyjaśnienia, na czym ma polegać sukces inicjatywy; 3) bardziej szczegółowego uzasadnienia wykazu wariantów strategicznych; 4) bardziej szczegółowego opracowania kosztów proponowanych środków. Ocenę skutków dostosowano tak, aby uwzględnić w niej te punkty, a także bardziej szczegółowe uwagi Rady ds. Kontroli Regulacyjnej. Zawiera ona teraz bardziej szczegółowe wyjaśnienia dotyczące roli transgranicznych efektów zewnętrznych w dziedzinie cyberbezpieczeństwa, wyraźniejsze zestawienie dotyczące pomiaru efektów inicjatywy, bardziej szczegółowe wyjaśnienie konstrukcji i logiki poszczególnych wariantów strategicznych i działań rozważanych w ramach tych wariantów, bardziej szczegółowe wyjaśnienie aspektów analizowanych w związku z zakresem sektorowym dyrektywy w sprawie bezpieczeństwa sieci i informacji, a także bardziej szczegółowe wyjaśnienia dotyczące kosztów.

Komisja rozważyła szereg wariantów strategicznych dotyczących udoskonalenia ram prawnych w obszarze cyberodporności i reagowania na incydenty:

- „brak działań”: dyrektywa w sprawie bezpieczeństwa sieci i informacji pozostałaby niezmieniona i nie zostałyby wdrożone żadne inne środki o charakterze nieustawodawczym służące rozwiązaniu problemów zidentyfikowanych w ocenie dyrektywy w sprawie bezpieczeństwa sieci i informacji;
- wariant 1: brak zmian na poziomie ustawodawczym. Zamiast tego Komisja – po przeprowadzeniu konsultacji z Grupą Współpracy, Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz, w stosownych przypadkach, z siecią zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) – wydałaby zalecenia i wytyczne (np. dotyczące identyfikacji operatorów usług kluczowych, wymogów w zakresie bezpieczeństwa, procedur zgłaszania incydentów oraz nadzoru);
- wariant 2: wariant ten obejmuje ukierunkowane zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji, obejmujące rozszerzenie jej zakresu oraz kilka

[6] Badanie mające na celu wsparcie przeglądu dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa w sprawie bezpieczeństwa sieci i informacji) – nr 2020-665. Wavestone, CEPS i ICF.

[7] **[Należy wstawić linki do ostatecznej wersji dokumentu oraz do streszczenia.]**

innych zmian służących zapewnieniu pewnych natychmiastowych rozwiązań zidentyfikowanych problemów, które zapewniłyby większą jasność i dalszą harmonizację (np. przepisy służące harmonizacji progów identyfikacji). W zmienionej dyrektywie w sprawie bezpieczeństwa sieci i informacji zachowano by jednak najistotniejsze elementy leżące u podstaw polityki, podejście i założenia;

- wariant 3: scenariusz ten obejmuje systemowe i strukturalne zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji (za pośrednictwem nowej dyrektywy) uwzględniające bardziej fundamentalną zmianę podejścia w kierunku objęcia zakresem dyrektywy szerszego segmentu gospodarek w całej Unii, przy założeniu jednak bardziej skoncentrowanego nadzoru ukierunkowanego na duże i kluczowe podmioty. Scenariusz ten zakładałby także uproszczenie obowiązków nałożonych na przedsiębiorstwa i zapewnienie wyższego poziomu ich harmonizacji, utworzenie otoczenia sprzyjającego skuteczniejszemu wdrażaniu aspektów operacyjnych, a także ustanowienie klarownej podstawy rozszerzonych wspólnych obowiązków i odpowiedzialności różnych zainteresowanych stron, jeżeli chodzi o środki w zakresie cyberbezpieczeństwa.

W ocenie skutków stwierdzono, że preferowanym wariantem jest wariant 3 (tj. systemowe i strukturalne zmiany ram prawnych dotyczących bezpieczeństwa sieci i systemów informatycznych). Pod względem skuteczności preferowanym wariantem byłoby wyraźne określenie zakresu stosowania dyrektywy w sprawie bezpieczeństwa sieci i informacji rozszerzonego na bardziej reprezentatywną część gospodarek i społeczeństw UE, a także uproszczenie wymogów wraz z doprecyzowaniem ram dotyczących nadzoru i egzekwowania, które miałyby na celu podniesienie poziomu zgodności. Scenariusz ten obejmuje także środki ukierunkowane na usprawnienie podejść do tworzenia polityki na poziomie państw członkowskich oraz zmianę ich paradygmatu, propagowanie nowych ram zarządzania ryzykiem związanym z relacjami z dostawcami oraz skoordynowane ujawnianie podatności. Jednocześnie w ramach preferowanego wariantu strategicznego ustanawia się jasną podstawę wspólnych obowiązków i odpowiedzialności oraz przewiduje się mechanizmy służące budowaniu większego zaufania między państwami członkowskimi, zarówno między organami, jak i branżami, które będą zachęcać do wymiany informacji oraz zapewniać bardziej operacyjne podejście, takie jak mechanizmy wzajemnej pomocy i wzajemnej oceny. Wariant ten zapewniłby także unijne ramy zarządzania kryzysowego, opierające się na uruchomionej niedawno unijnej sieci operacyjnej, a także większe zaangażowanie ENISA, w ramach jej obecnego mandatu, w przeprowadzanie dokładnego przeglądu stanu cyberbezpieczeństwa w Unii.

Pod względem efektywności preferowany wariant wiązałby się z dodatkowymi kosztami przestrzegania i egzekwowania przepisów dla przedsiębiorstw i państw członkowskich, prowadziłby jednak również do efektywnych kompromisów i synergii; spośród wszystkich przeanalizowanych wariantów strategicznych wariant ten ma największy potencjał, jeżeli chodzi o zapewnienie wysokiego i spójnego poziomu cyberodporności kluczowych podmiotów w całej Unii, co ostatecznie doprowadziłoby do oszczędności kosztów zarówno dla przedsiębiorstw, jak i dla społeczeństwa. Ten wariant strategiczny prowadziłby do pewnego dodatkowego obciążenia administracyjnego i dodatkowych kosztów przestrzegania przepisów dla organów państw członkowskich. W perspektywie średnio- i długoterminowej wariant ten przyniósłby jednak średnio znaczące korzyści dzięki ściślejszej współpracy między państwami członkowskimi, w tym na szczeblu operacyjnym, a także przyczyniłby się – za pośrednictwem mechanizmów wzajemnej pomocy i wzajemnej oceny oraz dokładniejszego przeglądu kluczowych przedsiębiorstw oraz interakcji z nimi – do ogólnego wzrostu zdolności w zakresie cyberbezpieczeństwa na szczeblu krajowym i regionalnym.

Preferowany wariant strategiczny zapewniłby także dużą spójność z innymi przepisami, inicjatywami lub środkami z zakresu polityki, w tym z sektorowym *lex specialis*.

Zaradzenie występującym obecnie brakom, jeżeli chodzi o gotowość w obszarze cyberbezpieczeństwa na szczeblu państw członkowskich oraz na poziomie przedsiębiorstw i innych organizacji, może przyczynić się do zwiększenia efektywności i ograniczenia dodatkowych kosztów wynikających z cyberincydentów.

- Z perspektywy podmiotów niezbędnych i istotnych podniesienie poziomu gotowości w obszarze cyberbezpieczeństwa może doprowadzić do ograniczenia zakresu potencjalnego uszczuplenia dochodów z powodu zakłóceń – w tym spowodowanych przez szpiegostwo przemysłowe – oraz ogromnych wydatków na niwelowanie zagrożeń *ad hoc*. Korzyści takie prawdopodobnie przeważą nad kosztami niezbędnych inwestycji. Zmniejszenie fragmentacji rynku wewnętrznego przyczyniłoby się również do wyrównania warunków działania wśród operatorów.
- Z perspektywy państw członkowskich może to jeszcze bardziej ograniczyć ryzyko wzrostu wydatków budżetowych na niwelowanie zagrożeń *ad hoc* oraz dodatkowych kosztów w przypadku wystąpienia sytuacji krytycznych związanych z cyberincydentami.
- Z perspektywy obywateli zaradzenie cyberincydentom powinno przyczynić się do ograniczenia zakresu uszczuplenia dochodów spowodowanego zakłóceniami gospodarczymi.

Wyższy poziom cyberbezpieczeństwa we wszystkich państwach członkowskich oraz możliwość szybkiego reagowania na incydent przez przedsiębiorstwa i organy oraz łagodzenia jego skutków prawdopodobnie przyczynią się do ogólnego wzrostu zaufania obywateli do gospodarki cyfrowej, co może mieć pozytywny wpływ ma wzrost gospodarczy i inwestycje.

Wzrost ogólnego poziomu cyberbezpieczeństwa prawdopodobnie przyczyni się do wzrostu ogólnego poziomu bezpieczeństwa oraz do płynnego, niezakłóconego funkcjonowania usług kluczowych, które mają podstawowe znaczenie dla społeczeństwa. Inicjatywa może także przełożyć się na inne skutki społeczne, takie jak obniżenie poziomu cyberprzestępczości i terroryzmu oraz wzrost poziomu ochrony ludności. Wzrost poziomu gotowości przedsiębiorstw i innych organizacji do reagowania w obszarze cyberbezpieczeństwa może przyczynić się do uniknięcia potencjalnych strat finansowych w wyniku cyberataków, a tym samym do zapobieżenia konieczności zwalniania pracowników.

Wzrost ogólnego poziomu cyberbezpieczeństwa może także prowadzić do zapobiegania zagrożeniom i szkodom dla środowiska w przypadku ataku na usługę kluczową. Może to dotyczyć w szczególności sektorów energetyki, zaopatrzenia w wodę i jej dystrybucji lub transportu. Dzięki wzmocnieniu zdolności w zakresie cyberbezpieczeństwa inicjatywa może prowadzić do większego wykorzystania infrastruktury i usług ICT najnowszej generacji, które są także bardziej zrównoważone pod względem środowiskowym, a także do zastąpienia nieefektywnej i mniej bezpiecznej dotychczasowej infrastruktury. Oczekuje się, że inicjatywa przyczyni się także do ograniczenia liczby kosztownych cyberincydentów, co uwolni zasoby na zrównoważone inwestycje.

- **Sprawność regulacyjna i uproszczenie**

We wniosku przewidziano ogólne wyłączenie z zakresu ram prawnych dotyczących bezpieczeństwa sieci i informacji mikro- i małych podmiotów, a także stosowanie lżejszego

systemu nadzoru *ex post* do dużej liczby nowych podmiotów objętych zakresem zmienionej dyrektywy (tzw. podmioty istotne). Celem tych środków jest ograniczenie do minimum oraz zrównoważenie obciążenia nakładanego na przedsiębiorstwa i administrację publiczną. Ponadto we wniosku zastępuje się złożony system identyfikacji operatorów usług kluczowych obowiązkiem mającym ogólne zastosowanie, a także wprowadza się wyższy poziom harmonizacji obowiązków w zakresie bezpieczeństwa i zgłaszania incydentów, co może zmniejszyć obciążenie związane z przestrzeganiem przepisów, zwłaszcza w przypadku podmiotów świadczących usługi transgraniczne.

We wniosku ogranicza się do minimum koszty przestrzegania przepisów dla MŚP, gdyż podmioty są zobowiązane do wdrożenia wyłącznie tych środków, które są niezbędne, aby zapewnić poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka.

- **Prawa podstawowe**

UE dąży do zapewnienia najwyższych standardów ochrony praw podstawowych. Wszelka dobrowolna wymiana informacji między podmiotami, do której zachęca się w niniejszej dyrektywie, odbywałaby się w zaufanym otoczeniu z pełnym poszanowaniem unijnych przepisów o ochronie danych, zwłaszcza rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[8].

4. WPŁYW NA BUDŻET

Zob. część finansowa

5. ELEMENTY FAKULTATYWNE

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

Wniosek obejmuje ogólny plan monitorowania i oceny wpływu na konkretne cele, co wymaga od Komisji przeprowadzenia przeglądu co najmniej [54 miesiące] od daty wejścia w życie oraz przedłożenia sprawozdania dla Parlamentu Europejskiego i Rady w sprawie głównych ustaleń tego przeglądu.

Przegląd przeprowadza się zgodnie z wytycznymi Komisji dotyczącymi lepszego stanowienia prawa.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

We wniosku skupiono się na kilku głównych obszarach polityki, które są ze sobą powiązane, a jego celem jest podniesienie poziomu cyberbezpieczeństwa w Unii.

Przedmiot i zakres (art. 1 i 2)

Dyrektywa w szczególności: a) określa obowiązki spoczywające na państwach członkowskich, dotyczące przyjęcia krajowej strategii cyberbezpieczeństwa, wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz CSIRT; b) stanowi, że państwa członkowskie muszą określić obowiązki związane z zarządzaniem

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

ryzykiem w cyberprzestrzeni oraz zgłaszaniem incydentów spoczywające na podmiotach, które w załączniku I nazywa się podmiotami niezbędnymi, a w załączniku II – podmiotami istotnymi; c) stanowi, że państwa członkowskie muszą określić obowiązki w zakresie wymiany informacji na temat cyberbezpieczeństwa.

Dyrektywa ma zastosowanie do niektórych publicznych lub prywatnych podmiotów niezbędnych działających w sektorach wymienionych w załączniku I (energetyki; transportu; bankowości; infrastruktury rynków finansowych; służby zdrowia; wody pitnej; ścieków; infrastruktury cyfrowej; administracji publicznej i przestrzeni kosmicznej), a także do niektórych podmiotów istotnych działających w sektorach wymienionych w załączniku II (usługi pocztowe i kurierskie; gospodarka odpadami; wytwarzanie, produkcja i dystrybucja chemikaliów; produkcja, przetwarzanie i dystrybucja żywności; wytwarzanie i dostawcy usług cyfrowych). W rozumieniu zalecenia Komisji 2003/361/WE z dnia 6 maja 2003 r. mikro- i małe podmioty są wyłączone z zakresu dyrektywy, z wyjątkiem dostawców sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej, dostawców usług zaufania, rejestrów nazw domen najwyższego poziomu (TLD) i administracji publicznej oraz niektórych innych podmiotów, takich jak wyłączny dostawca usługi w jakimś państwie członkowskim.

Krajowe ramy dotyczące cyberbezpieczeństwa (art. 5–11)

Państwa członkowskie są zobowiązane do przyjęcia krajowej strategii cyberbezpieczeństwa określającej cele strategiczne oraz odpowiednie środki polityczne i regulacyjne mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa.

W dyrektywie ustanawia się także ramy skoordynowanego ujawniania podatności oraz wymaga się, aby państwa członkowskie wyznaczyły CSIRT, by pełniły one rolę zaufanych pośredników i ułatwiały interakcję między podmiotami zgłaszającymi a producentami lub dostawcami produktów i usług ICT. ENISA jest zobowiązana do rozwijania i utrzymywania europejskiego rejestru podatności dotyczącego wykrytych podatności.

Państwa członkowskie są zobowiązane do wdrożenia krajowych ram zarządzania kryzysami cyberbezpieczeństwa, m.in. przez wyznaczenie właściwych organów krajowych odpowiedzialnych za zarządzanie cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę.

Państwa członkowskie są również zobowiązane do wyznaczenia co najmniej jednego właściwego organu krajowego ds. cyberbezpieczeństwa, który będzie wykonywał zadania nadzorcze na podstawie niniejszej dyrektywy, a także krajowego pojedynczego punktu kontaktowego do spraw cyberbezpieczeństwa, który będzie pełnił funkcję łącznikową w celu zapewnienia transgranicznej współpracy organów państw członkowskich. Państwa członkowskie są także zobowiązane do wyznaczenia CSIRT.

Współpraca (art. 12–16)

W dyrektywie ustanawia się Grupę Współpracy, aby wspierać i ułatwiać strategiczną współpracę i wymianę informacji między państwami członkowskimi oraz rozwijać zaufanie i pewność; Ponadto ustanawia się sieć CSIRT, aby przyczyniać się do rozwijania pewności i zaufania między państwami członkowskimi oraz promować szybką i skuteczną współpracę operacyjną.

Ustanawia się europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe), aby wspierać skoordynowane zarządzanie cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę oraz zapewniać regularną wymianę informacji między państwami członkowskimi a instytucjami UE.

ENISA jest zobowiązana do wydawania co dwa lata, we współpracy z Komisją, sprawozdania o stanie cyberbezpieczeństwa w Unii.

Komisja jest zobowiązana do ustanowienia systemu wzajemnej oceny umożliwiającego regularną wzajemną ocenę skuteczności polityk cyberbezpieczeństwa państw członkowskich.

Zarządzanie ryzykiem w cyberprzestrzeni i obowiązki w zakresie zgłaszania incydentów (art. 17–23)

W dyrektywie nakłada się na państwa członkowskie obowiązek zapewnienia, aby organy zarządzające wszystkich podmiotów objętych jej zakresem zatwierdziły środki w zakresie zarządzania ryzykiem w cyberprzestrzeni przyjęte przez odpowiednie podmioty oraz uczestniczyły w specjalnych szkoleniach poświęconych cyberbezpieczeństwu.

Państwa członkowskie są zobowiązane do zapewnienia, aby podmioty objęte zakresem dyrektywy stosowały odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem w cyberprzestrzeni stwarzanym dla bezpieczeństwa sieci i systemów informatycznych. Są one zobowiązane także do zapewnienia, aby podmioty powiadamiały właściwe organy krajowe lub CSIRT o każdym cyberincydencie mającym znaczący wpływ na świadczenie usługi, za którą odpowiadają te podmioty.

Rejestry TLD oraz podmioty świadczące usługi rejestracji nazwy domeny dla TLD powinny gromadzić i utrzymywać precyzyjne i kompletne dane dotyczące rejestracji nazw domen. Ponadto takie podmioty są zobowiązane do zapewnienia wnioskodawcom ubiegającym się o prawnie uzasadniony dostęp efektywnego dostępu do danych dotyczących rejestracji domeny.

Jurysdykcja i rejestracja (art. 24 i 25)

Co do zasady uznaje się, że podmioty niezbędne i istotne podlegają jurysdykcji państwa członkowskiego, w którym świadczą usługi. Niektóre rodzaje podmiotów (dostawców usług DNS, rejestry nazw TLD, dostawców usług w chmurze, dostawców usług ośrodka przetwarzania danych oraz dostawców sieci dostarczania treści, a także niektórych dostawców usług cyfrowych) uznaje się jednak za podlegające jurysdykcji państwa członkowskiego, w którym znajduje się główna jednostka organizacyjna danego podmiotu w Unii. Ma to na celu zapewnienie, aby takie podmioty nie musiały spełniać wielu różnych wymogów prawnych ze względu na fakt, iż w stosunkowo dużym zakresie świadczą swoje usługi w wymiarze transgranicznym. ENISA jest zobowiązana do utworzenia i prowadzenia rejestru tych ostatnich podmiotów.

Wymiana informacji (art. 26 i 27)

Państwa członkowskie zapewniają przepisy umożliwiające podmiotom podjęcie wymiany informacji związanych z cyberbezpieczeństwem w ramach szczegółowych rozwiązań dotyczących przekazywania informacji na temat cyberbezpieczeństwa zgodnie z art. 101 TFUE. Ponadto państwa członkowskie muszą umożliwić podmiotom nieobjętym zakresem

niniejszej dyrektywy zgłaszanie – na zasadzie dobrowolności – znaczących incydentów, cyberzagrożeń lub zdarzeń potencjalnie wypadkowych.

Nadzór i egzekwowanie przepisów (art. 28–34)

Właściwe organy są zobowiązane do sprawowania nadzoru nad podmiotami objętymi zakresem niniejszej dyrektywy, a w szczególności do zapewnienia przestrzegania przez nie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów. W dyrektywie rozróżnia się system nadzoru *ex ante* dotyczący podmiotów niezbędnych i system nadzoru *ex post* dotyczący podmiotów istotnych, w ramach którego właściwe organy są zobowiązane do podejmowania działań, jeżeli zostaną im dostarczone dowody lub wskazanie, że podmiot istotny nie spełnia wymogów dotyczących bezpieczeństwa i zgłaszania incydentów.

W dyrektywie zobowiązuje się państwa członkowskie także do nakładania na podmioty niezbędne i istotne administracyjnych kar pieniężnych oraz definiuje się określone maksymalne poziomy kar.

Państwa członkowskie są zobowiązane do współpracy i świadczenia sobie w stosownych przypadkach wzajemnej pomocy, w przypadku gdy podmioty świadczą usługi w więcej niż jednym państwie członkowskim lub jeżeli główna jednostka organizacyjna danego podmiotu lub jego przedstawiciel znajdują się w jednym państwie członkowskim, ale jego sieci i systemy informatyczne znajdują się w innym państwie członkowskim lub kilku innych państwach członkowskich.

2020/0359 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[9],

uwzględniając opinię Komitetu Regionów[10],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Celem dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148[11] było zbudowanie zdolności w zakresie cyberbezpieczeństwa w całej Unii, łagodzenie zagrożeń dla sieci i systemów informatycznych wykorzystywanych do celów świadczenia usług kluczowych w kluczowych sektorach oraz zapewnienie ciągłości takich usług w sytuacji zaistnienia cyberincydentów, a tym samym przyczynienie się do sprawnego funkcjonowania gospodarki i społeczeństwa Unii.

(2) Od momentu wejścia w życie dyrektywy (UE) 2016/1148 poczyniono znaczne postępy, jeżeli chodzi o podnoszenie poziomu odporności Unii pod względem cyberbezpieczeństwa. Przegląd tej dyrektywy pokazał, że stanowiła ona katalizator dla instytucjonalnego i regulacyjnego podejścia do cyberbezpieczeństwa w Unii, torując drogę do znaczącej zmiany w sposobie myślenia. Dyrektywa ta zapewniła ukończenie tworzenia krajowych ram przez określenie krajowych strategii cyberbezpieczeństwa, ustanowienie krajowych zdolności oraz wdrożenie środków regulacyjnych obejmujących niezbędną infrastrukturę i podmioty zidentyfikowane przez każde państwo członkowskie. Przyczyniła się ona także do współpracy na szczeblu unijnym dzięki ustanowieniu Grupy Współpracy[12] oraz sieci krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego („sieć CSIRT”)[13]. Pomimo tych

---

9 Dz.U. C […] z […], s. […].

10 Dz.U. C […] z […], s. […].

11 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 194/1 z 19.7.2016, s. 1).

12 Art. 11 dyrektywy (UE) 2016/1148.

13 Art. 12 dyrektywy (UE) 2016/1148.

osiągnąć przegląd dyrektywy (UE) 2016/1148 ujawnił tkwiące w niej braki, które uniemożliwiają skuteczne zaradzenie obecnym i pojawiającym się wyzwaniom w zakresie cyberbezpieczeństwa.

(3) Wraz z szybko postępującą transformacją cyfrową i siecią wzajemnych połączeń, jakie charakteryzują społeczeństwo, w tym w kontekście wymiany transgranicznej, sieci i systemy informatyczne stały się zasadniczym elementem codziennego życia. Zmiana ta doprowadziła do ewolucji krajobrazu zagrożeń dla cyberbezpieczeństwa, przynosząc nowe wyzwania, które wymagają dostosowanych, skoordynowanych i innowacyjnych reakcji we wszystkich państwach członkowskich. Liczba, skala, zaawansowanie, częstotliwość oraz wpływ cyberincydentów stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. W rezultacie cyberincydenty mogą utrudniać prowadzenie działalności gospodarczej na rynku wewnętrznym, powodować straty finansowe, podważać zaufanie użytkowników oraz powodować poważne straty dla gospodarki Unii i jej społeczeństwa. W związku z powyższym gotowość i skuteczność w obszarze cyberbezpieczeństwa są teraz bardziej istotne dla prawidłowego funkcjonowania rynku wewnętrznego niż kiedykolwiek wcześniej.

(4) Podstawę prawną dyrektywy (UE) 2016/1148 stanowił art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), którego celem jest ustanowienie i funkcjonowanie rynku wewnętrznego przez usprawnienie środków służących zbliżeniu przepisów krajowych. Wymogi w zakresie cyberbezpieczeństwa nałożone na podmioty świadczące usługi lub prowadzące działalność istotną z ekonomicznego punktu widzenia różnią się znacznie w zależności od państwa członkowskiego pod względem rodzaju wymogów, ich poziomu szczegółowości oraz metody nadzoru. Rozbieżności te pociągają za sobą dodatkowe koszty i powodują trudności dla podmiotów, które oferują towary lub usługi w wymiarze transgranicznym. Wymogi nałożone przez jedno państwo członkowskie, które różnią się od wymogów nałożonych przez inne państwo członkowskie lub są nawet z nimi sprzeczne, mogą w istotny sposób wpływać na taką transgraniczną działalność. Ponadto ewentualna nieoptymalna konstrukcja norm dotyczących cyberbezpieczeństwa lub ewentualny nieoptymalny sposób ich wdrażania prawdopodobnie będą miały negatywny wpływ na poziom cyberbezpieczeństwa innych państw członkowskich, zwłaszcza biorąc pod uwagę intensywną wymianę transgraniczną. Z przeglądu dyrektywy (UE) 2016/1148 wynika, że istnieją znaczne rozbieżności, jeżeli chodzi o jej wdrażanie przez państwa członkowskie, w tym w odniesieniu do jej zakresu, w odniesieniu do którego pozostawiono państwom członkowskim duży margines swobody. W dyrektywie (UE) 2016/1148 zapewniono państwom członkowskim bardzo duży margines swobody także w odniesieniu do wdrażania określonych w niej obowiązków dotyczących bezpieczeństwa i zgłaszania incydentów. W rezultacie obowiązki te wdrożono na szczeblu krajowym w bardzo różny sposób. Podobny rozdźwięk we wdrażaniu miał miejsce w odniesieniu do przepisów wspomnianej dyrektywy dotyczących nadzoru i egzekwowania przepisów.

(5) Wszystkie te rozbieżności pociągają za sobą fragmentację rynku wewnętrznego i mogą mieć szkodliwy wpływ na jego funkcjonowanie, oddziałując w szczególności na transgraniczne świadczenie usług i poziom odporności pod względem cyberbezpieczeństwa ze względu na stosowanie różnych norm. Celem niniejszej dyrektywy jest zatem wyeliminowanie takich rozbieżności między państwami członkowskimi, w szczególności przez określenie minimalnych przepisów dotyczących funkcjonowania skoordynowanych ram regulacyjnych, ustanowienie

mechanizmów skutecznej współpracy między odpowiedzialnymi organami w każdym państwie członkowskim, dokonanie aktualizacji wykazu sektorów i działań podlegających obowiązkom w zakresie cyberbezpieczeństwa oraz ustanowienie skutecznych środków naprawczych i sankcji, które są kluczowe dla skutecznego egzekwowania tych obowiązków. Dyrektywę (UE) 2016/1148 należy zatem uchylić i zastąpić niniejszą dyrektywą.

(6) Niniejsza dyrektywa nie wpływa na możliwość zastosowania przez państwa członkowskie środków niezbędnych do zapewnienia ochrony podstawowych interesów ich bezpieczeństwa, do ochrony porządku publicznego i bezpieczeństwa publicznego oraz do umożliwienia prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw zgodnie z prawem Unii. Zgodnie z art. 346 TFUE żadne państwo członkowskie nie ma obowiązku udzielania informacji, których ujawnienie jest sprzeczne z podstawowymi interesami jego bezpieczeństwa publicznego. W tym kontekście zastosowanie mają krajowe i unijne przepisy dotyczące ochrony informacji niejawnych, umowy o zachowaniu poufności oraz nieformalne porozumienia o zachowaniu poufności, takie jak kod poufności TLP[14].

(7) Wraz z uchyleniem dyrektywy (UE) 2016/1148 należy rozszerzyć zakres stosowania przepisów przez poszczególne sektory na większą część gospodarki ze względów przedstawionych w motywach 4–6. Wykaz sektorów objętych dyrektywą (UE) 2016/1148 należy zatem rozszerzyć, aby zapewnić całościowe uwzględnienie sektorów i usług mających istotne znaczenie dla kluczowych rodzajów działalności społecznej i gospodarczej w ramach rynku wewnętrznego. Przepisy nie powinny się różnić w zależności od tego, czy podmioty są operatorami usług kluczowych czy dostawcami usług cyfrowych. Rozróżnienie to okazało się nieaktualne, ponieważ nie odzwierciedla faktycznego znaczenia sektorów lub usług dla działalności społecznej i gospodarczej na rynku wewnętrznym.

(8) Zgodnie z dyrektywą (UE) 2016/1148 państwa członkowskie były odpowiedzialne za określanie, które podmioty spełniają kryteria decydujące o uznaniu ich za operatorów usług kluczowych („proces identyfikacji”). Aby wyeliminować znaczne rozbieżności w tym zakresie między państwami członkowskimi oraz zapewnić wszystkim właściwym podmiotom pewność prawa w odniesieniu do wymogów dotyczących zarządzania ryzykiem i obowiązków w zakresie zgłaszania incydentów, należy ustanowić jednolite kryterium decydujące o tym, które podmioty są objęte zakresem stosowania niniejszej dyrektywy. Kryterium to powinno przewidywać stosowanie zasady maksymalnej wielkości, zgodnie z którą w zakres dyrektywy wchodzą wszystkie średnie i duże przedsiębiorstwa zdefiniowane w zaleceniu Komisji 2003/361/WE[15], które działają w sektorach objętych zakresem niniejszej dyrektywy lub świadczą rodzaj usług objęty zakresem niniejszej dyrektywy. Państwa członkowskie nie powinny być zobowiązane do ustanowienia wykazu podmiotów, które spełniają to mające ogólne zastosowanie kryterium związane z wielkością.

(9) Zakres niniejszej dyrektywy powinien jednak obejmować także małe podmioty lub mikropodmioty spełniające określone kryteria, które wskazują na zasadnicze

[14] Kod poufności TLP (Traffic Light Protocol) to oznaczenie, za pomocą którego osoba udostępniająca informacje może poinformować odbiorców tych informacji o wszelkich ograniczeniach w zakresie dalszego ich rozpowszechniania. Z kodu tego korzystają niemal wszystkie społeczności CSIRT oraz niektóre ośrodki wymiany i analizy informacji.

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

znaczenie tych podmiotów dla gospodarek lub społeczeństw państw członkowskich lub dla konkretnych sektorów lub rodzajów usług. Państwa członkowskie powinny być odpowiedzialne za ustanowienie wykazu takich podmiotów i powinny przedłożyć go Komisji.

(10) Komisja, we współpracy z Grupą Współpracy, może sformułować wytyczne dotyczące wdrażania kryteriów mających zastosowanie do mikroprzedsiębiorstw i małych przedsiębiorstw.

(11) W zależności od sektora działalności lub rodzaju świadczonych usług podmioty objęte zakresem niniejszej dyrektywy należy podzielić na dwie kategorie: podmioty niezbędne i podmioty istotne. W podziale tym należy uwzględnić poziom krytyczności sektora lub rodzaju usługi, a także poziom zależności innych sektorów lub rodzajów usług. Zarówno podmioty niezbędne, jak i podmioty istotne powinny podlegać tym samym wymogom w zakresie zarządzania ryzykiem i tym samym obowiązkom w zakresie zgłaszania incydentów. Należy natomiast zróżnicować systemy nadzoru i kar między tymi dwoma kategoriami podmiotów, aby zapewnić odpowiednią równowagę między wymogami i obowiązkami z jednej strony a obciążeniem administracyjnym wynikającym z nadzoru nad zgodnością z przepisami z drugiej.

(12) Przepisy i instrumenty sektorowe mogą przyczynić się do zapewnienia wysokiego poziomu cyberbezpieczeństwa przy jednoczesnym uwzględnieniu w pełni specyfiki i złożoności tych sektorów. W przypadku gdy na mocy unijnego sektorowego aktu prawnego podmioty niezbędne lub istotne zobowiązano do przyjęcia środków zarządzania ryzykiem w cyberprzestrzeni lub zgłaszania incydentów lub znaczących cyberzagrożeń, które to wymogi mają skutki co najmniej równoważne skutkowi, jaki wywierają obowiązki przewidziane w niniejszej dyrektywie, powinny mieć zastosowanie takie przepisy sektorowe, w tym przepisy dotyczące nadzoru i egzekwowania przepisów. Komisja może wydać wytyczne w związku z wdrożeniem *lex specialis*. Niniejsza dyrektywa nie stanowi przeszkody dla przyjęcia dodatkowych sektorowych aktów Unii dotyczących środków zarządzania ryzykiem w cyberprzestrzeni i zgłaszania incydentów. Niniejsza dyrektywa pozostaje bez uszczerbku dla istniejących uprawnień wykonawczych, które powierzono Komisji w wielu sektorach, w tym w sektorach transportu i energetyki.

(13) Rozporządzenie Parlamentu Europejskiego i Rady XXXX/XXXX[16] należy uznać w kontekście niniejszej dyrektywy za unijny sektorowy akt prawny w odniesieniu do podmiotów sektora finansowego. Zamiast przepisów ustanowionych w niniejszej dyrektywie zastosowanie powinny mieć przepisy rozporządzenia XXXX/XXXX dotyczące środków zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (ICT), zarządzania incydentami związanymi z ICT, a zwłaszcza zgłaszania incydentów, a także testowania operacyjnej odporności cyfrowej, mechanizmów wymiany informacji oraz ryzyka związanego z zewnętrznymi dostawcami ICT. Do żadnych podmiotów objętych rozporządzeniem XXXX/XXXX państwa członkowskie nie powinny zatem stosować przepisów niniejszej dyrektywy dotyczących zarządzania ryzykiem w cyberprzestrzeni, obowiązków w zakresie zgłaszania incydentów, wymiany informacji oraz nadzoru i egzekwowania przepisów. Jednocześnie istotne jest, aby utrzymać silne relacje i skuteczną wymianę informacji z sektorem finansowym na gruncie niniejszej dyrektywy. W tym celu na podstawie rozporządzenia XXXX/XXXX wszystkim organom nadzoru finansowego,

[16] *[wstawić pełny tytuł i odniesienie do publikacji w Dzienniku Urzędowym, kiedy już będą znane]*

Europejskim Urzędom Nadzoru właściwym dla sektora finansowego oraz właściwym organom krajowym na mocy rozporządzenia XXXX/XXXX umożliwiono udział w strategicznych dyskusjach na temat polityki i pracach technicznych Grupy Współpracy, a także wymianę informacji i współpracę z pojedynczymi punktami kontaktowymi wyznaczonymi na podstawie niniejszej dyrektywy oraz z krajowymi CSIRT. Właściwe organy na mocy rozporządzenia XXXX/XXXX powinny przekazywać dane na temat poważnych incydentów dotyczących ICT także pojedynczym punktom kontaktowym wyznaczonym na podstawie niniejszej dyrektywy. Ponadto państwa członkowskie powinny w dalszym ciągu uwzględniać sektor finansowy w swoich strategiach w zakresie cyberbezpieczeństwa, a krajowe CSIRT mogą objąć go swoimi działaniami.

(14) Biorąc pod uwagę powiązania między cyberbezpieczeństwem a bezpieczeństwem fizycznym podmiotów, należy zapewnić spójność pod względem podejścia między dyrektywą Parlamentu Europejskiego i Rady (UE) XXX/XXX[17] a niniejszą dyrektywą. W tym celu państwa członkowskie powinny zapewnić, aby podmioty krytyczne, oraz równoważne podmioty, zgodnie z dyrektywą (UE) XXX/XXX uznawano za podmioty niezbędne w rozumieniu niniejszej dyrektywy. Państwa członkowskie powinny także zapewnić, aby ich strategie dotyczące cyberbezpieczeństwa obejmowały ramy polityki na rzecz zwiększonej koordynacji między właściwym organem na mocy niniejszej dyrektywy a właściwym organem na mocy dyrektywy (UE) XXX/XXX w kontekście udostępniania informacji na temat incydentów i cyberzagrożeń oraz w kontekście wykonywania zadań nadzorczych. Organy na mocy obu dyrektyw powinny ze sobą współpracować i prowadzić wymianę informacji, w szczególności w odniesieniu do identyfikacji podmiotów krytycznych, cyberzagrożeń, ryzyka w cyberprzestrzeni, incydentów wpływających na podmioty krytyczne, a także w odniesieniu do środków w zakresie cyberbezpieczeństwa przyjmowanych przez podmioty krytyczne. Na wniosek właściwych organów na mocy dyrektywy (UE) XXX/XXX właściwym organom na mocy niniejszej dyrektywy należy zezwolić na wykonywanie swoich uprawnień w zakresie nadzoru i egzekwowania przepisów względem podmiotu niezbędnego zidentyfikowanego jako podmiot krytyczny. Właściwe organy na mocy obu dyrektyw powinny w tej kwestii współpracować i prowadzić wymianę informacji.

(15) Utrzymywanie i zachowanie wiarygodnego, odpornego i bezpiecznego systemu nazw domen (DNS) odgrywa decydującą rolę w utrzymaniu integralności internetu oraz ma istotne znaczenie dla jego nieprzerwanego i stabilnego działania, od którego zależą gospodarka cyfrowa i społeczeństwo cyfrowe. W związku z tym niniejsza dyrektywa powinna mieć zastosowanie do wszystkich dostawców usług DNS w całym łańcuchu rozwiązywania nazw DNS, z uwzględnieniem operatorów głównych serwerów nazw, serwerów nazw domen najwyższego poziomu (TLD), autorytatywnych serwerów nazw dla nazw domen i rekurencyjnych resolwerów.

(16) Usługi w chmurze powinny obejmować usługi, które umożliwiają administrowanie na żądanie skalowalnym i elastycznym zbiorem rozproszonych zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru zasobów. Pojęcie „zasoby obliczeniowe” obejmuje zasoby, takie jak: sieci, serwery lub inną infrastrukturę, systemy operacyjne, oprogramowanie, pamięć masową, aplikacje i usługi. Modele rozmieszczenia usług w chmurze powinny obejmować chmury

[17] *[wstawić pełny tytuł i odniesienie do publikacji w Dzienniku Urzędowym, kiedy już będą znane]*

prywatne, zbiorowe, publiczne i hybrydowe. Wspomniane wyżej modele usług i modele rozmieszczenia mają takie samo znaczenie jak terminy dotyczące modeli usług i modeli rozmieszczenia zdefiniowane w normie ISO/IEC 17788:2014. Zdolność użytkownika usług w chmurze do jednostronnego zapewnienia sobie możliwości przetwarzania danych, takich jak czas serwera lub sieciowy magazyn danych, bez żadnej ingerencji człowieka ze strony dostawcy usług w chmurze można określić jako administrowanie na żądanie. Pojęcia „szeroki dostęp zdalny" używa się do opisu sytuacji, gdy zasoby w chmurze są udostępniane przez sieć, a dostęp do nich jest możliwy za pośrednictwem mechanizmów sprzyjających wykorzystywaniu różnorodnych platform cienkich lub grubych klientów (w tym telefonów komórkowych, tabletów, laptopów, stacji roboczych). Pojęcie „skalowalne" odnosi się do zasobów komputerowych, które są elastycznie przydzielane przez dostawcę usługi niezależnie od położenia geograficznego zasobów, jako reakcja na fluktuacje zapotrzebowania. Pojęcia „elastyczny zbiór" używa się do opisu tych zasobów obliczeniowych, które są przydzielane i uwalniane zależnie do zapotrzebowania, aby szybko zwiększać i zmniejszać dostępne zasoby w zależności od obciążenia. Pojęcia „wspólne wykorzystywanie" używa się do opisu zasobów obliczeniowych udostępnianych wielu użytkownikom, którzy dzielą wspólny dostęp do usługi, jednak przetwarzanie odbywa się oddzielnie dla każdego z użytkowników, choć usługa ta jest świadczona z tego samego sprzętu elektronicznego. Pojęcia „rozproszone" używa się do opisu zasobów obliczeniowych zlokalizowanych na rożnych komputerach lub urządzeniach połączonych w sieć, które komunikują się ze sobą i koordynują swoją pracę przez przekazywanie komunikatów.

(17) Biorąc pod uwagę pojawianie się innowacyjnych technologii i nowych modeli biznesowych, oczekuje się, iż w odpowiedzi na zmieniające się potrzeby klientów pojawią się nowe modele rozmieszczenia usług w chmurze oraz nowe modele usług w chmurze. W tym kontekście usługi w chmurze mogą być świadczone w sposób wysoce rozproszony, jeszcze bliżej miejsca generowania lub gromadzenia danych, co tym samym będzie wiązać się z przejściem od modelu tradycyjnego do modelu wysoce rozproszonego („przetwarzanie danych na obrzeżach sieci").

(18) Usługi oferowane przez dostawców usług ośrodka przetwarzania danych nie zawsze muszą być świadczone w postaci usług w chmurze. Ośrodki przetwarzania danych nie zawsze muszą zatem stanowić element infrastruktury usług w chmurze. W celu zarządzania wszystkimi zagrożeniami dla bezpieczeństwa sieci i systemów informatycznych niniejsza dyrektywa powinna obejmować także dostawców usług ośrodka przetwarzania danych niebędących usługami w chmurze. Na potrzeby niniejszej dyrektywy pojęcie „usługa ośrodka przetwarzania danych" powinno obejmować świadczenie usługi obejmującej struktury lub grupy struktur przeznaczone do scentralizowanego hostingu, zapewnienia wzajemnego połączenia i eksploatacji sprzętu informatycznego i sieciowego służącego do świadczenia usług przechowywania, przetwarzania i transportu danych wraz ze wszystkimi obiektami i całą infrastrukturą na potrzeby dystrybucji energii elektrycznej i kontroli środowiskowej. Pojęcie „usługa ośrodka przetwarzania danych" nie ma zastosowania do wewnętrznych, korporacyjnych ośrodków przetwarzania danych będących własnością danego podmiotu i eksploatowanych na jego własne potrzeby.

(19) Przepisom niniejszej dyrektywy powinni podlegać operatorzy świadczący usługi pocztowe w rozumieniu dyrektywy 97/67/WE Parlamentu Europejskiego i Rady[18], a także podmioty świadczące usługi doręczania przesyłek ekspresowych i kurierskich, jeżeli podmioty te świadczą usługi na co najmniej jednym z etapów łańcucha doręczania przesyłek pocztowych, a w szczególności przyjmowanie, sortowanie lub doręczanie, w tym odbiór przesyłek. Usługi transportowe, które nie są świadczone w związku z jednym z wymienionych etapów, nie powinny wchodzić w zakres usług pocztowych.

(20) Te coraz większe współzależności wynikają z coraz bardziej transgranicznej i współzależnej sieci świadczenia usług, wykorzystującej kluczową infrastrukturę w całej Unii w sektorach energetyki, transportu, infrastruktury cyfrowej, wody pitnej i ścieków, zdrowia, niektórych aspektów administracji publicznej, a także przestrzeni kosmicznej, jeżeli chodzi o świadczenie niektórych usług zależnych od naziemnej infrastruktury będącej własnością państw członkowskich albo podmiotów prywatnych oraz która jest zarządzana i obsługiwana przez państwa członkowskie albo podmioty prywatne, a zatem nieobejmującej infrastruktury będącej własnością Unii bądź zarządzanej lub obsługiwanej przez Unię lub w jej imieniu w ramach jej programów kosmicznych. Wspomniane współzależności oznaczają, że każde zakłócenie, nawet początkowo ograniczające się do jednego podmiotu lub jednego sektora, może wywołać szerzej zakrojony efekt kaskadowy, którego potencjalne negatywne skutki dla świadczenia usług na całym rynku wewnętrznym mogą być dalekosiężne i długotrwałe. Pandemia COVID-19 uwydatniła podatność naszych coraz bardziej współzależnych społeczeństw w obliczu ryzyka o niskim prawdopodobieństwie wystąpienia.

(21) Z uwagi na różnice w krajowych strukturach zarządzania oraz w celu zabezpieczenia obowiązujących już ustaleń sektorowych lub unijnych organów nadzorczych i regulacyjnych państwa członkowskie powinny móc wyznaczać więcej niż jeden właściwy organ krajowy odpowiedzialny za wykonywanie zadań związanych z bezpieczeństwem sieci i systemów informatycznych podmiotów niezbędnych i istotnych w rozumieniu niniejszej dyrektywy. Państwa członkowskie powinny mieć możliwość wyznaczenia istniejącego organu do pełnienia tej roli.

(22) W celu ułatwienia współpracy i komunikacji transgranicznej między organami oraz umożliwienia skutecznego wprowadzenia w życie niniejszej dyrektywy niezbędne jest, aby każde państwo członkowskie wyznaczyło krajowy pojedynczy punkt kontaktowy odpowiedzialny za koordynację kwestii związanych z bezpieczeństwem sieci i systemów informatycznych oraz współpracą transgraniczną na poziomie Unii.

(23) Właściwe organy lub CSIRT powinny otrzymywać zgłoszenia incydentów od podmiotów w sposób efektywny i skuteczny. Pojedynczym punktom kontaktowym należy powierzyć zadanie przekazywania zgłoszeń incydentów pojedynczym punktom kontaktowym innych państw członkowskich, których incydent dotyczy. Na szczeblu organów państw członkowskich, aby zapewnić w każdym państwie członkowskim jeden pojedynczy punkt kontaktowy, pojedyncze punkty kontaktowe powinny być również adresatem stosownych informacji na temat incydentów dotyczących podmiotów sektora finansowego przekazywanych przez właściwe organy na mocy

[18] Dyrektywa 97/67/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie wspólnych zasad rozwoju rynku wewnętrznego usług pocztowych Wspólnoty oraz poprawy jakości usług (Dz.U. L 15 z 21.1.1998, s. 14).

rozporządzenia XXXX/XXXX, które to informacje punkty te powinny być w stanie przekazywać, stosownie do przypadku, odpowiednim właściwym organom krajowym lub CSIRT na mocy niniejszej dyrektywy.

(24) Państwa członkowskie powinny zostać odpowiednio wyposażone, zarówno pod względem zdolności technicznych, jak i możliwości organizacyjnych, w celu zapobiegania incydentom i ryzykom dotyczącym sieci i systemów informatycznych, wykrywania ich, reagowania na nie i łagodzenia ich skutków. Państwa członkowskie powinny zatem zapewnić dobrze funkcjonujące CSIRT, zwane również zespołami reagowania na incydenty komputerowe (zwane dalej „CERT"), które spełniają zasadnicze wymogi w celu zagwarantowania efektywnych i kompatybilnych zdolności w zakresie postępowania z incydentami i ryzykami oraz zapewnienia skutecznej współpracy na poziomie Unii. Aby zwiększyć zaufanie między podmiotami a CSIRT, w przypadku gdy dany CSIRT funkcjonuje w ramach właściwego organu, państwa członkowskie powinny rozważyć funkcjonalne rozdzielenie zadań operacyjnych wykonywanych przez CSIRT, szczególnie w odniesieniu do przekazywania informacji i wspierania podmiotów, od działań nadzorczych właściwego organu.

(25) Jeżeli chodzi o dane osobowe, CSIRT powinny być w stanie zapewnić – zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679[19] – w imieniu i na wniosek podmiotu w rozumieniu niniejszej dyrektywy – proaktywne skanowanie sieci i systemów informatycznych wykorzystywanych przez te podmioty do świadczenia usług. Państwa członkowskie powinny dążyć do zapewnienia równego poziomu zdolności technicznych wszystkich sektorowych CSIRT. Państwa członkowskie mogą zwrócić się do Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) o pomoc przy tworzeniu krajowych CSIRT.

(26) Z uwagi na znaczenie współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa CSIRT powinny mieć możliwość uczestniczenia w międzynarodowych sieciach współpracy, niezależnie od współpracy w ramach sieci CSIRT ustanowionej na mocy niniejszej dyrektywy.

(27) Zgodnie z załącznikiem do zalecenia Komisji (UE) 2017/1548 w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę („plan")[20] incydent na dużą skalę powinien oznaczać incydent mający znaczący wpływ na co najmniej dwa państwa członkowskie lub taki, który powoduje na tyle duże zakłócenia, że dotknięte nimi państwo członkowskie nie jest samo w stanie na nie skutecznie zareagować. W zależności od przyczyny i wpływu incydenty na dużą skalę mogą przerodzić się w prawdziwy kryzys uniemożliwiający prawidłowe funkcjonowanie rynku wewnętrznego. Biorąc pod uwagę szeroki zakres oraz, w większości przypadków, transgraniczny charakter takich incydentów, państwa członkowskie i odpowiednie instytucje, organy i agencje Unii powinny współpracować na poziomie technicznym, operacyjnym i politycznym w celu odpowiedniej koordynacji reakcji w całej Unii.

---

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

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

(28) Ponieważ wykorzystywanie podatności sieci i systemów informatycznych może powodować znaczące zakłócenia i szkody, ważnym czynnikiem w ograniczaniu ryzyka w cyberprzestrzeni jest szybkie identyfikowanie takich podatności i ich eliminowanie. Podmioty, które opracowują takie systemy, powinny zatem ustanowić odpowiednie procedury postępowania w przypadku wykrycia takich podatności. Ponieważ podatności często są wykrywane i zgłaszane (ujawniane) przez osoby trzecie (podmioty zgłaszające), producent lub dostawca produktów lub usług ICT również powinien wprowadzić niezbędne procedury regulujące odbieranie od osób trzecich informacji na temat podatności. W tym względzie normy międzynarodowe ISO/IEC 30111 i ISO/IEC 29417 zawierają wytyczne dotyczące, odpowiednio, postępowania w przypadku wykrycia podatności i ujawniania podatności. Jeśli chodzi o ujawnianie podatności, szczególnie ważna jest koordynacja między podmiotami zgłaszającymi a producentami lub dostawcami produktów lub usług ICT. Skoordynowane ujawnianie podatności to ustrukturyzowany proces, w ramach którego podatności są zgłaszane organizacjom w sposób umożliwiający organizacji zdiagnozowanie i wyeliminowanie danej podatności, zanim szczegółowe informacje dotyczące podatności zostaną ujawnione osobom trzecim lub podane do wiadomości publicznej. Skoordynowane ujawnianie podatności powinno także obejmować koordynację między podmiotem zgłaszającym a organizacją w odniesieniu do terminarza eliminowania podatności i podania ich do wiadomości publicznej.

(29) W związku z tym państwa członkowskie powinny podjąć działania w celu ułatwienia skoordynowanego ujawniania podatności poprzez ustanowienie odpowiedniej polityki krajowej. W tym zakresie państwa członkowskie powinny wyznaczyć CSIRT do pełnienia roli „koordynatora", występującego w razie potrzeby w charakterze pośrednika między podmiotami zgłaszającymi a producentami lub dostawcami produktów lub usług ICT. Zadania CSIRT w charakterze koordynatora powinny w szczególności obejmować identyfikację zainteresowanych podmiotów i kontaktowanie się z nimi, wspieranie podmiotów zgłaszających, negocjowanie terminarza ujawniania oraz zarządzanie podatnościami, których skutki dotykają wielu organizacji (wielostronne ujawnianie podatności). W przypadku gdy podatności dotykają wielu producentów lub dostawców produktów lub usług ICT posiadających jednostkę organizacyjną w co najmniej dwóch państwach członkowskich, wyznaczone CSIRT z każdego państwa członkowskiego, w którym wykryto podatności, powinny współpracować ze sobą w ramach sieci CSIRT.

(30) Dostęp do prawidłowych i terminowych informacji na temat podatności dotyczących produktów i usług ICT pozwala usprawnić zarządzanie ryzykiem w cyberprzestrzeni. W tym względzie ważnym narzędziem dla podmiotów i ich użytkowników, ale również dla właściwych organów krajowych i CSIRT są źródła publicznie dostępnych informacji na temat podatności. Z tego powodu ENISA powinna ustanowić rejestr podatności, w którym podmioty niezbędne i istotne oraz ich dostawcy, a także podmioty, które nie są objęte zakresem stosowania niniejszej dyrektywy, mogą na zasadzie dobrowolności ujawniać podatności i przekazywać informacje na temat podatności, dzięki którym użytkownicy mogą wprowadzać odpowiednie środki ograniczające ryzyko.

(31) Choć istnieją podobne rejestry podatności lub bazy danych dotyczących podatności, są one prowadzone i utrzymywane przez podmioty, które nie mają siedziby w Unii. Europejski rejestr podatności utrzymywany przez ENISA zapewniłby lepszą przejrzystość w odniesieniu do procesu publikacji poprzedzającego oficjalne ujawnienie podatności, a także odporność w przypadku zakłóceń lub przerw

w świadczeniu podobnych usług. Aby uniknąć powielania podejmowanych działań i dążyć do jak największej komplementarności, ENISA powinna zbadać możliwość zawarcia umów o współpracy strukturalnej z podobnymi rejestrami w jurysdykcjach państw trzecich.

(32) Co dwa lata Grupa Współpracy powinna opracowywać program prac obejmujący działania, które mają zostać podjęte przez Grupę w celu realizacji jej celów i zadań. Aby uniknąć potencjalnych zakłóceń w pracy Grupy, ramy czasowe pierwszego programu przyjętego na podstawie niniejszej dyrektywy należy zharmonizować z ramami czasowymi ostatniego programu przyjętego na podstawie dyrektywy (UE) 2016/1148.

(33) Opracowując wytyczne, Grupa Współpracy powinna stale: ewidencjonować rozwiązania i doświadczenia krajowe, oceniać wpływ wyników prac Grupy Współpracy na podejścia krajowe, omawiać wyzwania w zakresie wdrażania i formułować konkretne zalecenia, które należy uwzględnić w ramach lepszego wdrażania istniejących przepisów.

(34) Grupa Współpracy powinna pozostać elastycznym forum i być w stanie reagować na zmieniające się i nowe priorytety i wyzwania polityczne, przy jednoczesnym uwzględnieniu dostępności zasobów. Powinna ona organizować regularne wspólne spotkania z odpowiednimi zainteresowanymi stronami z sektora prywatnego z całej Unii w celu omawiania działań realizowanych przez Grupę i gromadzenia informacji na temat pojawiających się wyzwań w zakresie polityki. Aby zacieśnić współpracę na szczeblu unijnym, Grupa powinna rozważyć zaproszenie organów i agencji unijnych zaangażowanych w kształtowanie polityki cyberbezpieczeństwa, takich jak Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3), Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA) oraz Agencja Unii Europejskiej ds. Programu Kosmicznego, do uczestnictwa w pracach Grupy.

(35) Właściwe organy i CSIRT powinny być upoważnione do uczestniczenia w programach wymiany dla urzędników z innych państw członkowskich w celu usprawnienia współpracy. Właściwe organy powinny podejmować działania niezbędne do zapewnienia urzędnikom z innych państw członkowskich możliwości efektywnego angażowania się w działalność przyjmującego właściwego organu.

(36) Unia powinna, w stosownych przypadkach, zawierać umowy międzynarodowe, zgodnie z art. 218 TFUE, z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiając i organizując ich udział w niektórych działaniach Grupy Współpracy i sieci CSIRT. Umowy takie powinny zapewniać odpowiednią ochronę danych.

(37) Państwa członkowskie powinny wnosić wkład w ustanowienie unijnych ram reagowania w sytuacji kryzysu cyberbezpieczeństwa, o których mowa w zaleceniu (UE) 2017/1584, poprzez istniejące sieci współpracy, w szczególności poprzez europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe), sieć CSIRT i Grupę Współpracy. EU-CyCLONe i sieć CSIRT powinny współpracować na podstawie uzgodnień proceduralnych określających tryb tej współpracy. W regulaminie EU-CyCLONe należy bardziej szczegółowo określić tryb funkcjonowania tej sieci, w tym między innymi podział ról, modele współpracy, interakcje z innymi odpowiednimi podmiotami i wzory formularzy na potrzeby wymiany informacji, a także środki komunikacji. W odniesieniu do zarządzania kryzysowego na szczeblu unijnym odpowiednie strony powinny opierać się na uzgodnieniach dotyczących zintegrowanego reagowania na szczeblu politycznym

w sytuacjach kryzysowych (IPCR). W tym celu Komisja powinna wykorzystywać międzysektorowy proces koordynacji na wysokim szczeblu w sytuacji kryzysowej ARGUS. Jeżeli sytuacja kryzysowa wiąże się z istotnymi kwestiami z zakresu polityki zewnętrznej lub wspólnej polityki bezpieczeństwa i obrony (WPBiO), należy uruchomić mechanizm reagowania kryzysowego Europejskiej Służby Działań Zewnętrznych (ESDZ).

(38) Na potrzeby niniejszej dyrektywy „ryzyko" powinno odnosić się do możliwych strat lub zakłóceń spowodowanych cyberincydentem i powinno być wyrażone jako wypadkowa skali takiej straty lub takich zakłóceń oraz prawdopodobieństwa wystąpienia takiego incydentu.

(39) Na potrzeby niniejszej dyrektywy termin „zdarzenie potencjalnie wypadkowe" powinien odnosić się do zdarzenia, które może spowodować szkodę, ale którego pełnemu wystąpieniu udało się skutecznie zapobiec.

(40) Środki w zakresie zarządzania ryzykiem powinny obejmować środki mające na celu identyfikację wszelkiego ryzyka wystąpienia incydentów, zapobieganie incydentom, wykrywanie ich i postępowanie z nimi, a także łagodzenie ich wpływu. Bezpieczeństwo sieci i systemów informatycznych powinno obejmować bezpieczeństwo danych przechowywanych, przekazywanych i przetwarzanych.

(41) Aby uniknąć nakładania nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na podmioty niezbędne i istotne, wymogi w zakresie zarządzania ryzykiem w cyberprzestrzeni powinny być proporcjonalne do ryzyka, jakie stwarza dana sieć oraz dany system informatyczny, oraz powinny uwzględniać najnowszy stan wiedzy na temat takich środków.

(42) Podmioty niezbędne i istotne powinny zapewniać bezpieczeństwo sieci i systemów informatycznych, których używają w swojej działalności. Dotyczy to przede wszystkim prywatnych sieci i systemów informatycznych, które są zarządzane przez własny personel informatyczny lub dla których zapewnienie bezpieczeństwa zlecono na zewnątrz. Wymogi w zakresie zarządzania ryzykiem w cyberprzestrzeni i zgłaszania incydentów na podstawie niniejszej dyrektywy powinny mieć zastosowanie do odpowiednich podmiotów niezbędnych i istotnych bez względu na to, czy same zapewniają utrzymanie swoich sieci i systemów informatycznych, czy też zlecają ich utrzymanie na zewnątrz.

(43) Biorąc pod uwagę, jak często dochodzi do incydentów, w których podmioty padają ofiarami cyberataków i w których agresorzy byli w stanie złamać zabezpieczenia sieci i systemów informatycznych podmiotu dzięki wykorzystaniu podatności występujących w produktach i usługach osób trzecich, szczególnie istotne jest zaradzenie ryzykom w cyberprzestrzeni wynikającym z łańcucha dostaw podmiotu oraz jego powiązań z dostawcami. W związku z tym podmioty powinny oceniać i uwzględniać ogólną jakość produktów i praktyk w zakresie cyberbezpieczeństwa swoich dostawców produktów i usług, w tym ich procedury bezpiecznego opracowywania.

(44) Wśród dostawców usług szczególnie ważną rolę we wspieraniu podmiotów w ich działaniach mających na celu wykrywanie incydentów i reagowanie na nie odgrywają dostawcy zarządzanych usług w zakresie bezpieczeństwa w obszarach takich jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo. Tacy dostawcy zarządzanych usług z zakresu bezpieczeństwa również sami padali jednak ofiarami cyberataków, a ponieważ ich działalność jest ściśle zintegrowana

z operacjami operatorów, stwarzają szczególne ryzyko w cyberprzestrzeni. W związku z tym przy wyborze dostawcy zarządzanych usług z zakresu bezpieczeństwa podmioty powinny dochować szczególnej staranności.

(45) Podmioty powinny również ograniczać ryzyko w cyberprzestrzeni wynikające z ich interakcji i powiązań z innymi zainteresowanymi stronami w ramach szerszego ekosystemu. W szczególności podmioty powinny wprowadzać odpowiednie środki zapewniające, aby ich współpraca z instytucjami akademickimi i badawczymi przebiegała zgodnie z ich polityką cyberbezpieczeństwa i z uwzględnieniem dobrych praktyk dotyczących bezpiecznego dostępu do informacji i ich rozpowszechniania ogółem, a w szczególności ochrony własności intelektualnej. Podobnie biorąc pod uwagę znaczenie i wartość danych w kontekście działalności podmiotów, w przypadku korzystania z usług przekształcania danych i analizy danych oferowanych przez osoby trzecie podmioty powinny stosować wszelkie odpowiednie środki w zakresie cyberbezpieczeństwa.

(46) Aby w większym stopniu ograniczyć kluczowe ryzyka w łańcuchu dostaw i wesprzeć podmioty działające w sektorach objętych niniejszą dyrektywą w odpowiednim zarządzaniu ryzykiem w cyberprzestrzeni związanym z łańcuchem dostaw i dostawcami, Grupa Współpracy przy udziale odpowiednich organów krajowych, we współpracy z Komisją i ENISA, powinna przeprowadzić skoordynowane sektorowe oceny ryzyka w łańcuchach dostaw, tak jak to miało już miejsce w przypadku sieci 5G w następstwie zalecenia (UE) 2019/534 w sprawie cyberbezpieczeństwa sieci 5G[21], aby zidentyfikować w każdym sektorze krytyczne usługi, systemy lub produkty ICT, istotne zagrożenia i podatności.

(47) W świetle specyfiki danego sektora w ocenach ryzyka w łańcuchu dostaw należy uwzględnić zarówno czynniki techniczne, jak i – w stosownych przypadkach – pozatechniczne, w tym te określone w zaleceniu (UE) 2019/534, w unijnej skoordynowanej ocenie ryzyka w zakresie bezpieczeństwa sieci 5G oraz w unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G uzgodnionym przez Grupę Współpracy. Aby zidentyfikować łańcuchy dostaw, które należy poddać skoordynowanej ocenie ryzyka, należy wziąć pod uwagę następujące kryteria: (i) zakres, w jakim podmioty niezbędne i istotne wykorzystują konkretne krytyczne usługi, systemy lub produkty ICT i na nich polegają; (ii) znaczenie konkretnych krytycznych usług, systemów lub produktów ICT dla wykonywania krytycznych lub wrażliwych funkcji, w tym przetwarzania danych osobowych; (iii) dostępność alternatywnych usług, systemów lub produktów ICT; (iv) odporność całego łańcucha dostaw usług, systemów lub produktów ICT na zdarzenia powodujące zakłócenia oraz (v) w przypadku pojawiających się usług, systemów lub produktów ICT – ich potencjalne przyszłe znaczenie dla działalności podmiotów.

(48) Aby uprościć zobowiązania prawne nałożone na dostawców publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej oraz dostawców usług zaufania w odniesieniu do bezpieczeństwa ich sieci i systemów informatycznych, a także zapewnić tym podmiotom i ich odpowiednim właściwym organom możliwość korzystania z ram prawnych ustanowionych na podstawie niniejszej dyrektywy (w tym wyznaczania CSIRT odpowiedzialnych za postępowanie w przypadku ryzyka i incydentu, uczestnictwa właściwych organów i jednostek

[21] Zalecenie Komisji (UE) 2019/534 z dnia 26 marca 2019 r. Cyberbezpieczeństwo sieci 5G (Dz.U. L 88 z 29.3.2019, s. 42).

w pracach Grupy Współpracy i w sieci CSIRT), należy objąć te podmioty zakresem stosowania niniejszej dyrektywy. W związku z tym należy uchylić odpowiednie przepisy określone w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014[22] oraz w dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/1972[23], na których podstawie na te rodzaje podmiotów nałożono wymogi w zakresie bezpieczeństwa i zgłaszania incydentów. Przepisy dotyczące obowiązków w zakresie zgłaszania incydentów nie powinny naruszać przepisów rozporządzenia (UE) 2016/679 i dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE[24].

(49) W stosownych przypadkach i aby uniknąć niepotrzebnych zakłóceń, właściwe organy odpowiedzialne do celów niniejszej dyrektywy za nadzór i egzekwowanie przepisów powinny w dalszym ciągu stosować istniejące wytyczne krajowe i przepisy krajowe przyjęte w celu transpozycji przepisów dotyczących środków bezpieczeństwa określonych w art. 40 ust. 1 dyrektywy (UE) 2018/1972, a także wymogów określonych w art. 40 ust. 2 tej dyrektywy dotyczących parametrów związanych z istotnością incydentu.

(50) Ze względu na rosnące znaczenie usług interpersonalnej łączności niewykorzystujących numerów należy zapewnić, aby usługi te podlegały również odpowiednim wymogom w zakresie bezpieczeństwa z uwagi na ich szczególny charakter i istotną rolę w gospodarce. Dostawcy takich usług powinni zatem również zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do stwarzanego ryzyka. Ze względu na to, że dostawcy usług interpersonalnej łączności niewykorzystujących numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach, stopień ryzyka w przypadku takich usług można uznać za niższy pod pewnymi względami niż w przypadku tradycyjnych usług łączności elektronicznej. To samo ma zastosowanie do dostawców usług interpersonalnej łączności wykorzystujących numery, którzy nie sprawują rzeczywistej kontroli nad transmisją sygnałów.

(51) Rynek wewnętrzny jest bardziej niż kiedykolwiek uzależniony od funkcjonowania internetu. Usługi niemal wszystkich podmiotów niezbędnych i istotnych zależą od usług świadczonych przez internet. Aby zapewnić sprawne świadczenie usług przez podmioty niezbędne i istotne, publiczne sieci łączności elektronicznej, jak na przykład internetowe sieci szkieletowe czy podmorskie kable telekomunikacyjne, powinny wprowadzić odpowiednie środki w zakresie cyberbezpieczeństwa i zgłaszać incydenty w tym zakresie.

(52) W stosownych przypadkach podmioty powinny informować odbiorców swoich usług o szczególnych i istotnych zagrożeniach oraz o środkach, które odbiorcy ci mogą zastosować w celu ograniczenia wynikłego ryzyka, na jakie są sami narażeni. Wymóg informowania tych odbiorców o takich zagrożeniach nie powinien zwalniać podmiotu z obowiązku zastosowania na własny koszt odpowiednich i natychmiastowych środków w celu zapobieżenia lub zaradzenia wszelkim cyberzagrożeniom oraz

---

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

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

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

przywrócenia normalnego poziomu bezpieczeństwa danej usługi. Udzielanie odbiorcom takich informacji na temat zagrożeń bezpieczeństwa powinno odbywać się bezpłatnie.

(53) W szczególności dostawcy publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej powinni informować odbiorców usługi o szczególnych i istotnych cyberzagrożeniach oraz o środkach, które mogą zastosować w celu ochrony bezpieczeństwa swoich środków łączności, na przykład przez zastosowanie szczególnych rodzajów oprogramowania lub technologii szyfrowania.

(54) Aby zagwarantować bezpieczeństwo sieci i usług łączności elektronicznej, należy promować korzystanie z szyfrowania, w szczególności szyfrowania *end-to-end*, a w razie konieczności uczynić je obowiązkowym dla dostawców takich usług i sieci zgodnie z zasadą uwzględniania bezpieczeństwa i prywatności w sposób domyślny i na etapie projektowania do celów art. 18. Korzystanie z szyfrowania *end-to-end* należy pogodzić z uprawnieniami państw członkowskich w zakresie zapewnienia ochrony ich podstawowych interesów bezpieczeństwa i bezpieczeństwa publicznego, a także w zakresie umożliwiania wykrywania i ścigania przestępstw oraz prowadzenia dochodzeń w ich sprawie zgodnie z prawem Unii. Rozwiązania zapewniające zgodny z prawem dostęp do informacji przesyłanych z wykorzystaniem transmisji szyfrowanej *end-to-end* powinny gwarantować zachowanie skuteczności szyfrowania pod względem ochrony prywatności i bezpieczeństwa łączności, zapewniając jednocześnie możliwość skutecznego reagowania na przestępstwa.

(55) W niniejszej dyrektywie określono dwuetapowe podejście do zgłaszania incydentów w celu zapewnienia odpowiedniej równowagi między szybkim zgłaszaniem, co pomoże zahamować potencjalne rozprzestrzenianie się incydentów i pozwoli podmiotom zwrócić się o wsparcie, a szczegółowym zgłaszaniem, co umożliwi wyciągnięcie cennych wniosków z poszczególnych incydentów i z czasem przyczyni się do zwiększenia odporności poszczególnych przedsiębiorstw i całych sektorów na cyberzagrożenia. W przypadku gdy podmioty powezmą wiedzę o incydencie, powinny mieć obowiązek dokonania wstępnego zgłoszenia w ciągu 24 godzin, a następnie przedłożenia – w terminie nie dłuższym niż miesiąc – sprawozdania końcowego. Wstępne zgłoszenie powinno zawierać jedynie informacje absolutnie niezbędne do tego, by poinformować właściwe organy o wystąpieniu incydentu i umożliwić podmiotowi zwrócenie się o wsparcie, jeśli zachodzi taka potrzeba. W stosownych przypadkach w takim zgłoszeniu należy wskazać, czy, jak przypuszcza się, incydent został wywołany działaniem bezprawnym lub działaniem w złym zamiarze. Państwa członkowskie powinny zapewnić, aby wymóg dokonania wstępnego zgłoszenia nie powodował przekierowania zasobów podmiotu zgłaszającego z działań podejmowanych w reakcji na incydent, które to działania powinny mieć charakter priorytetowy. Aby dodatkowo zapobiec sytuacji, w której obowiązki w zakresie zgłaszania incydentów ograniczą zdolność podmiotu do podjęcia reakcji na incydent albo w inny sposób osłabią działania podmiotu w tym zakresie, państwa członkowskie powinny również przewidzieć – w należycie uzasadnionych przypadkach i w porozumieniu z właściwymi organami lub CSIRT – możliwość odstąpienia w przypadku danego podmiotu od terminu 24 godzin na dokonanie wstępnego zgłoszenia i terminu jednego miesiąca na przedłożenie sprawozdania końcowego.

(56) Podmioty niezbędne i istotne znajdują się często w sytuacji, w której konkretny incydent, ze względu na jego cechy, należy zgłosić różnym organom w wyniku istnienia obowiązków w zakresie zgłaszania przewidzianych w różnych instrumentach prawnych. Takie przypadki powodują dodatkowe obciążenie, a ponadto mogą rodzić

niepewność dotyczącą formatu i procedur dokonywania takich zgłoszeń. W związku z tym i w celu uproszczenia zgłaszania incydentów bezpieczeństwa państwa członkowskie powinny ustanowić *pojedynczy punkt kontaktowy* na potrzeby wszystkich zgłoszeń wymaganych na podstawie niniejszej dyrektywy, a także na podstawie innych przepisów unijnych, takich jak rozporządzenie (UE) 2016/679 i dyrektywa 2002/58/WE. ENISA, we współpracy z Grupą Współpracy, powinna opracować wspólne wzory zgłoszeń w formie wytycznych, które ułatwiłyby i usprawniły zgłaszanie informacji wymaganych zgodnie z prawem Unii oraz zmniejszyłyby obciążenia spoczywające na przedsiębiorstwach.

(57) W razie podejrzenia, że incydent ma związek z poważnymi przestępstwami w rozumieniu prawa Unii lub prawa krajowego, państwa członkowskie powinny zachęcać podmioty niezbędne i istotne, w oparciu o mające zastosowanie przepisy z zakresu postępowania karnego zgodne z prawem Unii, do zgłaszania odpowiednim organom ścigania incydentów noszących znamiona poważnego przestępstwa. W stosownych przypadkach i bez uszczerbku dla przepisów o ochronie danych osobowych mających zastosowanie do Europolu pożądane jest, aby koordynację między właściwymi organami i organami ścigania z różnych państw członkowskich ułatwiały EC3 oraz ENISA.

(58) W wielu przypadkach istnieje niebezpieczeństwo naruszenia danych osobowych w wyniku incydentów. W tym kontekście właściwe organy powinny współpracować oraz wymieniać się informacjami dotyczącymi wszystkich istotnych kwestii z organami ochrony danych oraz organami nadzorczymi zgodnie z dyrektywą 2002/58/WE.

(59) Prowadzenie prawidłowych i kompletnych baz danych zawierających nazwy domen i dane rejestracyjne („dane WHOIS”) oraz zapewnienie zgodnego z prawem dostępu do takich danych jest niezbędne do zapewnienia bezpieczeństwa, stabilności i odporności systemu nazw domen (DNS), co z kolei przyczynia się do wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii. Gdy przetwarzanie dotyczy danych osobowych, powinno być ono zgodne z unijnymi przepisami o ochronie danych.

(60) Dostępność tych danych dla organów publicznych, w tym dla organów właściwych na mocy prawa Unii i prawa krajowego do spraw prewencji i ścigania przestępstw oraz prowadzenia dochodzeń w ich sprawie, zespołów CERT, sieci CSIRT oraz – w zakresie, w jakim dotyczy to danych ich klientów – dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług z zakresu cyberbezpieczeństwa działających w imieniu tych klientów, a także możliwość uzyskania szybkiego dostępu do tych danych przez wymienione podmioty jest niezbędna do przeciwdziałania nadużyciom systemu nazw domen oraz zwalczania takich nadużyć, w szczególności do przeciwdziałania cyberincydentom, wykrywania ich oraz reagowania na nie. Taki dostęp powinien być zgodny z unijnymi przepisami o ochronie danych w zakresie, w jakim dotyczy on danych osobowych.

(61) W celu zapewnienia dostępności prawidłowych i kompletnych danych dotyczących rejestracji nazw domen rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD (tzw. rejestratorzy) powinny gromadzić dane dotyczące rejestracji nazw domen oraz zapewniać ich integralność i dostępność. W szczególności rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD powinny ustanowić polityki i procedury na potrzeby gromadzenia i utrzymywania prawidłowych i kompletnych danych rejestracyjnych, a także przeciwdziałać

powstawaniu nieprawidłowych danych rejestracyjnych i poprawiać je zgodnie z unijnymi przepisami o ochronie danych.

(62) Rejestry TLD i podmioty świadczące dla nich usługi rejestracji nazw domen powinny podawać do wiadomości publicznej dane dotyczące rejestracji nazw domen nieobjęte zakresem stosowania unijnych przepisów o ochronie danych, takie jak dane dotyczące osób prawnych[25]. Rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD powinny ponadto umożliwiać wnioskodawcom ubiegającym się o prawnie uzasadniony dostęp uzyskanie takiego dostępu do konkretnych danych dotyczących rejestracji nazw domen, odnoszących się do osób fizycznych, zgodnie z unijnymi przepisami o ochronie danych. Państwa członkowskie powinny zapewniać, aby rejestry TLD i podmioty świadczące dla nich usługi rejestracji nazw domen odpowiadały bez zbędnej zwłoki na wnioski wnioskodawców ubiegających się o prawnie uzasadniony dostęp o ujawnienie danych dotyczących rejestracji nazw domen. Rejestry TLD i podmioty świadczące dla nich usługi rejestracji nazw domen powinny ustanowić polityki i procedury na potrzeby publikacji i ujawniania danych rejestracyjnych, w tym umowy o gwarantowanym poziomie usług regulujące rozpatrywanie wniosków o dostęp składanych przez wnioskodawców ubiegających się o prawnie uzasadniony dostęp. Procedura uzyskiwania dostępu może również obejmować wykorzystanie interfejsu, portalu lub innego narzędzia technicznego w celu zapewnienia skutecznego systemu umożliwiającego składanie wniosków o dostęp do danych rejestracyjnych i uzyskiwanie do nich dostępu. W celu promowania zharmonizowanych praktyk na całym rynku wewnętrznym Komisja może przyjąć wytyczne dotyczące takich procedur bez uszczerbku dla kompetencji Europejskiej Rady Ochrony Danych.

(63) Wszystkie podmioty niezbędne i istotne, o których mowa w niniejszej dyrektywie, powinny podlegać jurysdykcji państwa członkowskiego, w którym świadczą usługi. Jeżeli podmiot świadczy usługi w więcej niż jednym państwie członkowskim, powinien podlegać odrębnej i równoczesnej jurysdykcji każdego z tych państw członkowskich. Właściwe organy tych państw członkowskich powinny ze sobą współpracować, zapewniać sobie wzajemną pomoc oraz, w stosownych przypadkach, prowadzić wspólne działania nadzorcze.

(64) Aby uwzględnić transgraniczny charakter usług i działalności dostawców usług DNS, rejestrów nazw TLD, dostawców sieci dostarczania treści, dostawców usług w chmurze, dostawców usług ośrodka przetwarzania danych oraz dostawców usług cyfrowych, takie podmioty powinny podlegać jurysdykcji wyłącznie jednego państwa członkowskiego. Jurysdykcja powinna przynależeć państwu członkowskiemu, w którym dany podmiot ma główną jednostkę organizacyjną w Unii. Kryterium jednostki organizacyjnej do celów niniejszej dyrektywy oznacza faktyczne prowadzenie działalności poprzez stabilne struktury. Forma prawna takich struktur, niezależnie od tego, czy chodzi o oddział czy podmiot zależny posiadający osobowość prawną, nie jest w tym względzie czynnikiem decydującym. Spełnienie tego kryterium nie powinno zależeć od tego, czy sieci i systemy informatyczne są fizycznie zlokalizowane w danym miejscu; fizyczne położenie i wykorzystanie takich systemów nie stanowią same w sobie takiej głównej jednostki organizacyjnej i nie są zatem

[25] Motyw 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, zgodnie z którym „[n]iniejsze rozporządzenie nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej”.

przesądzającymi kryteriami pozwalającymi ustalić główną jednostkę organizacyjną. Za główną jednostkę organizacyjną należy uznać miejsce, w którym podejmuje się w Unii decyzje związane ze środkami zarządzania ryzykiem w cyberprzestrzeni. Będzie ono zazwyczaj odpowiadać miejscu centralnej administracji przedsiębiorstw w Unii. Jeżeli takich decyzji nie podejmuje się w Unii, należy uznać, że główna jednostka organizacyjna znajduje się w państwach członkowskich, w których dany podmiot ma jednostkę organizacyjną o największej liczbie pracowników w Unii. Jeżeli usługi świadczy grupa przedsiębiorstw, za główną jednostkę organizacyjną grupy przedsiębiorstw należy uznać główną jednostkę organizacyjną przedsiębiorstwa sprawującego kontrolę.

(65) W przypadkach gdy dostawca usług DNS, rejestr nazw TLD, dostawca sieci dostarczania treści, dostawca usług w chmurze, dostawca usług ośrodka przetwarzania danych oraz dostawca usług cyfrowych nieposiadający jednostki organizacyjnej w Unii oferuje usługi w Unii, powinien wyznaczyć przedstawiciela. Aby stwierdzić, czy podmiot oferuje usługi w Unii, należy ustalić, czy jest oczywiste, że dany podmiot zamierza oferować usługi osobom w co najmniej jednym państwie członkowskim. Do stwierdzenia takiego zamiaru nie wystarczy sama dostępność w Unii strony internetowej lub adresu poczty elektronicznej i innych danych kontaktowych podmiotu lub pośrednika ani posługiwanie się językiem powszechnie stosowanym w państwie trzecim, w którym podmiot ma jednostkę organizacyjną. Jednakże czynniki, takie jak posługiwanie się językiem lub walutą powszechnie stosowanymi w jednym lub większej liczbie państw członkowskich oraz możliwość zamówienia usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii, mogą potwierdzać oczywistość zamiaru oferowania przez podmiot usług w Unii. Przedstawiciel powinien występować w imieniu podmiotu, a właściwe organy lub CSIRT powinny móc kontaktować się z przedstawicielem. Przedstawiciel powinien zostać wyznaczony w sposób wyraźny za pomocą udzielonego przez podmiot pisemnego upoważnienia do występowania w jego imieniu w zakresie jego obowiązków wynikających z niniejszej dyrektywy, w tym zgłaszania incydentów.

(66) Gdy dochodzi do wymiany, zgłoszenia lub innego rodzaju udostępnienia na podstawie niniejszej dyrektywy informacji uznawanych za niejawne zgodnie z prawem krajowym lub prawem Unii, należy stosować odpowiednie przepisy szczegółowe dotyczące postępowania z informacjami niejawnymi.

(67) Biorąc pod uwagę, że cyberzagrożenia stają się coraz bardziej złożone i zaawansowane, skuteczność środków wykrywania i zapobiegania zależy w dużej mierze od regularnej wymiany między podmiotami danych wywiadowczych na temat zagrożeń i podatności. Wymiana informacji przyczynia się do większej świadomości na temat cyberzagrożeń, co z kolei wzmacnia zdolność podmiotów do zapobiegania urzeczywistnieniu się zagrożeń oraz umożliwia podmiotom skuteczniejsze ograniczanie skutków incydentów oraz sprawniejsze przywracanie gotowości. Wydaje się, że wobec braku wytycznych na szczeblu unijnym szereg czynników ogranicza taką wymianę danych wywiadowczych, zwłaszcza niepewność co do zgodności z regułami konkurencji i przepisami dotyczącymi odpowiedzialności.

(68) Należy zachęcać podmioty do wspólnego wykorzystywania ich indywidualnej wiedzy i praktycznego doświadczenia na szczeblu strategicznym, taktycznym i operacyjnym w celu wzmocnienia ich zdolności w zakresie odpowiedniego oceniania i monitorowania cyberzagrożeń, obrony przed nimi i reagowania na nie. Należy zatem umożliwić powstawanie na poziomie Unii mechanizmów dobrowolnej wymiany informacji. W tym celu państwa członkowskie powinny aktywnie wspierać również

odpowiednie podmioty nieobjęte zakresem niniejszej dyrektywy i zachęcać je do uczestnictwa w takich mechanizmach wymiany informacji. Mechanizmy te powinny funkcjonować w pełnej zgodności z unijnymi regułami konkurencji oraz z unijnymi przepisami dotyczącymi ochrony danych osobowych.

(69) Należy uznać, że przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji przez podmioty, organy publiczne, CERT, CSIRT oraz dostawców technologii i usług z zakresu bezpieczeństwa stanowi prawnie uzasadniony interes zainteresowanego administratora danych w rozumieniu rozporządzenia (UE) 2016/679. Powinno to obejmować środki związane z zapobieganiem incydentom, wykrywaniem i analizowaniem ich oraz reagowaniem na nie, środki zwiększające świadomość konkretnych cyberzagrożeń, wymianę informacji w kontekście usuwania oraz skoordynowanego ujawniania podatności, a także dobrowolną wymianę informacji na temat tych incydentów, a także na temat cyberzagrożeń i podatności, oznak naruszenia integralności systemu, taktyk, technik i procedur, ostrzeżeń dotyczących cyberbezpieczeństwa i narzędzi konfiguracji. Takie środki mogą wiązać się z koniecznością przetwarzania następujących rodzajów danych osobowych: adresów IP, ujednoliconych formatów adresowania zasobów (URL), nazw domen i adresów e-mail.

(70) Aby wzmocnić uprawnienia i działania nadzorcze, które pomagają zapewnić efektywną zgodność z przepisami, w niniejszej dyrektywie należy przewidzieć minimalny wykaz działań i środków nadzorczych, za pomocą których właściwe organy mogą sprawować nadzór nad podmiotami niezbędnymi i istotnymi. Ponadto w niniejszej dyrektywie należy wprowadzić rozróżnienie systemów nadzoru mających zastosowanie do podmiotów niezbędnych i podmiotów istotnych w celu zapewnienia sprawiedliwej równowagi pod względem obowiązków zarówno po stronie podmiotów, jak i właściwych organów. Podmioty niezbędne należy zatem objąć pełnym systemem nadzoru (*ex ante* i *ex post*), natomiast podmioty istotne należy objąć uproszczonym systemem nadzoru (wyłącznie *ex post*). W przypadku tego drugiego systemu podmioty istotne nie powinny mieć obowiązku systematycznego dokumentowania spełniania wymogów dotyczących zarządzania ryzykiem w cyberprzestrzeni, natomiast właściwe organy powinny realizować nadzór w oparciu o podejście reaktywne w trybie *ex post*, a zatem nie powinny mieć ogólnego obowiązku prowadzenia nadzoru nad tymi podmiotami.

(71) W celu zapewnienia skutecznego egzekwowania przepisów należy ustanowić minimalny wykaz sankcji administracyjnych za naruszenie przewidzianych w niniejszej dyrektywie obowiązków w zakresie zarządzania ryzykiem w cyberprzestrzeni oraz zgłaszania incydentów, określając jasne i spójne ramy dotyczące takich sankcji w całej Unii. Należy odpowiednio uwzględniać charakter, wagę oraz czas trwania naruszenia, faktycznie wyrządzone szkody lub poniesione straty lub potencjalne szkody lub straty, które mogły powstać, to, czy naruszenie było umyślne lub wynikało z niedbalstwa, działania podjęte, aby zapobiec szkodom lub stratom lub je ograniczyć, stopień odpowiedzialności lub wszelkie mające znaczenie wcześniejsze naruszenia, stopień współpracy z właściwym organem oraz wszelkie inne okoliczności obciążające lub łagodzące. Nakładanie sankcji, w tym administracyjnych kar pieniężnych, powinno przebiegać z zastrzeżeniem odpowiednich gwarancji proceduralnych zgodnych z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych Unii Europejskiej, w tym skutecznej ochrony prawnej i prawa do rzetelnego procesu sądowego.

(72) Aby zapewnić skuteczne egzekwowanie obowiązków przewidzianych w niniejszej dyrektywie, każdy właściwy organ powinien być uprawniony do nakładania lub żądania nałożenia administracyjnych kar pieniężnych.

(73) Jeżeli administracyjna kara pieniężna jest nakładana na przedsiębiorstwo, przez przedsiębiorstwo należy do tych celów rozumieć przedsiębiorstwo zgodnie z art. 101 i 102 TFUE. Jeżeli administracyjna kara pieniężna jest nakładana na osobę niebędącą przedsiębiorstwem, organ nadzorczy, ustalając właściwą wysokość kary pieniężnej, powinien brać pod uwagę ogólny poziom dochodów w danym państwie członkowskim oraz sytuację ekonomiczną tej osoby. Państwa członkowskie powinny określić, czy i w jakim zakresie administracyjnym karom pieniężnym powinny podlegać organy publiczne. Nałożenie administracyjnej kary pieniężnej nie wpływa na korzystanie przez właściwe organy z innych uprawnień ani na nakładanie innych sankcji przewidzianych w przepisach krajowych transponujących niniejszą dyrektywę.

(74) Państwa członkowskie powinny mieć możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie przepisów krajowych transponujących niniejszą dyrektywę. Jednak nałożenie sankcji karnych za naruszenie takich przepisów krajowych oraz nałożenie powiązanych kar administracyjnych nie powinno prowadzić do naruszenia zasady *ne bis in idem*, zgodnie z wykładnią Trybunału Sprawiedliwości.

(75) W sytuacjach, w których niniejsza dyrektywa nie harmonizuje kar administracyjnych, lub w razie potrzeby w innych przypadkach, na przykład w razie poważnego naruszenia obowiązków przewidzianych w niniejszej dyrektywie, państwa członkowskie powinny wdrożyć system przewidujący skuteczne, proporcjonalne i odstraszające sankcje. Charakter takich sankcji (karny lub administracyjny) powinno określać prawo państwa członkowskiego.

(76) Aby jeszcze bardziej wzmocnić skuteczność i odstraszający charakter sankcji mających zastosowanie do naruszeń obowiązków przewidzianych w niniejszej dyrektywie, właściwe organy powinny być uprawnione do stosowania sankcji polegających na zawieszeniu certyfikacji lub zezwolenia dotyczących części lub całości usług świadczonych przez podmiot niezbędny oraz na nałożeniu tymczasowego zakazu sprawowania funkcji zarządczych przez osobę fizyczną. Zważywszy na dotkliwość takich sankcji i ich wpływ na działalność podmiotów, a ostatecznie na ich konsumentów, należy je stosować proporcjonalnie do powagi naruszenia i z uwzględnieniem konkretnych okoliczności danej sprawy, w tym faktu, czy naruszenie ma charakter umyślny czy też wynika z niedbalstwa, oraz działań podjętych, aby zapobiec szkodom lub stratom lub je ograniczyć. Takie sankcje należy stosować wyłącznie w ostateczności, po wyczerpaniu przewidzianych w niniejszej dyrektywie pozostałych stosownych działań z zakresu egzekwowania przepisów i wyłącznie dopóki podmioty, na które nałożono sankcje, nie podejmą niezbędnych działań w celu usunięcia nieprawidłowości lub nie spełnią wymogów właściwego organu, z których tytułu zastosowano takie sankcje. Nakładanie takich sankcji powinno przebiegać z zastrzeżeniem odpowiednich gwarancji proceduralnych zgodnych z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych Unii Europejskiej, w tym skutecznej ochrony prawnej, prawa do rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony.

(77) Niniejszą dyrektywą należy ustanowić reguły współpracy między właściwymi organami i organami nadzorczymi zgodnie z rozporządzeniem (UE) 2016/679 w celu reagowania na naruszenia związane z danymi osobowymi.

(78) Celem niniejszej dyrektywy powinno być zapewnienie wysokiego poziomu odpowiedzialności za środki zarządzania ryzykiem w cyberprzestrzeni oraz za obowiązki w zakresie zgłaszania incydentów na poziomie organizacji. Dlatego też organy zarządzające podmiotów wchodzących w zakres stosowania niniejszej dyrektywy powinny zatwierdzić środki zarządzania ryzykiem w cyberprzestrzeni oraz sprawować nadzór nad ich wprowadzaniem.

(79) Należy wprowadzić mechanizm wzajemnej oceny umożliwiający przeprowadzanie przez ekspertów wyznaczonych przez państwa członkowskie oceny wdrożenia polityk cyberbezpieczeństwa, w tym poziomu zdolności państw członkowskich oraz dostępnych w nich zasobów.

(80) W celu uwzględnienia nowych cyberzagrożeń, postępu technologicznego lub specyfiki sektora należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 TFUE w odniesieniu do elementów związanych ze środkami zarządzania ryzykiem przewidzianymi w niniejszej dyrektywie. Komisja powinna być również uprawniona do przyjęcia aktów delegowanych określających, które kategorie podmiotów niezbędnych mają obowiązek uzyskać certyfikację i na podstawie których konkretnych europejskich programów certyfikacji cyberbezpieczeństwa mają ją uzyskać. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[26]. 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.

(81) Aby zapewnić jednolite warunki wdrażania odpowiednich przepisów niniejszej dyrektywy dotyczących procedur niezbędnych do funkcjonowania Grupy Współpracy, elementów technicznych związanych ze środkami zarządzania ryzykiem lub rodzaju zgłaszanych informacji, formatu i procedury dokonywania zgłoszeń incydentów, należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[27].

(82) Komisja powinna okresowo dokonywać przeglądu niniejszej dyrektywy, w drodze konsultacji z zainteresowanymi stronami, w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się warunków społecznych, politycznych, technologicznych lub rynkowych.

(83) Ponieważ cel niniejszej dyrektywy, a mianowicie osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na skutki działania możliwe jest lepsze jego osiągnięcie na poziomie Unii, Unia może podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej.

---

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

[27] 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).

Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(84) Niniejsza dyrektywa nie narusza praw podstawowych i jest zgodna z zasadami uznanymi w Karcie praw podstawowych Unii Europejskiej, w szczególności z zasadami dotyczącymi prawa do poszanowania życia prywatnego i komunikowania się, prawa do ochrony danych osobowych i wolności prowadzenia działalności gospodarczej, prawa własności, prawa do skutecznego środka prawnego i prawa do bycia wysłuchanym. Niniejszą dyrektywę należy wprowadzać w życie zgodnie z tymi prawami i zasadami,

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

Przepisy ogólne

Artykuł 1

Przedmiot

1. Niniejszą dyrektywą ustanawia się środki mające na celu zapewnienie wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii.

2. W tym celu niniejsza dyrektywa:

   a) określa spoczywające na państwach członkowskich obowiązki dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa, wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT);

   b) określa obowiązki w zakresie zarządzania ryzykiem w cyberprzestrzeni oraz zgłaszania incydentów spoczywające na podmiotach w rodzaju tych, które określono jako podmioty niezbędne w załączniku I oraz jako podmioty istotne w załączniku II;

   c) określa obowiązki w zakresie wymiany informacji na temat cyberbezpieczeństwa.

Artykuł 2

Zakres

1. Niniejsza dyrektywa ma zastosowanie do podmiotów publicznych i prywatnych w rodzaju tych, które określono jako podmioty niezbędne w załączniku I oraz jako podmioty istotne w załączniku II. Niniejsza dyrektywa nie ma zastosowania do

podmiotów kwalifikujących się jako mikroprzedsiębiorstwa i małe przedsiębiorstwa w rozumieniu zalecenia Komisji 2003/361/WE[28].

2. Niniejsza dyrektywa ma jednak zastosowanie do podmiotów, o których mowa w załącznikach I i II, niezależnie od ich wielkości, w przypadku gdy:

a) usługi świadczy jeden z poniższych podmiotów:

(i) publiczne sieci łączności elektronicznej lub publicznie dostępne usługi łączności elektronicznej, o których mowa w załączniku I pkt 8;

(ii) dostawcy usług zaufania, o których mowa w załączniku I pkt 8;

(iii) rejestry nazw domen najwyższego poziomu oraz dostawcy usług systemów nazw domen (DNS), o których mowa w załączniku I pkt 8;

b) podmiot jest podmiotem administracji publicznej zgodnie z definicją zawartą w art. 4 pkt 23;

c) podmiot jest jedynym dostawcą danej usługi w państwie członkowskim;

d) ewentualne zakłócenie usługi świadczonej przez podmiot mogłoby mieć wpływ na porządek publiczny, bezpieczeństwo publiczne lub zdrowie publiczne;

e) ewentualne zakłócenie usługi świadczonej przez podmiot mogłoby prowadzić do powstania ryzyka systemowego, w szczególności w sektorach, w których takie zakłócenie mogłoby mieć wpływ transgraniczny;

f) podmiot ma krytyczny charakter ze względu na jego szczególne znaczenie na poziomie regionalnym lub narodowym dla konkretnego sektora lub rodzaju usługi lub dla innych współzależnych sektorów w państwie członkowskim;

g) podmiot wskazano jako podmiot krytyczny zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) XXXX/XXXX[29] [dyrektywa w sprawie odporności podmiotów krytycznych] lub jako podmiot równoważny podmiotowi krytycznemu zgodnie z art. 7 tej dyrektywy.

Państwa członkowskie sporządzają wykaz podmiotów wskazywanych zgodnie z lit. b)–f) oraz przedkładają go Komisji do dnia [6 miesięcy po terminie transpozycji] r. Państwa członkowskie regularnie, nie rzadziej niż co dwa lata po wyżej wymienionej dacie, dokonują przeglądu tego wykazu oraz, w stosownych przypadkach, aktualizują go.

3. Niniejsza dyrektywa pozostaje bez uszczerbku dla kompetencji państw członkowskich dotyczących utrzymywania bezpieczeństwa publicznego, obrony i bezpieczeństwa narodowego zgodnie z prawem Unii.

4. Niniejszą dyrektywę stosuje się bez uszczerbku dla dyrektywy Rady 2008/114/WE[30] oraz dyrektyw Parlamentu Europejskiego i Rady 2011/93/UE[31] i 2013/40/UE[32].

---

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

29 *[wstawić pełny tytuł i odniesienie do publikacji w Dzienniku Urzędowym, kiedy już będą znane]*

30 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).

5. 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. W ramach wymiany informacji zachowuje się poufność tych informacji oraz chroni się bezpieczeństwo i interesy handlowe podmiotów niezbędnych lub istotnych.

6. W przypadku gdy na podstawie przepisów unijnych sektorowych aktów prawnych wymaga się od podmiotów niezbędnych lub istotnych przyjęcia środków zarządzania ryzykiem w cyberprzestrzeni albo zgłaszania incydentów lub znaczących cyberzagrożeń oraz w przypadku gdy skutki tych wymogów są co najmniej równoważne skutkowi obowiązków przewidzianych w niniejszej dyrektywie, nie stosuje się odpowiednich przepisów niniejszej dyrektywy, w tym przepisów dotyczących nadzoru i egzekwowania określonych w rozdziale VI.

Artykuł 3

Harmonizacja minimalna

Państwa członkowskie mogą, bez uszczerbku dla swoich innych obowiązków wynikających z prawa Unii, przyjmować lub utrzymywać – zgodnie z niniejszą dyrektywą – przepisy zapewniające wyższy poziom cyberbezpieczeństwa.

Artykuł 4

Definicje

Na potrzeby niniejszej dyrektywy stosuje się następujące definicje:

1) „sieci i systemy informatyczne” oznaczają:

   a) sieci łączności elektronicznej w rozumieniu art. 2 pkt 1 dyrektywy (UE) 2018/1972;

   b) wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których co najmniej jedno, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych;

   c) dane cyfrowe przechowywane, przetwarzane, pobierane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony i utrzymania;

---

[31] Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.U. L 335 z 17.12.2011, s. 1).

[32] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8).

2) „bezpieczeństwo sieci i systemów informatycznych” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub związanych z nimi usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;

3) „cyberbezpieczeństwo” oznacza cyberbezpieczeństwo w rozumieniu art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881[33];

4) „krajowa strategia cyberbezpieczeństwa” oznacza spójne ramy państwa członkowskiego zapewniające strategiczne cele i priorytety w zakresie bezpieczeństwa sieci i systemów informatycznych w tym państwie członkowskim;

5) „incydent” oznacza każde zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub związanych z nimi usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;

6) „postępowanie w przypadku incydentu” oznacza wszystkie działania i procedury mające na celu wykrywanie i analizowanie incydentu, ograniczenie jego skutków oraz reagowanie na niego;

7) „cyberzagrożenie” oznacza cyberzagrożenie w rozumieniu art. 2 pkt 8 rozporządzenia (UE) 2019/881;

8) „podatność” oznacza słabość, wrażliwość lub wadę zasobu, systemu, procesu lub mechanizmu kontroli, które mogą zostać wykorzystane w wyniku cyberzagrożenia;

9) „przedstawiciel” oznacza każdą osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, wyraźnie wyznaczoną do występowania w imieniu (i) dostawcy usług DNS, rejestru nazw domen najwyższego poziomu (TLD), dostawcy usług w chmurze, dostawcy usług ośrodka przetwarzania danych, dostawcy sieci dostarczania treści, o których mowa w załączniku I pkt 8, lub (ii) podmiotów, o których mowa w załączniku II pkt 6, nieposiadających jednostki organizacyjnej w Unii, do której właściwy organ krajowy lub CSIRT może się zwrócić zamiast do podmiotu w związku z obowiązkami tego podmiotu przewidzianymi w niniejszej dyrektywie;

10) „norma” oznacza normę w rozumieniu art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012[34];

11) „specyfikacja techniczna” oznacza specyfikację techniczną w rozumieniu art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012;

12) „punkt wymiany ruchu internetowego (IXP)” oznacza obiekt sieciowy, który umożliwia wzajemne połączenie więcej niż dwóch niezależnych sieci (systemów

---

[33] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

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

autonomicznych), głównie do celów ułatwienia wymiany ruchu internetowego; IXP zapewnia wzajemne połączenie wyłącznie dla systemów autonomicznych; IXP nie wymaga, aby ruch internetowy między jakąkolwiek parą uczestniczących systemów autonomicznych przechodził przez jakikolwiek trzeci system autonomiczny, ani nie powoduje zmian w tym ruchu, ani w inny sposób w niego nie ingeruje;

13) „system nazw domen (DNS)" oznacza hierarchiczny rozproszony system nazw umożliwiający użytkownikom końcowym uzyskanie dostępu do usług i zasobów w internecie;

14) „dostawca usług DNS" oznacza podmiot świadczący rekurencyjne lub autorytatywne usługi rozwiązywania nazw domen na rzecz użytkowników końcowych internetu oraz innych dostawców usług DNS;

15) „rejestr nazw domen najwyższego poziomu" oznacza podmiot, któremu powierzono konkretną domenę najwyższego poziomu (TLD) i który odpowiada za zarządzanie nią, w tym za rejestrację nazw domen w ramach TLD oraz za jej techniczne funkcjonowanie, w tym za obsługę jej serwerów nazw, utrzymanie jej baz danych oraz dystrybucję plików strefowych TLD we wszystkich serwerach nazw;

16) „usługa cyfrowa" oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady[35];

17) „internetowa platforma handlowa" oznacza usługę cyfrową w rozumieniu art. 2 lit. n) dyrektywy 2005/29/WE Parlamentu Europejskiego i Rady[36];

18) „wyszukiwarka internetowa" oznacza usługę cyfrową w rozumieniu art. 2 pkt 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150[37];

19) „usługa w chmurze" oznacza usługę cyfrową umożliwiającą administrowanie na żądanie skalowalnym i elastycznym zbiorem rozproszonych zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru;

20) „usługa ośrodka przetwarzania danych" oznacza usługę obejmującą struktury lub grupy struktur przeznaczone do scentralizowanego hostingu, zapewniania wzajemnego połączenia i eksploatacji sprzętu informatycznego i sieciowego służącego do świadczenia usług przechowywania, przetwarzania i transportu danych wraz ze wszystkimi obiektami i całą infrastrukturą na potrzeby dystrybucji energii elektrycznej i kontroli środowiskowej;

21) „sieć dostarczania treści" oznacza sieć rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności treści i usług cyfrowych lub ich

---

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

36 Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE i 2002/65/WE Parlamentu Europejskiego i Rady oraz rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady („dyrektywa o nieuczciwych praktykach handlowych") (Dz.U. L 149 z 11.6.2005, s. 22).

37 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz.U. L 186 z 11.7.2019, s. 57).

szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług;

22) „platforma usług sieci społecznościowych” oznacza platformę umożliwiającą użytkownikom końcowym łączenie się i komunikowanie ze sobą, a także udostępnianie i odkrywanie treści przy użyciu wielu urządzeń, w szczególności za pośrednictwem czatów, postów, filmów wideo i rekomendacji;

23) „podmiot administracji publicznej” oznacza podmiot w państwie członkowskim spełniający następujące kryteria:

a) został utworzony w celu zaspokajania potrzeb leżących w interesie ogólnym i nie ma charakteru przemysłowego ani handlowego;

b) posiada osobowość prawną;

c) jest finansowany w przeważającej części przez państwo, władze regionalne lub inne podmioty prawa publicznego; lub jego zarząd podlega nadzorowi ze strony tych władz lub podmiotów; lub ponad połowa członków jego organu administrującego, zarządzającego lub nadzorczego została wyznaczona przez państwo, władze regionalne lub przez inne podmioty prawa publicznego;

d) jest uprawniony do kierowania do osób fizycznych lub prawnych decyzji administracyjnych lub regulacyjnych mających wpływ na ich prawa w transgranicznym przepływie osób, towarów, usług lub kapitału.

Wyłączone są podmioty administracji publicznej, które prowadzą działalność w obszarach bezpieczeństwa publicznego, ścigania przestępstw, obronności lub bezpieczeństwa narodowego;

24) „podmiot” oznacza każdą osobę fizyczną lub prawną utworzoną jako taką i uznawaną za taką na podstawie prawa krajowego obowiązującego w miejscu, w którym osoba ta ma siedzibę, która może – działając we własnym imieniu – wykonywać prawa i podlegać obowiązkom;

25) „podmiot niezbędny” oznacza każdy podmiot w rodzaju tego, który określono jako podmiot niezbędny w załączniku I;

26) „podmiot istotny” oznacza każdy podmiot w rodzaju tego, który określono jako podmiot istotny w załączniku II.

ROZDZIAŁ II

Skoordynowane ramy regulacyjne w zakresie cyberbezpieczeństwa

Artykuł 5
Krajowa strategia cyberbezpieczeństwa

1. Każde państwo członkowskie przyjmuje krajową strategię cyberbezpieczeństwa określającą cele strategiczne i odpowiednie środki polityczne i regulacyjne mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Krajowa strategia cyberbezpieczeństwa obejmuje w szczególności:

a) określenie celów i priorytetów strategii cyberbezpieczeństwa państw członkowskich;

b) ramy zarządzania służące realizacji tych celów i priorytetów, w tym polityki, o których mowa w ust. 2, a także role i obowiązki instytucji i podmiotów publicznych, jak również innych odpowiednich podmiotów;

c) ocenę służącą określeniu istotnych zasobów i ryzyk w cyberprzestrzeni w tym państwie członkowskim;

d) wskazanie środków zapewniających gotowość na wypadek incydentów, reagowanie na nie i przywracanie stanu sprzed ich wystąpienia, z uwzględnieniem współpracy pomiędzy sektorami publicznym i prywatnym;

e) wykaz poszczególnych organów i podmiotów zaangażowanych we wdrażanie krajowej strategii cyberbezpieczeństwa;

f) ramy polityki na rzecz ściślejszej koordynacji między właściwymi organami na mocy niniejszej dyrektywy i dyrektywy Parlamentu Europejskiego i Rady (UE) XXXX/XXXX[38] [dyrektywa w sprawie odporności podmiotów krytycznych] do celów wymiany informacji na temat incydentów i cyberzagrożeń oraz wykonywania zadań nadzorczych.

2. W ramach krajowej strategii cyberbezpieczeństwa państwa członkowskie przyjmują w szczególności następujące polityki:

a) politykę dotyczącą cyberbezpieczeństwa w łańcuchu dostaw dla produktów i usług ICT wykorzystywanych przez podmioty niezbędne i istotne do świadczenia usług;

b) wytyczne dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów i usług ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień;

c) politykę mającą na celu promowanie i ułatwianie skoordynowanego ujawniania podatności w rozumieniu art. 6;

d) politykę związaną z utrzymywaniem ogólnej dostępności i integralności publicznego rdzenia otwartego internetu;

e) politykę dotyczącą promowania i rozwoju umiejętności z zakresu cyberbezpieczeństwa, zwiększania świadomości oraz inicjatyw badawczo-rozwojowych;

f) politykę dotyczącą wspierania instytucji akademickich i naukowych w celu opracowania narzędzi z zakresu cyberbezpieczeństwa oraz zabezpieczenia infrastruktury sieciowej;

g) politykę, właściwe procedury oraz odpowiednie narzędzia służące wymianie informacji mające na celu wspieranie dobrowolnej wymiany informacji na temat cyberbezpieczeństwa między przedsiębiorstwami zgodnie z prawem Unii;

h) politykę uwzględniającą konkretne potrzeby małych i średnich przedsiębiorstw, w szczególności tych wyłączonych z zakresu stosowania niniejszej dyrektywy, związane z wytycznymi i wsparciem na rzecz poprawy ich odporności na zagrożenia dla cyberbezpieczeństwa.

[38] *[wstawić pełny tytuł i odniesienie do publikacji w Dzienniku Urzędowym, kiedy już będą znane]*

3. Państwa członkowskie przekazują Komisji swoje krajowe strategie cyberbezpieczeństwa w terminie trzech miesięcy od ich przyjęcia. Państwa członkowskie mogą wyłączyć niektóre konkretne informacje ze zgłoszenia, jeżeli – i w zakresie w jakim – jest to absolutnie niezbędne do zachowania bezpieczeństwa narodowego.

4. Państwa członkowskie przeprowadzają ocenę swoich krajowych strategii cyberbezpieczeństwa co najmniej co cztery lata na podstawie kluczowych wskaźników skuteczności i w razie potrzeby wprowadzają do nich zmiany. Na wniosek państw członkowskich Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) udziela im wsparcia w opracowaniu strategii krajowej oraz kluczowych wskaźników skuteczności wykorzystywanych na potrzeby oceny strategii.

Artykuł 6

Skoordynowane ujawnianie podatności i europejski rejestr podatności

1. Każde państwo członkowskie wyznacza jeden spośród swoich CSIRT, o których mowa w art. 9, na koordynatora na potrzeby skoordynowanego ujawniania podatności. Wyznaczony CSIRT działa w charakterze zaufanego pośrednika, w stosownych przypadkach ułatwiając interakcję między podmiotem zgłaszającym a producentem lub dostawcą produktów lub usług ICT. Jeżeli zgłoszona podatność dotyczy wielu producentów lub dostawców produktów lub usług ICT w Unii, wyznaczony CSIRT z każdego państwa członkowskiego, w którym ujawniono podatność, współpracuje z siecią CSIRT.

2. ENISA opracowuje i prowadzi europejski rejestr podatności. W tym celu ENISA ustanawia i utrzymuje odpowiednie systemy informatyczne, polityki i procedury, w szczególności aby umożliwić podmiotom istotnym i niezbędnym oraz ich dostawcom sieci i systemów informatycznych ujawnianie i rejestrowanie podatności występujących w produktach lub usługach ICT, a także aby zapewnić wszystkim zainteresowanym stronom dostęp do informacji na temat podatności wykazanych w rejestrze. Rejestr zawiera w szczególności informacje na temat podatności, produktu lub usług ICT, których ta podatność dotyczy, oraz dotkliwości podatności pod względem okoliczności, w jakich może ona zostać wykorzystana, dostępności powiązanych łat oraz, w przypadku braku dostępnych łat, wytyczne skierowane do użytkowników produktów i usług, których dotyczy podatność, na temat sposobów ograniczania ryzyka wynikającego z ujawnionych podatności.

Artykuł 7

Krajowe ramy zarządzania kryzysami cyberbezpieczeństwa

1. Każde państwo członkowskie wyznacza co najmniej jeden właściwy organ odpowiedzialny za zarządzanie incydentami i kryzysami na dużą skalę. Państwa członkowskie zapewniają właściwym organom odpowiednie zasoby, aby mogły one efektywnie i skutecznie wykonywać powierzone im zadania.

2. Każde państwo członkowskie określa zdolności, zasoby i procedury, które można wykorzystać w razie kryzysu do celów niniejszej dyrektywy.

3. Każde państwo członkowskie przyjmuje krajowy plan reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa, w którym określa cele i tryb zarządzania cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę. W planie określa się w szczególności:

   a) cele krajowych środków i działań służących zapewnieniu gotowości;

   b) zadania i obowiązki właściwych organów krajowych;

   c) procedury zarządzania kryzysowego oraz kanały wymiany informacji;

   d) środki służące zapewnieniu gotowości, w tym ćwiczenia i szkolenia;

   e) odpowiednie zaangażowane publiczne i prywatne zainteresowane strony oraz odpowiednią infrastrukturę publiczną i prywatną;

   f) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie skutecznego uczestnictwa danego państwa członkowskiego w skoordynowanym zarządzaniu cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę na szczeblu Unii oraz skutecznego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania.

4. Państwa członkowskie informują Komisję o wyznaczeniu właściwych organów, o których mowa w ust. 1, i przedkładają krajowe plany reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa, o których mowa w ust. 3, w terminie trzech miesięcy od daty wyznaczenia tych organów oraz od daty przyjęcia tych planów. Państwa członkowskie mogą wyłączyć niektóre konkretne informacje z planu, jeżeli – i w zakresie w jakim – jest to absolutnie niezbędne dla zachowania bezpieczeństwa narodowego.

Artykuł 8

Właściwe organy krajowe i pojedyncze punkty kontaktowe

1. Każde państwo członkowskie wyznacza co najmniej jeden właściwy organ odpowiedzialny za cyberbezpieczeństwo oraz za zadania nadzorcze, o których mowa w rozdziale VI niniejszej dyrektywy. Państwa członkowskie mogą wyznaczyć w tym celu istniejący organ lub istniejące organy.

2. Właściwe organy, o których mowa w ust. 1, monitorują stosowanie niniejszej dyrektywy na poziomie krajowym.

3. Każde państwo członkowskie wyznacza jeden krajowy pojedynczy punkt kontaktowy ds. cyberbezpieczeństwa („pojedynczy punkt kontaktowy”). W przypadku gdy państwo członkowskie wyznacza tylko jeden właściwy organ, ten właściwy organ jest również pojedynczym punktem kontaktowym dla tego państwa członkowskiego.

4. Każdy pojedynczy punkt kontaktowy pełni funkcję łącznikową w celu zapewnienia transgranicznej współpracy organów swojego państwa członkowskiego z odpowiednimi organami w innych państwach członkowskich, a także w celu zapewnienia międzysektorowej współpracy z innymi właściwymi organami krajowymi w swoim państwie członkowskim.

5. Państwa członkowskie zapewniają właściwym organom, o których mowa w ust. 1, i pojedynczym punktom kontaktowym odpowiednie zasoby, aby mogły one

efektywnie i skutecznie wykonywać powierzone im zadania, a tym samym realizować cele niniejszej dyrektywy. Państwa członkowskie zapewniają efektywną, skuteczną i bezpieczną współpracę wyznaczonych przedstawicieli w ramach Grupy Współpracy, o której mowa w art. 12.

6. Każde państwo członkowskie bez zbędnej zwłoki powiadamia Komisję o wyznaczeniu właściwego organu, o którym mowa w ust. 1, i pojedynczego punktu kontaktowego, o którym mowa w ust. 3, o ich zadaniach i o wszelkich późniejszych zmianach w tym zakresie. Każde państwo członkowskie podaje informację o takim wyznaczeniu do wiadomości publicznej. Komisja publikuje wykaz wyznaczonych pojedynczych punktów kontaktowych.

Artykuł 9

Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)

1. Każde państwo członkowskie wyznacza co najmniej jeden CSIRT spełniający wymogi określone w art. 10 ust. 1, obejmujący przynajmniej sektory, podsektory lub podmioty, o których mowa w załącznikach I i II, i odpowiedzialny za postępowanie w przypadku incydentu zgodnie z jasno określoną procedurą. CSIRT można ustanowić w ramach właściwego organu, o którym mowa w art. 8.

2. Państwa członkowskie zapewniają, aby każdy CSIRT dysponował odpowiednimi zasobami, tak aby mógł skutecznie realizować swoje zadania określone w art. 10 ust. 2.

3. Państwa członkowskie zapewniają, aby każdy CSIRT miał do dyspozycji odpowiednią, bezpieczną i odporną infrastrukturę komunikacyjno-informacyjną w celu wymiany informacji z podmiotami niezbędnymi i istotnymi, a także innymi odpowiednimi zainteresowanymi stronami. W tym celu państwa członkowskie zapewniają, aby CSIRT przyczyniały się do wdrażania bezpiecznych narzędzi wymiany informacji.

4. CSIRT współpracują z zaufanymi sektorowymi i międzysektorowymi społecznościami podmiotów niezbędnych i istotnych oraz, w odpowiednich przypadkach, wymieniają z nimi stosowne informacje zgodnie z art. 26.

5. CSIRT biorą udział we wzajemnej ocenie organizowanej zgodnie z art. 16.

6. Państwa członkowskie zapewniają skuteczną, efektywną i bezpieczną współpracę swoich CSIRT w ramach sieci CSIRT, o której mowa w art. 13.

7. Państwa członkowskie bez zbędnej zwłoki przekazują Komisji informacje na temat CSIRT wyznaczonych zgodnie z ust. 1, koordynatora CSIRT wyznaczonego zgodnie z art. 6 ust. 1 oraz ich odpowiednich zadań realizowanych w odniesieniu do podmiotów, o których mowa w załącznikach I i II.

8. Państwa członkowskie mogą zwrócić się do ENISA o pomoc przy tworzeniu krajowych CSIRT.

Artykuł 10

Wymogi dotyczące CSIRT i ich zadania

1. CSIRT spełniają następujące wymogi:

a) CSIRT zapewniają wysoką dostępność swoich usług łączności poprzez unikanie pojedynczych punktów awarii oraz dysponują różnymi kanałami, za pomocą których zawsze można się z nimi skontaktować i za pomocą których one same mogą się kontaktować z innymi podmiotami. CSIRT jasno określają kanały komunikacji i informują o nich użytkowników CSIRT i współpracujących partnerów;

b) pomieszczenia CSIRT oraz wspierające systemy informatyczne muszą być zlokalizowane w bezpiecznych miejscach;

c) CSIRT dysponują systemem zarządzania kierowanymi do nich wnioskami i ich przekierowywania, w szczególności w celu ułatwienia skutecznego i efektywnego późniejszego przekazywania danej sprawy;

d) CSIRT dysponują odpowiednio licznym personelem, aby zapewnić nieprzerwaną dostępność;

e) CSIRT dysponują systemami redundantnymi i rezerwowym miejscem pracy w celu zapewnienia ciągłości usług;

f) CSIRT muszą mieć możliwość udziału w międzynarodowych sieciach współpracy.

2. CSIRT mają następujące zadania:

a) monitorowanie cyberzagrożeń, podatności i incydentów na poziomie krajowym;

b) wczesne ostrzeganie i alarmowanie podmiotów niezbędnych i istotnych oraz innych zainteresowanych stron o cyberzagrożeniach, podatnościach i incydentach, a także kierowanie do nich ogłoszeń oraz przekazywanie im informacji dotyczących cyberzagrożeń, podatności i incydentów;

c) reagowanie na incydenty;

d) zapewnianie dynamicznej analizy ryzyka i incydentów oraz orientacji sytuacyjnej w zakresie cyberbezpieczeństwa;

e) przeprowadzanie, na wniosek podmiotu, aktywnego skanowania sieci i systemów informatycznych wykorzystywanych przez dany podmiot do świadczenia usług;

f) uczestnictwo w sieci CSIRT oraz udzielanie wzajemnej pomocy innym członkom sieci na ich wniosek.

3. CSIRT nawiązują współpracę z odpowiednimi podmiotami w sektorze prywatnym w celu skuteczniejszej realizacji celów niniejszej dyrektywy.

4. Aby ułatwić współpracę, CSIRT promują przyjmowanie i stosowanie wspólnych lub znormalizowanych praktyk, systemów klasyfikacji oraz taksonomii związanych z:

a) procedurami postępowania w przypadku incydentu;

b) zarządzaniem kryzysami cyberbezpieczeństwa;

c) skoordynowanym ujawnianiem podatności.

Artykuł 11

Współpraca na poziomie krajowym

1. Jeżeli właściwe organy, o których mowa w art. 8, pojedynczy punkt kontaktowy i CSIRT z tego samego państwa członkowskiego są odrębne względem siebie, współpracują ze sobą w kontekście realizacji obowiązków przewidzianych w niniejszej dyrektywie.

2. Państwa członkowskie zapewniają, aby ich właściwe organy albo ich CSIRT odbierały zgłoszenia incydentów, istotnych cyberzagrożeń i zdarzeń potencjalnie wypadkowych dokonywane na podstawie niniejszej dyrektywy. W przypadku gdy państwo członkowskie postanowi, że jego CSIRT nie będą odbierać takich zgłoszeń, CSIRT otrzymają, w stopniu koniecznym do wykonywania swoich zadań, dostęp do danych dotyczących incydentów zgłaszanych przez podmioty niezbędne lub istotne na podstawie art. 20.

3. Każde państwo członkowskie zapewnia, aby jego właściwe organy lub CSIRT informowały jego pojedynczy punkt kontaktowy o zgłoszeniach incydentów, istotnych cyberzagrożeń i zdarzeń potencjalnie wypadkowych dokonywanych na podstawie niniejszej dyrektywy.

4. W zakresie niezbędnym do skutecznej realizacji zadań i obowiązków przewidzianych w niniejszej dyrektywie państwa członkowskie zapewniają odpowiednią współpracę między właściwymi organami i pojedynczymi punktami kontaktowymi a organami ścigania, organami ochrony danych i organami odpowiedzialnymi za infrastrukturę krytyczną na mocy dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych] oraz krajowymi organami finansowymi wyznaczonymi na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego][39] w danym państwie członkowskim.

5. Państwa członkowskie zapewniają, aby ich właściwe organy regularnie przekazywały właściwym organom wyznaczonym na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych] informacje na temat ryzyka w cyberprzestrzeni, cyberzagrożeń i incydentów mających wpływ na podmioty niezbędne uznane za podmioty krytyczne lub za podmioty równoważne z podmiotami krytycznymi na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych], a także na temat środków wprowadzonych przez właściwe organy w odpowiedzi na takie ryzyko i incydenty.

ROZDZIAŁ III

[39] *[wstawić pełny tytuł i odniesienie do publikacji w Dzienniku Urzędowym, kiedy już będą znane]*

Współpraca

Artykuł 12
Grupa Współpracy

1. Aby wspierać i ułatwiać strategiczną współpracę i wymianę informacji między państwami członkowskimi w obszarze stosowania dyrektywy, ustanawia się Grupę Współpracy.

2. Grupa Współpracy wykonuje swoje zadania na podstawie dwuletnich programów prac, o których mowa w ust. 6.

3. Grupa Współpracy składa się z przedstawicieli państw członkowskich, Komisji i ENISA. Europejska Służba Działań Zewnętrznych uczestniczy w działaniach Grupy Współpracy w charakterze obserwatora. Zgodnie z art. 17 ust. 5 lit. c) rozporządzenia (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego] Europejskie Urzędy Nadzoru mogą uczestniczyć w działaniach Grupy Współpracy.

   W stosownych przypadkach Grupa Współpracy może zapraszać przedstawicieli odpowiednich zainteresowanych stron do udziału w swoich pracach.

   Komisja zapewnia obsługę sekretariatu.

4. Grupa Współpracy ma następujące zadania:

   a) udzielanie wskazówek właściwym organom w związku z transpozycją i wdrażaniem niniejszej dyrektywy;

   b) wymiana najlepszych praktyk i informacji w związku z wdrażaniem niniejszej dyrektywy, w tym w odniesieniu do cyberzagrożeń, incydentów, podatności, zdarzeń potencjalnie wypadkowych, inicjatyw na rzecz podnoszenia świadomości, szkoleń, ćwiczeń i umiejętności, budowania zdolności, a także norm i specyfikacji technicznych;

   c) wymiana porad i współpraca z Komisją w zakresie nowych inicjatyw dotyczących polityki cyberbezpieczeństwa;

   d) wymiana porad i współpraca z Komisją w zakresie projektów aktów wykonawczych lub delegowanych Komisji przyjmowanych na podstawie niniejszej dyrektywy;

   e) wymiana najlepszych praktyk i informacji z odpowiednimi instytucjami, organami i jednostkami organizacyjnymi Unii;

   f) omawianie sprawozdań z wzajemnej oceny, o których mowa w art. 16 ust. 7;

   g) omawianie wyników działań w zakresie wspólnego nadzoru w sprawach transgranicznych, o których mowa w art. 34;

   h) zapewnianie sieci CSIRT wytycznych strategicznych dotyczących konkretnych pojawiających się kwestii;

   i) przyczynianie się do rozwoju zdolności w zakresie cyberbezpieczeństwa w całej Unii przez ułatwianie wymiany urzędników krajowych w ramach programu budowania zdolności obejmującego pracowników właściwych organów lub CSIRT z państw członkowskich;

j) organizowanie regularnych wspólnych spotkań z odpowiednimi prywatnymi zainteresowanymi stronami z całej Unii w celu omawiania działań realizowanych przez Grupę i gromadzenia informacji na temat pojawiających się wyzwań w zakresie polityki;

k) omawianie działań podjętych w związku z ćwiczeniami z zakresu cyberbezpieczeństwa, w tym pracy wykonanej przez ENISA.

5. Grupa Współpracy może zwracać się do sieci CSIRT o sporządzenie sprawozdania technicznego na wybrane tematy.

6. W terminie do dnia ...[, 24 miesiące od daty wejścia w życie niniejszej dyrektywy] r., a następnie co dwa lata Grupa Współpracy opracowuje program prac obejmujący działania, które mają zostać podjęte w celu realizacji jej celów i zadań. Ramy czasowe pierwszego programu przyjętego na podstawie niniejszej dyrektywy muszą być zharmonizowane z ramami czasowymi ostatniego programu przyjętego na podstawie dyrektywy (UE) 2016/1148.

7. Komisja może przyjąć akty wykonawcze określające ustalenia proceduralne niezbędne do funkcjonowania Grupy Współpracy. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2.

8. Grupa Współpracy spotyka się regularnie, przy czym co najmniej raz w roku, z Grupą ds. Odporności Podmiotów Krytycznych ustanowioną na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych] w celu propagowania współpracy strategicznej i wymiany informacji.

Artykuł 13
Sieć CSIRT

1. Ustanawia się sieć krajowych CSIRT, aby przyczyniać się do rozwijania pewności i zaufania oraz promować szybką i skuteczną współpracę operacyjną między państwami członkowskimi.

2. Sieć CSIRT składa się z przedstawicieli CSIRT państw członkowskich i CERT-EU. Komisja uczestniczy w pracach sieci CSIRT jako obserwator. ENISA zapewnia obsługę sekretariatu oraz aktywnie wspiera współpracę między CSIRT.

3. Sieć CSIRT ma następujące zadania:

a) wymiana informacji na temat zdolności CSIRT;

b) wymiana stosownych informacji na temat incydentów, zdarzeń potencjalnie wypadkowych, cyberzagrożeń, ryzyk i podatności;

c) na wniosek przedstawiciela sieci CSIRT, na którego potencjalnie może mieć wpływ incydent – wymiana i omówienie informacji dotyczących tego incydentu i związanych z nim cyberzagrożeń, ryzyk i podatności;

d) na wniosek przedstawiciela sieci CSIRT – omówienie oraz, w miarę możliwości, wdrożenie skoordynowanej reakcji na incydent, który zidentyfikowano w granicach jurysdykcji tego państwa członkowskiego;

e) zapewnianie państwom członkowskim wsparcia w podejmowaniu odpowiednich działań w reakcji na incydenty transgraniczne zgodnie z niniejszą dyrektywą;

f) współpraca z wyznaczonymi CSIRT, o których mowa w art. 6, oraz zapewnianie im pomocy w odniesieniu do zarządzania wielostronnym skoordynowanym ujawnianiem podatności mających wpływ na wielu producentów lub dostawców produktów ICT, usług ICT oraz procesów ICT ustanowionych w różnych państwach członkowskich;

g) omawianie i wskazywanie dalszych form współpracy operacyjnej, w tym w związku z:

(i) kategoriami cyberzagrożeń i incydentów;

(ii) wczesnym ostrzeganiem;

(iii) wzajemną pomocą;

(iv) zasadami i trybem koordynacji w odpowiedzi na transgraniczne ryzyka i incydenty;

(v) udziałem w opracowaniu krajowego planu reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa, o którym mowa w art. 7 ust. 3;

h) informowanie Grupy Współpracy o swoich działaniach i o dalszych formach współpracy operacyjnej omawianych zgodnie z lit. g), w tym występowanie w razie potrzeby z wnioskami o wskazówki w tym zakresie;

i) omawianie wniosków z ćwiczeń z zakresu cyberbezpieczeństwa, w tym ćwiczeń organizowanych przez ENISA;

j) na wniosek danego CSIRT – omawianie zdolności i gotowości tego CSIRT;

k) współpraca i wymiana informacji z regionalnymi i unijnymi centrami monitorowania bezpieczeństwa (SOC) w celu poprawy wspólnej orientacji sytuacyjnej w zakresie incydentów i zagrożeń w całej Unii;

l) omawianie sprawozdań z wzajemnej oceny, o których mowa w art. 16 ust. 7;

m) wydawanie wytycznych w celu ułatwienia konwergencji praktyk operacyjnych w odniesieniu do stosowania przepisów niniejszego artykułu dotyczących współpracy operacyjnej.

4. Na potrzeby przeglądu, o którym mowa w art. 35, oraz w terminie do dnia ...[24 miesiące od daty wejścia w życie niniejszej dyrektywy] r., a następnie co dwa lata sieć CSIRT ocenia postępy we współpracy operacyjnej i sporządza sprawozdanie. Sprawozdanie to zawiera w szczególności wnioski dotyczące wyników wzajemnych ocen, o których mowa w art. 16, przeprowadzonych w odniesieniu do krajowych CSIRT, w tym wnioski i zalecenia sformułowane na podstawie tego artykułu. Sprawozdanie to przedkłada się także Grupie Współpracy.

5. Sieć CSIRT przyjmuje swój regulamin wewnętrzny.

Artykuł 14

Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe)

1. Niniejszym ustanawia się europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe), aby wspierać skoordynowane zarządzanie cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę oraz

zapewniać regularną wymianę informacji między państwami członkowskimi a instytucjami, organami i jednostkami organizacyjnymi Unii.

2. EU-CyCLONe składa się z przedstawicieli organów zarządzania kryzysowego państw członkowskich, wyznaczonych zgodnie z art. 7, Komisji i ENISA. ENISA zapewnia obsługę sekretariatu sieci i wspiera bezpieczną wymianę informacji.

3. EU-CyCLONe ma następujące zadania:

   a) podnoszenie poziomu gotowości w zakresie zarządzania incydentami i kryzysami na dużą skalę;

   b) rozwijanie wspólnej orientacji sytuacyjnej w zakresie istotnych zdarzeń związanych z cyberbezpieczeństwem;

   c) koordynowanie zarządzania incydentami i kryzysami na dużą skalę oraz wspieranie procesu decyzyjnego na szczeblu politycznym w odniesieniu do takich incydentów i kryzysów;

   d) omawianie krajowych planów reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa, o których mowa w art. 7 ust. 2.

4. EU-CyCLONe przyjmuje swój regulamin wewnętrzny.

5. EU-CyCLONe regularnie składa Grupie Współpracy sprawozdania na temat cyberzagrożeń, incydentów i tendencji w dziedzinie cyberbezpieczeństwa, koncentrując się w szczególności na ich wpływie na podmioty niezbędne i istotne.

6. EU-CyCLONe współpracuje z siecią CSIRT na podstawie uzgodnionych ustaleń proceduralnych.

Artykuł 15

Sprawozdanie o stanie cyberbezpieczeństwa w Unii

1. ENISA wydaje co dwa lata, we współpracy z Komisją, sprawozdanie o stanie cyberbezpieczeństwa w Unii. Sprawozdanie zawiera w szczególności ocenę następujących elementów:

   a) rozwoju zdolności w zakresie cyberbezpieczeństwa w całej Unii;

   b) zasobów technicznych, finansowych i ludzkich dostępnych właściwym organom oraz na potrzeby polityki cyberbezpieczeństwa, a także wdrożenia środków nadzoru i działań z zakresu egzekwowania przepisów w świetle wyników wzajemnych ocen, o których mowa w art. 16;

   c) wskaźnika cyberbezpieczeństwa zapewniającego zbiorczą ocenę poziomu dojrzałości zdolności w zakresie cyberbezpieczeństwa.

2. Sprawozdanie zawiera konkretne zalecenia polityczne dotyczące zwiększenia poziomu cyberbezpieczeństwa w całej Unii oraz streszczenie ustaleń za dany okres zawartych w raportach technicznych Agencji o stanie cyberbezpieczeństwa w UE wydanych przez ENISA zgodnie z art. 7 ust. 6 rozporządzenia (UE) 2019/881.

Artykuł 16

Wzajemne oceny

1. Komisja ustanawia, po konsultacji z Grupą Współpracy i ENISA i najpóźniej 18 miesięcy po wejściu w życie niniejszej dyrektywy, metodykę i zawartość systemu wzajemnej oceny służącego do oceny skuteczności polityki cyberbezpieczeństwa państw członkowskich. Oceny są przeprowadzane przez ekspertów technicznych ds. cyberbezpieczeństwa pochodzących z innych państw członkowskich niż państwo poddawane ocenie i obejmują co najmniej następujące kwestie:

   (i) skuteczność wdrażania wymogów w zakresie zarządzania ryzykiem w cyberprzestrzeni oraz obowiązków w zakresie zgłaszania incydentów, o których mowa w art. 18 i 20;

   (ii) poziom zdolności, w tym dostępne zasoby finansowe, techniczne i ludzkie, oraz skuteczność wykonywania zadań przez właściwe organy krajowe;

   (iii) zdolność operacyjną i skuteczność CSIRT;

   (iv) skuteczność wzajemnej pomocy, o której mowa w art. 34;

   (v) skuteczność ram wymiany informacji, o których mowa w art. 26 niniejszej dyrektywy.

2. Metodyka ta obejmuje obiektywne, niedyskryminacyjne, sprawiedliwe i przejrzyste kryteria, na podstawie których państwa członkowskie wyznaczają ekspertów uprawnionych do przeprowadzania wzajemnych ocen. ENISA i Komisja wyznaczają ekspertów do udziału we wzajemnych ocenach w charakterze obserwatorów. Komisja, przy wsparciu ENISA, ustanawia w ramach metodyki, o której mowa w ust. 1, obiektywny, niedyskryminacyjny, sprawiedliwy i przejrzysty system wyboru i losowego przydzielania ekspertów do każdej wzajemnej oceny.

3. O organizacyjnych aspektach wzajemnej oceny decyduje Komisja, przy wsparciu ENISA i po konsultacjach z Grupą Współpracy, na podstawie kryteriów określonych w metodyce, o której mowa w ust. 1. W ramach wzajemnych ocen oceniane są aspekty, o których mowa w ust. 1, w odniesieniu do wszystkich państw członkowskich i sektorów, w tym ukierunkowane kwestie specyficzne dla jednego państwa członkowskiego lub kilku państw członkowskich bądź dla jednego sektora lub kilku sektorów.

4. Wzajemne oceny wiążą się z faktycznymi lub wirtualnymi kontrolami na miejscu i zdalną wymianą informacji. Mając na uwadze zasadę dobrej współpracy, państwa członkowskie objęte oceną dostarczają wyznaczonym ekspertom wymaganych informacji niezbędnych do oceny aspektów poddawanych ocenie. Wszelkie informacje uzyskane w trakcie przeprowadzania wzajemnej oceny wykorzystuje się wyłącznie do tego celu. Eksperci uczestniczący we wzajemnej ocenie nie ujawniają osobom trzecim żadnych informacji szczególnie chronionych ani poufnych uzyskanych w trakcie tej oceny.

5. Po dokonaniu oceny w danym państwie członkowskim te same aspekty nie podlegają dalszej wzajemnej ocenie w tym państwie członkowskim przez kolejne dwa lata od zakończenia wzajemnej oceny, chyba że Komisja, po konsultacji z ENISA i Grupą Współpracy, postanowi inaczej.

6. Państwo członkowskie zapewnia, aby wszelkie ryzyko konfliktu interesów dotyczące wyznaczonych ekspertów zostało bez zbędnej zwłoki ujawnione pozostałym państwom członkowskim, Komisji i ENISA.

7. Eksperci uczestniczący we wzajemnych ocenach sporządzają sprawozdania dotyczące ustaleń i wniosków z ocen. Sprawozdania są przedkładane Komisji, Grupie Współpracy, sieci CSIRT i ENISA. Sprawozdania są omawiane w ramach Grupy Współpracy i sieci CSIRT. Sprawozdania mogą być publikowane na specjalnej stronie internetowej Grupy Współpracy.

ROZDZIAŁ IV

Zarządzanie ryzykiem w cyberprzestrzeni i obowiązki w zakresie zgłaszania incydentów

SEKCJA I

Zarządzanie ryzykiem w cyberprzestrzeni i zgłaszanie incydentów

Artykuł 17

Zarządzanie

1. Państwa członkowskie zapewniają, aby organy zarządzające podmiotów niezbędnych i istotnych zatwierdzały środki zarządzania ryzykiem w cyberprzestrzeni przyjęte przez te podmioty w celu zapewnienia zgodności z art. 18, nadzorowały ich wdrażanie i ponosiły odpowiedzialność za niewypełnianie przez te podmioty obowiązków wynikających z niniejszego artykułu.

2. Państwa członkowskie zapewniają, aby członkowie organu zarządzającego regularnie odbywali specjalne szkolenia w celu zdobycia wiedzy i umiejętności wystarczających do zrozumienia i oceny ryzyk w cyberprzestrzeni oraz praktyk z zakresu zarządzania takimi ryzykami oraz ich wpływu na działalność podmiotu.

Artykuł 18

Środki zarządzania ryzykiem w cyberprzestrzeni

1. Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne wprowadzały odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do świadczenia usług. Uwzględniając najnowszy stan wiedzy, środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka.

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

   a) analizę ryzyka i politykę bezpieczeństwa systemów informatycznych;

   b) postępowanie w przypadku incydentu (zapobieganie incydentom, wykrywanie ich i reagowanie na nie);

c) ciągłość działania i zarządzanie kryzysowe;

d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego dostawcami lub usługodawcami, takimi jak dostawcy usług przechowywania i przetwarzania danych lub zarządzanych usług w zakresie bezpieczeństwa;

e) bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;

f) polityki i procedury (z zakresu testowania i audytu) służące ocenie skuteczności środków zarządzania ryzykiem w cyberprzestrzeni;

g) stosowanie kryptografii i szyfrowania.

3. Państwa członkowskie zapewniają, aby w przypadku rozważania odpowiednich środków, o których mowa w ust. 2 lit. d), podmioty uwzględniały podatności charakterystyczne dla każdego dostawcy i usługodawcy oraz ogólną jakość produktów i praktyk w zakresie cyberbezpieczeństwa swoich dostawców produktów i usług, w tym ich procedury bezpiecznego opracowywania.

4. Państwa członkowskie zapewniają, aby w przypadku gdy podmiot stwierdzi, że jego usługi lub zadania nie są zgodne z wymogami określonymi w ust. 2, bez zbędnej zwłoki wprowadzał on wszelkie niezbędne środki naprawcze w celu zapewnienia zgodności danej usługi.

5. Komisja może przyjąć akty wykonawcze w celu określenia specyfikacji technicznych i metodycznych elementów, o których mowa w ust. 2. Przygotowując te akty, Komisja postępuje zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2, i w jak najszerszym zakresie stosuje się do norm międzynarodowych i europejskich, a także odpowiednich specyfikacji technicznych.

6. Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 36, aby uzupełnić elementy określone w ust. 2 w celu uwzględnienia nowych cyberzagrożeń, rozwoju technologicznego lub specyfiki sektora.

Artykuł 19

Unijna skoordynowana ocena ryzyka krytycznych łańcuchów dostaw

1. Grupa Współpracy, we współpracy z Komisją i ENISA, może przeprowadzać skoordynowane oceny ryzyka dotyczące bezpieczeństwa w odniesieniu do określonych krytycznych łańcuchów dostaw usług, systemów lub produktów ICT, z uwzględnieniem technicznych i, w stosownych przypadkach, pozatechnicznych czynników ryzyka.

2. Komisja, po konsultacji z Grupą Współpracy i ENISA, wskazuje konkretne krytyczne usługi, systemy lub produkty ICT, które mogą podlegać skoordynowanej ocenie ryzyka, o której mowa w ust. 1.

Artykuł 20

Obowiązki w zakresie zgłaszania incydentów

1. Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne bez zbędnej zwłoki zgłaszały właściwym organom lub CSIRT, zgodnie z ust. 3 i 4, każdy incydent mający istotny wpływ na świadczenie przez nich usług. W stosownych przypadkach podmioty te bez zbędnej zwłoki powiadamiają odbiorców swoich usług o incydentach, które mogą mieć niekorzystny wpływ na świadczenie danej usługi. Państwa członkowskie zapewniają, aby wspomniane podmioty zgłaszały m.in. wszelkie informacje umożliwiające właściwym organom lub CSIRT ustalenie transgranicznego wpływu incydentu.

2. Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne bez zbędnej zwłoki zgłaszały właściwym organom lub CSIRT wszelkie istotne cyberzagrożenia, które zidentyfikują jako zagrożenia mogące doprowadzić do wystąpienia znaczącego incydentu.

   W stosownych przypadkach podmioty te bez zbędnej zwłoki powiadamiają odbiorców swoich usług, których potencjalnie dotyczy znaczące cyberzagrożenie, o wszelkich środkach zaradczych lub innych środkach, które ci odbiorcy mogą zastosować w odpowiedzi na to zagrożenie. W stosownych przypadkach podmioty powiadamiają również tych odbiorców o samym zagrożeniu. Zgłoszenie nie może narażać podmiotu zgłaszającego na zwiększoną odpowiedzialność.

3. Incydent uznaje się za znaczący, jeżeli:

   a) incydent spowodował lub może spowodować istotne zakłócenia operacyjne lub straty finansowe dla danego podmiotu;

   b) incydent wpłynął lub może wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne straty materialne lub niematerialne.

4. Państwa członkowskie zapewniają, aby do celów zgłoszenia, o którym mowa w ust. 1, zainteresowane podmioty przedkładały właściwym organom lub CSIRT:

   a) bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia wiedzy o incydencie – zgłoszenie wstępne, w którym, w stosownych przypadkach, wskazuje się, czy incydent został wywołany, jak przypuszcza się, działaniem bezprawnym lub działaniem w złym zamiarze;

   b) na wniosek właściwego organu lub CSIRT – sprawozdanie okresowe na temat odpowiednich aktualizacji statusu;

   c) sprawozdanie końcowe nie później niż miesiąc po dokonaniu zgłoszenia, o którym mowa w lit. a), zawierające co najmniej następujące elementy:

      (i) szczegółowy opis incydentu, jego dotkliwości i skutków;

      (ii) rodzaj zagrożenia lub pierwotną przyczynę, które prawdopodobnie były źródłem incydentu;

      (iii) zastosowane i bieżące środki ograniczające ryzyko.

   Państwa członkowskie przewidują – w należycie uzasadnionych przypadkach i w porozumieniu z właściwymi organami lub CSIRT – możliwość odstąpienia przez dany podmiot od terminu określonego w lit. a) i c).

5. W ciągu 24 godzin od otrzymania zgłoszenia wstępnego, o którym mowa w ust. 4 lit. a), właściwe organy krajowe lub CSIRT udzielają podmiotowi zgłaszającemu odpowiedzi, w tym wstępnych informacji zwrotnych na temat incydentu oraz, na wniosek podmiotu, wytycznych dotyczących wdrożenia możliwych środków ograniczających ryzyko. W przypadku gdy CSIRT nie otrzymał zgłoszenia, o którym mowa w ust. 1, wytyczne przekazuje właściwy organ we współpracy z CSIRT. Na wniosek zainteresowanego podmiotu CSIRT zapewnia dodatkowe wsparcie techniczne. Jeżeli zachodzi podejrzenie, że incydent ma charakter przestępczy, właściwe organy krajowe lub CSIRT udzielają również wytycznych dotyczących zgłaszania incydentu organom ścigania.

6. W stosownych przypadkach, w szczególności gdy incydent, o którym mowa w ust. 1, dotyczy co najmniej dwóch państw członkowskich, właściwy organ lub CSIRT informują o incydencie pozostałe państwa członkowskie, których dotyczy incydent, i ENISA. W działaniach tych właściwe organy, CSIRT i pojedyncze punkty kontaktowe – zgodnie z prawem Unii lub prawodawstwem krajowym zgodnym z prawem Unii – chronią interesy bezpieczeństwa i interesy handlowe podmiotu, jak również zachowują poufność przekazywanych informacji.

7. W przypadku gdy świadomość społeczeństwa jest niezbędna, żeby zapobiec wystąpieniu incydentu lub poradzić sobie z trwającym incydentem, lub w przypadku gdy ujawnienie incydentu z innych względów leży w interesie publicznym, właściwy organ lub CSIRT oraz, w stosownych przypadkach, organy lub CSIRT innych zainteresowanych państw członkowskich mogą, po konsultacji z zainteresowanym podmiotem, poinformować społeczeństwo o incydencie lub zobowiązać do tego ten podmiot.

8. Na wniosek właściwego organu lub CSIRT pojedynczy punkt kontaktowy przekazuje zgłoszenia, otrzymane zgodnie z ust. 1 i 2, pojedynczym punktom kontaktowym w innych państwach członkowskich, których dotyczy incydent.

9. Pojedynczy punkt kontaktowy co miesiąc przedkłada ENISA sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane dotyczące incydentów, znaczących cyberzagrożeń i zdarzeń potencjalnie wypadkowych zgłoszonych zgodnie z ust. 1 i 2 oraz zgodnie z art. 27. Aby przyczynić się do dostarczania porównywalnych informacji, ENISA może wydawać wytyczne techniczne dotyczące parametrów informacji zawartych w sprawozdaniu podsumowującym.

10. Właściwe organy przekazują właściwym organom wyznaczonym na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych] informacje na temat incydentów i cyberzagrożeń zgłaszanych zgodnie z ust. 1 i 2 przez podmioty niezbędne uznane za podmioty krytyczne lub za podmioty równoważne z podmiotami krytycznymi na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych].

11. Komisja może przyjąć akty wykonawcze doprecyzowujące rodzaj informacji, format i procedurę zgłoszenia dokonywanego zgodnie z ust. 1 i 2. Komisja może również przyjąć akty wykonawcze w celu doprecyzowania przypadków, w których incydent uznaje się za znaczący, o czym mowa w ust. 3. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2.

Artykuł 21

Stosowanie europejskich programów certyfikacji cyberbezpieczeństwa

1. Aby wykazać zgodność z niektórymi wymogami określonymi w art. 18, państwa członkowskie mogą wymagać od podmiotów niezbędnych i istotnych certyfikacji niektórych produktów, usług i procesów ICT w oparciu o określone europejskie programy certyfikacji cyberbezpieczeństwa przyjęte na podstawie art. 49 rozporządzenia (UE) 2019/881. Produkty, usługi i procesy podlegające certyfikacji mogą być opracowywane przez podmiot niezbędny lub istotny lub mogą być zamawiane u osób trzecich.
2. Komisja jest uprawniona do przyjęcia aktów delegowanych określających, które kategorie podmiotów niezbędnych mają obowiązek na podstawie ust. 1 uzyskać certyfikację i na podstawie których konkretnych europejskich programów certyfikacji cyberbezpieczeństwa mają ją uzyskać. Akty delegowane przyjmuje się zgodnie z art. 36.
3. Komisja może zwrócić się do ENISA o przygotowanie propozycji programu zgodnie z art. 48 ust. 2 rozporządzenia (UE) 2019/881 w przypadkach, gdy do celów ust. 2 nie jest dostępny odpowiedni europejski program certyfikacji cyberbezpieczeństwa.

Artykuł 22

Normalizacja

1. Aby wspierać spójne wdrażanie art. 18 ust. 1 i 2, państwa członkowskie, nie narzucając ani nie faworyzując wykorzystywania określonego rodzaju technologii, zachęcają do stosowania europejskich lub uznanych międzynarodowo norm i specyfikacji istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych.
2. ENISA, we współpracy z państwami członkowskimi, opracowuje porady i wytyczne dotyczące kwestii technicznych, które powinny zostać wzięte pod uwagę w odniesieniu do ust. 1, a także dotyczące już istniejących norm, w tym krajowych norm państw członkowskich, które pozwoliłyby na uwzględnienie tych obszarów.

Artykuł 23

Bazy danych zawierające nazwy domen i dane rejestracyjne

1. W celu wzmocnienia bezpieczeństwa, stabilności i odporności DNS państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD z należytą starannością gromadziły i zachowywały w specjalnej bazie danych dokładne i kompletne dane dotyczące rejestracji nazw domen, z zastrzeżeniem unijnych przepisów o ochronie danych w odniesieniu do danych będących danymi osobowymi.
2. Państwa członkowskie zapewniają, aby w bazach danych zawierających dane dotyczące rejestracji nazw domen, o których mowa w ust. 1, znajdowały się informacje niezbędne do zidentyfikowania posiadaczy nazw domen i punktów kontaktowych zarządzających nazwami domen w ramach TLD i do skontaktowania się z nimi.

3. Państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD wdrożyły polityki i procedury służące zapewnieniu, by bazy danych zawierały dokładne i kompletne dane. Państwa członkowskie zapewniają, aby takie polityki i procedury podawano do wiadomości publicznej.

4. Państwa członkowskie zapewniają, aby po rejestracji nazwy domeny rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD bez zbędnej zwłoki publikowały dane dotyczące rejestracji domeny, które nie są danymi osobowymi.

5. Państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD, na zgodny z prawem i należycie uzasadniony wniosek złożony przez wnioskodawców ubiegających się o prawnie uzasadniony dostęp, udzielały dostępu do konkretnych danych dotyczących rejestracji nazw domen zgodnie z unijnym prawem ochrony danych. Państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD bez zbędnej zwłoki udzielały odpowiedzi na wszystkie wnioski o dostęp. Państwa członkowskie zapewniają, aby polityki i procedury regulujące ujawnianie takich danych podawano do wiadomości publicznej.

Sekcja II

Jurysdykcja i rejestracja

Artykuł 24

Jurysdykcja i terytorialność

1. Uznaje się, że dostawcy usług DNS, rejestry nazw TLD, dostawcy usług w chmurze, dostawcy usług ośrodka przetwarzania danych oraz dostawcy sieci dostarczania treści, o których mowa w załączniku I pkt 8, a także dostawcy usług cyfrowych, o których mowa w załączniku II pkt 6, podlegają jurysdykcji państwa członkowskiego, w którym znajduje się ich główna jednostka organizacyjna w Unii.

2. Do celów niniejszej dyrektywy uznaje się, że podmioty, o których mowa w ust. 1, posiadają swoją główną jednostkę organizacyjną w Unii w tym państwie członkowskim, w którym podejmowane są decyzje związane ze środkami zarządzania ryzykiem w cyberprzestrzeni. Jeżeli takich decyzji nie podejmuje się w jednostce organizacyjnej położonej w Unii, uznaje się, że główna jednostka organizacyjna znajduje się w państwie członkowskim, w którym podmioty mają jednostkę organizacyjną o największej liczbie pracowników w Unii.

3. W przypadku gdy podmiot, o którym mowa w ust. 1, nie posiada jednostki organizacyjnej w Unii, ale oferuje usługi w Unii, wyznacza przedstawiciela w Unii. Przedstawiciel musi posiadać jednostkę organizacyjną w jednym z tych państw członkowskich, w których oferowane są usługi. Uznaje się, że podmiot taki podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel posiada jednostkę organizacyjną. W przypadku braku przedstawiciela w Unii wyznaczonego na podstawie niniejszego artykułu każde państwo członkowskie, w którym dany podmiot świadczy usługi, może podjąć wobec tego podmiotu działania prawne w związku z niewykonaniem obowiązków wynikających z niniejszej dyrektywy.

4. Wyznaczenie przedstawiciela przez podmiot, o którym mowa w ust. 1, pozostaje bez uszczerbku dla działań prawnych, które mogłyby zostać podjęte przeciwko samemu podmiotowi.

Artykuł 25

Rejestr podmiotów niezbędnych i istotnych

1. ENISA tworzy i prowadzi rejestr podmiotów niezbędnych i istotnych, o których mowa w art. 24 ust. 1. Do dnia [12 miesięcy po wejściu w życie niniejszej dyrektywy] r. podmioty te przekazują ENISA następujące informacje:

   a) nazwę podmiotu;

   b) adres jego głównej jednostki organizacyjnej oraz jego innych prawnych jednostek organizacyjnych w Unii lub – jeżeli nie posiada on jednostki organizacyjnej w Unii – jego przedstawiciela wyznaczonego zgodnie z art. 24 ust. 3;

   c) aktualne dane kontaktowe, w tym adresy e-mail i numery telefonów podmiotów.

2. Podmioty, o których mowa w ust. 1, powiadamiają ENISA o wszelkich zmianach danych, które przekazały na podstawie ust. 1, niezwłocznie, a w każdym razie w terminie trzech miesięcy od dnia, w którym nastąpiła zmiana.

3. Po otrzymaniu informacji na podstawie ust. 1 ENISA przekazuje je pojedynczym punktom kontaktowym zgodnie ze wskazaną lokalizacją głównej jednostki organizacyjnej każdego podmiotu lub – jeżeli nie posiada on jednostki organizacyjnej w Unii – jego wyznaczonego przedstawiciela. W przypadku gdy podmiot, o którym mowa w ust. 1, oprócz głównej jednostki organizacyjnej w Unii posiada dodatkowe jednostki organizacyjne w innych państwach członkowskich, ENISA przekazuje informacje również pojedynczym punktom kontaktowym tych państw członkowskich.

4. Jeżeli podmiot nie zarejestruje działalności lub nie przekaże stosownych informacji w terminie przewidzianym w ust. 1, każde państwo członkowskie, w którym podmiot ten świadczy usługi, jest właściwe, aby zapewnić przestrzeganie przez ten podmiot obowiązków określonych w niniejszej dyrektywie.

ROZDZIAŁ V

Wymiana informacji

Artykuł 26

Mechanizmy wymiany informacji na temat cyberbezpieczeństwa

1. Nie naruszając przepisów rozporządzenia (UE) 2016/679, państwa członkowskie zapewniają, aby podmioty niezbędne i istotne mogły wymieniać się odpowiednimi informacjami na temat cyberbezpieczeństwa, w tym informacjami dotyczącymi cyberzagrożeń, podatności, oznak naruszenia integralności systemu, taktyk, technik i procedur, alarmów dotyczących cyberbezpieczeństwa i narzędzi konfiguracji, jeżeli wymiana takich informacji:

a) ma na celu zapobieganie incydentom, ich wykrywanie, reagowanie na nie lub łagodzenie ich skutków;

b) zwiększa poziom cyberbezpieczeństwa, w szczególności poprzez podnoszenie świadomości w odniesieniu do cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się tych cyberzagrożeń, wspieranie różnorodnego potencjału obronnego, eliminowanie i ujawnianie podatności, techniki wykrywania zagrożeń, strategie ich minimalizowania lub etapy reagowania i przywracania gotowości do pracy.

2. Państwa członkowskie zapewniają, aby wymiana informacji odbywała się w ramach zaufanych społeczności podmiotów niezbędnych i istotnych. Wymianę taką prowadzi się za pośrednictwem mechanizmów wymiany informacji ze względu na potencjalnie poufny charakter wymienianych informacji i zgodnie z przepisami prawa Unii, o których mowa w ust. 1.

3. Państwa członkowskie ustanawiają przepisy określające procedurę, elementy operacyjne (w tym korzystanie ze specjalnych platform ICT), treść i warunki funkcjonowania mechanizmów wymiany informacji, o których mowa w ust. 2. Przepisy takie określają również szczegóły zaangażowania organów publicznych we wspomniane mechanizmy, a także elementy operacyjne, w tym wykorzystanie specjalnych platform informatycznych. Państwa członkowskie oferują wsparcie w stosowaniu takich mechanizmów zgodnie ze swoją polityką, o której mowa w art. 5 ust. 2 lit. g).

4. Podmioty niezbędne i istotne powiadamiają właściwe organy o swoim uczestnictwie w mechanizmach wymiany informacji, o których mowa w ust. 2, po przystąpieniu do tych mechanizmów lub, w stosownych przypadkach, o wycofaniu się z takich mechanizmów, gdy wycofanie stanie się skuteczne.

5. Zgodnie z prawem Unii ENISA pomaga w ustanowieniu mechanizmów wymiany informacji na temat cyberbezpieczeństwa, o których mowa w ust. 2, zapewniając najlepsze praktyki i wytyczne.

Artykuł 27

Dobrowolne zgłaszanie stosownych informacji

Nie naruszając przepisów art. 3, państwa członkowskie zapewniają, aby podmioty nieobjęte zakresem niniejszej dyrektywy mogły na zasadzie dobrowolności dokonywać zgłoszeń znaczących incydentów, cyberzagrożeń lub zdarzeń potencjalnie wypadkowych. Przy rozpatrywaniu zgłoszeń państwa członkowskie postępują zgodnie z procedurą określoną w art. 20. Państwa członkowskie mogą rozpatrywać zgłoszenia obowiązkowe priorytetowo względem zgłoszeń dobrowolnych. Zgłaszanie dobrowolne nie może skutkować nałożeniem na podmiot zgłaszający żadnych dodatkowych obowiązków, którym by nie podlegał, gdyby nie dokonał tego zgłoszenia.

ROZDZIAŁ VI

Nadzór i egzekwowanie przepisów

Artykuł 28

Ogólne aspekty dotyczące nadzoru i egzekwowania przepisów

1. Państwa członkowskie zapewniają, aby właściwe organy skutecznie monitorowały zgodność z niniejszą dyrektywą, w szczególności z obowiązkami przewidzianymi w art. 18 i 20, i stosowały środki niezbędne do zagwarantowania takiej zgodności.

2. Podejmując działania w odpowiedzi na incydenty, które doprowadziły do naruszeń danych osobowych, właściwy organ działa w ścisłej współpracy z organami ochrony danych.

Artykuł 29

Nadzór i egzekwowanie przepisów w stosunku do podmiotów niezbędnych

1. Państwa członkowskie zapewniają, aby środki nadzoru lub egzekwowania przepisów stosowane wobec podmiotów niezbędnych w odniesieniu do obowiązków określonych w niniejszej dyrektywie były skuteczne, proporcjonalne i odstraszające, biorąc pod uwagę okoliczności każdego pojedynczego przypadku.

2. Państwa członkowskie zapewniają, aby wykonując swoje zadania nadzorcze wobec podmiotów niezbędnych, właściwe organy były uprawnione do obejmowania tych podmiotów:

   a) kontrolami na miejscu i nadzorem zdalnym, w tym kontrolami wyrywkowymi;

   b) regularnymi audytami;

   c) ukierunkowanymi audytami bezpieczeństwa w oparciu o oceny ryzyka lub dostępne informacje dotyczące ryzyka;

   d) skanami bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów oceny ryzyka;

   e) żądaniami przekazania informacji niezbędnych do oceny środków w zakresie cyberbezpieczeństwa przyjętych przez podmiot, w tym dokumentów dotyczących polityki cyberbezpieczeństwa, jak również wypełnienia obowiązku powiadomienia ENISA na podstawie art. 25 ust. 1 i 2;

   f) żądaniami udzielenia dostępu do danych, dokumentów lub wszelkich informacji koniecznych do wykonywania ich zadań nadzorczych;

   g) żądaniami przedstawienia dowodów realizacji polityki cyberbezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora oraz potwierdzające je dowody.

3. Wykonując swoje uprawnienia zgodnie z ust. 2 lit. e)–g), właściwe organy podają cel żądania i określają żądane informacje.

4. Państwa członkowskie zapewniają, aby wykonując swoje uprawnienia w zakresie egzekwowania przepisów wobec podmiotów niezbędnych, właściwe organy były uprawnione do:

   a) wydawania ostrzeżeń dotyczących niewypełniania przez te podmioty obowiązków przewidzianych w niniejszej dyrektywie;

b) wydawania wiążących poleceń lub nakazu zobowiązujących te podmioty do wprowadzenia środków zaradczych w odniesieniu do stwierdzonych uchybień lub naruszeń obowiązków przewidzianych w niniejszej dyrektywie;

c) nakazania tym podmiotom, aby zaniechały postępowania, które stoi w sprzeczności z obowiązkami przewidzianymi w niniejszej dyrektywie, i powstrzymały się od jego powtarzania;

d) nakazania tym podmiotom, aby w określony sposób i w określonym terminie zapewniły zgodność swoich środków zarządzania ryzykiem lub obowiązków w zakresie zgłaszania incydentów z obowiązkami przewidzianymi w art. 18 i 20;

e) nakazania tym podmiotom, aby poinformowały osoby fizyczne lub prawne, na rzecz których świadczą usługi lub prowadzą działania, których potencjalnie dotyczy znaczące cyberzagrożenie, o wszelkich możliwych środkach ochronnych lub naprawczych, które mogą zastosować te osoby fizyczne lub prawne w odpowiedzi na takie zagrożenie;

f) nakazania tym podmiotom, aby w rozsądnym terminie wdrożyły zalecenia wydane w wyniku audytu bezpieczeństwa;

g) wyznaczenia urzędnika monitorującego – ze ściśle określonymi zadaniami na oznaczony okres – do nadzorowania wypełniania przez te podmioty obowiązków przewidzianych w art. 18 i 20;

h) nakazania tym podmiotom, aby w określony sposób podały do wiadomości publicznej informacje o aspektach niewypełnienia obowiązków przewidzianych w niniejszej dyrektywie;

i) wydania publicznego oświadczenia, w którym zostaną wskazane osoby fizyczne i prawne odpowiedzialne za naruszenie obowiązku przewidzianego w niniejszej dyrektywie oraz charakter tego naruszenia;

j) zastosowania lub zwrócenia się o zastosowanie przez właściwe organy lub sądy zgodnie z przepisami krajowymi administracyjnej kary pieniężnej na podstawie art. 31 oprócz lub zamiast środków, o których mowa w lit. a)–i) niniejszego ustępu, zależnie od okoliczności konkretnej sprawy.

5. Jeżeli działania z zakresu egzekwowania przepisów zastosowane na podstawie ust. 4 lit. a)–d) oraz f) okażą się nieskuteczne, państwa członkowskie zapewniają, aby właściwe organy były uprawnione do wyznaczenia terminu, w którym podmiot niezbędny jest zobowiązany podjąć niezbędne działania mające na celu usunięcie uchybień lub zapewnienie zgodności z wymogami określonymi przez te organy. W przypadku gdy wymagane działanie nie zostanie podjęte w wyznaczonym terminie, państwa członkowskie zapewniają, aby właściwe organy były uprawnione do:

a) zawieszenia lub zwrócenia się do organu, który dokonał certyfikacji lub udzielił zezwolenia, o zawieszenie certyfikacji lub zezwolenia w odniesieniu do części lub wszystkich usług świadczonych bądź części lub całości działalności prowadzonej przez podmiot niezbędny;

b) nałożenia lub zwrócenia się o nałożenie przez właściwe organy lub sądy zgodnie z przepisami krajowymi tymczasowego zakazu pełnienia funkcji zarządczych w takim podmiocie niezbędnym na każdą osobę wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela

prawnego w tym podmiocie oraz na każdą inną osobę fizyczną uznaną za odpowiedzialną za naruszenie.

Sankcje te stosuje się wyłącznie do czasu, aż podmiot podejmie niezbędne działania w celu usunięcia uchybień lub spełni wymogi właściwego organu, z których tytułu zastosowano takie sankcje.

6. Państwa członkowskie zapewniają, aby każda osoba fizyczna odpowiedzialna za podmiot niezbędny lub działająca w charakterze przedstawiciela tego podmiotu na podstawie uprawnienia do jego reprezentowania, podejmowania decyzji w jego imieniu lub sprawowania nad nim kontroli posiadała uprawnienia do zapewnienia wypełnienia przez ten podmiot obowiązków przewidzianych w niniejszej dyrektywie. Państwa członkowskie zapewniają, aby te osoby fizyczne mogły zostać pociągnięte do odpowiedzialności za niewywiązanie się z obowiązku zapewnienia przestrzegania obowiązków przewidzianych w niniejszej dyrektywie.

7. Podejmując którekolwiek z działań z zakresu egzekwowania przepisów lub stosując sankcje na podstawie ust. 4 i 5, właściwe organy przestrzegają prawa do obrony oraz biorą pod uwagę okoliczności każdego przypadku i należycie uwzględniają przynajmniej

   a) wagę naruszenia i znaczenie naruszonych przepisów. Naruszenia, które należy uznać za poważne: powtarzające się naruszenia, niedopełnienie obowiązku zgłoszenia lub usunięcia incydentów o istotnym skutku zakłócającym, nieusunięcie uchybień w następstwie wiążących poleceń właściwych organów, utrudnianie prowadzenia audytów lub działań monitorujących nakazanych przez właściwy organ w wyniku stwierdzenia naruszenia, dostarczanie nieprawdziwych lub rażąco niedokładnych informacji w odniesieniu do wymogów w zakresie zarządzania ryzykiem lub obowiązków w zakresie zgłaszania incydentów określonych w art. 18 i 20;

   b) czas trwania naruszenia, w tym element powtarzających się naruszeń;

   c) faktycznie wyrządzone szkody lub poniesione straty lub potencjalne szkody lub straty, które mogły powstać, o ile można je ustalić. Przy ocenie tego aspektu uwzględnia się między innymi faktyczne lub potencjalne straty finansowe lub gospodarcze, wpływ na inne usługi, liczbę użytkowników, których to dotyczy lub może dotyczyć;

   d) fakt, czy naruszenie ma charakter umyślny lub wynika z zaniedbania;

   e) środki zastosowane przez podmiot, aby zapobiec szkodom lub stratom lub je ograniczyć;

   f) stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji;

   g) stopień współpracy odpowiedzialnych osób fizycznych lub prawnych z właściwymi organami.

8. Właściwe organy przedstawiają szczegółowe uzasadnienie swoich decyzji z zakresu egzekwowania przepisów. Przed podjęciem takich decyzji właściwe organy powiadamiają zainteresowane podmioty o swoich wstępnych ustaleniach i wyznaczają im rozsądny termin na przedstawienie uwag.

9. Państwa członkowskie zapewniają, aby ich właściwe organy informowały odpowiednie właściwe organy zainteresowanego państwa członkowskiego

wyznaczone na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych], w przypadku gdy wykonują swoje uprawnienia w zakresie nadzoru i egzekwowania przepisów, które to uprawnienia mają na celu zapewnienie wypełniania obowiązków przewidzianych w niniejszej dyrektywie przez podmiot niezbędny uznany za podmiot krytyczny lub za podmiot równoważny z podmiotem krytycznym na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych]. Na wniosek właściwych organów na mocy dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych] właściwe organy mogą wykonywać swoje uprawnienia w zakresie nadzoru i egzekwowania przepisów względem podmiotu niezbędnego uznanego za podmiot krytyczny lub równoważny.

Artykuł 30

Nadzór i egzekwowanie przepisów w stosunku do podmiotów istotnych

1. W przypadku otrzymania dowodu lub wskazania, że podmiot istotny nie spełnia obowiązków przewidzianych w niniejszej dyrektywie, w szczególności w art. 18 i 20, państwa członkowskie zapewniają, aby właściwe organy podejmowały działania, w razie konieczności, w drodze środków nadzoru *ex post*.

2. Państwa członkowskie zapewniają, aby wykonując swoje zadania nadzorcze wobec podmiotów istotnych, właściwe organy były uprawnione do obejmowania tych podmiotów:

   a) kontrolami na miejscu i nadzorowi zdalnemu *ex post*;

   b) ukierunkowanymi audytami bezpieczeństwa w oparciu o oceny ryzyka lub dostępne informacje dotyczące ryzyka;

   c) skanami bezpieczeństwa na podstawie obiektywnych, sprawiedliwych i przejrzystych kryteriów oceny ryzyka;

   d) żądaniami przekazania informacji niezbędnych do przeprowadzenia oceny *ex post* dotyczącej środków w zakresie cyberbezpieczeństwa, w tym dokumentów dotyczących polityki cyberbezpieczeństwa, jak również wypełnienia obowiązku powiadomienia ENISA na podstawie art. 25 ust. 1 i 2;

   e) żądaniami udzielenia dostępu do danych, dokumentów lub informacji koniecznych do wykonywania zadań nadzorczych.

3. Wykonując swoje uprawnienia zgodnie z ust. 2 lit. d) lub e), właściwe organy podają cel żądania i określają żądane informacje.

4. Państwa członkowskie zapewniają, aby wykonując swoje uprawnienia w zakresie egzekwowania przepisów wobec podmiotów istotnych, właściwe organy były uprawnione do:

   a) wydawania ostrzeżeń dotyczących niewypełniania przez te podmioty obowiązków przewidzianych w niniejszej dyrektywie;

   b) wydawania wiążących poleceń lub nakazu zobowiązujących te podmioty do wprowadzenia środków zaradczych w odniesieniu do stwierdzonych uchybień lub naruszenia obowiązków przewidzianych w niniejszej dyrektywie;

c) nakazania tym podmiotom, aby zaniechały postępowania, które stoi w sprzeczności z obowiązkami przewidzianymi w niniejszej dyrektywie, i powstrzymały się od jego powtarzania;

d) nakazania tym podmiotom, aby w określony sposób i w określonym terminie zapewniły zgodność swoich środków zarządzania ryzykiem lub obowiązków w zakresie zgłaszania incydentów z obowiązkami przewidzianymi w art. 18 i 20;

e) nakazania tym podmiotom, aby poinformowały osoby fizyczne lub prawne, na rzecz których świadczą usługi lub prowadzą działania, których potencjalnie dotyczy znaczące cyberzagrożenie, o wszelkich możliwych środkach ochronnych lub naprawczych, które mogą zastosować te osoby fizyczne lub prawne w odpowiedzi na takie zagrożenie;

f) nakazania tym podmiotom, aby w rozsądnym terminie wdrożyły zalecenia wydane w wyniku audytu bezpieczeństwa;

g) nakazania tym podmiotom, aby w określony sposób podały do wiadomości publicznej informacje o aspektach niewypełnienia swoich obowiązków przewidzianych w niniejszej dyrektywie;

h) wydania publicznego oświadczenia, w którym zostaną wskazane osoby fizyczne i prawne odpowiedzialne za naruszenie obowiązku przewidzianego w niniejszej dyrektywie oraz charakter tego naruszenia;

i) zastosowania lub zwrócenia się o zastosowanie przez właściwe organy lub sądy zgodnie z przepisami krajowymi administracyjnej kary pieniężnej na podstawie art. 31 oprócz lub zamiast środków, o których mowa w lit. a)–h) niniejszego ustępu, zależnie od okoliczności konkretnej sprawy.

5. Art. 29 ust. 6–8 stosuje się również do środków nadzoru i egzekwowania przepisów przewidzianych w niniejszym artykule w odniesieniu do podmiotów istotnych wymienionych w załączniku II.

Artykuł 31

Ogólne warunki nakładania administracyjnych kar pieniężnych na podmioty niezbędne i istotne

1. Państwa członkowskie zapewniają, aby administracyjne kary pieniężne nakładane na podmioty niezbędne i istotne na podstawie niniejszego artykułu za naruszenia obowiązków przewidzianych w niniejszej dyrektywie były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

2. Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków, o których mowa w art. 29 ust. 4 lit. a)–i), art. 29 ust. 5 oraz art. 30 ust. 4 lit. a)–h).

3. Przy podejmowaniu decyzji o tym, czy nałożyć administracyjną karę pieniężną, oraz przy ustalaniu jej wysokości w każdym indywidualnym przypadku należycie uwzględnia się co najmniej elementy przewidziane w art. 29 ust. 7.

4. Państwa członkowskie zapewniają, aby naruszenia obowiązków przewidzianych w art. 18 lub 20 podlegały na mocy ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej 10 000 000 EUR lub 2 %

całkowitego rocznego światowego obrotu przedsiębiorstwa, do którego należy podmiot niezbędny lub istotny, z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

5. Państwa członkowskie mogą przewidzieć uprawnienie do nakładania okresowych kar pieniężnych w celu przymuszenia podmiotu niezbędnego lub istotnego do zaprzestania naruszenia zgodnie z wcześniejszą decyzją właściwego organu.

6. Bez uszczerbku dla uprawnień właściwych organów na mocy art. 29 i 30 każde państwo członkowskie może określić przepisy regulujące, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na podmioty administracji publicznej, o których mowa w art. 4 pkt 23, podlegające obowiązkom przewidzianym w niniejszej dyrektywie.

Artykuł 32

Naruszenia pociągające za sobą naruszenie ochrony danych osobowych

1. Jeżeli właściwe organy mają przesłanki wskazujące na to, że naruszenie przez podmiot niezbędny lub istotny obowiązków przewidzianych w art. 18 i 20 pociąga za sobą naruszenie ochrony danych osobowych, zdefiniowane w art. 4 pkt 12 rozporządzenia (UE) 2016/679, które podlega zgłoszeniu na podstawie art. 33 tego rozporządzenia, informują one o tym w rozsądnym terminie organy nadzorcze właściwe na mocy art. 55 i 56 tego rozporządzenia.

2. W przypadku gdy organy nadzorcze właściwe na mocy art. 55 i 56 rozporządzenia (UE) 2016/679 podejmą decyzję o wykonaniu swoich uprawnień na podstawie art. 58 ust. 2 lit. i) tego rozporządzenia i nałożą administracyjną karę pieniężną, właściwe organy nie nakładają administracyjnej kary pieniężnej za to samo naruszenie na podstawie art. 31 niniejszej dyrektywy. Właściwe organy mogą jednak zastosować działania z zakresu egzekwowania przepisów lub skorzystać z uprawnień do nakładania sankcji, które to działania i uprawnienia przewidziano w art. 29 ust. 4 lit. a)–i), art. 29 ust. 5 i art. 30 ust. 4 lit. a)–h) niniejszej dyrektywy.

3. Jeżeli organ nadzorczy właściwy na mocy rozporządzenia (UE) 2016/679 jest ustanowiony w innym państwie członkowskim niż właściwy organ, właściwy organ może poinformować organ nadzorczy ustanowiony w tym samym państwie członkowskim.

Artykuł 33

Sankcje

1. Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszeń przepisów krajowych przyjętych na podstawie niniejszej dyrektywy i wprowadzają wszelkie niezbędne środki w celu zapewnienia ich wykonywania. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające.

2. Państwa członkowskie najpóźniej w ciągu [dwóch] lat od wejścia w życie niniejszej dyrektywy powiadamiają Komisję o tych przepisach i środkach, a następnie niezwłocznie powiadamiają ją o wszelkich zmianach mających na nie wpływ.

Artykuł 34

Wzajemna pomoc

1. Jeżeli podmiot niezbędny lub istotny świadczy usługi w więcej niż jednym państwie członkowskim lub posiada główną jednostkę organizacyjną lub przedstawiciela w jednym państwie członkowskim, ale jego sieć i systemy informatyczne są zlokalizowane w co najmniej jednym innym państwie członkowskim, właściwy organ państwa członkowskiego głównej jednostki organizacyjnej lub innej jednostki organizacyjnej, lub przedstawiciela oraz właściwe organy tych innych państw członkowskich współpracują ze sobą i udzielają sobie wzajemnie pomocy, odpowiednio do potrzeb. Współpraca ta obejmuje co najmniej następujące kwestie:

   a) właściwe organy stosujące środki nadzoru lub egzekwowania przepisów w państwie członkowskim informują – za pośrednictwem pojedynczego punktu kontaktowego – właściwe organy w tych innych zainteresowanych państwach członkowskich o zastosowanych środkach nadzoru i egzekwowania przepisów oraz związanych z nimi działaniach następczych i konsultują się z tymi właściwymi organami w tej sprawie, zgodnie z art. 29 i 30;

   b) właściwy organ może zwrócić się do innego właściwego organu o zastosowanie środków nadzoru lub egzekwowania przepisów, o których to środkach mowa w art. 29 i 30;

   c) właściwy organ, po otrzymaniu uzasadnionego wniosku od innego właściwego organu, udziela temu innemu właściwemu organowi pomocy, tak aby środki nadzoru lub egzekwowania przepisów, o których to środkach mowa w art. 29 i 30, mogły być wdrażane w sposób skuteczny, wydajny i spójny. Taka wzajemna pomoc może obejmować wnioski o udzielenie informacji i środki nadzoru, w tym wnioski o przeprowadzenie kontroli na miejscu lub nadzoru zdalnego, lub ukierunkowanych audytów bezpieczeństwa. Właściwy organ, do którego skierowany jest wniosek o pomoc, nie może odmówić wykonania tego wniosku, chyba że po wymianie informacji z innymi zainteresowanymi organami, ENISA i Komisją zostanie ustalone, że organ ten nie jest organem właściwym do udzielenia wnioskowanej pomocy albo że pomoc, której dotyczy wniosek, nie jest proporcjonalna do zadań nadzorczych realizowanych przez właściwy organ zgodnie z art. 29 lub 30.

2. W stosownych przypadkach i za obopólnym porozumieniem właściwe organy z poszczególnych państw członkowskich mogą przeprowadzać wspólne działania nadzorcze, o których mowa w art. 29 i 30.

ROZDZIAŁ VII

Przepisy przejściowe i końcowe

Artykuł 35

Przegląd

Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. W sprawozdaniu ocenia się w szczególności znaczenie sektorów, podsektorów, wielkości i rodzaju podmiotów, o których mowa w załącznikach I i II, dla funkcjonowania gospodarki i społeczeństwa w kontekście cyberbezpieczeństwa. W tym celu oraz z myślą o dalszym rozwijaniu współpracy strategicznej i operacyjnej Komisja bierze pod uwagę sprawozdania Grupy Współpracy i sieci CSIRT na temat doświadczeń zdobytych na poziomie strategicznym i operacyjnym. Pierwsze sprawozdanie przedkłada się do dnia [54 miesiące od daty wejścia w życie niniejszej dyrektywy] r.

Artykuł 36

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. 18 ust. 6 i art. 21 ust. 2, powierza się Komisji na okres pięciu lat od dnia [...] r.
3. Przekazanie uprawnień, o którym mowa w art. 18 ust. 6 i art. 21 ust. 2, 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. 18 ust. 6 i art. 21 ust. 2 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 37

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.

3. W przypadku gdy opinia komitetu ma zostać uzyskana w drodze procedury pisemnej, procedura ta kończy się bez osiągnięcia rezultatu, gdy – przed upływem terminu na wydanie opinii – zdecyduje o tym przewodniczący komitetu lub wniesie o to członek komitetu.

Artykuł 38

Transpozycja

1. Państwa członkowskie przyjmują i publikują, najpóźniej do dnia [18 miesięcy od daty wejścia w życie niniejszej dyrektywy] r., przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają o nich Komisję. Państwa członkowskie stosują te przepisy od dnia [jeden dzień od daty, o której mowa w akapicie pierwszym] r.

2. 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.

Artykuł 39

Zmiana rozporządzenia (UE) nr 910/2014

Uchyla się art. 19 rozporządzenia (UE) nr 910/2014.

Artykuł 40

Zmiana dyrektywy (UE) 2018/1972

Uchyla się art. 40 i 41 dyrektywy (UE) 2018/1972.

Artykuł 41

Uchylenie

Dyrektywa (UE) 2016/1148 traci moc ze skutkiem od dnia [...] [dzień, w którym upływa termin transpozycji dyrektywy] r.

Odesłania do dyrektywy (UE) 2016/1148 uznaje się za odesłania do niniejszej dyrektywy i odczytuje zgodnie z tabelą korelacji zawartą w załączniku III.

Artykuł 42

Wejście w życie

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

Artykuł 43

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

Spis treści

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, uchylającej dyrektywę (UE) 2016/1148

1.2. Obszary polityki, których dotyczy wniosek/inicjatywa *(klaster programów)*

Sieci komunikacyjne, treści i technologie

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. Uzasadnienie wniosku/inicjatywy

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

Celem zmiany jest podniesienie poziomu cyberodporności szeroko określonego zbioru przedsiębiorstw prowadzących działalność w Unii Europejskiej we wszystkich odpowiednich sektorach, ograniczenie zróżnicowania odporności na całym rynku wewnętrznym w sektorach już objętych dyrektywą oraz podniesienie poziomu wspólnej orientacji sytuacyjnej i zbiorowej zdolności do przygotowania się i reagowania.

1.4.2. 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.

Nie można osiągnąć skutecznej odporności pod względem cyberbezpieczeństwa w całej Unii, jeżeli podchodzi się do niej w zróżnicowany sposób za pomocą rozwiązań krajowych lub regionalnych. Dyrektywa w sprawie bezpieczeństwa sieci i informacji miała usunąć to niedociągnięcie przez ustanowienie ram dotyczących bezpieczeństwa sieci i systemów informatycznych na szczeblu krajowym i unijnym. Pierwszy przegląd okresowy dyrektywy w sprawie bezpieczeństwa sieci i informacji ujawnił jednak szereg tkwiących w niej wad, które ostatecznie doprowadziły do znacznych rozbieżności między państwami członkowskimi pod względem zdolności, planowania i poziomu ochrony wpływających jednocześnie na równe warunki działania dla podobnych przedsiębiorstw na rynku wewnętrznym.

Interwencję UE wykraczającą poza obecne środki określone w dyrektywie w sprawie bezpieczeństwa sieci i informacji uzasadnia przede wszystkim: (i) transgraniczny

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

charakter problemu; (ii) potencjał działań UE mających na celu usprawnienie i ułatwienie wprowadzania skutecznych polityk krajowych; (iii) wpływ uzgodnionych i opierających się na współpracy działań z zakresu polityki w dziedzinie bezpieczeństwa sieci i systemów informatycznych na skuteczną ochronę danych osobowych i prywatności.

Wytyczone cele mogą zostać lepiej osiągnięte poprzez działania na poziomie UE niż poprzez działania podejmowane tylko na poziomie państw członkowskich.

1.4.3. Główne wnioski wyciągnięte z podobnych działań

Dyrektywa w sprawie bezpieczeństwa sieci i informacji jest pierwszym horyzontalnym instrumentem rynku wewnętrznego ukierunkowanym na poprawę odporności sieci i systemów w Unii na ryzyka w cyberprzestrzeni. Przyczyniła się już ona w znacznym stopniu do podniesienia wspólnego poziomu cyberbezpieczeństwa wśród państw członkowskich. Przegląd funkcjonowania i wdrażania dyrektywy ujawnił jednak szereg niedociągnięć, którymi należy się zająć w zmienionym akcie prawnym obok konieczności uwzględnienia nabierającej tempa cyfryzacji oraz potrzeby reagowania bardziej na bieżąco.

1.4.4. Spójność z innymi właściwymi instrumentami oraz możliwa synergia

Nowy wniosek jest w pełni spójny i zgodny z innymi powiązanymi inicjatywami, takimi jak wniosek dotyczący rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego („DORA”) oraz wniosek dotyczący dyrektywy w sprawie odporności krytycznych operatorów usług kluczowych. Jest on również spójny z Europejskim kodeksem łączności elektronicznej, ogólnym rozporządzeniem o ochronie danych i rozporządzeniem eIDAS.

Wniosek stanowi zasadniczą część strategii UE w zakresie unii bezpieczeństwa.

1.5. Okres trwania działania i jego wpływ finansowy

☐ **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 2022 r. do 2025 r.,

– po którym następuje faza operacyjna.

1.6. 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;

– X☐ 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

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), której udzielono nowego stałego mandatu na mocy aktu o cyberbezpieczeństwie, pomogłaby państwom członkowskim i Komisji we wdrażaniu zmienionej dyrektywy w sprawie bezpieczeństwa sieci i informacji.

[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

W wyniku zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji od 2022/2023 r. ENISA będzie miała dodatkowe obszary działania. Chociaż te obszary działania wchodziłyby w zakres ogólnych zadań ENISA zgodnie z jej mandatem, będą się one wiązać z dodatkowym obciążeniem pracą Agencji. Ściślej rzecz biorąc, oprócz obecnych obszarów działania, zgodnie z wnioskiem Komisji dotyczącym zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji ENISA będzie zobowiązana uwzględnić wyraźnie w swoim programie prac m.in. następujące działania: (i) opracowanie i utrzymywanie europejskiego rejestru podatności (art. 6 ust. 2 wniosku), (ii) zapewnienie obsługi sekretariatu na potrzeby europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (CyCLONe) (art. 14 wniosku) oraz sporządzanie rocznego sprawozdania o stanie cyberbezpieczeństwa w Unii (art. 15 wniosku), (iii) wspieranie organizacji wzajemnych ocen między państwami członkowskimi (art. 16 wniosku), (iv) gromadzenie zagregowanych danych o incydentach od państw członkowskich i wydawanie wytycznych technicznych (art. 20 ust. 9 wniosku), (v) utworzenie i prowadzenie rejestru podmiotów świadczących usługi transgraniczne (art. 25 wniosku).

W związku z tym zostanie złożony wniosek o 5 dodatkowych EPC od 2022 r. z powiązanym budżetem wynoszącym około 0,61 mln EUR rocznie na sfinansowanie tych nowych stanowisk (zob. odrębna ocena skutków finansowych dotycząca agencji).

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Określić częstotliwość i warunki

Komisja będzie dokonywać okresowych przeglądów funkcjonowania niniejszej dyrektywy i będzie składać Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat, po raz pierwszy trzy lata po wejściu w życie dyrektywy. Komisja oceni również prawidłowość transpozycji dyrektywy przez państwa członkowskie.

2.2. System zarządzania i kontroli

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

Wdrażaniem dyrektywy będzie zarządzać dział DG CNECT odpowiedzialny za tę dziedzinę polityki.

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

Bardzo niskie ryzyko, ponieważ ekosystem określony w dyrektywie w sprawie bezpieczeństwa sieci i informacji już funkcjonuje.

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)

Nie dotyczy. Wykorzystanie wyłącznie budżetu administracyjnego („globalna koperta finansowa”).

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

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

Nie dotyczy. Wykorzystanie wyłącznie budżetu administracyjnego („globalna koperta finansowa”).

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Dział wieloletnich ram finansowych i proponowane nowe linie budżetowe po stronie wydatków

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer [Dział…7……...……]	Zróżn. / niezróżn.[42]	państw EFTA[43]	krajów kandydujących[44]	państw trzecich	w rozumieniu art. [21 ust. 2 lit. b)] rozporządzenia finansowego
	20 02 06 wydatki na zarządzanie 20 02 06	Niezróżn.	NIE	NIE	NIE	NIE

42 Środki zróżnicowane / środki niezróżnicowane

43 EFTA: Europejskie Stowarzyszenie Wolnego Handlu

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

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	**<…>**	[Dział……...……]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***po 2027 r.***	**OGÓŁEM**
Środki operacyjne (w podziale na linie budżetowe wymienione w pkt 3.1)	Środki na zobowiązania	(1)									
	Środki na płatności	(2)									
Środki administracyjne finansowane ze środków przydzielonych na program[45]	Środki na zobowiązania = środki na płatności	(3)									
OGÓŁEM środki przydzielone na program	Środki na zobowiązania	=1+3									
	Środki na płatności	=2+3									

Dział wieloletnich ram finansowych	7	„Wydatki administracyjne” Posiedzenia: posiedzenia plenarne Grupy Współpracy w zakresie bezpieczeństwa sieci i systemów informatycznych odbywają się zazwyczaj 4 razy w roku. Komisja pokrywa koszty cateringu i podróży przedstawicieli 27 państw członkowskich (po jednym przedstawicielu z każdego państwa członkowskiego). Koszty jednego

[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.

		posiedzenia mogą wynosić do 15 tys. EUR. Podróże służbowe: podróże służbowe wiążą się z monitorowaniem wdrażania dyrektywy w sprawie bezpieczeństwa sieci i informacji. Przykład: w ciągu jednego roku (maj 2019 r. – lipiec 2020 r.) mieliśmy zorganizować tzw. wizyty krajowe dotyczące bezpieczeństwa sieci i systemów informatycznych i odwiedzić wszystkie 27 państw członkowskich w celu omówienia wdrażania dyrektywy w sprawie bezpieczeństwa sieci i informacji w całej UE.

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

w mln EUR (do trzech miejsc po przecinku)

		2021	2022	2023	2024	2025	2026	2027	*po 2027 r.*	OGÓŁEM
Zasoby ludzkie		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Pozostałe wydatki administracyjne		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
OGÓŁEM środki na DZIAŁ 7 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

w mln EUR (do trzech miejsc po przecinku)

		2021	2022	2023	2024	2025	2026	2027	*po 2027 r.*	OGÓŁEM
OGÓŁEM środki z wszystkich DZIAŁÓW wieloletnich ram finansowych	Środki na zobowiązania									
	Środki na płatności									

3.2.2. Podsumowanie szacunkowego wpływu na środki administracyjne

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

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

w mln EUR (do trzech miejsc po przecinku)

Rok	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**OGÓŁEM**
DZIAŁ 7 wieloletnich ram finansowych								
Zasoby ludzkie	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Pozostałe wydatki administracyjne	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Suma cząstkowa DZIAŁU 7 wieloletnich ram finansowych	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**

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

OGÓŁEM	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

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.

3.2.2.1. Szacowane zapotrzebowanie na zasoby ludzkie

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

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

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy

Rok		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
•Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)								
W centrali i w biurach przedstawicielstw Komisji		6	6	6	6	6	6	6
W delegaturach								
Badania naukowe								
• Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC) – CA, LA, SNE, INT i JED [47] Dział 7								
Finansowanie z DZIAŁU 7 wieloletnich ram finansowych	- w centrali	3	3	3	3	3	3	3
	- w delegaturach							
Finansowanie ze środków przydzielonych na program [48]	- w centrali							
	- w delegaturach							
Badania naukowe								
Inne (określić)								
OGÓŁEM		**9**	**9**	**9**	**9**	**9**	**9**	**9**

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG 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	• Przygotowanie aktów delegowanych zgodnie z art. 18 ust. 6, art. 21 ust. 2, art. 36; • przygotowanie aktów wykonawczych zgodnie z art. 12 ust. 8, art. 18 ust. 5, art. 20 ust. 11; • zapewnienie obsługi sekretariatu na potrzeby Grupy Współpracy ds. bezpieczeństwa sieci i systemów informatycznych; • organizacja posiedzeń plenarnych i posiedzeń roboczych Grupy Współpracy ds. bezpieczeństwa sieci i systemów informatycznych; • koordynacja prac państw członkowskich nad różnymi dokumentami (wytycznymi, zestawami narzędzi itp.); • kontakty z innymi służbami Komisji, ENISA i organami krajowymi na potrzeby wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji; • analiza krajowych metod i najlepszych praktyk związanych z wdrażaniem dyrektywy w sprawie bezpieczeństwa sieci i informacji.

[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").

Personel zewnętrzny	Pomoc w realizacji powyższych zadań, jeżeli okaże się konieczna.

3.2.3. Udział osób trzecich w finansowaniu

Wniosek/inicjatywa:

– X☐ 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	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**OGÓŁEM**
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

3.3. Szacunkowy wpływ na dochody

– ☐X 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	Wpływ wniosku/inicjatywy[49]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
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).

[49] 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.

ZAŁĄCZNIK
do OCENY SKUTKÓW FINANSOWYCH REGULACJI

Tytuł wniosku/inicjatywy:

Wniosek dotyczący dyrektywy zmieniającej dyrektywę 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

……
……

1. LICZBA i KOSZT ZASOBÓW LUDZKICH UZNANYCH ZA NIEZBĘDNE

2. KOSZT POZOSTAŁYCH WYDATKÓW ADMINISTRACYJNYCH

3. METODY OBLICZANIA SZACUNKOWYCH KOSZTÓW

3.1 Zasoby ludzkie

3.2 Pozostałe wydatki administracyjne

*Niniejszy załącznik, **wypełniony przez wszystkie dyrekcje generalne/służby uczestniczące we wniosku/inicjatywie**, musi towarzyszyć ocenie skutków finansowych regulacji, kiedy zostaną uruchomione międzywydziałowe konsultacje.*

Tabele danych są wykorzystywane jako materiał wyjściowy dla tabel zawartych w ocenie skutków finansowych regulacji. Służą one wyłącznie do użytku wewnętrznego w Komisji.

1. Koszt zasobów ludzkich uznanych za niezbędne

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

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

w mln EUR (do trzech miejsc po przecinku)

DZIAŁ 7 wieloletnich ram finansowych		**2021**		**2022**		**2023**		**2024**		**2025**		**2026**		**2027**		**OGÓŁEM**	
		EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)																	
W centrali i w biurach przedstawicielstw Komisji	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
w delegaturach Unii	AD																
	AST																
• Personel zewnętrzny [50] 0,24																	
Globalna koperta finansowa	CA	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	SNE																
	INT																
w delegaturach Unii	CA																
	LA																
	SNE																

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

	INT																
	JPD																
Inna linia budżetowa (*określić*)																	
Suma cząstkowa DZIAŁU 7 wieloletnich ram finansowych		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG 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.

Poza DZIAŁEM 7 wieloletnich ram finansowych			2021		2022		2023		2024		2025		2025		2025		OGÓŁEM	
			EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki	EPC	Środki
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)																		
Badania naukowe		AD																
		AST																
• Personel zewnętrzny[51]																		
Personel zewnętrzny w ramach środków operacyjnych (dawne linie „BA").	- w centrali	CA																
		SNE																
		INT																
	– w delegaturach Unii	CA																
		LA																
		SNE																
		INT																
		JPD																
Badania naukowe		CA																
		SNE																
		INT																
Inna linia budżetowa (*określić*)																		

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

Suma cząstkowa – poza DZIAŁEM 7 wieloletnich ram finansowych																	

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG 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.

Szacunkowy wpływ na zasoby ludzkie ENISA

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), której udzielono nowego stałego mandatu na mocy aktu o cyberbezpieczeństwie, pomogłaby państwom członkowskim i Komisji we wdrażaniu zmienionej dyrektywy w sprawie bezpieczeństwa sieci i informacji. W wyniku zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji od 2022/2023 r. ENISA będzie miała dodatkowe obszary działania. Chociaż te obszary działania wchodziłyby w zakres ogólnych zadań ENISA zgodnie z jej mandatem, będą się one wiązać z dodatkowym obciążeniem pracą Agencji. Ściślej rzecz biorąc, oprócz obecnych obszarów działania, zgodnie z wnioskiem Komisji dotyczącym zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji ENISA będzie zobowiązana uwzględnić wyraźnie w swoim programie prac m.in. następujące działania: (i) opracowanie i utrzymywanie europejskiego rejestru podatności (art. 6 ust. 2 wniosku), (ii) zapewnienie obsługi sekretariatu na potrzeby europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (CyCLONe) (art. 14 wniosku) oraz sporządzanie rocznego sprawozdania o stanie cyberbezpieczeństwa w Unii (art. 15 wniosku), (iii) wspieranie organizacji wzajemnych ocen między państwami członkowskimi (art. 16 wniosku), (iv) gromadzenie zagregowanych danych o incydentach od państw członkowskich i wydawanie wytycznych technicznych (art. 20 ust. 9 wniosku), (v) utworzenie i prowadzenie rejestru podmiotów świadczących usługi transgraniczne (art. 25 wniosku). W związku z tym zostanie złożony wniosek o 5 dodatkowych EPC od 2022 r. z powiązanym budżetem wynoszącym około 0,61 mln EUR rocznie na sfinansowanie tych nowych stanowisk (zob. odrębna ocena skutków finansowych dotycząca agencji).

W związku z tym zostanie złożony wniosek o 5 dodatkowych EPC od 2022 r. z powiązanym budżetem na sfinansowanie tych nowych stanowisk.

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

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

w mln EUR (do trzech miejsc po przecinku)

	Rok **N** [52] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)	**OGÓŁEM**

[52] 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.

Pracownicy zatrudnieni na czas określony (AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Pracownicy zatrudnieni na czas określony (AST)								
Personel kontraktowy	0,160	0,160	0,160	0,160	0,160	0,160		
Oddelegowani eksperci krajowi								**0,96**

OGÓŁEM	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Wymagania dotyczące pracowników (EPC):

	Rok **N** [53] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)	**OGÓŁEM**

Pracownicy zatrudnieni na czas określony (AD)	3	3	3	3	3	3		**18**
Pracownicy zatrudnieni na czas								

[53] 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.

określony (AST)								
Personel kontraktowy	2	2	2	2	2	2		**12**
Oddelegowani eksperci krajowi								

OGÓŁEM	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Koszt pozostałych wydatków administracyjnych

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

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

w mln EUR (do trzech miejsc po przecinku)

DZIAŁ 7 wieloletnich ram finansowych	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Ogółem**
W centrali:								
Wydatki na podróże służbowe i cele reprezentacyjne	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Koszty konferencji i spotkań	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**

Komitety[54]								
Analizy i konsultacje								
Systemy informacyjne i zarządzania								
Sprzęt i usługi w zakresie ICT[55]								
Inna linia budżetowa (*określić w stosownych przypadkach*)								
W delegaturach Unii								
Wydatki na podróże służbowe, konferencje i cele reprezentacyjne								
Dalsze szkolenie personelu								
Nabywanie, wynajem i wydatki powiązane								
Sprzęt, meble, materiały i usługi								
Suma cząstkowa DZIAŁU 7 wieloletnich ram finansowych	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

[54] Należy określić rodzaj komitetu i grupę, do której należy.

[55] ICT: technologie informacyjno-komunikacyjne: konieczność konsultacji z DG ds. Informatyki.

w mln EUR (do trzech miejsc po przecinku)

Poza DZIAŁEM 7 wieloletnich ram finansowych	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Ogółem**
Wydatki na pomoc techniczną i administracyjną (oprócz personelu zewnętrznego) ze środków operacyjnych (dawne linie „BA”)								
- w centrali								
– w delegaturach Unii								
Inne wydatki na zarządzanie w dziedzinie badań								
Inna linia budżetowa (*określić w stosownych przypadkach*)								
Suma cząstkowa – poza DZIAŁEM 7 wieloletnich ram finansowych								

OGÓŁEM DZIAŁ 7 i poza DZIAŁEM 7 wieloletnich ram finansowych	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Potrzeby w zakresie środków administracyjnych zostaną pokryte ze środków już przydzielonych na zarządzanie tym działaniem lub przesuniętych, 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.

3. Metody obliczania szacunkowych kosztów

3.1 Zasoby ludzkie

W niniejszej części określono metodę obliczania szacunkowych kosztów zasobów ludzkich uznanych za niezbędne (założenia co do obciążenia pracą, w tym konkretne stanowiska pracy (profile zawodowe wg Sysper 2), kategorie personelu i odpowiadające im średnie koszty)

DZIAŁ 7 wieloletnich ram finansowych
Uwaga: średnie koszty dla poszczególnych kategorii pracowników w centrali są dostępne na stronie BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Urzędnicy i pracownicy zatrudnieni na czas określony 6 pracowników w przeliczeniu na EPC (średni koszt 0,150) = 0,9 rocznie - Przygotowanie aktów delegowanych zgodnie z art. 18 ust. 6, art. 21 ust. 2, art. 36; - przygotowanie aktów wykonawczych zgodnie z art. 12 ust. 8, art. 18 ust. 5, art. 20 ust. 11; - zapewnienie obsługi sekretariatu na potrzeby Grupy Współpracy ds. bezpieczeństwa sieci i systemów informatycznych; - organizacja posiedzeń plenarnych i posiedzeń roboczych Grupy Współpracy ds. bezpieczeństwa sieci i systemów informatycznych; - koordynacja prac państw członkowskich nad różnymi dokumentami (wytycznymi, zestawami narzędzi itp.); - kontakty z innymi służbami Komisji, ENISA i organami krajowymi na potrzeby wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji; - analiza krajowych metod i najlepszych praktyk związanych z wdrażaniem dyrektywy w sprawie bezpieczeństwa sieci i informacji.
• Personel zewnętrzny 3 pracowników kontraktowych (średni koszt 0,08) = 0,24 rocznie - Pomoc w realizacji powyższych zadań, jeżeli okaże się konieczna.

Poza DZIAŁEM 7 wieloletnich ram finansowych
• Jedynie stanowiska finansowane z budżetu na badania naukowe
• Personel zewnętrzny

3.2 Pozostałe wydatki administracyjne

Należy wskazać metodę obliczeń zastosowaną w odniesieniu do poszczególnych linii budżetowych, a w szczególności założenia będące podstawą obliczeń (np. liczba posiedzeń rocznie, średnie koszty itp.)

DZIAŁ 7 wieloletnich ram finansowych

Posiedzenia: posiedzenia plenarne Grupy Współpracy ds. bezpieczeństwa sieci i systemów informatycznych odbywają się zazwyczaj 4 razy w roku. Komisja pokrywa koszty cateringu i podróży przedstawicieli 27 państw członkowskich (po jednym przedstawicielu z każdego państwa członkowskiego). Koszty jednego posiedzenia mogą wynieść do 15 tys. EUR, co daje 60 tys. EUR rocznie.

Podróże służbowe: podróże służbowe wiążą się z monitorowaniem wdrażania dyrektywy w sprawie bezpieczeństwa sieci i informacji. Przykład: w ciągu jednego roku (maj 2019 r. – lipiec 2020 r.) mieliśmy zorganizować tzw. wizyty krajowe dotyczące bezpieczeństwa sieci i systemów informatycznych i odwiedzić wszystkie 27 państw członkowskich w celu omówienia

wdrażania dyrektywy w sprawie bezpieczeństwa sieci i informacji w całej UE.

Poza DZIAŁEM 7 wieloletnich ram finansowych

ZAŁĄCZNIK 7

do
DECYZJI KOMISJI

w sprawie przepisów wewnętrznych dotyczących wykonania budżetu ogólnego Unii Europejskiej (sekcja dotycząca Komisji Europejskiej) na użytek służb Komisji

OCENA SKUTKÓW FINANSOWYCH REGULACJI – „AGENCJE”

Niniejsza ocena skutków finansowych regulacji obejmuje wniosek o zwiększenie liczby pracowników ENISA o 5 EPC od 2022 r. w celu realizacji dodatkowych działań związanych z wdrażaniem dyrektywy w sprawie bezpieczeństwa sieci i informacji. Działania te są już objęte mandatem ENISA.

Spis treści

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, uchylającej dyrektywę (UE) 2016/1148

1.2. Dziedziny polityki, których dotyczy wniosek/inicjatywa

Sieci komunikacyjne, treści i technologie

1.3. Wniosek dotyczy

☐ **nowego działania**

☐ **nowego działania, będącego następstwem projektu pilotażowego/działania przygotowawczego**[56]

☒ **przedłużenia bieżącego działania**

☐ **połączenia co najmniej jednego działania w inne lub nowe działanie**

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

Celem zmiany jest podniesienie poziomu cyberodporności szeroko określonego zbioru przedsiębiorstw prowadzących działalność w Unii Europejskiej we wszystkich odpowiednich sektorach, ograniczenie zróżnicowania odporności na całym rynku wewnętrznym w sektorach już objętych dyrektywą oraz podniesienie poziomu wspólnej orientacji sytuacyjnej i zbiorowej zdolności do przygotowania się i reagowania.

1.4.2. Cel(e) szczegółowy(e)

Aby rozwiązać problem niskiego poziomu cyberodporności przedsiębiorstw działających w Unii Europejskiej, celem szczegółowym jest zapewnienie, aby podmioty we wszystkich sektorach, które są zależne od sieci i systemów informatycznych i które świadczą kluczowe usługi na rzecz gospodarki i całego społeczeństwa, były zobowiązane do wprowadzania środków w zakresie cyberbezpieczeństwa i zgłaszania incydentów w celu podniesienia ogólnego poziomu cyberodporności na całym rynku wewnętrznym.

Aby rozwiązać problem zróżnicowanej odporności w poszczególnych państwach członkowskich i sektorach, celem szczegółowym jest zapewnienie, aby wszystkie podmioty o podobnej wielkości, które działają w sektorach objętych ramami prawnymi dotyczącymi bezpieczeństwa sieci i systemów informatycznych i które pełnią porównywalną rolę, podlegały temu samemu systemowi regulacyjnemu (wchodząc w jego zakres albo nie), bez względu na jurysdykcję w UE, którą są objęte.

W celu zapewnienia, aby wszystkie podmioty działające w sektorach objętych ramami prawnymi dotyczącymi bezpieczeństwa sieci i systemów informatycznych były zobowiązane do wypełniania tych samych obowiązków opartych na koncepcji zarządzania ryzykiem w odniesieniu do środków bezpieczeństwa i musiały zgłaszać wszelkie incydenty na

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

podstawie jednolitego zestawu kryteriów, cele szczegółowe obejmują zapewnienie skuteczniejszego egzekwowania przez właściwe organy przepisów określonych w instrumencie prawnym za pomocą dostosowanych środków nadzoru i egzekwowania oraz zapewnienie we wszystkich państwach członkowskich porównywalnego poziomu zasobów przydzielanych właściwym organom, umożliwiających im wykonywanie podstawowych zadań określonych w ramach prawnych dotyczących bezpieczeństwa sieci i systemów informatycznych.

Aby rozwiązać problem wspólnej orientacji sytuacyjnej i braku wspólnego reagowania na sytuacje kryzysowe, celem szczegółowym jest zapewnienie wymiany istotnych informacji między państwami członkowskimi przez nałożenie na właściwe organy wyraźnych obowiązków w zakresie wymiany informacji i współpracy w dziedzinie cyberzagrożeń i cyberincydentów oraz przez rozwijanie wspólnej unijnej zdolności operacyjnej w zakresie reagowania kryzysowego.

1.4.3. Oczekiwane wyniki i wpływ

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

Oczekuje się, że wniosek przyniesie znaczące korzyści: zgodnie z szacunkami może on doprowadzić do obniżenia kosztów cyberincydentów o 11,3 mld EUR. Za sprawą ram prawnych dotyczących bezpieczeństwa sieci i systemów informatycznych zakres sektorowy zostałby znacznie rozszerzony, a oprócz powyższych korzyści obciążenia, które mogą spowodować wymogi w zakresie bezpieczeństwa sieci i systemów informatycznych, zwłaszcza z perspektywy nadzoru, byłyby też zrównoważone zarówno w przypadku nowych podmiotów, jak i właściwych organów. Wynika to z faktu, że w nowych ramach prawnych dotyczących bezpieczeństwa sieci i systemów informatycznych ustanowiono by podejście dwupoziomowe, skupione na dużych i kluczowych podmiotach oraz przewidujące zróżnicowanie systemu nadzoru, które umożliwia wyłącznie nadzór *ex post* w odniesieniu do dużej liczby takich podmiotów, zwłaszcza tych uznanych za „istotne", ale nie „niezbędne".

Ogólnie rzecz biorąc, wniosek prowadziłby jednak również do skutecznych kompromisów i synergii, przy zapewnieniu największego potencjału spośród wszystkich przeanalizowanych wariantów, jeżeli chodzi o zapewnienie wysokiego i spójnego poziomu cyberodporności kluczowych podmiotów w całej Unii, co ostatecznie doprowadziłoby do oszczędności kosztów zarówno dla przedsiębiorstw, jak i dla społeczeństwa.

W wyniku wniosku powstałyby również pewne koszty przestrzegania i egzekwowania przepisów dla odpowiednich organów państw członkowskich (szacuje się, że niezbędne zasoby wzrosłyby ogółem o ok. 20–30 %). Nowe ramy prawne przyniosłyby jednak również znaczące korzyści dzięki lepszemu przeglądowi kluczowych przedsiębiorstw i interakcji z nimi, zacieśnieniu transgranicznej współpracy operacyjnej, a także mechanizmom wzajemnej pomocy i wzajemnej oceny. Doprowadziłoby to do ogólnego zwiększenia zdolności w zakresie cyberbezpieczeństwa we wszystkich państwach członkowskich.

Szacuje się, że przedsiębiorstwa, które byłyby objęte zakresem ram prawnych dotyczących bezpieczeństwa sieci i systemów informatycznych, musiałyby zwiększyć obecne wydatki na bezpieczeństwo ICT w pierwszych latach po wprowadzeniu nowych ram prawnych o maksymalnie 22 % (w przypadku przedsiębiorstw już objętych zakresem obowiązującej dyrektywy w sprawie bezpieczeństwa sieci i informacji byłoby to 12 %). Ten średni wzrost wydatków na bezpieczeństwo ICT doprowadziłby jednak do proporcjonalnych korzyści z takich inwestycji, w szczególności ze względu na znaczne obniżenie kosztów cyberincydentów (szacowanych na 118 mld EUR w okresie dziesięciu lat).

Małe przedsiębiorstwa i mikroprzedsiębiorstwa byłyby wyłączone z zakresu ram prawnych dotyczących bezpieczeństwa sieci i systemów informatycznych. W przypadku średnich przedsiębiorstw można oczekiwać, że w pierwszych latach po wprowadzeniu nowych ram prawnych dotyczących bezpieczeństwa sieci i systemów informatycznych poziom wydatków na bezpieczeństwo ICT się zwiększy. Zaostrzenie wymogów w zakresie bezpieczeństwa spoczywających na tych podmiotach stanowiłoby jednocześnie dla nich zachętę do rozwijania zdolności w zakresie cyberbezpieczeństwa i przyczyniłoby się do poprawy zarządzania przez nich ryzykiem ICT.

Przewiduje się skutki dla budżetów i administracji krajowych: zgodnie z oszacowaniami w perspektywie krótko- i średnioterminowej oczekiwany wzrost zasobów wyniesie około 20–30 %.

Nie przewiduje się innych znaczących negatywnych skutków. Oczekuje się, że wniosek doprowadzi do zwiększenia zdolności w zakresie cyberbezpieczeństwa, a w konsekwencji będzie miał bardziej znaczący wpływ na ograniczenie liczby i dotkliwości incydentów, w tym naruszeń ochrony danych. Może mieć on również pozytywny wpływ na zapewnienie wszystkim podmiotom objętym zakresem dyrektywy w sprawie bezpieczeństwa sieci i informacji równych warunków działania we wszystkich państwach członkowskich oraz na zmniejszenie asymetrii informacji w dziedzinie cyberbezpieczeństwa.

1.4.4. Wskaźniki dotyczące realizacji celów

Należy wskazać wskaźniki stosowane do monitorowania postępów i osiągnięć.

Ocena wskaźników będzie przeprowadzana przez Komisję przy wsparciu ENISA i Grupy Współpracy po upływie trzech lat od wejścia w życie nowego aktu prawnego w sprawie bezpieczeństwa sieci i informacji. Niektóre wskaźniki monitorowania, na podstawie których zostanie oceniony sukces zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji, są następujące:

• • Skuteczniejsze postępowanie w przypadku incydentu: Wprowadzając środki w zakresie cyberbezpieczeństwa, przedsiębiorstwa nie tylko poprawiają swoją zdolność do całkowitego zapobiegania niektórym incydentom, ale także zwiększają swoją zdolność reagowania na incydenty. Miarami sukcesu inicjatywy są zatem: (i) skrócenie średniego czasu potrzebnego do wykrycia incydentu, (ii) czas, jakiego organizacje potrzebują przeciętnie do przywrócenia normalnego działania po incydencie, oraz (iii) średni koszt szkód spowodowanych incydentem.

• Podniesienie świadomości kadry kierowniczej najwyższego szczebla przedsiębiorstw na temat ryzyka w cyberprzestrzeni: Ustanowienie w zmienionej dyrektywie w sprawie bezpieczeństwa sieci i informacji wymogu wprowadzenia środków przez przedsiębiorstwa przyczyniłoby się do podniesienia świadomości kadry kierowniczej wyższego szczebla na temat ryzyka w cyberprzestrzeni. Skutek ten można zmierzyć, badając, w jakim stopniu przedsiębiorstwa objęte zakresem dyrektywy w sprawie bezpieczeństwa sieci i informacji traktują priorytetowo cyberbezpieczeństwo w swoich wewnętrznych politykach i procesach, co można ustalić na podstawie dokumentacji wewnętrznej, odpowiednich skierowanych do pracowników programów szkoleń i działań mających na celu podnoszenie świadomości, a także w jakim stopniu traktują one priorytetowo inwestycje w technologie informacyjno-komunikacyjne związane z bezpieczeństwem. Ponadto kierownictwo wszystkich podmiotów niezbędnych i istotnych powinno dysponować wiedzą na temat przepisów określonych w dyrektywie w sprawie bezpieczeństwa sieci i informacji.

• Wyrównanie wydatków sektorowych: wydatki na bezpieczeństwo ICT różnią się znacznie w poszczególnych sektorach w UE. Nałożenie na przedsiębiorstwa w większej liczbie sektorów wymogu wprowadzenia środków powinno sprawić, że odchylenia od średnich wydatków na bezpieczeństwo ICT w poszczególnych sektorach, wyrażone jako odsetek całkowitych wydatków na ICT, zmniejszą się między sektorami i w poszczególnych państwach członkowskich.

• Wzmocnienie właściwych organów i zacieśnienie współpracy: W zmienionej dyrektywie w sprawie bezpieczeństwa sieci i informacji potencjalnie powierzono by właściwym organom dodatkowe zadania. Miałoby to wymierny wpływ na zasoby finansowe i ludzkie przeznaczone dla agencji ds. cyberbezpieczeństwa na szczeblu krajowym, a ponadto powinno pozytywnie wpłynąć na zdolność właściwych organów do aktywnej współpracy,

a tym samym na zwiększenie liczby przypadków, w których właściwe organy współpracują ze sobą, aby poradzić sobie z incydentami transgranicznymi lub prowadzić wspólne działania nadzorcze.

• Zwiększona wymiana informacji: Zmieniona dyrektywa w sprawie bezpieczeństwa sieci i informacji poprawiłaby również wymianę informacji między przedsiębiorstwami i z właściwymi organami. Jednym z celów zmiany mogłoby być zwiększenie liczby podmiotów uczestniczących w poszczególnych formach wymiany informacji.

1.5. Uzasadnienie wniosku/inicjatywy

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

Celem wniosku jest podniesienie poziomu cyberodporności kompleksowego zbioru przedsiębiorstw prowadzących działalność w Unii Europejskiej we wszystkich odpowiednich sektorach, ograniczenie zróżnicowania odporności na całym rynku wewnętrznym w sektorach już objętych dyrektywą oraz podniesienie poziomu wspólnej orientacji sytuacyjnej i zbiorowej zdolności do przygotowania się i reagowania. Będzie on opierać się na tym, co osiągnięto dzięki wdrożeniu dyrektywy (UE) 2016/1148 w ciągu ostatnich 4 lat.

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.

Nie można osiągnąć skutecznej odporności pod względem cyberbezpieczeństwa w całej Unii, jeżeli podchodzi się do niej w zróżnicowany sposób za pomocą rozwiązań krajowych lub regionalnych. Dyrektywa w sprawie bezpieczeństwa sieci i informacji miała usunąć to niedociągnięcie przez ustanowienie ram dotyczących bezpieczeństwa sieci i systemów informatycznych na szczeblu krajowym i unijnym. Pierwszy przegląd okresowy dyrektywy w sprawie bezpieczeństwa sieci i informacji ujawnił jednak szereg tkwiących w niej wad, które ostatecznie doprowadziły do znacznych rozbieżności między państwami członkowskimi pod względem zdolności, planowania i poziomu ochrony wpływających jednocześnie na równe warunki działania dla podobnych przedsiębiorstw na rynku wewnętrznym.

Interwencję UE wykraczającą poza obecne środki określone w dyrektywie w sprawie bezpieczeństwa sieci i informacji uzasadnia przede wszystkim: (i) transgraniczny charakter problemu; (ii) potencjał działań UE mających na celu usprawnienie i ułatwienie wprowadzania skutecznych polityk krajowych; (iii) wpływ uzgodnionych i opierających się na współpracy działań z zakresu polityki w dziedzinie bezpieczeństwa sieci i systemów informatycznych na skuteczną ochronę danych osobowych i prywatności.

Wytyczone cele mogą zostać lepiej osiągnięte poprzez działania na poziomie UE niż poprzez działania podejmowane tylko na poziomie państw członkowskich.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Dyrektywa w sprawie bezpieczeństwa sieci i informacji jest pierwszym horyzontalnym instrumentem rynku wewnętrznego ukierunkowanym na poprawę odporności sieci i systemów w Unii na ryzyka w cyberprzestrzeni. Od wejścia w życie w 2016 r. przyczyniła się już ona

w znacznym stopniu do podniesienia wspólnego poziomu cyberbezpieczeństwa wśród państw członkowskich. Przegląd funkcjonowania i wdrażania dyrektywy ujawnił jednak szereg niedociągnięć, którymi należy się zająć w zmienionym akcie prawnym obok konieczności uwzględnienia nabierającej tempa cyfryzacji oraz potrzeby reagowania bardziej na bieżąco.

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

Nowy wniosek jest w pełni spójny i zgodny z innymi powiązanymi inicjatywami, takimi jak wniosek dotyczący rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego („DORA") oraz wniosek dotyczący dyrektywy w sprawie odporności krytycznych operatorów usług kluczowych. Jest on również spójny z Europejskim kodeksem łączności elektronicznej, ogólnym rozporządzeniem o ochronie danych i rozporządzeniem eIDAS.

Wniosek stanowi zasadniczą część strategii UE w zakresie unii bezpieczeństwa.

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

Zarządzanie tymi zadaniami przez ENISA wymaga konkretnych profili zawodowych i dodatkowego obciążenia pracą, których nie można wdrożyć inaczej niż w drodze zwiększenia zasobów ludzkich.

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.

☒ **Nieograniczony czas trwania**

– Wprowadzenie w życie z okresem rozruchu od 2022 r. do 2025 r.,

– po którym następuje faza operacyjna.

1.7. Planowane tryby zarządzania[57]

☒ **Bezpośrednie zarządzanie** przez Komisję

przez

– ☐ agencje wykonawcze

☐ **Zarządzanie dzielone** z państwami członkowskimi

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

☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

☐ EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

☒ organom, o których mowa w art. 70 i 71;

☐ organom prawa publicznego;

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

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

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

Uwagi

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), której udzielono nowego stałego mandatu na mocy aktu o cyberbezpieczeństwie, pomogłaby państwom członkowskim i Komisji we wdrażaniu zmienionej dyrektywy w sprawie bezpieczeństwa sieci i informacji.

W wyniku zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji od 2022/2023 r. ENISA będzie miała dodatkowe obszary działania. Chociaż te obszary działania wchodziłyby w zakres ogólnych zadań ENISA zgodnie z jej mandatem, będą się one wiązać z dodatkowym obciążeniem pracą Agencji. Ściślej rzecz biorąc, oprócz obecnych obszarów działania, zgodnie z wnioskiem Komisji dotyczącym zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji ENISA będzie zobowiązana uwzględnić wyraźnie w swoim programie prac m.in. następujące działania: (i)

[57] 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

opracowanie i utrzymywanie europejskiego rejestru podatności (art. 6 ust. 2 wniosku), (ii) zapewnienie obsługi sekretariatu na potrzeby europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (CyCLONe) (art. 14 wniosku) oraz sporządzanie rocznego sprawozdania o stanie cyberbezpieczeństwa w Unii (art. 15 wniosku), (iii) wspieranie organizacji wzajemnych ocen między państwami członkowskimi (art. 16 wniosku), (iv) gromadzenie zagregowanych danych o incydentach od państw członkowskich i wydawanie wytycznych technicznych (art. 20 ust. 9 wniosku), (v) utworzenie i prowadzenie rejestru podmiotów świadczących usługi transgraniczne (art. 25 wniosku).

W związku z tym zostanie złożony wniosek o 5 dodatkowych EPC od 2022 r. z powiązanym budżetem wynoszącym około 0,61 mln EUR rocznie na sfinansowanie tych nowych stanowisk.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Określić częstotliwość i warunki

Komisja będzie dokonywać okresowych przeglądów funkcjonowania niniejszej dyrektywy i będzie składać Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat, po raz pierwszy trzy lata po wejściu w życie dyrektywy.

Komisja oceni również prawidłowość transpozycji dyrektywy przez państwa członkowskie.

Monitorowanie i sprawozdawczość w odniesieniu do wniosku będą zgodne z zasadami określonymi w stałym mandacie ENISA na mocy rozporządzenia (UE) 2019/881 (akt o cyberbezpieczeństwie).

Danych wykorzystywanych do planowanego monitorowania dostarczałyby głównie ENISA, Grupa Współpracy, sieć CSIRT i organy państw członkowskich. Oprócz danych zaczerpniętych ze sprawozdań (w tym corocznych sprawozdań z działalności) składanych przez ENISA, Grupę Współpracy i sieć CSIRT w razie potrzeby można byłoby korzystać z określonych narzędzi gromadzenia danych (na przykład ankiet kierowanych do organów krajowych, Eurobarometru oraz sprawozdań z kampanii „Miesiąc Cyberbezpieczeństwa" i z działań ogólnoeuropejskich).

2.2. System zarządzania i kontroli

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

Wdrażaniem dyrektywy będzie zarządzać dział DG CNECT odpowiedzialny za tę dziedzinę polityki.

Jeżeli chodzi o kierownictwo ENISA, art. 15 aktu o cyberbezpieczeństwie zawiera szczegółowy wykaz funkcji kontrolnych Zarządu ENISA.

Zgodnie z art. 31 aktu o cyberbezpieczeństwie za wykonanie budżetu ENISA odpowiedzialny jest Dyrektor Wykonawczy ENISA, a audytor wewnętrzny Komisji ma te same uprawnienia wobec ENISA co wobec departamentów Komisji. Zarząd ENISA wydaje opinię na temat końcowego sprawozdania finansowego ENISA.

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

Bardzo niskie ryzyko, ponieważ ekosystem określony w dyrektywie w sprawie bezpieczeństwa sieci i informacji już funkcjonuje i obejmuje już ENISA, która posiada stały mandat po wejściu w życie aktu o cyberbezpieczeństwie w 2019 r.

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)

Przewidziane we wniosku zwiększenie budżetu dotyczy tytułu 1 i jest przeznaczone na sfinansowanie wynagrodzeń. Oznacza to bardzo niskie ryzyko błędu na poziomie płatności.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

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

ENISA stosowałaby środki zapobiegania i ochrony, a mianowicie:

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

W celu zwalczania nadużyć finansowych, korupcji i innych działań bezprawnych stosuje się bez ograniczeń przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 25 maja 1999 r. dotyczącego dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF).

– Na mocy art. 33 aktu o cyberbezpieczeństwie do dnia 28 grudnia 2019 r. ENISA przystąpiła do Porozumienia międzyinstytucjonalnego z dnia 25 maja 1999 r. między Parlamentem Europejskim, Radą Unii Europejskiej i Komisją Wspólnot Europejskich dotyczącego dochodzeń wewnętrznych prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF). ENISA niezwłocznie wydaje odpowiednie przepisy, które mają zastosowanie do wszystkich pracowników Agencji.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

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

- Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych.

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn. / niezróżn.[58]	państw EFTA[59]	krajów kandydujących[60]	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
2	02 10 04	/niezróżn.	TAK	NIE	NIE	/NIE

- Nowe linie budżetowe, o których utworzenie się wnioskuje

Według działów wieloletnich ram finansowych i linii budżetowych.

[58] Środki zróżnicowane / środki niezróżnicowane

[59] EFTA: Europejskie Stowarzyszenie Wolnego Handlu

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

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn./niezróżn.	państw EFTA	krajów kandydujących	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
	[XX.YY.YY.YY]		TAK/ NIE	TAK/ NIE	TAK/ NIE	TAK/ NIE

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	Numer	[Dział...2. Jednolity rynek, innowacje i gospodarka cyfrowa……...……]

[Organ]: <…ENISA….>			Rok **N**[61] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6) **2026** **2027**			**OGÓŁEM**
Tytuł 1:	Środki na zobowiązania	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Środki na płatności	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Tytuł 2:	Środki na zobowiązania	(1a)								
	Środki na płatności	(2 a)								
Tytuł 3:	Środki na zobowiązania	(3 a)								
	Środki na płatności	(3 b)								
OGÓŁEM środki dla [organ] <ENISA…….>	Środki na zobowiązania	=1+1a +3a	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Środki na płatności	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[61] 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.

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

w mln EUR (do trzech miejsc po przecinku)

		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)			**OGÓŁEM**
Dyrekcja Generalna: <…….>									
• Zasoby ludzkie									
• Pozostałe wydatki administracyjne									
OGÓŁEM Dyrekcja Generalna <….>	Środki								

OGÓŁEM środki na DZIAŁ 5 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)								

w mln EUR (do trzech miejsc po przecinku)

		Rok **N**[62] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6) **2026**	**2027**		**OGÓŁEM**
OGÓŁEM środki na DZIAŁY 1 do 5 wieloletnich ram finansowych	Środki na zobowiązania	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Środki na płatności	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[62] 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.

3.2.2. Szacunkowy wpływ na środki operacyjne [organu]

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

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

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

Określić cele i produkty ⇩			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)						**OGÓŁEM**	
	PRODUKT																	
	Rodzaj[63]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[64]																		
- Produkt																		
- Produkt																		
- Produkt																		
Cel szczegółowy nr 1 – suma cząstkowa																		
CEL SZCZEGÓŁOWY nr 2																		
- Produkt																		
Cel szczegółowy nr 2 – suma cząstkowa																		

63 Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

64 Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

KOSZT OGÓŁEM															

3.2.3. Szacunkowy wpływ na zasoby ludzkie ENISA

3.2.3.1. Streszczenie

W wyniku zmiany dyrektywy w sprawie bezpieczeństwa sieci i informacji od 2022/2023 r. ENISA będzie miała dodatkowe zadania. Chociaż zadania te byłyby objęte mandatem ENISA, będą się one wiązać z dodatkowym obciążeniem pracą Agencji. Dokładniej rzecz ujmując, poza obecnymi zadaniami, zgodnie z wnioskiem Komisji dotyczącym zmienionej dyrektywy w sprawie bezpieczeństwa sieci i informacji ENISA zostaną powierzone m.in. zadania: (i) opracowania i utrzymywania europejskiego rejestru podatności (art. 6 ust. 2), (ii) zapewnienia obsługi sekretariatu na potrzeby europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (CyCLONe) (art. 14) oraz sporządzania rocznego sprawozdania o stanie cyberbezpieczeństwa w Unii (art. 15), (iii) wspierania organizacji wzajemnych ocen między państwami członkowskimi (art. 16), (iv) gromadzenia zagregowanych danych o incydentach od państw członkowskich i wydawania wytycznych technicznych (art. 20 ust. 9), (v) utworzenia i prowadzenia rejestru podmiotów świadczących usługi transgraniczne (art. 25).

W związku z tym zostanie złożony wniosek o 5 dodatkowych EPC od 2022 r. z powiązanym budżetem na sfinansowanie tych nowych stanowisk.

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

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

w mln EUR (do trzech miejsc po przecinku)

	Rok **N** [65] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6) **2026** **2027**			**OGÓŁEM**
Pracownicy zatrudnieni na czas określony (AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Pracownicy zatrudnieni na czas określony (AST)								
Personel kontraktowy	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Oddelegowani eksperci krajowi								

[65] 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.

OGÓŁEM	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Wymagania dotyczące pracowników (EPC):

	Rok **N** [66] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6) **2026** **2027**			**OGÓŁEM**
Pracownicy zatrudnieni na czas określony (AD)	3	3	3	3	3	3		**18**
Pracownicy zatrudnieni na czas określony (AST)								
Personel kontraktowy	2	2	2	2	2	2		**12**
Oddelegowani eksperci krajowi								

OGÓŁEM	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Szacowane zapotrzebowanie na zasoby ludzkie macierzystej DG

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

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

Wartości szacunkowe należy wyrazić w pełnych kwotach (lub najwyżej z dokładnością do jednego miejsca po przecinku)

	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)		
• **Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)**							

[66] 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.

XX 01 01 01 (w centrali i w biurach przedstawicielstw Komisji)								
XX 01 01 02 (w delegaturach)								
XX 01 05 01 (pośrednie badania naukowe)								
10 01 05 01 (bezpośrednie badania naukowe)								
• **Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC)**[67]								
XX 01 02 01 (CA, SNE, INT z globalnej koperty finansowej)								
XX 01 02 02 (CA, LA, SNE, INT i JPD w delegaturach)								
XX 01 04 ***yy***[68]	- w centrali[69]							
	- w delegaturach							
XX 01 05 02 (CA, SNE, INT – pośrednie badania naukowe)								
10 01 05 02 (CA, SNE, INT – bezpośrednie badania naukowe)								
Inna linia budżetowa (określić)								
OGÓŁEM								

XX oznacza odpowiedni obszary polityki lub odpowiedni tytuł w budżecie.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG 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	
Personel zewnętrzny	

Opis metody obliczenia kosztów ekwiwalentów pełnego czasu pracy powinien zostać zamieszczony w załączniku V pkt 3.

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

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

69 Przede wszystkim fundusze strukturalne, Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich (EFRROW) oraz Europejski Fundusz Rybacki.

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

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

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

Należy wyjaśnić, na czym ma polegać przeprogramowanie, określając linie budżetowe, których ma ono dotyczyć, oraz podając odpowiednie kwoty. Wniosek jest zgodny z WFR na lata 2021–2027. Kompensacja budżetu, o który wniesiono, aby sfinansować zwiększenie zasobów kadrowych w ENISA, zostanie dokonana przez zmniejszenie o tę samą kwotę budżetu programu „Cyfrowa Europa” w tym samym dziale.

– ☐ Wniosek/inicjatywa wymaga zastosowania instrumentu elastyczności lub zmiany wieloletnich ram finansowych[70].

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

– Wniosek/inicjatywa przewiduje współfinansowanie szacowane zgodnie z poniższym:

w mln EUR (do trzech miejsc po przecinku)

	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)			Ogółem
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

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

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[71]						
		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 różne „przeznaczone na określony cel” należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

Należy określić metodę obliczania wpływu na dochody.

[71] 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.