Rada
Unii Europejskiej

Bruksela, 26 listopada 2021 r.
(OR. en)

14337/21

Międzyinstytucjonalny numer referencyjny:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

NOTA

Od:	Sekretariat Generalny Rady
Do:	Rada
Nr poprz. dok.:	9583/2/21, 11724/21
Nr dok. Kom.:	14150/20
Dotyczy:	Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 *– Podejście ogólne*

I. WPROWADZENIE

1. W dniu 16 grudnia 2020 r. Komisja przyjęła wniosek dotyczący dyrektywy w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii (zwanej dalej „zmienioną dyrektywą NIS" lub „NIS 2")[1] mający na celu zastąpienie obecnej dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych (zwanej dalej „dyrektywą NIS")[2].

[1] Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148.

[2] 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.

Wniosek ten był jednym z działań przewidzianych w strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[3] w celu zapewnienia obywatelom i przedsiębiorstwom możliwości korzystania z wiarygodnych technologii cyfrowych.

2. Przedmiotowy wniosek oparty jest na art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) i ma na celu dalsze wzmacnianie zdolności podmiotów publicznych i prywatnych, właściwych organów oraz Unii jako całości w zakresie odporności i reagowania na incydenty.

3. W Parlamencie Europejskim komisją przedmiotowo właściwą dla wniosku jest Komisja Przemysłu, Badań Naukowych i Energii (ITRE). Komisja ITRE przyjęła sprawozdanie sprawozdawcy w dniu 28 października 2021 r.

4. Europejski Komitet Ekonomiczno-Społeczny przyjął opinię w dniu 28 kwietnia 2021 r.

5. W dniu 3 lutego 2021 r. Komitet Stałych Przedstawicieli zdecydował o przeprowadzeniu konsultacji w sprawie wniosku z Europejskim Komitetem Regionów[4]. Europejski Komitet Regionów na razie nie wydał opinii.

6. Europejski Inspektor Ochrony Danych przyjął opinię w dniu 11 marca 2021 r.[5]

7. W swoich konkluzjach z dnia 22 marca 2021 r. w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[6] Rada przyjęła do wiadomości nowy wniosek, który czerpie z dyrektywy w sprawie bezpieczeństwa sieci i informacji, i ponownie podkreśliła swoje poparcie dla wzmocnienia i harmonizacji krajowych ram dotyczących cyberbezpieczeństwa oraz stałej współpracy państw członkowskich.

8. W swoich konkluzjach z dni 21–22 października 2021 r. Rada Europejska wezwała do przyspieszenia prac nad wnioskiem dotyczącym zmienionej dyrektywy NIS.

---

3 Dok. 14133/20.
4 Dok. 5573/21.
5 Opinia 5/2021 w sprawie strategii cyberbezpieczeństwa i dyrektywy NIS 2.0.
6 Dok. 6722/21.

II. PRACE W ORGANACH PRZYGOTOWAWCZYCH RADY

9. Na forum Rady analizę wniosku prowadzi Horyzontalna Grupa Robocza ds. Cyberprzestrzeni (zwana dalej „grupą roboczą ds. cyberprzestrzeni"). Analiza wniosku rozpoczęła się w dniu 19 stycznia podczas prezydencji portugalskiej od starannej analizy wniosku, podczas której państwa członkowskie miały możliwość zadawania pytań i przedstawienia swoich głównych obaw oraz uzyskania od Komisji szczegółowych wyjaśnień na temat zmian w poddawanej przeglądowi dyrektywie.

10. Jak dotąd w czasie prezydencji portugalskiej grupa robocza ds. cyberprzestrzeni poświęciła na prezentację i analizę wniosku 17 posiedzeń. W dniu 4 czerwca 2021 r. sprawozdanie z postępu tej analizy przedłożono Radzie ds. Transportu, Telekomunikacji i Energii.

11. Od tego czasu podczas prezydencji słoweńskiej prowadzone są dalsze i nasilone prace, a ich celem jest wypracowanie podejścia ogólnego na posiedzeniu Rady (ds. Transportu, Telekomunikacji i Energii) w dniu 3 grudnia 2021 r. Przeglądowi wniosku w sprawie NIS 2 prezydencja słoweńska poświęciła 15 posiedzeń i wiele dwustronnych dyskusji na wszystkich szczeblach.

12. Początkowo grupa robocza ds. cyberprzestrzeni skoncentrowała swoje prace nad przeformułowaniem tekstu wniosku m.in. na interakcjach dyrektywy NIS 2 z przepisami sektorowymi i na zakresie jej stosowania, w szczególności w odniesieniu do administracji publicznej, głównych serwerów DNS i klauzuli wyłączającej, a następnie skupiła się na innych zagadnieniach, takich jak oceny wzajemne, jurysdykcja i wzajemna pomoc, skoordynowane ujawnianie podatności, bazy danych nazw domen i dane dotyczące rejestracji domen oraz współpraca międzynarodowa.

13. Pierwszy kompromisowy wniosek dotyczący tekstu proponowanej dyrektywy został przedstawiony w dniu 21 września 2021 r.[7], w oparciu o pisemne uwagi i dokumenty robocze otrzymane od państw członkowskich, a także wcześniejsze kompromisowe propozycje dotyczące interakcji dyrektywy NIS 2 z przepisami sektorowymi oraz zakresu jej stosowania.

[7] Dok. 12019/21.

14. Ostatnia wersja[8] kompromisowej propozycji prezydencji była omawiana na szczeblu grupy roboczej w dniu 22 listopada 2021 r. Choć delegacje zasadniczo z zadowoleniem przyjęły tekst kompromisowy, kilka z nich zgłosiło zastrzeżenia weryfikacji lub uwagi do niektórych jego części. W niektórych częściach tekstu nadal sugerowano pewne techniczne przeformułowania.

III. KWESTIE MERYTORYCZNE

15. Na podstawie dyskusji na szczeblu grupy roboczej za główne kwestie polityczne uznano następujące zagadnienia:

a) Zakres stosowania (art. 2)

Od początku dyskusji nad wnioskiem w sprawie NIS 2 główna obawa wyrażana przez państwa członkowskie dotyczyła znacznego wzrostu liczby podmiotów objętych dyrektywą, a w szczególności wprowadzenia zasady maksymalnej wielkości, zgodnie z którą dyrektywie NIS 2 podlegają wszystkie średnie i duże podmioty działające w sektorach objętych zakresem stosowania dyrektywy NIS 2 lub świadczące usługi objęte zakresem stosowania dyrektywy NIS 2. Wniosek kompromisowy zachowuje tę ogólną zasadę, ale zawiera też dodatkowe przepisy mające na celu zapewnienie niezbędnej proporcjonalności, wyższego poziomu zarządzania ryzykiem i jasnych kryteriów decydujących o krytyczności przy określaniu podmiotów objętych zakresem stosowania tej dyrektywy. Ponadto wniosek kompromisowy zawiera szczegółowe przepisy dotyczące priorytetowego traktowania stosowania środków nadzoru na podstawie podejścia opartego na analizie ryzyka.

[8] Dok. 12019/5/21 REV 5.

b) Administracja publiczna (art. 2 ust. 2a)

Włączenie administracji publicznej do zakresu stosowania dyrektywy NIS 2 było tematem bardzo dyskutowanym z uwagi na to, że sektor administracji publicznej ma bardziej odrębny charakter niż inne sektory objęte dyrektywą NIS 2. Prezydencja dążyła do przyjęcia wyważonego podejścia, które uwzględni specyfikę krajowych ram administracji publicznej i zapewni państwom członkowskim pewien stopień elastyczności przy określaniu podmiotów administracji publicznej objętych zakresem stosowania dyrektywy NIS 2. W związku z tym w tekście kompromisowym dyrektywa NIS 2 ma zastosowanie do podmiotów administracji publicznej rządów centralnych, natomiast państwa członkowskie mogą również postanowić, że dyrektywa ma zastosowanie do jednostek administracji publicznej na szczeblu regionalnym i lokalnym.

c) Klauzula wyłączająca (art. 2 ust. 3a i art. 3aa)

Państwa członkowskie chciały doprecyzować klauzulę wyłączającą, tak by dyrektywa nie miała zastosowania do podmiotów, które prowadzą działalność głównie w obszarach obronności, bezpieczeństwa narodowego, bezpieczeństwa publicznego lub ścigania przestępstw, ani do działań związanych z bezpieczeństwem narodowym lub obronnością. Wyłączenie dotyczy także sądownictwa, parlamentów i banków centralnych.

d) Interakcja z przepisami sektorowymi

Państwa członkowskie podkreśliły potrzebę dostosowania dyrektywy NIS 2 do prawodawstwa sektorowego, w szczególności do rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (rozporządzenie DORA") oraz dyrektywy w sprawie odporności podmiotów krytycznych („dyrektywa CER"). Dyrektywa NIS 2, która powinna stanowić punkt odniesienia dla minimalnej harmonizacji w zakresie cyberbezpieczeństwa, zawiera specjalny artykuł dotyczący unijnych aktów sektorowych (art. 2b). Jeżeli chodzi o interakcje z dyrektywą CER, wniosek kompromisowy zapewnia większą jasność w odniesieniu do podejścia uwzględniającego wszystkie zagrożenia. Inne ważne uzupełnienia dotyczą ustaleń dotyczących współpracy między właściwymi organami na mocy poszczególnych aktów prawnych.

e) Wzajemne uczenie się (art. 16)

Niemal wszystkie państwa członkowskie sprzeciwiły się ustanowieniu przez Komisję obowiązkowych ocen wzajemnych. Proponowany kompromis zapewnia, że nowy mechanizm wzajemnego uczenia się opierać się będzie na wzajemnym zaufaniu, będzie miał charakter dobrowolny i będzie sterowany przez państwa członkowskie.

f) Jurysdykcja i terytorialność (art. 24) oraz wzajemna pomoc (art. 34)

Państwa członkowskie wyraziły obawy co do konsekwencji zróżnicowanej jurysdykcji dla podmiotów sektora ICT, wynikającej z propozycji Komisji. Tekst kompromisowy doprecyzował jurysdykcję w zależności od rodzaju podmiotu, a także wzmocnił sformułowania dotyczące wzajemnej pomocy.

g) Obowiązki w zakresie zgłaszania incydentów (art. 20)

Państwa członkowskie wyraziły obawy, że obowiązki te nadmiernie obciążą podmioty objęte zakresem stosowania dyrektywy NIS 2 i doprowadzą do zbyt częstego zgłaszania incydentów, dlatego w tekście kompromisowym wykluczono obowiązek zgłaszania znaczących cyberzagrożeń.

IV. PODSUMOWANIE

16. W dniu 24 listopada 2021 r. Komitet Stałych Przedstawicieli osiągnął porozumienie w sprawie tekstu kompromisowego w wersji zamieszczonej w załączniku i postanowił przedłożyć go Radzie (ds. Transportu, Telekomunikacji i Energii) w celu przyjęcia podejścia ogólnego.

17. Rada jest zatem proszona o to, by na posiedzeniu 3 grudnia 2021 r. zatwierdziła kompromisowy tekst prezydencji, w wersji zawartej w załączniku, a także by przyjęła podejście ogólne.

ZAŁĄCZNIK

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

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

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[9],

uwzględniając opinię Komitetu Regionów[10],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

[9] Dz.U. C z , s. .
[10] Dz.U. C z , s. .

a także mając na uwadze, co następuje:

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

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

---

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

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

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

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

(4) Podstawę prawną dyrektywy (UE) 2016/1148 stanowił art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), którego celem jest ustanowienie i funkcjonowanie rynku wewnętrznego przez usprawnienie środków służących zbliżeniu przepisów krajowych. Wymogi w zakresie cyberbezpieczeństwa nałożone na podmioty świadczące usługi lub prowadzące działalność istotną z ekonomicznego punktu widzenia różnią się znacznie w zależności od państwa członkowskiego pod względem rodzaju wymogów, ich poziomu szczegółowości oraz metody nadzoru. Rozbieżności te pociągają za sobą dodatkowe koszty i powodują trudności dla przedsiębiorstw, które oferują towary lub usługi w wymiarze transgranicznym. Wymogi nałożone przez jedno państwo członkowskie, które różnią się od wymogów nałożonych przez inne państwo członkowskie lub są nawet z nimi sprzeczne, mogą w istotny sposób wpływać na taką transgraniczną działalność.

Ponadto ewentualna nieoptymalna konstrukcja [...] **środków** dotyczących cyberbezpieczeństwa lub ewentualny nieoptymalny sposób ich wdrażania prawdopodobnie będą miały negatywny wpływ na poziom cyberbezpieczeństwa innych państw członkowskich, zwłaszcza biorąc pod uwagę intensywną wymianę transgraniczną. Z przeglądu dyrektywy (UE) 2016/1148 wynika, że istnieją znaczne rozbieżności, jeżeli chodzi o jej wdrażanie przez państwa członkowskie, w tym w odniesieniu do jej zakresu, w odniesieniu do którego pozostawiono państwom członkowskim duży margines swobody. W dyrektywie (UE) 2016/1148 zapewniono państwom członkowskim bardzo duży margines swobody także w odniesieniu do wdrażania określonych w niej obowiązków dotyczących bezpieczeństwa i zgłaszania incydentów. W rezultacie obowiązki te wdrożono na szczeblu krajowym w bardzo różny sposób. Podobny rozdźwięk we wdrażaniu miał miejsce w odniesieniu do przepisów wspomnianej dyrektywy dotyczących nadzoru i egzekwowania przepisów.

(5) Wszystkie te rozbieżności pociągają za sobą fragmentację rynku wewnętrznego i mogą mieć szkodliwy wpływ na jego funkcjonowanie, oddziałując w szczególności na transgraniczne świadczenie usług i poziom odporności pod względem cyberbezpieczeństwa ze względu na stosowanie różnych [...] **środków**. Celem niniejszej dyrektywy jest zatem wyeliminowanie takich rozbieżności między państwami członkowskimi, w szczególności przez określenie minimalnych przepisów dotyczących funkcjonowania skoordynowanych ram regulacyjnych, ustanowienie mechanizmów skutecznej współpracy między odpowiedzialnymi organami w każdym państwie członkowskim, dokonanie aktualizacji wykazu sektorów i działań podlegających obowiązkom w zakresie cyberbezpieczeństwa oraz ustanowienie skutecznych środków naprawczych i sankcji, które są kluczowe dla skutecznego egzekwowania tych obowiązków. Dyrektywę (UE) 2016/1148 należy zatem uchylić i zastąpić niniejszą dyrektywą.

(6) [...] Państwa członkowskie **powinny mieć możliwość** podjęcia środków niezbędnych do zapewnienia ochrony podstawowych interesów swojego bezpieczeństwa, do ochrony porządku publicznego i bezpieczeństwa publicznego oraz do umożliwienia prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw [...]. [...] **Niniejsza dyrektywa nie powinna mieć zastosowania do niektórych podmiotów publicznych lub prywatnych, które prowadzą działalność w tych obszarach. Nie powinna również mieć zastosowania do działalności podmiotów prowadzonej w tych obszarach. Ponadto** żadne państwo członkowskie nie ma obowiązku udzielania informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami jego bezpieczeństwa publicznego. [...] **Z**astosowanie mają krajowe [...] **lub** unijne przepisy dotyczące ochrony informacji niejawnych, umowy o zachowaniu poufności oraz nieformalne porozumienia o zachowaniu poufności, takie jak kod poufności TLP[14].

(6a) Prawo Unii dotyczące ochrony danych osobowych i prywatności ma zastosowanie do każdego przetwarzania danych osobowych na podstawie niniejszej dyrektywy. W szczególności niniejsza dyrektywa pozostaje bez uszczerbku dla rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 i dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady, a zatem nie powinna w szczególności wpływać na zadania i uprawnienia niezależnych organów nadzorczych właściwych w zakresie monitorowania przestrzegania odpowiednich unijnych przepisów o ochronie danych.

---

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

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

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

---

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

(8a) W celu uzyskania jasności co do tego, które podmioty są objęte zakresem stosowania niniejszej dyrektywy, państwa członkowskie powinny mieć możliwość ustanowienia krajowych mechanizmów samodzielnego powiadamiania, które zobowiążą podmioty podlegające niniejszej dyrektywie, do przedłożenia właściwym organom na mocy niniejszej dyrektywy lub jednostkom wyznaczonym do tego celu przez państwa członkowskie co najmniej swojego imienia i nazwiska lub swojej nazwy, adresu, danych kontaktowych i sektora, w którym prowadzą działalność, lub rodzaju usług, jakie świadczą, oraz, w stosownych przypadkach, wykazu państw członkowskich, w których świadczą usługi. Państwa członkowskie mogą podjąć decyzję w sprawie odpowiednich mechanizmów, jeżeli na szczeblu krajowym istnieją rejestry, które umożliwiają identyfikację podmiotów objętych zakresem stosowania niniejszej dyrektywy.

(9) Zakres stosowania niniejszej dyrektywy powinien obejmować także **mikropodmioty lub** małe podmioty [...] spełniające określone kryteria, które wskazują na zasadnicze znaczenie tych podmiotów dla gospodarek lub społeczeństw państw członkowskich lub dla konkretnych sektorów lub rodzajów usług. Państwa członkowskie powinny być odpowiedzialne za przedkładanie [...] Komisji **co najmniej odpowiednich informacji na temat liczby wskazanych podmiotów, sektora, do którego należą, lub rodzaju usług, jakie świadczą, oraz na temat konkretnych kryteriów, na podstawie których podmioty te zostały wskazane. Państwa członkowskie mogą również zdecydować, o ile jest to zgodne z krajowymi przepisami bezpieczeństwa, o przedłożeniu Komisji imion i nazwisk lub nazw tych podmiotów.**

(9a) Z zakresu stosowania niniejszej dyrektywy wyłączone są podmioty administracji publicznej prowadzące działalność w obszarach bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego, egzekwowania prawa, a także sądownictwa, parlamentów i banków centralnych. Do celów niniejszej dyrektywy podmioty posiadające kompetencje regulacyjne nie są uznawane za prowadzące działalność w obszarze egzekwowania prawa i w związku z tym nie są na tej podstawie wyłączone z zakresu stosowania niniejszej dyrektywy. Ponadto zakresem stosowania niniejszej dyrektywy nie są objęte podmioty administracji publicznej rządu centralnego utworzone wspólnie z państwem trzecim zgodnie z umową międzynarodową.

(9aa) Państwa członkowskie powinny mieć możliwość ustalenia, że podmioty wskazane przed wejściem w życie niniejszej dyrektywy jako operatorzy usług kluczowych zgodnie z dyrektywą (UE) 2016/1148 należy uznać za podmioty niezbędne.

(9aaa) Niniejsza dyrektywa nie ma zastosowania do misji dyplomatycznych i konsularnych państw członkowskich za granicą ani do ich infrastruktury ICT wykorzystywanej przez takie misje, o ile infrastruktura ta znajduje się za granicą lub jest wykorzystywana dla użytkowników za granicą.

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

(11) [...] **Podmioty objęte zakresem stosowania niniejszej dyrektywy należy podzielić na dwie kategorie: niezbędne i istotne, z uwzględnieniem poziomu krytyczności sektora lub rodzaju świadczonych przez nie usług, a także ich wielkości. W związku z tym właściwe organy powinny w stosownych przypadkach należycie uwzględniać wszelkie odpowiednie sektorowe oceny ryzyka lub wskazówki.** Zarówno podmioty niezbędne, jak i podmioty istotne powinny podlegać [...] wymogom w zakresie zarządzania ryzykiem i [...] obowiązkom w zakresie zgłaszania incydentów. Należy natomiast zróżnicować systemy nadzoru i kar między tymi dwoma kategoriami podmiotów, aby zapewnić odpowiednią równowagę między **opartymi na ryzyku** wymogami i obowiązkami z jednej strony a obciążeniem administracyjnym wynikającym z nadzoru nad zgodnością z przepisami z drugiej.

(12) **Niniejsza dyrektywa określa poziom odniesienia dla środków zarządzania ryzykiem w cyberprzestrzeni i obowiązków dotyczących zgłaszania incydentów we wszystkich sektorach, które wchodzą w zakres jej stosowania. Aby uniknąć fragmentacji przepisów dotyczących cyberbezpieczeństwa zawartych w aktach prawnych Unii, w przypadku gdy dodatkowe przepisy sektorowe dotyczące** środków zarządzania ryzykiem w cyberprzestrzeni i **obowiązków dotyczących zgłaszania incydentów uznaje się za niezbędne do zapewnienia wysokiego poziomu cyberbezpieczeństwa, Komisja powinna ocenić, czy takie przepisy mogłyby zostać określone w akcie wykonawczym na mocy uprawnienia przewidzianego w niniejszej dyrektywie. Gdyby takie akty nie były odpowiednie do tego celu,** przepisy sektorowe **mogłyby** przyczynić się do zapewnienia wysokiego poziomu [...] cyberbezpieczeństwa, przy pełnym uwzględnieniu specyfiki i złożoności [...] sektorów**, których to dotyczy**. **Powody, dla których akt wykonawczy na mocy uprawnienia przewidzianego w niniejszej dyrektywie nie jest odpowiedni, należy wyjaśnić w przepisach sektorowych. Jednocześnie takie sektorowe przepisy unijnych aktów prawnych powinny należycie uwzględniać potrzebę zapewnienia kompleksowych i zharmonizowanych ram cyberbezpieczeństwa.** [...] Pozostaje to bez uszczerbku dla istniejących uprawnień wykonawczych, które powierzono Komisji w wielu sektorach, w tym w sektorach transportu i energetyki.

(12a) W przypadku gdy unijny sektorowy akt prawny **zawiera przepisy** wymagające od podmiotów niezbędnych lub istotnych przyjęcia **środków co najmniej równoważnych pod względem skutku z obowiązkami określonymi w niniejszej dyrektywie dotyczącymi** zarządzania ryzykiem w cyberprzestrzeni [...] i **obowiązków** dotyczących zgłaszania **znaczących** incydentów lub znaczących cyberzagrożeń [...], zastosowanie powinny mieć te przepisy sektorowe**, w tym przepisy dotyczące nadzoru i egzekwowania przepisów**. **Przy określaniu równoważności pod względem skutku obowiązków określonych w przepisach sektorowych unijnego aktu prawnego należy wziąć pod uwagę następujące aspekty: (i) środki zarządzania ryzykiem w cyberprzestrzeni powinny obejmować odpowiednie i proporcjonalne środki techniczne i organizacyjne służące zarządzaniu ryzykami dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez odpowiednie podmioty w świadczeniu swoich usług oraz powinny obejmować co najmniej wszystkie elementy określone w niniejszej dyrektywie; (ii) obowiązek zgłaszania znaczących incydentów i cyberzagrożeń powinien być co najmniej równoważny z obowiązkami określonymi w niniejszej dyrektywie w odniesieniu do treści, formatu i terminów zgłoszeń; (iii) przewidziane w unijnych sektorowych aktach prawnych zasady zgłaszania przez podmioty i właściwe organy powinny być co najmniej równoważne z wymogami określonymi w niniejszej dyrektywie w odniesieniu do ich treści, formatu i terminów oraz powinny uwzględniać rolę CSIRT; (iv) wymogi w zakresie współpracy transgranicznej dotyczące właściwych organów powinny być co najmniej równoważne z wymogami określonymi w niniejszej dyrektywie. Jeżeli sektorowe przepisy unijnego aktu prawnego nie obejmują wszystkich podmiotów w konkretnym sektorze wchodzącym w zakres stosowania niniejszej dyrektywy, odpowiednie przepisy niniejszej dyrektywy powinny nadal mieć zastosowanie do podmiotów nieobjętych tymi przepisami sektorowymi.**

(12aa) Komisja **powinna dokonywać okresowego przeglądu stosowania równoważnego pod względem skutku wymogu w odniesieniu do sektorowych przepisów unijnych aktów prawnych** [...]. **Przygotowując ten okresowy przegląd, Komisja powinna konsultować się z Grupą Współpracy.**

(12aaa) Przyszłe unijne sektorowe akty prawne powinny należycie uwzględniać definicje określone w art. 4 niniejszej dyrektywy oraz ramy nadzoru i egzekwowania przepisów określone w rozdziale VI niniejszej dyrektywy.

(12ab) W przypadku gdy sektorowe przepisy unijnych aktów prawnych wymagają od niezbędnych lub istotnych podmiotów przyjęcia środków co najmniej równoważnych pod względem skutku z obowiązkami dotyczącymi zgłaszania incydentów określonymi w niniejszej dyrektywie, należy unikać nakładania się obowiązków dotyczących zgłaszania incydentów oraz zapewnić spójność i skuteczność postępowania ze zgłoszeniami cyberzagrożeń lub incydentów. W tym celu wspomniane przepisy sektorowe mogą umożliwiać państwom członkowskim ustanowienie wspólnego, automatycznego i bezpośredniego mechanizmu zgłaszania znaczących incydentów i cyberzagrożeń zarówno organom, których zadania są określone w odpowiednich przepisach sektorowych, jak i właściwym organom, w tym w stosownych przypadkach pojedynczemu punktowi kontaktowemu i CSIRT, odpowiedzialnym za zadania w zakresie cyberbezpieczeństwa przewidziane w niniejszej dyrektywie, lub mechanizmu zapewniającego systematyczną i natychmiastową wymianę informacji i współpracę między właściwymi organami i CSIRT w zakresie postępowania z takimi zgłoszeniami. Do celów uproszczenia zgłaszania i wdrożenia wspólnego, automatycznego i bezpośredniego mechanizmu zgłaszania incydentów państwa członkowskie mogą, zgodnie z przepisami sektorowymi, korzystać z pojedynczego punktu kontaktowego ustanowionego przez nie zgodnie z art. 11 ust. 5a niniejszej dyrektywy. Aby zapewnić harmonizację, należy dostosować obowiązki w zakresie zgłaszania incydentów zawarte w unijnych sektorowych aktach prawnych do obowiązków określonych w niniejszej dyrektywie. Państwa członkowskie mogą uznać, że właściwe organy na mocy niniejszej dyrektywy lub krajowe CSIRT są adresatami zgłoszeń, zgodnie z przepisami sektorowymi.

(13) Rozporządzenie Parlamentu Europejskiego i Rady XXXX/XXXX należy uznać w kontekście niniejszej dyrektywy za unijny sektorowy akt prawny w odniesieniu do podmiotów sektora finansowego. Zamiast przepisów **ustanowionych w** niniejszej dyrektywie zastosowanie powinny mieć przepisy rozporządzenia XXXX/XXXX dotyczące środków zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (ICT), zarządzania incydentami związanymi z ICT, a zwłaszcza zgłaszania incydentów, a także testowania operacyjnej odporności cyfrowej, mechanizmów wymiany informacji oraz ryzyka związanego z zewnętrznymi dostawcami ICT. Do żadnych podmiotów objętych rozporządzeniem XXXX/XXXX państwa członkowskie nie powinny zatem stosować przepisów niniejszej dyrektywy dotyczących zarządzania ryzykiem w cyberprzestrzeni, obowiązków w zakresie zgłaszania incydentów [...] oraz nadzoru i egzekwowania przepisów. Jednocześnie istotne jest, aby utrzymać silne relacje i skuteczną wymianę informacji z sektorem finansowym na gruncie niniejszej dyrektywy. W tym celu na podstawie rozporządzenia XXXX/XXXX Europejskim Urzędom Nadzoru właściwym dla sektora finansowego oraz właściwym organom krajowym na mocy rozporządzenia XXXX/XXXX umożliwiono udział w [...] **pracach** [...] Grupy Współpracy, a także wymianę informacji i współpracę z pojedynczymi punktami kontaktowymi wyznaczonymi na podstawie niniejszej dyrektywy, **jak również** [...] z krajowymi CSIRT. Właściwe organy na mocy rozporządzenia XXXX/XXXX powinny przekazywać dane na temat poważnych incydentów dotyczących ICT i **znaczących cyberzagrożeń** także pojedynczym punktom kontaktowym**, właściwym organom lub krajowym CSIRT wyznaczonym** na podstawie niniejszej dyrektywy. **Można to osiągnąć za pomocą automatycznego i bezpośredniego przekazywania zgłoszeń incydentów lub wspólnej platformy zgłaszania incydentów.** Ponadto państwa członkowskie powinny w dalszym ciągu uwzględniać sektor finansowy w swoich strategiach cyberbezpieczeństwa, a krajowe CSIRT **mogą** objąć go swoimi działaniami.

(13a) Aby uniknąć luk w obowiązkach i powielania obowiązków w zakresie cyberbezpieczeństwa nałożonych na podmioty w sektorze lotnictwa, o których mowa w pkt 2 lit. a) załącznika I, organy krajowe wyznaczone na mocy rozporządzenia (WE) nr 300/2008[16] Parlamentu Europejskiego i Rady i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139[17] oraz właściwe organy na mocy niniejszej dyrektywy powinny współpracować w zakresie wdrażania środków zarządzania ryzykiem w cyberprzestrzeni oraz nadzoru nad tymi środkami na szczeblu krajowym. Organy krajowe wyznaczone na podstawie rozporządzeń (WE) nr 300/2008 i (UE) 2018/1139 mogą uznać podmiot spełniający wymogi dotyczące środków zarządzania ryzykiem w cyberprzestrzeni na podstawie niniejszej dyrektywy za spełniający wymogi określone w tych rozporządzeniach oraz w odpowiednich aktach delegowanych i wykonawczych przyjętych na podstawie tych rozporządzeń.

---

16 **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).**

17 **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).**

(14) Biorąc pod uwagę powiązania między cyberbezpieczeństwem a bezpieczeństwem fizycznym podmiotów, należy zapewnić spójność pod względem podejścia między dyrektywą Parlamentu Europejskiego i Rady (UE) XXX/XXX a niniejszą dyrektywą. W tym celu państwa członkowskie powinny zapewnić, aby podmioty krytyczne, **[**oraz równoważne podmioty**]**, zgodnie z dyrektywą (UE) XXX/XXX uznawano za podmioty niezbędne w rozumieniu niniejszej dyrektywy. Państwa członkowskie powinny także zapewnić, aby ich strategie cyberbezpieczeństwa obejmowały ramy polityki na rzecz zwiększonej koordynacji między właściwym organem na mocy niniejszej dyrektywy a właściwym organem na mocy dyrektywy (UE) XXX/XXX w kontekście udostępniania informacji na temat incydentów i cyberzagrożeń oraz w kontekście wykonywania zadań nadzorczych. **Właściwe** [...] organy na mocy obu dyrektyw powinny ze sobą współpracować i prowadzić wymianę informacji, w szczególności w odniesieniu do identyfikacji podmiotów krytycznych, cyberzagrożeń, ryzyka w cyberprzestrzeni, incydentów**, a także niecybernetycznych ryzyk, zagrożeń i incydentów** wpływających na podmioty krytyczne **[**lub **podmioty równoważne z podmiotami krytycznymi]**, w **tym** na temat środków w zakresie cyberbezpieczeństwa **i środków fizycznych** podjętych przez podmioty krytyczne**, a także na temat wyników działań nadzorczych przeprowadzonych w odniesieniu do takich podmiotów. Ponadto w celu usprawnienia działań nadzorczych między właściwymi organami wyznaczonymi na mocy obu dyrektyw oraz w celu zminimalizowania obciążeń administracyjnych dla podmiotów, których to dotyczy, właściwe organy powinny dążyć do harmonizacji wzorów zgłoszeń incydentów i procesów ich przetwarzania.** [...] W **stosownych przypadkach** właściwe organy na mocy dyrektywy (UE) XXX/XXX **mogą zwrócić się** do właściwych organów na mocy niniejszej dyrektywy [...] o wykonanie ich uprawnień w zakresie nadzoru i egzekwowania przepisów [...] **względem** podmiotu niezbędnego zidentyfikowanego jako podmiot krytyczny. [...]

(14a) Podmioty należące do sektora infrastruktury cyfrowej opierają się zasadniczo na sieciach i systemach informatycznych, w związku z czym obowiązki nałożone na te podmioty na podstawie niniejszej dyrektywy powinny w kompleksowy sposób dotyczyć bezpieczeństwa fizycznego takich systemów i stanowić część spoczywających na tych podmiotach obowiązków w zakresie zarządzania ryzykiem w cyberprzestrzeni i obowiązków w zakresie zgłaszania incydentów. Ponieważ kwestie te są objęte niniejszą dyrektywą, obowiązki określone w rozdziałach III–VI dyrektywy (UE) XXX/XXX [CER] nie mają zastosowania do takich podmiotów.

(15) Utrzymywanie i zachowanie wiarygodnego, odpornego i bezpiecznego systemu nazw domen (DNS) odgrywa decydującą rolę w utrzymaniu integralności internetu oraz ma istotne znaczenie dla jego nieprzerwanego i stabilnego działania, od którego zależą gospodarka cyfrowa i społeczeństwo cyfrowe. W związku z tym niniejsza dyrektywa powinna mieć zastosowanie do [...] dostawców usług DNS w całym łańcuchu **dostarczania i** rozwiązywania nazw DNS**, które mają znaczenie dla rynku wewnętrznego,** w tym [...] **rejestrów** nazw domen najwyższego poziomu (TLD), **podmiotów świadczących usługi rejestracji nazwy domeny, operatorów** autorytatywnych serwerów nazw dla nazw domen i **operatorów** rekurencyjnych resolwerów. **Termin „dostawca usług DNS" nie powinien mieć zastosowania do usług DNS świadczonych na potrzeby własne danego podmiotu i jego podmiotów powiązanych. Obowiązki w zakresie cyberbezpieczeństwa wynikające z niniejszej dyrektywy w odniesieniu do tej kategorii dostawców są ściśle ograniczone do środków zarządzania ryzykiem w cyberprzestrzeni i zgłaszania incydentów, a zatem pozostają bez uszczerbku dla zarządzania globalnym DNS przez społeczność obejmującą wiele zainteresowanych stron.**

(16) Usługi w chmurze powinny obejmować usługi, które umożliwiają administrowanie na żądanie skalowalnym i elastycznym zbiorem rozproszonych zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru zasobów. Pojęcie „zasoby obliczeniowe” obejmuje zasoby, takie jak: sieci, serwery lub inną infrastrukturę, systemy operacyjne, oprogramowanie, pamięć masową, aplikacje i usługi. **Do modeli usług w chmurze należą między innymi infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS), oprogramowanie jako usługa (SaaS) oraz sieć jako usługa (NaaS).** Modele rozmieszczenia usług w chmurze powinny obejmować chmury prywatne, zbiorowe, publiczne i hybrydowe. Wspomniane wyżej modele usług i modele rozmieszczenia mają takie samo znaczenie jak terminy dotyczące modeli usług i modeli rozmieszczenia zdefiniowane w normie ISO/IEC 17788:2014. Zdolność użytkownika usług w chmurze do jednostronnego zapewnienia sobie możliwości przetwarzania danych, takich jak czas serwera lub sieciowy magazyn danych, bez żadnej ingerencji człowieka ze strony dostawcy usług w chmurze można określić jako administrowanie na żądanie. Pojęcia „szeroki dostęp zdalny” używa się do opisu sytuacji, gdy zasoby w chmurze są udostępniane przez sieć, a dostęp do nich jest możliwy za pośrednictwem mechanizmów sprzyjających wykorzystywaniu różnorodnych platform cienkich lub grubych klientów (w tym telefonów komórkowych, tabletów, laptopów, stacji roboczych).

Pojęcie „skalowalne” odnosi się do zasobów komputerowych, które są elastycznie przydzielane przez dostawcę usługi niezależnie od położenia geograficznego zasobów, jako reakcja na fluktuacje zapotrzebowania. Pojęcia „elastyczny zbiór” używa się do opisu tych zasobów obliczeniowych, które są przydzielane i uwalniane zależnie do zapotrzebowania, aby szybko zwiększać i zmniejszać dostępne zasoby w zależności od obciążenia. Pojęcia „wspólne wykorzystywanie” używa się do opisu zasobów obliczeniowych udostępnianych wielu użytkownikom, którzy dzielą wspólny dostęp do usługi, jednak przetwarzanie odbywa się oddzielnie dla każdego z użytkowników, choć usługa ta jest świadczona z tego samego sprzętu elektronicznego. Pojęcia „rozproszone” używa się do opisu zasobów obliczeniowych zlokalizowanych na rożnych komputerach lub urządzeniach połączonych w sieć, które komunikują się ze sobą i koordynują swoją pracę przez przekazywanie komunikatów.

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

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

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

---

18 Dyrektywa 97/67/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. dotycząca wspólnych zasad rozwoju wewnętrznego rynku usług pocztowych Wspólnoty oraz poprawy jakości usług (Dz.U. L 15 z 21. 21,1. 1998, s. 14).

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

(**20a**) **W celu osiągnięcia i utrzymania wysokiego poziomu cyberbezpieczeństwa krajowe strategie cyberbezpieczeństwa wymagane na mocy niniejszej dyrektywy powinny składać się ze spójnych ram zapewniających zarządzanie w obszarze cyberbezpieczeństwa. Strategie te mogą składać się z jednego lub kilku dokumentów o charakterze ustawodawczym lub nieustawodawczym.**

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

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

(23) Właściwe organy lub CSIRT powinny otrzymywać zgłoszenia incydentów od podmiotów w sposób efektywny i skuteczny**, również z myślą o ułatwianiu, w stosownych przypadkach, terminowego reagowania na incydenty oraz udzielenia odpowiedzi podmiotowi zgłaszającemu**. Pojedynczym punktom kontaktowym należy powierzyć zadanie przekazywania zgłoszeń incydentów pojedynczym punktom kontaktowym innych państw członkowskich, których incydent dotyczy. [...]

(23a) Unijne sektorowe akty prawne, które wymagają środków zarządzania ryzykiem w cyberprzestrzeni lub obowiązków dotyczących zgłaszania incydentów co najmniej równoważnych pod względem skutku z tymi określonymi w niniejszej dyrektywie, mogą przewidywać, że wyznaczone na ich podstawie właściwe organy wykonują swoje uprawnienia w zakresie nadzoru i egzekwowania przepisów w odniesieniu do takich środków lub obowiązków z pomocą właściwych organów wyznaczonych zgodnie z niniejszą dyrektywą. Odnośne właściwe organy mogą w tym celu przyjąć ustalenia dotyczące współpracy. W takich ustaleniach dotyczących współpracy można by określić m.in. procedury dotyczące koordynacji działań nadzorczych, w tym procedury dochodzeń i kontroli na miejscu zgodnie z prawem krajowym, oraz mechanizm do celów wymiany między właściwymi organami istotnych informacji na temat nadzoru i egzekwowania przepisów, w tym do celów udostępniania informacji związanych z cyberprzestrzenią, o które zwracają się właściwe organy wyznaczone zgodnie z niniejszą dyrektywą.

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

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

(26) Z uwagi na znaczenie współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa CSIRT powinny mieć możliwość uczestniczenia w międzynarodowych sieciach współpracy, niezależnie od współpracy w ramach sieci CSIRT ustanowionej na mocy niniejszej dyrektywy. W **związku z tym na potrzeby wykonywania swoich zadań zgodnie z rozporządzeniem (UE) 2016/679 CSIRT i właściwe organy mogą wymieniać informacje, w tym dane osobowe, z CSIRT z państw trzecich lub ich organami. W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony przyjętej zgodnie z art. 45 rozporządzenia (UE) 2016/679 lub braku odpowiednich zabezpieczeń zgodnie z art. 46 tego rozporządzenia wymianę danych osobowych, którą uznaje się za niezbędną do łagodzenia znaczących cyberzagrożeń i do reagowania na trwający znaczący incydent, można uznać za umotywowaną ważnymi względami interesu publicznego w rozumieniu art. 49 ust. 1 lit. d) rozporządzenia (UE) 2016/679.**

---

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

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

(28) Ponieważ wykorzystywanie podatności sieci i systemów informatycznych może powodować znaczące zakłócenia i szkody, ważnym czynnikiem w ograniczaniu ryzyka w cyberprzestrzeni jest szybkie identyfikowanie takich podatności i ich eliminowanie. Podmioty, które opracowują takie systemy **lub takimi systemami zarządzają**, powinny zatem ustanowić odpowiednie procedury postępowania w przypadku wykrycia takich podatności. Ponieważ podatności często są wykrywane i zgłaszane (ujawniane) przez osoby trzecie (podmioty zgłaszające), producent lub dostawca produktów lub usług ICT również powinien wprowadzić niezbędne procedury regulujące odbieranie od osób trzecich informacji na temat podatności. W tym względzie normy międzynarodowe ISO/IEC 30111 i ISO/IEC [...] **29147** zawierają wskazówki dotyczące, odpowiednio, postępowania w przypadku wykrycia podatności i ujawniania podatności. Jeśli chodzi o ujawnianie podatności, szczególnie ważna jest koordynacja między podmiotami zgłaszającymi a producentami lub dostawcami produktów lub usług ICT. Skoordynowane ujawnianie podatności to ustrukturyzowany proces, w ramach którego podatności są zgłaszane organizacjom w sposób umożliwiający organizacji zdiagnozowanie i wyeliminowanie danej podatności, zanim szczegółowe informacje dotyczące podatności zostaną ujawnione osobom trzecim lub podane do wiadomości publicznej. Skoordynowane ujawnianie podatności powinno także obejmować koordynację między podmiotem zgłaszającym a organizacją w odniesieniu do terminarza eliminowania podatności i podania ich do wiadomości publicznej.

---

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

(29) W związku z tym państwa członkowskie powinny podjąć działania w celu ułatwienia skoordynowanego ujawniania podatności poprzez ustanowienie odpowiedniej polityki krajowej. W **ramach swojej polityki krajowej państwa członkowskie powinny dążyć do wyeliminowania, w miarę możliwości, wyzwań stojących przed naukowcami zajmującymi się kwestią podatności, w tym ich potencjalnego narażenia na odpowiedzialność karną, zgodnie z ich krajowym porządkiem prawnym.** [...] Państwa członkowskie powinny wyznaczyć CSIRT do pełnienia roli „koordynatora", występującego w razie potrzeby w charakterze pośrednika między podmiotami zgłaszającymi a producentami lub dostawcami produktów lub usług ICT. Zadania CSIRT w charakterze koordynatora powinny w szczególności obejmować identyfikację zainteresowanych podmiotów i kontaktowanie się z nimi, wspieranie podmiotów zgłaszających, negocjowanie terminarza ujawniania oraz zarządzanie podatnościami, których skutki dotykają wielu organizacji (wielostronne **skoordynowane** ujawnianie podatności). Jeżeli **zgłoszona** podatność **może mieć znaczący wpływ na podmioty** [...] w więcej niż jednym państwie członkowskim, [...] wyznaczone CSIRT**, w stosownych przypadkach,** [...] powinny współpracować ze sobą w ramach sieci CSIRT.

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

(31) Choć istnieją podobne rejestry podatności lub bazy danych dotyczących podatności, są one prowadzone i utrzymywane przez podmioty, które nie mają siedziby w Unii. Europejski rejestr podatności utrzymywany przez ENISA zapewniłby lepszą przejrzystość w odniesieniu do procesu publikacji poprzedzającego oficjalne ujawnienie podatności, a także odporność w przypadku zakłóceń lub przerw w świadczeniu podobnych usług. Aby uniknąć powielania podejmowanych działań i dążyć do jak największej komplementarności, ENISA powinna zbadać możliwość zawarcia umów o współpracy strukturalnej z podobnymi rejestrami w jurysdykcjach państw trzecich. **W szczególności ENISA powinna zbadać możliwość ścisłej współpracy z operatorami systemu Wspólnych Podatności i Ekspozycji na Ryzyko (*Common Vulnerabilities and Exposures* – CVE), w tym możliwość przyjęcia roli głównego organu odpowiedzialnego za nadawanie numerów CVE.**

(32) **Grupa Współpracy powinna w dalszym ciągu wspierać i ułatwiać strategiczną współpracę i wymianę informacji między państwami członkowskimi oraz zwiększać wśród nich zaufanie i pewność.** Co dwa lata Grupa Współpracy powinna opracowywać program prac obejmujący działania, które mają zostać podjęte przez Grupę w celu realizacji jej celów i zadań. Aby uniknąć potencjalnych zakłóceń w pracy Grupy, ramy czasowe pierwszego programu przyjętego na podstawie niniejszej dyrektywy należy zharmonizować z ramami czasowymi ostatniego programu przyjętego na podstawie dyrektywy (UE) 2016/1148.

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

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

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

(35a) Sieć CSIRT powinna w dalszym ciągu 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.

(36) [...]

(36a) Aby ułatwić skuteczne wdrażanie przepisów niniejszej dyrektywy, dotyczących np. zarządzania podatnościami, zarządzania ryzykiem w cyberprzestrzeni, środków dotyczących zgłaszania incydentów i ustaleń dotyczących wymiany informacji, państwa członkowskie mogą współpracować z państwami trzecimi i podejmować działania uznane za odpowiednie do tego celu, obejmujące wymianę informacji na temat zagrożeń, incydentów, podatności, narzędzi i metod, taktyki, technik i procedur, zapewnianie gotowości i ćwiczeń w zakresie zarządzania kryzysowego w cyberprzestrzeni, szkolenia, budowanie zaufania i ustrukturyzowane ustalenia w zakresie wymiany informacji. Takie porozumienia o współpracy powinny być zgodne z unijnymi przepisami dotyczącymi ochrony danych.

(37) Państwa członkowskie powinny wnosić wkład w ustanowienie unijnych ram reagowania w sytuacji kryzysu cyberbezpieczeństwa, o których mowa w zaleceniu (UE) 2017/1584, poprzez istniejące sieci współpracy, w szczególności poprzez **europejską** sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe), sieć CSIRT i Grupę Współpracy. EU-CyCLONe i sieć CSIRT powinny współpracować na podstawie uzgodnień proceduralnych określających tryb tej współpracy i **unikać wszelkiego powielania zadań**. **W** regulaminie EU-CyCLONe należy bardziej szczegółowo określić tryb funkcjonowania tej sieci, w tym między innymi podział ról, modele współpracy, interakcje z innymi odpowiednimi podmiotami i wzory formularzy na potrzeby wymiany informacji, a także środki komunikacji. W odniesieniu do zarządzania kryzysowego na **politycznym** szczeblu unijnym odpowiednie strony powinny opierać się na uzgodnieniach dotyczących zintegrowanego reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR). W tym celu Komisja powinna wykorzystywać międzysektorowy proces koordynacji na wysokim szczeblu w sytuacji kryzysowej ARGUS. Jeżeli sytuacja kryzysowa wiąże się z istotnymi kwestiami z zakresu polityki zewnętrznej lub wspólnej polityki bezpieczeństwa i obrony (WPBiO), należy uruchomić mechanizm reagowania kryzysowego Europejskiej Służby Działań Zewnętrznych (ESDZ).

(37a) EU-CyCLONe powinna działać jako sieć pośrednia między szczeblem technicznym a politycznym podczas cyberincydentów i cyberkryzysów na dużą skalę. Powinna zacieśnić współpracę na poziomie operacyjnym, opierając się na ustaleniach sieci CSIRT i wykorzystując własne zdolności do sporządzania analizy skutków incydentów i kryzysów na dużą skalę oraz wspierając proces podejmowania decyzji na szczeblu politycznym. Instytucje, organy i agencje UE powinny wyznaczyć właściwy organ odpowiedzialny za zarządzanie incydentami i kryzysami w zakresie bezpieczeństwa na dużą skalę, który to organ zostałby członkiem EU-CyCLONe.

(38) [...]

(39) [...]

(39a) Odpowiedzialność za zapewnienie bezpieczeństwa sieci i systemów informatycznych w dużym stopniu spoczywa na podmiotach niezbędnych i istotnych. Należy wspierać i rozwijać kulturę zarządzania ryzykiem, obejmującą przeprowadzanie ocen ryzyka i wdrażanie środków bezpieczeństwa odpowiednich dla danego ryzyka.

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

(40a) Ponieważ zagrożenia dla bezpieczeństwa sieci i systemów informatycznych mogą mieć różne źródła, w niniejszej dyrektywie stosuje się podejście uwzględniające wszystkie zagrożenia, które obejmuje ochronę sieci i systemów informatycznych i ich środowiska fizycznego przed wszelkimi zdarzeniami, takimi jak kradzież, pożar, powódź, awarie telekomunikacyjne lub awarie zasilania, lub przed jakimkolwiek nieuprawnionym dostępem fizycznym do należących do podmiotu obiektów dotyczących informacji lub przetwarzania informacji, ich uszkodzeniem i ingerencją w nie, które to zdarzenia mogłyby naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub oferowanych przez sieci i systemy informatyczne usług lub usług dostępnych za pośrednictwem tych sieci i systemów. Środki zarządzania ryzykiem powinny zatem dotyczyć również bezpieczeństwa fizycznego i ochrony przed zagrożeniami środowiskowymi i obejmować środki ochrony sieci i systemów informatycznych należących do danego podmiotu przed awariami systemu, błędem ludzkim, złośliwymi działaniami lub zjawiskami naturalnymi, zgodnie z normami europejskimi lub międzynarodowymi, takimi jak normy zawarte w serii ISO 27000. W związku z tym w ramach swoich środków zarządzania ryzykiem podmioty powinny również zająć się kwestią bezpieczeństwa zasobów ludzkich i posiadać odpowiednią politykę kontroli dostępu. Środki te powinny być spójne z dyrektywą XXXX [dyrektywa CER].

(40b) W przypadku braku odpowiednich europejskich programów certyfikacji cyberbezpieczeństwa przyjętych zgodnie z rozporządzeniem (UE) 2019/881 państwa członkowskie mogą wymagać od podmiotów korzystania z certyfikowanych produktów, usług i procesów ICT lub uzyskania certyfikatu w ramach dostępnych krajowych systemów cyberbezpieczeństwa w celu spełnienia wymogów w zakresie zarządzania ryzykiem w cyberprzestrzeni przewidzianych w niniejszej dyrektywie.

(41) Aby uniknąć nakładania nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na podmioty niezbędne i istotne, wymogi w zakresie zarządzania ryzykiem w cyberprzestrzeni powinny być proporcjonalne do istniejącego ryzyka [...] **dla** danej sieci oraz danego systemu informatycznego, oraz powinny uwzględniać najnowszy stan wiedzy na temat takich środków i **koszty ich wdrożenia**. **Należy również odpowiednio uwzględnić wielkość danego podmiotu, a także prawdopodobieństwo wystąpienia incydentów i ich dotkliwość.**

(41a) W celu zmniejszenia obciążeń regulacyjnych wymogi dotyczące wdrażania środków zarządzania ryzykiem w cyberprzestrzeni w odniesieniu do średnich lub małych podmiotów lub mikropodmiotów powinny być zasadniczo łagodniejsze, chyba że kryteria decydujące o krytyczności lub krajowe oceny ryzyka uzasadniałyby zaostrzenie wymogów, w szczególności w odniesieniu do podmiotów, które spełniają kryteria decydujące o krytyczności określone w niniejszej dyrektywie.

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

(42aa) Biorąc pod uwagę ich transgraniczny charakter, dostawcy usług DNS, rejestry nazw TLD oraz podmioty świadczące usługi rejestracji nazwy domeny dla TLD, dostawcy usług w chmurze, dostawcy ośrodków przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych oraz dostawcy zarządzanych usług w zakresie bezpieczeństwa powinni podlegać większej harmonizacji na poziomie Unii. Wdrażanie środków w zakresie cyberbezpieczeństwa powinno być zatem ułatwione aktem wykonawczym.

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

(44) Wśród dostawców usług szczególnie ważną rolę we wspieraniu podmiotów w ich działaniach mających na celu wykrywanie incydentów i reagowanie na nie odgrywają dostawcy zarządzanych usług w zakresie bezpieczeństwa w obszarach takich jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo. Tacy dostawcy zarządzanych usług z zakresu bezpieczeństwa również sami padali jednak ofiarami cyberataków, a ponieważ ich działalność jest ściśle zintegrowana z operacjami operatorów, stwarzają szczególne ryzyko w cyberprzestrzeni. W związku z tym przy wyborze dostawcy zarządzanych usług z zakresu bezpieczeństwa podmioty powinny dochować szczególnej staranności.

(44a) Właściwe organy krajowe, w kontekście swoich zadań nadzorczych, mogą również korzystać z usług w zakresie cyberbezpieczeństwa, takich jak audyty bezpieczeństwa, testy penetracyjne lub reagowanie na incydenty. Aby pomóc podmiotom, a także właściwym organom krajowym w wyborze wykwalifikowanych i wiarygodnych dostawców usług w zakresie cyberbezpieczeństwa, Komisja, z pomocą Grupy Współpracy i ENISA, powinna rozważyć możliwość wystąpienia o europejskie programy certyfikacji cyberbezpieczeństwa zgodnie z art. 48 rozporządzenia (UE) 2019/881.

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

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

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

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

(48) Aby uprościć zobowiązania prawne nałożone na dostawców publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej oraz dostawców usług zaufania w odniesieniu do bezpieczeństwa ich sieci i systemów informatycznych, a także zapewnić tym podmiotom i ich odpowiednim właściwym organom możliwość korzystania z ram prawnych ustanowionych na podstawie niniejszej dyrektywy (w tym wyznaczania CSIRT odpowiedzialnych za postępowanie w przypadku ryzyka i incydentu, uczestnictwa właściwych organów i jednostek w pracach Grupy Współpracy i w sieci CSIRT), należy objąć te podmioty zakresem stosowania niniejszej dyrektywy. W związku z tym należy uchylić odpowiednie przepisy określone w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014[22] oraz w dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/1972[23], na których podstawie na te rodzaje podmiotów nałożono wymogi w zakresie bezpieczeństwa i zgłaszania incydentów.

---

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

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

(48a) Obowiązki w zakresie bezpieczeństwa określone w niniejszej dyrektywie należy uznać za uzupełniające względem wymogów nałożonych na dostawców usług zaufania na podstawie rozporządzenia (UE) nr 910/2014 (rozporządzenie eIDAS). 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 osób trzecich, oraz do zgłaszania incydentów związanych z bezpieczeństwem na podstawie niniejszej dyrektywy. Takie obowiązki w zakresie bezpieczeństwa i zgłaszania incydentów powinny również dotyczyć fizycznej ochrony świadczonej usługi. Nadal zastosowanie ma art. 24 rozporządzenia (UE) 910/2014.

(48aa) Państwa członkowskie mogą powierzyć rolę właściwych organów w zakresie usług zaufania organom nadzorczym eIDAS w celu zapewnienia ciągłości obecnych praktyk oraz w celu wykorzystania wiedzy i doświadczenia zdobytego podczas stosowania rozporządzenia eIDAS. W przypadkach gdy ta rola jest przypisana innemu organowi, właściwe organy krajowe na mocy niniejszej dyrektywy powinny ściśle i terminowo współpracować ze sobą poprzez wymianę odpowiednich informacji w celu zapewnienia skutecznego nadzoru nad dostawcami usług zaufania i przestrzegania przez nich wymogów określonych w niniejszej dyrektywie i rozporządzeniu [XXXX/XXXX].

W stosownych przypadkach właściwy organ krajowy na mocy niniejszej dyrektywy powinien niezwłocznie poinformować organ nadzorczy eIDAS o każdym zgłoszonym znaczącym cyberzagrożeniu lub incydencie mającym wpływ na usługi zaufania, a także o każdym przypadku nieprzestrzegania przez dostawcę usług zaufania wymogów wynikających z niniejszej dyrektywy. Do celów dokonywania zgłoszeń państwa członkowskie mogą korzystać, w stosownych przypadkach, z pojedynczego punktu kontaktowego ustanowionego w celu zapewnienia wspólnego i automatycznego zgłaszania incydentów zarówno organowi nadzorczemu eIDAS, jak i właściwemu organowi na mocy niniejszej dyrektywy. Przepisy dotyczące obowiązków w zakresie zgłaszania incydentów nie powinny naruszać przepisów rozporządzenia (UE) 2016/679 i dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE[24].

---

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

(49) W stosownych przypadkach i aby uniknąć niepotrzebnych zakłóceń, [...] **we wdrażanych przez państwa członkowskie ustaleniach dotyczących transpozycji należy uwzględnić** istniejące wytyczne krajowe przyjęte w celu transpozycji przepisów dotyczących środków bezpieczeństwa określonych w art. 40 i 41 dyrektywy (UE) 2018/1972 [...]**, co pozwoli wykorzystać wiedzę i umiejętności nabyte już na podstawie dyrektywy (UE) 2018/1972 w odniesieniu do środków zarządzania ryzykiem dla bezpieczeństwa i do zgłaszania incydentów. ENISA może również opracować wskazówki dotyczące wymogów w zakresie bezpieczeństwa i zgłaszania incydentów dla dostawców publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej w celu ułatwienia harmonizacji, procesu przejścia i zminimalizowania zakłóceń. Państwa członkowskie mogą powierzyć rolę właściwych organów w zakresie usług łączności elektronicznej krajowym organom regulacyjnym w celu zapewnienia ciągłości obecnych praktyk oraz w celu wykorzystania wiedzy i doświadczenia zdobytego podczas stosowania dyrektywy (UE) 2018/1972.**

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

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

(52) W [...] **stosownych** przypadkach podmioty powinny informować odbiorców swoich usług o szczególnych środkach, które odbiorcy ci mogą zastosować w celu ograniczenia wynikłego ryzyka, na jakie są sami narażeni w **związku ze znaczącym cyberzagrożeniem**. **Podmioty powinny, w stosownych przypadkach, a w szczególności w przypadkach, w których znaczące cyberzagrożenie może się urzeczywistnić, powiadamiać o samym zagrożeniu również swoich usługobiorców, równolegle z właściwymi organami lub CSIRT.** Wymóg informowania tych odbiorców o takich zagrożeniach nie powinien zwalniać podmiotu z obowiązku zastosowania na własny koszt odpowiednich i natychmiastowych środków w celu zapobieżenia lub zaradzenia wszelkim cyberzagrożeniom oraz przywrócenia normalnego poziomu bezpieczeństwa danej usługi. Udzielanie odbiorcom takich informacji na temat **cyber**zagrożeń [...] powinno odbywać się bezpłatnie.

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

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

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

(55a) Proaktywne podejście do cyberzagrożeń jest istotnym elementem zarządzania ryzykiem w cyberprzestrzeni, które powinno umożliwić właściwym organom skuteczne zapobieganie urzeczywistnianiu się cyberzagrożeń w formie rzeczywistych incydentów, które mogą spowodować znaczne straty materialne lub niematerialne. W związku z tym powiadamianie o znaczących cyberzagrożeniach ma kluczowe znaczenie.

(56) Podmioty niezbędne i istotne znajdują się często w sytuacji, w której konkretny incydent, ze względu na jego cechy, należy zgłosić różnym organom w wyniku istnienia obowiązków w zakresie zgłaszania przewidzianych w różnych instrumentach prawnych. Takie przypadki powodują dodatkowe obciążenie, a ponadto mogą rodzić niepewność dotyczącą formatu i procedur dokonywania takich zgłoszeń. W związku z tym i w celu uproszczenia zgłaszania incydentów bezpieczeństwa państwa członkowskie [...] **mogą** ustanowić *pojedynczy punkt kontaktowy* na potrzeby wszystkich zgłoszeń wymaganych na podstawie niniejszej dyrektywy, a także na podstawie innych przepisów unijnych, takich jak rozporządzenie (UE) 2016/679 i dyrektywa 2002/58/WE. ENISA, we współpracy z Grupą Współpracy, powinna opracować wspólne wzory zgłoszeń w formie wytycznych, które ułatwiłyby i usprawniły zgłaszanie informacji wymaganych zgodnie z prawem Unii oraz zmniejszyłyby obciążenia spoczywające na przedsiębiorstwach.

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

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

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

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

(61) W celu zapewnienia dostępności prawidłowych i kompletnych danych dotyczących rejestracji nazw domen rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD (tzw. rejestratorzy) powinny gromadzić dane dotyczące rejestracji nazw domen oraz zapewniać ich integralność i dostępność. **W odniesieniu do danych dotyczących rejestracji podmioty powinny w szczególności zweryfikować imię i nazwisko lub nazwę i adres e-mail rejestrującego.** [...] Rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD powinny ustanowić polityki i procedury na potrzeby gromadzenia i utrzymywania prawidłowych i kompletnych danych rejestracyjnych, a także przeciwdziałać powstawaniu nieprawidłowych danych rejestracyjnych i poprawiać je zgodnie z unijnymi przepisami o ochronie danych.

(62) Rejestry TLD i podmioty świadczące dla nich usługi rejestracji nazw domen powinny podawać do wiadomości publicznej dane dotyczące rejestracji nazw domen nieobjęte zakresem stosowania unijnych przepisów o ochronie danych, takie jak dane dotyczące osób prawnych[25]. Rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD powinny ponadto umożliwiać wnioskodawcom ubiegającym się o prawnie uzasadniony dostęp uzyskanie takiego dostępu do konkretnych danych dotyczących rejestracji nazw domen, odnoszących się do osób fizycznych, zgodnie z unijnymi przepisami o ochronie danych. Państwa członkowskie powinny zapewniać, aby rejestry TLD i podmioty świadczące dla nich usługi rejestracji nazw domen odpowiadały bez zbędnej zwłoki na wnioski [...] o [...] dostęp o ujawnienie danych dotyczących rejestracji nazw domen **składane przez wnioskodawców ubiegających się o prawnie uzasadniony dostęp, takich jak właściwe organy na mocy prawa Unii lub prawa krajowego w obszarze bezpieczeństwa narodowego i wymiaru sprawiedliwości w sprawach karnych lub sieci CSIRT**. Rejestry TLD i podmioty świadczące dla nich usługi rejestracji nazw domen powinny ustanowić polityki i procedury na potrzeby publikacji i ujawniania danych rejestracyjnych, w tym umowy o gwarantowanym poziomie usług regulujące rozpatrywanie wniosków o dostęp składanych przez wnioskodawców ubiegających się o prawnie uzasadniony dostęp. Procedura uzyskiwania dostępu może również obejmować wykorzystanie interfejsu, portalu lub innego narzędzia technicznego w celu zapewnienia skutecznego systemu umożliwiającego składanie wniosków o dostęp do danych rejestracyjnych i uzyskiwanie do nich dostępu. **Państwa członkowskie powinny zapewnić, aby każdy rodzaj dostępu do danych dotyczących rejestracji domen (zarówno danych osobowych, jak i nieosobowych) był bezpłatny. W** celu promowania zharmonizowanych praktyk na całym rynku wewnętrznym Komisja może przyjąć wytyczne dotyczące takich procedur bez uszczerbku dla kompetencji Europejskiej Rady Ochrony Danych**, zgodnie z normami międzynarodowymi opracowanymi przez społeczność obejmującą wiele zainteresowanych stron i w ramach uzupełnienia tych norm**.

---

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

(63) [...] **P**odmioty niezbędne i istotne w rozumieniu niniejszej dyrektywy powinny podlegać jurysdykcji państwa członkowskiego, w którym świadczą usługi. **Podmioty, o których mowa w załączniku I pkt 1–7 i 10, dostawcy usług zaufania i dostawcy punktów wymiany ruchu internetowego, o których mowa w załączniku I pkt 8 oraz w załączniku II pkt 1–5 do niniejszej dyrektywy, powinni podlegać jurysdykcji państwa członkowskiego, na którego terytorium mają jednostkę organizacyjną.** Jeżeli podmiot świadczy usługi **lub ma jednostkę organizacyjną** 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 postanowią wykonywać jurysdykcję, powinny unikać sytuacji, w której ten sam czyn byłby karany więcej niż jeden raz za naruszenie obowiązków przewidzianych w niniejszej dyrektywie.**

(64) Aby uwzględnić transgraniczny charakter usług i działalności dostawców usług DNS, rejestrów nazw TLD, **podmiotów świadczących usługi rejestracji nazw domen dla TLD,** dostawców sieci dostarczania treści, dostawców usług w chmurze, dostawców usług ośrodka przetwarzania danych oraz dostawców usług cyfrowych, takie podmioty powinny podlegać jurysdykcji wyłącznie jednego państwa członkowskiego. Jurysdykcja powinna przynależeć państwu członkowskiemu, w którym dany podmiot ma główną jednostkę organizacyjną w Unii. Kryterium jednostki organizacyjnej do celów niniejszej dyrektywy oznacza faktyczne prowadzenie działalności poprzez stabilne struktury. Forma prawna takich struktur, niezależnie od tego, czy chodzi o oddział czy podmiot zależny posiadający osobowość prawną, nie jest w tym względzie czynnikiem decydującym.

Spełnienie tego kryterium nie powinno zależeć od tego, czy sieci i systemy informatyczne są fizycznie zlokalizowane w danym miejscu; fizyczne położenie i wykorzystanie takich systemów nie stanowią same w sobie takiej głównej jednostki organizacyjnej i nie są zatem przesądzającymi kryteriami pozwalającymi ustalić główną jednostkę organizacyjną. Za główną jednostkę organizacyjną należy uznać miejsce w Unii, w którym **głównie** podejmowane są decyzje związane ze środkami zarządzania ryzykiem w cyberprzestrzeni Będzie ono zazwyczaj odpowiadać miejscu centralnej administracji przedsiębiorstw w Unii. Jeżeli **nie można określić miejsca, w którym takie decyzje są głównie podejmowane, lub** takich decyzji nie podejmuje się w Unii, uznaje się, że główna jednostka organizacyjna znajduje się w państwie członkowskim, w którym dany podmiot ma jednostkę organizacyjną o największej liczbie pracowników w Unii. Jeżeli usługi świadczy grupa przedsiębiorstw, za główną jednostkę organizacyjną grupy przedsiębiorstw należy uznać główną jednostkę organizacyjną przedsiębiorstwa sprawującego kontrolę.

(64a) W przypadku gdy rekurencyjna usługa DNS jest świadczona przez dostawcę publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej jedynie w ramach usługi dostępu do internetu, dany podmiot należy uznać za podlegający jurysdykcji wszystkich państw członkowskich, w których świadczone są jego usługi.

(64aa) W celu uzyskania jasności co do objętych zakresem stosowania niniejszej dyrektywy dostawców usług DNS, rejestrów nazw TLD, podmiotów świadczących usługi rejestracji nazw domen dla TLD, dostawców sieci dostarczania treści, dostawców usług w chmurze, dostawców usług ośrodka przetwarzania danych oraz dostawców usług cyfrowych świadczących usługi w całej Unii, ENISA powinna stworzyć i utrzymywać rejestr takich podmiotów w oparciu o powiadomienia otrzymane przez państwa członkowskie, w stosownych przypadkach za pośrednictwem krajowych mechanizmów samodzielnego powiadamiania. W celu zapewnienia dokładności i kompletności informacji, które powinny być zawarte w tym rejestrze, państwa członkowskie powinny przekazywać ENISA dostępne w ich rejestrach krajowych informacje na temat tych podmiotów. ENISA i państwa członkowskie powinny podjąć środki w celu ułatwienia interoperacyjności takich rejestrów, zapewniając jednocześnie ochronę informacji poufnych lub niejawnych.

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

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

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

(68) Należy zachęcać podmioty do wspólnego wykorzystywania ich indywidualnej wiedzy i praktycznego doświadczenia na szczeblu strategicznym, taktycznym i operacyjnym w celu wzmocnienia ich zdolności w zakresie odpowiedniego oceniania i monitorowania cyberzagrożeń, obrony przed nimi i reagowania na nie. Należy zatem umożliwić powstawanie na poziomie Unii mechanizmów dobrowolnej wymiany informacji. W tym celu państwa członkowskie powinny aktywnie wspierać również odpowiednie podmioty nieobjęte zakresem niniejszej dyrektywy i zachęcać je do uczestnictwa w takich mechanizmach wymiany informacji. Mechanizmy te powinny funkcjonować w pełnej zgodności z unijnymi regułami konkurencji oraz z unijnymi przepisami dotyczącymi ochrony danych osobowych.

(69) [...] **Można uznać, że przetwarzanie danych osobowych** przez podmioty **niezbędne i istotne** [...] oraz dostawców technologii i usług z zakresu bezpieczeństwa w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji **jest niezbędne do wywiązania się z prawnego obowiązku lub** [...] stanowi prawnie uzasadniony interes odnośnego administratora danych **[...]** w rozumieniu rozporządzenia (UE) 2016/679. **Może** [...] to obejmować środki związane z zapobieganiem incydentom, wykrywaniem i analizowaniem ich oraz reagowaniem na nie, środki zwiększające świadomość konkretnych cyberzagrożeń, wymianę informacji w kontekście usuwania oraz skoordynowanego ujawniania podatności, a także dobrowolną wymianę informacji na temat tych incydentów, [...] cyberzagrożeń i podatności, oznak naruszenia integralności systemu, taktyk, technik i procedur, ostrzeżeń dotyczących cyberbezpieczeństwa i narzędzi konfiguracji. Takie środki mogą wiązać się z koniecznością przetwarzania [...] **różnych** rodzajów danych osobowych**, takich jak**: adresy IP, ujednolicone formaty adresowania zasobów (URL), nazwy domen i adresy e-mail. **Przetwarzanie danych osobowych przez właściwe organy, centra monitorowania bezpieczeństwa i CSIRT powinno być określone w prawie krajowym i uznawane za niezbędne do wywiązania się z prawnego obowiązku lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi danych, o czym mowa w art. 6 ust. 1 lit. c) lub e) rozporządzenia (UE) 2016/679.**

(69a) W przepisach wykonawczych państwa członkowskie mogą ustanawiać zasady umożliwiające właściwym organom, centrom monitorowania bezpieczeństwa i CSIRT – w zakresie, w jakim jest to absolutnie niezbędne i proporcjonalne do celów zapewnienia bezpieczeństwa sieci i systemów informatycznych podmiotów niezbędnych i istotnych – przetwarzanie szczególnych kategorii danych osobowych zgodnie z art. 9 [...] rozporządzenia (UE) 2016/679, w szczególności poprzez wprowadzenie odpowiednich i szczegółowych środków mających na celu ochronę podstawowych praw i interesów osób fizycznych, w tym środków technicznych ograniczających ponowne wykorzystanie tych danych i najnowocześniejszych środków służących zapewnieniu bezpieczeństwa i ochrony prywatności, takich jak pseudonimizacja lub – w przypadku gdy anonimizacja może znacząco wpłynąć na możliwość realizacji zakładanego celu – szyfrowanie.

(70) Aby wzmocnić uprawnienia i działania nadzorcze, które pomagają zapewnić efektywną zgodność z przepisami, w niniejszej dyrektywie należy przewidzieć minimalny wykaz działań i środków nadzorczych, za pomocą których właściwe organy mogą sprawować nadzór nad podmiotami niezbędnymi i istotnymi. Ponadto w niniejszej dyrektywie należy wprowadzić rozróżnienie systemów nadzoru mających zastosowanie do podmiotów niezbędnych i podmiotów istotnych w celu zapewnienia sprawiedliwej równowagi pod względem obowiązków zarówno po stronie podmiotów, jak i właściwych organów. Podmioty niezbędne należy zatem objąć pełnym systemem nadzoru (*ex ante* i *ex post*), natomiast podmioty istotne należy objąć uproszczonym systemem nadzoru (wyłącznie *ex post*). W przypadku tego drugiego systemu podmioty istotne nie powinny mieć obowiązku systematycznego **dokumentowania** spełniania wymogów dotyczących zarządzania ryzykiem w cyberprzestrzeni, natomiast właściwe organy powinny realizować nadzór w oparciu o podejście reaktywne w trybie *ex post*, a zatem nie powinny mieć ogólnego obowiązku prowadzenia nadzoru nad tymi podmiotami. W **przypadku podmiotów istotnych nadzór *ex post* może być uruchamiany w oparciu o dowody lub wszelkie wskazania lub informacje przekazane właściwym organom, które te organy uznają za sugerujące potencjalne niewypełnienie obowiązków przewidzianych w niniejszej dyrektywie. Takie dowody, wskazania lub informacje mogą na przykład być w rodzaju tych, jakie są przekazywane właściwym organom przez inne organy, podmioty, obywateli, media lub inne źródła, mogą to być publicznie dostępne informacje lub mogą one wynikać z innej działalności prowadzonej przez właściwe organy w ramach wykonywania ich zadań.**

(70bis) W ramach sprawowania nadzoru *ex ante* właściwe organy powinny mieć możliwość decydowania o priorytetowym traktowaniu stosowania działań i środków nadzorczych, którymi dysponują, w sposób proporcjonalny. Oznacza to, że właściwe organy mogą decydować o takim priorytetowym traktowaniu w oparciu o metodyki nadzorcze, w ramach których powinno być stosowane podejście oparte na analizie ryzyka. W szczególności metodyki takie mogłyby obejmować kryteria lub wartości odniesienia dotyczące klasyfikacji podmiotów istotnych w ramach kategorii ryzyka oraz odpowiednie działania i środki nadzorcze zalecane w zależności od kategorii ryzyka, takie jak stosowanie, częstotliwość lub rodzaj kontroli na miejscu lub ukierunkowanych audytów bezpieczeństwa lub skanów bezpieczeństwa, rodzaj wymaganych informacji oraz poziom szczegółowości tych informacji. Takim metodykom nadzorczym mogą również towarzyszyć programy prac i mogą one podlegać regularnym ocenom i przeglądom, w tym w odniesieniu do takich aspektów jak przydział zasobów i potrzeby.

(70bisa) W odniesieniu do podmiotów administracji publicznej uprawnienia w zakresie nadzoru powinny być wykonywane zgodnie z krajowymi ramami i krajowym porządkiem prawnym. Państwa członkowskie powinny mieć możliwość zdecydowania o nałożeniu odpowiednich, proporcjonalnych i skutecznych środków nadzoru i egzekwowania przepisów w odniesieniu do tych podmiotów.

(70bisaa) Aby wykazać przestrzeganie niektórych środków zarządzania ryzykiem w cyberprzestrzeni, państwa członkowskie mogą wymagać od podmiotów niezbędnych i istotnych korzystania z kwalifikowanych usług zaufania lub notyfikowanych systemów identyfikacji elektronicznej na podstawie rozporządzenia (UE) nr 910/2014.

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

(71bis) Przepisy dotyczące odpowiedzialności osób fizycznych sprawujących w danym podmiocie określone funkcje za niedopełnienie obowiązku polegającego na zapewnieniu wypełnienia obowiązków przewidzianych w niniejszej dyrektywie nie zobowiązują państw członkowskich do wszczęcia postępowania karnego lub pociągnięcia takich osób do odpowiedzialności cywilnej za szkody wyrządzone osobom trzecim w wyniku takiego niedopełnienia obowiązku.

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

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

(74) Państwa członkowskie [...] **mogą** ustanowić przepisy przewidujące sankcje karne za naruszenie przepisów krajowych transponujących niniejszą dyrektywę. Jednak nałożenie sankcji karnych za naruszenie takich przepisów krajowych oraz nałożenie powiązanych kar administracyjnych nie powinno prowadzić do naruszenia zasady *ne bis in idem*, zgodnie z wykładnią Trybunału Sprawiedliwości.

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

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

(76bis) W celu zapewnienia skutecznego nadzoru i egzekwowania przepisów, zwłaszcza w przypadkach o wymiarze transgranicznym, państwa członkowskie, które otrzymały wniosek o wzajemną pomoc, powinny w zakresie objętym wnioskiem podjąć odpowiednie środki nadzoru i egzekwowania przepisów w odniesieniu do danego podmiotu świadczącego usługi lub posiadającego sieć i system informatyczny na ich terytorium.

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

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

(79) **W celu wzmocnienia wzajemnego** zaufania i **uczenia się na dobrych praktykach i doświadczeniach** należy ustanowić **system** [...] wzajemnego **uczenia się** umożliwiający wyznaczonym przez państwa członkowskie ekspertom [...] **partnerską wymianę** na temat realizacji polityki cyberbezpieczeństwa [...]. **Wdrażając system wzajemnego uczenia się, należy zwrócić szczególną uwagę na zapewnienie, aby nie nakładał on niepotrzebnego lub nieproporcjonalnego obciążenia na odpowiednie organy państw członkowskich. Komisja powinna zbadać wszystkie możliwości ewentualnego zagwarantowania finansowego pokrycia kosztów, które mogą wyniknąć z organizacji delegacji w ramach wzajemnego uczenia się. Ponadto system wzajemnego uczenia się powinien uwzględniać wyniki podobnych mechanizmów, takich jak system wzajemnej oceny sieci CSIRT, zapewniać wartość dodaną i unikać powielania działań. Wdrożenie systemu wzajemnego uczenia się powinno pozostawać bez uszczerbku dla krajowych lub unijnych przepisów dotyczących ochrony informacji poufnych i niejawnych. Przed rozpoczęciem rund wzajemnego uczenia się państwa członkowskie mogą przeprowadzić samodzielną ocenę istotnych aspektów. Na wniosek Grupy Współpracy ENISA może w razie potrzeby udzielać wskazówek dotyczących samodzielnej oceny i odpowiednich wzorów. Państwa członkowskie mogą zdecydować o publicznym udostępnieniu swoich sprawozdań.**

(80) [...]

(81) Aby zapewnić jednolite warunki wdrażania odpowiednich przepisów niniejszej dyrektywy dotyczących procedur niezbędnych do funkcjonowania Grupy Współpracy, elementów technicznych związanych ze środkami zarządzania ryzykiem lub rodzaju zgłaszanych informacji, formatu i procedury dokonywania zgłoszeń incydentów**, kategorii podmiotów, które podlegają wymogowi używania pewnych certyfikowanych produktów, usług i procesów ICT**, należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[26].

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

---

[26] 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).

(83) Ponieważ cel niniejszej dyrektywy, a mianowicie osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na skutki działania możliwe jest lepsze jego osiągnięcie na poziomie Unii, Unia może podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

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

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

Przepisy ogólne

Artykuł 1

Przedmiot

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

2. W tym celu niniejsza dyrektywa:

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

   b) określa obowiązki w zakresie zarządzania ryzykiem w cyberprzestrzeni oraz zgłaszania incydentów spoczywające na podmiotach w rodzaju tych, które określono [...] w załącznikach I i **II** [...];

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

Artykuł 2

Zakres

1. Niniejsza dyrektywa ma zastosowanie do podmiotów publicznych i prywatnych w rodzaju tych **wymienionych** w [...] **załącznikach I i II**, [...] **które spełniają lub przekraczają pułapy dla średnich przedsiębiorstw** [...] w rozumieniu zalecenia Komisji 2003/361/WE[27]. **Do celów niniejszej dyrektywy nie mają zastosowania art. 3 ust. 4 oraz art. 6 ust. 2 akapit drugi i trzeci załącznika do tego zalecenia.**

2. Niniejsza dyrektywa ma jednak zastosowanie [...] niezależnie od wielkości **podmiotów, o których mowa w ust. 1, w przypadku gdy:** [...]

   a) usługi świadczy jeden z poniższych podmiotów:

      (i) **dostawcy** publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej, o których mowa w załączniku I pkt 8;

      (ii) **kwalifikowani dostawcy usług zaufania, o których mowa w załączniku I pkt XX;**

      (iii) **niekwalifikowani dostawcy usług zaufania, o których mowa w załączniku I pkt XX;**

      (iv) rejestry nazw domen najwyższego poziomu [...], o których mowa w załączniku I pkt 8;

   b) [...]

---

27 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).

c) podmiot jest jedynym w **danym państwie członkowskim** dostawcą usługi [...]**, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej**;

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

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

f) [...];

g) podmiot wskazano jako podmiot krytyczny zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) XXXX/XXXX[28] [dyrektywa w sprawie odporności podmiotów krytycznych] **[**lub jako podmiot równoważny podmiotowi krytycznemu zgodnie z art. 7 tej dyrektywy**]**.

2a. **Niniejsza dyrektywa ma również zastosowanie do podmiotów administracji publicznej rządów centralnych, które zostały uznane za takie w danym państwie członkowskim zgodnie z prawem krajowym i o których mowa w załączniku I pkt 9, niezależnie od ich wielkości. Państwa członkowskie mogą postanowić, że niniejsza dyrektywa ma również zastosowanie do podmiotów administracji publicznej na szczeblu regionalnym i lokalnym.**

---

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

3. [...]

Niniejsza dyrektywa pozostaje bez uszczerbku dla obowiązków państw członkowskich w zakresie ochrony bezpieczeństwa narodowego lub ich uprawnień do zabezpieczania innych podstawowych funkcji państwa, w tym zapewniania integralności terytorialnej państwa i utrzymywania porządku publicznego.

3a. 1) Niniejsza dyrektywa nie ma zastosowania do:

a) podmiotów nieobjętych zakresem stosowania prawa Unii, a w każdym przypadku wszystkich podmiotów, które prowadzą działalność głównie w obszarach obronności, bezpieczeństwa narodowego, bezpieczeństwa publicznego lub ścigania przestępstw, niezależnie od tego, który podmiot prowadzi taką działalność, i niezależnie od tego, czy jest to podmiot publiczny czy prywatny, bez uszczerbku dla pkt 2;

b) podmiotów, które prowadzą działalność w obszarach sądownictwa, parlamentów lub banków centralnych. [...]

2) W przypadku gdy podmioty administracji publicznej prowadzą działalność w tych obszarach i działalność ta jest jedynie częścią ich działalności ogólnej, są one w całości wyłączone z zakresu stosowania niniejszej dyrektywy.

3aa. Niniejsza dyrektywa nie ma zastosowania do:

(i) działalności podmiotów nieobjętych zakresem stosowania prawa Unii, a w każdym przypadku wszelkiej działalności dotyczącej bezpieczeństwa narodowego lub obronności, niezależnie od tego, który podmiot prowadzi taką działalność, i niezależnie od tego, czy jest to podmiot publiczny czy prywatny;

(ii) działalności podmiotów w obszarach sądownictwa, parlamentów, banków centralnych oraz w obszarze bezpieczeństwa publicznego, w tym podmiotów administracji publicznej prowadzących działalność w obszarze ścigania przestępstw do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw oraz wykonywania kar.

3aaa. Obowiązki ustanowione w niniejszej dyrektywie nie wiążą się z dostarczaniem informacji, których ujawnienie jest sprzeczne z podstawowymi interesami państw członkowskich w zakresie bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności.

3aaaa. Niniejsza dyrektywa pozostaje bez uszczerbku dla prawa Unii w sprawie ochrony danych osobowych, w szczególności przepisów rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE.

3b. Niniejsza dyrektywa nie ma zastosowania do podmiotów wyłączonych z zakresu stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej] zgodnie z art. 2 ust. 4 rozporządzenia w sprawie operacyjnej odporności cyfrowej.

4. Niniejszą dyrektywę stosuje się bez uszczerbku dla [...][29] [...] dyrektyw Parlamentu Europejskiego i Rady 2011/93/UE[30] i 2013/40/UE[31].

5. Bez uszczerbku dla art. 346 TFUE informacje, które są poufne zgodnie z przepisami unijnymi i krajowymi, takimi jak przepisy dotyczące tajemnicy przedsiębiorstwa, podlegają wymianie z Komisją i innymi odpowiednimi organami **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. W ramach wymiany informacji zachowuje się poufność tych informacji oraz chroni się bezpieczeństwo i interesy handlowe podmiotów niezbędnych lub istotnych.

---

29 [...]

30 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).

31 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).

Artykuł 2bis

Podmioty niezbędne i istotne

1. Spośród podmiotów, do których ma zastosowanie niniejsza dyrektywa, za niezbędne uznaje się:

(i) podmioty w rodzaju tych wskazanych w załączniku I pkt 1–8a i 10 do niniejszej dyrektywy, które przekraczają pułapy dla średnich przedsiębiorstw określone w zaleceniu Komisji 2003/361/WE;

(ii) średnie podmioty, o których mowa w art. 2 ust. 2 lit. a) ppkt (i);

(iii) podmioty, o których mowa w art. 2 ust. 2 lit. a) ppkt (ii) oraz (iv) niniejszej dyrektywy, niezależnie od wielkości;

(iv) podmioty, o których mowa w art. 2 ust. 2 lit. g) i art. 2 ust. 2a niniejszej dyrektywy, niezależnie od wielkości;

(v) jeżeli zostały ustanowione przez państwa członkowskie – podmioty, które państwa członkowskie wskazały przed wejściem w życie niniejszej dyrektywy jako operatorów usług kluczowych zgodnie z dyrektywą (UE) 2016/1148 lub prawem krajowym;

(vi) podmioty w rodzaju tych wskazanych w załączniku II przekraczające pułapy dla średnich przedsiębiorstw określone w zaleceniu Komisji 2003/361/WE, które to podmioty państwa członkowskie uznają za niezbędne na podstawie kryteriów, o których mowa w art. 2 ust. 2 lit. c)–e);

(vii) średnie podmioty w rozumieniu zalecenia Komisji 2003/361/WE, które państwa członkowskie uznają za niezbędne na podstawie kryteriów, o których mowa w art. 2 ust. 2 lit. c)–e);

(viii) mikropodmioty lub małe podmioty w rozumieniu zalecenia Komisji 2003/361/WE wskazane w ust. 2 lit. a) ppkt (i) lub wskazane zgodnie z ust. 2 lit. c)–e) niniejszego artykułu, które państwa członkowskie uznają za niezbędne na podstawie krajowych ocen ryzyka.

2. Spośród podmiotów, do których ma zastosowanie niniejsza dyrektywa, za istotne uznaje się:

(i) podmioty w rodzaju tych wskazanych w załączniku I do niniejszej dyrektywy, które kwalifikują się jako średnie przedsiębiorstwa w rozumieniu zalecenia Komisji 2003/361/WE, oraz podmioty w rodzaju tych wskazanych w załączniku II, które spełniają lub przekraczają pułapy dla średnich przedsiębiorstw w rozumieniu zalecenia Komisji 2003/361/WE[32];

(ii) podmioty, o których mowa w art. 2 ust. 2 lit. a) ppkt (iii) niniejszej dyrektywy, niezależnie od wielkości;

(iii) małe podmioty i mikropodmioty, o których mowa w art. 2 ust. 2 lit. a) ppkt (i);

(iv) małe podmioty i mikropodmioty, które państwa członkowskie uznają za istotne podmioty na podstawie art. 2 ust. 2 lit. c)–e).

---

[32] **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).**

Artykuł 2a

Mechanizmy zgłoszeń

1. **Państwa członkowskie mogą ustanowić krajowe mechanizmy w zakresie samodzielnego zgłaszania, które zobowiązują wszystkie podmioty objęte zakresem stosowania niniejszej dyrektywy do zgłaszania właściwym organom na mocy niniejszej dyrektywy lub jednostkom wyznaczonym do tego celu przez państwa członkowskie co najmniej swojego imienia i nazwiska lub swojej nazwy, adresu, danych kontaktowych, sektora, w którym prowadzą działalność lub rodzaju usług, jakie świadczą, oraz, w stosownych przypadkach, wykazu państw członkowskich, w których świadczą usługi objęte zakresem stosowania niniejszej dyrektywy.**

2. **Do [12 miesięcy po terminie transpozycji niniejszej dyrektywy]** państwa członkowskie [...] przedkładają Komisji w **odniesieniu do podmiotów, które wskazały zgodnie z art. 2 ust. 2 lit. b)–e), co najmniej odpowiednie informacje na temat liczby wskazanych podmiotów, sektora, do którego należą, lub rodzaju usług, jakie świadczą, zgodnie z załącznikami, oraz na temat konkretnego przepisu lub konkretnych przepisów art. 2 ust. 2, na podstawie którego lub których podmioty te zostały wskazane.** Państwa członkowskie regularnie, nie rzadziej niż co dwa lata po wyżej wymienionej dacie, dokonują przeglądu [...] **tych informacji** oraz, w stosownych przypadkach, aktualizują [...] je.

Artykuł 2b

Unijne akty sektorowe

1. W przypadku gdy na podstawie przepisów **unijnych** sektorowych aktów **prawnych** [...] wymaga się od podmiotów niezbędnych lub istotnych przyjęcia środków zarządzania ryzykiem w cyberprzestrzeni albo zgłaszania **znaczących** incydentów lub [...] cyberzagrożeń oraz w przypadku gdy wymogi te są co najmniej równoważne pod względem skutku z obowiązkami określonymi w niniejszej dyrektywie, nie stosuje się **do takich podmiotów** odpowiednich przepisów niniejszej dyrektywy**, w tym przepisów dotyczących nadzoru i egzekwowania określonych w rozdziale VI**. **Jeżeli unijne sektorowe akty prawne nie obejmują wszystkich podmiotów w konkretnym sektorze wchodzącym w zakres stosowania niniejszej dyrektywy, odpowiednie przepisy niniejszej dyrektywy nadal mają zastosowanie do podmiotów nieobjętych tymi przepisami sektorowymi.**

2. Wymogi, o których mowa w ust. 1 niniejszego artykułu, uznaje się za równoważne pod względem skutku z obowiązkami określonymi w niniejszej dyrektywie, jeżeli w odpowiednim sektorowym akcie Unii przewidziano natychmiastowy, i w stosownych przypadkach automatyczny i bezpośredni dostęp właściwych organów na mocy niniejszej dyrektywy lub wyznaczonych CSIRT do zgłoszeń incydentów oraz jeżeli:

a) środki zarządzania ryzykiem w cyberprzestrzeni są co najmniej równoważne pod względem skutku ze środkami określonymi w art. 18 ust. 1 i 2 niniejszej dyrektywy; albo

b) wymogi dotyczące zgłaszania znaczących incydentów są co najmniej równoważne pod względem skutku z wymogami określonymi w art. 20 ust. 1–6.

3. Komisja dokonuje okresowego przeglądu stosowania równoważnych pod względem skutku wymogów przewidzianych w ust. 1 i 2 niniejszego artykułu w odniesieniu do sektorowych przepisów unijnych aktów prawnych. Przygotowując te okresowe przeglądy, Komisja konsultuje się z Grupą Współpracy i ENISA.

Artykuł 3

Minimalna harmonizacja

Państwa członkowskie mogą, bez uszczerbku dla swoich innych obowiązków wynikających z prawa Unii, [...] przyjmować lub utrzymywać przepisy zapewniające wyższy poziom cyberbezpieczeństwa w **obszarach objętych zakresem stosowania niniejszej dyrektywy**.

Artykuł 4

Definicje

Na potrzeby niniejszej dyrektywy stosuje się następujące definicje:

1) „sieci i systemy informatyczne” oznaczają:

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

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

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

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;

2a) „usługi łączności elektronicznej” oznaczają usługi [...] łączności elektronicznej w rozumieniu art. 2 pkt 4 dyrektywy (UE) 2018/1972;

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

4) „krajowa strategia **cyberbezpieczeństwa**” oznacza spójne ramy państwa członkowskiego zapewniające zarządzanie na rzecz osiągnięcia strategicznych celów i priorytetów [...] w **dziedzinie cyberbezpieczeństwa** [...] w tym państwie członkowskim;

5) „incydent” oznacza każde 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;

5a) „cyberincydent na dużą skalę” oznacza incydent, który ma znaczący wpływ na co najmniej dwa państwa członkowskie lub który powoduje zakłócenie przekraczające zdolność państwa członkowskiego do reagowania na niego;

---

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

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

6a) „ryzyko” oznacza możliwe straty lub zakłócenia spowodowane incydentem i jest wyrażone jako wypadkowa skali takiej straty lub takich zakłóceń oraz prawdopodobieństwa wystąpienia takiego incydentu.

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

7a) **„znaczące cyberzagrożenie” oznacza cyberzagrożenie, co do którego – w oparciu o jego charakterystykę techniczną – można uznać, że może wywrzeć poważny wpływ na sieci i systemy informatyczne danego podmiotu lub jego użytkowników, powodując znaczne straty materialne lub niematerialne;**

8) „podatność” oznacza słabość, wrażliwość lub wadę zasobu ICT [...] lub systemu, które mogą zostać wykorzystane w wyniku cyberzagrożenia;

8a) „zdarzenie potencjalnie wypadkowe” oznacza zdarzenie, które może potencjalnie uszkodzić sieci i systemy informatyczne podmiotu lub przynieść szkodę jego użytkownikom, ale którego pełnemu wystąpieniu udało się skutecznie zapobiec;

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

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

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

12) „punkt wymiany ruchu internetowego (IXP)” oznacza obiekt sieciowy, który umożliwia wzajemne połączenie więcej niż dwóch niezależnych sieci (systemów autonomicznych), głównie do celów ułatwienia wymiany ruchu internetowego; IXP zapewnia wzajemne połączenie wyłącznie dla systemów autonomicznych; IXP nie wymaga, aby ruch internetowy między jakąkolwiek parą uczestniczących systemów autonomicznych przechodził przez jakikolwiek trzeci system autonomiczny, ani nie powoduje zmian w tym ruchu, ani w inny sposób w niego nie ingeruje;

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

14) „dostawca usług DNS” oznacza podmiot świadczący rekurencyjne lub autorytatywne usługi rozwiązywania nazw domen [...] **na rzecz używania przez osoby trzecie, z wyjątkiem głównych serwerów nazw** [...];

---

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

15) „rejestr nazw domen najwyższego poziomu” oznacza podmiot, któremu powierzono konkretną domenę najwyższego poziomu (TLD) i który odpowiada za zarządzanie nią, w tym za rejestrację nazw domen w ramach TLD oraz za jej techniczne funkcjonowanie, w tym za obsługę jej serwerów nazw, utrzymanie jej baz danych oraz dystrybucję plików strefowych TLD we wszystkich serwerach nazw**, z wyłączeniem sytuacji, w których nazwy domen najwyższego poziomu są wykorzystywane przez rejestr wyłącznie na użytek własny**;

15a) „podmioty świadczące usługi rejestracji nazw domen dla TLD” oznaczają rejestry nazw TLD, rejestratorów TLD oraz agentów rejestratorów, takich jak odsprzedawcy i dostawcy usług proxy;

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

16a) „usługi zaufania” oznaczają usługi zaufania w rozumieniu art. 3 pkt 16 rozporządzenia (UE) nr 910/2014;

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

16b) „kwalifikowany dostawca usług zaufania” oznacza kwalifikowanego dostawcę usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia (UE) nr 910/2014;

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

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

19) „usługa w chmurze” oznacza usługę cyfrową umożliwiającą administrowanie na żądanie skalowalnym i elastycznym zbiorem rozproszonych zasobów obliczeniowych do wspólnego wykorzystywania**, w tym gdy są one rozmieszczone w kilku lokalizacjach,** oraz szeroki dostęp zdalny do tego zbioru;

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

---

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

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

21) „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;

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

23) „podmiot administracji publicznej” oznacza podmiot **uznany za taki w danym państwie członkowskim zgodnie z prawem krajowym**, [...] spełniający następujące kryteria:

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

   b) posiada osobowość prawną **lub zgodnie z przepisami jest uprawniony do działania w imieniu innego podmiotu posiadającego osobowość prawną**;

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

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

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

25) „podmiot niezbędny” oznacza każdy podmiot w rodzaju tego, który [...] **wskazano w załączniku I i wskazano jako „niezbędny” zgodnie z art. 2bis ust. 1**;

26) „podmiot istotny” oznacza każdy podmiot w rodzaju tego, który [...] **wskazano w załącznikach I i II i wyznaczono jako „istotny” zgodnie z art. 2bis ust. 2**;

26a) „produkt ICT” oznacza produkt ICT w rozumieniu art. 2 pkt 12 rozporządzenia (UE) nr 2019/881;

26aa) „usługa ICT” oznacza usługę ICT w rozumieniu art. 2 pkt 13 rozporządzenia (UE) nr 2019/881;

26ab) „proces ICT” oznacza proces ICT w rozumieniu art. 2 pkt 14 rozporządzenia (UE) 2019/881;

26ac) „dostawca usług zarządzanych” oznacza każdy podmiot, który świadczy usługi, takie jak sieć, aplikacja, infrastruktura i bezpieczeństwo, poprzez bieżące i regularne zarządzanie, wsparcie i aktywne zarządzanie w pomieszczeniach klientów, w swoim ośrodku przetwarzania danych (*hosting*) lub w ośrodku przetwarzania danych należącym do osoby trzeciej;

26ad) „dostawca zarządzanych usług w zakresie bezpieczeństwa” oznacza każdy podmiot, który zapewnia zlecone na zewnątrz monitorowanie i zarządzanie urządzeniami i systemami bezpieczeństwa. Wspólne usługi obejmują zarządzane usługi w zakresie zapory sieciowej, wykrywania wtargnięć, wirtualnej sieci prywatnej, skanowania podatności i usług antywirusowych.

Obejmuje to również korzystanie z centrów monitorowania bezpieczeństwa o wysokiej dostępności (z ich własnych obiektów lub z obiektów innych dostawców ośrodków przetwarzania danych) w celu świadczenia przez 24 godziny na dobę przez 7 dni w tygodniu usług mających na celu zmniejszenie liczby pracowników zajmujących się monitorowaniem bezpieczeństwa, których przedsiębiorstwo musi zatrudniać, szkolić i utrzymywać, aby zachować akceptowalny stan bezpieczeństwa.

ROZDZIAŁ II

Skoordynowane ramy regulacyjne w zakresie cyberbezpieczeństwa

Artykuł 5

Krajowa strategia cyberbezpieczeństwa

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

   a) [...] cele i priorytety strategii cyberbezpieczeństwa państw członkowskich;

   b) ramy zarządzania służące realizacji tych celów i priorytetów, w tym polityk, o których mowa w ust. 2, a także role i obowiązki poszczególnych organów i stron zaangażowanych we wdrażanie tej strategii [...];

   c) [...] **wskazówki** służące określeniu istotnych zasobów i **ocenie** ryzyka w cyberprzestrzeni w tym państwie członkowskim [...];

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

   e) [...]

f) ramy polityki na rzecz ściślejszej koordynacji między właściwymi organami na mocy niniejszej dyrektywy i dyrektywy Parlamentu Europejskiego i Rady (UE) XXXX/XXXX[38] [dyrektywa w sprawie odporności podmiotów krytycznych] do celów wymiany informacji na temat **ryzyka w cyberprzestrzeni**, [...] cyberzagrożeń i **cyberincydentów, a także na temat niecybernetycznych ryzyk, zagrożeń i incydentów** oraz, w **stosownych przypadkach**, na temat wykonywania zadań nadzorczych;

fa) ramy polityki na rzecz koordynacji i współpracy między właściwymi organami na mocy niniejszej dyrektywy a właściwymi organami wyznaczonymi na mocy przepisów sektorowych.

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

a) politykę dotyczącą cyberbezpieczeństwa w łańcuchu dostaw dla produktów i usług ICT wykorzystywanych przez podmioty [...] do świadczenia usług;

b) **politykę** [...] dotyczącą uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów i usług ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień**, w tym certyfikacji cyberbezpieczeństwa**;

c) politykę **dotyczącą zarządzania podatnościami, obejmującą promowanie i ułatwianie dobrowolnego** [...] skoordynowanego ujawniania podatności w rozumieniu art. 6 **ust. 1**;

d) politykę związaną z utrzymywaniem ogólnej dostępności, [...] integralności i **poufności** publicznego rdzenia otwartego internetu;

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

---

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

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

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

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

3. Państwa członkowskie przekazują Komisji swoje krajowe strategie cyberbezpieczeństwa w terminie trzech miesięcy od ich przyjęcia. **Przekazując te strategie,** państwa członkowskie mogą wyłączyć **elementy strategii, które są związane z** bezpieczeństwem narodowym.

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

Artykuł 6

Skoordynowane ujawnianie podatności i europejski rejestr podatności

1. Każde państwo członkowskie wyznacza jeden spośród swoich CSIRT, o których mowa w art. 9, na koordynatora na potrzeby skoordynowanego ujawniania podatności. Wyznaczony CSIRT działa w charakterze zaufanego pośrednika, w razie potrzeby ułatwiając interakcję między podmiotem zgłaszającym, **potencjalnym właścicielem podatności** a producentem lub dostawcą produktów lub usług ICT. **Każda osoba fizyczna lub prawna może zgłosić wyznaczonemu CSIRT, w miarę możliwości anonimowo, podatność, o której mowa w art. 4 ust. 8. Wyznaczony CSIRT zapewnia staranne działania następcze w związku ze zgłoszeniem oraz poufność tożsamości osoby zgłaszającej podatność.** Jeżeli zgłoszona podatność [...] **może mieć potencjalnie znaczący wpływ na podmioty w więcej niż jednym państwie członkowskim**, wyznaczony CSIRT z każdego państwa członkowskiego, w którym ujawniono podatność, współpracuje**, w stosownych przypadkach,** z **innymi wyznaczonymi CSIRT w ramach** sieci CSIRT.

2. ENISA opracowuje i prowadzi europejski rejestr podatności **konsultując się z Grupą Współpracy**. W tym celu ENISA ustanawia i utrzymuje odpowiednie systemy informatyczne, polityki i procedury, w szczególności aby umożliwić podmiotom istotnym i niezbędnym oraz ich dostawcom sieci i systemów informatycznych ujawnianie i rejestrowanie**, na zasadzie dobrowolności, publicznie znanych** podatności występujących w produktach lub usługach ICT, a także aby zapewnić wszystkim zainteresowanym stronom dostęp do informacji na temat podatności wykazanych w rejestrze. Rejestr zawiera w szczególności informacje na temat podatności, produktu lub usług ICT, których ta podatność dotyczy, oraz dotkliwości podatności pod względem okoliczności, w jakich może ona zostać wykorzystana, dostępności powiązanych łat oraz, w przypadku braku dostępnych łat, wskazówki **wydane przez właściwe organy krajowe lub CSIRT,** skierowane do użytkowników produktów i usług, których dotyczy podatność, na temat sposobów ograniczania ryzyka wynikającego z ujawnionych podatności. **ENISA zapewnia, aby europejski rejestr podatności korzystał z bezpiecznej i odpornej infrastruktury komunikacyjno-informacyjnej.**

Artykuł 7

Krajowe ramy zarządzania kryzysami cyberbezpieczeństwa

1. Każde państwo członkowskie wyznacza co najmniej jeden właściwy organ odpowiedzialny za zarządzanie **cyber**incydentami i kryzysami **cyberbezpieczeństwa** na dużą skalę. Państwa członkowskie zapewniają właściwym organom odpowiednie zasoby, aby mogły one efektywnie i skutecznie wykonywać powierzone im zadania. **Państwa członkowskie zapewniają spójność z istniejącymi ramami ogólnego zarządzania kryzysowego.**

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

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

   a) cele krajowych środków i działań służących zapewnieniu gotowości;

   b) zadania i obowiązki właściwych organów krajowych;

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

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

   e) odpowiednie zaangażowane publiczne i prywatne [...] strony oraz odpowiednią infrastrukturę publiczną i prywatną;

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

4. Państwa członkowskie [...] **informują** Komisję o wyznaczeniu właściwych organów, o których mowa w ust. 1, i przedkładają **odpowiednie informacje odnoszące się do wymogów określonych w ust. 3 niniejszego artykułu na temat** swoich krajowych planów reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa [...] w terminie trzech miesięcy od daty wyznaczenia tych organów oraz od daty przyjęcia tych planów. Państwa członkowskie mogą wyłączyć niektóre konkretne informacje [...], jeżeli – i w zakresie, w jakim – jest to [...] niezbędne dla bezpieczeństwa narodowego**, bezpieczeństwa publicznego lub obronności**.

Artykuł 8

Właściwe organy krajowe i pojedyncze punkty kontaktowe

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

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

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

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

5. Państwa członkowskie zapewniają właściwym organom, o których mowa w ust. 1, i pojedynczym punktom kontaktowym odpowiednie zasoby, aby mogły one efektywnie i skutecznie wykonywać powierzone im zadania, a tym samym realizować cele niniejszej dyrektywy. Państwa członkowskie zapewniają efektywną, skuteczną i bezpieczną współpracę wyznaczonych przedstawicieli w ramach Grupy Współpracy, o której mowa w art. 12.

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

Artykuł 9

Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)

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

2. Państwa członkowskie zapewniają, aby każdy CSIRT dysponował odpowiednimi zasobami, tak aby mógł skutecznie realizować swoje zadania określone w art. 10 ust. 2. **Wykonując te zadania, CSIRT mogą, na podstawie podejścia opartego na ryzyku, priorytetowo traktować świadczenie określonych usług na rzecz podmiotów.**

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

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

5. CSIRT biorą udział we wzajemnym [...] **uczeniu się** organizowanym zgodnie z art. 16.

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

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

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

Artykuł 10

Wymogi dotyczące CSIRT i ich zadania

1. CSIRT spełniają następujące wymogi:

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

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

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

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

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

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

2. CSIRT mają następujące zadania:

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

b) wczesne ostrzeganie i alarmowanie podmiotów niezbędnych i istotnych oraz **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;

c) reagowanie na incydenty;

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

e) przeprowadzanie **[...]** aktywnego skanowania sieci i systemów informatycznych [...] w **celu wykrycia podatności mających potencjalnie znaczący wpływ, pod warunkiem że, w przypadku braku zgody tego podmiotu, nie nastąpiło naruszenie sieci i systemów informatycznych ani ich funkcjonowanie nie podlegało negatywnemu wpływowi;**

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

fa) w stosownych przypadkach, działanie w charakterze koordynatora do celów skoordynowanego procesu ujawniania podatności na podstawie art. 6 ust. 1, który obejmuje w szczególności ułatwianie interakcji między podmiotami zgłaszającymi, potencjalnym właścicielem podatności oraz producentem lub dostawcą produktów lub usług ICT, w przypadkach gdy jest to konieczne, identyfikowanie odnośnych podmiotów i kontaktowanie się z nimi, wspieranie podmiotów zgłaszających, negocjowanie harmonogramów ujawniania i zarządzanie podatnościami, które mają wpływ na wiele organizacji (wielostronne skoordynowane ujawnianie podatności).

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

3a. CSIRT mogą nawiązać współpracę z krajowymi CSIRT z państw trzecich. W ramach tej współpracy mogą one wymieniać istotne informacje, w tym dane osobowe, zgodnie z unijnymi przepisami o ochronie danych.

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

a) procedurami postępowania w przypadku incydentu;

b) zarządzaniem kryzysami cyberbezpieczeństwa;

c) skoordynowanym ujawnianiem podatności.

Artykuł 11

Współpraca na poziomie krajowym

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

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

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

4. W zakresie niezbędnym do skutecznej realizacji zadań i obowiązków przewidzianych w niniejszej dyrektywie państwa członkowskie zapewniają odpowiednią współpracę między właściwymi organami, **CSIRT,** pojedynczymi punktami kontaktowymi, a także organami ścigania, organami ochrony danych i **właściwymi** organami **wyznaczonymi** [...] na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych[...]], **właściwymi organami na mocy rozporządzenia wykonawczego Komisji 2019/1583, krajowymi organami regulacyjnymi wyznaczonymi zgodnie z dyrektywą (UE) 2018/1972, krajowymi organami wyznaczonymi na podstawie art. 17 rozporządzenia (UE) nr 910/2014,** [...] krajowymi organami finansowymi wyznaczonymi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego]**, a także właściwymi organami wyznaczonymi na mocy innych sektorowych unijnych aktów prawnych,** w danym państwie członkowskim.

5. Państwa członkowskie zapewniają, aby ich właściwe organy **na mocy niniejszej dyrektywy i właściwe organy wyznaczone na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych]** regularnie **dokonywały wymiany** [...] informacji na temat **identyfikacji podmiotów krytycznych,** ryzyka w cyberprzestrzeni, cyber**zagrożeń i incydentów, a także niecybernetycznych ryzyk, zagrożeń i incydentów**, mających wpływ na podmioty niezbędne uznane za podmioty krytyczne **[**lub za podmioty równoważne z podmiotami krytycznymi**]** na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych], a także na temat środków wprowadzonych [...] w odpowiedzi na takie ryzyko i incydenty. **Państwa członkowskie zapewniają również, aby właściwe organy na mocy niniejszej dyrektywy** [...] i **właściwe organy wyznaczone na mocy rozporządzenia (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego], dyrektywy 2018/1972 i rozporządzenia (UE) 910/2014 regularnie wymieniały odpowiednie informacje.**

W odniesieniu do dostawców usług zaufania, a [...] w szczególności [...] w przypadkach gdy ta rola nadzorcza na mocy niniejszej dyrektywy jest przypisana innemu organowi niż organy nadzorcze wyznaczone na podstawie rozporządzenia (UE) nr 910/2014, właściwe organy krajowe na mocy niniejszej dyrektywy ściśle i terminowo współpracują ze sobą poprzez wymianę odpowiednich informacji w celu zapewnienia skutecznego nadzoru nad dostawcami usług zaufania i przestrzegania przez nich wymogów określonych w niniejszej dyrektywie i rozporządzeniu [XXXX/XXXX] **oraz, w stosownych przypadkach, właściwy organ krajowy na mocy niniejszej dyrektywy niezwłocznie informuje organ nadzorczy eIDAS o każdym zgłoszonym znaczącym cyberzagrożeniu lub incydencie mającym wpływ na usługi zaufania**.

5a. W celu [...] uproszczenia zgłaszania incydentów państwa członkowskie mogą ustanowić pojedynczy punkt kontaktowy na potrzeby wszystkich zgłoszeń wymaganych na podstawie niniejszej dyrektywy, a także na podstawie rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE, stosownie do przypadku. Państwa członkowskie mogą korzystać z pojedynczego punktu kontaktowego na potrzeby zgłoszeń wymaganych na mocy innych sektorowych unijnych aktów prawnych. Ten pojedynczy punkt kontaktowy nie wpływa na stosowanie przepisów rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE, w szczególności przepisów dotyczących niezależnych organów nadzorczych.

ROZDZIAŁ III

*Współpraca **UE***

Artykuł 12

Grupa Współpracy

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

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

3. Grupa Współpracy składa się z przedstawicieli państw członkowskich, Komisji i ENISA. Europejska Służba Działań Zewnętrznych uczestniczy w działaniach Grupy Współpracy w charakterze obserwatora. Europejskie Urzędy Nadzoru i **właściwe organy wyznaczone na mocy rozporządzenia (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego]** [...] mogą uczestniczyć w działaniach Grupy Współpracy **zgodnie z art. 42 ust. 1 rozporządzenia (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego].**

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

   Komisja zapewnia obsługę sekretariatu.

4. Grupa Współpracy ma następujące zadania:

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

   aa) udzielanie wskazówek w odniesieniu do opracowywania i wdrażania polityk dotyczących skoordynowanego ujawniania podatności, o którym mowa w art. 5 ust. 2 lit. c) i art. 6 ust. 1;

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

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

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

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

ea) wymiana poglądów na temat wdrażania przepisów sektorowych dotyczących aspektów cyberbezpieczeństwa;

f) omawianie sprawozdań z wzajemnego [...] **uczenia się**, o którym mowa w art. 16 ust. 7;

g) omawianie **doświadczeń** [...] w zakresie wspólnego nadzoru w sprawach transgranicznych, o których mowa w art. 34;

h) zapewnianie sieci CSIRT i **EU–CyCLONe** wskazówek strategicznych dotyczących konkretnych pojawiających się kwestii;

ha) wymiana poglądów na temat działań następczych w zakresie polityki w związku z cyberincydentami na dużą skalę na podstawie doświadczeń zdobytych w ramach sieci CSIRT i EU–CyCLONe;

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

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

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

ka) ustanowienie mechanizmu wzajemnego uczenia się zgodnie z art. 16 niniejszej dyrektywy.

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

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

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

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

Artykuł 13

Sieć CSIRT

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

2. Sieć CSIRT składa się z przedstawicieli CSIRT państw członkowskich **wyznaczonych zgodnie z art. 9** i CERT-EU. Komisja uczestniczy w pracach sieci CSIRT jako obserwator. ENISA zapewnia obsługę sekretariatu oraz aktywnie wspiera współpracę między CSIRT.

3. Sieć CSIRT ma następujące zadania:

   a) wymiana informacji na temat zdolności CSIRT;

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

ba) wymiana informacji w odniesieniu do publikacji i zaleceń dotyczących cyberbezpieczeństwa;

bb) dzielenie się rozwiązaniami technicznymi ułatwiającymi techniczne postępowanie w przypadku incydentów;

bc) wymiana najlepszych praktyk, narzędzi i procesów w odniesieniu do zadań CSIRT;

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

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

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

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

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

(i) kategoriami cyberzagrożeń i incydentów;

(ii) wczesnym ostrzeganiem;

(iii) wzajemną pomocą;

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

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

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

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

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

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

l) omawianie sprawozdań z wzajemnego [...] **uczenia się**, o którym mowa w art. 16 ust. 7;

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

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

5. Sieć CSIRT przyjmuje swój regulamin wewnętrzny.

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

Artykuł 14

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

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

2. EU-CyCLONe składa się z przedstawicieli organów państw członkowskich do spraw zarządzania kryzysami cyberbezpieczeństwa, wyznaczonych zgodnie z art. 7 [...]. **Komisja uczestniczy w działaniach sieci jako obserwator.** ENISA zapewnia obsługę sekretariatu sieci i wspiera bezpieczną wymianę informacji, a **także zapewnia narzędzia niezbędne do wspierania współpracy między państwami członkowskimi, zapewniając bezpieczną wymianę informacji.**

W stosownych przypadkach EU-CyCLONe może zapraszać przedstawicieli odpowiednich zainteresowanych stron do udziału w swoich pracach.

3. EU-CyCLONe ma następujące zadania:

a) podnoszenie poziomu gotowości w zakresie zarządzania cyberincydentami i kryzysami cyberbezpieczeństwa [...] na dużą skalę;

b) rozwijanie wspólnej orientacji sytuacyjnej [...] w zakresie cyberincydentów i kryzysów cyberbezpieczeństwa [...] na dużą skalę;

ba) ocena konsekwencji i wpływu odnośnych cyberincydentów na dużą skalę oraz proponowanie możliwych środków ograniczające ryzyko;

c) koordynowanie **zarządzania** cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę [...] oraz wspieranie procesu decyzyjnego na szczeblu politycznym w odniesieniu do takich incydentów i kryzysów;

d) **na żądanie państwa członkowskiego,** omawianie **jego** krajowych planów reagowania na cyberincydenty i **kryzysy** cyberbezpieczeństwa, o których mowa w art. 7 ust. **3** [...]**;**[...]

4. EU-CyCLONe przyjmuje swój regulamin wewnętrzny.

5. EU-CyCLONe regularnie składa Grupie Współpracy sprawozdania na temat **zarządzania cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę** [...], koncentrując się w szczególności na ich wpływie na podmioty niezbędne i istotne.

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

7. Do dnia [24 miesiące po wejściu w życie niniejszej dyrektywy] EU-CyCLONe przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie oceniające prace sieci.

Artykuł 14a

Współpraca międzynarodowa

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 i EU-CyCLONe, zgodnie z unijnymi przepisami o ochronie danych.

Artykuł 15

Sprawozdanie o stanie cyberbezpieczeństwa w Unii

1. ENISA wydaje co dwa lata, we współpracy z Komisją i **Grupą Współpracy**, sprawozdanie o stanie cyberbezpieczeństwa w Unii. W **szczególności** [...] sprawozdanie to [...] zawiera [...], co następuje:

   aa) ocenę ryzyka w cyberprzestrzeni na szczeblu Unii, z uwzględnieniem krajobrazu zagrożeń;

   a) [...] **ocenę** rozwoju zdolności w zakresie cyberbezpieczeństwa w sektor**ach** publicznym i prywatnym w całej Unii;

   b) [...]

   c) **zbiorczą ocenę opartą na** [...] **ilościowych i jakościowych wskaźnikach** cyberbezpieczeństwa, zapewniającą [...] **przegląd** poziomu dojrzałości zdolności w zakresie cyberbezpieczeństwa**, w tym zdolności sektorowych**.

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

Artykuł 16

Wzajemne uczenie się

1. **Z myślą o zwiększeniu wzajemnego zaufania, osiągnięciu wysokiego wspólnego poziomu cyberbezpieczeństwa, a także wzmocnieniu zdolności i polityk państw członkowskich w zakresie cyberbezpieczeństwa niezbędnych do skutecznego wdrożenia niniejszej dyrektywy, Grupa Współpracy** [...] ustanawia, **przy wsparciu ze strony Komisji oraz** po konsultacji z [...] ENISA **i, w stosownych przypadkach, z siecią CSIRT,** i najpóźniej **24 [...]** miesiące po wejściu w życie niniejszej dyrektywy, metodykę [...] **dotyczącą obiektywnego, niedyskryminacyjnego i uczciwego** systemu wzajemnego **uczenia się w odniesieniu do** wdrażania niniejszej dyrektywy przez państwa członkowskie i zawartość systemu wzajemnej oceny służącego do oceny skuteczności polityki cyberbezpieczeństwa państw członkowskich. **Udział we wzajemnym uczeniu się jest dobrowolny. System ten składa się z rund ocen** [...] prowadzonych przez [...] ekspertów ds. cyberbezpieczeństwa pochodzących z państw członkowskich [...] i obejmuje [...] **co najmniej jeden z** następujących aspektów:

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

   (ii) [...] zdolności, w tym dostępne zasoby [...], oraz [...] wykonywanie zadań przez właściwe organy krajowe, o **których mowa w art. 8, i CSIRT, o których mowa w art. 9**;

[...]

(i**ii**[...]) [...] **realizacja** wzajemnej pomocy, o której mowa w art. 34;

(**iv**) [...] **realizacja** ram wymiany informacji, o których mowa w art. 26 [...].

2. **Kryteria, na podstawie których państwa członkowskie mają wyznaczać ekspertów kwalifikujących się do udziału w rundach wzajemnego uczenia się, są** [...] obiektywne, niedyskryminacyjne, sprawiedliwe i przejrzyste [...] i **są zawarte w metodyce, o której mowa w ust. 1**. ENISA i Komisja [...] **mogą** wyznaczać ekspertów do udziału w [...] **rundach wzajemnego uczenia się** w charakterze obserwatorów. [...]

3. [...].

3a. Przed rozpoczęciem rund wzajemnego uczenia się państwa członkowskie mogą przeprowadzić samodzielną ocenę aspektów objętych daną rundą wzajemnego uczenia się i przekazać tę samoocenę wyznaczonym ekspertom, o których mowa w ust. 2.

4. Wzajemne [...] **uczenie się** [...] **może** wiązać się z [...] **fizycznymi** lub wirtualnymi kontrolami na miejscu i zdalną wymianą informacji. Mając na uwadze zasadę dobrej współpracy, państwa członkowskie [...] **uczestniczące we wzajemnym uczeniu się** dostarczają wyznaczonym ekspertom [...] informacji niezbędnych do oceny [...]**, bez uszczerbku dla krajowych lub unijnych przepisów dotyczących ochrony poufnych lub niejawnych informacji ani dla zagwarantowania podstawowych funkcji państwowych, takich jak bezpieczeństwo narodowe.** Wszelkie informacje uzyskane w trakcie procesu wzajemnego [...] **uczenia się** wykorzystuje się wyłącznie do tego celu. Eksperci uczestniczący we wzajemnym [...] **uczeniu się** nie ujawniają osobom trzecim żadnych informacji szczególnie chronionych ani poufnych uzyskanych w [...] **tym kontekście**. **Państwa członkowskie uczestniczące we wzajemnym uczeniu się mogą z należycie uzasadnionych powodów, o których powiadomiono Grupę Współpracy, sprzeciwić się wyznaczeniu konkretnych ekspertów.**

5. Po **przeanalizowaniu podczas rundy wzajemnego uczenia się** [...] te same aspekty nie podlegają kolejnym **rundom** wzajemnego **uczenia się** [...] w **uczestniczących** państwach członkowskich przez [...] **cztery** lata od zakończenia **tej** rundy **wzajemnego** [...] **uczenia się, chyba że zainteresowane państwo członkowskie tego zażąda lub zgodzi się na propozycję** [...] **Grupy Współpracy[...]**.

6. [...]

7. Eksperci uczestniczący w **rundach** wzajemnego [...] **uczenia się** sporządzają sprawozdania dotyczące ustaleń i wniosków z [...] **ocen**. **Państwa członkowskie mogą zgłaszać uwagi do swoich projektów sprawozdań, załączane do sprawozdania.** Sprawozdania **końcowe** są przedkładane [...] Grupie Współpracy [...]. **Państwa członkowskie mogą zdecydować o publicznym udostępnieniu swoich sprawozdań.**

ROZDZIAŁ IV

Zarządzanie ryzykiem w cyberprzestrzeni i obowiązki w zakresie zgłaszania incydentów

SEKCJA I

Zarządzanie ryzykiem w cyberprzestrzeni i zgłaszanie incydentów

Artykuł 17

Zarządzanie

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

   Stosowanie niniejszego ustępu pozostaje bez uszczerbku dla przepisów krajowych państw członkowskich dotyczących zasad odpowiedzialności w instytucjach publicznych, jak również odpowiedzialności urzędników publicznych oraz urzędników wybranych i mianowanych.

2. Państwa członkowskie zapewniają, aby **członkowie organu zarządzającego** [...] **podlegali wymogowi** odbywania [...] szkoleń w celu zdobycia wiedzy i umiejętności wystarczających do zrozumienia i oceny ryzyk w cyberprzestrzeni oraz praktyk z zakresu zarządzania takimi ryzykami oraz ich wpływu na działalność podmiotu.

Artykuł 18

Środki zarządzania ryzykiem w cyberprzestrzeni

1**a. W niniejszej dyrektywie stosuje się podejście uwzględniające wszystkie zagrożenia, które obejmuje ochronę sieci i systemów informatycznych i ich środowiska fizycznego przed wszelkimi zdarzeniami, które mogłyby naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem.**

1. Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne [...] wprowadzały odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami dla bezpieczeństwa sieci [...] i systemów informatycznych wykorzystywanych przez te podmioty do świadczenia usług. Z uwagi na najnowszy stan wiedzy i **koszty wdrażania**, środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. **Przy ocenie proporcjonalności tych środków należy odpowiednio uwzględnić stopień narażenia podmiotu na ryzyko, jego wielkość, prawdopodobieństwo wystąpienia incydentów i ich dotkliwość. Z uwagi na poziom i rodzaj ryzyka dla społeczeństwa w przypadku incydentów mających wpływ na podmioty niezbędne lub istotne środki zarządzania ryzykiem w cyberprzestrzeni nakładane na podmioty istotne mogą być mniej rygorystyczne niż środki nakładane na podmioty niezbędne.**

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

a) analizę ryzyka i politykę bezpieczeństwa systemów informatycznych;

b) postępowanie w przypadku incydentu (zapobieganie incydentom, ich wykrywanie, [...] reagowanie na nie i **przywracanie stanu sprzed** [...] ich wystąpienia);

c) ciągłość działania i zarządzanie kryzysowe;

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

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

f) polityki i procedury [...] służące ocenie skuteczności środków zarządzania ryzykiem w cyberprzestrzeni;

g) **politykę w zakresie** stosowania kryptografii i szyfrowania;

ga) bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami.

3. Państwa członkowskie zapewniają, aby w przypadku rozważania odpowiednich środków, o których mowa w ust. 2 lit. d), podmioty [...] **podlegały wymogowi** uwzględniania podatności charakterystycznych dla każdego **bezpośredniego** dostawcy produktów i usług oraz ogólnej jakości produktów i praktyk w zakresie cyberbezpieczeństwa swoich dostawców produktów i usług, w tym ich procedury bezpiecznego opracowywania. **Państwa członkowskie zapewniają również, aby przy rozważaniu odpowiednich środków, o których mowa w ust. 2 lit. d), podmioty podlegały wymogowi uwzględniania wyników skoordynowanych ocen ryzyka przeprowadzonych zgodnie z art. 19 ust. 1.**

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

5. Komisja może przyjąć akty wykonawcze w celu określenia specyfikacji technicznych i metodologicznych, a **także, w razie potrzeby, sektorowych specyfikacji elementów,** o których mowa w ust. 2 **niniejszego artykułu**. **Komisja przyjmie do dnia [18 miesięcy po wejściu w życie niniejszej dyrektywy] akty wykonawcze w celu określenia technicznych i metodologicznych specyfikacji dotyczących podmiotów, o których mowa w art. 24 ust. 1, i dostawców usług zaufanych, o których mowa w załączniku I pkt 8. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2.** [...] Przygotowując [...] **takie** akty **wykonawcze**, Komisja [...], w jak najszerszym zakresie, **stosuje się do** norm międzynarodowych i europejskich, a także odpowiednich specyfikacji technicznych, **oraz wymienia się poradami z Grupą Współpracy i ENISA na temat projektu aktu wykonawczego zgodnie z art. 12 ust. 4 lit. d).**

6. [...]

Artykuł 19

Unijna skoordynowana ocena ryzyka krytycznych łańcuchów dostaw

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

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

Artykuł 20

Obowiązki w zakresie zgłaszania incydentów

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

2. [...]

   W stosownych przypadkach [...] podmioty **niezbędne i istotne** bez zbędnej zwłoki powiadamiają odbiorców swoich usług, których potencjalnie dotyczy znaczące cyberzagrożenie, o wszelkich środkach zaradczych lub innych środkach, które ci odbiorcy mogą zastosować w odpowiedzi na to zagrożenie. W stosownych przypadkach podmioty powiadamiają również tych odbiorców o samym zagrożeniu. **Akt** zgłoszenia nie może **sam w sobie** narażać podmiotu zgłaszającego na zwiększoną odpowiedzialność.

3. Incydent uznaje się za znaczący, jeżeli:

a) incydent spowodował lub może spowodować poważne [...] zakłócenia operacyjne **usługi** lub straty finansowe dla danego podmiotu;

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

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

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

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

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

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

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

(iii) zastosowane i bieżące środki ograniczające ryzyko.

Państwa członkowskie przewidują – w należycie uzasadnionych przypadkach i w porozumieniu z właściwymi organami lub CSIRT – możliwość odstąpienia przez dany podmiot od terminu określonego w lit. a) i c). W **szczególności odstępstwo od terminu, o którym mowa w lit. c), może być uzasadnione w przypadkach, gdy incydent nadal trwa.**

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

6. W stosownych przypadkach, w szczególności gdy incydent, o którym mowa w ust. 1, dotyczy co najmniej dwóch państw członkowskich, właściwy organ, CSIRT lub **pojedynczy punkt kontaktowy** informują o incydencie pozostałe państwa członkowskie, których dotyczy incydent, i ENISA. **Informacje takie obejmują co najmniej elementy przewidziane w ust. 4 niniejszego artykułu.** W działaniach tych właściwe organy, CSIRT i pojedyncze punkty kontaktowe – zgodnie z prawem Unii lub prawodawstwem krajowym zgodnym z prawem Unii – chronią interesy bezpieczeństwa i interesy handlowe podmiotu, jak również zachowują poufność przekazywanych informacji.

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

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

9. Pojedynczy punkt kontaktowy [...] **co sześć miesięcy** przedkłada ENISA sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane dotyczące incydentów, znaczących cyberzagrożeń i zdarzeń potencjalnie wypadkowych zgłoszonych zgodnie z ust. [...] 1 [...] oraz zgodnie z art. 27. Aby przyczynić się do dostarczania porównywalnych informacji, ENISA może wydawać wskazówki techniczne dotyczące parametrów informacji zawartych w sprawozdaniu podsumowującym. **ENISA co sześć miesięcy informuje Grupę Współpracy i sieć CSIRT o swoich ustaleniach dotyczących otrzymanych zgłoszeń.**

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

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

Artykuł 21

Stosowanie europejskich programów certyfikacji cyberbezpieczeństwa

1. Aby wykazać zgodność z niektórymi wymogami określonymi w art. 18, **państwa członkowskie mogą wymagać od podmiotów używania konkretnych produktów,** [...] **usług i** [...] **procesów ICT certyfikowanych** w oparciu o określone europejskie programy certyfikacji cyberbezpieczeństwa przyjęte na podstawie art. 49 rozporządzenia (UE) 2019/881. Produkty, usługi i procesy **ICT** podlegające certyfikacji mogą być opracowywane przez podmiot niezbędny lub istotny lub mogą być zamawiane u osób trzecich.

2. Komisja może [...] przyjąć [...] akty **wykonawcze** określające, które kategorie podmiotów niezbędnych **lub istotnych** podlegają wymogowi **używania pewnych certyfikowanych produktów, usług i procesów ICT lub** uzyskania certyfikacji [...] i na podstawie których [...] europejskich programów certyfikacji cyberbezpieczeństwa **przyjętych na podstawie art. 49 rozporządzenia (UE) 2019/881.** [...]**Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2. Przygotowując takie akty wykonawcze, Komisja, zgodnie z art. 56 rozporządzenia (UE) 2019/881:**

   (i) bierze pod uwagę wpływ danych środków na producentów lub dostawców takich produktów, usług lub procesów ICT oraz na użytkowników pod względem kosztów tych środków lub korzyści społecznych lub gospodarczych wynikających z przewidywanego zwiększonego poziomu bezpieczeństwa wskazanych produktów, usług lub procesów ICT, a także dostępności ich alternatyw na rynku;

   (ii) prowadzi otwarty, przejrzysty i integracyjny proces konsultacji ze wszystkimi odpowiednimi zainteresowanymi stronami i państwami członkowskimi;

(iii) bierze pod uwagę terminy wdrożenia, środki i okresy przejściowe, w szczególności pod względem ewentualnego wpływu danego środka na producentów lub dostawców produktów, usług lub procesów ICT lub też ich użytkowników, w szczególności MŚP;

(iv) bierze pod uwagę istnienie i wdrażanie odpowiednich przepisów państw członkowskich.

3. Komisja może zwrócić się do ENISA o przygotowanie propozycji programu **lub o dokonanie przeglądu istniejącego europejskiego programu certyfikacji cyberbezpieczeństwa** na podstawie art. 48 ust. 2 rozporządzenia (UE) 2019/881 w przypadkach, gdy do celów ust. 2 **niniejszego artykułu** nie jest dostępny odpowiedni europejski program certyfikacji cyberbezpieczeństwa.

Artykuł 22

Normalizacja

1. Aby wspierać spójne wdrażanie art. 18 ust. 1 i 2, państwa członkowskie, nie narzucając ani nie faworyzując wykorzystywania określonego rodzaju technologii, zachęcają do stosowania europejskich lub uznanych międzynarodowo norm i specyfikacji istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych.

2. ENISA, we współpracy z państwami członkowskimi, opracowuje porady i wytyczne dotyczące kwestii technicznych, które powinny zostać wzięte pod uwagę w odniesieniu do ust. 1, a także dotyczące już istniejących norm, w tym krajowych norm państw członkowskich, które pozwoliłyby na uwzględnienie tych obszarów.

Artykuł 23

Bazy danych zawierające nazwy domen i dane rejestracyjne

1. W celu wzmocnienia bezpieczeństwa, stabilności i odporności DNS państwa członkowskie zapewniają, aby rejestry **nazw** TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD z należytą starannością gromadziły i zachowywały w specjalnej bazie danych dokładne i kompletne dane dotyczące rejestracji nazw domen, **zgodnie z** [...] unijnymi przepisami o ochronie danych w odniesieniu do danych będących danymi osobowymi.

2. Państwa członkowskie zapewniają, aby w bazach danych zawierających dane dotyczące rejestracji nazw domen, o których mowa w ust. 1, znajdowały się informacje niezbędne do zidentyfikowania posiadaczy nazw domen i punktów kontaktowych zarządzających nazwami domen w ramach TLD i do skontaktowania się z nimi**, w tym co najmniej następujące dane:**

   a) nazwa domeny

   b) data rejestracji

   c) dane rejestrującego, w tym:

      (i) w przypadku osób fizycznych – imię i nazwisko i adres e-mail;

      (ii) w przypadku osób prawnych – nazwa i adres e-mail.

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

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

5. Państwa członkowskie zapewniają, aby rejestry **nazw** TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD, na zgodny z prawem i należycie uzasadniony wniosek złożony przez wnioskodawców ubiegających się o prawnie uzasadniony dostęp, udzielały dostępu do konkretnych danych dotyczących rejestracji nazw domen zgodnie z unijnymi przepisami o ochronie danych. Państwa członkowskie zapewniają, aby rejestry **nazw** TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD bez zbędnej zwłoki i w **każdym razie w ciągu 72 godzin** udzielały odpowiedzi na wszystkie wnioski o dostęp. Państwa członkowskie zapewniają, aby polityki i procedury regulujące ujawnianie takich danych podawano do wiadomości publicznej.

Sekcja II

Jurysdykcja i rejestracja

Artykuł 24

Jurysdykcja i terytorialność

1a. Uznaje się, że podmioty objęte zakresem niniejszej dyrektywy podlegają jurysdykcji państwa członkowskiego, w którym świadczą usługi. Uznaje się, że podmioty, o których mowa w załączniku I pkt 1–7 i 10, dostawcy usług zaufania i dostawcy punktów wymiany ruchu internetowego, o których mowa w załączniku I pkt 8 oraz w załączniku II pkt 1–5 do niniejszej dyrektywy, podlegają jurysdykcji państwa członkowskiego, na którego terytorium mają jednostkę organizacyjną.

1. Uznaje się, że dostawcy usług DNS, rejestry nazw TLD [...] i **podmioty świadczące usługi rejestracji nazw domen dla TLD**, dostawcy usług w chmurze, dostawcy usług ośrodka przetwarzania danych, [...] dostawcy sieci dostarczania treści**, dostawcy usług zarządzanych oraz dostawcy zarządzanych usług w zakresie bezpieczeństwa**, o których mowa w załączniku I pkt 8 i **8a**, a także dostawcy usług cyfrowych, o których mowa w załączniku II pkt 6, podlegają jurysdykcji państwa członkowskiego, w którym znajduje się ich główna jednostka organizacyjna w Unii.

2. Do celów niniejszej dyrektywy uznaje się, że podmioty, o których mowa w ust. 1, posiadają swoją główną jednostkę organizacyjną w Unii w tym państwie członkowskim, w którym **głównie** podejmowane są decyzje związane ze środkami zarządzania ryzykiem w cyberprzestrzeni. Jeżeli **nie można określić miejsca, w którym takie decyzje są głównie podejmowane, lub** takich decyzji nie podejmuje się w żadnej jednostce w Unii, uznaje się, że główna jednostka organizacyjna znajduje się w państwie członkowskim, w którym dany podmiot ma jednostkę organizacyjną o największej liczbie pracowników w Unii. **Jeżeli usługi świadczy grupa przedsiębiorstw, za główną jednostkę organizacyjną uznaje się główną jednostkę organizacyjną grupy przedsiębiorstw.**

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

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

4a. Państwa członkowskie, które otrzymały wniosek o wzajemną pomoc w odniesieniu do podmiotów, o których mowa w ust. 1, mogą, w granicach wniosku, podjąć odpowiednie środki nadzoru i egzekwowania przepisów w odniesieniu do danego podmiotu świadczącego usługi lub posiadającego sieć i system informatyczny na ich terytorium.

Artykuł 25

Rejestr niektórych podmiotów infrastruktury cyfrowej i dostawców usług cyfrowych

1. [...] **Państwa członkowskie zapewniają, aby** [...] podmioty, o **których mowa w art. 24 ust. 1, mające swoją główną jednostkę organizacyjną na ich terytorium lub, w przypadku braku jednostki organizacyjnej w Unii, mające swojego wyznaczonego przedstawiciela w Unii mającego jednostkę organizacyjną na ich terytorium, podlegały wymogowi** [...] przekazania **właściwym organom** następujących informacji [...] do dnia [najpóźniej 12 miesięcy od wejścia w życie niniejszej dyrektywy]:

a) nazwa podmiotu;

aa) rodzaj podmiotu zgodnie z załącznikami I i II do niniejszej dyrektywy;

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

c) aktualne dane kontaktowe, w tym adresy e-mail i numery telefonów podmiotów oraz ich przedstawicieli;

d) państwa członkowskie, w których podmiot świadczy usługę.

W stosownych przypadkach informacje te przekazuje się za pośrednictwem krajowego mechanizmu [...] samodzielnego zgłaszania, o którym mowa w art. 2a.

2. **Państwa członkowskie zapewniają, aby** [...] podmioty, o których mowa w ust. 1, [...] **powiadamiały także** o wszelkich zmianach danych, które przekazały na podstawie ust. 1, niezwłocznie, a w każdym razie w terminie trzech miesięcy od dnia, w którym nastąpiła zmiana.

3. [...] **Pojedyncze punkty kontaktowe państw członkowskich** przekazują [...] do [...] **ENISA informacje, o których mowa w ust. 1 i 2**. [...]

3a. Na podstawie informacji otrzymanych zgodnie z ust. 3 niniejszego artykułu ENISA tworzy i utrzymuje rejestr podmiotów, o których mowa w ust. 1. Na wniosek państw członkowskich ENISA umożliwia odpowiednim właściwym organom dostęp do rejestru, zapewniając jednocześnie, w stosownych przypadkach, gwarancje niezbędne do ochrony poufności informacji.

4. [...]

ROZDZIAŁ V

Wymiana informacji

Artykuł 26

Uzgodnienia dotyczące wymiany informacji na temat cyberbezpieczeństwa

1. [...] Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne mogły, **na zasadzie dobrowolności**, wymieniać się odpowiednimi informacjami na temat cyberbezpieczeństwa, w tym informacjami dotyczącymi cyberzagrożeń, **zdarzeń potencjalnie wypadkowych,** podatności, oznak naruszenia integralności systemu, taktyk, technik i procedur, alarmów dotyczących cyberbezpieczeństwa i narzędzi konfiguracji, jeżeli wymiana takich informacji:

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

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

2. Państwa członkowskie zapewniają, aby wymiana informacji odbywała się w [...] społecznościach podmiotów niezbędnych i istotnych. Wymianę taką prowadzi się za pośrednictwem mechanizmów wymiany informacji ze względu na potencjalnie poufny charakter wymienianych informacji [...].

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

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

5. [...] ENISA pomaga w ustanowieniu mechanizmów wymiany informacji na temat cyberbezpieczeństwa, o których mowa w ust. 2, zapewniając najlepsze praktyki i wskazówki.

Artykuł 27

Dobrowolne zgłaszanie odpowiednich informacji

1. Bez uszczerbku dla art. 20 państwa członkowskie zapewniają, aby podmioty niezbędne i istotne mogły na zasadzie dobrowolności zgłaszać właściwym organom lub CSIRT wszelkie istotne incydenty, cyberzagrożenia lub zdarzenia potencjalnie wypadkowe.

2. Bez uszczerbku dla art. 3, państwa członkowskie zapewniają, aby podmioty nieobjęte zakresem niniejszej dyrektywy mogły na zasadzie dobrowolności dokonywać zgłoszeń znaczących incydentów, cyberzagrożeń lub zdarzeń potencjalnie wypadkowych. Przy rozpatrywaniu zgłoszeń państwa członkowskie postępują zgodnie z procedurą określoną w art. 20. Państwa członkowskie mogą rozpatrywać zgłoszenia obowiązkowe priorytetowo względem zgłoszeń dobrowolnych. **Bez uszczerbku dla prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw** [...] dobrowolne zgłaszanie nie może skutkować nałożeniem na podmiot zgłaszający żadnych dodatkowych obowiązków, którym by nie podlegał, gdyby nie dokonał tego zgłoszenia.

3. Zgłoszenia dobrowolne są rozpatrywane wyłącznie wtedy, gdy takie rozpatrywanie nie stanowi nieproporcjonalnego czy nadmiernego obciążenia dla danego państwa członkowskiego.

ROZDZIAŁ VI

Nadzór i egzekwowanie przepisów

Artykuł 28

Ogólne aspekty nadzoru i egzekwowania przepisów

1. Państwa członkowskie zapewniają, aby właściwe organy skutecznie monitorowały zgodność z niniejszą dyrektywą[...], w szczególności z obowiązkami przewidzianymi w art. 18**,** [...] 20 **i 23**, i stosowały środki niezbędne do zapewnienia takiej zgodności. **Państwa członkowskie mogą zezwolić właściwym organom na priorytetowe traktowanie nadzoru, która to decyzja opiera się na podejściu opartym na ryzyku.**

2. Podejmując działania w odpowiedzi na cyberincydenty, właściwe organy działają w ścisłej współpracy z organami ochrony danych, **właściwymi organami wyznaczonymi na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych], organami nadzorczymi wyznaczonymi na podstawie rozporządzenia (UE) nr 910/2014 i właściwymi organami wyznaczonymi na mocy innych sektorowych unijnych aktów prawnych**. [...]

3. Bez uszczerbku dla krajowych ram ustawodawczych i instytucjonalnych państwa członkowskie zapewniają, aby w ramach nadzoru nad przestrzeganiem niniejszej dyrektywy przez podmioty administracji publicznej oraz egzekwowania ewentualnych sankcji za nieprzestrzeganie przepisów właściwe organy posiadały odpowiednie uprawnienia do wykonywania takich zadań w sposób niezależny pod względem operacyjnym wobec nadzorowanych podmiotów. Państwa członkowskie mogą podjąć decyzję o nałożeniu odpowiednich, proporcjonalnych i skutecznych środków nadzoru i egzekwowania przepisów w odniesieniu do tych podmiotów zgodnie z ramami krajowymi i porządkiem prawnym.

Artykuł 29

Nadzór i egzekwowanie przepisów w odniesieniu do podmiotów niezbędnych

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

2. Państwa członkowskie zapewniają, aby wykonując swoje zadania nadzorcze wobec podmiotów niezbędnych, właściwe organy **stosowały podejście oparte na ryzyku i** były uprawnione do obejmowania tych podmiotów **co najmniej**:

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

   b) b) regularnymi audytami **bezpieczeństwa**;

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

   d) skanami bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów oceny ryzyka**, w razie potrzeby ze względów technicznych we współpracy z danym podmiotem;**

   e) żądaniami przekazania informacji niezbędnych do oceny środków w zakresie cyberbezpieczeństwa przyjętych przez podmiot, w tym dokumentów dotyczących polityki cyberbezpieczeństwa[...];

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

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

2a. Wykonując swoje zadania nadzorcze przewidziane w ust. 2 niniejszego artykułu, właściwe organy mogą ustanowić metodyki nadzorcze umożliwiające priorytetowe traktowanie takich zadań na podstawie podejścia opartego na ryzyku.

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

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

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

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

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

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

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

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

g) [...]

h) nakazania tym podmiotom, aby w określony sposób podały do wiadomości publicznej informacje o aspektach niewypełnienia obowiązków określonych w niniejszej dyrektywie**, gdy takie publiczne ujawnienie nie prowadzi do szkodliwego narażenia danego podmiotu**;

i) [...]

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

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

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

b) nałożenia lub zwrócenia się o nałożenie przez właściwe organy lub sądy zgodnie z przepisami krajowymi tymczasowego zakazu pełnienia funkcji zarządczych w takim podmiocie niezbędnym na każdą osobę wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela prawnego w tym podmiocie oraz na każdą inną osobę fizyczną uznaną za odpowiedzialną za naruszenie.

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

Sankcje przewidziane w niniejszym ustępie nie mają zastosowania do podmiotów administracji publicznej podlegających niniejszej dyrektywie.

6. Państwa członkowskie zapewniają, aby każda osoba fizyczna odpowiedzialna za podmiot niezbędny lub działająca w charakterze przedstawiciela tego podmiotu na podstawie uprawnienia do jego reprezentowania, podejmowania decyzji w jego imieniu lub sprawowania nad nim kontroli posiadała uprawnienia do zapewnienia wypełnienia przez ten podmiot obowiązków przewidzianych w niniejszej dyrektywie. Państwa członkowskie zapewniają, aby te osoby fizyczne mogły zostać pociągnięte do odpowiedzialności za niewywiązanie się z obowiązku zapewnienia przestrzegania obowiązków przewidzianych w niniejszej dyrektywie. W **odniesieniu do podmiotów administracji publicznej niniejszy przepis pozostaje bez uszczerbku dla przepisów państw członkowskich dotyczących odpowiedzialności urzędników publicznych oraz urzędników wybranych i mianowanych.**

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

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

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

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

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

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

f) stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji;

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

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

9. Państwa członkowskie zapewniają, aby ich właściwe organy **na mocy niniejszej dyrektywy** informowały odpowiednie właściwe organy w **tym samym** [...] państwie członkowskim [...] wyznaczone na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych], w przypadku gdy wykonują swoje uprawnienia w zakresie nadzoru i egzekwowania przepisów, które to uprawnienia mają na celu zapewnienie wypełniania obowiązków przewidzianych w niniejszej dyrektywie przez podmiot niezbędny uznany za podmiot krytyczny **[**lub za podmiot równoważny z podmiotem krytycznym**]** na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych]. W **stosownych przypadkach** [...] właściwe organy na mocy dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych] [...] **mogą zwrócić się do** właściwych organów **na mocy niniejszej dyrektywy** [...] o wykonywanie ich **uprawnień** w zakresie nadzoru i egzekwowania przepisów **względem** podmiotu niezbędnego objętego zakresem stosowania niniejszego dyrektywy, uznanego również za podmiot krytyczny **[**lub równoważny**] na mocy dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych].**

10. Państwa członkowskie zapewniają, aby ich właściwe organy na mocy niniejszej dyrektywy informowały forum nadzoru na podstawie art. 29 ust. 1 rozporządzenia (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej] o wykonywaniu uprawnień w zakresie nadzoru i egzekwowania przepisów mających na celu zapewnienie przestrzegania obowiązków na podstawie niniejszej dyrektywy przez podmiot niezbędny wyznaczony jako dostawca usług ICT będący stroną trzecią o krytycznym znaczeniu na podstawie art. 28 rozporządzenia (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej].

10a. Państwa członkowskie zapewniają, aby ich właściwe organy na mocy niniejszej dyrektywy informowały odpowiednie właściwe organy wyznaczone na podstawie rozporządzenia (UE) 910/2014 o wykonywaniu uprawnień w zakresie nadzoru i egzekwowania przepisów mających na celu zapewnienie przestrzegania obowiązków na podstawie niniejszej dyrektywy przez podmiot wyznaczony jako dostawca usług zaufania na podstawie rozporządzenia (UE) 910/2014.

Artykuł 30

Nadzór i egzekwowanie przepisów w stosunku do podmiotów istotnych

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

2. Państwa członkowskie zapewniają, aby wykonując swoje zadania nadzorcze wobec podmiotów istotnych, właściwe organy **stosowały podejście oparte na ryzyku i** były uprawnione do obejmowania tych podmiotów **co najmniej**:

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

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

   c) skanami bezpieczeństwa na podstawie obiektywnych, **niedyskryminacyjnych,** sprawiedliwych i przejrzystych kryteriów oceny ryzyka**, w razie potrzeby ze względów technicznych we współpracy z danym podmiotem;**

   d) żądaniami przekazania informacji niezbędnych do przeprowadzenia oceny *ex post* dotyczącej środków w zakresie cyberbezpieczeństwa[...];

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

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

2a. Wykonując swoje zadania nadzorcze przewidziane w ust. 2 niniejszego artykułu, właściwe organy mogą ustanowić metodyki nadzorcze umożliwiające priorytetowe traktowanie takich zadań na podstawie podejścia opartego na ryzyku.

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

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

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

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

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

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

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

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

g) nakazania tym podmiotom, aby w określony sposób podały do wiadomości publicznej informacje o aspektach niewypełnienia obowiązków określonych w niniejszej dyrektywie**, gdy takie publiczne ujawnienie nie prowadzi do szkodliwego narażenia danego podmiotu**;

h) [...]

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

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

Artykuł 31

Ogólne warunki nakładania administracyjnych kar pieniężnych na podmioty niezbędne i istotne

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

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

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

4. Państwa członkowskie zapewniają, aby naruszenia obowiązków przewidzianych w art. 18 lub 20 **dokonane przez podmioty niezbędne** podlegały na mocy ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej **4**[...] 000 000 EUR lub**, w przypadku osoby prawnej,** [...] 2 % całkowitego rocznego światowego obrotu przedsiębiorstwa, do którego należy podmiot niezbędny [...], z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

4a. Państwa członkowskie zapewniają, aby naruszenia obowiązków przewidzianych w art. 18 lub 20 dokonane przez podmioty istotne podlegały na mocy ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej 2 000 000 EUR lub, w przypadku osoby prawnej, 1 % całkowitego rocznego światowego obrotu przedsiębiorstwa, do którego należy podmiot niezbędny, z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

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

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

6a. Jeżeli system prawny państwa członkowskiego nie przewiduje administracyjnych kar pieniężnych, państwa członkowskie zapewniają, aby niniejszy artykuł można było stosować w ten sposób, że o zastosowanie kary pieniężnej wnosi właściwy organ, a nakłada ją właściwy sąd krajowy, o ile zapewniona zostaje skuteczność tych rozwiązań prawnych i równoważność ich skutku względem administracyjnej kary pieniężnej nakładanej przez właściwe organy. Nakładane kary pieniężne muszą być w każdym przypadku skuteczne, proporcjonalne i odstraszające. Takie państwa członkowskie zawiadamiają Komisję o przepisach swojego prawa, które przyjęły zgodnie z niniejszym ustępem do dnia […], a następnie niezwłocznie o wszelkich późniejszych aktach zmieniających lub zmianach mających wpływ na te przepisy.

Artykuł 32

Naruszenia pociągające za sobą naruszenie ochrony danych osobowych

1. Jeżeli w **czasie nadzoru lub egzekwowania przepisów** właściwe organy [...] **powzięły wiedzę**, że naruszenie przez podmiot niezbędny lub istotny obowiązków przewidzianych w art. 18 i 20 **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 one o tym [...] organy nadzorcze właściwe na mocy art. 55 i 56 tego rozporządzenia.

2. W przypadku gdy organy nadzorcze właściwe na mocy art. 55 i 56 rozporządzenia (UE) 2016/679 podejmą decyzję o wykonaniu swoich uprawnień na podstawie art. 58 **ust. 2** lit. i) tego rozporządzenia i nałożą administracyjną karę pieniężną, właściwe organy, o **których mowa w art. 8 niniejszej dyrektywy**, nie nakładają na mocy art. 31 niniejszej dyrektywy administracyjnej kary pieniężnej za [...] naruszenie, które nastąpiło w **ramach tego samego czynu** [...]. Właściwe organy mogą jednak zastosować działania z zakresu egzekwowania przepisów lub skorzystać z uprawnień do nakładania sankcji, które to działania i uprawnienia przewidziano w art. 29 ust. 4 lit. a)–i), art. 29 ust. 5 i art. 30 ust. 4 lit. a)–h) niniejszej dyrektywy.

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

Artykuł 33

Kary

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

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

Artykuł 34

Wzajemna pomoc

1. Jeżeli podmiot niezbędny lub istotny świadczy usługi w więcej niż jednym państwie członkowskim lub [...] **świadczy usługi** w **co najmniej jednym** państwie członkowskim, ale jego sieć i systemy informatyczne są zlokalizowane w co najmniej jednym innym państwie członkowskim, właściwe organ**y odnośnych** państw członkowskich [...] współpracują ze sobą i udzielają sobie wzajemnie pomocy, odpowiednio do potrzeb. Współpraca ta obejmuje co najmniej następujące kwestie:

a) właściwe organy stosujące środki nadzoru lub egzekwowania przepisów w państwie członkowskim informują – za pośrednictwem pojedynczego punktu kontaktowego – właściwe organy w tych innych zainteresowanych państwach członkowskich o zastosowanych środkach nadzoru i egzekwowania przepisów 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 **proporcjonalnej do zasobów, którymi dysponuje**, tak aby środki nadzoru lub egzekwowania przepisów [...] mogły być wdrażane w sposób skuteczny, wydajny i spójny. Taka wzajemna pomoc może obejmować wnioski o udzielenie informacji i środki nadzoru, w tym wnioski o przeprowadzenie kontroli na miejscu lub nadzoru zdalnego lub ukierunkowanych audytów bezpieczeństwa. Właściwy organ, do którego skierowany jest wniosek o pomoc, nie może odmówić wykonania tego wniosku, chyba że po wymianie informacji z innymi zainteresowanymi organami [...] zostanie ustalone, że [...] organ ten nie jest organem właściwym do udzielenia wnioskowanej pomocy **lub nie ma niezbędnych zasobów** lub że pomoc, której dotyczy wniosek, nie jest proporcjonalna do zadań nadzorczych realizowanych przez właściwy organ [...] **lub wniosek dotyczy informacji lub obejmuje działania, które stoją w sprzeczności z bezpieczeństwem narodowym, bezpieczeństwem publicznym lub obroną tego państwa członkowskiego**.

2. W stosownych przypadkach i za obopólnym porozumieniem właściwe organy z poszczególnych państw członkowskich mogą przeprowadzać wspólne działania nadzorcze [...].

ROZDZIAŁ VII

Przepisy przejściowe i końcowe

Artykuł 35

Przegląd

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

Artykuł 36

[...]

[...]

[...]

Artykuł 37

Procedura komitetowa

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

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

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

Artykuł 38

Transpozycja

1. **Do dnia** … [[...]**24** miesiące od daty wejścia w życie niniejszej dyrektywy**]** państwa członkowskie przyjmują i publikują[...] przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają o tym Komisję. Państwa członkowskie stosują te środki od dnia … [jeden dzień po dniu, o którym mowa w akapicie pierwszym].

2. Przepisy 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 39

Zmiana rozporządzenia (UE) nr 910/2014

W rozporządzeniu (UE) nr 901/2014 uchyla się art. 19 [...] **ze skutkiem od dnia… [data terminu transpozycji niniejszej dyrektywy].**

Artykuł 40

Zmiana dyrektywy (UE) 2018/1972

W dyrektywie (UE) 2018/1972 uchyla się art. 40 i 41 [...] **ze skutkiem od dnia… [data terminu transpozycji niniejszej dyrektywy].**

Artykuł 41

Uchylenie

Dyrektywa (UE) 2016/1148 traci moc ze skutkiem od dnia.. [data terminu transpozycji dyrektywy].

Odniesienia do dyrektywy (UE) 2016/1148 interpretowane są jako odniesienia to niniejszej dyrektywy i odczytywane są zgodnie z tabelą korelacji w załączniku II[...].

Artykuł 42

Wejście w życie

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

Artykuł 43

Adresaci

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia […] r.

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

ZAŁĄCZNIK I

SEKTORY, PODSEKTORY I RODZAJE PODMIOTÓW

Sektor	Podsektor	Rodzaj podmiotu
1. Energia	a) Energia elektryczna	– przedsiębiorstwa energetyczne, o których mowa w art. 2 pkt 57 dyrektywy (UE) 2019/944, które wykonują funkcję „dostawy”, o której mowa w art. 2 pkt 12 tej dyrektywy([39])
		– operatorzy systemu dystrybucyjnego, o których mowa w art. 2 pkt 29 dyrektywy (UE) 2019/944
		– operatorzy systemu przesyłowego, o których mowa w art. 2 pkt 35 dyrektywy (UE) 2019/944
		– wytwórcy, o których mowa w art. 2 pkt 38 dyrektywy (UE) 2019/944
		— wyznaczeni operatorzy rynku energii elektrycznej, o których mowa w art. 2 pkt 8 rozporządzenia (UE) 2019/943([40])
		– uczestnicy rynku energii elektrycznej, o których mowa w art. 2 pkt 25 rozporządzenia (UE) 2019/943 i świadczący usługi agregacji, odpowiedzi odbioru lub magazynowania energii, o których mowa w art. 2 pkt 18, 20 i 59

[39] 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).

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

		dyrektywy (UE) 2019/944
	b) system ciepłowniczy lub chłodniczy	– system ciepłowniczy lub system chłodniczy, o którym mowa w art. 2 pkt 19 dyrektywy (UE) 2018/2001([41]) w sprawie promowania stosowania energii ze źródeł odnawialnych
	c) ropa naftowa	– operatorzy ropociągów
		– operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej
		— krajowe centrale zapasów naftowych, o których mowa w art. 2 lit. f) dyrektywy Rady 2009/119/WE([42])
	d) gaz	– przedsiębiorstwa dostarczające gaz, o których mowa w art. 2 pkt 8 dyrektywy (UE) 2009/73/WE([43])
		– operatorzy systemu dystrybucyjnego, o których mowa w art. 2 pkt 6 dyrektywy 2009/73/WE
		– operatorzy systemu przesyłowego, o których mowa w art. 2 pkt 4 dyrektywy 2009/73/WE
		– operatorzy systemu magazynowania, o których mowa

41 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).

42 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).

43 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).

		w art. 2 pkt 10 dyrektywy 2009/73/WE
		– operatorzy systemu LNG, o których mowa 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
2. Transport	a) transport lotniczy	– przewoźnicy lotniczy, o których mowa w art. 3 pkt 4 rozporządzenia (WE) nr 300/2008([44]), **wykorzystywani do celów handlowych**
		– zarządzający portem lotniczym, o których mowa w art. 2 pkt 2 dyrektywy 2009/12/WE([45]), porty lotnicze, o których mowa w art. 2 pkt 1 tej dyrektywy, w tym porty lotnicze sieci bazowej wymienione w sekcji 2 załącznika II do rozporządzenia (UE) nr 1315/2013([46]); oraz jednostki obsługujące urządzenia pomocnicze znajdujące się w portach lotniczych
		– operatorzy zarządzający ruchem lotniczym zapewniający służbę kontroli ruchu lotniczego (ATC),

[44] 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).

[45] 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).

[46] 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).

		o której mowa w art. 2 pkt 1 rozporządzenia (WE) nr 549/2004([47])
	b) transport kolejowy	– zarządcy infrastruktury, o których mowa w art. 3 pkt 2 dyrektywy 2012/34/UE([48])
		– przedsiębiorstwa kolejowe, o których mowa w art. 3 pkt 1 dyrektywy 2012/34/UE, w tym operatorzy obiektów infrastruktury usługowej, o których mowa w art. 3 pkt 12 dyrektywy 2012/34/UE
	c) transport wodny	– armatorzy śródlądowego, morskiego i przybrzeżnego wodnego transportu pasażerów i towarów, o których mowa w odniesieniu do transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004([49]), z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy
		– organy zarządzające portami, o których mowa w art. 3 pkt 1 dyrektywy 2005/65/WE([50]), w tym ich obiekty portowe, o których mowa w art. 2 pkt 11 rozporządzenia (WE) nr 725/2004; oraz jednostki wykonujące prace i operujące sprzętem znajdującym się w tych portach

[47] 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).

[48] 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).

[49] 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).

[50] 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).

		– operatorzy systemu ruchu statków, o którym mowa w art. 3 lit. o) dyrektywy 2002/59/WE([51])
	d) transport drogowy	– organy administracji drogowej, o których mowa w art. 2 pkt 12 rozporządzenia delegowanego Komisji (UE) 2015/962([52]), odpowiedzialne za zarządzanie ruchem drogowym**, z wyłączeniem podmiotów publicznych, dla których zarządzanie ruchem lub obsługa inteligentnych systemów transportowych stanowią jedynie inną niż istotna część ich ogólnej działalności.**
		– operatorzy inteligentnych systemów transportowych, o których mowa w art. 4 pkt 1 dyrektywy 2010/40/UE([53])
3. Bankowość		— instytucje kredytowe, o których mowa w art. 4 pkt 1 rozporządzenia (UE) nr 575/2013([54])**, [z wyjątkiem tych, o których mowa w art. 2 ust. 5 pkt 8 dyrektywy 2013/36/UE, które są wyłączone zgodnie z art. 2 ust. 4 rozporządzenia XX [rozporządzenie w sprawie operacyjnej odporności cyfrowej]]**

[51] 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).

[52] 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).

[53] 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).

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

4. Infrastruktura rynków finansowych		– operatorzy systemu obrotu, o którym mowa w art. 4 pkt 24 dyrektywy 2014/65/UE([55])
		– kontrahenci centralni, o których mowa w art. 2 pkt 1 rozporządzenia (UE) nr 648/2012([56])
5. Zdrowie		— świadczeniodawcy, o których mowa w art. 3 lit. g) dyrektywy 2011/24/UE([57])
		— laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia XXXX/XXXX w sprawie poważnych transgranicznych zagrożeń zdrowia[58]
		— podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych, o których mowa w art. 1 pkt 2 dyrektywy 2001/83/WE([59]) — 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, dla których uznano, że mają one krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego („wykaz

[55] 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).

[56] 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).

[57] 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).

[58] [Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylające decyzję nr 1082/2013/UE, odniesienie należy zaktualizować, kiedy już zostanie przyjęty wniosek COM(2020) 727 final].

[59] 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).

		wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego"), i o których mowa w art. 20 rozporządzenia XXXX[60]
6. Woda pitna		dostawcy i dystrybutorzy „wody przeznaczonej do spożycia przez ludzi", o której mowa w art. 2 pkt 1 lit. a) dyrektywy Rady 98/83/WE([61]), ale z wyłączeniem dystrybutorów, dla których dystrybucja wody przeznaczonej do spożycia przez ludzi stanowi jedynie **inną niż istotna** część ich ogólnej działalności polegającej na dystrybucji innych produktów i towarów [...]
7. Ścieki		przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki komunalne, bytowe i przemysłowe, o których mowa w art. 2 pkt 1–3 dyrektywy Rady 91/271/EWG([62]), **lecz z wyłączeniem przedsiębiorstw, dla których zbieranie, odprowadzanie lub oczyszczanie ścieków komunalnych, bytowych i przemysłowych stanowi jedynie inną niż istotna część ich ogólnej działalności.** [...]
8. Infrastruktura cyfrowa		– dostawcy punktu wymiany ruchu internetowego
		– dostawcy usług DNS**, z wyłączeniem operatorów głównych serwerów nazw**
		— rejestry nazw TLD

60 [Rozporządzenie Parlamentu Europejskiego i Rady 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; odniesienie należy zaktualizować, kiedy już zostanie przyjęty wniosek COM(2020) 725 final].

61 Dyrektywa Rady 98/83/WE z dnia 3 listopada 1998 r. w sprawie jakości wody przeznaczonej do spożycia przez ludzi (Dz.U. L 330 z 5.12.1998, s. 32).

62 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).

		– dostawcy usługi w chmurze
		– dostawcy usług ośrodka przetwarzania danych
		– dostawcy sieci dostarczania treści
		– dostawcy usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia (UE) nr 910/2014([63])
		– dostawcy publicznych sieci łączności elektronicznej, o których mowa w art. 2 pkt 8 dyrektywy (UE) 2018/1972([64]), lub dostawcy usług łączności elektronicznej, o których mowa w art. 2 pkt 4 dyrektywy (UE) 2018/1972, w przypadku gdy ich usługi są publicznie dostępne
8a. Zarządzanie usługami ICT **(B2B)**		**— Dostawcy usług zarządzanych (MSP)** **— Dostawcy zarządzanych usług w zakresie bezpieczeństwa (MSSP)**

[63] 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).

[64] 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).

9. **Podmioty** administracji publicznej		— Podmioty administracji publicznej rządów centralnych **zdefiniowanych przez państwa członkowskie zgodnie z prawem krajowym** — [...][65][...] — [...]
10. 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, o której mowa w art. 2 pkt 8 dyrektywy (UE) 2018/1972

65 [...]

ZAŁĄCZNIK II

SEKTORY, PODSEKTORY I RODZAJE PODMIOTÓW

Sektor	Podsektor	Rodzaj podmiotu
1. Usługi pocztowe i kurierskie		operatorzy świadczący usługi pocztowe, o których mowa w art. 2 pkt 1[...] dyrektywy 97/67/WE([66]), w **tym** [...] dostawcy usług kurierskich
2. Gospodarowanie odpadami		przedsiębiorstwa zajmujące się gospodarowaniem odpadami, o którym mowa w art. 3 pkt 9 dyrektywy 2008/98/WE([67]), z wyłączeniem przedsiębiorstw, dla których gospodarowanie odpadami nie stanowi głównej działalności gospodarczej

[66] 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)**, zmieniona dyrektywą 2008/6/WE Parlamentu Europejskiego i Rady z dnia 20 lutego 2008 r. zmieniającą dyrektywę 97/67/WE w odniesieniu do pełnego urzeczywistnienia rynku wewnętrznego usług pocztowych Wspólnoty (Dz.U. L 52 z 27.2.2008, s. 3)**.

[67] 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).

3. Produkcja, wytwarzanie i dystrybucja chemikaliów		przedsiębiorstwa zajmujące się produkcją[...] i dystrybucją substancji i [...] **mieszanin**, o których mowa w art. 3 pkt [...] 9 i 14 rozporządzenia (WE) nr 1907/2006([68]), **oraz przedsiębiorstwa zajmujące się produkcją wyrobów, o których mowa w art. 3 pkt 3 tego rozporządzenia, z substancji lub mieszanin.**
4. Produkcja, przetwarzanie i dystrybucja żywności		przedsiębiorstwa spożywcze, o których mowa w art. 3 pkt 2 rozporządzenia (WE) nr 178/2002([69]), **zajmujące się dystrybucją hurtową oraz produkcją przemysłową i przetwórstwem**
5. Produkcja	a) produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki *in vitro*	podmioty produkujące wyroby medyczne, o których mowa w art. 2 ust. 1 rozporządzenia (UE) 2017/745([70]), oraz podmioty produkujące wyroby medyczne do diagnostyki *in vitro*, o których mowa w art. 2 ust. 2 rozporządzenia (UE) 2017/746([71]), z wyjątkiem podmiotów

[68] 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).

[69] 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).

[70] 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).

[71] 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).

		produkujących wyroby medyczne wymienione w załączniku 1 pkt 5
	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
6. dostawcy usług cyfrowych		– dostawcy internetowych platform handlowych
		– dostawcy wyszukiwarek internetowych
		– dostawcy platform usług sieci społecznościowych