DYREKTYWY

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555

z dnia 14 grudnia 2022 r.

w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)

(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 Banku Centralnego ([1]),

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([2]),

po konsultacji z Komitetem Regionów,

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

a także mając na uwadze, co następuje:

(1) Celem dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 ([4]) 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 przypadku wystąpienia incydentów, a tym samym przyczynienie się do bezpieczeństwa Unii oraz do sprawnego funkcjonowania jej gospodarki i społeczeństwa.

(2) Od momentu wejścia w życie dyrektywy (UE) 2016/1148 poczyniono znaczne postępy w podnoszeniu poziomu cyberodporności Unii. Przegląd tej dyrektywy pokazał, że stanowiła ona katalizator zmian w instytucjonalnym i regulacyjnym podejściu do cyberbezpieczeństwa w Unii oraz spowodowała znaczącą zmianę w sposobie myślenia. Dzięki tej dyrektywie utworzono ramy krajowe w zakresie bezpieczeństwa sieci i systemów informatycznych poprzez przyjęcie krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych i określenie krajowych zdolności oraz wdrożenie środków regulacyjnych obejmujących niezbędną infrastrukturę i podmioty wskazane przez poszczególne państwa członkowskie. Dyrektywa (UE) 2016/1148 przyczyniła się także do współpracy na poziomie Unii dzięki ustanowieniu Grupy Współpracy oraz sieci krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego. Pomimo tych osiągnięć 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 w społeczeństwie, w tym w kontekście wymiany transgranicznej, sieci i systemy informatyczne stały się zasadniczym elementem codziennego życia. Zmiana ta doprowadziła do ewolucji krajobrazu cyberzagrożeń, przynosząc nowe wyzwania, które wymagają dostosowanych, skoordynowanych i innowacyjnych reakcji we wszystkich państwach członkowskich. Liczba, skala, zaawansowanie, częstotliwość oraz wpływ incydentów stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. W rezultacie incydenty mogą utrudniać prowadzenie działalności gospodarczej na rynku wewnętrznym, powodować straty finansowe, podważać zaufanie użytkowników oraz

([1]) Dz.U. C 233 z 16.6.2022, s. 22.
([2]) Dz.U. C 286 z 16.7.2021, s. 170.
([3]) Stanowisko Parlamentu Europejskiego z dnia 10 listopada 2022 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 28 listopada 2022 r.
([4]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

powodować poważne szkody dla gospodarki i społeczeństwa Unii. Dlatego gotowość i skuteczność w obszarze cyberbezpieczeństwa stają się coraz ważniejsze dla prawidłowego funkcjonowania rynku wewnętrznego niż kiedykolwiek wcześniej. Ponadto w wielu sektorach krytycznych cyberbezpieczeństwo należy do kluczowych czynników umożliwiających udany przebieg transformacji cyfrowej i pełne wykorzystanie ekonomicznych i społecznych korzyści wynikających z cyfryzacji.

(4) Podstawę prawną dyrektywy (UE) 2016/1148 stanowił art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), którego celem jest ustanowienie i zapewnienie funkcjonowania rynku wewnętrznego przez usprawnienie środków służących zbliżeniu przepisów krajowych. Wymogi w zakresie cyberbezpieczeństwa nałożone na podmioty świadczące usługi lub prowadzące działalność kluczową z ekonomicznego punktu widzenia różnią się znacznie – swoim rodzajem i poziomem szczegółowości, a także metodami nadzoru – w zależności od państwa członkowskiego. Rozbieżności te pociągają za sobą dodatkowe koszty i powodują trudności dla podmiotów, które oferują towary lub usługi transgranicznie. Wymogi nałożone przez jedno państwo członkowskie, które różnią się od wymogów nałożonych przez inne państwo członkowskie lub nawet są z nimi sprzeczne, mogą w istotny sposób wpływać na taką transgraniczną działalność. Ponadto ewentualne nieodpowiednie zaprojektowanie lub wdrożenie wymogów dotyczących cyberbezpieczeństwa prawdopodobnie wywrze negatywny wpływ na poziom cyberbezpieczeństwa innych państw członkowskich, w szczególności z uwagi na intensywność wymiany transgranicznej. Z przeglądu dyrektywy (UE) 2016/1148 wynika, że istnieją znaczne rozbieżności w jej wdrażaniu przez państwa członkowskie, w tym pod względem jej zakresu, którego ustalenie w znacznej mierze pozostawiono do uznania państw członkowskich. W dyrektywie (UE) 2016/1148 zapewniono państwom członkowskim bardzo duży margines swobody także w odniesieniu do wdrażania ustanowionych w niej obowiązków dotyczących bezpieczeństwa i zgłaszania incydentów. W rezultacie obowiązki te zostały wdrożone na poziomie krajowym w bardzo różny sposób. Podobne rozbieżności we wdrażaniu wystąpiły w odniesieniu do przepisów dyrektywy (UE) 2016/1148 dotyczących nadzoru i egzekwowania prawa.

(5) Wszystkie te rozbieżności pociągają za sobą fragmentację rynku wewnętrznego i mogą szkodliwie wpływać na jego funkcjonowanie, oddziałując w szczególności na transgraniczne świadczenie usług i poziom cyberodporności ze względu na stosowanie zróżnicowanych środków. Ostatecznie rozbieżności te mogą prowadzić do większej podatności niektórych państw członkowskich na cyberzagrożenia, co może wywołać reperkusje dla całej Unii. Celem niniejszej dyrektywy jest wyeliminowanie takich rozbieżności między państwami członkowskimi, w szczególności przez określenie przepisów minimalnych dotyczących funkcjonowania skoordynowanych ram regulacyjnych, ustanowienie mechanizmów skutecznej współpracy między odpowiedzialnymi organami w poszczególnych państwach członkowskich, zaktualizowanie wykazu sektorów i działań podlegających obowiązkom w zakresie cyberbezpieczeństwa oraz wprowadzenie skutecznych środków naprawczych i środków egzekwowania, które są kluczowe dla skutecznego egzekwowania tych obowiązków. Dyrektywę (UE) 2016/1148 należy zatem uchylić i zastąpić niniejszą dyrektywą.

(6) Wraz z uchyleniem dyrektywy (UE) 2016/1148 należy rozszerzyć zakres stosowania przepisów przez poszczególne sektory na większą część gospodarki, aby zapewnić całościowe uwzględnienie sektorów i usług mających istotne znaczenie dla kluczowych rodzajów działalności społecznej i gospodarczej na rynku wewnętrznym. W szczególności niniejsza dyrektywa ma na celu wyeliminowanie niedociągnięć wynikających z rozróżnienia operatorów usług kluczowych i dostawców usług cyfrowych, które okazało się nieaktualne, ponieważ nie odzwierciedla znaczenia danych sektorów lub usług dla działalności społecznej i gospodarczej na rynku wewnętrznym.

(7) Na podstawie dyrektywy (UE) 2016/1148 państwa członkowskie były odpowiedzialne za identyfikację podmiotów spełniających kryteria pozwalające na uznanie ich za operatorów usług kluczowych. Aby wyeliminować znaczne rozbieżności pod tym względem między państwami członkowskimi oraz zapewnić wszystkim podmiotom objętym regulacją pewność prawa w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie i do obowiązków dotyczących zgłaszania incydentów, należy ustanowić jednolite kryterium określające, które podmioty są objęte zakresem stosowania niniejszej dyrektywy. Kryterium to powinno przewidywać stosowanie zasady wielkościowej przewidującej, że zakres stosowania niniejszej dyrektywy obejmuje wszystkie podmioty, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia Komisji 2003/361/WE ([5]) lub które przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu oraz które działają w sektorach objętych

([5]) 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).

tą dyrektywą lub świadczą objęte nią rodzaje usług lub prowadzą objętą nią działalność. Państwa członkowskie powinny również zapewnić objęcie zakresem niniejszej dyrektywy niektórych małych przedsiębiorstw i mikroprzedsiębiorstw zgodnie z definicją w art. 2 ust. 2 i 3 tego załącznika, które spełniają szczególne kryteria wskazujące na kluczową rolę dla społeczeństwa, gospodarki lub konkretnych sektorów lub rodzajów usług.

(8) Wyłączenie podmiotów administracji publicznej z zakresu stosowania niniejszej dyrektywy powinno mieć zastosowanie do podmiotów, które prowadzą działalność głównie w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności, lub egzekwowania prawa, w tym działania związane z zapobieganiem przestępstwom, prowadzeniem postępowań w ich sprawie, wykrywaniem ich i ściganiem. Jednakże podmioty administracji publicznej, których działalność jedynie w niewielkim stopniu wiąże się z tymi obszarami, nie są wyłączone z zakresu stosowania niniejszej dyrektywy. Do celów niniejszej dyrektywy podmioty posiadające kompetencje regulacyjne nie są uznawane za prowadzące działalność w obszarze egzekwowania prawa i dlatego nie są wyłączone z tej przyczyny z zakresu stosowania niniejszej dyrektywy. Podmioty administracji publicznej ustanowione wspólnie z państwem trzecim zgodnie z umową międzynarodową są wyłączone z zakresu stosowania niniejszej dyrektywy. Niniejsza dyrektywa nie ma zastosowania do misji dyplomatycznych i konsularnych państw członkowskich w państwach trzecich ani do ich sieci i systemów informatycznych, o ile takie systemy znajdują się na terenie misji lub są eksploatowane na potrzeby użytkowników w państwie trzecim.

(9) Państwa członkowskie powinny móc stosować niezbędne środki zapewniające ochronę podstawowych interesów bezpieczeństwa narodowego, gwarantujące porządek publiczny i bezpieczeństwo publiczne oraz umożliwiające zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie, ich wykrywanie i ściganie. W tym celu państwa członkowskie powinny móc zwolnić określone podmioty, które prowadzą działania w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie, ich wykrywanie i ściganie, z niektórych obowiązków określonych w niniejszej dyrektywie w odniesieniu do tych działań. Jeżeli dany podmiot świadczy usługi wyłącznie na rzecz podmiotu administracji publicznej, który jest wyłączony z zakresu stosowania niniejszej dyrektywy, państwa członkowskie powinny móc zwolnić ten podmiot z niektórych obowiązków określonych w niniejszej dyrektywie w odniesieniu do tych usług. Ponadto żadne państwo członkowskie nie powinno mieć obowiązku udzielania informacji, których ujawnienie jest sprzeczne z podstawowymi interesami jego bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności. W tym kontekście należy wziąć pod uwagę unijne lub krajowe przepisy o ochronie informacji niejawnych, umowy dotyczące zachowania poufności oraz nieformalne porozumienia dotyczące zachowania poufności, takie jak kod poufności TLP (Traffic Light Protocol). Kod poufności TLP należy rozumieć jako narzędzie służące informowaniu o ograniczeniach w dalszym rozpowszechnianiu informacji. Jest on wykorzystywany w niemal wszystkich zespołach reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz w niektórych centrach analizy i wymiany informacji.

(10) Mimo iż niniejsza dyrektywa ma zastosowanie do podmiotów prowadzących działalność w zakresie wytwarzania energii elektrycznej w elektrowniach jądrowych, niektóre rodzaje takiej działalności mogą być powiązane z bezpieczeństwem narodowym. W takim przypadku państwo członkowskie powinno móc wykonywać swoje obowiązki dotyczące ochrony bezpieczeństwa narodowego w odniesieniu do tej działalności, w tym działalności w łańcuchu wartości sektora jądrowego, zgodnie z Traktatami.

(11) Niektóre podmioty prowadzą działania w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie, wykrywanie ich i ściganie, a jednocześnie świadczą usługi zaufania. Dostawców usług zaufania, którzy są objęci zakresem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([6]), należy objąć zakresem stosowania niniejszej dyrektywy, aby zapewnić poziom wymogów bezpieczeństwa i nadzoru identyczny z określonym wcześniej w tym rozporządzeniu w odniesieniu do dostawców usług zaufania. W związku z wyłączeniem niektórych konkretnych usług z zakresu stosowania rozporządzenia (UE) nr 910/2014 niniejsza dyrektywa nie powinna mieć zastosowania do świadczenia usług zaufania wykorzystywanych wyłącznie w obrębie zamkniętych systemów wynikających z prawa krajowego lub z porozumień zawartych przez określoną grupę uczestników.

([6]) 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).

(12) Operatorzy świadczący usługi pocztowe zdefiniowani w dyrektywie Parlamentu Europejskiego i Rady 97/67/WE ([7]), w tym dostawcy usług kurierskich, powinni podlegać niniejszej dyrektywie, jeżeli świadczą usługi na co najmniej jednym z etapów łańcucha doręczania przesyłek pocztowych, a w szczególności przyjmowania, sortowania, transportu lub doręczania, w tym odbioru przesyłek, przy uwzględnieniu stopnia ich zależności od sieci i systemów informatycznych. Usługi transportowe, które nie są świadczone w związku z jednym z wymienionych etapów, powinny być wyłączone z zakresu usług pocztowych.

(13) Zważywszy na intensyfikację i coraz większe wyrafinowanie cyberzagrożeń, państwa członkowskie powinny starać się zapewnić osiągnięcie wysokiego poziomu cyberbezpieczeństwa przez podmioty wyłączone z zakresu stosowania niniejszej dyrektywy oraz wspierać wdrażanie równoważnych środków zarządzania ryzykiem w cyberbezpieczeństwie, które odzwierciedlają wrażliwy charakter tych podmiotów.

(14) Do przetwarzania danych osobowych na podstawie niniejszej dyrektywy mają zastosowanie unijne przepisy dotyczące ochrony danych oraz unijne przepisy dotyczące prywatności. W szczególności niniejsza dyrektywa nie narusza rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([8]) i dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady ([9]). Niniejsza dyrektywa nie powinna zatem wpływać między innymi na zadania i uprawnienia organów właściwych do spraw monitorowania zgodności z obowiązującymi unijnymi przepisami dotyczącymi ochrony danych i unijnymi przepisami dotyczącymi ochrony prywatności.

(15) Podmioty, które są objęte zakresem stosowania niniejszej dyrektywy w celu przestrzegania środków zarządzania ryzykiem w cyberbezpieczeństwie i obowiązków dotyczących zgłaszania incydentów, należy podzielić na dwie kategorie – podmioty kluczowe i podmioty ważne, w zależności od tego, jak bardzo ich znaczenie jest zasadnicze dla ich sektorów lub dla rodzaju świadczonych przez nie usług, a także od ich wielkości. W związku z tym właściwe organy powinny w stosownych przypadkach należycie uwzględniać odpowiednie sektorowe oszacowania ryzyka lub wskazówki. Należy zróżnicować systemy nadzoru i egzekwowania między tymi dwiema kategoriami podmiotów, aby zapewnić odpowiednią równowagę między wymogami i obowiązkami związanymi z ryzykiem a obciążeniem administracyjnym wynikającym z nadzoru nad zgodnością z przepisami.

(16) Stosując art. 6 ust. 2 załącznika do zalecenia 2003/361/WE, państwa członkowskie mogą uwzględnić stopień niezależności podmiotu w stosunku do jego przedsiębiorstw partnerskich lub powiązanych, aby uniknąć uznawania podmiotów, które mają przedsiębiorstwa partnerskie lub które są przedsiębiorstwami powiązanymi, za podmioty kluczowe lub ważne, gdyby było to nieproporcjonalne. W szczególności państwa członkowskie mogą uwzględnić fakt, że dany podmiot jest niezależny od przedsiębiorstw partnerskich lub powiązanych pod względem sieci i systemów informatycznych, z których korzysta przy świadczeniu usług, a także pod względem świadczonych przez siebie usług. Na tej podstawie, w stosownych przypadkach, państwa członkowskie mogą uznać, że taki podmiot nie kwalifikuje się jako średnie przedsiębiorstwo na podstawie art. 2 załącznika do zalecenia 2003/361/WE, ani nie przekracza określonych dla średniego przedsiębiorstwa pułapów, określonych w ust. 1 tego artykułu, jeżeli po uwzględnieniu stopnia niezależności tego podmiotu nie zostałby on uznany za kwalifikujący się jako średnie przedsiębiorstwo lub przekraczający te pułapy, w przypadku gdy uwzględniono tylko jego własne dane. Nie wpływa to na określone w niniejszej dyrektywie obowiązki przedsiębiorstw partnerskich i powiązanych, które są objęte zakresem jej stosowania.

(17) Państwa członkowskie powinny mieć możliwość decydowania, że za podmioty kluczowe należy uznać podmioty zidentyfikowane przed wejściem w życie niniejszej dyrektywy jako operatorzy usług kluczowych zgodnie z dyrektywą (UE) 2016/1148.

([7]) 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).

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

([9]) 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).

(18) W celu zapewnienia przejrzystego przeglądu podmiotów objętych zakresem stosowania niniejszej dyrektywy, państwa członkowskie powinny utworzyć wykaz podmiotów kluczowych i ważnych, a także podmiotów świadczących usługi rejestracji nazw domen. W tym celu państwa członkowskie powinny zobowiązać podmioty do przekazywania właściwym organom co najmniej następujących informacji: nazwy, adresu i aktualnych danych kontaktowych, w tym adresów poczty elektronicznej, zakresów adresów IP i numerów telefonicznych podmiotu oraz, w stosownych przypadkach, odpowiedniego sektora i podsektora, o których mowa w załącznikach, a także, w stosownych przypadkach, wykazu państw członkowskich, w których dany podmiot świadczy usługi objęte zakresem stosowania niniejszej dyrektywy. W tym celu Komisja, z pomocą Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), powinna bez zbędnej zwłoki podać wytyczne i wzory na potrzeby obowiązku przekazywania informacji. Aby ułatwić utworzenie i aktualizację wykazu podmiotów kluczowych i ważnych, a także podmiotów świadczących usługi rejestracji nazw domen, państwa członkowskie powinny móc ustanowić mechanizmy krajowe umożliwiające podmiotom samodzielną rejestrację. Jeżeli rejestry istnieją na poziomie krajowym, państwa członkowskie mogą decydować o odpowiednich mechanizmach umożliwiających identyfikację podmiotów objętych zakresem stosowania niniejszej dyrektywy.

(19) Państwa członkowskie powinny być odpowiedzialne za poinformowanie Komisji co najmniej o liczbie podmiotów kluczowych i ważnych dla każdego sektora i podsektora, o których mowa w załącznikach, a także przekazanie jej odpowiednich informacji o liczbie zidentyfikowanych podmiotów i o tym, na podstawie którego przepisu – spośród ustanowionych w niniejszej dyrektywie – zostały one zidentyfikowane oraz rodzaju świadczonej przez te podmioty usługi. Zachęca się państwa członkowskie, aby wymieniały z Komisją informacje o podmiotach kluczowych i ważnych oraz – w przypadku incydentu dotyczącego cyberbezpieczeństwa na dużą skalę – odpowiednie informacje takie jak nazwa danego podmiotu.

(20) Komisja powinna, we współpracy z Grupą Współpracy i po konsultacji z odpowiednimi zainteresowanymi stronami, podać wytyczne dotyczące wdrażania kryteriów mających zastosowanie do mikroprzedsiębiorstw i małych przedsiębiorstw, do celów oceny, czy są one objęte zakresem stosowania niniejszej dyrektywy. Komisja powinna też zapewnić, aby mikroprzedsiębiorstwa i małe przedsiębiorstwa objęte zakresem stosowania niniejszej dyrektywy otrzymywały odpowiednie wytyczne. Komisja powinna – z pomocą państw członkowskich – udostępniać mikroprzedsiębiorstwom i małym przedsiębiorstwom informacje w tym zakresie.

(21) Komisja może wydawać wytyczne, aby pomóc państwom członkowskim w prawidłowym wdrażaniu przepisów niniejszej dyrektywy dotyczących zakresu jej stosowania oraz w ocenie proporcjonalności środków do zastosowania na podstawie niniejszej dyrektywy, w szczególności w odniesieniu do podmiotów o złożonych modelach biznesowych lub środowiskach operacyjnych, gdzie podmiot może jednocześnie spełniać kryteria bycia podmiotem kluczowym i podmiotem ważnym lub może jednocześnie prowadzić działania, z których jedne są objęte zakresem stosowania niniejszej dyrektywy, a inne są z niego wyłączone.

(22) Niniejsza dyrektywa określa poziom odniesienia dla środków zarządzania ryzykiem w cyberbezpieczeństwie i dla obowiązków dotyczących zgłaszania incydentów w sektorach, które wchodzą w zakres jej stosowania. Aby uniknąć fragmentacji przepisów o cyberbezpieczeństwie zawartych w aktach prawnych Unii, jeżeli kolejne sektorowe akty prawne Unii regulujące środki zarządzania ryzykiem w cyberbezpieczeństwie i obowiązki w zakresie zgłaszania incydentów zostaną uznane za niezbędne do zapewnienia wysokiego poziomu cyberbezpieczeństwa w całej Unii, Komisja powinna ocenić, czy takie przepisy można określić w akcie wykonawczym na podstawie niniejszej dyrektywy. Gdyby taki akt wykonawczy nie był odpowiedni do tego celu, do zapewnienia wysokiego poziomu cyberbezpieczeństwa w całej Unii można wykorzystać sektorowe akty prawne Unii, przy pełnym uwzględnieniu specyfiki i złożoności danych sektorów. W związku z tym niniejsza dyrektywa nie stanowi przeszkody dla przyjęcia kolejnych sektorowych aktów prawnych Unii regulujących środki zarządzania ryzykiem w cyberbezpieczeństwie i obowiązki w zakresie zgłaszania incydentów, należycie uwzględniających potrzebę kompleksowych i spójnych ram dotyczących cyberbezpieczeństwa. Niniejsza dyrektywa nie narusza istniejących uprawnień wykonawczych, które powierzono Komisji w wielu sektorach, w tym w sektorach transportu i energetyki.

(23) Jeżeli sektorowy akt prawny Unii zawiera przepisy wymagające od podmiotów kluczowych lub ważnych, aby przyjęły środki zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszały poważne incydenty, i jeżeli wymogi te są co najmniej równoważne pod względem skutku obowiązkom określonym w niniejszej dyrektywie, wówczas te przepisy, w tym dotyczące nadzoru i egzekwowania prawa, powinny mieć zastosowanie do takich podmiotów. Jeżeli

sektorowy akt prawny Unii nie obejmuje wszystkich podmiotów w danym sektorze wchodzących w zakres stosowania niniejszej dyrektywy, odnośne przepisy niniejszej dyrektywy powinny nadal mieć zastosowanie do podmiotów nieobjętych tym aktem.

(24) Jeżeli przepisy sektorowego aktu prawnego Unii wymagają, aby podmioty kluczowe lub ważne spełniały obowiązki w zakresie zgłaszania incydentów, które są co najmniej równoważne pod względem skutku obowiązkom w zakresie zgłaszania incydentów określonym w niniejszej dyrektywie, należy zapewnić spójność i skuteczność postępowania w przypadku zgłoszeń incydentów. W tym celu przepisy dotyczące zgłaszania incydentów sektorowego aktu prawnego Unii powinny zapewniać CSIRT, właściwym organom lub pojedynczym punktom kontaktowym do spraw cyberbezpieczeństwa (pojedynczym punktom kontaktowym) na podstawie niniejszej dyrektywy natychmiastowy dostęp do zgłoszeń incydentów zgodnie z sektorowym aktem prawnym Unii. W szczególności taki natychmiastowy dostęp można zapewnić, jeżeli zgłoszenia incydentów są przekazywane bez zbędnej zwłoki CSIRT, właściwemu organowi lub pojedynczemu punktowi kontaktowemu) na podstawie niniejszej dyrektywy. W stosownych przypadkach państwa członkowskie powinny wprowadzić mechanizm automatycznego i bezpośredniego zgłaszania incydentów, zapewniający systematyczną i natychmiastową wymianę informacji z CSIRT, właściwymi organami lub pojedynczymi punktami kontaktowymi dotyczącą postępowania w przypadku takich zgłoszeń incydentów. W celu uproszczenia zgłaszania incydentów oraz wdrożenia mechanizm automatycznego i bezpośredniego zgłaszania incydentów, państwa członkowskie mogą, zgodnie z sektorowym aktem prawnym Unii, korzystać z pojedynczego punktu zgłaszania incydentów.

(25) Sektorowe akty prawne Unii, które przewidują środki zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązki w zakresie zgłaszania incydentów, które są co najmniej równoważne pod względem skutku obowiązkom określonym w niniejszej dyrektywie, mogą przewidywać, że właściwe organy na podstawie takich aktów wykonują swoje uprawnienia dotyczące nadzoru i egzekwowania prawa w odniesieniu do takich środków lub obowiązków z pomocą właściwych organów na podstawie niniejszej dyrektywy. Odpowiednie właściwe organy mogą w tym celu przyjąć ustalenia dotyczące współpracy. W takich ustaleniach dotyczących współpracy można określić między innymi procedury dotyczące koordynacji działań nadzorczych, w tym procedury dochodzeń i kontroli na miejscu zgodnie z prawem krajowym, oraz mechanizm wymiany między właściwymi organami istotnych informacji na temat nadzoru i egzekwowania prawa, obejmujący dostęp do informacji związanych z cyberprzestrzenią, o które właściwe organy zwracają się na podstawie niniejszej dyrektywy.

(26) Jeżeli sektorowe akty prawne Unii zobowiązują lub motywują podmioty do zgłaszania poważnych cyberzagrożeń, państwa członkowskie powinny również zachęcać do przekazywania informacji o poważnych cyberzagrożeniach CSIRT, właściwym organom lub pojedynczym punktom kontaktowym na podstawie niniejszej dyrektywy, tak by organy te miały lepszy obraz cyberzagrożeń i mogły skutecznie i terminowo reagować w przypadku wystąpienia poważnych cyberzagrożeń.

(27) Przyszłe sektorowe akty prawne Unii powinny należycie uwzględniać definicje oraz ramy nadzoru i egzekwowania prawa określone w niniejszej dyrektywie.

(28) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 ([10]) należy uznać za sektorowy akt prawny Unii powiązany z niniejszą dyrektywą w odniesieniu do podmiotów finansowych. Zamiast przepisów niniejszej dyrektywy zastosowanie powinny mieć przepisy rozporządzenia (UE) 2022/2554 dotyczące zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (ICT), zarządzania incydentami związanymi z ICT, a w szczególności zgłaszania poważnych incydentów związanych z ICT, a także testowania operacyjnej odporności cyfrowej, mechanizmów wymiany informacji oraz ryzyka związanego z zewnętrznymi dostawcami ICT. Do podmiotów finansowych objętych rozporządzeniem (UE) 2022/2554 państwa członkowskie nie powinny zatem stosować przepisów niniejszej dyrektywy dotyczących zarządzania ryzykiem w cyberbezpieczeństwie i obowiązków w zakresie zgłaszania incydentów oraz nadzoru i egzekwowania prawa. Jednocześnie istotne jest, aby utrzymać silne relacje i skuteczną wymianę informacji z sektorem finansowym na podstawie niniejszej dyrektywy. W tym celu rozporządzenie (UE) 2022/2554 umożliwia Europejskim Urzędom Nadzoru oraz właściwym organom na podstawie tego rozporządzenia udział w działaniach Grupy Współpracy oraz wymianę informacji i współpracę z pojedynczymi punktami kontaktowymi, a także z CSIRT i właściwymi organami na podstawie niniejszej dyrektywy. Właściwe organy na podstawie rozporządzenia (UE) 2022/2554 powinny także przekazywać dane na temat poważnych incydentów związanych z ICT i, w odpowiednich przypadkach, poważnych cyberzagrożeń także CSIRT, właściwym organom lub pojedynczym punktom kontaktowym na podstawie niniejszej dyrektywy. Można to osiągnąć

([10]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (zob. s. 1 niniejszego Dziennika Urzędowego).

przez zapewnienie natychmiastowego dostępu do zgłoszeń incydentów i ich bezpośrednie przekazywanie bezpośrednio lub za pośrednictwem pojedynczego punktu. Ponadto państwa członkowskie powinny w dalszym ciągu uwzględniać sektor finansowy w swoich strategiach cyberbezpieczeństwa, a CSIRT mogą objąć go swoimi działaniami.

(29) Aby uniknąć luk w obowiązkach lub powielania obowiązków dotyczących cyberbezpieczeństwa nałożonych na podmioty w sektorze lotnictwa, organy krajowe na podstawie rozporządzeń Parlamentu Europejskiego i Rady (WE) nr 300/2008 ([11]) i (UE) 2018/1139 ([12]) oraz właściwe organy na podstawie niniejszej dyrektywy powinny współpracować przy wdrażaniu środków zarządzania ryzykiem w cyberbezpieczeństwie oraz przy nadzorowaniu przestrzegania tych środków na poziomie krajowym. Spełnienie przez podmiot wymogów bezpieczeństwa określonych w rozporządzeniach (WE) nr 300/2008 i (UE) 2018/1139 oraz w odpowiednich aktach delegowanych i wykonawczych przyjętych na podstawie tych rozporządzeń może zostać uznane przez właściwe organy na podstawie niniejszej dyrektywy za spełnienie odpowiednich wymogów określonych w niniejszej dyrektywie.

(30) Zważywszy na powiązania między cyberbezpieczeństwem a bezpieczeństwem fizycznym podmiotów, należy zapewnić spójność podejścia między dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2557 ([13]) a niniejszą dyrektywą. W tym celu podmioty zidentyfikowane jako podmioty krytyczne na mocy dyrektywy (UE) 2022/2557 powinny być uznawane za podmioty kluczowe na podstawie niniejszej dyrektywy. Ponadto każde państwo członkowskie powinno zapewnić, aby w jego krajowej strategii dotyczącej cyberbezpieczeństwa przewidziano ramy polityki umożliwiające zwiększoną koordynację w obrębie tego państwa członkowskiego między jego właściwymi organami na podstawie niniejszej dyrektywy i tymi na podstawie dyrektywy (UE) 2022/2557 w kontekście wymiany informacji na temat ryzyka, cyberzagrożeń i incydentów, a także ryzyka, cyberzagrożeń i incydentów poza cyberprzestrzenią, a także wykonywania zadań nadzorczych. Właściwe organy na podstawie niniejszej dyrektywy i te na podstawie dyrektywy (UE) 2022/2557 powinny ze sobą współpracować i wymieniać się informacjami bez zbędnej zwłoki, w szczególności w odniesieniu do identyfikacji podmiotów krytycznych, ryzyka, zagrożenia i incydentów w cyberprzestrzeni oraz ryzyka, zagrożeń i incydentów poza cyberprzestrzenią wpływających na podmioty krytyczne, co obejmuje środki dotyczące cyberbezpieczeństwa i środki fizyczne stosowane przez podmioty krytyczne, a także wyniki działań nadzorczych przeprowadzonych wobec takich podmiotów.

Ponadto aby usprawnić działania nadzorcze między właściwymi organami na podstawie niniejszej dyrektywy oraz tymi na podstawie dyrektywy (UE) 2022/2557 oraz zminimalizować obciążenie administracyjne podmiotów, których to dotyczy, te właściwe organy powinny starać się zharmonizować wzory zgłoszeń incydentów i procesy nadzorcze. W stosownych przypadkach właściwe organy działające na podstawie dyrektywy (UE) 2022/2557 powinny móc zwrócić się do właściwych organów na podstawie niniejszej dyrektywy, aby wykonały swoje uprawnienia nadzorcze i wykonawcze w stosunku do podmiotu, który został zidentyfikowany jako podmiot krytyczny na podstawie dyrektywy (UE) 2022/2557. Właściwe organy na podstawie niniejszej dyrektywy i te na podstawie dyrektywy (UE) 2022/2557 powinny, w miarę możliwości w czasie rzeczywistym, współpracować i prowadzić wymianę informacji w tym celu.

(31) Podmioty należące do sektora infrastruktury cyfrowej opierają się zasadniczo na sieciach i systemach informatycznych, w związku z czym obowiązki nałożone na te podmioty na mocy niniejszej dyrektywy powinny w kompleksowy sposób odnosić się do bezpieczeństwa fizycznego takich systemów, w ramach środków zarządzania ryzykiem w cyberbezpieczeństwie stosowanych przez te podmioty i ich obowiązków w zakresie zgłaszania incydentów. Ponieważ kwestie te są objęte niniejszą dyrektywą, obowiązki określone w rozdziałach III, IV i VI dyrektywy (UE) 2022/2557 nie mają zastosowania do takich podmiotów.

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

([12]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 (Dz.U. L 212 z 22.8.2018, s. 1).

([13]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (zob. s. 164 niniejszego Dziennika Urzędowego).

(32) Utrzymywanie i zachowanie wiarygodnego, odpornego i bezpiecznego systemu nazw domen (DNS) należy do kluczowych czynników umożliwiających utrzymanie integralności internetu oraz ma istotne znaczenie dla jego nieprzerwanego i stabilnego działania, od którego zależą gospodarka cyfrowa i społeczeństwo cyfrowe. Dlatego niniejsza dyrektywa powinna mieć zastosowanie do rejestrów nazw domen najwyższego poziomu (TLD) i do dostawców usług DNS, których należy rozumieć jako podmioty dostarczające dostępne publicznie rekurencyjne usługi rozpoznawania nazw domen dla użytkowników końcowych internetu lub autorytatywne usługi rozpoznawania nazw domen na użytek osób trzecich. Niniejsza dyrektywa nie powinna mieć zastosowania do głównych serwerów nazw (ang. root name servers).

(33) Usługi chmurowe powinny obejmować usługi cyfrowe umożliwiające administrowanie na żądanie skalowalnym i elastycznym zbiorem rozproszonych zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru, w tym gdy takie zasoby są rozmieszczone w kilku lokalizacjach. Zasoby obliczeniowe obejmują zasoby takie jak sieci, serwery lub inna infrastruktura, systemy operacyjne, oprogramowanie, pamięć masowa, aplikacje i usługi. Do modeli usług chmurowych należą m.in. infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS), oprogramowanie jako usługa (SaaS) oraz sieć jako usługa (NaaS). Modele rozmieszczenia usług chmurowych powinny obejmować chmury prywatne, zbiorowe, publiczne i hybrydowe. Modele usług chmurowych i modele rozmieszczenia oznaczają to samo co usługi i modele ich realizacji zdefiniowane w normie ISO/IEC 17788:2014. Zdolność użytkowników usług chmurowych do jednostronnego zapewnienia sobie możliwości obliczeniowych, takich jak czas serwera lub magazyn sieciowy, bez żadnej interakcji z udziałem człowieka ze strony dostawcy usług chmurowych można określić jako administrowanie na żądanie.

Terminu „szeroki dostęp zdalny" używa się do opisu sytuacji, gdy zasoby chmurowe są udostępniane przez sieć, a dostęp do nich jest możliwy za pośrednictwem mechanizmów sprzyjających wykorzystywaniu różnorodnych platform typu *thin client* lub *thick client*, w tym telefonów komórkowych, tabletów, laptopów oraz stacji roboczych. Termin „skalowalne" odnosi się do zasobów komputerowych, które są elastycznie przydzielane przez dostawcę usługi niezależnie od położenia geograficznego zasobów w reakcji na fluktuacje zapotrzebowania. Terminu „elastyczny zbiór" używa się do opisu zasobów obliczeniowych, które są dostarczane i uwalniane według zapotrzebowania, aby szybko zwiększać i zmniejszać dostępne zasoby w zależności od obciążenia. Terminu „wspólnie wykorzystywane" 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 jest świadczona z tego samego sprzętu elektronicznego. Terminu „rozproszone" używa się do opisu zasobów obliczeniowych zlokalizowanych na różnych komputerach lub urządzeniach połączonych w sieć, które komunikują się ze sobą i koordynują swoją pracę przez przekazywanie komunikatów.

(34) Zważywszy na pojawianie się innowacyjnych technologii i nowych modeli biznesowych, oczekuje się, że w odpowiedzi na zmieniające się potrzeby klientów nowe modele usług chmurowych i modele rozmieszczenia zaistnieją na rynku wewnętrznym. W tym kontekście usługi chmurowe mogą być świadczone w sposób wysoce rozproszony, jeszcze bliżej miejsca generowania lub gromadzenia danych, co będzie wiązać się z przejściem od modelu tradycyjnego do modelu wysoce rozproszonego (przetwarzanie danych na obrzeżach sieci).

(35) Usługi oferowane przez dostawców usług ośrodka przetwarzania danych nie zawsze muszą być świadczone w postaci usług chmurowych. Przetwarzanie danych nie zawsze musi zatem stanowić element infrastruktury usług chmurowych. W celu zarządzania ogółem ryzyka dla bezpieczeństwa sieci i systemów informatycznych niniejsza dyrektywa powinna zatem obejmować dostawców usług ośrodka przetwarzania danych niebędących usługami chmurowymi. Do celów niniejszej dyrektywy termin „usługa ośrodka przetwarzania danych" powinien obejmować świadczenie usługi, w skład której wchodzą struktury lub grupy struktur służące scentralizowanemu hostingowi, wzajemnym połączeniom i eksploatacji sprzętu informatycznego i sieciowego służącego do przechowywania, przetwarzania i transportu danych wraz z całością obiektów i infrastruktury zapewniających dystrybucję energii elektrycznej i kontrolę środowiskową. Terminu „usługa ośrodka przetwarzania danych" nie należy stosować w odniesieniu do wewnętrznych, korporacyjnych ośrodków przetwarzania danych będących własnością danego podmiotu i eksploatowanych przez niego na własne potrzeby.

(36) Działania badawcze odgrywają kluczową rolę w rozwoju nowych produktów i procesów. Wiele z tych działań jest prowadzonych przez podmioty, które udostępniają, rozpowszechniają lub wykorzystują wyniki swoich badań do celów handlowych. Podmioty te mogą zatem być ważnymi uczestnikami łańcuchów wartości, co sprawia, że bezpieczeństwo ich sieci i systemów informatycznych stanowi integralną część ogólnego cyberbezpieczeństwa rynku wewnętrznego. Organizacje badawcze należy rozumieć jako obejmujące podmioty, które koncentrują zasadniczą część swojej działalności na prowadzeniu badań stosowanych lub eksperymentalnych prac rozwojowych w rozumieniu

Podręcznika Frascati Organizacji Współpracy Gospodarczej i Rozwoju z 2015 r.: Wytyczne dotyczące gromadzenia i prezentowania danych z badań i eksperymentalnych prac rozwojowych z myślą o wykorzystaniu ich wyników do celów handlowych, takich jak wytwarzanie lub rozwój produktu lub procesu, świadczenie usługi lub jego wprowadzanie do obrotu.

(37) Coraz większe współzależności wynikają z coraz bardziej transgranicznej i współzależnej sieci świadczenia usług, wykorzystującej kluczową infrastrukturę w całej Unii w sektorach takich jak energetyka, transport, infrastruktura cyfrowa, woda pitna i ścieki, zdrowie, niektóre aspekty administracji publicznej, a także przestrzeni kosmicznej, jeżeli chodzi o świadczenie niektórych usług zależnych od naziemnej infrastruktury, która jest własnością państw członkowskich albo podmiotów prywatnych oraz jest przez nie zarządzana i obsługiwana, a zatem nieobejmującej infrastruktury, która jest własnością Unii lub podmiotów działających w jej imieniu lub jest zarządzana lub obsługiwana przez Unię lub podmioty działające w jej imieniu w ramach jej programu kosmicznego. 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. Nasilone cyberataki podczas pandemii COVID-19 uwydatniły podatność coraz bardziej współzależnych społeczeństw w obliczu ryzyka o niskim prawdopodobieństwie wystąpienia.

(38) Z uwagi na różnice w krajowych strukturach zarządzania oraz aby zabezpieczyć obowiązujące już ustalenia sektorowe lub unijne organy nadzorcze i regulacyjne, państwa członkowskie powinny móc wyznaczyć lub ustanowić co najmniej jeden właściwy organ odpowiedzialny za cyberbezpieczeństwo i zadania nadzorcze na podstawie niniejszej dyrektywy.

(39) Aby ułatwić współpracę i komunikację transgraniczną między organami oraz umożliwić skuteczne wprowadzenie w życie niniejszej dyrektywy, niezbędne jest, by każde państwo członkowskie wyznaczyło pojedynczy punkt kontaktowy odpowiedzialny za koordynację kwestii związanych z bezpieczeństwem sieci i systemów informatycznych oraz współpracą transgraniczną na poziomie Unii.

(40) Pojedyncze punkty kontaktowe powinny zapewniać skuteczną współpracę transgraniczną z właściwymi organami innych państw członkowskich oraz, w stosownych przypadkach, z Komisją i ENISA. Pojedynczym punktom kontaktowym należy zatem powierzyć zadanie przekazywania zgłoszeń poważnych incydentów mających skutki transgraniczne pojedynczym punktom kontaktowym innych państw członkowskich, których dany incydent dotyczy, na wniosek CSIRT lub właściwego organu. Na poziomie krajowym pojedyncze punkty kontaktowe powinny umożliwiać sprawną współpracę międzysektorową z innymi właściwymi organami. Pojedyncze punkty kontaktowe mogłyby być również odbierać stosowne informacje na temat incydentów dotyczących podmiotów finansowych przekazywane przez właściwe organy na mocy rozporządzenia (UE) 2022/2554 i powinny być w stanie przekazywać te informacje, stosownie do przypadku, CSIRT lub właściwym organom na podstawie niniejszej dyrektywy.

(41) Państwa członkowskie powinny być odpowiednio wyposażone, zarówno pod względem zdolności technicznych, jak i możliwości organizacyjnych, aby zapobiegać incydentom i ryzyku, wykrywać je, reagować na nie i przywracać normalne działanie po ich wystąpieniu oraz łagodzić ich skutki. Państwa członkowskie powinny zatem ustanowić lub wyznaczyć co najmniej jeden CSIRT na podstawie niniejszej dyrektywy oraz zapewnić im odpowiednie zasoby i możliwości techniczne. CSIRT powinny spełniać wymogi określone w niniejszej dyrektywie, aby zagwarantować efektywne i kompatybilne zdolności w zakresie postępowania z incydentami i ryzykiem oraz zapewnić skuteczną współpracę na poziomie Unii. Państwa członkowskie powinny móc wyznaczyć jako CSIRT również istniejące zespoły reagowania na incydenty komputerowe (CERT). Aby zwiększyć zaufanie między podmiotami a CSIRT, jeżeli dany CSIRT funkcjonuje w ramach właściwego organu, państwa członkowskie powinny móc rozważyć funkcjonalne rozdzielenie zadań operacyjnych wykonywanych przez CSIRT – w szczególności odnoszących się do przekazywania informacji i do wspomagania podmiotów – od działań nadzorczych właściwych organów.

(42) Zadaniem CSIRT jest obsługa incydentów. Obejmuje ono przetwarzanie dużych ilości danych, w niektórych przypadkach danych szczególnie chronionych. Państwa członkowskie powinny zapewnić, aby CSIRT dysponowały infrastrukturą służącą do wymiany i przetwarzania informacji, a także odpowiednio wyposażonym personelem, co zapewni poufność i wiarygodność ich operacji. CSIRT mogłyby również przyjąć kodeksy postępowania w tym zakresie.

(43) Jeżeli chodzi o dane osobowe, CSIRT powinny być w stanie zapewnić zgodnie z rozporządzeniem (UE) 2016/679 – na wniosek kluczowego lub ważnego podmiotu, proaktywne skanowanie sieci i systemów informatycznych wykorzystywanych przez te podmioty do świadczenia usług. W odpowiednim przypadku państwa członkowskie powinny dążyć do zapewnienia równego poziomu zdolności technicznych wszystkich sektorowych CSIRT. Państwa członkowskie powinny móc zwrócić się do ENISA o pomoc przy tworzeniu CSIRT.

(44) CSIRT powinny mieć zdolność do monitorowania – na wniosek podmiotu kluczowego lub ważnego –jego aktywów połączonych z internetem, zarówno w należących do niego obiektach, jak i poza nimi, aby zidentyfikować i zrozumieć ogólne ryzyko organizacyjne tego podmiotu związane z nowo zidentyfikowanymi naruszeniami bezpieczeństwa w łańcuchach dostaw lub z podatnościami krytycznymi. Podmiot należy zachęcać do informowania CSIRT o tym, czy korzysta z uprzywilejowanego interfejsu zarządzania, ponieważ mogłoby to wpłynąć na szybkość podejmowania działań łagodzących.

(45) Z uwagi na znaczenie współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa CSIRT powinny móc uczestniczyć w międzynarodowych sieciach współpracy, niezależnie od współpracy w sieci CSIRT ustanowionej na mocy niniejszej dyrektywy. Dlatego w celu wykonywania swoich zadań CSIRT i właściwe organy powinny mieć możliwość wymiany informacji, w tym danych osobowych, z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego lub z właściwymi organami państw trzecich, pod warunkiem że spełnione są warunki określone w unijnym prawie dotyczącym ochrony danych w odniesieniu do przekazywania danych osobowych do państw trzecich, między innymi warunki określone w art. 49 rozporządzenia (UE) 2016/679.

(46) Zasadnicze znaczenie ma zapewnienie zasobów do realizacji celów niniejszej dyrektywy oraz do umożliwienia właściwym organom i CSIRT wykonywania ustanowionych w niej zadań. Państwa członkowskie mogą wprowadzić na poziomie krajowym mechanizm finansowania, aby pokryć niezbędne wydatki związane z wykonywaniem zadań przez podmioty publiczne odpowiedzialne za cyberbezpieczeństwo w danym państwie członkowskim na podstawie niniejszej dyrektywy. Taki mechanizm powinien być zgodny z prawem Unii, proporcjonalny i niedyskryminujący, a także powinien uwzględniać różne podejścia do świadczenia bezpiecznych usług.

(47) Sieć CSIRT powinna nadal przyczyniać się do zwiększania zaufania i pewności oraz do wspierania szybkiej i skutecznej współpracy operacyjnej między państwami członkowskimi. W celu zacieśnienia współpracy operacyjnej na szczeblu Unii sieć CSIRT powinna rozważyć zaproszenie do udziału w jej pracach organów i agencji Unii zaangażowanych w politykę cyberbezpieczeństwa, takich jak Europol.

(48) W celu osiągnięcia i utrzymania wysokiego poziomu cyberbezpieczeństwa krajowe strategie cyberbezpieczeństwa wymagane na podstawie niniejszej dyrektywy powinny składać się ze spójnych ram określających strategiczne cele i priorytety w obszarze cyberbezpieczeństwa oraz sposób zarządzania służący ich osiągnięciu. Strategie te mogą składać się z jednego lub większej liczby aktów ustawodawczych lub nieustawodawczych.

(49) Polityka cyberhigieny stanowi podstawę pozwalającą chronić infrastrukturę sieci i systemów informatycznych, bezpieczeństwo sprzętu, oprogramowania i aplikacji internetowych oraz dane przedsiębiorstw lub użytkowników końcowych wykorzystywane przez podmioty. Polityka cyberhigieny obejmująca wspólny podstawowy zestaw praktyk – w tym aktualizacje oprogramowania i sprzętu, zmianę haseł, zarządzanie nowymi instalacjami, ograniczanie kont dostępu na poziomie administratora oraz tworzenie kopii zapasowych danych – umożliwia utworzenie proaktywnych ram gotowości oraz zapewnienie ogólnego bezpieczeństwa i ochrony w razie incydentów lub cyberzagrożeń. ENISA powinna monitorować i analizować politykę państw członkowskich dotyczącą cyberhigieny.

(50) Świadomość zagadnień cyberbezpieczeństwa i cyberhigiena mają zasadnicze znaczenie dla podniesienia poziomu cyberbezpieczeństwa w Unii, w szczególności w świetle rosnącej liczby urządzeń podłączonych do internetu, które są coraz częściej wykorzystywane w cyberatakach. Należy dołożyć starań, aby zwiększyć ogólną świadomość ryzyka związanego z takimi urządzeniami, zaś oceny na poziomie Unii mogłyby pomóc w zapewnieniu wspólnego rozumienia takich zagrożeń na rynku wewnętrznym.

(51) Państwa członkowskie powinny zachęcać do korzystania z innowacyjnych technologii, w tym sztucznej inteligencji, których stosowanie mogłoby poprawić wykrywanie cyberataków i zapobieganie im, umożliwiając skuteczniejsze przekierowywanie zasobów na cyberataki. W krajowych strategiach cyberbezpieczeństwa państwa członkowskie powinny zatem zachęcać do działań badawczo-rozwojowych mających ułatwiać korzystanie z takich technologii, w szczególności technologii związanych z automatycznymi lub półautomatycznymi narzędziami w dziedzinie cyberbezpieczeństwa, oraz, w stosownych przypadkach, wymianę danych potrzebnych do szkolenia użytkowników takiej technologii i do jej doskonalenia. Stosowanie innowacyjnych technologii, w tym sztucznej inteligencji, powinno być zgodne z unijnymi przepisami o ochronie danych, w tym z zasadami ochrony danych zakładającymi dokładność danych, minimalizację danych, uczciwość i przejrzystość oraz z wymogami bezpieczeństwa danych, takimi jak najnowocześniejsze dostępne szyfrowanie. Należy w pełni wykorzystywać wymogi dotyczące uwzględniania ochrony danych w fazie projektowania, a które zostały określone jako domyślne w rozporządzeniu (UE) 2016/679

(52) Narzędzia i aplikacje z zakresu cyberbezpieczeństwa oparte na oprogramowaniu otwartym mogą przyczyniać się do zwiększenia otwartości i pozytywnie wpływać na skuteczność innowacji przemysłowych. Standardy otwarte ułatwiają interoperacyjność między narzędziami bezpieczeństwa, z korzyścią dla bezpieczeństwa zainteresowanych stron z branży. Narzędzia i aplikacje z zakresu cyberbezpieczeństwa oparte na otwartym oprogramowaniu mogą umożliwić pozyskanie szerszej społeczności programistów, umożliwiając dywersyfikację dostawców. Otwarte oprogramowanie może prowadzić do bardziej przejrzystego procesu weryfikacji narzędzi związanych z cyberbezpieczeństwem oraz do kierowanego przez społeczność procesu wykrywania podatności. Państwa członkowskie powinny zatem móc promować wykorzystywanie otwartego oprogramowania i otwartych standardów przez prowadzenie polityki związanej z wykorzystywaniem otwartych danych i otwartego oprogramowania na zasadzie bezpieczeństwa dzięki przejrzystości. Polityka wspierająca wprowadzenie i zrównoważone wykorzystywanie narzędzi z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu ma szczególne znaczenie dla małych i średnich przedsiębiorstw ponoszących znaczne koszty wdrożenia, które można by zminimalizować przez ograniczenie zapotrzebowania na konkretne aplikacje lub narzędzia.

(53) W miastach usługi użyteczności publicznej w coraz większym stopniu łączą się z sieciami cyfrowymi, aby poprawić sieci cyfrowe transportu miejskiego, usprawnić zaopatrzenie w wodę i unieszkodliwianie odpadów oraz zwiększyć efektywność oświetlenia i ogrzewania budynków. Te cyfrowe usługi użyteczności publicznej są narażone na cyberataki, a skuteczny cyberatak grozi obywatelom szkodami na dużą skalę ze względu na wzajemne powiązanie tych usług. W ramach krajowych strategii cyberbezpieczeństwa państwa członkowskie powinny opracować politykę uwzględniającą rozwój takich połączonych z siecią lub inteligentnych miast oraz ich potencjalny wpływ na społeczeństwo.

(54) W ostatnich latach Unia doświadcza gwałtownego wzrostu liczby cyberataków z użyciem oprogramowania typu "ransomware", w których złośliwe oprogramowanie szyfruje dane i systemy oraz domaga się okupu za ich odblokowanie. Coraz większa częstotliwość i dotkliwość cyberataków z użyciem oprogramowania typu „ransomware" może wynikać z szeregu czynników, takich jak różne wzorce ataków, przestępcze modele biznesowe typu „oprogramowanie wymuszające okup jako usługa" i kryptowaluty, żądania okupu oraz wzrost liczby ataków w łańcuchu dostaw. W ramach krajowych strategii cyberbezpieczeństwa państwa członkowskie powinny opracować politykę odnoszącą się do wzrostu liczby cyberataków z wykorzystaniem oprogramowania typu „ransomware".

(55) Partnerstwa publiczno-prywatne (PPP) w dziedzinie cyberbezpieczeństwa mogą stanowić właściwe ramy służące wymianie wiedzy, dzieleniu się dobrymi praktykami oraz osiągnięciu wspólnego poziomu porozumienia wśród zainteresowanych stron. Państwa członkowskie powinny promować politykę wspierającą tworzenie PPP w dziedzinie cyberbezpieczeństwa. W ramach takiej polityki należy sprecyzować między innymi zakres i zainteresowane strony, model zarządzania, dostępne warianty finansowania oraz interakcje między uczestniczącymi zainteresowanymi stronami w odniesieniu do PPP. PPP mogą wykorzystywać wiedzę specjalistyczną podmiotów z sektora prywatnego, aby pomagać właściwym organom w opracowywaniu usług i procesów zgodnie z najnowszym stanem wiedzy, obejmujących wymianę informacji, wczesne ostrzeganie, ćwiczenia w zakresie cyberzagrożeń i incydentów, zarządzanie kryzysowe i planowanie odporności.

(56) W krajowych strategiach cyberbezpieczeństwa państwa członkowskie powinny uwzględniać szczególne potrzeby małych i średnich przedsiębiorstw związane z cyberbezpieczeństwem. W całej Unii małe i średnie przedsiębiorstwa stanowią znaczny odsetek rynku przemysłu oraz gospodarki i często mają trudności, by dostosować się do nowych praktyk biznesowych w coraz bardziej cyfrowym świecie i do środowiska cyfrowego, z pracownikami pracującymi z domów, a działalnością gospodarczą w coraz większym stopniu prowadzoną w internecie. Niektóre małe i średnie przedsiębiorstwa mierzą się ze szczególnymi wyzwaniami w zakresie cyberbezpieczeństwa, takimi jak niska świadomość zagadnień cyberbezpieczeństwa, brak zdalnych zabezpieczeń informatycznych, wysokie koszty rozwiązań dotyczących cyberbezpieczeństwa oraz zwiększony poziom zagrożeń, np. oprogramowanie wymuszające okup, w związku z czym powinny otrzymywać wskazówki i pomoc. Małe i średnie przedsiębiorstwa coraz częściej stają się celem ataków w łańcuchu dostaw ze względu na ich niewystarczający poziom zarządzania ryzykiem w cyberbezpieczeństwie i zarządzania w razie ataków oraz fakt, że mają one ograniczony dostęp do zasobów na potrzeby bezpieczeństwa. Takie ataki w łańcuchu dostaw wpływają nie tylko na małe i średnie przedsiębiorstwa i działalność każ-

dego z nich z osobna, lecz także mogą mieć efekt kaskadowy w postaci większych ataków na zaopatrywane przez nie podmioty. Państwa członkowskie powinny, za pośrednictwem krajowych strategii cyberbezpieczeństwa, pomagać małym i średnim przedsiębiorstwom w reagowaniu na wyzwania dotyczące łańcuchów dostaw. Państwa członkowskie powinny posiadać punkt kontaktowy dla małych i średnich przedsiębiorstw na szczeblu krajowym lub regionalnym, który zapewniałby wskazówki i pomoc małym i średnim przedsiębiorstwom albo kierowałby je do właściwych organów udzielających wskazówek i pomocy w sprawach związanych z cyberbezpieczeństwem. Państwa członkowskie zachęca się również, aby oferowały usługi takie jak konfiguracja stron internetowych i funkcje logowania małym przedsiębiorstwom i mikroprzedsiębiorstwom, które nie posiadają tych zdolności.

(57) W ramach krajowych strategii cyberbezpieczeństwa będących częścią szerszej strategii obronnej państwa członkowskie powinny przyjąć politykę promowania aktywnej cyberobrony. W przeciwieństwie do działania reaktywnego aktywna cyberobrona polega na aktywnym zapobieganiu naruszeniom bezpieczeństwa sieci, ich wykrywaniu, monitorowaniu, analizowaniu i ograniczaniu, w połączeniu z wykorzystaniem zdolności rozmieszczonych w sieci, która padła ofiarą ataku, i poza tą siecią. Może to obejmować bezpłatne usługi lub narzędzia, w tym kontrole samoobsługowe, narzędzia wykrywania i usługi usuwania oferowane przez państwa członkowskie niektórym podmiotom. Zdolność do szybkiego i automatycznego przekazywania i rozumienia informacji i analiz dotyczących zagrożeń, do ostrzegania o aktywności w cyberprzestrzeni i do reagowania ma krytyczne znaczenie dla spójności wysiłków na rzecz skutecznego zapobiegania atakom na sieci i systemy informatyczne, ich wykrywania, eliminowania i blokowania. Aktywna cyberobrona opiera się na strategii, która wyklucza środki ofensywne.

(58) Ponieważ wykorzystywanie podatności sieci i systemów informatycznych może powodować znaczące zakłócenia i szkody, ważnym czynnikiem w ograniczaniu ryzyka jest szybkie identyfikowanie takich podatności i ich eliminowanie. Podmioty, które opracowują takie sieci i systemy informatyczne lub administrują nimi, powinny zatem ustanowić odpowiednie procedury postępowania w przypadku wykrycia takich podatności. Ponieważ podatności często są wykrywane i ujawniane przez osoby trzecie, producent lub dostawca produktów ICT 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 29147 zawierają wskazówki odnoszące się do postępowania w przypadku podatności i do ujawniania podatności. Wzmocnienie koordynacji między zgłaszającymi osobami fizycznymi i osobami prawnymi a producentami lub dostawcami produktów ICT lub usług ICT jest szczególnie ważne, aby usprawnić dobrowolne zasady ramowe dotyczące ujawniania podatności. Skoordynowane ujawnianie podatności to ustrukturyzowany proces, w ramach którego podatności są zgłaszane producentowi lub dostawcy potencjalnie podatnych produktów ICT lub usług ICT w sposób umożliwiający im zdiagnozowanie i wyeliminowanie danej podatności, zanim dotyczące jej szczegółowe informacje zostaną ujawnione osobom trzecim lub podane do wiadomości publicznej. Skoordynowane ujawnianie podatności powinno także obejmować koordynację między zgłaszającymi osobami fizycznymi lub osobami prawnymi a producentem lub dostawcą potencjalnie podatnych produktów ICT lub usług ICT w odniesieniu do harmonogramu eliminowania podatności i podawania ich do wiadomości publicznej.

(59) Komisja, ENISA i państwa członkowskie powinny nadal wspierać dostosowanie do norm międzynarodowych i istniejących dobrych praktyk branżowych w dziedzinie zarządzania ryzykiem w cyberbezpieczeństwie, na przykład w takich dziedzinach jak oceny bezpieczeństwa łańcucha dostaw, wymiana informacji i ujawnianie podatności.

(60) Państwa członkowskie we współpracy z ENISA powinny podjąć działania w celu ułatwienia skoordynowanego ujawniania podatności przez ustanowienie odpowiedniej polityki krajowej. W ramach polityki krajowej państwa członkowskie powinny w miarę możliwości dążyć do wyeliminowania problemów, z którymi mierzą się osoby prowadzące badania kwestii podatności, w tym ich potencjalnego narażenia na odpowiedzialność karną, zgodnie prawem krajowym. W związku z tym, że osoby fizyczne i prawne wyszukujące podatności mogą w niektórych państwach członkowskich być narażone na odpowiedzialność karną i cywilną, zachęca się państwa członkowskie do przyjęcia wytycznych przewidujących odstąpienie od postępowania cywilnego lub karnego wobec osób prowadzących badania kwestii podatności i bezpieczeństwa informacji oraz zwolnienie ich z odpowiedzialności cywilnej lub karnej za te działania.

(61) Państwa członkowskie powinny wyznaczyć jeden ze swoich CSIRT do pełnienia roli koordynatora, występującego w razie potrzeby w charakterze zaufanego pośrednika między zgłaszającymi osobami fizycznymi lub prawnymi a producentami lub dostawcami produktów ICT lub usług ICT, na które podatność może mieć wpływ. Zadania CSIRT wyznaczonego do roli koordynacyjnej powinny obejmować identyfikację danych podmiotów i kontaktowanie się z nimi, udzielanie pomocy osobom fizycznym i prawnym zgłaszającym podatność, negocjowanie harmonogramu ujawniania oraz zarządzanie podatnościami, których skutki dotykają wielu podmiotów (wielostronne skoor-

dynowane ujawnianie podatności). Jeżeli zgłoszona podatność może mieć znaczący wpływ na podmioty w więcej niż jednym państwie członkowskim, CSIRT wyznaczone na koordynatorów powinny w stosownych przypadkach współpracować w ramach sieci CSIRT.

(62) Dostęp do prawidłowych i terminowych informacji na temat podatności dotyczących produktów ICT i usług ICT pozwala usprawnić zarządzanie ryzykiem w cyberbezpieczeństwie. Ważnym narzędziem dla podmiotów i użytkowników ich usług, ale również dla właściwych organów i CSIRT są źródła publicznie dostępnych informacji na temat podatności. Z tego powodu ENISA powinna ustanowić europejską bazę danych dotyczących podatności, w której podmioty, niezależnie czy są objęte zakresem stosowania niniejszej dyrektywy oraz ich dostawcy sieci i systemów informatycznych, jak również właściwe organy i CSIRT, mogłyby na zasadzie dobrowolności ujawniać i rejestrować publicznie znane podatności, aby umożliwić użytkownikom wprowadzanie odpowiednich środków ograniczających ryzyko. Celem tej bazy danych jest reagowanie na wyjątkowe wyzwania wynikające z ryzyka dla podmiotów unijnych. Ponadto ENISA powinna ustanowić właściwą procedurę dotyczącą procesu publikacji, aby dać podmiotom czas na zastosowanie środków ograniczających ich podatność i najnowocześniejszych dostępnych środków zarządzania ryzykiem w cyberbezpieczeństwie, a także zbiorów danych nadających się do odczytu maszynowego i odpowiednich interfejsów. Aby wspierać kulturę ujawniania podatności, ujawnianie nie powinno mieć negatywnych skutków dla zgłaszającej osoby fizycznej lub osoby prawnej.

(63) Choć istnieją podobne rejestry podatności lub bazy danych dotyczących podatności, są one prowadzone i obsługiwane przez podmioty, które nie mają miejsca prowadzenia działalności w Unii. Europejska baza danych dotyczących podatności obsługiwana przez ENISA zapewniłaby lepszą przejrzystość w odniesieniu do procesu publikacji poprzedzającego publiczne ujawnienie podatności, a także odporność w przypadku zakłócenia lub przerwy w świadczeniu podobnych usług. Aby w miarę możliwości uniknąć powielania podejmowanych działań i dążyć do komplementarności, ENISA powinna zbadać możliwość zawarcia umów o ustrukturyzowanej współpracy z podobnymi rejestrami lub bazami danych podlegającymi jurysdykcji państw trzecich. ENISA powinna w szczególności zbadać możliwość ścisłej współpracy z operatorami systemu wspólnych podatności i zagrożeń (CVE).

(64) Grupa Współpracy powinna wspierać i ułatwiać współpracę strategiczną i wymianę informacji między państwami członkowskimi, a także zwiększać wśród nich zaufanie i pewność. Co dwa lata Grupa Współpracy powinna opracowywać program prac. Program ten powinien obejmować działania, które mają zostać podjęte przez Grupę Współpracy z myślą o realizacji jej celów i zadań. Aby uniknąć potencjalnych zakłóceń w pracy Grupy Współpracy, ramy czasowe opracowania pierwszego programu prac wprowadzonego na podstawie niniejszej dyrektywy należy zharmonizować z ramami czasowymi ostatniego programu prac opracowanego na podstawie dyrektywy (UE) 2016/1148.

(65) 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 – w szczególności dotyczące łatwiejszej harmonizacji aktów transponujących niniejszą dyrektywę w państwach członkowskich – które należy uwzględnić w ramach lepszego wdrażania istniejących przepisów. Grupa Współpracy mogłaby też ewidencjonować rozwiązania krajowe, aby promować kompatybilność rozwiązań w dziedzinie cyberbezpieczeństwa mających zastosowanie do każdego z poszczególnych sektorów w całej Unii. Jest to szczególnie istotne dla sektorów o charakterze międzynarodowym lub transgranicznym.

(66) Grupa Współpracy powinna pozostać elastycznym forum i być w stanie reagować na zmieniające się i nowe priorytety i wyzwania dotyczące polityki, przy jednoczesnym uwzględnieniu dostępności zasobów. Mogłaby ona organizować regularne wspólne spotkania z odpowiednimi zainteresowanymi stronami z sektora prywatnego z całej Unii, aby omawiać działania realizowane przez Grupę Współpracy oraz zbierać dane i informacje na temat pojawiających się wyzwań dotyczących polityki. Ponadto Grupa Współpracy powinna prowadzić regularne oceny aktualnej sytuacji związanej z cyberzagrożeniami lub incydentami, np. obejmującymi wykorzystanie oprogramowania typu „ransomware". Aby zacieśnić współpracę na szczeblu unijnym, Grupa Współpracy powinna rozważyć zaproszenie do uczestnictwa w swoich pracach właściwych instytucji, organów, urzędów i agencji Unii zaangażowanych w politykę

cyberbezpieczeństwa, takich jak Parlament Europejski, Europol, Europejska Rada Ochrony Danych, Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego ustanowiona rozporządzeniem (UE) 2018/1139 oraz Agencja Unii Europejskiej ds. Programu Kosmicznego ustanowiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/696 ([14]).

(67) Właściwe organy i CSIRT powinny móc uczestniczyć w programach wymiany dla urzędników z innych państw członkowskich – w konkretnych ramach i, w stosownych przypadkach, pod warunkiem posiadania poświadczenia bezpieczeństwa przez urzędników uczestniczących w takich programach wymiany – z myślą o usprawnieniu współpracy i zwiększeniu zaufania między państwami członkowskimi. Właściwe organy powinny podejmować działania niezbędne do zapewnienia urzędnikom z innych państw członkowskich możliwości skutecznego angażowania się w działalność przyjmującego właściwego organu lub przyjmującego CSIRT.

(68) Państwa członkowskie powinny wnosić wkład w ustanowienie unijnych ram reagowania w sytuacji kryzysu cybernetycznego, o których mowa w zaleceniu Komisji (UE) 2017/1584 ([15]), poprzez istniejące sieci współpracy, w szczególności Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe), sieć CSIRT i Grupę Współpracy. EU-CyCLONe i sieć CSIRT powinny współpracować w oparciu o uzgodnienia proceduralne, które określają szczegóły tej współpracy i unikać powielania zadań. W regulaminie EU-CyCLONe należy bardziej szczegółowo określić tryb funkcjonowania tej sieci, w tym role sieci, sposoby 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 zintegrowanych uzgodnieniach UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych na podstawie decyzji wykonawczej Rady (UE) 2018/1993 ([16]) (uzgodnienia 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, należy uruchomić mechanizm reagowania kryzysowego Europejskiej Służby Działań Zewnętrznych.

(69) Zgodnie z załącznikiem do zalecenia (UE) 2017/1584 incydent w cyberbezpieczeństwie na dużą skalę powinien oznaczać incydent, który powoduje poziom zakłóceń przekraczający zdolność danego państwa członkowskiego do reakcji lub który ma znaczący wpływ na co najmniej dwa państwa członkowskie. W zależności od przyczyny i wpływu incydenty na dużą skalę mogą przerodzić się w prawdziwe kryzysy uniemożliwiające prawidłowe funkcjonowanie rynku wewnętrznego lub stanowiące poważne zagrożenie dla bezpieczeństwa publicznego i ryzyko dla bezpieczeństwa podmiotów lub obywateli w kilku państwach członkowskich lub w całej Unii. Biorąc pod uwagę szeroki zakres oraz, w większości przypadków, transgraniczny charakter takich incydentów, państwa członkowskie i odpowiednie instytucje, organy, urzędy i agencje Unii powinny współpracować na poziomie technicznym, operacyjnym i politycznym w celu odpowiedniej koordynacji reakcji w całej Unii.

(70) Incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę na poziomie Unii wymagają skoordynowanych działań w celu zapewnienia szybkiej i skutecznej reakcji ze względu na wysoki stopień współzależności między sektorami i państwami członkowskimi. Dostępność sieci i systemów informatycznych odpornych na cyberzagrożenia oraz dostępność, poufność i integralność danych mają zasadnicze znaczenie dla bezpieczeństwa Unii oraz dla ochrony jej obywateli, przedsiębiorstw i instytucji przed incydentami i cyberzagrożeniami, a także dla zwiększenia zaufania osób fizycznych i organizacji do zdolności Unii do promowania i ochrony globalnej, otwartej, wolnej, stabilnej i bezpiecznej cyberprzestrzeni opartej na prawach człowieka, podstawowych wolnościach, demokracji i praworządności.

([14]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/696 z dnia 28 kwietnia 2021 r. ustanawiające program kosmiczny Unii i Agencję Unii Europejskiej ds. Programu Kosmicznego oraz uchylające rozporządzenia (UE) nr 912/2010, (UE) nr 1285/2013, (UE) nr 377/2014 i decyzję nr 541/2014/UE (Dz.U. L 170 z 12.5.2021, s. 69).

([15]) Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L239 z 19.9.2017, s. 36).

([16]) Decyzja wykonawcza Rady (UE) 2018/1993 z dnia 11 grudnia 2018 r. w sprawie zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (Dz.U. L 320 z 17.12.2018, s. 28).

(71) EU-CyCLONe powinna pośredniczyć między poziomem technicznym i politycznym podczas incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę oraz zacieśnić współpracę na szczeblu operacyjnym i wspierać proces decyzyjny na szczeblu politycznym. We współpracy z Komisją, uwzględniając kompetencje Komisji w dziedzinie zarządzania kryzysowego, EU-CyCLONe powinna opierać się na ustaleniach sieci CSIRT i wykorzystywać własne zdolności do sporządzania analizy skutków incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę.

(72) Cyberataki mają charakter transgraniczny, a poważne incydenty mogą zakłócać i uszkadzać krytyczną infrastrukturę informatyczną, od której zależy sprawne funkcjonowanie rynku wewnętrznego. Zalecenie (UE) 2017/1584 odnosi się do roli wszystkich właściwych podmiotów. Ponadto Komisja odpowiada, w ramach Unijnego Mechanizmu Ochrony Ludności ustanowionego decyzją Parlamentu Europejskiego i Rady nr 1313/2013/UE ([17]), za ogólne działania dotyczące gotowości, w tym zarządzanie Centrum Koordynacji Reagowania Kryzysowego i wspólnym systemem łączności i informacji w sytuacjach nadzwyczajnych, utrzymywanie i dalszy rozwój zdolności w zakresie świadomości i analizy sytuacyjnej oraz tworzenie zdolności do mobilizacji i wysyłania zespołów ekspertów w razie wniosku o pomoc ze strony państwa członkowskiego lub państwa trzeciego oraz zarządzanie tymi zdolnościami. Komisja odpowiada też za przedstawianie sprawozdań analitycznych dotyczących uzgodnień IPCR na podstawie decyzji wykonawczej (UE) 2018/1993, w tym w odniesieniu do analizy sytuacyjnej i gotowości w zakresie cyberbezpieczeństwa, a także do analizy sytuacyjnej i reagowania kryzysowego w następujących obszarach: rolnictwo, niekorzystne warunki pogodowe, mapowanie i prognozowanie konfliktów, systemy wczesnego ostrzegania w przypadku klęsk żywiołowych, stany zagrożenia zdrowia, nadzór nad chorobami zakaźnymi, zdrowie roślin, incydenty chemiczne, bezpieczeństwo żywności i pasz, zdrowie zwierząt, migracja, cła, zagrożenia jądrowe i radiologiczne i energetyka.

(73) Unia może, 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, sieci CSIRT oraz EU-CyCLONe. Umowy takie powinny gwarantować interesy Unii i odpowiednią ochronę danych. Nie powinno to wykluczać prawa państw członkowskich do współpracy z państwami trzecimi przy zarządzaniu podatnościami i zarządzaniu ryzykiem w cyberbezpieczeństwie, ułatwianiu zgłaszania i ogólnej wymianie informacji zgodnie z prawem Unii.

(74) Aby ułatwić skuteczne wdrażanie niniejszej dyrektywy między innymi w odniesieniu do zarządzania podatnościami, środków zarządzania ryzykiem w cyberprzestrzeni, obowiązków w zakresie zgłaszania incydentów oraz mechanizmów wymiany informacji na temat cyberbezpieczeństwa, państwa członkowskie mogą współpracować z państwami trzecimi i podejmować działania uznane za odpowiednie do tego celu, obejmujące wymianę informacji dotyczących cyberzagrożeń, incydentów, podatności, narzędzi i metod, taktyki, technik i procedur, gotowości i ćwiczeń dotyczących zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa, szkolenia, budowania zaufania i ustrukturyzowanych mechanizmów wymiany informacji.

(75) Należy wprowadzić oceny wzajemne aby pomóc w wyciąganiu wniosków ze wspólnych doświadczeń, wzmocnić wzajemne zaufanie i osiągnąć wysoki wspólny poziom cyberbezpieczeństwa. Efektem ocen wzajemnych mogą być wartościowe spostrzeżenia i zalecenia służące wzmocnieniu ogólnych zdolności w zakresie cyberbezpieczeństwa, tworzące kolejną funkcjonalną ścieżkę wymiany dobrych praktyk między państwami członkowskimi i przyczyniające się do zwiększenia poziomu dojrzałości państw członkowskich w dziedzinie cyberbezpieczeństwa. Ponadto w ocenach wzajemnych należy uwzględniać wyniki podobnych mechanizmów, takich jak system oceny wzajemnej sieci CSIRT, oraz należy zapewniać wartość dodaną i unikać powielania działań. Stosowanie ocen wzajemnych powinno pozostawać bez uszczerbku dla unijnych lub krajowych przepisów dotyczących ochrony informacji poufnych lub niejawnych.

(76) Grupa Współpracy powinna ustanowić metodykę oceny własnej dla państw członkowskich, starając się uwzględnić takie czynniki jak: poziom wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie i obowiązków sprawozdawczych, poziom zdolności i skuteczność wykonywania zadań przez właściwe organy, zdolności operacyjne CSIRT, poziom wdrożenia wzajemnej pomocy, poziom wdrożenia mechanizmów wymiany informacji o cyberbezpieczeństwie lub szczególne kwestie o charakterze transgranicznym lub międzysektorowym. Należy zachęcać państwa członkowskie, aby regularnie przeprowadzały ocenę własną oraz przedstawiały i omawiały wyniki swojej oceny własnej na forum Grupy Współpracy.

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

(77) Odpowiedzialność za zapewnienie bezpieczeństwa sieci i systemów informatycznych w dużym stopniu spoczywa na podmiotach kluczowych i ważnych. Należy wspierać i rozwijać kulturę zarządzania ryzykiem, obejmującą szacowanie ryzyka i wdrażanie środków zarządzania ryzykiem w cyberbezpieczeństwie odpowiednich dla danego ryzyka.

(78) Środki zarządzania ryzykiem w cyberbezpieczeństwie powinny uwzględniać stopień zależności podmiotu kluczowego lub ważnego od sieci i systemów informatycznych i obejmować środki mające na celu identyfikację ryzyka wystąpienia incydentów, zapobieganie incydentom, wykrywanie ich, reagowanie na nie i przywracanie normalnego działanie po ich wystąpieniu oraz łagodzenie ich skutków. Bezpieczeństwo sieci i systemów informatycznych powinno obejmować bezpieczeństwo danych przechowywanych, przekazywanych i przetwarzanych. Środki zarządzania ryzykiem w cyberbezpieczeństwie powinny umożliwiać analizę systemową z uwzględnieniem czynnika ludzkiego, aby dawać kompletny obraz bezpieczeństwa sieci i systemu informatycznego.

(79) Ponieważ zagrożenia bezpieczeństwa sieci i systemów informatycznych mogą mieć różne źródła, środki zarządzania ryzykiem w cyberbezpieczeństwie powinny opierać się na podejściu uwzględniającym wszystkie zagrożenia, mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed zdarzeniami takimi jak kradzież, pożar, powódź, awaria telekomunikacyjna bądź awaria zasilania lub nieuprawniony dostęp fizyczny do infrastruktury związanej z informacjami i przetwarzaniem informacji należącej do podmiotu kluczowego lub ważnego, jej uszkodzenie i ingerencja w nią, które to zdarzenia mogłyby naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub też usług oferowanych przez sieci i systemy informatyczne lub dostępnych za pośrednictwem sieci i systemów informatycznych. Środki zarządzania ryzykiem w cyberbezpieczeństwie powinny zatem dotyczyć również bezpieczeństwa fizycznego i środowiskowego sieci i systemów informatycznych przez włączenie środków ochrony takich systemów przed awariami, błędem ludzkim, złośliwymi działaniami lub zjawiskami naturalnymi, zgodnie z normami europejskimi i międzynarodowymi, takimi jak normy zawarte w serii ISO/IEC 27000. W związku z tym w ramach swoich środków zarządzania ryzykiem w cyberbezpieczeństwie podmioty kluczowe i ważne powinny zająć się również bezpieczeństwem zasobów ludzkich i prowadzić odpowiednią politykę kontroli dostępu. Środki te powinny być zgodne z dyrektywą (UE) 2022/2557.

(80) W celu wykazania zgodności ze środkami zarządzania ryzykiem w cyberbezpieczeństwie i w razie braku odpowiednich europejskich programów certyfikacji cyberbezpieczeństwa przyjętych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 ([18]) państwa członkowskie powinny, w porozumieniu z Grupą Współpracy i Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa, promować stosowanie odpowiednich norm europejskich i międzynarodowych przez podmioty kluczowe i ważne lub mogą wymagać od podmiotów korzystania z certyfikowanych produktów ICT, usług ICT i procesów ICT.

(81) Aby uniknąć nakładania nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na podmioty kluczowe i ważne, środki zarządzania ryzykiem w cyberbezpieczeństwie powinny być proporcjonalne do ryzyka, jakie zagraża danym sieciom i systemom informatycznym, przy czym należy uwzględniać najnowszy stan wiedzy na temat takich środków oraz, w stosownych przypadkach, normy europejskie i międzynarodowe, a także koszt ich wdrożenia.

(82) Środki zarządzania ryzykiem w cyberbezpieczeństwie powinny być proporcjonalne do stopnia narażenia podmiotu kluczowego lub ważnego na ryzyko oraz do wpływu społecznego i gospodarczego, jaki wywarłby incydent. Przy ustanawianiu środków zarządzania ryzykiem w cyberprzestrzeni dostosowanych do podmiotów kluczowych i ważnych należy odpowiednio uwzględnić odmienne czynniki narażenia na ryzyko w przypadku podmiotów kluczowych i ważnych, takie jak krytyczność danego podmiotu, ryzyko, w tym ryzyko społeczne, na które jest on narażony, wielkość podmiotu oraz prawdopodobieństwo wystąpienia incydentów i ich dotkliwość, w tym ich skutki społeczne i gospodarcze.

([18]) 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).

(83) Podmioty kluczowe i ważne powinny zapewniać bezpieczeństwo sieci i systemów informatycznych, których używają w swojej działalności. Systemy te to przede wszystkim prywatne sieci i systemy informatyczne, którymi zarządza własny personel informatyczny podmiotów kluczowych i ważnych lub w których zapewnienie bezpieczeństwa zlecono na zewnątrz. Środki zarządzania ryzykiem w cyberbezpieczeństwie i obowiązki dotyczące zgłaszania incydentów określone w niniejszej dyrektywie powinny mieć zastosowanie do właściwych podmiotów kluczowych i ważnych bez względu na to, czy te podmioty zapewniają utrzymanie swoich sieci i systemów informatycznych, czy też zlecają ich utrzymanie na zewnątrz.

(84) Zważywszy na ich transgraniczny charakter, dostawcy usług DNS, podmioty świadczące usługi rejestracji nazw domen dla TLD, dostawcy usług chmurowych, dostawcy usług ośrodka przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie bezpieczeństwa, dostawcy internetowych platform handlowych, wyszukiwarek internetowych oraz platform usług sieci społecznościowych, oraz dostawcy usług zaufania powinni podlegać daleko idącej harmonizacji na poziomie Unii. Wdrażanie środków zarządzania ryzykiem w cyberbezpieczeństwie w odniesieniu do tych podmiotów należy zatem ułatwić za pomocą aktu wykonawczego.

(85) Zaradzenie ryzyku wynikającemu z łańcucha dostaw danego podmiotu i jego powiązań z dostawcami – takimi jak dostawcy usług przechowywania i przetwarzania danych lub dostawcy usług zarządzanych w zakresie bezpieczeństwa oraz edytorzy oprogramowania – jest szczególnie istotne z uwagi na częstość incydentów, w których podmioty są ofiarami cyberataków i w których agresorzy są w stanie złamać zabezpieczenia sieci i systemów informatycznych danego podmiotu, wykorzystując podatności występujące w produktach i usługach osób trzecich. Dlatego podmioty kluczowe i ważne powinny oceniać i uwzględniać ogólną jakość i odporność produktów i usług oraz środków zarządzania ryzykiem w cyberbezpieczeństwie stanowiący ich część, a także praktyki dotyczące cyberbezpieczeństwa stosowane przez dostawców produktów i usług, w tym ich procedury bezpiecznego opracowywania. Podmioty kluczowe i ważne należy w szczególności zachęcać, aby włączały środki zarządzania ryzykiem w cyberbezpieczeństwie do ustaleń umownych z bezpośrednimi dostawcami i usługodawcami. Podmioty te mogłyby rozważyć ryzyko pochodzące od dostawców i usługodawców z innych poziomów.

(86) Wśród dostawców usług szczególnie ważną rolę w pomaganiu podmiotom w działaniach mających na celu zapobieganie incydentom, wykrywanie ich, reagowanie na nie lub przywracanie normalnego działania po ich wystąpieniu odgrywają dostawcy usług zarządzanych w zakresie bezpieczeństwa zajmujący się obszarami takimi jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo. Dostawcy usług zarządzanych w zakresie bezpieczeństwa również sami padają jednak ofiarą cyberataków, a ponieważ ich działalność jest ściśle zintegrowana z operacjami podmiotów, stanowią oni szczególne ryzyko. Dlatego przy wyborze dostawcy usług zarządzanych w zakresie bezpieczeństwa podmioty kluczowe i ważne powinny dochować szczególnej staranności.

(87) Właściwe organy, w kontekście swoich zadań nadzorczych, mogą również korzystać z usług cyberbezpieczeństwa takich jak audyty bezpieczeństwa, testy penetracyjne lub reagowanie na incydenty.

(88) Podmioty kluczowe i ważne powinny również ograniczać ryzyko wynikające z ich interakcji i powiązań z innymi zainteresowanymi stronami w szerszym ekosystemie, w tym w związku z przeciwdziałaniem szpiegostwu przemysłowemu i ochroną tajemnic handlowych. W szczególności podmioty te 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 ogólnie bezpiecznego dostępu do informacji i ich rozpowszechniania, a w szczególności ochrony własności intelektualnej. Podobnie, zważywszy na znaczenie i wartość danych dla działalności podmiotów, jeżeli podmioty kluczowe i ważne wykorzystują usługi przekształcania danych i analizy danych oferowane przez osoby trzecie, wówczas podmioty te powinny stosować odpowiednie środki zarządzania ryzykiem w cyberbezpieczeństwie.

(89) Podmioty kluczowe i ważne powinny przyjąć szeroki wachlarz podstawowych praktyk dotyczących cyberhigieny, takich jak zasady zerowego zaufania, aktualizacje oprogramowania, konfiguracja urządzeń, segmentacja sieci, zarządzanie tożsamością i dostępem lub świadomość użytkowników, organizować szkolenia dla pracowników oraz szerzyć wiedzę na temat cyberzagrożeń, phishingu lub technik inżynierii społecznej. Ponadto podmioty te powinny ocenić własne zdolności w zakresie cyberbezpieczeństwa i w stosownych przypadkach dążyć do integracji technologii poprawiających cyberbezpieczeństwo, takich jak systemy oparte na sztucznej inteligencji lub uczeniu maszynowym, aby poprawić swoje zdolności oraz wzmocnić bezpieczeństwo sieci i systemów informatycznych.

(90) Aby w większym stopniu ograniczyć kluczowe ryzyka w łańcuchu dostaw i pomóc podmiotom kluczowym i ważnym działającym w sektorach objętych niniejszą dyrektywą w odpowiednim zarządzaniu ryzykiem związanym z łańcuchami dostaw i dostawcami, Grupa Współpracy, we współpracy z Komisją i ENISA oraz, w stosownych przypadkach, po konsultacji z właściwymi zainteresowanymi stronami, w tym z przemysłu, powinna przeprowadzić skoordynowane oszacowanie ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw, jak miało to miejsce w przypadku sieci 5G w następstwie zalecenia Komisji (UE) 2019/534 ([19]), w celu identyfikacji w każdym sektorze krytycznych usług ICT, systemów ICT lub produktów ICT, istotnych zagrożeń i podatności. W takich skoordynowanych oszacowaniach ryzyka dla bezpieczeństwa należy określić środki, plany ograniczania ryzyka i najlepsze praktyki dotyczące przeciwdziałania krytycznym zależnościom, potencjalnym pojedynczym punktom awarii, zagrożeniom, podatnościom i innemu ryzyku związanemu z łańcuchem dostaw, a także zbadać sposoby dalszego zachęcania podmiotów kluczowych i ważnych do ich szerszego stosowania. Potencjalne pozatechniczne czynniki ryzyka, takie jak nadmierny wpływ państwa trzeciego na dostawców i usługodawców, w szczególności w przypadku alternatywnych modeli zarządzania, obejmują ukryte podatności lub backdoory oraz potencjalne systemowe zakłócenia dostaw, w szczególności w przypadku blokady technologicznej lub zależności od dostawcy.

(91) W świetle specyfiki danego sektora w skoordynowanych oszacowaniach ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw należy uwzględnić zarówno czynniki techniczne, jak i – w stosownych przypadkach – pozatechniczne, w tym te określone w zaleceniu (UE) 2019/534, w unijnym skoordynowanym oszacowaniu ryzyka dotyczącym cyberbezpieczeństwa sieci 5G oraz w unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G uzgodnionym przez Grupę Współpracy. Aby zidentyfikować łańcuchy dostaw, które należy poddać skoordynowanemu oszacowaniu ryzyka dla bezpieczeństwa, należy wziąć pod uwagę następujące kryteria: (i) zakres, w jakim podmioty kluczowe i ważne wykorzystują konkretne krytyczne usługi ICT, systemy ICT lub produkty ICT i są od nich zależne; (ii) znaczenie konkretnych krytycznych usług ICT, systemów ICT lub produktów ICT dla wykonywania krytycznych lub wrażliwych funkcji, w tym przetwarzania danych osobowych; (iii) dostępność alternatywnych usług ICT, systemów ICT lub produktów ICT; (iv) odporność całego łańcucha dostaw usług ICT, systemów ICT lub produktów ICT, w ciągu ich cyklu życia, na zdarzenia powodujące zakłócenia; (v) w przypadku pojawiających się usług ICT, systemów ICT lub produktów ICT – ich potencjalne przyszłe znaczenie dla działalności podmiotów. Ponadto szczególny nacisk należy położyć na usługi ICT, systemy ICT lub produkty ICT podlegające specjalnym wymogom pochodzącym z państw trzecich.

(92) Aby uprościć obowiązki 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 właściwym organom na podstawie odpowiednio dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 ([20]) oraz rozporządzenia (UE) nr 910/2014 możliwość korzystania z ram prawnych ustanowionych na podstawie niniejszej dyrektywy, co obejmuje wyznaczanie CSIRT odpowiedzialnego za obsługę incydentów oraz uczestnictwo właściwych organów w działaniach Grupy Współpracy i w sieci CSIRT, podmioty te powinny być objęte zakresem stosowania niniejszej dyrektywy. W związku z tym należy uchylić odpowiednie przepisy określone w rozporządzeniu (UE) nr 910/2014 i w dyrektywie (UE) 2018/1972, na których podstawie na te rodzaje podmiotów nałożono wymogi w zakresie bezpieczeństwa i zgłaszania incydentów. Przepisy dotyczące obowiązków w zakresie zgłaszania incydentów określone w niniejszej dyrektywie nie powinny naruszać rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE.

(93) Obowiązki dotyczące cyberbezpieczeństwa określone w niniejszej dyrektywie należy uznać za uzupełniające względem wymogów nałożonych na dostawców usług zaufania na podstawie rozporządzenia (UE) nr 910/2014. Dostawcy usług zaufania powinni być zobowiązani do podjęcia wszelkich odpowiednich i proporcjonalnych środków w celu zarządzania ryzykiem, na jakie narażone są ich usługi, w tym w odniesieniu do klientów i ufających stron trzecich, oraz do zgłaszania incydentów na podstawie niniejszej dyrektywy. Takie obowiązki w zakresie cyberbezpieczeństwa i zgłaszania incydentów powinny również dotyczyć fizycznej ochrony świadczonych usług. Wymogi dotyczące dostawców kwalifikowanych usług zaufania określone w art. 24 rozporządzenia (UE) nr 910/2014 nadal mają zastosowanie.

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

([20]) 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).

(94) Państwa członkowskie mogą powierzyć rolę właściwych organów do spraw usług zaufania organom nadzorczym na podstawie rozporządzenia (UE) nr 910/2014, aby zapewnić ciągłość obecnych praktyk oraz wykorzystać wiedzę i doświadczenie zdobyte podczas stosowania tego rozporządzenia. W takim przypadku, właściwe organy działające na podstawie niniejszej dyrektywy powinny ściśle i terminowo współpracować z tymi organami nadzorczymi przez wymianę odpowiednich informacji, aby zapewnić skuteczny nadzór nad dostawcami usług zaufania i przestrzeganie przez nich wymogów określonych w niniejszej dyrektywie i w rozporządzeniu (UE) nr 910/2014. W stosownych przypadkach CSIRT lub właściwy organ na podstawie niniejszej dyrektywy powinien niezwłocznie poinformować organ nadzorczy na podstawie rozporządzenia (UE) nr 910/2014 o każdym zgłoszonym poważnym cyberzagrożeniu lub incydencie mającym wpływ na usługi zaufania, a także o każdym przypadku naruszenia niniejszej dyrektywy przez dostawcę usług zaufania. W celu zgłoszeń państwa członkowskie mogą korzystać, w stosownych przypadkach, z pojedynczego punktu zgłaszania utworzonego w celu zapewnienia wspólnego i automatycznego zgłaszania incydentów zarówno organowi nadzorczemu na podstawie rozporządzenia (UE) nr 910/2014, jak i CSIRT lub właściwemu organowi na podstawie niniejszej dyrektywy.

(95) W stosownych przypadkach i aby uniknąć niepotrzebnych zakłóceń, przy transpozycji niniejszej dyrektywy należy uwzględniać istniejące wytyczne krajowe przyjęte w celu transpozycji przepisów art. 40 i 41 dyrektywy (UE) 2018/1972 dotyczących środków bezpieczeństwa, bazując na wiedzy i umiejętnościach już zdobytych w związku z dyrektywą (UE) 2018/1972 w odniesieniu do środków bezpieczeństwa i zgłaszania incydentów. ENISA może również opracować wskazówki dotyczące wymogów dotyczących bezpieczeństwa i obowiązku zgłaszania incydentów dla dostawców publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej, aby ułatwić harmonizację i proces przejścia oraz zminimalizować zakłócenia. Państwa członkowskie na mocy dyrektywy (UW) 2018/1972 mogą powierzyć rolę właściwych organów do spraw łączności elektronicznej krajowym organom regulacyjnym, aby zapewnić ciągłość obecnych praktyk oraz wykorzystać wiedzę i doświadczenie zdobyte w wyniku wdrożenia tej dyrektywy.

(96) Zważywszy na rosnące znaczenie usług łączności interpersonalnej niewykorzystujących numerów zdefiniowanych w dyrektywie (UE) 2018/1972, należy zapewnić, aby usługi te podlegały również odpowiednim wymogom w zakresie bezpieczeństwa z uwagi na ich szczególny charakter i istotną rolę w gospodarce. Ponieważ obszar podatny na ataki stale się rozszerza, usługi łączności interpersonalnej niewykorzystujące numerów, takie jak komunikatory, stają się powszechnymi wektorami ataku. Cyberprzestępcy wykorzystują platformy do komunikacji i nakłaniania ofiar do otwierania niezabezpieczonych stron internetowych, co zwiększa prawdopodobieństwo incydentów związanych z wykorzystaniem danych osobowych, a tym samym naruszających bezpieczeństwo sieci i systemów informatycznych. Dostawcy usług łączności interpersonalnej niewykorzystujących numerów powinni zatem również zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do stwarzanego ryzyka. Zważywszy, że dostawcy usług łączności interpersonalnej niewykorzystujących numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach, stopień ryzyka zachodzącego 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 łączności interpersonalnej zgodnie z definicją w dyrektywie (UE) 2018/1972 wykorzystujących numery, którzy nie sprawują rzeczywistej kontroli nad transmisją sygnałów.

(97) Rynek wewnętrzny jest bardziej niż kiedykolwiek uzależniony od funkcjonowania internetu. Usługi niemal wszystkich podmiotów kluczowych i ważnych zależą od usług świadczonych przez internet. Aby zapewnić sprawne świadczenie usług przez podmioty kluczowe i ważne, wszyscy dostawcy publicznych sieci łączności elektronicznej powinni dysponować odpowiednimi środkami zarządzania ryzykiem w cyberbezpieczeństwie i zgłaszać poważne incydenty w tym zakresie. Państwa członkowskie powinny zapewnić utrzymanie bezpieczeństwa publicznych sieci łączności elektronicznej oraz ochronę ich żywotnych interesów bezpieczeństwa przed sabotażem i szpiegostwem. Ponieważ łączność międzynarodowa wzmacnia i przyspiesza konkurencyjną cyfryzację Unii i jej gospodarki, incydenty mające wpływ na podmorskie kable komunikacyjne powinny być zgłaszane CSIRT lub, w stosownych przypadkach, właściwemu organowi. Krajowe strategie cyberbezpieczeństwa powinny, w stosownych przypadkach, uwzględniać cyberbezpieczeństwo podmorskich kabli komunikacyjnych i obejmować mapowanie potencjalnych zagrożeń cyberbezpieczeństwa oraz środki łagodzące w celu zapewnienia najwyższego poziomu ich ochrony.

(98) Aby zagwarantować bezpieczeństwo publicznych sieci łączności elektronicznej i publicznie dostępnych usług łączności elektronicznej, należy promować korzystanie z technologii szyfrowania, w szczególności szyfrowania end-to-end, a także koncepcje bezpieczeństwa skoncentrowane na danych, takie jak kartografia, segmentacja, tagowanie, polityka dostępu i zarządzanie dostępem oraz automatyczne decyzje o dostępie. W razie konieczności korzystanie z szyfrowania, w szczególności szyfrowania end-to-end, należy uczynić obowiązkowym dla dostawców publicznych sieci łączności elektronicznej i publicznie dostępnych usług łączności elektronicznej zgodnie z zasadami uwzględniania bezpieczeństwa i prywatności w sposób domyślny i na etapie projektowania do celów niniejszej dyrektywy. Korzystanie z szyfrowania end-to-end należy pogodzić z uprawnieniami państw członkowskich do tego, by zapewniać ochronę swoich podstawowych interesów związanych z bezpieczeństwem oraz bezpieczeństwa publicznego, a także umożliwiać zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie oraz ich wykrywanie i ściganie zgodnie z prawem Unii. Nie powinno to jednak osłabiać szyfrowania end-to-end, które jest technologią kluczową dla skutecznej ochrony danych oraz dla prywatności i bezpieczeństwa łączności.

(99) Aby zagwarantować bezpieczeństwo oraz przeciwdziałać nadużyciom i manipulacjom w publicznych sieciach łączności elektronicznej i w publicznie dostępnych usługach łączności elektronicznej, należy promować stosowanie interoperacyjnych bezpiecznych standardów routingu w celu zapewnienia integralności i niezawodności funkcji routingu w całym środowisku dostawców usług dostępu do internetu.

(100) Aby zagwarantować funkcjonalność i integralność internetu oraz promować bezpieczeństwo i odporność DNS, należy zachęcać właściwe zainteresowane strony, w tym unijne podmioty w sektorze prywatnym, dostawców publicznie dostępnych usług łączności elektronicznej, w szczególności dostawców usług dostępu do internetu, a także dostawców wyszukiwarek internetowych do przyjęcia strategii dywersyfikacji rozwiązywania nazw DNS. Państwa członkowskie powinny również sprzyjać rozwijaniu i korzystaniu z publicznej i bezpiecznej europejskiej usługi resolwera DNS.

(101) W niniejszej dyrektywie określono wieloetapowe podejście do zgłaszania poważnych incydentów, aby zapewnić odpowiednią równowagę między szybkim zgłaszaniem, które pomaga zahamować potencjalne rozprzestrzenianie się poważnych incydentów i pozwala podmiotom kluczowym i ważnym zwrócić się o pomoc, a szczegółowym zgłaszaniem, które umożliwia wyciągnięcie cennych wniosków z poszczególnych incydentów i z czasem poprawia cyberodporność poszczególnych podmiotów i całych sektorów. W tym względzie niniejsza dyrektywa powinna obejmować zgłaszanie incydentów, które – w oparciu o wstępną ocenę przeprowadzoną przez dany podmiot – mogą doprowadzić do dotkliwych zakłóceń operacyjnych w usługach bądź do strat finansowych tego podmiotu lub dotknąć inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe lub niemajątkowe. W takiej ocenie wstępnej należy wziąć pod uwagę między innymi sieci i systemy informatyczne, których dotyczy incydent, a w szczególności ich znaczenie dla świadczenia usług danego podmiotu, dotkliwość i charakterystykę techniczną cyberzagrożenia oraz bazowe podatności, które są wykorzystywane, a także doświadczenia podmiotu z podobnymi incydentami. Wskaźniki takie jak zakres skutków dla funkcjonowania usługi, czas trwania incydentu lub liczba dotkniętych nim odbiorców usług mogą odegrać ważną rolę w ustaleniu, czy zakłócenie operacyjne usługi jest dotkliwe.

(102) Jeżeli podmioty kluczowe lub ważne dowiedzą się o poważnym incydencie, powinny mieć obowiązek wydania wczesnego ostrzeżenia bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin. Po tym wczesnym ostrzeżeniu powinno nastąpić zgłoszenie incydentu. Dane podmioty powinny przekazać zgłoszenie incydentu bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od powzięcia informacji o poważnym incydencie, aby w szczególności zaktualizować informacje zawarte we wczesnym ostrzeżeniu oraz wstępnie ocenić poważny incydent, w tym jego dotkliwość i skutki, a także oznaki naruszenia integralności systemu, jeśli występują. Sprawozdanie końcowe należy złożyć nie później niż miesiąc po zgłoszeniu incydentu. Wczesne ostrzeżenie powinno zawierać tylko informacje niezbędne do tego, by powiadomić CSIRT lub, w stosownych przypadkach, właściwy organ o wystąpieniu incydentu i umożliwić danemu podmiotowi zwrócenie się o pomoc w razie potrzeby. Takie wczesne ostrzeżenie, w stosownych przypadkach, powinno wskazywać, czy istnieje podejrzenie, że poważny incydent jest spowodowany czynami niezgodnymi z prawem lub popełnionymi w złym zamiarze, oraz czy może on mieć skutki transgraniczne. Państwa członkowskie powinny zapewnić, aby obowiązek takiego wczesnego ostrzeżenia lub późniejszego zgłoszenia incydentu nie powodował przekierowania zasobów podmiotu zgłaszającego przeznaczonych na obsługę incydentów, które powinno być traktowane priorytetowo, tak by zapobiec sytuacji, w której obowiązki dotyczące zgłaszania incydentów powodowałyby przekierowanie zasobów przeznaczonych na reagowanie na poważne incydenty albo w inny sposób utrudniałyby działania danego podmiotu w tym zakresie. Jeżeli incydent trwa w chwili składania

sprawozdania końcowego, państwa członkowskie powinny zapewnić, aby dane podmioty przedstawiły w tym czasie sprawozdanie z postępów, a sprawozdanie końcowe w ciągu jednego miesiąca od rozwiązania przez nie poważnego incydentu.

(103) W stosownych przypadkach podmioty kluczowe i ważne powinny niezwłocznie informować odbiorców swoich usług o działaniach lub środkach zaradczych, które mogą oni podjąć, aby ograniczyć ryzyko wynikające z poważnego cyberzagrożenia. W stosownych przypadkach, a w szczególności gdy prawdopodobne jest wystąpienie poważnego cyberzagrożenia, podmioty te powinny poinformować również odbiorców swoich usług o samym zagrożeniu. Wymóg informowania tych odbiorców o poważnych cyberzagrożeniach powinien być spełniany na zasadzie najlepszych starań, lecz nie powinien zwalniać tych podmiotów z obowiązku zastosowania na własny koszt odpowiednich i natychmiastowych środków w celu zapobieżenia lub zaradzenia takim zagrożeniom oraz przywrócenia normalnego poziomu bezpieczeństwa danej usługi. Informacji na temat poważnych cyberzagrożeń należy udzielać bezpłatnie i powinny one być zredagowane w przystępnym języku.

(104) Dostawcy publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej powinni uwzględniać bezpieczeństwo na etapie projektowania i domyślnie oraz informować odbiorców swoich usług o poważnych cyberzagrożeniach i o środkach, które odbiorcy mogą zastosować w celu ochrony bezpieczeństwa swoich urządzeń i połączeń, na przykład przez wykorzystanie szczególnych rodzajów oprogramowania lub technologii szyfrowania.

(105) Proaktywne podejście do cyberzagrożeń jest istotnym elementem zarządzania ryzykiem w cyberbezpieczeństwie, które powinny umożliwiać właściwym organom skuteczne zapobieganie przeradzaniu się cyberzagrożeń w incydenty mogące spowodować znaczne szkody majątkowe lub niemajątkowe. W związku z tym zgłaszanie cyberzagrożeń ma kluczowe znaczenie. Dlatego zachęca się podmioty do dobrowolnego zgłaszania cyberzagrożeń.

(106) Aby uprościć zgłaszanie informacji wymaganych na podstawie niniejszej dyrektywy, a także zmniejszyć obciążenie administracyjne podmiotów, państwa członkowskie powinny zapewnić środki techniczne, takie jak pojedynczy punkt zgłaszania incydentów, systemy zautomatyzowane, formularze internetowe, interfejsy przyjazne dla użytkowników, szablony, specjalne platformy do użytku podmiotów – bez względu na to, czy są one objęte zakresem stosowania niniejszej dyrektywy – na potrzeby przekazywania odpowiednich informacji, które należy zgłosić. Finansowanie unijne wspierające wdrażanie niniejszej dyrektywy, w szczególności w ramach programu „Cyfrowa Europa" ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/694 ([21]), mogłoby obejmować wsparcie dla pojedynczych punktów zgłaszania incydentów. Ponadto podmioty 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 administracyjne, a ponadto mogą rodzić niepewność dotyczącą formatu i procedur dokonywania takich zgłoszeń. Jeżeli utworzony został pojedynczy punkt zgłaszania incydentów, państwa członkowskie zachęca się również do korzystania z tego pojedynczego punktu zgłaszania incydentów bezpieczeństwa zgodnie z wymogami innych unijnych aktów prawnych, takich jak rozporządzenie (UE) 2016/679 i dyrektywa 2002/58/WE. Korzystanie z takiego pojedynczego punktu zgłaszania incydentów bezpieczeństwa na podstawie rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE nie powinno mieć wpływu na stosowanie przepisów rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE, w szczególności przepisów dotyczących niezależności organów, o których mowa w tych aktach. ENISA, we współpracy z Grupą Współpracy, powinna opracować wspólne wzory zgłoszeń w formie wytycznych służących ułatwieniu i usprawnieniu przekazywania informacji, które należy zgłosić na podstawie prawa Unii oraz zmniejszeniu obciążenia administracyjnego podmiotów zgłaszających.

(107) W razie podejrzenia, że incydent ma związek z poważnymi przestępstwami w rozumieniu prawa Unii lub prawa krajowego, państwa członkowskie powinny zachęcać podmioty kluczowe i ważne, w oparciu o mające zastosowanie przepisy z zakresu postępowania karnego zgodnie 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 Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) oraz ENISA.

([21]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa" oraz uchylające decyzję (UE) 2015/2240 (Dz.U. L 166 z 11.5.2021, s. 1).

(108) 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, o których mowa w rozporządzeniu (UE) 2016/679 i dyrektywie 2002/58/WE.

(109) Prowadzenie prawidłowych i kompletnych baz danych dotyczących rejestracji nazw domen (dane WHOIS) oraz zapewnienie zgodnego z prawem dostępu do takich danych jest niezbędne do zapewnienia bezpieczeństwa, stabilności i odporności DNS, co z kolei przyczynia się do wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii. W tym konkretnym celu rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen powinny być zobowiązane do przetwarzania niektórych danych niezbędnych do osiągnięcia tego celu. Takie przetwarzanie powinno stanowić obowiązek prawny w rozumieniu art. 6 ust. 1 lit. c) rozporządzenia (UE) 2016/679. Obowiązek ten pozostaje bez uszczerbku dla możliwości gromadzenia danych dotyczących rejestracji nazw domen do innych celów, na przykład na podstawie ustaleń umownych lub wymogów prawnych ustanowionych w innych przepisach prawa Unii lub prawa krajowego. Obowiązek ten ma na celu stworzenie kompletnego i dokładnego zbioru danych rejestracyjnych i nie powinien skutkować gromadzeniem tych samych danych wielokrotnie. Rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen powinny ze sobą współpracować, aby uniknąć powielania tego zadania.

(110) Dostępność danych dotyczących rejestracji nazw domen dla wnioskodawców ubiegających się o prawnie uzasadniony dostęp, a także możliwość uzyskania przez nich szybkiego dostępu do tych danych mają zasadnicze znaczenie dla zapobiegania nadużywaniu DNS i zwalczania ich, a także dla zapobiegania incydentom oraz ich wykrywania i reagowania na nie. Przez wnioskodawcę ubiegającego się o prawnie uzasadniony dostęp należy rozumieć osobę fizyczną lub prawną występującą z wnioskiem na podstawie prawa Unii lub prawa krajowego. Mogą to być organy właściwe na mocy niniejszej dyrektywy oraz organy właściwe na mocy prawa Unii lub prawa krajowego do spraw zapobiegania przestępstwom, prowadzenia postępowań w ich sprawie, wykrywania ich i ścigania, a także CERT lub CSIRT. Rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen powinny być zobowiązane umożliwić wnioskodawcom ubiegającym się o prawnie uzasadniony dostęp uzyskanie zgodnego z prawem dostępu do konkretnych danych dotyczących rejestracji nazw domen niezbędnych do celów wniosku o uzyskanie dostępu zgodnie z prawem Unii i prawem krajowym. Do wniosku osób ubiegających się o prawnie uzasadniony dostęp należy dołączyć uzasadnienie pozwalające ocenić konieczność dostępu do danych.

(111) W celu zapewnienia dostępności prawidłowych i kompletnych danych dotyczących rejestracji nazw domen rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen powinny gromadzić dane dotyczące rejestracji nazw domen oraz zapewniać ich integralność i dostępność. W szczególności rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen powinny ustanowić polityki i procedury na potrzeby gromadzenia i utrzymywania prawidłowych i kompletnych danych dotyczących rejestracji nazw domen, a także przeciwdziałać powstawaniu nieprawidłowych danych rejestracyjnych i poprawiać je zgodnie z unijnymi przepisami o ochronie danych. W tych politykach i procedurach należy w miarę możliwości uwzględniać normy opracowane przez struktury zarządzania z udziałem wielu zainteresowanych stron na poziomie międzynarodowym. Rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen powinny przyjąć i stosować wyważone procedury weryfikacji danych dotyczących rejestracji nazw domen. Procedury te powinny odzwierciedlać najlepsze praktyki stosowane w branży oraz, w miarę możliwości, postępy w dziedzinie identyfikacji elektronicznej. Wśród przykładów procedur weryfikacji można wymienić kontrole *ex ante* przeprowadzane w momencie rejestracji oraz kontrole e*x post* przeprowadzane po rejestracji. Rejestry nazw TLD oraz podmioty świadczące usługi rejestracji nazw domen powinny w szczególności zweryfikować co najmniej jeden ze sposobów kontaktu z rejestrującym.

(112) Rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen powinny być zobowiązane podawać do wiadomości publicznej dane dotyczące rejestracji nazw domen nieobjęte zakresem stosowania unijnych przepisów o ochronie danych, takie jak dane dotyczące osób prawnych, zgodnie z preambułą rozporządzenia (UE) 2016/679. W przypadku osób prawnych rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen powinny podawać do wiadomości publicznej co najmniej nazwę rejestrującego i kontaktowy numer telefonu. Należy również podawać kontaktowy adres poczty elektronicznej, pod warunkiem że nie zawiera on żadnych danych osobowych, tak jak w przypadku aliasów poczty elektronicznej lub skrzynek funkcyjnych. Rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen 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 wymagać, aby rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen odpowiadały bez zbędnej zwłoki na wnioski o ujawnienie danych dotyczących rejestracji nazw domen składane przez wnioskodawców ubiegających się o prawnie uzasadniony dostęp. Rejestry nazw TLD i podmioty świadczące 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 wnio-

skodawców ubiegających się o prawnie uzasadniony dostęp. W tych politykach i procedurach należy w miarę możliwości uwzględnić wskazówki i normy opracowane przez struktury zarządzania z udziałem wielu zainteresowanych stron na poziomie międzynarodowym. Procedura uzyskiwania dostępu może 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, bez uszczerbku dla kompetencji Europejskiej Rady Ochrony Danych, podać wytyczne dotyczące takich procedur, uwzględniające w miarę możliwości normy opracowane przez struktury zarządzania z udziałem wielu zainteresowanych stron na poziomie międzynarodowym. Państwa członkowskie powinny zapewnić, aby każdy rodzaj dostępu do danych osobowych i nieosobowych dotyczących rejestracji domen był bezpłatny.

(113) Podmioty objęte zakresem stosowania niniejszej dyrektywy należy uznać za podlegające jurysdykcji państwa członkowskiego, w którym mają miejsce prowadzenia działalności. Jednak dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej należy uznać za podlegających jurysdykcji państwa członkowskiego, w którym świadczą usługi. Należy uznać, że dostawcy usług DNS, rejestry nazw TLD, podmioty świadczące usługi rejestracji nazw domen, dostawcy usług chmurowych, dostawcy usług ośrodka przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie bezpieczeństwa, a także dostawcy internetowych platform handlowych, wyszukiwarek internetowych oraz platform usług sieci społecznościowych podlegają jurysdykcji państwa członkowskiego, w którym mają główne miejsce prowadzenia działalności w Unii. Podmioty administracji publicznej powinny podlegać jurysdykcji państwa członkowskiego, które je ustanowiło. Jeżeli podmiot świadczy usługi lub ma miejsce prowadzenia działalności 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. W przypadku gdy państwa członkowskie sprawują jurysdykcję, nie powinny one nakładać środków egzekwowania przepisów lub kar za to samo zachowanie więcej niż jeden raz, zgodnie z zasadą *ne bis in idem*.

(114) Aby uwzględnić transgraniczny charakter usług i działalności dostawców usług DNS, rejestrów nazw TLD, podmiotów świadczących usługi rejestracji nazw domen, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, a także dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform usług sieci społecznościowych, takie podmioty powinny podlegać jurysdykcji wyłącznie jednego państwa członkowskiego. Jurysdykcja powinna należeć do państwa członkowskiego, w którym dany podmiot ma główne miejsce prowadzenia działalności w Unii. Kryterium miejsca prowadzenia działalności 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 mający 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 takiego głównego miejsca prowadzenia działalności i nie są zatem przesądzającymi kryteriami pozwalającymi ustalić główne miejsce prowadzenia działalności. Należy uznać, że główne miejsce prowadzenia działalności znajduje się w państwie członkowskim, w którym głównie podejmuje się w Unii decyzje związane ze środkami zarządzania ryzykiem w cyberbezpieczeństwie. Będzie ono zazwyczaj odpowiadać miejscu centralnej administracji podmiotów w Unii. Jeżeli nie można ustalić takiego państwa członkowskiego lub jeżeli takich decyzji nie podejmuje się w Unii, należy uznać, że główne miejsce prowadzenia działalności znajduje się w państwie członkowskim, w którym prowadzone są działania w zakresie cyberbezpieczeństwa. Jeżeli nie można ustalić takiego państwa członkowskiego, należy uznać, że główne miejsce prowadzenia działalności znajduje się w państwie członkowskim, w którym dany podmiot prowadzi działalność z największą liczbą pracowników w Unii. Jeżeli usługi świadczy grupa przedsiębiorstw, za główne miejsce prowadzenia działalności grupy przedsiębiorstw należy uznać główne miejsce prowadzenia działalności przedsiębiorstwa sprawującego kontrolę.

(115) W przypadku gdy dostawca publicznych sieci łączności elektronicznej lub dostawca publicznie dostępnych usług łączności elektronicznej świadczy publicznie dostępną rekurencyjną usługę DNS jedynie w ramach usługi dostępu do internetu, dany podmiot należy uznać za podlegający jurysdykcji wszystkich państw członkowskich, w których świadczy usługi.

(116) Jeżeli dostawca usług DNS, rejestr nazw TLD, podmiot świadczący usługi rejestracji nazw domen, dostawca usług chmurowych, dostawca usług ośrodka przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie bezpieczeństwa, a także dostawca internetowych platform handlowych, wyszukiwarek internetowych oraz platform usług sieci społecznościowych, który nie ma miejsca prowadzenia działalności w Unii, oferuje usługi w Unii, powinien on wyznaczyć przedstawiciela. Aby stwierdzić, czy podmiot oferuje usługi w Unii, należy ustalić, czy dany podmiot zamierza oferować usługi osobom w co najmniej jednym państwie członkowskim. Należy uznać, że 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 miejsce prowadzenia działalności. 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 zwracać się do przedstawiciela. Przedstawiciel powinien zostać wyznaczony wyraźnie za pomocą udzielonego przez podmiot pisemnego upoważnienia do występowania w jego imieniu w zakresie jego obowiązków ustanowionych w niniejszej dyrektywie, w tym zgłaszania incydentów.

(117) Aby zapewnić jasny obraz dostawców usług DNS, rejestrów nazw TLD, podmiotów świadczących usługi rejestracji nazw domen, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, a także dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform usług sieci społecznościowych, świadczących w całej Unii usługi podlegające zakresowi stosowania niniejszej dyrektywy, ENISA powinna utworzyć i prowadzić rejestr takich podmiotów, w oparciu o informacje otrzymane przez państwa członkowskie, w stosownych przypadkach za pośrednictwem mechanizmów krajowych ustanowionych dla podmiotów celem ich rejestracji. Pojedyncze punkty kontaktowe powinny przekazywać ENISA informacje i powiadamiać ją o wszelkich ich zmianach. W celu zapewnienia dokładności i kompletności informacji, które powinny być zawarte w tym rejestrze, państwa członkowskie mogą przekazywać ENISA informacje na temat tych podmiotów dostępne we wszelkich rejestrach krajowych. ENISA i państwa członkowskie powinny podjąć środki w celu ułatwienia interoperacyjności takich rejestrów i zapewnić jednocześnie ochronę informacji poufnych lub niejawnych. ENISA powinna ustanowić odpowiednie protokoły klasyfikacji informacji i zarządzania informacjami, aby zapewnić bezpieczeństwo i poufność ujawnianych informacji oraz ograniczyć dostęp do takich informacji, ich przechowywanie i przekazywanie docelowym użytkownikom.

(118) Gdy dochodzi do wymiany, zgłoszenia lub innego rodzaju udostępnienia na podstawie niniejszej dyrektywy informacji, które są niejawne zgodnie z prawem Unii lub prawem krajowym, należy stosować odpowiednie przepisy dotyczące postępowania z informacjami niejawnymi. Ponadto ENISA powinna dysponować infrastrukturą, procedurami i zasadami umożliwiającymi przetwarzanie informacji szczególnie chronionych i niejawnych zgodnie z obowiązującymi przepisami bezpieczeństwa w zakresie ochrony informacji niejawnych UE.

(119) Biorąc pod uwagę, że cyberzagrożenia stają się coraz bardziej złożone i zaawansowane, skuteczne wykrywanie takich zagrożeń i środki zapobiegania im zależą 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 zwiększa zdolność podmiotów do zapobiegania przeradzaniu się takich zagrożeń w incydenty oraz umożliwia podmiotom skuteczniejsze ograniczanie skutków incydentów oraz sprawniejsze przywracanie normalnego działania. Wydaje się, że wobec braku wytycznych na poziomie Unii różne czynniki, w szczególności niepewność co do zgodności z regułami konkurencji i przepisami dotyczącymi odpowiedzialności, ograniczają taką wymianę danych wywiadowczych.

(120) Należy zachęcać podmioty do wspólnego wykorzystywania ich indywidualnej wiedzy i praktycznego doświadczenia na szczeblu strategicznym, taktycznym i operacyjnym – a państwa członkowskie powinny im w tym pomagać – w celu wzmocnienia zdolności podmiotów w zakresie odpowiedniego zapobiegania incydentom, wykrywania ich, reagowania na nie lub przywracania normalnego działania lub łagodzenia skutków incydentów. Należy zatem umożliwić powstawanie na poziomie Unii mechanizmów dobrowolnej wymiany informacji o cyberbezpieczeństwie. W tym celu państwa członkowskie powinny aktywnie wspierać podmioty, takie jak podmioty świadczące usługi i prowadzące badania w zakresie cyberbezpieczeństwa, jak również odpowiednie podmioty nieobjęte zakresem niniejszej dyrektywy, i zachęcać je do uczestnictwa w takich mechanizmach wymiany informacji o cyberbezpieczeństwie. Mechanizmy te należy ustanowić zgodnie z unijnymi regułami konkurencji i unijnymi przepisami o ochronie danych.

(121) Przetwarzanie danych osobowych, w zakresie, w jakim jest to konieczne i proporcjonalne do zapewnienia bezpieczeństwa sieci i systemów informatycznych przez podmioty kluczowe i ważne można uznać za zgodne z prawem na podstawie tego, że takie przetwarzanie jest zgodne z obowiązkiem prawnym, któremu podlega administrator, zgodnie z wymogami art. 6 ust. 1 lit. c) i art. 6 ust. 3 rozporządzenia (UE) 2016/679. Przetwarzanie danych osobowych może być również konieczne ze względu na uzasadnione interesy podmiotów kluczowych i ważnych, a także dostawców technologii i usług w zakresie bezpieczeństwa działających w imieniu tych podmiotów, zgodnie z art. 6 ust. 1 lit. f) rozporządzenia (UE) 2016/679, w tym w przypadku gdy takie przetwarzanie jest niezbędne w związku z mechanizmami wymiany informacji o cyberbezpieczeństwie lub do dobrowolnego zgłaszania odpowiednich informacji zgodnie z niniejszą dyrektywą. Środki związane z zapobieganiem incydentom, ich wykrywaniem i identyfikacją, ograniczaniem ich zasięgu i ich analizowaniem oraz reagowaniem na nie, środki zwiększające świadomość konkretnych cyberzagrożeń, wymianę informacji w kontekście usuwania oraz skoordynowanego ujawniania podatności, 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 mogą wymagać przetwarzania pewnych kategorii danych osobowych, takich jak adresy IP, ujednolicone formaty adresowania zasobów (URL), nazwy domen, adresy poczty elektronicznej oraz znaczniki czasu, w przypadku gdy ujawniane są w nich dane osobowe. Przetwarzanie danych osobowych przez właściwe organy, pojedyncze punkty kontaktowe i CSIRT może stanowić obowiązek prawny lub może zostać uznane za niezbędne do wykonania zadania w interesie publicznym lub sprawowania władzy publicznej powierzonej administratorowi na podstawie art. 6 ust. 1 lit. c) lub e) i art. 6 ust. 3 rozporządzenia (UE) 2016/679 lub do realizacji uzasadnionego interesu podmiotów kluczowych i ważnych, o którym mowa w art. 6 ust. 1 lit. f) tego rozporządzenia. Ponadto w prawie krajowym można ustanowić przepisy umożliwiające właściwym organom, pojedynczym punktom kontaktowym i CSIRT – w zakresie, w jakim jest to konieczne i proporcjonalne do zapewnienia bezpieczeństwa sieci i systemów informatycznych podmiotów kluczowych i ważnych – przetwarzanie szczególnych kategorii danych osobowych zgodnie z art. 9 rozporządzenia (UE) 2016/679, w szczególności poprzez ustanowienie odpowiednich i konkretnych środków ochrony praw podstawowych i interesów osób fizycznych, w tym ograniczeń technicznych w zakresie ponownego wykorzystywania takich danych oraz stosowania najnowocześniejszych środków bezpieczeństwa i ochrony prywatności, takich jak pseudonimizacja lub szyfrowanie, jeżeli anonimizacja może mieć znaczący wpływ na zamierzony cel.

(122) Aby wzmocnić uprawnienia i środki nadzorcze, które pomagają zapewnić faktyczną zgodność z przepisami, w niniejszej dyrektywie należy przewidzieć minimalny wykaz działań i środków nadzorczych, za pomocą których właściwe organy mogą sprawować nadzór nad podmiotami kluczowymi i ważnymi. Ponadto w niniejszej dyrektywie należy wprowadzić rozróżnienie systemów nadzoru mających zastosowanie do podmiotów kluczowych i podmiotów ważnych w celu zapewnienia sprawiedliwej równowagi pod względem obowiązków zarówno po stronie tych podmiotów, jak i właściwych organów. W związku z tym podmioty kluczowe powinny być objęte kompleksowym systemem nadzoru *ex ante* i *ex post*, natomiast podmioty ważne należy objąć uproszczonym systemem nadzoru wyłącznie *ex post*. Od podmiotów ważnych nie należy zatem wymagać, aby systematycznie dokumentowały przestrzeganie środków zarządzania ryzykiem w cyberbezpieczeństwie, natomiast właściwe organy powinny sprawować nadzór w oparciu o podejście reaktywne w trybie *ex post*, a zatem nie powinny mieć ogólnego obowiązku prowadzenia nadzoru nad tymi podmiotami. Nadzór *ex post* nad podmiotami ważnymi może być uruchamiany w oparciu o przekazane właściwym organom dowody, wskazówki lub informacje, gdy na ich podstawie organy te uznają, że zachodzi możliwość naruszenia niniejszej dyrektywy. Takie dowody, wskazówki lub informacje mogą na przykład być w rodzaju tych, jakie są przekazywane właściwym organom przez inne organy, podmioty, obywateli, media lub inne źródła, lub mogą to być informacje dostępne publicznie lub mogą one wynikać z innych działań prowadzonych przez właściwe organy podczas wykonywania ich zadań.

(123) Wykonywanie zadań nadzorczych przez właściwe organy nie powinno niepotrzebnie utrudniać działalności prowadzonej przez dany podmiot. W przypadku gdy właściwe organy wykonują zadania nadzorcze w odniesieniu do podmiotów niezbędnych, w tym prowadzenie kontroli na miejscu i nadzoru zdalnego, badanie naruszeń niniejszej dyrektywy, przeprowadzanie audytów bezpieczeństwa lub skanowanie bezpieczeństwa, powinny one minimalizować wpływ tych czynności na działalność gospodarczą danego podmiotu.

(124) Podczas sprawowania nadzoru *ex ante* właściwe organy powinny mieć możliwość decydowania w proporcjonalny sposób o hierarchii priorytetów w stosowaniu działań i środków nadzorczych, którymi dysponują. Oznacza to, że właściwe organy mogą decydować o takim priorytetowym traktowaniu, stosując metodyki nadzorcze zgodne z podejściem opartym na analizie ryzyka. W szczególności metodyki takie mogłyby obejmować kryteria lub wartości odniesienia dotyczące klasyfikacji podmiotów ważnych pod względem kategorii ryzyka oraz odpowiednie działania i środki nadzorcze zalecane w zależności od kategorii ryzyka, takie jak stosowanie, częstotliwość lub rodzaj kontroli na miejscu, ukierunkowanych audytów bezpieczeństwa lub skanów bezpieczeństwa, rodzaj wymaganych informacji oraz poziom szczegółowości tych informacji. Takim metodykom nadzorczym mogłyby również

towarzyszyć programy prac i mogłyby one podlegać regularnym ocenom i przeglądom, w tym w odniesieniu do takich aspektów jak przydział zasobów i potrzeby. W odniesieniu do podmiotów administracji publicznej uprawnienia nadzorcze powinny być wykonywane zgodnie z krajowymi ramami ustawodawczymi i instytucjonalnymi.

(125) Właściwe organy powinny zapewnić, aby ich zadania nadzorcze w odniesieniu do podmiotów kluczowych i ważnych wykonywali wyszkoleni specjaliści, którzy powinni mieć umiejętności niezbędne do wykonywania tych zadań, w szczególności jeśli chodzi o prowadzenie kontroli na miejscu i nadzoru zdalnego, w tym identyfikacji słabych punktów w bazach danych, sprzęcie, zaporach sieciowych, szyfrowaniu i sieciach. Te kontrole i ten nadzór powinny być prowadzone w sposób obiektywny.

(126) W należycie uzasadnionych przypadkach, gdy właściwy organ wie o poważnym cyberzagrożeniu lub o nadchodzącym ryzyku, powinien on mieć możliwość podjęcia natychmiastowej decyzji o środkach egzekwowania przepisów, aby zapobiec incydentowi lub zareagować na incydent.

(127) W celu zapewnienia skutecznego egzekwowania przepisów należy ustanowić minimalny wykaz uprawnień do egzekwowania, które mogą zostać wykonane w przypadku naruszenia przewidzianych w niniejszej dyrektywie środków zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązków w zakresie zgłaszania incydentów, określając jasne i spójne ramy dotyczące takiego egzekwowania w całej Unii. Należy odpowiednio uwzględniać charakter, wagę oraz czas trwania naruszenia niniejszej dyrektywy, wyrządzone szkody majątkowe i niemajątkowe, to, czy naruszenie było umyślne lub wynikało z niedbalstwa, działania podjęte, aby zapobiec szkodom majątkowym lub niemajątkowym lub je ograniczyć, stopień odpowiedzialności lub mające znaczenie wcześniejsze naruszenia, stopień współpracy z właściwym organem oraz inne okoliczności obciążające lub łagodzące. Środki egzekwowania przepisów, w tym administracyjne kary pieniężne, powinny być proporcjonalne, a ich nakładanie powinno przebiegać z zastrzeżeniem odpowiednich gwarancji proceduralnych zgodnych z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych Unii Europejskiej („Karta"), w tym prawa do skutecznego środka prawnego i do rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony.

(128) Niniejsza dyrektywa nie wymaga od państw członkowskich ustanowienia odpowiedzialności karnej lub cywilnej osób fizycznych odpowiedzialnych za zapewnienie, aby podmiot przestrzegał niniejszej dyrektywy, za szkody poniesione przez osoby trzecie w wyniku naruszenia niniejszej dyrektywy.

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

(130) W przypadku nałożenia administracyjnej kary pieniężnej na podmiot będący przedsiębiorstwem, przez przedsiębiorstwo należy rozumieć do tych celów przedsiębiorstwo zgodnie z art. 101 i 102 TFUE. W przypadku nałożenia administracyjnej kary pieniężnej na osobę niebędącą przedsiębiorstwem, właściwy organ, 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 kar przewidzianych w przepisach krajowych transponujących niniejszą dyrektywę.

(131) 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 Unii Europejskiej.

(132) W sytuacjach, w których niniejsza dyrektywa nie harmonizuje kar administracyjnych, lub w razie potrzeby w innych przypadkach, na przykład w razie poważnego naruszenia niniejszej dyrektywy, państwa członkowskie powinny wdrożyć system przewidujący skuteczne, proporcjonalne i odstraszające kary. Charakter takich kar oraz to, czy są to sankcje karne czy kary administracyjne, należy określić w prawie krajowym.

(133) Aby jeszcze bardziej wzmocnić skuteczność i odstraszający charakter środków egzekwowania przepisów mających zastosowanie do naruszeń niniejszej dyrektywy, właściwe organy powinny być uprawnione do tymczasowego zawieszenia certyfikacji lub zezwolenia dotyczących części lub całości odpowiednich usług świadczonych przez podmiot niezbędny lub prowadzonej przezeń działalności oraz do żądania nałożenia tymczasowego zakazu sprawowania funkcji zarządczych przez osobę fizyczną wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela prawnego. Z uwagi na dotkliwość takich kar i ich wpływ na działalność podmiotów, a ostatecznie na użytkowników, takie tymczasowe zawieszenia lub zakazy należy wyłącznie stosować proporcjonalnie do powagi naruszenia i z uwzględnieniem okoliczności danej sprawy, w tym tego, czy naruszenie było umyślne czy też wynikało z niedbalstwa, oraz działań podjętych, aby zapobiec szkodom majątkowym lub niemajątkowym lub je ograniczyć. Takie tymczasowe zawieszenia lub zakazy należy stosować wyłącznie w ostateczności, tj. po wyczerpaniu innych stosownych środków egzekwowania przepisów przewidzianych w niniejszej dyrektywie, i wyłącznie dopóki podmioty, których to dotyczy, nie podejmą niezbędnych działań w celu usunięcia nieprawidłowości lub nie spełnią wymagań właściwego organu, z których tytułu zastosowano takie tymczasowe zawieszenia lub zakazy. Nakładanie takich tymczasowych zawieszeń lub zakazów powinno stosować się z zastrzeżeniem odpowiednich gwarancji proceduralnych zgodnych z ogólnymi zasadami prawa Unii i z Kartą, w tym prawa do skutecznego środka prawnego i do rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony.

(134) Aby zapewnić wypełnianie przez podmioty obowiązków określonych w niniejszej dyrektywie, państwa członkowskie powinny współpracować ze sobą i pomagać sobie nawzajem w zakresie środków nadzoru i egzekwowania przepisów, w szczególności w przypadku gdy podmiot świadczy usługi w więcej niż jednym państwie członkowskim lub gdy jego sieci i systemy informatyczne znajdują się w państwie członkowskim innym niż państwo, w którym świadczy usługi. Udzielając pomocy, właściwy organ, do którego skierowano wniosek, powinien podjąć środki nadzoru lub egzekwowania przepisów zgodnie z prawem krajowym. W celu zapewnienia sprawnego funkcjonowania wzajemnej pomocy na mocy niniejszej dyrektywy właściwe organy powinny wykorzystywać Grupę Współpracy jako forum do omawiania spraw i konkretnych wniosków o pomoc.

(135) W celu zapewnienia skutecznego nadzoru i egzekwowania przepisów, w szczególności w sytuacjach o wymiarze transgranicznym, państwo członkowskie, które otrzymało wniosek o wzajemną pomoc, powinny – nie wykraczając poza zakres tego wniosku – podjąć odpowiednie środki nadzoru i egzekwowania przepisów w stosunku do podmiotu, który jest przedmiotem wniosku i który świadczy usługi lub ma sieć i system informatyczny na terytorium tego państwa członkowskiego.

(136) Niniejszą dyrektywą należy ustanowić reguły współpracy między właściwymi organami i organami nadzorczymi na mocy rozporządzenia (UE) 2016/679 w celu reagowania na naruszenia niniejszej dyrektywy związane z danymi osobowymi.

(137) Celem niniejszej dyrektywy powinno być zapewnienie wysokiego poziomu odpowiedzialności za środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów na poziomie podmiotów kluczowych i ważnych. W związku z tym organy zarządzające podmiotów kluczowych i ważnych powinny zatwierdzić środki zarządzania ryzykiem w cyberbezpieczeństwie oraz nadzorować ich stosowanie.

(138) W celu zapewnienia wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii na podstawie niniejszej dyrektywy należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w odniesieniu do uzupełnienia niniejszej dyrektywy poprzez określenie, które kategorie podmiotów kluczowych i ważnych mają być zobowiązane do korzystania z niektórych certyfikowanych produktów ICT, usług ICT i procesów ICT lub uzyskania certyfikacji na podstawie europejskiego systemu certyfikacji cyberbezpieczeństwa. 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 ([22]). W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach 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.

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

(139) W celu zapewnienia jednolitych warunków wykonywania niniejszej dyrektywy należy powierzyć Komisji uprawnienia wykonawcze do określenia ustaleń proceduralnych niezbędnych do funkcjonowania Grupy Współpracy oraz wymogów technicznych, metodologicznych i sektorowych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie, oraz do doprecyzowania rodzaju zgłaszanych informacji, formatu i procedury powiadamiania o incydencie, cyberzagrożeniu i potencjalnym zdarzeniu dla cyberbezpieczeństwa oraz komunikatów o poważnych cyberzagrożeniach, a także doprecyzowania przypadków, w których incydent należy uznać za poważny. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([23]).

(140) Komisja powinna okresowo dokonywać przeglądu niniejszej dyrektywy, po konsultacji z zainteresowanymi stronami, w szczególności w celu sprawdzenia, czy właściwe jest zaproponowanie zmian w świetle zmieniających się warunków społecznych, politycznych, technologicznych lub rynkowych. W ramach tych przeglądów Komisja powinna ocenić znaczenie wielkości danych podmiotów oraz sektorów, podsektorów i rodzajów podmiotu, o którym mowa w załącznikach do niniejszej dyrektywy, dla funkcjonowania gospodarki i społeczeństwa w kontekście cyberbezpieczeństwa. Komisja powinna ocenić między innymi, czy dostawcy objęci zakresem niniejszej dyrektywy wyznaczeni jako bardzo duże platformy internetowe w rozumieniu art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 ([24]) mogą zostać wskazani jako podmioty kluczowe na mocy niniejszej dyrektywy.

(141) Niniejsza dyrektywa przydziela ENISA nowe zadania, zwiększając tym samym jej rolę, i może również spowodować, że ENISA będzie zobowiązana do wykonywania obecnych zadań powierzonych jej na mocy rozporządzenia (UE) 2019/881 na wyższym niż dotychczas poziomie. Aby zapewnić ENISA niezbędne zasoby finansowe i ludzkie do realizacji obecnych i nowych zadań, a także do tego, by mogła sprostać wykonaniu tych zadań na wyższym poziomie wynikającym z jej zwiększonej roli, należy odpowiednio zwiększyć jej budżet. Ponadto aby zapewnić efektywne wykorzystanie zasobów, ENISA powinna mieć większą elastyczność w wewnętrznym przydzielaniu zasobów w celu skutecznej realizacji zadań i spełnienia oczekiwań.

(142) Ponieważ cel niniejszej dyrektywy, a mianowicie osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej 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, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(143) Niniejsza dyrektywa nie narusza praw podstawowych i jest zgodna z zasadami uznanymi w Karcie, w szczególności dotyczącymi prawa do poszanowania życia prywatnego i komunikowania się, ochrony danych osobowych, wolności prowadzenia działalności gospodarczej, prawa własności, prawa do skutecznego środka prawnego i rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony. Prawo do skutecznego środka prawnego dotyczy także odbiorców usług świadczonych przez podmioty kluczowe i ważne. Niniejszą dyrektywę należy wprowadzać w życie zgodnie z tymi prawami i zasadami,

(144) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([25]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 11 marca 2021 r. ([26]),

---

([23]) 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).

([24]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych i zmieniające dyrektywę 2000/31/WE (akt o usługach cyfrowych) (Dz.U. L 277 z 27.10.2022, s. 1).

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

([26]) Dz.U. C 183 z 11.5.2021, s. 3.

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

1. Niniejszą dyrektywą ustanawia się środki mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego.

2. W tym celu niniejsza dyrektywa określa:

a) obowiązki państw członkowskich dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa oraz wyznaczenia lub powołania właściwych organów, organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, pojedynczych punktów kontaktowych ds. cyberbezpieczeństwa (pojedyncze punkty kontaktowe) oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT);

b) środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów spoczywające na podmiotach w rodzaju tych, o których mowa w załączniku I lub II, jak również na podmiotach zidentyfikowanych jako podmioty o charakterze krytycznym na podstawie dyrektywy (UE) 2022/2557;

c) zasady i obowiązki w zakresie wymiany informacji o cyberbezpieczeństwie;

d) obowiązki w zakresie nadzoru i egzekwowania przepisów spoczywające na państwach członkowskich.

Artykuł 2

Zakres

1. Niniejsza dyrektywa ma zastosowanie do podmiotów publicznych lub prywatnych w rodzaju tych, o których mowa w załączniku I lub II, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE lub które przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu oraz które świadczą usługi lub prowadzą działalność w Unii.

Art. 3 ust. 4 załącznika do tego zalecenia nie ma zastosowania do celów niniejszej dyrektywy.

2. Niniejsza dyrektywa ma również zastosowanie do podmiotów w rodzaju tych, o których mowa w załączniku I lub II, w przypadku gdy:

a) usługi świadczone są przez:

   (i) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej;

   (ii) dostawców usług zaufania;

   (iii) rejestry nazw domen najwyższego poziomu, oraz dostawców usług systemów nazw domen;

b) podmiot jest jedynym w danym państwie członkowskim dostawcą usługi, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej;

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

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

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

f) podmiot jest podmiotem administracji publicznej:

(i) na poziomie rządu centralnego, zdefiniowanym przez państwo członkowskie, zgodnie z prawem krajowym; lub

(ii) na poziomie regionalnym, zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym, który zgodnie z oceną opartą na analizie ryzyka świadczy usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą.

3. Niniejsza dyrektywa ma zastosowanie do podmiotów zidentyfikowanych jako podmioty mające charakter krytyczny na mocy dyrektywy (UE) 2022/2557, niezależnie od ich wielkości.

4. Niniejsza dyrektywa ma zastosowanie do podmiotów świadczących usługi rejestracji nazw domen, niezależnie od ich wielkości.

5. Państwa członkowskie mogą postanowić, że niniejsza dyrektywa ma zastosowanie do:

a) podmiotów administracji publicznej na poziomie lokalnym;

b) instytucji edukacyjnych, zwłaszcza gdy prowadzą one działalność badawczą o krytycznym znaczeniu.

6. Niniejsza dyrektywa pozostaje bez uszczerbku dla spoczywającego na państwach członkowskich obowiązku ochrony bezpieczeństwa narodowego oraz dla ich uprawnień do zabezpieczania innych podstawowych funkcji państwa, w tym zapewniania integralności terytorialnej państwa i utrzymywania porządku publicznego.

7. Niniejsza dyrektywa nie ma zastosowania do podmiotów administracji publicznej, które prowadzą działalność w dziedzinach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobiegania im, prowadzenia postępowań w sprawie przestępstw, ich wykrywania oraz ścigania.

8. Państwa członkowskie mogą zwolnić określone podmioty, które prowadzą działania w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie, wykrywanie ich i ściganie, lub które świadczą usługi wyłącznie na rzecz podmiotów administracji publicznej, o których mowa w ust. 7 niniejszego artykułu, z obowiązków ustanowionych w art. 21 lub 23 w odniesieniu do tych działań lub tych usług. W takich przypadkach środki nadzoru i egzekwowania przepisów, o których mowa w rozdziale VII, nie mają zastosowania do tej konkretnej działalności lub tych usług. W przypadku gdy podmioty prowadzą działalność lub świadczą usługi wyłącznie w rodzaju tych, o których mowa w niniejszym ustępie, państwa członkowskie mogą również podjąć decyzję o zwolnieniu tych podmiotów z obowiązków określonych w art. 3 i 27.

9. Ust. 7 i 8 nie mają zastosowania w przypadku, gdy podmiot działa jako dostawca usług zaufania.

10. Niniejsza dyrektywa nie ma zastosowania do podmiotów, które państwa członkowskie zwolniły z zakresu stosowania rozporządzenia (UE) 2022/2554 zgodnie z art. 2 ust. 4 tego rozporządzenia.

11. Obowiązki ustanowione w niniejszej dyrektywie nie wiążą się z dostarczaniem informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami państw członkowskich w zakresie bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności.

12. Niniejszą dyrektywę stosuje się bez uszczerbku dla rozporządzenia (UE) 2016/679, dyrektywy 2002/58/WE, dyrektyw Parlamentu Europejskiego i Rady 2011/93/UE ([27]) i 2013/40/UE ([28]) oraz dyrektywy (UE) 2022/2557.

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

([27]) 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).

([28]) 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).

14. Podmioty, właściwe organy, pojedyncze punkty kontaktowe i CSIRT przetwarzają dane osobowe w zakresie niezbędnym do celów niniejszej dyrektywy i zgodnie z rozporządzeniem (UE) 2016/679, w szczególności takie przetwarzanie odbywa się na podstawie jego art. 6.

Przetwarzanie danych osobowych na mocy niniejszej dyrektywy przez dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej odbywa się zgodnie z unijnymi przepisami o ochronie danych i unijnym prawem dotyczącym prywatności, w szczególności dyrektywą 2002/58/WE.

Artykuł 3

Podmioty kluczowe i ważne

1. Do celów niniejszej dyrektywy następujące podmioty uznaje się za podmioty kluczowe:

a) podmioty w rodzaju tych, o których mowa w załączniku I, przekraczające pułapy dla średnich przedsiębiorstw, określone w art. 2 ust. 1 załącznika do zalecenia 2003/361/WE;

b) kwalifikowanych dostawców usług zaufania i rejestry nazw domen najwyższego poziomu, a także dostawców usług DNS, niezależnie od ich wielkości;

c) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE;

d) podmioty administracji publicznej, o których mowa w art. 2 ust. 2 lit. f) ppkt (i);

e) inne podmioty w rodzaju tych, o których mowa w załączniku I lub II, które zostały wskazane przez państwo członkowskie jako podmioty kluczowe zgodnie z art. 2 ust. 2 lit. b)–e);

f) podmioty wskazane jako podmioty krytyczne na podstawie dyrektywy (UE) 2022/2557, o których mowa w art. 2 ust. 3 niniejszej dyrektywy;

g) jeżeli państwo członkowskie tak postanowi, podmioty, które to państwo członkowskie wskazało przed 16 stycznia 2023 r. jako operatorów usług kluczowych zgodnie z dyrektywą (UE) 2016/1148 lub prawem krajowym.

2. Do celów niniejszej dyrektywy podmioty w rodzaju tych, o których mowa w załączniku I lub II, które nie kwalifikują się jako podmioty kluczowe zgodnie z ust. 1 niniejszego artykułu, uznaje się za podmioty ważne. Odnosi się to również do podmiotów, które zostały wskazane przez państwa członkowskie jako podmioty ważne zgodnie z art. 2 ust. 2 lit. b)–e).

3. Do dnia 17 kwietnia 2025 r. państwa członkowskie ustanawiają wykaz podmiotów kluczowych i ważnych, a także podmiotów świadczących usługi rejestracji nazw domen. Państwa członkowskie regularnie, i nie rzadziej niż co dwa lata po wyżej wymienionej dacie, dokonują przeglądu i – w stosownych przypadkach – aktualizacji tego wykazu.

4. W celu ustanowienia wykazu, o którym mowa w ust. 3, państwa członkowskie wymagają od podmiotów, o których mowa w tym ustępie, przedłożenia właściwym organom co najmniej następujących informacji:

a) nazwy podmiotu;

b) adresu i aktualnych danych kontaktowych, w tym adresów poczty elektronicznej, zakresów adresów IP i numerów telefonów;

c) w stosownych przypadkach, odpowiedniego sektora i podsektora, o których mowa w załączniku I lub II; oraz

d) w stosownych przypadkach, wykazu państw członkowskich, w których świadczą one usługi objęte zakresem stosowania niniejszej dyrektywy.

Podmioty, o których mowa w ust. 3, niezwłocznie powiadamiają o zmianach danych przedłożonych zgodnie z akapitem pierwszym niniejszego ustępu, a w każdym razie w terminie dwóch tygodni od dnia, w którym nastąpiła zmiana.

Komisja, z pomocą Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), bez zbędnej zwłoki podaje wytyczne i wzory dokumentów związane z obowiązkami ustanowionymi w niniejszym ustępie.

Państwa członkowskie mogą ustanowić krajowe mechanizmy umożliwiające podmiotom samodzielną rejestrację.

5. Do dnia 17 kwietnia 2025 r., a następnie co dwa lata właściwe organy powiadamiają:

a) Komisję i Grupę Współpracy o liczbie podmiotów kluczowych i ważnych wymienionych w wykazie zgodnie z ust. 3 dla każdego sektora i podsektora, o których mowa w załączniku I lub II; oraz

b) Komisję o istotnych informacjach na temat liczby podmiotów kluczowych i ważnych wskazanych na podstawie art. 2 ust. 2 lit. b)–e), sektora i podsektora, o których mowa w załączniku I lub II i do których podmioty te należą, rodzaju świadczonej przez nie usługi oraz przepisu spośród tych ustanowionych na podstawie art. 2 ust. 2 lit. b)–e), na podstawie którego zostały one wskazane.

6. Do dnia 17 kwietnia 2025 r. i na wniosek Komisji państwa członkowskie mogą zgłaszać Komisji nazwy podmiotów kluczowych i ważnych, o których mowa w ust. 5 lit. b).

Artykuł 4

Sektorowe akty prawne Unii

1. W przypadku gdy na podstawie sektorowych aktów prawnych Unii wymaga się od podmiotów kluczowych lub ważnych przyjęcia środków zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania poważnych incydentów i w przypadku gdy wymogi te są co najmniej równoważne pod względem skutku obowiązkom określonym w niniejszej dyrektywie, nie stosuje się do takich podmiotów odpowiednich przepisów niniejszej dyrektywy, w tym przepisów dotyczących nadzoru i egzekwowania przepisów określonych w rozdziale VII. Jeżeli sektorowe akty prawne Unii nie obejmują wszystkich podmiotów w konkretnym sektorze, objętych zakresem stosowania niniejszej dyrektywy, odpowiednie przepisy niniejszej dyrektywy nadal mają zastosowanie do podmiotów nieobjętych tymi sektorowymi aktami prawnymi Unii.

2. Wymogi, o których mowa w ust. 1 niniejszego artykułu, uznaje się za równoważne pod względem skutku obowiązkom określonym w niniejszej dyrektywie, jeżeli:

a) środki zarządzania ryzykiem w cyberbezpieczeństwie są co najmniej równoważne pod względem skutku środkom określonym w art. 21 ust. 1 i 2; lub

b) sektorowy akt prawny Unii przewiduje natychmiastowy dostęp CSIRT, właściwych organów lub pojedynczych punktów kontaktowych na mocy niniejszej dyrektywy do zgłoszeń incydentów – w stosownych przypadkach automatycznie i bezpośrednio, oraz w przypadkach, gdy wymogi dotyczące zgłaszania poważnych incydentów są co najmniej równoważne pod względem skutku wymogom określonym w art. 23 ust. 1–6 niniejszej dyrektywy.

3. Komisja do dnia 17 lipca 2023 r. podaje wytyczne wyjaśniające stosowanie ust. 1 i 2. Komisja regularnie dokonuje przeglądu tych wytycznych. Przygotowując te wytyczne, Komisja bierze pod uwagę uwagi Grupy Współpracy i ENISA.

Artykuł 5

Harmonizacja minimalna

Niniejsza dyrektywa nie uniemożliwia państwom członkowskim przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie przepisy są spójne z obowiązkami państw członkowskich, ustanowionymi w prawie Unii.

Artykuł 6

Definicje

Do celów niniejszej dyrektywy stosuje się następujące definicje:

1) „sieci i systemy informatyczne” oznaczają:

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

b) urządzenie lub grupę wzajemnie połączonych lub powiązanych urządzeń, z których co najmniej jedno, na podstawie programu, automatycznie przetwarza dane cyfrowe; lub

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

2) „bezpieczeństwo sieci i systemów informatycznych" oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;

3) „cyberbezpieczeństwo" oznacza cyberbezpieczeństwo zdefiniowane w art. 2 pkt 1 rozporządzenia (UE) 2019/881;

4) „krajowa strategia cyberbezpieczeństwa" oznacza spójne ramy państwa członkowskiego określające strategiczne cele i priorytety w obszarze cyberbezpieczeństwa oraz środki służące ich realizacji w tym państwie członkowskim;

5) „potencjalne zdarzenie dla cyberbezpieczeństwa" oznacza zdarzenie, które mogło naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem, któremu udało się jednak zapobiec lub które jednak nie wystąpiło;

6) „incydent" oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;

7) „incydent w cyberbezpieczeństwie na dużą skalę" oznacza incydent, który powoduje zakłócenia na poziomie przekraczającym zdolność państwa członkowskiego do reagowania na ten incydent lub który wywiera znaczące skutki w co najmniej dwóch państwach członkowskich;

8) „obsługa incydentu" oznacza działania i procedury mające na celu zapobieżenie incydentowi, wykrywanie i analizowanie go, ograniczanie jego zasięgu lub reagowanie na niego i przywrócenie normalnego działania;

9) „ryzyko" oznacza możliwość wystąpienia strat lub zakłóceń spowodowanych incydentem, wyrażoną jako wypadkową wielkości takiej straty lub takich zakłóceń oraz prawdopodobieństwo wystąpienia takiego incydentu;

10) „cyberzagrożenie" oznacza cyberzagrożenie zdefiniowane w art. 2 pkt 8 rozporządzenia (UE) 2019/881;

11) „poważne cyberzagrożenie" oznacza cyberzagrożenie, co do którego można założyć w oparciu o jego charakterystykę techniczną, że może wywrzeć znaczący wpływ na sieć i systemy informatyczne danego podmiotu lub użytkowników, korzystających z usług tego podmiotu, powodując i znaczne szkody majątkowe lub niemajątkowe;

12) „produkt ICT" oznacza produkt ICT zdefiniowany w art. 2 pkt 12 rozporządzenia (UE) 2019/881;

13) „usługa ICT" oznacza usługę ICT zdefiniowaną w art. 2 pkt 13 rozporządzenia (UE) 2019/881;

14) „proces ICT" oznacza proces ICT zdefiniowany w art. 2 pkt 14 rozporządzenia (UE) 2019/881;

15) „podatność" oznacza słabość, wrażliwość lub wadę produktów ICT lub usług ICT, które to cechy mogą zostać wykorzystane w wyniku cyberzagrożenia;

16) „norma" oznacza normę zdefiniowaną w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 ([29]);

17) „specyfikacja techniczna" oznacza specyfikację techniczną zdefiniowaną w art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012;

([29]) 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).

18) „punkt wymiany ruchu internetowego" oznacza obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi sieciami (systemami autonomicznymi), głównie w celu ułatwienia wymiany ruchu internetowego; punkt wymiany ruchu internetowego zapewnia połączenie międzysystemowe wyłącznie systemów autonomicznych i 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;

19) „system nazw domen" lub „DNS" oznacza hierarchiczny rozproszony system nazw, który umożliwia identyfikację usług i zasobów internetowych, pozwalając urządzeniom użytkowników końcowych na korzystanie z usług routingu internetowego i usług łączności w celu dotarcia do tych usług i zasobów;

20) „dostawca usług DNS" oznacza podmiot świadczący:

    a) dostępne publicznie rekurencyjne usługi rozpoznawania nazw domen na rzecz użytkowników końcowych internetu; lub

    b) autorytatywne usługi rozpoznawania nazw domen do użytku osób trzecich, z wyjątkiem głównych serwerów nazw;

21) „rejestr nazw domen najwyższego poziomu" lub „rejestr nazw TLD" 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, bez względu na to, czy którekolwiek z tych działań jest wykonywane przez sam podmiot czy zlecane na zewnątrz, ale z wyłączeniem sytuacji, w których rejestr wykorzystuje nazwy TDL wyłącznie do własnego użytku;

22) „podmiot świadczący usługi rejestracji nazw domen" oznacza rejestratora lub agenta działającego w imieniu rejestratorów, np. dostawcę lub odsprzedawcę usług w zakresie rejestracji prywatności lub serwerów proxy;

23) „usługa cyfrowa" oznacza usługę zdefiniowaną w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady ([30]);

24) „usługa zaufania" oznacza usługę zaufania zdefiniowaną w art. 3 pkt 16 rozporządzenia (UE) nr 910/2014;

25) „dostawca usług zaufania" oznacza dostawcę usług zaufania zdefiniowanego w art. 3 pkt 19 rozporządzenia (UE) nr 910/2014;

26) „kwalifikowana usługa zaufania" oznacza kwalifikowaną usługę zaufania zdefiniowaną w art. 3 pkt 17 rozporządzenia (UE) nr 910/2014;

27) „kwalifikowany dostawca usług zaufania" oznacza kwalifikowanego dostawcę usług zaufania zdefiniowanego w art. 3 pkt 20 rozporządzenia (UE) nr 910/2014;

28) „internetowa platforma handlowa" oznacza internetową platformę handlową zdefiniowaną w art. 2 lit. n) dyrektywy 2005/29/WE Parlamentu Europejskiego i Rady ([31]);

29) „wyszukiwarka internetowa" oznacza wyszukiwarkę internetową zdefiniowaną w art. 2 pkt 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150 ([32]);

30) „usługa chmurowa" oznacza usługę cyfrową umożliwiającą administrowanie na żądanie skalowalnym i elastycznym zbiorem zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru, w tym również gdy takie zasoby są rozproszone w kilku lokalizacjach;

([30]) 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).

([31]) 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).

([32]) 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).

31) „usługa ośrodka przetwarzania danych" oznacza usługę obejmującą struktury lub grupy struktur przeznaczone do scentralizowanego hostingu, zapewniania wzajemnego połączenia i eksploatacji sprzętu IT i sieciowego służącego do świadczenia usług przechowywania, przetwarzania i transportu danych wraz ze wszystkimi obiektami i całą infrastrukturą, zapewniającymi dystrybucję energii elektrycznej i kontrolę środowiskową;

32) „sieć dostarczania treści" oznacza sieć rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług;

33) „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;

34) „przedstawiciel" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub miejsce prowadzenia działalności w Unii, wyraźnie wyznaczoną do występowania w imieniu dostawcy usług DNS, rejestru nazw TLD, podmiotu świadczącego usługi rejestracji nazw domen, dostawcy usług chmurowych, dostawcy usług ośrodka przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie bezpieczeństwa lub dostawcy internetowej platformy handlowej, wyszukiwarki internetowej lub platformy usług sieci społecznościowych, niemających miejsca prowadzenia działalności w Unii, do której właściwy organ krajowy lub CSIRT może się zwrócić zamiast do samego podmiotu w związku z obowiązkami tego podmiotu przewidzianymi w niniejszej dyrektywie;

35) „podmiot administracji publicznej" oznacza podmiot uznany za taki w danym państwie członkowskim zgodnie z prawem krajowym, z wyłączeniem sądownictwa, parlamentów lub banków centralnych, spełniający następujące kryteria:

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

   b) ma osobowość prawną lub zgodnie z przepisami jest uprawniony do działania w imieniu innego podmiotu mającego osobowość prawną;

   c) jest finansowany w przeważającej części przez państwo, władze regionalne lub inne podmioty prawa publicznego, jego zarząd podlega nadzorowi ze strony tych organów lub podmiotów albo 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;

36) „publiczna sieć łączności elektronicznej" oznacza publiczną sieć łączności elektronicznej zdefiniowaną w art. 2 pkt 8 dyrektywy (UE) 2018/1972;

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

38) „podmiot" oznacza osobę fizyczną lub prawną utworzoną i uznawaną za taką na podstawie prawa krajowego obowiązującego w miejscu, w którym osoba ta ma miejsce prowadzenia działalności, która może – działając we własnym imieniu – wykonywać prawa i podlegać obowiązkom;

39) „dostawca usług zarządzanych" oznacza podmiot, który świadczy usługi związane z instalacją, eksploatacją lub konserwacją produktów, sieci, infrastruktury, aplikacji ICT lub innych sieci i systemów informatycznych lub z zarządzaniem nimi, poprzez pomoc lub aktywną administrację prowadzoną u klientów lub zdalnie;

40) „dostawca usług zarządzanych w zakresie bezpieczeństwa" oznacza dostawcę usług zarządzanych, który prowadzi działania związane z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa lub zapewnia pomoc dla tych działań;

41) „organizacja badawcza" oznacza podmiot, którego głównym celem jest prowadzenie badań stosowanych lub eksperymentalnych prac rozwojowych z myślą o wykorzystaniu wyników tych badań do celów komercyjnych, z wyłączeniem instytucji edukacyjnych.

ROZDZIAŁ II

SKOORDYNOWANE RAMY W ZAKRESIE CYBERBEZPIECZEŃSTWA

Artykuł 7

Krajowa strategia cyberbezpieczeństwa

1. Każde państwo członkowskie przyjmuje krajową strategię cyberbezpieczeństwa, która przewiduje cele strategiczne, zasoby kluczowe do osiągnięcia tych celów i odpowiednie środki z zakresu polityk publicznych i regulacji, z myślą o osiągnięciu i utrzymaniu wysokiego poziomu cyberbezpieczeństwa. Krajowa strategia cyberbezpieczeństwa zawiera:

a) cele i priorytety strategii cyberbezpieczeństwa państwa członkowskiego obejmujące w szczególności sektory, o których mowa w załącznikach I II;

b) ramy zarządzania służące realizacji celów i priorytetów, o których mowa w lit. a) niniejszego ustępu, w tym polityki, o których mowa w ust. 2;

c) ramy zarządzania wyjaśniające role i obowiązki zainteresowanych stron na szczeblu krajowym, stanowiące podstawę współpracy i koordynacji na szczeblu krajowym między właściwymi organami, pojedynczymi punktami kontaktowymi i CSIRT na mocy niniejszej dyrektywy, a także koordynacji i współpracy między tymi podmiotami a właściwymi organami na podstawie sektorowych aktów prawnych Unii;

d) mechanizm służący określeniu istotnych zasobów i szacowanie ryzyka w tym państwie członkowskim;

e) wskazanie środków zapewniających gotowość na wypadek incydentów, zdolność reagowania na nie i przywracanie normalnego działania, z uwzględnieniem współpracy pomiędzy sektorami publicznym i prywatnym;

f) wykaz poszczególnych organów i zainteresowanych stron zaangażowanych we wdrażanie krajowej strategii cyberbezpieczeństwa;

g) ramy polityki na rzecz ściślejszej koordynacji między właściwymi organami na mocy niniejszej dyrektywy a właściwymi organami na mocy dyrektywy (UE) 2022/2557 do celu wymiany informacji na temat ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią oraz wykonywania zadań nadzorczych, stosownie do przypadku;

h) plan, zawierający kluczowe środki do podniesienia ogólnego poziomu wiedzy obywateli o cyberbezpieczeństwie.

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

a) dotyczące cyberbezpieczeństwa w łańcuchu dostaw produktów ICT i usług ICT wykorzystywanych przez podmioty do świadczenia usług;

b) dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT i usług ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa, szyfrowania oraz wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu;

c) dotyczące zarządzania podatnościami, obejmującą promowanie i ułatwianie skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1;

d) związane z utrzymywaniem ogólnej dostępności, integralności i poufności publicznego rdzenia otwartego internetu, w tym, w stosownych przypadkach, cyberbezpieczeństwa podmorskich kabli komunikacyjnych;

e) promującą rozwój i integrację odpowiednich zaawansowanych technologii służących wdrożeniu najnowocześniejszych środków zarządzania ryzykiem w cyberbezpieczeństwie;

f) promujące i rozwijające kształcenie i szkolenie w dziedzinie cyberbezpieczeństwa, umiejętności z zakresu cyberbezpieczeństwa, podnoszenia świadomości oraz inicjatyw badawczo-rozwojowych, a także wytyczne dotyczące dobrych praktyk i kontroli w zakresie cyberhigieny, skierowane do obywateli, zainteresowanych stron i podmiotów;

g) wspierające instytucje akademickie i naukowe, w opracowywaniu, usprawnianiu i propagowaniu wprowadzania narzędzi z zakresu cyberbezpieczeństwa oraz bezpiecznej infrastruktury sieciowej;

h) obejmującą właściwe procedury oraz odpowiednie narzędzia służące wymianie informacji mające na celu wspieranie dobrowolnej wymiany informacji o cyberbezpieczeństwie między podmiotami zgodnie z prawem Unii;

i) wzmacniające podstawowy poziom cyberodporności i cyberhigieny małych i średnich przedsiębiorstw, w szczególności tych wyłączonych z zakresu stosowania niniejszej dyrektywy, poprzez zapewnienie łatwo dostępnych wytycznych i pomocy w zakresie ich szczególnych potrzeb;

j) propagujące aktywną cyberochronę.

3. Państwa członkowskie przekazują Komisji krajowe strategie cyberbezpieczeństwa w terminie trzech miesięcy od ich przyjęcia. Państwa członkowskie mogą wyłączyć z takich zgłoszeń informacje, które odnoszą się do ich bezpieczeństwa narodowego.

4. Państwa członkowskie regularnie, co najmniej co pięć lat, przeprowadzają na podstawie kluczowych wskaźników skuteczności ocenę krajowych strategii cyberbezpieczeństwa i w razie potrzeby je aktualizują. ENISA pomaga państwom członkowskim, na ich wniosek, w opracowaniu lub aktualizacji krajowej strategii cyberbezpieczeństwa i kluczowych wskaźników skuteczności działania stosowanych do oceny tej strategii w celu dostosowania jej do wymogów i obowiązków ustanowionych w niniejszej dyrektywie.

Artykuł 8

Właściwe organy i pojedyncze punkty kontaktowe

1. Każde państwo członkowskie wyznacza lub ustanawia co najmniej jeden właściwy organ odpowiedzialny za cyberbezpieczeństwo oraz za zadania nadzorcze, o których mowa w rozdziale VII (właściwe organy).

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

3. Każde państwo członkowskie wyznacza lub ustanawia pojedynczy punkt kontaktowy. W przypadku gdy państwo członkowskie wyznacza lub ustanawia tylko jeden właściwy organ zgodnie z ust. 1, 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 ze swojego państwa członkowskiego z odpowiednimi organami w innych państwach członkowskich, a w stosownym przypadku z Komisją i ENISA, a także w celu zapewnienia międzysektorowej współpracy z innymi właściwymi organami krajowymi w swoim państwie członkowskim.

5. Państwa członkowskie zapewniają swoim właściwym organom i pojedynczym punktom kontaktowym odpowiednie zasoby, aby mogły one efektywnie i skutecznie wykonywać powierzone im zadania i tym samym realizować cele niniejszej dyrektywy.

6. Każde państwo członkowskie bez zbędnej zwłoki przekazuje Komisji dane identyfikacyjne właściwego organu, o którym mowa w ust. 1, i pojedynczego punktu kontaktowego, o którym mowa w ust. 3, oraz powiadamia ją o zadaniach tych organów i o późniejszych zmianach w tym zakresie. Każde państwo członkowskie podaje dane identyfikacyjne właściwego organu do wiadomości publicznej. Komisja udostępnia publicznie wykaz pojedynczych punktów kontaktowych.

Artykuł 9

Krajowe ramy zarządzania kryzysowego w cyberbezpieczeństwie

1. Każde państwo członkowskie wyznacza lub ustanawia co najmniej jeden właściwy organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę (organy ds. zarządzania kryzysowego w cyberbezpieczeństwie). Państwa członkowskie zapewniają tym organom odpowiednie zasoby, aby mogły one efektywnie i skutecznie wykonywać powierzone im zadania. Państwa członkowskie zapewniają spójność z istniejącymi ogólnymi krajowymi ramami zarządzania kryzysowego.

2. Jeżeli państwo członkowskie wyznaczy lub ustanowi więcej niż jeden organ ds. zarządzania kryzysowego w cyberbezpieczeństwie zgodnie z ust. 1, jasno wskazuje, który z tych organów ma pełnić rolę koordynatora zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę.

3. Każde państwo członkowskie określa zdolności, zasoby i procedury, które można wykorzystać w razie sytuacji kryzysowej do celów niniejszej dyrektywy.

4. Każde państwo członkowskie przyjmuje krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. W planie tym określa się w szczególności:

a) cele krajowych środków i działań służących w zakresie gotowości;

b) zadania i obowiązki organów ds. zarządzania kryzysowego w cyberbezpieczeństwie;

c) procedury zarządzania kryzysowego w cyberprzestrzeni, w tym ich włączenie do ogólnych krajowych ram zarządzania kryzysowego, oraz kanały wymiany informacji;

d) krajowe środki w zakresie gotowości, w tym ćwiczenia i szkolenia;

e) odpowiednie zainteresowane strony publiczne i prywatne oraz infrastrukturę;

f) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa danego państwa członkowskiego w skoordynowanym zarządzaniu incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę na poziomie Unii oraz efektywnego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania.

5. W terminie trzech miesięcy od wyznaczenia lub ustanowienia organu ds. zarządzania kryzysowego w cyberbezpieczeństwie, o którym mowa w ust. 1, każde państwo członkowskie przekazuje Komisji dane indentyfikacyjne swojego organu oraz powiadamia ją o późniejszych zmianach w tym zakresie. Państwa członkowskie przedkładają Komisji i europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) ważne informacje związane z wymogami określonymi w ust. 4, dotyczące krajowych planów reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę w terminie trzech miesięcy od daty przyjęcia tych planów. Państwa członkowskie mogą wyłączyć niektóre informacje, jeżeli i w zakresie w jakim jest to kluczowe z punktu widzenia ich bezpieczeństwa narodowego.

Artykuł 10

Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)

1. Każde państwo członkowskie wyznacza lub ustanawia co najmniej jeden CSIRT. CSIRT można wyznaczyć lub ustanowić w ramach właściwego organu. CSIRT spełniają wymogi określone w art. 11 ust. 1, obejmują co najmniej sektory, podsektory i rodzaje podmiotów, o których mowa w załącznikach I i II, i są odpowiedzialne za obsługę incydentów zgodnie z wyraźnie określoną procedurą.

2. Państwa członkowskie zapewniają, aby każdy CSIRT dysponował odpowiednimi zasobami, tak aby mógł skutecznie realizować swoje zadania określone w art. 11 ust. 3.

3. Państwa członkowskie zapewniają, aby każdy CSIRT miał do dyspozycji odpowiednią, bezpieczną i odporną infrastrukturę komunikacyjno-informacyjną do wymiany informacji z podmiotami kluczowymi i ważnymi oraz innymi odpowiednimi zainteresowanymi stronami. W tym celu państwa członkowskie zapewniają, aby każdy CSIRT uczestniczył we wdrażaniu bezpiecznych narzędzi wymiany informacji.

4. CSIRT współpracują z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i ważnych oraz, w odpowiednich przypadkach, wymieniają z nimi stosowne informacje zgodnie z art. 29.

5. CSIRT biorą udział w ocenie wzajemnej organizowanej zgodnie z art. 19.

6. Państwa członkowskie zapewniają skuteczną, efektywną i bezpieczną współpracę swoich CSIRT w sieci CSIRT.

7. CSIRT mogą nawiązać stosunki współpracy z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich. W ramach takich stosunków współpracy państwa członkowskie wspierają skuteczną, efektywną i bezpieczną wymianę informacji z tymi krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich, z wykorzystaniem odpowiednich protokołów wymiany informacji, w tym kodu poufności TLP. CSIRT mogą wymieniać ważne informacje z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich, w tym dane osobowe zgodnie z unijnymi przepisami o ochronie danych.

8. CSIRT mogą współpracować z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich lub równoważnymi organami z państw trzecich, w szczególności w celu zapewnienia im pomocy w zakresie cyberbezpieczeństwa.

9. Każde państwo członkowskie bez zbędnej zwłoki powiadamia Komisję o danych identyfikacyjnych CSIRT, o którym mowa w ust. 1 niniejszego artykułu, i CSIRT wyznaczonego na koordynatora zgodnie z art. 12 ust. 1, o ich odpowiednich zadaniach w odniesieniu do podmiotów kluczowych i ważnych oraz o późniejszych zmianach w tym zakresie.

10. Państwa członkowskie mogą zwrócić się do ENISA o pomoc przy rozwijaniu CSIRT.

Artykuł 11

Wymogi dotyczące CSIRT, ich zdolności techniczne i zadania

1. CSIRT spełniają następujące wymogi:

a) CSIRT zapewniają wysoką dostępność swoich kanałów komunikacji poprzez takie ich ukształtowanie, aby wyłączenie jednego elementu systemu nie uniemożliwiało przesłania informacji do adresata, 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; jasno określają one kanały komunikacji i informują o nich podmioty będące w ich właściwości oraz współpracujących partnerów;

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

c) CSIRT dysponują odpowiednim systemem zarządzania w zakresie kierowanych do nich zgłoszeń oraz ich przekierowywania, w szczególności w celu ułatwienia skutecznego i efektywnego dalszego przekazywania danej sprawy;

d) CSIRT zapewniają poufność i wiarygodność swoich działań;

e) CSIRT dysponują odpowiednio licznym personelem, aby zapewnić nieprzerwaną dostępność ich usług, oraz zapewniają odpowiednie przeszkolenie personelu;

f) CSIRT dysponują systemami redundantnymi i rezerwowym miejscem pracy w celu zapewnienia ciągłości ich usług.

CSIRT mogą uczestniczyć w międzynarodowych sieciach współpracy.

2. Państwa członkowskie zapewniają, aby ich CSIRT wspólnie miały zdolności techniczne niezbędne do realizacji zadań, o których mowa w ust. 3. Państwa członkowskie zapewniają ich CSIRT zasoby gwarantujące odpowiedni poziom zatrudnienia, aby umożliwić CSIRT rozwój ich zdolności technicznych.

3. CSIRT mają następujące zadania:

a) monitorowanie i analizowanie cyberzagrożeń, podatności i incydentów na poziomie krajowym oraz, na wniosek, udzielanie pomocy danym podmiotom kluczowym i ważnym w zakresie monitorowania ich sieci i systemów informatycznych w czasie rzeczywistym lub zbliżonym do rzeczywistego;

b) wczesne ostrzeganie i alarmowanie danych podmiotów kluczowych i ważnych oraz właściwych organów i innych zainteresowanych stron o cyberzagrożeniach, podatnościach i incydentach, a także kierowanie do nich ogłoszeń oraz przekazywanie im informacji dotyczących cyberzagrożeń, podatności i incydentów, w miarę możliwości w czasie zbliżonym do rzeczywistego;

c) reagowanie na incydenty i w stosownych przypadkach udzielanie pomocy danym podmiotom kluczowym i ważnym;

d) gromadzenie i analizowanie danych kryminalistycznych i zapewnianie dynamicznej analizy ryzyka i incydentów oraz świadomości sytuacyjnej w zakresie cyberbezpieczeństwa;

e) przeprowadzanie, na wniosek podmiotu kluczowego lub ważnego, aktywnego skanowania sieci i systemów informatycznych danego podmiotu w celu wykrycia podatności o potencjalnym znaczącym wpływie;

f) uczestnictwo w sieci CSIRT oraz udzielanie wzajemnej pomocy innym członkom sieci CSIRT na ich wniosek, w miarę własnych zdolności i kompetencji;

g) w stosownych przypadkach działanie w charakterze koordynatora w celu skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1;

h) udział we wdrażaniu bezpiecznych narzędzi wymiany informacji zgodnie z art. 10 ust. 3.

CSIRT mogą prowadzić aktywne, nieinwazyjne skanowanie publicznie dostępnych sieci i systemów informatycznych podmiotów kluczowych i ważnych. Takie skanowanie przeprowadza się w celu wykrycia sieci i systemów informatycznych podatnych na zagrożenia lub skonfigurowanych bez właściwego zabezpieczenia i poinformowania o tym podmiotów, których to dotyczy. Takie skanowanie nie może mieć negatywnego wpływu na funkcjonowanie usług świadczonych przez te podmioty.

Wykonując zadania, o których mowa w akapicie pierwszym, CSIRT mogą priorytetowo traktować niektóre zadania na podstawie podejścia opartego na analizie ryzyka.

4. CSIRT nawiązują współpracę z odpowiednimi zainteresowanymi stronami w sektorze prywatnym w celu realizacji celów niniejszej dyrektywy.

5. Aby ułatwić współpracę, o której mowa w ust. 4, CSIRT promują przyjmowanie i stosowanie wspólnych lub znormalizowanych praktyk, systemów klasyfikacji i systematyki związanych z:

a) procedurami obsługi incydentu;

b) zarządzaniem kryzysowym; oraz

c) skoordynowanym ujawnianiem podatności na mocy art. 12 ust. 1.

Artykuł 12

Skoordynowane ujawnianie podatności i europejska baza danych dotyczących podatności

1. Każde państwo członkowskie wyznacza jeden spośród swoich CSIRT na koordynatora na potrzeby skoordynowanego ujawniania podatności. CSIRT wyznaczony na koordynatora działa w charakterze zaufanego pośrednika, w razie konieczności ułatwiając interakcję między osobą fizyczną lub prawną zgłaszającą podatność a producentem lub dostawcą potencjalnie podatnych produktów ITC lub usług ICT, na wniosek którejkolwiek ze stron. Zadania CSIRT wyznaczonego na koordynatora obejmują:

a) identyfikację danych podmiotów i kontaktowanie się z nimi;

b) udzielanie pomocy osobom fizycznym lub prawnym zgłaszającym podatność; oraz

c) negocjowanie harmonogramu ujawniania oraz zarządzanie podatnościami, których skutki mają wpływ na wiele podmiotów.

Państwa członkowskie zapewniają, aby osoby fizyczne lub prawne mogły zgłaszać anonimowo, jeśli o to wystąpią, podatność wyznaczonemu na koordynatora CSIRT. CSIRT wyznaczony na koordynatora zapewnia przeprowadzenie z należytą starannością działań podjętych w związku ze zgłoszoną podatnością oraz zapewnia anonimowość osoby fizycznej lub prawnej zgłaszającej podatność. Jeżeli zgłoszona podatność może mieć znaczący wpływ na podmioty w więcej niż jednym państwie członkowskim, CSIRT wyznaczony na koordynatora każdego państwa członkowskiego, którego podatność dotyczy, współpracuje, w stosownych przypadkach z innymi CSIRT wyznaczonymi na koordynatorów w ramach sieci CSIRT.

2. ENISA opracowuje i prowadzi, po konsultacji z Grupą Współpracy, europejską bazę danych dotyczącą podatności. W tym celu ENISA ustanawia i utrzymuje odpowiednie systemy informatyczne, polityki i procedury oraz przyjmuje środki techniczne i organizacyjne niezbędne do zapewnienia bezpieczeństwa i integralności europejskiej bazy danych dotyczącej podatności, w szczególności aby umożliwić podmiotom, niezależnie od tego czy są objęte zakresem stosowania niniejszej dyrektywy oraz ich dostawcom sieci i systemów informatycznych ujawnianie i rejestrowanie – na zasadzie dobrowolności – znanych publicznie podatności występujących w produktach ICT lub usługach ICT. Wszystkie zainteresowane strony otrzymują dostęp do informacji na temat podatności zawartych w europejskiej bazie danych dotyczącej podatności. Baza danych zawiera:

a) informacje opisujące podatność;

b) produkty ICT lub usługi ICT, których dotyczy podatność, oraz dotkliwość podatności z punktu widzenia okoliczności, w jakich może ona zostać wykorzystana;

c) dostępność powiązanych aktualizacji, a w razie braku dostępnych aktualizacji – wytyczne podane przez właściwe organy lub CSIRT, skierowane do użytkowników produktów ICT i usług ICT, których dotyczy podatność, na temat sposobów ograniczania ryzyka wynikającego z ujawnionych podatności.

Artykuł 13

Współpraca na poziomie krajowym

1. Jeżeli właściwe organy, pojedynczy punkt kontaktowy i CSIRT z tego samego państwa członkowskiego są odrębne względem siebie, współpracują one ze sobą przy wypełnianiu obowiązków określonych w niniejszej dyrektywie.

2. Państwa członkowskie zapewniają, aby ich CSIRT lub, w stosownych przypadkach, ich właściwe organy odbierały zgłoszenia o poważnych incydentach zgodnie z art. 23 oraz incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgodnie z art. 30.

3. Państwa członkowskie zapewniają, aby ich CSIRT lub, w stosownych przypadkach, właściwe organy informowały ich pojedyncze punkty kontaktowe o zgłoszeniach incydentów, cyberzagrożeń i potencjalnych zdarzeń dla cyberbezpieczeństwa dokonywanych na podstawie niniejszej dyrektywy.

4. Aby zapewnić skuteczne wykonywanie zadań i obowiązków właściwych organów, pojedynczych punktów kontaktowych i CSIRT, państwa członkowskie zapewniają w miarę możliwości odpowiednią współpracę między tymi podmiotami a organami ścigania, organami ochrony danych, organami krajowymi na mocy rozporządzeń (WE) nr 300/2008 i (UE) 2018/1139, organami nadzoru na mocy rozporządzenia (UE) nr 910/2014, właściwymi organami na mocy rozporządzenia (UE) 2022/2554, krajowymi organami regulacyjnymi na mocy dyrektywy (UE) 2018/1972, właściwymi organami na mocy dyrektywy (UE) 2022/2557, a także właściwymi organami na mocy innych sektorowych aktów prawnych Unii w tym państwie członkowskim.

5. Państwa członkowskie zapewniają, aby ich właściwe organy na mocy niniejszej dyrektywy oraz ich właściwe organy na mocy dyrektywy (UE) 2022/2557 współpracowały i regularnie wymieniały się informacjami dotyczącymi identyfikacji podmiotów krytycznych, ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią mających wpływ na podmioty kluczowe wskazane jako podmioty krytyczne na podstawie dyrektywy (UE) 2022/2557, oraz na temat środków podjętych w odpowiedzi na takie ryzyko, zagrożenia i incydenty. Państwa członkowskie zapewniają również, aby ich właściwe organy na mocy niniejszej dyrektywy oraz ich właściwe organy na mocy rozporządzenia (UE) nr 910/2014, rozporządzenia (UE) 2022/2554 i dyrektywy (UE) 2018/1972 regularnie wymieniały się odpowiednimi informacjami, w tym dotyczącymi poważnych incydentów i cyberzagrożeń.

6. Państwa członkowskie upraszczają za pomocą środków technicznych sprawozdawczość dotyczącą zgłoszeń, o których mowa w art. 23 i 30.

ROZDZIAŁ III

WSPÓŁPRACA NA POZIOMIE UNIJNYM I MIĘDZYNARODOWYM

Artykuł 14

Grupa Współpracy

1. Aby wspierać i ułatwiać strategiczną współpracę i wymianę informacji między państwami członkowskimi, a także aby zwiększać zaufanie między nimi, ustanawia się Grupę Współpracy.

2. Grupa Współpracy wykonuje swoje zadania na podstawie dwuletnich programów prac, o których mowa w ust. 7.

3. Grupa Współpracy składa się z przedstawicieli państw członkowskich, Komisji i ENISA. W działaniach Grupy Współpracy uczestniczy w charakterze obserwatora Europejska Służba Działań Zewnętrznych. Europejskie Urzędy Nadzoru i organy właściwe na mocy rozporządzenia (UE) 2022/2554 mogą uczestniczyć w działaniach Grupy Współpracy zgodnie z art. 47 ust. 1 tego rozporządzenia.

W stosownych przypadkach Grupa Współpracy może zapraszać Parlament Europejski i 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) udzielanie wskazówek właściwym organom w związku z tworzeniem i wdrażaniem polityki skoordynowanego ujawniania podatności, o którym mowa w art. 7 ust. 2 lit. c);

c) wymianę najlepszych praktyk i informacji w związku z wdrażaniem niniejszej dyrektywy, w tym w odniesieniu do cyberzagrożeń, incydentów, podatności, potencjalnych zdarzeń dla cyberbezpieczeństwa, inicjatyw na rzecz podnoszenia świadomości, szkoleń, ćwiczeń i umiejętności, budowania zdolności, norm i specyfikacji technicznych, a także wskazywania podmiotów kluczowych i ważnych na podstawie art. 2 ust. 2 lit. b)–e);

d) wymianę porad i współpraca z Komisją w zakresie nowych inicjatyw dotyczących polityki cyberbezpieczeństwa oraz całościowej spójności sektorowych wymogów dotyczących cyberbezpieczeństwa;

e) wymianę porad i współpraca z Komisją w zakresie projektów aktów delegowanych lub wykonawczych przyjmowanych na podstawie niniejszej dyrektywy;

f) wymianę najlepszych praktyk i informacji z odpowiednimi instytucjami, organami, urzędami i agencjami Unii;

g) wymianę opinii na temat wdrażania sektorowych aktów prawnych Unii zawierających przepisy dotyczące cyberbezpieczeństwa;

h) w stosownych przypadkach omawianie sprawozdań z oceny wzajemnej, o których mowa w art. 19 ust. 9, oraz formułowanie wniosków i zaleceń;

i) prowadzenie skoordynowanych oszacowań ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw zgodnie z art. 22 ust. 1;

j) omawianie przypadków wzajemnej pomocy, w tym doświadczeń ze wspólnych transgranicznych działań nadzorczych, o których mowa w art. 37, i wyników tych działań;

k) na wniosek co najmniej jednego zainteresowanego państwa członkowskiego – omawianie konkretnych wniosków o wzajemną pomoc, o której mowa w art. 37;

l) zapewnianie sieci CSIRT i EU-CyCLONe wskazówek strategicznych dotyczących konkretnych pojawiających się kwestii;

m) wymianę opinii na temat polityki działań następczych po incydentach i sytuacjach kryzysowych w cyberbezpieczeństwie na dużą skalę, na podstawie doświadczeń zdobytych w sieci CSIRT i EU-CyCLONe;

n) wkład w rozwój zdolności w zakresie cyberbezpieczeństwa w całej Unii przez ułatwianie wymiany urzędników krajowych w programie budowania zdolności z udziałem pracowników właściwych organów lub CSIRT;

o) organizowanie regularnych wspólnych spotkań z odpowiednimi prywatnymi zainteresowanymi stronami z całej Unii w celu omawiania działań Grupy Współpracy i zbierania informacji o pojawiających się wyzwaniach politycznych;

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

q) ustalenie metodyki i aspektów organizacyjnych ocen wzajemnych, o których mowa w art. 19 ust. 1, a także – z pomocą Komisji i ENISA – określenie zgodnie z art. 19 ust. 5 metodyki oceny własnej dla państw członkowskich oraz – we współpracy z Komisją i ENISA – opracowanie zgodnie z art. 19 ust. 6 kodeksów postępowania jako podstawy metod pracy wyznaczonych ekspertów ds. cyberbezpieczeństwa;

r) przygotowywanie – na potrzeby przeglądu, o którym mowa w art. 40 – sprawozdań z doświadczeń zdobytych na poziomie strategicznym i w ocenach wzajemnych;

s) omawianie i regularne ocenianie sytuacji pod względem cyberzagrożeń lub incydentów, na przykład w postaci oprogramowania typu „ransomware".

Grupa Współpracy przedkłada Komisji, Parlamentowi Europejskiemu i Radzie sprawozdania, o których mowa w akapicie pierwszym lit. r).

5. Państwa członkowskie zapewniają efektywną, skuteczną i bezpieczną współpracę swoich przedstawicieli w Grupie Współpracy.

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

7. Do 1 lutego 2024 r., a następnie co dwa lata Grupa Współpracy opracowuje program prac przedstawiający działania, które należy podjąć, by osiągnąć jej cele i wykonać jej zadania.

8. Komisja może przyjąć akty wykonawcze określające ustalenia proceduralne kluczowe do funkcjonowania Grupy Współpracy.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Komisja dzieli się poradami i współpracuje z Grupą Współpracy, tworząc projekty aktów wykonawczych, o których mowa w akapicie pierwszym niniejszego ustępu, zgodnie z ust. 4 lit. e).

9. Grupa Współpracy spotyka się regularnie, w każdym razie co najmniej raz w roku, z Grupą ds. Odporności Podmiotów Krytycznych utworzoną na podstawie dyrektywy (UE) 2022/2557, by propagować i ułatwiać współpracę strategiczną i wymianę informacji.

Artykuł 15

Sieć CSIRT

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

2. Sieć CSIRT składa się z przedstawicieli CSIRT wyznaczonych lub utworzonych zgodnie z art. 10 oraz zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach Unii (CERT-EU). Komisja uczestniczy w pracach sieci CSIRT jako obserwator. ENISA zapewnia sekretariat oraz aktywnie wspiera współpracę między CSIRT.

3. Do zadań sieci CSIRT należy:

a) wymiana informacji na temat zdolności CSIRT;

b) ułatwianie udostępniania, przekazywania i wymiany między CSIRT technologii i odpowiednich środków, polityki, narzędzi, procesów, dobrych praktyk i ram;

c) wymiana stosownych informacji na temat incydentów, potencjalnych zdarzeń dla cyberbezpieczeństwa, cyberzagrożeń, ryzyka i podatności;

d) wymiana informacji o publikacjach i rekomendacjach dotyczących cyberbezpieczeństwa;

e) zapewnienie interoperacyjności w specyfikacjach i protokołach wymiany informacji;

f) na wniosek członka sieci CSIRT, na którego potencjalnie może mieć wpływ incydent – wymiana i omówienie informacji o tym incydencie i związanych z nim cyberzagrożeniach, ryzyku i podatnościach;

g) na wniosek członka sieci CSIRT – omówienie oraz, w miarę możliwości, wdrożenie skoordynowanej reakcji na incydent wykryty w granicach jurysdykcji danego państwa członkowskiego;

h) pomaganie państwom członkowskim w reagowaniu na incydenty transgraniczne zgodnie z niniejszą dyrektywą;

i) współpraca i wymiana dobrych praktyk z CSIRT wyznaczonymi na koordynatorów zgodnie z art. 12 ust. 1 oraz pomaganie im w związku z zarządzaniem skoordynowanym ujawnianiem podatności mogących mieć znaczny wpływ na podmioty w więcej niż jednym państwie członkowskim;

j) 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 reagowaniu na ryzyka i incydenty transgraniczne;

   (v) wkładem w krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, o którym mowa w art. 9 ust. 4, na wniosek państwa członkowskiego;

k) informowanie Grupy Współpracy o działaniach sieci i o dalszych formach współpracy operacyjnej omawianych zgodnie z lit. j) oraz występowanie w razie potrzeby o wskazówki w tym zakresie;

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

m) na wniosek danego CSIRT – omawianie jego zdolności i gotowości;

n) współpraca i wymiana informacji z regionalnymi i unijnymi centrami monitorowania bezpieczeństwa (SOC) w celu poprawy wspólnej świadomości sytuacyjnej pod kątem incydentów i cyberzagrożeń w całej Unii;

o) w stosownych przypadkach omawianie sprawozdań z oceny wzajemnej, o których mowa w art. 19 ust. 9;

p) podawanie wytycznych mających ułatwić konwergencję praktyk operacyjnych w stosowaniu przepisów niniejszego artykułu dotyczących współpracy operacyjnej.

4. Na potrzeby przeglądu, o którym mowa w art. 40, sieć CSIRT do 17 stycznia 2025 r., a następnie co dwa lata ocenia postępy we współpracy operacyjnej i przyjmuje sprawozdanie. Sprawozdanie to zawiera w szczególności wnioski i zalecenia wynikające z ocen wzajemnych, o których mowa w art. 19, przeprowadzanych w odniesieniu do krajowych CSIRT. Sprawozdanie to przedkłada się Grupie Współpracy.

5. Sieć CSIRT przyjmuje swój regulamin.

6. Sieć CSIRT i EU-CyCLONe uzgadniają procedury i współpracują na ich podstawie.

Artykuł 16

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

1. Ustanawia się EU-CyCLONe, aby pomagać w skoordynowanym zarządzaniu na szczeblu operacyjnym incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę oraz zapewniać regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami, urzędami i agencjami Unii.

2. EU-CyCLONe składa się z przedstawicieli organów państw członkowskich ds. zarządzania kryzysowego w cyberbezpieczeństwie, a jeśli potencjalny lub trwający incydent w cyberbezpieczeństwie na dużą skalę ma lub może mieć znaczny wpływ na usługi i działania objęte zakresem stosowania niniejszej dyrektywy – także Komisji. W pozostałych przypadkach Komisja uczestniczy w działaniach EU-CyCLONe jako obserwator.

ENISA zapewnia obsługę sekretariatu EU-CyCLONe i pomaga w bezpiecznej wymianie informacji, a także dostarcza narzędzia kluczowe do wsparcia współpracy między państwami członkowskimi przez zapewnienie bezpiecznej wymiany informacji.

W stosownych przypadkach EU-CyCLONe może zapraszać przedstawicieli odpowiednich zainteresowanych stron, by uczestniczyli w jej pracach w charakterze obserwatorów.

3. EU-CyCLONe ma następujące zadania:

a) podnoszenie poziomu gotowości do zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę;

b) rozwijanie wspólnej świadomości sytuacyjnej pod kątem incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę;

c) ocenę konsekwencji i wpływu istotnych incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę oraz proponowanie możliwych środków ograniczających ryzyko;

d) koordynowanie zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę oraz wspieranie procesu decyzyjnego na szczeblu politycznym w odniesieniu do takich incydentów i sytuacji kryzysowych;

e) na wniosek zainteresowanego państwa członkowskiego – omawianie krajowych planów reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, o których mowa w art. 9 ust. 4.

4. EU-CyCLONe przyjmuje swój regulamin.

5. EU-CyCLONe regularnie składa Grupie Współpracy sprawozdania na temat zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę, a także na temat tendencji w tej dziedzinie, koncentrując się zwłaszcza na ich wpływie na podmioty kluczowe i ważne.

6. EU-CyCLONe współpracuje z siecią CSIRT na podstawie uzgodnionych ustaleń proceduralnych określonych w art. 15 ust. 6.

7. Do dnia 17 lipca 2024 r., a następnie co 18 miesięcy EU-CyCLONe przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie, w którym ocenia swoją pracę.

Artykuł 17

Współpraca międzynarodowa

Unia może w stosownych przypadkach zawierać zgodnie z art. 218 TFUE umowy międzynarodowe z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiające i organizujące ich udział w niektórych działaniach Grupy Współpracy oraz sieci CSIRT i EU-CyCLONe. Umowy takie są zgodne z unijnymi przepisami o ochronie danych.

Artykuł 18

Sprawozdanie o stanie cyberbezpieczeństwa w Unii

1. Co dwa lata ENISA przyjmuje we współpracy z Komisją i Grupą Współpracy sprawozdanie o stanie cyberbezpieczeństwa w Unii oraz przedkłada i przedstawia to sprawozdanie Parlamentowi Europejskiemu. Sprawozdanie udostępnia się m. in. jako dane nadające się do odczytu maszynowego i zawiera ono następujące elementy:

a) oszacowanie ryzyka w cyberbezpieczeństwie na poziomie Unii, z uwzględnieniem krajobrazu cyberzagrożeń;

b) ocenę rozwoju zdolności w zakresie cyberbezpieczeństwa w sektorach publicznym i prywatnym w całej Unii;

c) ocenę ogólnego poziomu wiedzy o cyberbezpieczeństwie i cyberhigienie wśród obywateli i podmiotów, w tym małych i średnich przedsiębiorstw;

d) zbiorczą ocenę wyników ocen wzajemnych, o których mowa w art. 19;

e) zbiorczą ocenę poziomu dojrzałości zdolności i zasobów w zakresie cyberbezpieczeństwa w całej Unii, w tym na poziomie sektorowym, a także stopnia wzajemnego dostosowania krajowych strategii cyberbezpieczeństwa państw członkowskich.

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

3. We współpracy z Komisją, Grupą Współpracy i siecią CSIRT ENISA opracowuje metodykę zbiorczej oceny, o której mowa w ust. 1 lit. e), w tym odpowiednie zmienne – np. wskaźniki ilościowe i jakościowe.

Artykuł 19

Oceny wzajemne

1. Do 17 stycznia 2025 r. Grupa Współpracy ustala – z pomocą Komisji i ENISA oraz, w stosownych przypadkach, sieci CSIRT – metodykę i aspekty organizacyjne ocen wzajemnych, by wyciągać wnioski ze wspólnych doświadczeń, zwiększać wzajemne zaufanie, osiągnąć wysoki wspólny poziom cyberbezpieczeństwa, a także zwiększać kluczowe do wdrożenia niniejszej dyrektywy zdolności państw członkowskich w zakresie cyberbezpieczeństwa i doskonalić ich politykę w tej dziedzinie. Udział w ocenach wzajemnych jest dobrowolny. Oceny wzajemne przeprowadzą eksperci ds. cyberbezpieczeństwa. Ekspertów ds. cyberbezpieczeństwa wyznaczają co najmniej dwa państwa członkowskie inne niż państwo członkowskie poddawane ocenie.

Oceny wzajemne dotyczą co najmniej jednej z następujących kwestii:

a) stopień wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązków dotyczących zgłaszania incydentów określonych w art. 21 i 23;

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

c) zdolność operacyjna CSIRT;

d) poziom wdrożenia wzajemnej pomocy, o której mowa w art. 37;

e) poziom wdrożenia ustaleń dotyczących mechanizmów wymiany informacji, o których mowa w art. 29;

f) szczególne zagadnienia transgraniczne lub międzysektorowe.

2. Metodyka, o której mowa w ust. 1, obejmuje obiektywne, niedyskryminacyjne, sprawiedliwe i przejrzyste kryteria, na podstawie których państwa członkowskie wyznaczają ekspertów ds. cyberbezpieczeństwa uprawnionych do prowadzenia ocen wzajemnych. Komisja i ENISA uczestniczą w ocenach wzajemnych w charakterze obserwatorów.

3. Państwa członkowskie mogą wskazać do oceny wzajemnej konkretne zagadnienia, o których mowa w ust. 1 lit. f).

4. Przed rozpoczęciem oceny wzajemnej, o której mowa w ust. 1, państwa członkowskie powiadamiają uczestniczące państwa członkowskim o jej zakresie, w tym o konkretnych zagadnieniach wskazanych na podstawie ust. 3.

5. Przed rozpoczęciem oceny wzajemnej państwa członkowskie mogą przeprowadzić ocenę własną aspektów poddawanych ocenie i przekazać jej wyniki wyznaczonym ekspertom ds. cyberbezpieczeństwa. Grupa Współpracy z pomocą Komisji i ENISA określa metodykę oceny własnej prowadzonej przez państwa członkowskie.

6. Oceny wzajemne wiążą się z fizycznymi lub zdalnymi kontrolami na miejscu i zdalną wymianą informacji. Zgodnie z zasadą dobrej współpracy państwo członkowskie poddane ocenie wzajemnej dostarcza wyznaczonym ekspertom ds. cyberbezpieczeństwa informacji potrzebnych do oceny, bez uszczerbku dla unijnych lub krajowych przepisów o ochronie informacji poufnych lub niejawnych oraz dla zagwarantowania podstawowych funkcji państwa, takich jak bezpieczeństwo narodowe. Grupa Współpracy we współpracy z Komisją i ENISA opracowuje odpowiednie kodeksy postępowania jako podstawę metod pracy wyznaczonych ekspertów ds. cyberbezpieczeństwa. Informacje uzyskane w trakcie oceny wzajemnej wykorzystuje się wyłącznie na potrzeby tej oceny. Eksperci ds. cyberbezpieczeństwa uczestniczący w ocenie wzajemnej nie ujawniają osobom trzecim informacji szczególnie chronionych lub poufnych uzyskanych w trakcie tej oceny.

7. Aspektów poddanych ocenie wzajemnej i ocenionych w danym państwie członkowskim nie poddaje się dalszej ocenie wzajemnej w tym państwie członkowskim przez dwa lata od zakończenia oceny wzajemnej, chyba że to państwo członkowskie zwróci się o przeprowadzenie takiej oceny lub zostanie ona uzgodniona na wniosek Grupy Współpracy.

8. Państwa członkowskie zapewniają ujawnienie pozostałym państwom członkowskim, Grupie Współpracy, Komisji i ENISA – przed rozpoczęciem oceny wzajemnej – ryzyka konfliktu interesów dotyczącego wyznaczonych ekspertów ds. cyberbezpieczeństwa. Państwo członkowskie poddane ocenie wzajemnej może sprzeciwić się wyznaczeniu konkretnych ekspertów ds. cyberbezpieczeństwa z należycie uzasadnionych powodów, o których informuje się Grupę Współpracy.

9. Eksperci ds. cyberbezpieczeństwa uczestniczący w ocenach wzajemnych sporządzają sprawozdania zawierające ustalenia i wnioski z tych ocen. Państwa członkowskie poddane ocenie wzajemnej mogą zgłaszać uwagi do projektów sprawozdań, które ich dotyczą, a uwagi te załącza się do sprawozdań. Sprawozdania te zawierają zalecenia umożliwiające poprawę w aspektach objętych oceną wzajemną. W stosownych przypadkach sprawozdania przedkłada się Grupie Współpracy i sieci CSIRT. Państwo członkowskie poddane ocenie wzajemnej może podjąć decyzję o podaniu do wiadomości publicznej sprawozdania z oceny wzajemnej lub jego zredagowanej wersji.

ROZDZIAŁ IV

ŚRODKI ZARZĄDZANIA RYZYKIEM W CYBERBEZPIECZEŃSTWIE I OBOWIĄZKI DOTYCZĄCE ZGŁASZANIA INCYDENTÓW

Artykuł 20

Zarządzanie

1. Państwa członkowskie zapewniają, aby organy zarządzające podmiotów kluczowych i ważnych zatwierdzały środki zarządzania ryzykiem w cyberbezpieczeństwie przyjęte przez te podmioty w celu zapewnienia zgodności z art. 21, nadzorowały ich wdrażanie i mogły być pociągnięte do odpowiedzialności za naruszanie przez te podmioty tego artykułu.

Stosowanie niniejszego ustępu nie narusza przepisów krajowych dotyczących zasad odpowiedzialności instytucji publicznych oraz odpowiedzialności urzędników publicznych oraz urzędników wybranych lub mianowanych.

2. Państwa członkowskie zapewniają, aby członkowie organu zarządzającego podmiotów kluczowych i ważnych mieli obowiązek odbywać regularne szkolenia w celu zdobycia wystarczającej wiedzy i umiejętności pozwalających im rozpoznać ryzyko i ocenić praktyki zarządzania ryzykiem w cyberbezpieczeństwie oraz ich wpływ na usługi świadczone przez dany podmiot, a także zachęcają podmioty kluczowe i ważne do oferowania podobnych szkoleń ich pracownikom.

Artykuł 21

Środki zarządzania ryzykiem w cyberbezpieczeństwie

1. Państwa członkowskie zapewniają, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.

Przy uwzględnieniu najnowszego stanu wiedzy oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, a także kosztów wdrożenia środki, o których mowa w akapicie pierwszym, zapewniają poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. Oceniając proporcjonalność tych środków, należycie uwzględnia się stopień narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze.

2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy:

a) politykę analizy ryzyka i bezpieczeństwa systemów informatycznych;

b) obsługę incydentu;

c) ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe;

d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;

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 służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;

g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;

h) polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;

i) bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;

j) w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

3. Państwa członkowskie zapewniają, aby rozważając które ze środków, o których mowa w ust. 2 lit. d) niniejszego artykułu, są odpowiednie, podmioty uwzględniały podatności charakterystyczne dla każdego bezpośredniego dostawcy i usługodawcy oraz ogólną jakość produktów i praktyk cyberbezpieczeństwa dostawców i usługodawców, w tym ich procedury bezpiecznego opracowywania. Państwa członkowskie zapewniają również, aby rozważając, które ze środków, o których mowa w tej literze, są odpowiednie, podmioty musiały uwzględniać wyniki skoordynowanych oszacowań ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw przeprowadzonych zgodnie z art. 22 ust. 1.

4. Państwa członkowskie zapewniają, aby podmiot, który stwierdzi, że nie spełnia środków określonych w ust. 2, bez zbędnej zwłoki wprowadził wszelkie istotne, odpowiednie i proporcjonalne środki naprawcze.

5. Do 17 października 2024 r. Komisja przyjmuje akty wykonawcze określające wymogi techniczne i metodykę dotyczącą środków, o których mowa w ust. 2, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform sieci społecznościowych i dostawców usług zaufania.

Komisja może przyjąć akty wykonawcze określające wymogi techniczne i metodykę, a w razie potrzeby również wymogi sektorowe dotyczące środków, o których mowa w ust. 2, w odniesieniu do podmiotów kluczowych i ważnych innych niż te, o których mowa w akapicie pierwszym niniejszego ustępu.

Przygotowując akty wykonawcze, o których mowa w akapitach pierwszym i drugim niniejszego ustępu, Komisja na tyle, na ile to możliwe stosuje się do norm międzynarodowych i europejskich, a także odpowiednich specyfikacji technicznych. Komisja wymienia się poradami i wraz z Grupą Współpracy i ENISA współpracuje nad projektami aktów wykonawczych zgodnie z art. 14 ust. 4 lit. e).

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Artykuł 22

Skoordynowane na poziomie Unii szacowanie ryzyka krytycznych łańcuchów dostaw

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

2. Po konsultacji z Grupą Współpracy i ENISA oraz w razie potrzeby z odpowiednimi zainteresowanymi stronami Komisja wskazuje konkretne krytyczne usługi ICT, systemy ICT lub produkty ICT, które można poddać skoordynowanemu oszacowaniu ryzyka dla bezpieczeństwa, o którym mowa w ust. 1.

Artykuł 23

Obowiązki w zakresie zgłaszania incydentów

1. Każde państwo członkowskie zapewnia, aby podmioty kluczowe i ważne bez zbędnej zwłoki zgłaszały swojemu właściwemu CSIRT lub, jeżeli ma to zastosowanie, swojemu właściwemu organowi, zgodnie z ust. 4, incydent mający istotny wpływ na świadczenie przez nie usług, o którym mowa w ust. 3 (poważny incydent). W stosownych przypadkach dane podmioty bez zbędnej zwłoki powiadamiają odbiorców swoich usług o poważnych incydentach, które mogą mieć niekorzystny wpływ na świadczenie tych usług. Każde państwo członkowskie zapewnia, aby podmioty te zgłaszały m.in. informacje umożliwiające CSIRT lub, jeżeli ma to zastosowanie, właściwemu organowi ustalenie transgranicznego wpływu incydentu. Samo zgłoszenie nie nakłada na podmiot zgłaszający zwiększonej odpowiedzialności.

Jeżeli dane podmioty zgłoszą poważny incydent właściwemu organowi na podstawie akapitu pierwszego, państwo członkowskie zapewnia, aby ten właściwy organ po otrzymaniu zgłoszenia przekazał je CSIRT.

W razie wystąpienia transgranicznego lub międzysektorowego poważnego incydentu państwa członkowskie zapewniają, aby ich pojedyncze punkty kontaktowe w stosownym czasie otrzymały ważne informacje zgłoszone zgodnie z ust. 4.

2. Jeżeli ma to zastosowanie, państwa członkowskie zapewniają, aby podmioty kluczowe i ważne bez zbędnej zwłoki powiadamiały odbiorców swoich usług, których potencjalnie dotyczy poważne cyberzagrożenie, o środkach zaradczych lub innych środkach, które ci odbiorcy mogą zastosować w reakcji na to zagrożenie. W stosownych przypadkach podmioty te informują również tych odbiorców o samym poważnym cyberzagrożeniu.

3. Incydent uznaje się za poważny, jeżeli:

a) spowodował lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu;

b) wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe.

4. Państwa członkowskie zapewniają, aby do celów zgłoszenia na podstawie ust. 1 dane podmioty przedkładały CSIRT lub, jeżeli ma to zastosowanie, właściwemu organowi:

a) bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia wiedzy o poważnym incydencie – wczesne ostrzeżenie, w którym w stosownych przypadkach wskazuje się, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze lub czy mógł wywrzeć wpływ transgraniczny;

b) bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od powzięcia wiedzy o poważnym incydencie – zgłoszenie incydentu, w stosownych przypadkach z aktualizacją informacji, o których mowa w lit. a), i wskazaniem wstępnej oceny poważnego incydentu, w tym jego dotkliwości i skutków, a w stosownych przypadkach także wskaźników integralności systemu;

c) na wniosek CSIRT lub, jeżeli ma to zastosowanie, właściwego organu – sprawozdanie okresowe na temat odpowiednich aktualizacji statusu;

d) sprawozdanie końcowe nie później niż miesiąc po zgłoszeniu incydentu na podstawie lit. b), zawierające następujące elementy:

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

   (ii) rodzaj zagrożenia lub pierwotną przyczynę, która prawdopodobnie była źródłem incydentu;

   (iii) zastosowane i wdrażane środki ograniczające ryzyko;

   (iv) w stosownych przypadkach transgraniczne skutki incydentu;

e) jeżeli incydent nie zakończył się w terminie składania sprawozdania końcowego, o którym mowa w lit. d), państwa członkowskie zapewniają, aby zainteresowane podmioty przedstawiły w tym momencie sprawozdanie z postępu prac, a sprawozdanie końcowe – w ciągu miesiąca od zakończenia przez nich obsługi incydentu.

Na zasadzie odstępstwa od akapitu pierwszego lit. b) dostawca usług zaufania zgłasza poważne incydenty, które mają wpływ na świadczenie jego usług zaufania CSIRT lub, w stosownych przypadkach, właściwemu organowi, bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia informacji o takim poważnym incydencie.

5. CSIRT lub właściwy organ bez zbędnej zwłoki i w miarę możliwości w ciągu 24 godzin od otrzymania wczesnego ostrzeżenia, o którym mowa w ust. 4 lit. a), odpowiada podmiotowi zgłaszającemu, w tym przekazuje mu wstępne informacje zwrotne na temat poważnego incydentu oraz, na wniosek podmiotu, wytyczne lub porady operacyjne dotyczące wdrożenia możliwych środków ograniczających ryzyko. Jeżeli CSIRT nie jest pierwszym odbiorcą zgłoszenia, o którym mowa w ust. 1, wytyczne przedstawia właściwy organ we współpracy z CSIRT. Na wniosek zainteresowanego podmiotu CSIRT zapewnia dodatkowe wsparcie techniczne. Jeżeli zachodzi podejrzenie, że poważny incydent ma cechy przestępstwa, CSIRT lub właściwy organ przedstawia również wytyczne dotyczące zgłaszania poważnego incydentu organom ścigania.

6. W stosownych przypadkach, zwłaszcza gdy poważny incydent dotyczy co najmniej dwóch państw członkowskich, CSIRT, właściwy organ lub pojedynczy punkt kontaktowy bez zbędnej zwłoki informują o tym poważnym incydencie pozostałe państwa członkowskie, których on dotyczy, i ENISA. Takie informacje obejmują informacje otrzymane zgodnie z ust. 4. W działaniach tych CSIRT, właściwy organ lub pojedynczy punkt kontaktowy zgodnie z prawem Unii lub prawem krajowym chronią bezpieczeństwo i interesy handlowe podmiotu oraz poufność przekazanych informacji.

7. Jeżeli świadomość społeczeństwa jest niezbędna, żeby zapobiec wystąpieniu poważnego incydentu lub poradzić sobie z trwającym poważnym incydentem, lub jeżeli ujawnienie poważnego incydentu z innych względów leży w interesie publicznym, CSIRT państwa członkowskiego lub, jeżeli ma to zastosowanie, jego właściwy organ, a w stosownych przypadkach CSIRT lub właściwe organy innych zainteresowanych państw członkowskich mogą, po konsultacji z zainteresowanym podmiotem, poinformować społeczeństwo o poważnym incydencie lub zobowiązać do tego ten podmiot.

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

9. Pojedynczy punkt kontaktowy co trzy miesiące przedkłada ENISA sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane o poważnych incydentach, incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgłoszonych zgodnie z ust. 1 niniejszego artykułu oraz art. 30. Aby przyczynić się do dostarczania porównywalnych informacji, ENISA może przyjąć wytyczne techniczne dotyczące parametrów informacji, jakie należy zawrzeć w sprawozdaniu podsumowującym. Co sześć miesięcy ENISA informuje Grupę Współpracy i sieć CSIRT o ustaleniach wynikających z otrzymanych zgłoszeń.

10. CSIRT lub, w stosownych przypadkach, właściwe organy przekazują właściwym organom zgodnie z dyrektywą (UE) 2022/2557 informacje o poważnych incydentach, incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgłoszonych zgodnie z ust. 1 niniejszego artykułu i z art. 30 przez podmioty wskazane jako podmioty krytyczne na mocy dyrektywy (UE) 2022/2557.

11. Komisja może przyjąć akty wykonawcze doprecyzowujące rodzaj informacji, format i procedurę zgłoszenia składanego zgodnie z ust. 1 niniejszego artykułu i z art. 30 oraz powiadomienia składanych zgodnie z ust. 2 niniejszego artykułu.

Do dnia 17 października 2024 r. Komisja, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych, przyjmuje akty wykonawcze doprecyzowujące przypadki, w których incydent uznaje się za poważny zgodnie z ust. 3. Komisja może przyjąć takie akty wykonawcze w odniesieniu do innych podmiotów kluczowych i ważnych.

Komisja zgodnie z art. 14 ust. 4 lit. e) wymienia się poradami i współpracuje z Grupą Współpracy, tworząc projekty aktów wykonawczych, o których mowa w akapitach pierwszym i drugim niniejszego ustępu.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

Artykuł 24

Stosowanie europejskich programów certyfikacji cyberbezpieczeństwa

1. Aby wykazać zgodność ze szczególnymi wymogami art. 21, państwa członkowskie mogą wymagać od podmiotów kluczowych i ważnych stosowania konkretnych produktów ICT, usług ICT i procesów ICT opracowanych przez dany podmiot kluczowy lub ważny lub nabytych od osób trzecich, certyfikowanych zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa przyjętymi na podstawie art. 49 rozporządzenia (UE) 2019/881. Ponadto państwa członkowskie zachęcają podmioty kluczowe i ważne do korzystania z kwalifikowanych usług zaufania.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 38 w celu uzupełnienia niniejszej dyrektywy przez określenie, od których kategorii podmiotów kluczowych i ważnych należy wymagać stosowania certyfikowanych produktów ICT, usług ICT i procesów ICT lub uzyskania certyfikacji dla swoich własnych produktów ICT, usług ICT i procesów ICT na podstawie europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego zgodnie z art. 49 rozporządzenia (UE) 2019/881. Te akty delegowane przyjmuje się w razie stwierdzenia niewystarczających poziomów cyberbezpieczeństwa i określa się w nich termin wdrażania.

Przed przyjęciem takich aktów delegowanych Komisja przeprowadza ocenę skutków i prowadzi konsultacje zgodnie z art. 56 rozporządzenia (UE) 2019/881.

3. Jeżeli do celów ust. 2 żaden z europejskich programów certyfikacji cyberbezpieczeństwa nie jest odpowiedni, Komisja może – po zasięgnięciu opinii Grupy Współpracy i Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa – zwrócić się do ENISA o przygotowanie propozycji programu zgodnie z art. 48 ust. 2 rozporządzenia (UE) 2019/881.

Artykuł 25

Normalizacja

1. Aby wspierać spójne wdrażanie art. 21 ust. 1 i 2, państwa członkowskie, nie narzucając ani nie faworyzując stosowania określonego rodzaju technologii, zachęcają do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych.

2. ENISA we współpracy z państwami członkowskimi i – w stosownych przypadkach – po zasięgnięciu opinii odpowiednich zainteresowanych stron opracowuje porady i wytyczne dotyczące obszarów technicznych, które należy wziąć pod uwagę w związku z ust.1, a także już istniejących norm, w tym norm krajowych, które pozwoliłyby uwzględnić te obszary.

ROZDZIAŁ V

JURYSDYKCJA I REJESTRACJA

Artykuł 26

Jurysdykcja i terytorialność

1. Podmioty objęte zakresem stosowania niniejszej dyrektywy uznaje się za podlegające jurysdykcji państwa członkowskiego, w którym mają miejsce prowadzenia działalności, z następującymi wyjątkami:

a) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej uznaje się za podlegających jurysdykcji państwa członkowskiego, w którym świadczą usługi;

b) dostawców usług DNS, rejestry nazw TLD, podmioty świadczące usługi rejestracji nazw domen, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, a także dostawców internetowych platform handlowych, wyszukiwarek internetowych lub platform usług sieci społecznościowych uznaje się za podlegających jurysdykcji państwa członkowskiego, w której mają główne miejsce prowadzenia działalności w Unii zgodnie z ust. 2;

c) podmioty administracji publicznej uznaje się za podlegające jurysdykcji państwa członkowskiego, które je ustanowiło.

2. Do celów niniejszej dyrektywy uznaje się, że podmiot, o którym mowa w ust. 1 lit. b), ma swoje główne miejsce prowadzenia działalności w Unii w tym państwie członkowskim, w którym przeważnie podejmuje decyzje związane ze środkami zarządzania ryzykiem w cyberbezpieczeństwie. Jeżeli nie można ustalić takiego państwa członkowskiego lub jeżeli takich decyzji nie podejmuje się w Unii, uznaje się, że główne miejsce prowadzenia działalności znajduje się w państwie członkowskim, w którym prowadzone są działania w zakresie cyberbezpieczeństwa. Jeżeli nie można ustalić takiego państwa członkowskiego, uznaje się, że główne miejsce prowadzenia działalności znajduje się w państwie członkowskim, w którym dany podmiot ma miejsce prowadzenia działalności o największej liczbie pracowników w Unii.

3. Jeżeli podmiot, o którym mowa w ust. 1 lit. b), nie ma miejsca prowadzenia działalności w Unii, ale oferuje usługi w Unii, wyznacza przedstawiciela w Unii. Przedstawiciel musi mieć miejsce prowadzenia działalności w jednym z tych państw członkowskich, w których oferowane są usługi. Uznaje się, że taki podmiot podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel ma miejsce prowadzenia działalności. W razie niewyznaczenia przedstawiciela w Unii na podstawie niniejszego artykułu państwo członkowskie, w którym dany podmiot świadczy usługi, może podjąć wobec tego podmiotu działania prawne w związku z naruszeniem niniejszej dyrektywy.

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

5. Państwa członkowskie, które otrzymały wniosek o wzajemną pomoc w odniesieniu do podmiotu, o którym mowa w ust. 1 lit. b), mogą – nie wykraczając poza zakres tego wniosku – zastosować odpowiednie środki nadzoru i egzekwowania przepisów w odniesieniu do danego podmiotu świadczącego usługi lub mającego sieć i system informatyczny na ich terytorium.

Artykuł 27

Rejestr podmiotów

1. ENISA tworzy i prowadzi rejestr dostawców usługi DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych, na podstawie informacji otrzymanych z pojedynczych punktów kontaktowych, zgodnie z ust. 4. Na wniosek ENISA zezwala właściwym organom na dostęp do rejestru, w stosownych przypadkach zapewniając jednocześnie gwarancje niezbędne do ochrony poufności informacji.

2. Do dnia 17 stycznia 2025 r. państwa członkowskie wymagają od podmiotów, o których mowa w ust. 1, przedłożenia właściwym organom następujących informacji:

a) nazwy podmiotu;

b) odpowiedniego sektora, podsektora i rodzaju podmiotu, o których mowa w załączniku I lub II, w stosownych przypadkach;

c) adresu głównego miejsca prowadzenia działalności podmiotu oraz jego innych prawnych miejsc prowadzenia działalności w Unii lub – jeżeli nie ma on miejsca prowadzenia działalności w Unii – przedstawiciela wyznaczonego zgodnie z art. 26 ust. 3;

d) aktualnych danych kontaktowych, w tym adresów poczty elektronicznej i numerów telefonów podmiotu oraz, w stosownych przypadkach, przedstawiciela wyznaczonego zgodnie z art. 26 ust. 3;

e) państwa członkowskie, w których podmiot świadczy usługi; oraz

f) zakresów IP podmiotu.

3. Państwa członkowskie zapewniają, aby podmioty, o których mowa w ust. 1, powiadamiały właściwy organ o zmianach w danych przedłożonych na podstawie ust. 2 niezwłocznie, a w każdym razie w ciągu trzech miesięcy od dnia, w którym nastąpiła zmiana.

4. Po otrzymaniu informacji, o których mowa w ust. 2 i 3, z wyjątkiem informacji, o których mowa w ust. 2 lit. f), pojedynczy punkt kontaktowy danego państwa członkowskiego przekazuje te informacje, bez zbędnej zwłoki, ENISA.

5. W stosownych przypadkach informacje, o których mowa w ust. 2 i 3 niniejszego artykułu, przedkłada się z wykorzystaniem mechanizmu krajowego, o którym mowa w art. 3 ust. 4 akapit czwarty.

Artykuł 28

Baza danych dotyczących rejestracji nazw domen

1. By przyczynić się do bezpieczeństwa, stabilności i odporności DNS, państwa członkowskie wymagają by rejestrów nazw TLD i podmioty świadczące usługi rejestracji nazw domen gromadziły i zachowywały z należytą starannością w specjalnej bazie danych dokładne i kompletne dane dotyczące rejestracji nazw domen zgodnie z unijnymi przepisami o ochronie danych w odniesieniu do danych będących danymi osobowymi.

2. Do celów ust. 1 państwa członkowskie wymagają, by baza danych dotycząca rejestracji nazw domen zawierała informacje kluczowe do zidentyfikowania posiadaczy nazw domen i punktów kontaktowych zarządzających nazwami domen TLD oraz do skontaktowania się z nimi. Informacje te obejmują:

a) nazwę domeny;

b) datę rejestracji;

c) imię i nazwisko lub nazwę osoby rejestrującej oraz adres poczty elektronicznej i numer telefonu;

d) adres poczty elektronicznej i numer telefonu, pod którymi można skontaktować się z punktem kontaktowym zarządzającym nazwą domeny, w przypadku gdy różnią się od adresu poczty elektronicznej i numeru telefonu osoby rejestrującej.

3. Państwa członkowskie wymagają, by rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen wdrożyły polityki i procedury, w tym procedury weryfikacji, służące zapewnieniu, aby bazy danych, o których mowa w ust. 1, zawierały dokładne i kompletne dane. Państwa członkowskie wymagają podania takich polityk i procedur do wiadomości publicznej.

4. Państwa członkowskie wymagają, aby po rejestracji nazwy domeny rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen bez zbędnej zwłoki podawały do wiadomości publicznej dane dotyczące rejestracji nazwy domeny niebędące danymi osobowymi.

5. Państwa członkowskie wymagają, by rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen na zgodny z prawem i należycie uzasadniony wniosek o prawnie uzasadniony dostęp udzielały dostępu do konkretnych danych dotyczących rejestracji nazw domen zgodnie z unijnymi przepisami o ochronie danych. Państwa członkowskie wymagają, by rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen udzielały odpowiedzi bez zbędnej zwłoki, a w każdym razie w ciągu nie więcej niż 72 godzin od otrzymania wniosku o dostęp. Państwa członkowskie wymagają podania do wiadomości publicznej polityk i procedur ujawniania takich danych.

6. Wypełnianie obowiązków określonych w ust. 1–5 nie prowadzi do powielania gromadzenia danych dotyczących rejestracji nazw domen. W tym celu państwa członkowskie wymagają wzajemnej współpracy od rejestrów nazw TLD i podmiotów świadczących usługi rejestracji nazw domen.

ROZDZIAŁ VI

WYMIANA INFORMACJI

Artykuł 29

Mechanizmy wymiany informacji na temat cyberbezpieczeństwa

1. Państwa członkowskie zapewniają, aby podmioty objęte zakresem stosowania niniejszej dyrektywy, a w stosownych przypadkach również inne podmioty nieobjęte zakresem niniejszej dyrektywy mogły dobrowolnie wymieniać się odpowiednimi informacjami na temat cyberbezpieczeństwa, w tym informacjami o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacjami o grupach przestępczych, ostrzeżeniami dotyczącymi cyberbezpieczeństwa i zaleceniami dotyczącymi konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki, jeżeli wymiana takich informacji:

a) ma na celu zapobieganie incydentom, ich wykrywanie, reagowanie na nie, przywracanie normalnego działania po incydentach lub łagodzenie ich skutków;

b) zwiększa poziom cyberbezpieczeństwa, zwłaszcza przez podnoszenie świadomości na temat cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się cyberzagrożeń, wspieranie różnorodnych zdolności do obrony przed nimi, eliminowanie i ujawnianie podatności, techniki wykrywania zagrożeń, ograniczania ich zasięgu i zapobiegania im, strategie ograniczania ryzyka, etapy reagowania i przywracania normalnego działania lub sprzyjanie współpracy między podmiotami publicznymi i prywatnymi w badaniach nad cyberzagrożeniami.

2. Państwa członkowskie zapewniają, aby wymiana informacji odbywała się w społecznościach podmiotów kluczowych i ważnych, a w stosownych przypadkach również ich dostawców lub usługodawców. Wymianę taką prowadzi się za pośrednictwem mechanizmów wymiany informacji o cyberbezpieczeństwie ze względu na potencjalnie poufny charakter wymienianych informacji.

3. Państwa członkowskie ułatwiają tworzenie mechanizmów wymiany informacji o cyberbezpieczeństwie, o których mowa w ust. 2 niniejszego artykułu. W mechanizmach tych można określić elementy operacyjne, w tym korzystanie ze specjalnych platform ICT i narzędzi automatyzacji, a także treści i warunki funkcjonowania mechanizmów wymiany informacji. Określając szczegóły udziału organów publicznych w tych mechanizmach, państwa członkowskie mogą ustalać warunki udostępniania informacji przez właściwe organy lub CSIRT. Państwa członkowskie oferują pomoc w stosowaniu takich mechanizmów zgodnie ze swoją polityką, o której mowa w art. 7 ust. 2 lit. h).

4. Państwa członkowskie zapewniają, by podmioty kluczowe i ważne powiadamiały właściwe organy, że uczestniczą w mechanizmach wymiany informacji, o których mowa w ust. 2, gdy przystępują do tych mechanizmów, lub, w stosownych przypadkach, o wycofaniu się z takich mechanizmów, gdy wycofanie stanie się skuteczne.

5. ENISA pomaga w tworzeniu mechanizmów wymiany informacji na temat cyberbezpieczeństwa, o których mowa w ust. 2, przez wymianę najlepszych praktyk i udzielanie wskazówek.

Artykuł 30

Dobrowolne zgłaszanie ważnych informacji

1. Państwa członkowskie zapewniają, by w uzupełnieniu obowiązków zgłaszania, o których mowa w art. 23, następujące podmioty mogły dobrowolnie przekazywać zgłoszenia CSIRT lub, w stosownych przypadkach, właściwym organom:

a) podmioty kluczowe i ważne w przypadku incydentów, cyberzagrożeń i potencjalnych zdarzeń dla cyberbezpieczeństwa;

b) podmioty inne niż te, o których mowa w lit. a), niezależnie od tego, czy są objęte zakresem stosowania niniejszej dyrektywy, w odniesieniu do poważnych incydentów, cyberzagrożeń oraz potencjalnych zdarzeń dla cyberbezpieczeństwa.

2. Państwa członkowskie rozpatrują zgłoszenia, o których mowa w ust. 1 niniejszego artykułu, zgodnie z procedurą określoną w art. 23. Państwa członkowskie mogą rozpatrywać zgłoszenia obowiązkowe priorytetowo względem zgłoszeń dobrowolnych.

W razie potrzeby CSIRT oraz, w stosownych przypadkach, właściwe organy przekazują pojedynczym punktom kontaktowym informacje o zgłoszeniach otrzymanych na podstawie niniejszego artykułu, zapewniając przy tym poufność i odpowiednią ochronę informacji przekazanych przez podmiot zgłaszający. Bez uszczerbku dla zapobiegania, prowadzenia postępowań, wykrywania i ścigania przestępstw dobrowolne zgłaszanie nie może powodować nałożenia na podmiot zgłaszający żadnych dodatkowych obowiązków, którym by nie podlegał, gdyby nie przekazał zgłoszenia.

ROZDZIAŁ VII

NADZÓR I EGZEKWOWANIE PRZEPISÓW

Artykuł 31

Ogólne aspekty nadzoru i egzekwowania przepisów

1. Państwa członkowskie zapewniają, aby ich właściwe organy skutecznie monitorowały przestrzeganie niniejszej dyrektywy i stosowały środki niezbędne do zagwarantowania tego przestrzegania.

2. Państwa członkowskie mogą zezwolić ich właściwym organom na wprowadzenie hierarchii priorytetów w odniesieniu do zadań nadzorczych. Taka hierarchia priorytetów bazuje na podejściu uwzględniającym analizę ryzyka. W tym celu, wykonując zadania nadzorcze określone w art. 32 i 33, właściwe organy mogą określić metodykę nadzorczą pozwalającą ustalić hierarchię priorytetów w tych zadaniach na podstawie podejścia uwzględniającego analizę ryzyka.

3. Właściwe organy odpowiadając na incydenty, które doprowadziły do naruszeń danych osobowych, ściśle współpracują z organami nadzorczymi, na mocy rozporządzenia (UE) 2016/679, bez uszczerbku dla właściwości i zadań organów nadzorczych określonych w tym rozporządzeniu.

4. Bez uszczerbku dla krajowych ram ustawodawczych i instytucjonalnych państwa członkowskie zapewniają, aby nadzorując przestrzeganie niniejszej dyrektywy przez podmioty administracji publicznej oraz nakładając środki egzekwowania przepisów w odniesieniu do naruszeń niniejszej dyrektywy, właściwe organy posiadały odpowiednie uprawnienia do podejmowania takich zadań w sposób niezależny pod względem operacyjnym wobec nadzorowanych podmiotów administracji publicznej. Państwa członkowskie mogą podjąć decyzję o nałożeniu na te podmioty odpowiednich, proporcjonalnych i skutecznych środków nadzoru i egzekwowania przepisów zgodnie z krajowymi ramami ustawodawczymi i instytucjonalnymi.

Artykuł 32

Środki nadzoru i egzekwowania przepisów dla podmiotów kluczowych

1. Państwa członkowskie zapewniają, by środki nadzoru lub egzekwowania przepisów nakładane na podmioty kluczowe w odniesieniu do obowiązków określonych w niniejszej dyrektywie były skuteczne, proporcjonalne i odstraszające, stosownie do okoliczności każdego indywidualnego przypadku.

2. Państwa członkowskie zapewniają, by wykonując uprawnienia nadzorcze wobec podmiotów kluczowych, właściwe organy były uprawnione do objęcia tych podmiotów co najmniej:

a) kontrolami na miejscu i nadzorem zdalnym, w tym wyrywkowymi kontrolami prowadzonymi przez przeszkolonych specjalistów;

b) regularnymi ukierunkowanymi audytami bezpieczeństwa prowadzonymi przez niezależną instytucję lub właściwy organ;

c) audytami doraźnymi, w tym w uzasadnionych przypadkach w związku z wystąpieniem poważnego incydentu lub z naruszeniem niniejszej dyrektywy przez podmiot kluczowy;

d) skanami bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów szacowania ryzyka, w razie potrzeby we współpracy z danym podmiotem;

e) wnioskami o udzielenie informacji niezbędnych do oceny środków zarządzania ryzykiem w cyberbezpieczeństwie przyjętych przez dany podmiot, w tym udokumentowanej polityki cyberbezpieczeństwa, a także zgodności z obowiązkiem przedkładania informacji właściwym organom zgodnie z art. 27;

f) wnioskami o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania ich zadań nadzorczych;

g) wnioskami o przedstawienie dowodów realizacji polityki cyberbezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora oraz odpowiednie dowody.

Ukierunkowane audyty bezpieczeństwa, o których mowa w akapicie pierwszym lit. b), opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot bądź na innych dostępnych informacjach dotyczących ryzyka.

Wyniki ukierunkowanych audytów bezpieczeństwa udostępnia się właściwemu organowi. Koszty takiego ukierunkowanego audytu bezpieczeństwa prowadzonego przez niezależną instytucję pokrywa podmiot poddawany audytowi, z wyjątkiem należycie uzasadnionych przypadków, gdy właściwy organ postanowi inaczej.

3. Wykonując swoje uprawnienia na mocy ust. 2 lit. e), f) lub g), właściwe organy podają cel wniosku i określają informacje, o które wnoszą.

4. Państwa członkowskie zapewniają, aby wykonując uprawnienia w zakresie egzekwowania przepisów wobec podmiotów kluczowych, ich właściwe organy były uprawnione co najmniej do:

a) wydawania ostrzeżeń dotyczących naruszeń przez dane podmioty niniejszej dyrektywy;

b) wydawania wiążących poleceń – w tym dotyczących podjęcia środków niezbędnych do zapobieżenia incydentowi lub usunięcia jego skutków oraz określenia terminów wdrożenia takich środków i zgłoszenia ich wdrożenia – lub nakazów zobowiązujących dane podmioty do naprawienia stwierdzonych uchybień lub usunięcia naruszeń niniejszej dyrektywy;

c) nakazania danym podmiotom, by zaniechały postępowania naruszającego niniejszą dyrektywę i nie powtarzały takiego postępowania;

d) nakazania danym podmiotom, by w określony sposób i w określonym terminie zapewniły zgodność swoich środków zarządzania ryzykiem w cyberbezpieczeństwie z art. 21 lub wypełniły obowiązki zgłaszania incydentów określone w art. 23;

e) nakazania danym podmiotom, by poinformowały osoby fizyczne lub prawne, w odniesieniu do których świadczą usługi lub prowadzą działania, a których potencjalnie dotyczy poważne cyberzagrożenie, o charakterze tego zagrożenia, a także o możliwych środkach ochronnych lub naprawczych, jakie te osoby fizyczne lub prawne mogą zastosować w reakcji na to zagrożenie;

f) nakazania danym podmiotom, by w rozsądnym terminie wdrożyły zalecenia wydane w wyniku audytu bezpieczeństwa;

g) wyznaczenia urzędnika monitorującego – ze ściśle określonymi zadaniami na oznaczony okres – do nadzorowania przestrzegania przez dane podmioty art. 21 i 23;

h) nakazania danym podmiotom, by w określony sposób podały do wiadomości publicznej informacje o naruszeniach niniejszej dyrektywy;

i) nałożenia lub zwrócenia się o nałożenie przez właściwe organy lub sądy zgodnie z prawem krajowym administracyjnej kary pieniężnej zgodnie z art. 34 niezależnie od środków, o których mowa w lit. a)–h) niniejszego ustępu.

5. Jeżeli środki z zakresu egzekwowania przepisów zastosowane na podstawie ust. 4 lit. a)–d) i f) okażą się nieskuteczne, państwa członkowskie zapewniają, by ich właściwe organy były uprawnione do wyznaczenia terminu, do którego podmiot kluczowy jest zobowiązany podjąć działania konieczne do usunięcia uchybień lub zapewnienia zgodności z wymogami określonymi przez te organy. Jeżeli żądane działanie nie zostanie podjęte w wyznaczonym terminie, państwa członkowskie zapewniają, by właściwe organy były uprawnione do:

a) tymczasowego zawieszenia lub zwrócenia się do organu, który przyznał certyfikację lub udzielił zezwolenia, lub do sądu, zgodnie z prawem krajowym, o tymczasowe zawieszenie certyfikacji lub zezwolenia na niektóre lub wszystkie odpowiednie usługi świadczone bądź na część lub całość działalności prowadzonej przez podmiot kluczowy;

b) zwrócenia się do właściwych instytucji lub sądów, zgodnie z prawem krajowym**,** o nałożenie tymczasowego zakazu pełnienia funkcji zarządczych w tym podmiocie kluczowym na osobę fizyczną wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela prawnego w tym podmiocie.

Tymczasowe zawieszenie lub zakaz pełnienia funkcji na podstawie niniejszego ustępu stosuje się tylko do czasu, gdy dany podmiot podejmie działania niezbędne do usunięcia uchybień lub spełnienia wymogów właściwego organu, w związku z którymi nałożono na niego środki egzekwowania przepisów. Takie tymczasowe zawieszenie lub zakaz stosuje się z zastrzeżeniem odpowiednich gwarancji proceduralnych zgodnych z ogólnymi zasadami prawa Unii i z Kartą, w tym prawa do skutecznej ochrony prawnej i do rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony.

Środki egzekwowania przepisów określone w niniejszym ustępie nie mają zastosowania do podmiotów administracji publicznej objętych zakresem niniejszej dyrektywy.

6. Państwa członkowskie zapewniają, aby każda osoba fizyczna odpowiedzialna za podmiot kluczowy lub działająca w charakterze przedstawiciela prawnego tego podmiotu na podstawie uprawnienia do jego reprezentowania, podejmowania decyzji w jego imieniu lub sprawowania nad nim kontroli była uprawniona do zapewnienia przestrzegania przez ten podmiot niniejszej dyrektywy. Państwa członkowskie zapewniają, by te osoby fizyczne mogły być pociągnięte do odpowiedzialności za niewywiązanie się z obowiązku zapewnienia przestrzegania niniejszej dyrektywy.

W odniesieniu do podmiotów administracji publicznej niniejszy ustęp pozostaje bez uszczerbku dla przepisów krajowych dotyczących odpowiedzialności urzędników publicznych oraz osób pełniących funkcję z wyboru lub powołania.

7. Przyjmując środki egzekwowania przepisów, o których mowa w ust. 4 lub 5, właściwe organy przestrzegają prawa do obrony oraz biorą pod uwagę okoliczności każdego indywidualnego przypadku i należycie uwzględniają co najmniej:

a) wagę naruszenia i znaczenie naruszonych przepisów, przy czym za poważne należy uznać w każdym przypadku m.in. następujące naruszenia:

   (i) powtarzające się naruszenia;

   (ii) niezgłoszenie lub nieusunięcie poważnych incydentów;

   (iii) nieusunięcie uchybień zgodnie z wiążącymi nakazami właściwych organów;

   (iv) utrudnianie prowadzenia audytów lub działań monitorujących nakazanych przez właściwy organ po stwierdzeniu naruszenia;

   (v) dostarczanie nieprawdziwych lub rażąco niedokładnych informacji w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków zgłaszania incydentów ustanowionych w art. 21 i 23;

b) czas trwania naruszenia;

c) istotne wcześniejsze naruszenia ze strony danego podmiotu;

d) spowodowane szkody majątkowe i niemajątkowe, w tym straty finansowe lub gospodarcze, wpływ na inne usługi i liczbę użytkowników, których dotyka incydent;

e) umyślny lub nieumyślny charakter czynu ze strony sprawcy naruszenia;

f) środki zastosowane przez podmiot, aby zapobiec szkodom majątkowym i niemajątkowym lub je ograniczyć;

g) stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji;

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

8. Właściwe organy przedstawiają szczegółowe uzasadnienie zastosowanych środków z zakresu egzekwowania przepisów. Zanim zastosują takie środki, właściwe organy powiadamiają dane podmioty o swoich wstępnych ustaleniach. Dają im one też rozsądny czas na przedstawienie uwag, z wyjątkiem należycie uzasadnionych przypadków, gdy utrudniłoby to natychmiastowe działanie w celu zapobieżenia incydentom lub reakcji na nie.

9. Państwa członkowskie zapewniają, aby ich właściwe organy na mocy niniejszej dyrektywy informowały odpowiednie właściwe organy w tym samym państwie członkowskim na podstawie dyrektywy (UE) 2022/2557, gdy wykonują uprawnienia w zakresie nadzoru i egzekwowania przepisów, aby zapewnić przestrzeganie niniejszej dyrektywy przez podmiot uznany za krytyczny zgodnie z dyrektywą (UE) 2022/2557. W stosownych przypadkach właściwe organy na podstawie dyrektywy (UE) 2022/2557 mogą zwrócić się do właściwych organów na podstawie niniejszej dyrektywy o wykonanie ich uprawnień z zakresu nadzoru i egzekwowania przepisów w stosunku do podmiotu i wskazanego jako podmiot krytyczny na podstawie dyrektywy (UE) 2022/2557.

10. Państwa członkowskie zapewniają, by ich właściwe organy zgodnie z niniejszą dyrektywą współpracowały z odpowiednimi właściwymi organami zainteresowanego państwa członkowskiego zgodnie z rozporządzeniem (UE) 2022/2554. W szczególności państwa członkowskie zapewniają, by ich właściwe organy na mocy niniejszej dyrektywy informowały forum nadzoru, ustanowione zgodnie z art. 32 ust. 1 rozporządzenia (UE) 2022/2554, gdy wykonują uprawnienia w zakresie nadzoru i egzekwowania przepisów, by zapewnić przestrzeganie niniejszej dyrektywy przez podmiot kluczowy, wyznaczony jako kluczowy dostawca usług ICT będący osobą trzecią zgodnie z art. 31 rozporządzenia (UE) 2022/2554.

Artykuł 33

Środki nadzoru i egzekwowania przepisów w odniesieniu do podmiotów ważnych

1. W przypadku otrzymania dowodu, wskazania lub informacji, że podmiot ważny rzekomo nie stosuje się do niniejszej dyrektywy, w szczególności jej w art. 21 i 23, państwa członkowskie zapewniają, by w razie potrzeby właściwe organy podjęły działania w postaci środków nadzoru *ex post*. Państwa członkowskie zapewniają, aby środki te były skuteczne, proporcjonalne i odstraszające stosownie do okoliczności każdego indywidualnego przypadku.

2. Państwa członkowskie zapewniają, by wykonując zadania nadzorcze wobec podmiotów ważnych, właściwe organy były uprawnione do objęcia tych podmiotów co najmniej:

a) kontrolami na miejscu i nadzorem zdalnym *ex post* prowadzonymi przez przeszkolonych specjalistów;

b) ukierunkowanymi audytami bezpieczeństwa prowadzonymi przez niezależną instytucję lub właściwy organ;

c) skanami bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów szacowania ryzyka, w razie potrzeby we współpracy z danym podmiotem;

d) wnioskami o udzielenie informacji niezbędnych do oceny *ex post* środków zarządzania ryzykiem w cyberbezpieczeństwie przyjętych przez dany podmiot, w tym udokumentowanej polityki cyberbezpieczeństwa, a także wypełnienia obowiązku przedłożenia informacji właściwym organom zgodnie z art. 27;

e) wnioskami o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania ich zadań nadzorczych;

f) wnioskami o przedstawienie dowodów realizacji polityki cyberbezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora oraz odpowiednie dowody.

Ukierunkowane audyty bezpieczeństwa, o których mowa w akapicie pierwszym lit. b), opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot bądź na innych dostępnych informacjach o ryzyku.

Wyniki ukierunkowanych audytów bezpieczeństwa udostępnia się właściwemu organowi. Koszty takiego ukierunkowanego audytu bezpieczeństwa prowadzonego przez niezależną instytucję pokrywa podmiot poddany audytowi, z wyjątkiem należycie uzasadnionych przypadków, gdy właściwy organ postanowi inaczej.

3. Wykonując swoje uprawnienia na mocy ust. 2 lit. d), e) lub f), właściwe organy podają cel wniosku i określają informacje, o które wnoszą.

4. Państwa członkowskie zapewniają, by wykonując uprawnienia w zakresie egzekwowania przepisów wobec podmiotów ważnych, właściwe organy były uprawnione co najmniej do:

a) wydawania ostrzeżeń dotyczących naruszania przez dane podmioty niniejszej dyrektywy;

b) przyjmowania wiążących poleceń lub nakazów zobowiązujących dane podmioty do naprawienia stwierdzonych uchybień lub usunięcia naruszenia niniejszej dyrektywy;

c) nakazania danym podmiotom, by zaniechały postępowania, które narusza niniejszą dyrektywę i nie powtarzały tego postępowania;

d) nakazania danym podmiotom, by w określony sposób i w określonym terminie zapewniły zgodność swoich środków zarządzania ryzykiem w cyberbezpieczeństwie z art. 21 lub wypełniły obowiązki zgłaszania incydentów określone w art. 23;

e) nakazania danym podmiotom, by poinformowały osoby fizyczne lub prawne, w odniesieniu do których świadczą usługi lub prowadzą działania, a których potencjalnie dotyczy poważne cyberzagrożenie, o charakterze tego zagrożenia, a także o możliwych środkach ochronnych lub naprawczych, jakie te osoby fizyczne lub prawne mogą zastosować w reakcji na to zagrożenie;

f) nakazania danym podmiotom, by w rozsądnym terminie wdrożyły zalecenia wydane w wyniku audytu bezpieczeństwa;

g) nakazania danym podmiotom, by w określony sposób podały do wiadomości publicznej informacje o naruszeniach przez nie niniejszej dyrektywy;

h) zastosowania lub zwrócenia się o zastosowanie przez właściwe organy lub sądy, zgodnie z prawem krajowym, administracyjnej kary pieniężnej na podstawie art. 34 oprócz środków, o których mowa w lit. a)–g) niniejszego ustępu.

5. Art. 32 ust. 6, 7 i 8 stosuje się odpowiednio do środków nadzoru i egzekwowania przepisów określonych w niniejszym artykule w odniesieniu do podmiotów ważnych.

6. Państwa członkowskie zapewniają, by ich właściwe organy zgodnie z niniejszą dyrektywą współpracowały z odpowiednimi właściwymi organami zainteresowanego państwa członkowskiego zgodnie z rozporządzeniem (UE) 2022/2554. W szczególności państwa członkowskie zapewniają, by ich właściwe organy na mocy niniejszej dyrektywy informowały forum nadzoru, ustanowione zgodnie z art. 32 ust. 1 rozporządzenia (UE) 2022/2554, gdy wykonują uprawnienia w zakresie nadzoru i egzekwowania przepisów, by zapewnić przestrzeganie niniejszej dyrektywy przez podmiot ważny, wyznaczony jako kluczowy dostawca usług ICT będący osobą trzecią zgodnie z art. 31 rozporządzenia (UE) 2022/2554.

Artykuł 34

Ogólne warunki nakładania administracyjnych kar pieniężnych na podmioty kluczowe i ważne

1. Państwa członkowskie zapewniają, by administracyjne kary pieniężne nakładane na podmioty kluczowe i ważne zgodnie z niniejszym artykułem za naruszenia niniejszej dyrektywy były skuteczne, proporcjonalne i odstraszające, stosownie do okoliczności każdego indywidualnego przypadku.

2. Administracyjne kary pieniężne nakłada się niezależnie od środków, o których mowa w art. 32 ust. 4 lit. a)–h), art. 32 ust. 5 i art. 33 ust. 4 lit. a)–g).

3. Podejmując decyzję o nałożeniu administracyjnej kary pieniężnej i o jej wysokości, w każdym indywidualnym przypadku należycie uwzględnia się co najmniej elementy wymienione w art. 32 ust. 7.

4. Państwa członkowskie zapewniają, by podmioty kluczowe dokonujące naruszeń art. 21 lub 23 podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej 10 000 000 EUR lub co najmniej 2 % łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot kluczowy, przy czym zastosowanie ma kwota wyższa.

5. Państwa członkowskie zapewniają, by podmioty ważne dokonujące naruszeń art. 21 lub 23 podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej 7 000 000 EUR lub 1,4 % łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot ważny, przy czym zastosowanie ma kwota wyższa.

6. Państwa członkowskie mogą przewidzieć uprawnienie do nakładania okresowych kar pieniężnych w celu przymuszenia podmiotu kluczowego lub ważnego do zaprzestania naruszenia niniejszej dyrektywy zgodnie z wcześniejszą decyzją właściwego organu.

7. Bez uszczerbku dla uprawnień właściwych organów na mocy art. 32 i 33, każde państwo członkowskie może ustanowić przepisy określające, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na podmioty administracji publicznej.

8. Jeżeli system prawny danego państwa członkowskiego nie przewiduje administracyjnych kar pieniężnych, to państwo członkowskie zapewnia takie stosowanie niniejszego artykułu, by o nałożenie kary pieniężnej wnosił właściwy organ, a nakładał ją właściwy sąd krajowy, przy zapewnieniu skuteczności tych rozwiązań prawnych i równoważności ich skutku względem administracyjnej kary pieniężnej nakładanej przez właściwe organy. W każdym przypadku nakładane kary pieniężne muszą być skuteczne, proporcjonalne i odstraszające. Do dnia 17 października 2024 r. państwo członkowskie powiadamia Komisję o przepisach, które przyjęło zgodnie z niniejszym ustępem, oraz niezwłocznie powiadamia o późniejszych przepisach zmieniających lub zmianach mających na nie wpływ.

Artykuł 35

Naruszenia pociągające za sobą naruszenie ochrony danych osobowych

1. Jeżeli w czasie nadzoru lub egzekwowania przepisów właściwe organy powzięły wiedzę, że naruszenie przez podmiot kluczowy lub ważny obowiązków określonych w art. 21 i 23 niniejszej dyrektywy może pociągać 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, bez zbędnej zwłoki informują o tym organy nadzorcze, o których mowa w art. 55 i 56 tego rozporządzenia.

2. Jeżeli organy nadzorcze, o których mowa w art. 55 lub 56 rozporządzenia (UE) 2016/679, nałożą administracyjną karę pieniężną na podstawie art. 58 ust. 2 lit. i) tego rozporządzenia, właściwe organy nie nakładają na podstawie art. 34 niniejszej dyrektywy administracyjnej kary pieniężnej za naruszenie, o którym mowa w ust. 1 niniejszego artykułu, wynikające z tego samego zachowania, za które nałożono administracyjną karę pieniężną na podstawie art. 58 ust. 2 lit. i) rozporządzenia (UE) 2016/679. Właściwe organy mogą jednak zastosować środki egzekwowania przepisów, określone w art. 32 ust. 4 lit. a)–h), art. 32 ust. 5 i art. 33 ust. 4 lit. a)–g) niniejszej dyrektywy.

3. Jeżeli organ nadzorczy właściwy na mocy rozporządzenia (UE) 2016/679 jest ustanowiony w innym państwie członkowskim niż właściwy organ, właściwy organ informuje organ nadzorczy ustanowiony w jego państwie członkowskim o naruszeniu ochrony danych osobowych, o którym mowa w ust. 1.

Artykuł 36

Kary

Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń przepisów i środków krajowych przyjętych na podstawie niniejszej dyrektywy i wprowadzają wszelkie środki niezbędne do zapewnienia wykonywania tych sankcji. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie najpóźniej do dnia 17 stycznia 2025 r. powiadamiają Komisję o tych przepisach i środkach, a następnie niezwłocznie powiadamiają ją o zmianach mających na nie wpływ.

Artykuł 37

Wzajemna pomoc

1. Jeżeli podmiot świadczy usługi w więcej niż jednym państwie członkowskim lub świadczy usługi w co najmniej jednym państwie członkowskim, a jego sieć i systemy informatyczne są zlokalizowane w co najmniej jednym innym państwie członkowskim, właściwe organy zainteresowanych 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 pozostałych zainteresowanych państwach członkowskich o zastosowanych środkach nadzoru i egzekwowania przepisów i konsultują się z tymi właściwymi organami w tej sprawie;

b) właściwy organ może zwrócić się do innego właściwego organu o zastosowanie środków nadzoru lub egzekwowania przepisów;

c) właściwy organ po otrzymaniu uzasadnionego wniosku od innego właściwego organu udziela temu innemu właściwemu organowi pomocy współmiernej do swoich zasobów, tak by można było skutecznie, wydajnie i spójnie wdrożyć środki nadzoru lub egzekwowania przepisów.

Wzajemna pomoc, o której mowa w akapicie pierwszym lit. c), może obejmować wnioski o udzielenie informacji i zastosowanie środków nadzoru, w tym wnioski o przeprowadzenie kontroli na miejscu lub nadzoru zewnętrznego lub ukierunkowanych audytów bezpieczeństwa. Właściwy organ, do którego skierowany jest wniosek o pomoc, nie może odmówić wykonania tego wniosku, chyba że zostanie ustalone, że organ ten nie jest organem właściwym do udzielenia pomocy, której dotyczy wniosek, że pomoc ta jest niewspółmierna do zadań nadzorczych właściwego organu lub że wniosek dotyczy informacji lub obejmuje działania, których ujawnienie lub wykonanie byłoby sprzeczne z podstawowymi interesami państwa członkowskiego w zakresie bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronnością. Zanim właściwy organ odmówi wykonania wniosku, zasięga opinii innych zainteresowanych właściwych organów, a na wniosek jednego z zainteresowanych państw członkowskich – także opinii Komisji i ENISA.

2. W stosownych przypadkach i za obopólnym porozumieniem właściwe organy z różnych państw członkowskich mogą prowadzić wspólne działania nadzorcze.

ROZDZIAŁ VIII

AKTY DELEGOWANE I WYKONAWCZE

Artykuł 38

Wykonywanie przekazanych uprawnień

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

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 24 ust. 2, powierza się Komisji na okres pięciu lat od 16 stycznia 2023 r.

3. Przekazanie uprawnień, o którym mowa w art. 24 ust. 2, może zostać odwołane w dowolnym momencie przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym 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. 24 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 39

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.

ROZDZIAŁ IX

PRZEPISY KOŃCOWE

Artykuł 40

Przegląd

Do dnia 17 października 2027 r., a następnie co 36 miesięcy Komisja przeprowadza przegląd funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdanie na ten temat. W sprawozdaniu ocenia się w szczególności znaczenie wielkości danych podmiotów oraz sektorów, podsektorów, rodzaju podmiotu, o którym 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. Sprawozdaniu towarzyszy w razie potrzeby wniosek ustawodawczy.

Artykuł 41

Transpozycja

1. Do dnia 17 października 2024 r. państwa członkowskie przyjmują i publikują przepisy niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają one o tym Komisję.

Państwa członkowskie stosują te przepisy od dnia 18 października 2024 r.

2. Przepisy, o których mowa w ust. 1, przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Sposób dokonywania takiego odniesienia określany jest przez państwa członkowskie.

Artykuł 42

Zmiana rozporządzenia (UE) nr 910/2014

W rozporządzeniu (UE) nr 910/2014 uchyla się art. 19 ze skutkiem od dnia 18 października 2024 r.

Artykuł 43

Zmiana dyrektywy (UE) 2018/1972

W dyrektywie (UE) 2018/1972 uchyla się art. 40 i 41 ze skutkiem od dnia 18 października 2024 r.

Artykuł 44

Uchylenie

Dyrektywa (UE) 2016/1148 traci moc ze skutkiem od dnia 18 października 2024 r.

Odesłania do uchylonej dyrektywy uznaje się za odesłania do niniejszej dyrektywy i odczytuje się zgodnie z tabelą korelacji w załączniku III.

Artykuł 45

Wejście w życie

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

Artykuł 46

Adresaci

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w Strasburgu dnia 14 grudnia 2022 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*
R. METSOLA	M. BEK

ZAŁĄCZNIK I

SEKTORY KLUCZOWE

Sektor	Podsektor	Rodzaj podmiotu
1. Energetyka	a) energia elektryczna	— przedsiębiorstwa energetyczne zgodnie z definicją w art. 2 pkt 57 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/944 ([1]), wykonujące funkcję dostaw zgodnie z definicją w art. 2 pkt 12 tej dyrektywy
		— operatorzy systemów dystrybucyjnych zgodnie z definicją w art. 2 pkt 29 dyrektywy (UE) 2019/944
		— operatorzy systemów przesyłowych zgodnie z definicją w art. 2 pkt 35 dyrektywy (UE) 2019/944
		— wytwórcy zgodnie z definicją w art. 2 pkt 38 dyrektywy (UE) 2019/944
		— wyznaczeni operatorzy rynku energii elektrycznej zgodnie z definicją w art. 2 pkt 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/943 ([2]) — uczestnicy rynku zgodnie z definicją w art. 2 pkt 25 rozporządzenia (UE) 2019/943 świadczący usługi agregacji, odpowiedzi odbioru lub magazynowania energii zgodnie z definicją w art. 2 pkt 18, 20 i 59 dyrektywy (UE) 2019/944 — operatorzy punktów ładowania odpowiedzialni za zarządzanie punktem ładowania i jego obsługę, świadczący usługę ładowania użytkownikom końcowym, w tym w imieniu i na rzecz dostawcy usług w zakresie mobilności
	b) system ciepłowniczy lub chłodniczy	— operatorzy systemów ciepłowniczych lub chłodniczych zgodnie z definicją w art. 2 pkt 19 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/2001 ([3])
	c) ropa naftowa	— operatorzy ropociągów
		— operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej
		— krajowe centrale zapasów zgodnie z definicją w art. 2 lit. f) dyrektywy Rady 2009/119/WE ([4])
	d) gaz	— przedsiębiorstwa dostarczające gaz zgodnie z definicją w art. 2 pkt 8 dyrektywy Parlamentu Europejskiego i Rady 2009/73/WE ([5])
		— operatorzy systemów dystrybucyjnych zgodnie z definicją w art. 2 pkt 6 dyrektywy 2009/73/WE
		— operatorzy systemów przesyłowych zgodnie z definicją w art. 2 pkt 4 dyrektywy 2009/73/WE
		— operatorzy systemów magazynowania zgodnie z definicją w art. 2 pkt 10 dyrektywy 2009/73/WE
		— operatorzy systemów LNG zgodnie z definicją w art. 2 pkt 12 dyrektywy 2009/73/WE
		— przedsiębiorstwa gazowe zgodnie z definicją w art. 2 pkt 1 dyrektywy 2009/73/WE
		— operatorzy instalacji służących do rafinacji i przetwarzania gazu ziemnego
	e) wodór	— operatorzy instalacji służących do produkcji, magazynowania i przesyłu wodoru

Sektor	Podsektor	Rodzaj podmiotu
2. Transport	a) transport lotniczy	— przewoźnicy lotniczy zgodnie z definicją w art. 3 pkt 4 rozporządzenia (WE) nr 300/2008, wykorzystywani do celów komercyjnych
		— zarządzający portem lotniczym zgodnie z definicją w art. 2 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2009/12/WE ([6]), porty lotnicze zgodnie z definicją w art. 2 pkt 1 tej dyrektywy, w tym porty bazowe wymienione w sekcji 2 załącznika II do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1315/2013 ([7]); oraz jednostki obsługujące urządzenia pomocnicze znajdujące się w portach lotniczych
		— operatorzy zarządzający ruchem lotniczym zapewniający służbę kontroli ruchu lotniczego (ATC) zgodnie z definicją w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 549/2004 ([8])
	b) transport kolejowy	— zarządcy infrastruktury zgodnie z definicją w art. 3 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2012/34/UE ([9])
		— przedsiębiorstwa kolejowe zgodnie z definicją w art. 3 pkt 1 dyrektywy 2012/34/UE, w tym operatorzy infrastruktury kolejowej zdefiniowanej w art. 3 pkt 12 tej dyrektywy
	c) transport wodny	— armatorzy śródlądowego, morskiego i przybrzeżnego wodnego transportu pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 725/2004 ([10]), z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy
		— organy zarządzające portami zgodnie z definicją w art. 3 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2005/65/WE ([11]), w tym ich obiekty portowe zgodnie z definicją w art. 2 pkt 11 rozporządzenia (WE) nr 725/2004; oraz jednostki wykonujące prace i operujące sprzętem znajdującym się w tych portach
		— operatorzy systemów ruchu statków (SRS) zgodnie z definicją w art. 3 lit. o) dyrektywy 2002/59/WE Parlamentu Europejskiego i Rady ([12])
	d) transport drogowy	— organy administracji drogowej zgodnie z definicją w art. 2 pkt 12 rozporządzenia delegowanego Komisji (UE) 2015/962 ([13]) odpowiedzialne za zarządzanie ruchem drogowym, z wyłączeniem podmiotów publicznych, dla których zarządzanie ruchem lub obsługa inteligentnych systemów transportowych jest inną niż istotna częścią ich ogólnej działalności
		— operatorzy inteligentnych systemów transportowych zgodnie z definicją w art. 4 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2010/40/UE ([14])
3. Bankowość		instytucje kredytowe zgodnie z definicją w art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 ([15])
4. Infrastruktura rynków finansowych		— operatorzy systemów obrotu zgodnie z definicją w art. 4 pkt 24 dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE ([16])
		— kontrahenci centralni (CCP) zgodnie z definicją w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 648/2012 ([17])

Sektor	Podsektor	Rodzaj podmiotu
5. Opieka zdrowotna		— świadczeniodawcy zgodnie z definicją w art. 3 lit. g) dyrektywy Parlamentu Europejskiego i Rady 2011/24/UE ([18])
		— laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2371 ([19])
		— podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych zdefiniowanych w art. 1 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2001/83/WE ([20]) — podmioty produkujące podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, o których mowa w sekcji C dział 21 klasyfikacji NACE Rev. 2 — podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego („wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego") w rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123 ([21])
6. Woda pitna		dostawcy i dystrybutorzy „wody przeznaczonej do spożycia przez ludzi" zdefiniowanej w art. 2 pkt 1 lit. a) dyrektywy Parlamentu Europejskiego i Rady (UE) 2020/2184 ([22]), z wyłączeniem dystrybutorów, dla których dystrybucja wody przeznaczonej do spożycia przez ludzi jest inną niż istotna częścią ich ogólnej działalności polegającej na dystrybucji innych produktów i towarów
7. Ścieki		przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki komunalne, bytowe lub przemysłowe zgodnie z definicją w art. 2 pkt 1, 2 i 3 dyrektywy Rady 91/271/EWG ([23]), z wyłączeniem przedsiębiorstw, dla których zbieranie, odprowadzanie lub oczyszczanie ścieków komunalnych, bytowych lub przemysłowych jest inną niż istotna częścią ich ogólnej działalności
8. Infrastruktura cyfrowa		— dostawcy punktu wymiany ruchu internetowego
		— dostawcy usług DNS, z wyłączeniem operatorów głównych serwerów nazw
		— rejestry nazw TLD
		— dostawcy usług chmurowych
		— dostawcy usług ośrodka przetwarzania danych
		— dostawcy sieci dostarczania treści
		— dostawcy usług zaufania
		— dostawcy publicznych sieci łączności elektronicznej
		— dostawcy publicznie dostępnych usług łączności elektronicznej
9. Zarządzanie usługami ICT (między przedsiębiorstwami)		— dostawcy usług zarządzanych — dostawcy usług zarządzanych w zakresie bezpieczeństwa

Sektor	Podsektor	Rodzaj podmiotu
10. Podmioty administracji publicznej,		— podmioty administracji publicznej w ramach instytucji rządowych na szczeblu centralnym zdefiniowane przez państwo członkowskie zgodnie z prawem krajowym
		— podmioty administracji publicznej na szczeblu regionalnym zdefiniowane przez państwo członkowskie zgodnie z prawem krajowym
11. Przestrzeń kosmiczna		operatorzy infrastruktury naziemnej należącej do, zarządzanej i obsługiwanej przez państwa członkowskie lub podmioty prywatne, które wspierają świadczenie usług kosmicznych, z wyjątkiem dostawców publicznych sieci łączności elektronicznej

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/944 z dnia 5 czerwca 2019 r. w sprawie wspólnych zasad rynku wewnętrznego energii elektrycznej oraz zmieniająca dyrektywę 2012/27/UE (Dz.U. L 158 z 14.6.2019, s. 125).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 z dnia 5 czerwca 2019 r. w sprawie rynku wewnętrznego energii elektrycznej (Dz.U. L 158 z 14.6.2019, s. 54).

([3]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/2001 z dnia 11 grudnia 2018 r. w sprawie promowania stosowania energii ze źródeł odnawialnych (Dz.U. L 328 z 21.12.2018, s. 82).

([4]) Dyrektywa Rady 2009/119/WE z dnia 14 września 2009 r. nakładająca na państwa członkowskie obowiązek utrzymywania minimalnych zapasów ropy naftowej lub produktów ropopochodnych (Dz.U. L 265 z 9.10.2009, s. 9).

([5]) Dyrektywa Parlamentu Europejskiego i Rady 2009/73/WE z dnia 13 lipca 2009 r. dotycząca wspólnych zasad rynku wewnętrznego gazu ziemnego i uchylająca dyrektywę 2003/55/WE (Dz.U. L 211 z 14.8.2009, s. 94).

([6]) Dyrektywa Parlamentu Europejskiego i Rady 2009/12/WE z dnia 11 marca 2009 r. w sprawie opłat lotniskowych (Dz.U. L 70 z 14.3.2009, s. 11).

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1315/2013 z dnia 11 grudnia 2013 r. w sprawie unijnych wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej i uchylające decyzję nr 661/2010/UE (Dz.U. L 348 z 20.12.2013, s. 1).

([8]) Rozporządzenie (WE) nr 549/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające ramy tworzenia Jednolitej Europejskiej Przestrzeni Powietrznej (rozporządzenie ramowe) (Dz.U. L 96 z 31.3.2004, s. 1).

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

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

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

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

([13]) Rozporządzenie delegowane Komisji (UE) 2015/962 z dnia 18 grudnia 2014 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2010/40/UE w odniesieniu do świadczenia ogólnounijnych usług informacyjnych w czasie rzeczywistym dotyczących ruchu (Dz.U. L 157 z 23.6.2015, s. 21).

([14]) Dyrektywa Parlamentu Europejskiego i Rady 2010/40/UE z dnia 7 lipca 2010 r. w sprawie ram wdrażania inteligentnych systemów transportowych w obszarze transportu drogowego oraz interfejsów z innymi rodzajami transportu (Dz.U. L 207 z 6.8.2010, s. 1).

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

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

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

([18]) Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.U. L 88 z 4.4.2011, s. 45).

([19]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylające decyzję nr 1082/2013/UE (Dz.U. L 314 z 6.12.2022, s. 26).

([20]) Dyrektywa 2001/83/WE Parlamentu Europejskiego i Rady z dnia 6 listopada 2001 r. w sprawie wspólnotowego kodeksu odnoszącego się do produktów leczniczych stosowanych u ludzi (Dz.U. L 311 z 28.11.2001, s. 67).

([21]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/123 z dnia 25 stycznia 2022 r. w sprawie wzmocnienia roli Europejskiej Agencji Leków w zakresie gotowości na wypadek sytuacji kryzysowej i zarządzania kryzysowego w odniesieniu do produktów leczniczych i wyrobów medycznych (Dz.U. L 20 z 31.1.2022, s. 1).

([22]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2020/2184 z dnia 16 grudnia 2020 r. w sprawie jakości wody przeznaczonej do spożycia przez ludzi (Dz.U. L 435 z 23.12.2020, s. 1).

([23]) Dyrektywa Rady 91/271/EWG z dnia 21 maja 1991 r. dotycząca oczyszczania ścieków komunalnych (Dz.U. L 135 z 30.5.1991, s. 40).

ZAŁĄCZNIK II

SEKTORY WAŻNE

Sektor	Podsektor	Rodzaj podmiotu
1. Usługi pocztowe i kurierskie		operatorzy świadczący usługi pocztowe zgodnie z definicją w art. 2 pkt 1a dyrektywy 97/67/WE, w tym dostawcy usług kurierskich
2. Gospodarowanie odpadami		przedsiębiorstwa zajmujące się gospodarowaniem odpadami zgodnie z definicją w art. 3 pkt 9 dyrektywy Parlamentu Europejskiego i Rady 2008/98/WE ([1]), z wyłączeniem przedsiębiorstw, dla których gospodarowanie odpadami nie stanowi głównej działalności gospodarczej
3. Produkcja, wytwarzanie i dystrybucja chemikaliów		przedsiębiorstwa zajmujące się produkcją substancji oraz wytwarzaniem i dystrybucją substancji lub mieszanin, o których mowa w art. 3 pkt 9 i 14 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady ([2]), a także przedsiębiorstwa zajmujące się wytwarzaniem z substancji lub mieszanin wyrobów zgodnie z definicją w art. 3 pkt 3 tego rozporządzenia
4. Produkcja, przetwarzanie i dystrybucja żywności		przedsiębiorstwa spożywcze zgodnie z definicją w art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady ([3]), zajmujące się dystrybucją hurtową oraz przemysłowymi produkcją i przetwarzaniem
5. Produkcja	a) produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	podmioty produkujące wyroby medyczne zdefiniowane w art. 2 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 ([4]) oraz podmioty produkujące wyroby medyczne do diagnostyki in vitro zdefiniowane w art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746 ([5]), z wyjątkiem podmiotów produkujących wyroby medyczne wymienione w załączniku I pkt 5 tiret piąte niniejszej dyrektywy
	b) produkcja komputerów, wyrobów elektronicznych i optycznych	przedsiębiorstwa prowadzące którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 26 klasyfikacji NACE Rev. 2
	c) produkcja urządzeń elektrycznych	przedsiębiorstwa prowadzące którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 27 klasyfikacji NACE Rev. 2
	d) produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana	przedsiębiorstwa prowadzące którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 28 klasyfikacji NACE Rev. 2
	e) produkcja pojazdów samochodowych, przyczep i naczep	przedsiębiorstwa prowadzące którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2
	f) produkcja pozostałego sprzętu transportowego	przedsiębiorstwa prowadzące którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2

Sektor	Podsektor	Rodzaj podmiotu
6. dostawcy usług cyfrowych		— dostawcy internetowych platform handlowych
		— dostawcy wyszukiwarek internetowych
		— dostawcy platform usług sieci społecznościowych
7. Badania naukowe		organizacje badawcze

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

([2]) Rozporządzenie (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH), utworzenia Europejskiej Agencji Chemikaliów, zmieniające dyrektywę 1999/45/WE oraz uchylające rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE (Dz.U. L 396 z 30.12.2006, s. 1).

([3]) Rozporządzenie (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności (Dz.U. L 31 z 1.2.2002, s. 1).

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz.U. L 117 z 5.5.2017, s. 1).

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz.U. L 117 z 5.5.2017, s. 176).

ZAŁĄCZNIK III

TABELA KORELACJI

Dyrektywa (UE) 2016/1148	Niniejsza dyrektywa
art. 1 ust. 1	art. 1 ust. 1
art. 1 ust. 2	art. 1 ust. 2
art. 1 ust. 3	–
art. 1 ust. 4	art. 2 ust. 12
art. 1 ust. 5	art. 2 ust. 13
art. 1 ust. 6	art. 2 ust. 6 i 11
art. 1 ust. 7	art. 2 ust. 4
art. 2	art. 2 ust. 14
art. 3	art. 5
art. 4	art. 6
art. 5	–
art. 6	–
art. 7 ust. 1	art. 7 ust. 1 i 2
art. 7 ust. 2	art. 7 ust. 4
art. 7 ust. 3	art. 7 ust. 3
art. 8 ust. 1–5	art. 8 ust. 1–5
art. 8 ust. 6	art. 13 ust. 4
art. 8 ust. 7	art. 8 ust. 6
art. 9 ust. 1, 2 i 3	art. 10 ust. 1, 2 i 3
art. 9 ust. 4	art. 10 ust. 9
art. 9 ust. 5	art. 10 ust. 19
art. 10 ust. 1, 2 i 3 akapit pierwszy	art. 11 ust. 1–3
Art. 10 ust. 3 akapit drugi	art. 23 ust. 9
art. 11 ust. 1	art. 14 ust. 1 i 2
art. 11 ust. 2	art. 14 ust. 3
art. 11 ust. 3	art. 14 ust. 4 i 6 akapit pierwszy lit. a)–q) i lit. s) oraz ust. 7
art. 11 ust. 4	art. 14 ust. 4 akapit pierwszy lit. r) i akapit drugi
art. 11 ust. 5	art. 14 ust. 8
art. 12 ust. 1–5	art. 15 ust. 1–5
art. 13	art. 17
art. 14 ust. 1 i 2	art. 21 ust. 1–4
art. 14 ust. 3	art. 23 ust. 1
art. 14 ust. 4	art. 23 ust. 3
art. 14 ust. 5	art. 23 ust. 5, 6 i 8

Dyrektywa (UE) 2016/1148	Niniejsza dyrektywa
art. 14 ust. 6	art. 23 ust. 7
art. 14 ust. 7	art. 23 ust. 11
art. 15 ust. 1	art. 31 ust. 1
art. 15 ust. 2 akapit pierwszy lit. a)	art. 32 ust. 2 lit. e)
art. 15 ust. 2 akapit pierwszy lit. b)	art. 32 ust. 2 lit. g)
art. 15 ust. 2 akapit drugi	art. 32 ust. 3
art. 15 ust. 3	art. 32 ust. 4 lit. b)
art. 15 ust. 4	art. 31 ust. 3
art. 16 ust. 1	art. 21 ust. 1–4
art. 16 ust. 3	art. 23 ust. 1
art. 16 ust. 4	art. 23 ust. 3
art. 16 ust. 5	–
art. 16 ust. 6	art. 23 ust. 6
art. 16 ust. 7	art. 23 ust. 7
art. 16 ust. 8 i 9	art. 21 ust. 5 i art. 23 ust. 11
art. 16 ust. 10	–
art. 16 ust. 11	art. 2 ust. 1, 2 i 3
art. 17 ust. 1	art. 33 ust. 1
art. 17 ust. 2 lit. a)	art. 32 ust. 2 lit. e)
art. 17 ust. 2 lit. b)	art. 32 ust. 4 lit. b)
art. 17 ust. 3	art. 37 ust. 1 lit. a) i b)
art. 18 ust. 1	art. 26 ust. 1–2
art. 18 ust. 2	art. 26 ust. 3
art. 18 ust. 3	art. 26 ust. 4
art. 19	art. 25
art. 20	art. 30
art. 21	art. 36
art. 22	art. 39
art. 23	art. 40
art. 24	–
art. 25	art. 41
art. 26	art. 45
art. 27	art. 46
załącznik I pkt 1	art. 11 ust. 1
załącznik I pkt 2 lit. a) ppkt (i)–(iv)	art. 11 ust. 2 lit. a)–d)

Dyrektywa (UE) 2016/1148	Niniejsza dyrektywa
załącznik I pkt 2 lit. a) ppkt (v)	art. 11 ust. 2 lit. f)
załącznik I pkt 2 lit. b)	art. 11 ust. 4
załącznik I pkt 2 lit. c) ppkt (i) i(ii)	art. 11 ust. 5 lit. a)
załącznik II	załącznik I
załącznik III pkt 1, 2	załącznik II pkt 6
załącznik III pkt 3	załącznik I pkt 8