DYREKTYWA NIS(2) – SKRYPT

Spis treści:

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

1. TROCHĘ HISTORII, CZYLI DYREKTYWA NIS(1)

Dyrektywa NIS(1) – „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.”[1]

Pełen tekst Dyrektywy NIS(1) dostępny na stronie:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

„19.7.2016 PL Dziennik Urzędowy Unii Europejskiej L 194/1”

„Dyrektywa NIS [1] została przyjęta 6 lipca 2016 r. Jest pierwszym europejskim prawem w zakresie cyberbezpieczeństwa. Dyrektywa nakłada na państwa członkowskie szereg obowiązków, obliguje je do powołania konkretnych instytucji oraz wprowadzenia mechanizmów współpracy. W Polsce jej zapisy realizuje ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 roku.

Dyrektywa zobowiązuje wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego. Jej przepisy umożliwiają stworzenie zarówno scentralizowanego systemu na poziomie krajowym, jak i podzielenie kompetencji między różne podmioty.

Dyrektywa NIS nie dotyczy bezpośrednio usług administracji publicznej, o ile nie są to usługi kluczowe wymienione w dyrektywie. Dokument stanowi jednak harmonizację minimalną, a zatem wyznacza pewne minimalne warunki, które należy spełniać. Nie ogranicza przy tym możliwości państw członkowskich do regulowania problematyki cyberbezpieczeństwa administracji publicznej.

Tekst dyrektywy koncentruje się na trzech filarach:
- Instytucjach, które powinny powstać we wszystkich państwach członkowskich.
- Współpracy na poziomie europejskim.
- Zobowiązaniach w zakresie bezpieczeństwa sieci i informacji.”[2]

W Dzienniku Urzędowym Unii Europejskiej, który zawiera treść Dyrektywy NIS(2), na początku w opisie, podsumowano funkcjonowanie Dyrektywy NIS(1) i zwrócono uwagę dlaczego wymagało to wprowadzenia kolejnego, bardziej aktualnego dokumentu:

„(1) Celem dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 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

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

[2] https://cyberpolicy.nask.pl/dyrektywa-nis-czyli-pierwsze-europejskie-prawo-w-zakresie-cyberbezpieczenstwa/

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

zapewnienie ciągłości takich usług w przypadku wystąpienia incydentów, a tym samym przyczynienie się do bezpieczeństwa Unii oraz do sprawnego funkcjonowania jej gospodarki i społeczeństwa.

(2) Od momentu wejścia w życie dyrektywy (UE) 2016/1148 poczyniono znaczne postępy w podnoszeniu poziomu cyberodporności Unii. Przegląd tej dyrektywy pokazał, że stanowiła ona katalizator zmian w instytucjonalnym i regulacyjnym podejściu do cyberbezpieczeństwa w Unii oraz spowodowała znaczącą zmianę w sposobie myślenia. Dzięki tej dyrektywie utworzono ramy krajowe w zakresie bezpieczeństwa sieci i systemów informatycznych poprzez przyjęcie krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych i określenie krajowych zdolności oraz wdrożenie środków regulacyjnych obejmujących niezbędną infrastrukturę i podmioty wskazane przez poszczególne państwa członkowskie. Dyrektywa (UE) 2016/1148 przyczyniła się także do współpracy na poziomie Unii dzięki ustanowieniu Grupy Współpracy oraz sieci krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego. Pomimo tych osiągnięć przegląd dyrektywy (UE) 2016/1148 ujawnił tkwiące w niej braki, które uniemożliwiają skuteczne zaradzenie obecnym i pojawiającym się wyzwaniom w zakresie cyberbezpieczeństwa.

(3) Wraz z szybko postępującą transformacją cyfrową i siecią wzajemnych połączeń w społeczeństwie, w tym w kontekście wymiany transgranicznej, sieci i systemy informatyczne stały się zasadniczym elementem codziennego życia. Zmiana ta doprowadziła do ewolucji krajobrazu cyberzagrożeń, przynosząc nowe wyzwania, które wymagają dostosowanych, skoordynowanych i innowacyjnych reakcji we wszystkich państwach członkowskich. Liczba, skala, zaawansowanie, częstotliwość oraz wpływ incydentów stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. W rezultacie incydenty mogą utrudniać prowadzenie działalności gospodarczej na rynku wewnętrznym, powodować straty finansowe, podważać zaufanie użytkowników oraz powodować poważne szkody dla gospodarki i społeczeństwa Unii. Dlatego gotowość i skuteczność w obszarze cyberbezpieczeństwa stają się coraz ważniejsze dla prawidłowego funkcjonowania rynku wewnętrznego niż kiedykolwiek wcześniej. Ponadto w wielu sektorach krytycznych cyberbezpieczeństwo należy do kluczowych czynników umożliwiających udany przebieg transformacji cyfrowej i pełne wykorzystanie ekonomicznych i społecznych korzyści wynikających z cyfryzacji.

(4) Podstawę prawną dyrektywy (UE) 2016/1148 stanowił art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), którego celem jest ustanowienie i zapewnienie funkcjonowania rynku wewnętrznego przez usprawnienie środków służących zbliżeniu przepisów krajowych. Wymogi w zakresie cyberbezpieczeństwa nałożone na podmioty świadczące usługi lub prowadzące działalność kluczową z ekonomicznego punktu widzenia różnią się znacznie – swoim rodzajem i poziomem szczegółowości, a także metodami nadzoru – w zależności od państwa członkowskiego. Rozbieżności te pociągają za sobą dodatkowe koszty i powodują trudności dla podmiotów, które oferują towary lub usługi transgranicznie. Wymogi nałożone przez jedno państwo członkowskie, które różnią się od wymogów nałożonych przez inne państwo członkowskie lub nawet są z nimi sprzeczne, mogą w istotny sposób wpływać na taką transgraniczną działalność. Ponadto ewentualne nieodpowiednie zaprojektowanie lub wdrożenie wymogów dotyczących cyberbezpieczeństwa prawdopodobnie wywrze negatywny wpływ na poziom cyberbezpieczeństwa innych państw członkowskich, w szczególności z uwagi na intensywność wymiany transgranicznej.

Z przeglądu dyrektywy (UE) 2016/1148 wynika, że istnieją znaczne rozbieżności w jej wdrażaniu przez państwa członkowskie, w tym pod względem jej zakresu, którego ustalenie w znacznej mierze pozostawiono do uznania państw członkowskich. W dyrektywie (UE) 2016/1148 zapewniono państwom

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

członkowskim bardzo duży margines swobody także
w odniesieniu do wdrażania ustanowionych w niej obowiązków dotyczących bezpieczeństwa i zgłaszania incydentów. W rezultacie obowiązki te zostały wdrożone na poziomie krajowym w bardzo różny sposób. Podobne rozbieżności we wdrażaniu wystąpiły w odniesieniu do przepisów dyrektywy (UE) 2016/1148 dotyczących nadzoru i egzekwowania prawa.

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

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

(7) Na podstawie dyrektywy (UE) 2016/1148 państwa członkowskie były odpowiedzialne za identyfikację podmiotów spełniających kryteria pozwalające na uznanie ich za operatorów usług kluczowych. Aby wyeliminować znaczne rozbieżności pod tym względem między państwami członkowskimi oraz zapewnić wszystkim podmiotom objętym regulacją pewność prawa w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie i do obowiązków dotyczących zgłaszania incydentów, należy ustanowić jednolite kryterium określające, które podmioty są objęte zakresem stosowania niniejszej dyrektywy. Kryterium to powinno przewidywać stosowanie zasady wielkościowej przewidującej, że zakres stosowania niniejszej dyrektywy obejmuje wszystkie podmioty, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia Komisji 2003/361/WE (5) lub które przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu oraz które działają w sektorach objętych tą dyrektywą lub świadczą objęte nią rodzaje usług lub prowadzą objętą nią działalność. Państwa członkowskie powinny również zapewnić objęcie zakresem niniejszej dyrektywy niektórych małych przedsiębiorstw i mikroprzedsiębiorstw zgodnie z definicją w art. 2 ust. 2 i 3 tego załącznika, które spełniają szczególne kryteria wskazujące na kluczową rolę dla społeczeństwa, gospodarki lub konkretnych sektorów lub rodzajów usług.”[3]

[3] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

2. CO TO JEST DYREKTYWA NIS(2)?

Dyrektywa NIS(2) – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.[4]

Została sporządzona w Strasburgu dnia 14 grudnia 2022 r.

Pełen tekst Dyrektywy NIS2 dostępny na stronie:

https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

„L 333/80 PL Dziennik Urzędowy Unii Europejskiej 27.12.2022"

„W 2023 r. weszła w życie Dyrektywa NIS 2, która zmieni kształt cyberbezpieczeństwa w Państwach Członkowskich Unii Europejskiej. (…)

Od daty wejścia w życie Dyrektywy, czyli 16 stycznia 2023 r., Państwa Członkowskie UE mają 21 miesięcy na wprowadzenie postanowień Dyrektywy do prawa krajowego. Nowe przepisy powinny być stosowane we wszystkich krajach Unii Europejskiej od 18 października 2024 r."[5]

3. CO ZAWIERA DYREKTYWA NIS(2)?

TABELA: Zawartość Dyrektywy NIS(2)

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555 z dnia 14 grudnia 2022 r.	**ROZDZIAŁ I** PRZEPISY OGÓLNE	**Art. 1** - Przedmiot
		Art. 2 - Zakres
		Art. 3 - Podmioty kluczowe i ważne
		Art. 4 - Sektorowe akty prawne Unii
		Art. 5 - Harmonizacja minimalna
		Art. 6 - Definicje
	ROZDZIAŁ II SKOORDYNOWANE RAMY W ZAKRESIE CYBERBEZPIECZEŃSTWA	**Art. 7** - Krajowa strategia cyberbezpieczeństwa
		Art. 8 - Właściwe organy i pojedyncze punkty kontaktowe
		Art. 9 - Krajowe ramy zarządzania kryzysowego w cyberbezpieczeństwie
		Art. 10 - Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)
		Art. 11 - Wymogi dotyczące CSIRT, ich zdolności techniczne i zadania
		Art. 12 - Skoordynowane ujawnianie podatności i europejska baza danych dotyczących podatności
		Art. 13 - Współpraca na poziomie krajowym
	ROZDZIAŁ III WSPÓŁPRACA NA POZIOMIE UNIJNYM I MIĘDZYNARODOWYM	**Art. 14** - Grupa Współpracy
		Art. 15 - Sieć CSIRT
		Art. 16 - Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe)
		Art. 17 - Współpraca międzynarodowa
		Art. 18 - Sprawozdanie o stanie cyberbezpieczeństwa w Unii
		Art. 19 - Oceny wzajemne
	ROZDZIAŁ IV ŚRODKI ZARZĄDZANIA RYZYKIEM W CYBERBEZPIECZEŃSTWIE I OBOWIĄZKI DOTYCZĄCE	**Art. 20** - Zarządzanie
		Art.. 21 - Środki zarządzania ryzykiem w cyberbezpieczeństwie
		Art. 22 - Skoordynowane na poziomie Unii szacowanie ryzyka krytycznych łańcuchów dostaw

[4] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

[5] https://www.gov.pl/web/infrastruktura/informacje-biezace

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

	ZGŁASZANIA INCYDENTÓW	**Art. 23** - Obowiązki w zakresie zgłaszania incydentów
		Art. 24 - Stosowanie europejskich programów certyfikacji cyberbezpieczeństwa
		Art. 25 - Normalizacja
	ROZDZIAŁ V JURYSDYKCJA I REJESTRACJA	**Art. 26** - Jurysdykcja i terytorialność
		Art. 27 - Rejestr podmiotów
		Art. 28 - Baza danych dotyczących rejestracji nazw domen
	ROZDZIAŁ VI WYMIANA INFORMACJI	**Art. 29** - Mechanizmy wymiany informacji na temat cyberbezpieczeństwa
		Art. 30 - Dobrowolne zgłaszanie ważnych informacji
	ROZDZIAŁ VII NADZÓR I EGZEKWOWANIE PRZEPISÓW	**Art. 31** - Ogólne aspekty nadzoru i egzekwowania przepisów
		Art. 32 - Środki nadzoru i egzekwowania przepisów dla podmiotów kluczowych
		Art. 33 - Środki nadzoru i egzekwowania przepisów w odniesieniu do podmiotów ważnych
		Art. 34 - Ogólne warunki nakładania administracyjnych kar pieniężnych na podmioty kluczowe i ważne
		Art. 35 - Naruszenia pociągające za sobą naruszenie ochrony danych osobowych
		Art. 36 - Kary
		Art. 37 - Wzajemna pomoc
	ROZDZIAŁ VIII AKTY DELEGOWANE I WYKONAWCZE	**Art. 38** - Wykonywanie przekazanych uprawnień
		Art. 39 - Procedura komitetowa
	ROZDZIAŁ IX PRZEPISY KOŃCOWE	**Art. 40** - Przegląd
		Art. 41 - Transpozycja
		Art. 42 - Zmiana rozporządzenia (UE) nr 910/2014
		Art. 43 - Zmiana dyrektywy (UE) 2018/1972
		Art. 44 - Uchylenie
		Art. 45 - Wejście w życie
		Art. 46 - Adresaci
	ZAŁĄCZNIKI	**ZAŁĄCZNIK I** - SEKTORY KLUCZOWE
		ZAŁĄCZNIK II - SEKTORY WAŻNE
		ZAŁĄCZNIK III - TABELA KORELACJI

4. PRZEDMIOT DYREKTYWY NIS(2)

„1. Niniejszą dyrektywą ustanawia się środki mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego. W tym celu niniejsza dyrektywa określa:

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

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

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

d) obowiązki w zakresie nadzoru i egzekwowania przepisów spoczywające na państwach członkowskich.”[6]

5. ZAKRES DYREKTYWY NIS(2)

[6] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

„1. Niniejsza dyrektywa ma zastosowanie do podmiotów publicznych lub prywatnych w rodzaju tych, o których mowa w załączniku I lub II, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE lub które przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu oraz które świadczą usługi lub prowadzą działalność w Unii. (…)[7]

6. PODMIOTY KLUCZOWE I WAŻNE

„(15) Podmioty, które są objęte zakresem stosowania niniejszej dyrektywy w celu przestrzegania środków zarządzania ryzykiem w cyberbezpieczeństwie i obowiązków dotyczących zgłaszania incydentów, należy podzielić na dwie kategorie – podmioty kluczowe i podmioty ważne, w zależności od tego, jak bardzo ich znaczenie jest zasadnicze dla ich sektorów lub dla rodzaju świadczonych przez nie usług, a także od ich wielkości. W związku z tym właściwe organy powinny w stosownych przypadkach należycie uwzględniać odpowiednie sektorowe oszacowania ryzyka lub wskazówki. Należy zróżnicować systemy nadzoru i egzekwowania między tymi dwiema kategoriami podmiotów, aby zapewnić odpowiednią równowagę między wymogami i obowiązkami związanymi z ryzykiem a obciążeniem administracyjnym wynikającym z nadzoru nad zgodnością z przepisami.”[8]

„(18) W celu zapewnienia przejrzystego przeglądu podmiotów objętych zakresem stosowania niniejszej dyrektywy, państwa członkowskie powinny utworzyć wykaz podmiotów kluczowych i ważnych, a także podmiotów świadczących usługi rejestracji nazw domen. W tym celu państwa członkowskie powinny zobowiązać podmioty do przekazywania właściwym organom co najmniej następujących informacji: nazwy, adresu i aktualnych danych kontaktowych, w tym adresów poczty elektronicznej, zakresów adresów IP i numerów telefonicznych podmiotu oraz, w stosownych przypadkach, odpowiedniego sektora i podsektora, o których mowa w załącznikach, a także, w stosownych przypadkach, wykazu państw członkowskich, w których dany podmiot świadczy usługi objęte zakresem stosowania niniejszej dyrektywy. (…)”[9]

Podmioty kluczowe i ważne na podstawie artykułu 3:

„1. Do celów niniejszej dyrektywy następujące podmioty uznaje się za podmioty kluczowe:
a) podmioty w rodzaju tych, o których mowa w załączniku I, przekraczające pułapy dla średnich przedsiębiorstw, określone w art. 2 ust. 1 załącznika do zalecenia 2003/361/WE;
b) kwalifikowanych dostawców usług zaufania i rejestry nazw domen najwyższego poziomu, a także dostawców usług DNS, niezależnie od ich wielkości;
c) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE;
d) podmioty administracji publicznej, o których mowa w art. 2 ust. 2 lit. f) ppkt (i);
e) inne podmioty w rodzaju tych, o których mowa w załączniku I lub II, które zostały wskazane przez państwo członkowskie jako podmioty kluczowe zgodnie z art. 2 ust. 2 lit. b)–e);
f) podmioty wskazane jako podmioty krytyczne na podstawie dyrektywy (UE) 2022/2557, o których mowa w art. 2 ust. 3 niniejszej dyrektywy;

[7] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

[8] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

[9] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

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

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

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

4. W celu ustanowienia wykazu, o którym mowa w ust. 3, państwa członkowskie wymagają od podmiotów, o których mowa w tym ustępie, przedłożenia właściwym organom co najmniej następujących informacji:
a) nazwy podmiotu;
b) adresu i aktualnych danych kontaktowych, w tym adresów poczty elektronicznej, zakresów adresów IP i numerów telefonów;
c) w stosownych przypadkach, odpowiedniego sektora i podsektora, o których mowa w załączniku I lub II; oraz
d) w stosownych przypadkach, wykazu państw członkowskich, w których świadczą one usługi objęte zakresem stosowania niniejszej dyrektywy.

Podmioty, o których mowa w ust. 3, niezwłocznie powiadamiają o zmianach danych przedłożonych zgodnie z akapitem pierwszym niniejszego ustępu, a w każdym razie w terminie dwóch tygodni od dnia, w którym nastąpiła zmiana. Komisja, z pomocą Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), bez zbędnej zwłoki podaje wytyczne i wzory dokumentów związane z obowiązkami ustanowionymi w niniejszym ustępie. L 333/110 PL Dziennik Urzędowy Unii Europejskiej 27.12.2022 Państwa członkowskie mogą ustanowić krajowe mechanizmy umożliwiające podmiotom samodzielną rejestrację.

5. Do dnia 17 kwietnia 2025 r., a następnie co dwa lata właściwe organy powiadamiają:
a) Komisję i Grupę Współpracy o liczbie podmiotów kluczowych i ważnych wymienionych w wykazie zgodnie z ust. 3 dla każdego sektora i podsektora, o których mowa w załączniku I lub II; oraz
b) Komisję o istotnych informacjach na temat liczby podmiotów kluczowych i ważnych wskazanych na podstawie art. 2 ust. 2 lit. b)–e), sektora i podsektora, o których mowa w załączniku I lub II i do których podmioty te należą, rodzaju świadczonej przez nie usługi oraz przepisu spośród tych ustanowionych na podstawie art. 2 ust. 2 lit. b)–e), na podstawie którego zostały one wskazane.

6. Do dnia 17 kwietnia 2025 r. i na wniosek Komisji państwa członkowskie mogą zgłaszać Komisji nazwy podmiotów kluczowych i ważnych, o których mowa w ust. 5 lit. b).”[10]

[10] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

ZAŁĄCZNIK 1 – SEKTORY KLUCZOWE

(Źródło: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555)

ZAŁĄCZNIK I

SEKTORY KLUCZOWE

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

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

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

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

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

Arkanet
Bezpieczeństwo to my

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

(1) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/944 z dnia 5 czerwca 2019 r. w sprawie wspólnych zasad rynku wewnętrznego energii elektrycznej oraz zmieniająca dyrektywę 2012/27/UE (Dz.U. L 158 z 14.6.2019, s. 125).
(2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 z dnia 5 czerwca 2019 r. w sprawie rynku wewnętrznego energii elektrycznej (Dz.U. L 158 z 14.6.2019, s. 54).
(3) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/2001 z dnia 11 grudnia 2018 r. w sprawie promowania stosowania energii ze źródeł odnawialnych (Dz.U. L 328 z 21.12.2018, s. 82).
(4) Dyrektywa Rady 2009/119/WE z dnia 14 września 2009 r. nakładająca na państwa członkowskie obowiązek utrzymywania minimalnych zapasów ropy naftowej lub produktów ropopochodnych (Dz.U. L 265 z 9.10.2009, s. 9).
(5) Dyrektywa Parlamentu Europejskiego i Rady 2009/73/WE z dnia 13 lipca 2009 r. dotycząca wspólnych zasad rynku wewnętrznego gazu ziemnego i uchylająca dyrektywę 2003/55/WE (Dz.U. L 211 z 14.8.2009, s. 94).
(6) Dyrektywa Parlamentu Europejskiego i Rady 2009/12/WE z dnia 11 marca 2009 r. w sprawie opłat lotniskowych (Dz.U. L 70 z 14.3.2009, s. 11).
(7) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1315/2013 z dnia 11 grudnia 2013 r. w sprawie unijnych wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej i uchylające decyzję nr 661/2010/UE (Dz.U. L 348 z 20.12.2013, s. 1).
(8) Rozporządzenie (WE) nr 549/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające ramy tworzenia Jednolitej Europejskiej Przestrzeni Powietrznej (rozporządzenie ramowe) (Dz.U. L 96 z 31.3.2004, s. 1).
(9) Dyrektywa Parlamentu Europejskiego i Rady 2012/34/UE z dnia 21 listopada 2012 r. w sprawie utworzenia jednolitego europejskiego obszaru kolejowego (Dz.U. L 343 z 14.12.2012, s. 32).
(10) Rozporządzenie (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie wzmocnienia ochrony statków i obiektów portowych (Dz.U. L 129 z 29.4.2004, s. 6).
(11) Dyrektywa 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów (Dz.U. L 310 z 25.11.2005, s. 28).
(12) Dyrektywa 2002/59/WE Parlamentu Europejskiego i Rady z dnia 27 czerwca 2002 r. ustanawiająca wspólnotowy system monitorowania i informacji o ruchu statków i uchylająca dyrektywę Rady 93/75/EWG (Dz.U. L 208 z 5.8.2002, s. 10).
(13) Rozporządzenie delegowane Komisji (UE) 2015/962 z dnia 18 grudnia 2014 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2010/40/UE w odniesieniu do świadczenia ogólnounijnych usług informacyjnych w czasie rzeczywistym dotyczących ruchu (Dz.U. L 157 z 23.6.2015, s. 21).
(14) Dyrektywa Parlamentu Europejskiego i Rady 2010/40/UE z dnia 7 lipca 2010 r. w sprawie ram wdrażania inteligentnych systemów transportowych w obszarze transportu drogowego oraz interfejsów z innymi rodzajami transportu (Dz.U. L 207 z 6.8.2010, s. 1).
(15) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 176 z 27.6.2013, s. 1).
(16) Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.U. L 173 z 12.6.2014, s. 349).
(17) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz.U. L 201 z 27.7.2012, s. 1).
(18) Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.U. L 88 z 4.4.2011, s. 45).

(19) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylające decyzję nr 1082/2013/UE (Dz.U. L 314 z 6.12.2022, s. 26).
(20) Dyrektywa 2001/83/WE Parlamentu Europejskiego i Rady z dnia 6 listopada 2001 r. w sprawie wspólnotowego kodeksu odnoszącego się do produktów leczniczych stosowanych u ludzi (Dz.U. L 311 z 28.11.2001, s. 67).
(21) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/123 z dnia 25 stycznia 2022 r. w sprawie wzmocnienia roli Europejskiej Agencji Leków w zakresie gotowości na wypadek sytuacji kryzysowej i zarządzania kryzysowego w odniesieniu do produktów leczniczych i wyrobów medycznych (Dz.U. L 20 z 31.1.2022, s. 1).
(22) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2020/2184 z dnia 16 grudnia 2020 r. w sprawie jakości wody przeznaczonej do spożycia przez ludzi (Dz.U. L 435 z 23.12.2020, s. 1).
(23) Dyrektywa Rady 91/271/EWG z dnia 21 maja 1991 r. dotycząca oczyszczania ścieków komunalnych (Dz.U. L 135 z 30.5.1991, s. 40).

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

ZAŁĄCZNIK 2 – SEKTORY WAŻNE

(Źródło: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555)

ZAŁĄCZNIK II

SEKTORY WAŻNE

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

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

(1) Dyrektywa Parlamentu Europejskiego i Rady 2008/98/WE z dnia 19 listopada 2008 r. w sprawie odpadów oraz uchylająca niektóre dyrektywy (Dz.U. L 312 z 22.11.2008, s. 3).
(2) Rozporządzenie (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH), utworzenia Europejskiej Agencji Chemikaliów, zmieniające dyrektywę 1999/45/WE oraz uchylające rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE (Dz.U. L 396 z 30.12.2006, s. 1).
(3) Rozporządzenie (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności (Dz.U. L 31 z 1.2.2002, s. 1).
(4) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz.U. L 117 z 5.5.2017, s. 1).
(5) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz.U. L 117 z 5.5.2017, s. 176).

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

„Należy również pamiętać, że dyrektywy NIS 2 nie stosujemy do kilku grup podmiotów:

- podmiotów administracji publicznej prowadzących działalność w dziedzinach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa (w tym prewencji przestępstw, prowadzenia postępowań, wykrywania przestępstw i ich ścigania);
- określonych podmiotów, które prowadzą działania w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobiegania przestępstwom, prowadzenia postępowań w ich sprawie, wykrywania ich i ścigania, lub które świadczą usługi wyłącznie na rzecz podmiotów administracji publicznej, o których mowa w pkt. wyżej, które zostaną zwolnione przez państwa członkowskie z obowiązków ustanowionych w art. 21 lub 23 w odniesieniu do tych działań lub tych usług. Zwolniony podmiot nie podlega pod przepisy dotyczące nadzoru i egzekwowania przepisów (rozdział VII) w zakresie zwolnionej działalności. Jeżeli powyższa działalność jest jedyną, jaką prowadzi podmiot, może zostać zwolniony również z obowiązków wynikających z art. 3 i 27 (przekazanie danych w celach rejestracyjnych).

Na powyższych zasadach nie można jednak zwolnić z obowiązków dostawców usług zaufania. NIS2 nie stosuje się do podmiotów, które zostały zwolnione ze stosowania DORA, zgodnie z art. 2 ust. 4 tego aktu.

Prawodawca unijny przewidział, że w terminie do 27 miesięcy od dnia wejścia w życie NIS 2, państwa członkowskie ustanowią wykaz podmiotów kluczowych i ważnych, a także podmiotów świadczących usługi rejestracji nazw domen. W tym celu podmioty przekażą mu dane adresowe, kontaktowe, sektor i podsektor oraz wykaz państw członkowskich, w jakich świadczą usługi. Każda zmiana w tym zakresie będzie notyfikowana państwu członkowskiemu w terminie dwóch tygodni. Dyrektywa przewiduje również, że państwa członkowskie mogą ustanowić mechanizmy umożliwiające samodzielną rejestrację.

Liczba podmiotów kluczowych i ważnych w każdym sektorze i podsektorze będzie sprawozdawana Komisji i Grupie Współpracy, razem z istotnymi informacjami na temat tych podmiotów (sektor/podsektor, rodzaj świadczonej usługi, podstawa prawna wskazania za dany podmiot).”[11]

7. SKOORDYNOWANE RAMY W ZAKRESIE CYBERBEZPIECZEŃSTWA

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

(49) Polityka cyberhigieny stanowi podstawę pozwalającą chronić infrastrukturę sieci i systemów informatycznych, bezpieczeństwo sprzętu, oprogramowania i aplikacji internetowych oraz dane przedsiębiorstw lub użytkowników końcowych wykorzystywane przez podmioty. Polityka cyberhigieny obejmująca wspólny podstawowy zestaw praktyk – w tym aktualizacje oprogramowania i sprzętu, zmianę haseł, zarządzanie nowymi instalacjami, ograniczanie kont dostępu na poziomie administratora oraz tworzenie kopii zapasowych danych – umożliwia utworzenie proaktywnych ram gotowości oraz

[11] https://cyberpolicy.nask.pl/obowiazki-podmiotow-kluczowych-i-waznych-w-dyrektywie-nis2/

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

zapewnienie ogólnego bezpieczeństwa i ochrony w razie incydentów lub cyberzagrożeń. ENISA powinna monitorować i analizować politykę państw członkowskich dotyczącą cyberhigieny.

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

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

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

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

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

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

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

(56) W krajowych strategiach cyberbezpieczeństwa państwa członkowskie powinny uwzględniać szczególne potrzeby małych i średnich przedsiębiorstw związane z cyberbezpieczeństwem. W całej Unii małe i średnie przedsiębiorstwa stanowią znaczny odsetek rynku przemysłu oraz gospodarki i często mają trudności, by dostosować się do nowych praktyk biznesowych w coraz bardziej cyfrowym świecie i do środowiska cyfrowego, z pracownikami pracującymi z domów, a działalnością gospodarczą w coraz większym stopniu prowadzoną w internecie. Niektóre małe i średnie przedsiębiorstwa mierzą się ze szczególnymi wyzwaniami w zakresie cyberbezpieczeństwa, takimi jak niska świadomość zagadnień cyberbezpieczeństwa, brak zdalnych zabezpieczeń informatycznych, wysokie koszty rozwiązań dotyczących cyberbezpieczeństwa oraz zwiększony poziom zagrożeń, np. oprogramowanie wymuszające okup, w związku z czym powinny otrzymywać wskazówki i pomoc. Małe i średnie przedsiębiorstwa coraz częściej stają się celem ataków w łańcuchu dostaw ze względu na ich niewystarczający poziom zarządzania ryzykiem w cyberbezpieczeństwie i zarządzania w razie ataków oraz fakt, że mają one ograniczony dostęp do zasobów na potrzeby bezpieczeństwa. Takie ataki w łańcuchu dostaw wpływają nie tylko na małe i średnie przedsiębiorstwa i działalność każdego z nich z osobna, lecz także mogą mieć efekt kaskadowy w postaci większych ataków na zaopatrywane przez nie podmioty. Państwa członkowskie powinny, za pośrednictwem krajowych strategii cyberbezpieczeństwa, pomagać małym i średnim przedsiębiorstwom w reagowaniu na wyzwania dotyczące łańcuchów dostaw. Państwa członkowskie powinny posiadać punkt kontaktowy dla małych i średnich przedsiębiorstw na szczeblu krajowym lub regionalnym, który zapewniałby wskazówki i pomoc małym i średnim przedsiębiorstwom albo kierowałby je do właściwych organów udzielających wskazówek i pomocy w sprawach związanych z cyberbezpieczeństwem. Państwa członkowskie zachęca się również, aby oferowały usługi takie jak konfiguracja stron internetowych i funkcje logowania małym przedsiębiorstwom i mikroprzedsiębiorstwom, które nie posiadają tych zdolności.

(57) W ramach krajowych strategii cyberbezpieczeństwa będących częścią szerszej strategii obronnej państwa członkowskie powinny przyjąć politykę promowania aktywnej cyberobrony. W przeciwieństwie do działania reaktywnego aktywna cyberobrona polega na aktywnym zapobieganiu naruszeniom

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

bezpieczeństwa sieci, ich wykrywaniu, monitorowaniu, analizowaniu i ograniczaniu, w połączeniu z wykorzystaniem zdolności rozmieszczonych w sieci, która padła ofiarą ataku, i poza tą siecią. Może to obejmować bezpłatne usługi lub narzędzia, w tym kontrole samoobsługowe, narzędzia wykrywania i usługi usuwania oferowane przez państwa członkowskie niektórym podmiotom. Zdolność do szybkiego i automatycznego przekazywania i rozumienia informacji i analiz dotyczących zagrożeń, do ostrzegania o aktywności w cyberprzestrzeni i do reagowania ma krytyczne znaczenie dla spójności wysiłków na rzecz skutecznego zapobiegania atakom na sieci i systemy informatyczne, ich wykrywania, eliminowania i blokowania. Aktywna cyberobrona opiera się na strategii, która wyklucza środki ofensywne.

(58) Ponieważ wykorzystywanie podatności sieci i systemów informatycznych może powodować znaczące zakłócenia i szkody, ważnym czynnikiem w ograniczaniu ryzyka jest szybkie identyfikowanie takich podatności i ich eliminowanie. Podmioty, które opracowują takie sieci i systemy informatyczne lub administrują nimi, powinny zatem ustanowić odpowiednie procedury postępowania w przypadku wykrycia takich podatności. Ponieważ podatności często są wykrywane i ujawniane przez osoby trzecie, producent lub dostawca produktów ICT lub usług ICT również powinien wprowadzić niezbędne procedury regulujące odbieranie od osób trzecich informacji na temat podatności. W tym względzie normy międzynarodowe ISO/IEC 30111 i ISO/IEC 29147 zawierają wskazówki odnoszące się do postępowania w przypadku podatności i do ujawniania podatności. Wzmocnienie koordynacji między zgłaszającymi osobami fizycznymi i osobami prawnymi a producentami lub dostawcami produktów ICT lub usług ICT jest szczególnie ważne, aby usprawnić dobrowolne zasady ramowe dotyczące ujawniania podatności. Skoordynowane ujawnianie podatności to ustrukturyzowany proces, w ramach którego podatności są zgłaszane producentowi lub dostawcy potencjalnie podatnych produktów ICT lub usług ICT w sposób umożliwiający im zdiagnozowanie i wyeliminowanie danej podatności, zanim dotyczące jej szczegółowe informacje zostaną ujawnione osobom trzecim lub podane do wiadomości publicznej. Skoordynowane ujawnianie podatności powinno także obejmować koordynację między zgłaszającymi osobami fizycznymi lub osobami prawnymi a producentem lub dostawcą potencjalnie podatnych produktów ICT lub usług ICT w odniesieniu do harmonogramu eliminowania podatności i podawania ich do wiadomości publicznej.[12]

✓ ***Krajowa strategia cyberbezpieczeństwa***

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

Krajowa strategia cyberbezpieczeństwa zawiera:

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

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

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

[12] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

d) mechanizm służący określeniu istotnych zasobów i szacowanie ryzyka w tym państwie członkowskim;
e) wskazanie środków zapewniających gotowość na wypadek incydentów, zdolność reagowania na nie i przywracanie normalnego działania, z uwzględnieniem współpracy pomiędzy sektorami publicznym i prywatnym;
f) wykaz poszczególnych organów i zainteresowanych stron zaangażowanych we wdrażanie krajowej strategii cyberbezpieczeństwa;
g) ramy polityki na rzecz ściślejszej koordynacji między właściwymi organami na mocy niniejszej dyrektywy a właściwymi organami na mocy dyrektywy (UE) 2022/2557 do celu wymiany informacji na temat ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią oraz wykonywania zadań nadzorczych, stosownie do przypadku;
h) plan, zawierający kluczowe środki do podniesienia ogólnego poziomu wiedzy obywateli o cyberbezpieczeństwie.

2. W ramach krajowej strategii cyberbezpieczeństwa państwa członkowskie w szczególności przyjmują polityki:
a) dotyczące cyberbezpieczeństwa w łańcuchu dostaw produktów ICT i usług ICT wykorzystywanych przez podmioty do świadczenia usług;
b) dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT i usług ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa, szyfrowania oraz wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu;
c) dotyczące zarządzania podatnościami, obejmującą promowanie i ułatwianie skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1;
d) związane z utrzymywaniem ogólnej dostępności, integralności i poufności publicznego rdzenia otwartego internetu, w tym, w stosownych przypadkach, cyberbezpieczeństwa podmorskich kabli komunikacyjnych;
e) promującą rozwój i integrację odpowiednich zaawansowanych technologii służących wdrożeniu najnowocześniejszych środków zarządzania ryzykiem w cyberbezpieczeństwie;
f) promujące i rozwijające kształcenie i szkolenie w dziedzinie cyberbezpieczeństwa, umiejętności z zakresu cyberbezpieczeństwa, podnoszenia świadomości oraz inicjatyw badawczo-rozwojowych, a także wytyczne dotyczące dobrych praktyk i kontroli w zakresie cyberhigieny, skierowane do obywateli, zainteresowanych stron i podmiotów; 27.12.2022 PL Dziennik Urzędowy Unii Europejskiej L 333/115
g) wspierające instytucje akademickie i naukowe, w opracowywaniu, usprawnianiu i propagowaniu wprowadzania narzędzi z zakresu cyberbezpieczeństwa oraz bezpiecznej infrastruktury sieciowej;
h) obejmującą właściwe procedury oraz odpowiednie narzędzia służące wymianie informacji mające na celu wspieranie dobrowolnej wymiany informacji o cyberbezpieczeństwie między podmiotami zgodnie z prawem Unii;
i) wzmacniające podstawowy poziom cyberodporności i cyberhigieny małych i średnich przedsiębiorstw, w szczególności tych wyłączonych z zakresu stosowania niniejszej dyrektywy, poprzez zapewnienie łatwo dostępnych wytycznych i pomocy w zakresie ich szczególnych potrzeb;
j) propagujące aktywną cyberochronę.

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

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

4. Państwa członkowskie regularnie, co najmniej co pięć lat, przeprowadzają na podstawie kluczowych wskaźników skuteczności ocenę krajowych strategii cyberbezpieczeństwa i w razie potrzeby je aktualizują. ENISA pomaga państwom członkowskim, na ich wniosek, w opracowaniu lub aktualizacji krajowej strategii cyberbezpieczeństwa i kluczowych wskaźników skuteczności działania stosowanych do oceny tej strategii w celu dostosowania jej do wymogów i obowiązków ustanowionych w niniejszej dyrektywie."[13]

✓ ***Właściwe organy i pojedyncze punkty kontaktowe***

Zgodnie z artykułem 8 dyrektywy, każde państwo członkowskie wyznacza lub ustanawia co najmniej jeden właściwy organ odpowiedzialny za cyberbezpieczeństwo oraz za zadania nadzorcze. Ich zadaniem jest monitorowanie wdrażania niniejszej dyrektywy na poziomie krajowym. Każde państwo członkowskie wyznacza lub ustanawia także pojedynczy punkt kontaktowy, który pełni funkcję łącznikową w celu zapewnienia transgranicznej współpracy organów ze swojego państwa członkowskiego z odpowiednimi organami w innych państwach członkowskich, a w stosownym przypadku z Komisją i ENISA, a także w celu zapewnienia międzysektorowej współpracy z innymi właściwymi organami krajowymi w swoim państwie członkowskim.

✓ ***Krajowe ramy zarządzania kryzysowego w cyberbezpieczeństwie***

Zgodnie z artykułem 9 dyrektywy, każde państwo członkowskie wyznacza lub ustanawia co najmniej jeden właściwy organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę (organy ds. zarządzania kryzysowego w cyberbezpieczeństwie). Państwa członkowskie zapewniają tym organom odpowiednie zasoby, aby mogły one efektywnie i skutecznie wykonywać powierzone im zadania, zapewniają również spójność z istniejącymi ogólnymi krajowymi ramami zarządzania kryzysowego. Każde państwo członkowskie określa zdolności, zasoby i procedury, które można wykorzystać w razie sytuacji kryzysowej do celów niniejszej dyrektywy.

✓ ***Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)***

Zgodnie z artykułem 10 dyrektywy, każde państwo członkowskie wyznacza lub ustanawia co najmniej jeden CSIRT. CSIRT można wyznaczyć lub ustanowić w ramach właściwego organu. CSIRT spełniają wymogi określone w art. 11 ust. 1, obejmują co najmniej sektory, podsektory i rodzaje podmiotów, o których mowa w załącznikach I i II, i są odpowiedzialne za obsługę incydentów zgodnie z wyraźnie określoną procedurą.

Artykuł 11 dyrektywy zawiera „Wymogi dotyczące CSIRT, ich zdolności techniczne i zadania.

Więcej informacji o CSIRT znajduje się także na stronie: https://csirt.gov.pl/

„Zgłoszenie i obsługa incydentów przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV zostały określone w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2018 poz.1560)."[14]

[13] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

[14] https://csirt.gov.pl/cer/zgloszenie-incydentu/16,Zgloszenie-incydentu-do-CSIRT-GOV.html

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

8. WSPÓŁPRACA NA POZIOMIE UNIJNYM I MIĘDZYNARODOWYM

ROZDZIAŁ III dyrektywy opisuje współpracę na poziomie unijnym i międzynarodowym.
Obejmuje m. in. takie zagadnienia jak:
- Grupa Współpracy (Artykuł 14)
- Sieć CSIRT (Artykuł 15)
- Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) (Artykuł 16)
- Współpraca międzynarodowa (Artykuł 17)

✓ ***Sprawozdanie o stanie cyberbezpieczeństwa w Unii (Artykuł 18)***

„Co dwa lata ENISA przyjmuje we współpracy z Komisją i Grupą Współpracy sprawozdanie o stanie cyberbezpieczeństwa w Unii oraz przedkłada i przedstawia to sprawozdanie Parlamentowi Europejskiemu. (…)”[15]

✓ ***Oceny wzajemne (Artykuł 19)***

„Do 17 stycznia 2025 r. Grupa Współpracy ustala – z pomocą Komisji i ENISA oraz, w stosownych przypadkach, sieci CSIRT – metodykę i aspekty organizacyjne ocen wzajemnych, by wyciągać wnioski ze wspólnych doświadczeń, zwiększać wzajemne zaufanie, osiągnąć wysoki wspólny poziom cyberbezpieczeństwa, a także zwiększać kluczowe do wdrożenia niniejszej dyrektywy zdolności państw członkowskich w zakresie cyberbezpieczeństwa i doskonalić ich politykę w tej dziedzinie. Udział w ocenach wzajemnych jest dobrowolny. Oceny wzajemne przeprowadzą eksperci ds. cyberbezpieczeństwa. Ekspertów ds. cyberbezpieczeństwa wyznaczają co najmniej dwa państwa członkowskie inne niż państwo członkowskie poddawane ocenie. (…)”[16]

9. ŚRODKI ZARZĄDZANIA RYZYKIEM W CYBERBEZPIECZEŃSTWIE I OBOWIĄZKI DOTYCZACE ZŁASZANIA INCYDENTÓW

Rozdział IV dyrektywy opisuje środki zarządzania ryzykiem w cyberbezpieczeństwie i obowiązki dotyczące zgłaszania incydentów.

✓ ***Zarządzanie (Artykuł 20)***

„1. Państwa członkowskie zapewniają, aby organy zarządzające podmiotów kluczowych i ważnych zatwierdzały środkizarządzania ryzykiem w cyberbezpieczeństwie przyjęte przez te podmioty w celu zapewnienia zgodności z art. 21, nadzorowały ich wdrażanie i mogły być pociągnięte do odpowiedzialności za naruszanie przez te podmioty tego artykułu. Stosowanie niniejszego ustępu nie narusza przepisów krajowych dotyczących zasad odpowiedzialności instytucji publicznych oraz odpowiedzialności urzędników publicznych oraz urzędników wybranych lub mianowanych.

[15] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

[16] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

2. Państwa członkowskie zapewniają, aby członkowie organu zarządzającego podmiotów kluczowych i ważnych mieliobowiązek odbywać regularne szkolenia w celu zdobycia wystarczającej wiedzy i umiejętności pozwalających im rozpoznać ryzyko i ocenić praktyki zarządzania ryzykiem w cyberbezpieczeństwie oraz ich wpływ na usługi świadczone przez dany podmiot, a także zachęcają podmioty kluczowe i ważne do oferowania podobnych szkoleń ich pracownikom."[17]

✓ ***Środki zarządzania ryzykiem w cyberbezpieczeństwie (Artykuł 21)***

„1. Państwa członkowskie zapewniają, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu. Przy uwzględnieniu najnowszego stanu wiedzy oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, a także kosztów wdrożenia środki, o których mowa w akapicie pierwszym, zapewniają poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. Oceniając proporcjonalność tych środków, należycie uwzględnia się stopień narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze.

2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy:
a) politykę analizy ryzyka i bezpieczeństwa systemów informatycznych;
b) obsługę incydentu;
c) ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe;
d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;
e) bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;
f) polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;
g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;
h) polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;
i) bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;
j) w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.
(…)

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

[17] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform sieci społecznościowych i dostawców usług zaufania. Komisja może przyjąć akty wykonawcze określające wymogi techniczne i metodykę, a w razie potrzeby również wymogi sektorowe dotyczące środków, o których mowa w ust. 2, w odniesieniu do podmiotów kluczowych i ważnych innych niż te, o których mowa w akapicie pierwszym niniejszego ustępu.(…)"[18]

✓ ***Obowiązki w zakresie zgłaszania incydentów (Artykuł 23)***

„1. Każde państwo członkowskie zapewnia, aby podmioty kluczowe i ważne bez zbędnej zwłoki zgłaszały swojemu właściwemu CSIRT lub, jeżeli ma to zastosowanie, swojemu właściwemu organowi, zgodnie z ust. 4, incydent mający istotny wpływ na świadczenie przez nie usług, o którym mowa w ust. 3 (poważny incydent). W stosownych przypadkach dane podmioty bez zbędnej zwłoki powiadamiają odbiorców swoich usług o poważnych incydentach, które mogą mieć niekorzystny wpływ na świadczenie tych usług. Każde państwo członkowskie zapewnia, aby podmioty te zgłaszały m.in. informacje umożliwiające CSIRT lub, jeżeli ma to zastosowanie, właściwemu organowi ustalenie transgranicznego wpływu incydentu. Samo zgłoszenie nie nakłada na podmiot zgłaszający zwiększonej odpowiedzialności. Jeżeli dane podmioty zgłoszą poważny incydent właściwemu organowi na podstawie akapitu pierwszego, państwo członkowskie zapewnia, aby ten właściwy organ po otrzymaniu zgłoszenia przekazał je CSIRT. W razie wystąpienia transgranicznego lub międzysektorowego poważnego incydentu państwa członkowskie zapewniają, aby ich pojedyncze punkty kontaktowe w stosownym czasie otrzymały ważne informacje zgłoszone zgodnie z ust.4.

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

3. Incydent uznaje się za poważny, jeżeli:
a) spowodował lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu;
b) wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe.
4. Państwa członkowskie zapewniają, aby do celów zgłoszenia na podstawie ust. 1 dane podmioty przedkładały CSIRT lub, jeżeli ma to zastosowanie, właściwemu organowi:
a) bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia wiedzy o poważnym incydencie – wczesne ostrzeżenie, w którym w stosownych przypadkach wskazuje się, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze lub czy mógł wywrzeć wpływ transgraniczny;
b) bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od powzięcia wiedzy o poważnym incydencie – zgłoszenie incydentu, w stosownych przypadkach z aktualizacją informacji, o których mowa w lit. a), i wskazaniem wstępnej oceny poważnego incydentu, w tym jego dotkliwości i skutków, a w stosownych przypadkach także wskaźników integralności systemu;

[18] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

c) na wniosek CSIRT lub, jeżeli ma to zastosowanie, właściwego organu – sprawozdanie okresowe na temat odpowiednich aktualizacji statusu;
d) sprawozdanie końcowe nie później niż miesiąc po zgłoszeniu incydentu na podstawie lit. b), zawierające następujące elementy:

- szczegółowy opis incydentu, w tym jego dotkliwości i skutków;
- rodzaj zagrożenia lub pierwotną przyczynę, która prawdopodobnie była źródłem incydentu;
- zastosowane i wdrażane środki ograniczające ryzyko;
- w stosownych przypadkach transgraniczne skutki incydentu;
  (…)"[19]

✓ ***Stosowanie europejskich programów certyfikacji cyberbezpieczeństwa (Artykuł 24)***

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

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 38 w celu uzupełnienia niniejszej dyrektywy przez określenie, od których kategorii podmiotów kluczowych i ważnych należy wymagać stosowania certyfikowanych produktów ICT, usług ICT i procesów ICT lub uzyskania certyfikacji dla swoich własnych produktów ICT, usług ICT i procesów ICT na podstawie europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego zgodnie z art. 49 rozporządzenia (UE) 2019/881. Te akty delegowane przyjmuje się w razie stwierdzenia niewystarczających poziomów cyberbezpieczeństwa i określa się w nich termin wdrażania. Przed przyjęciem takich aktów delegowanych Komisja przeprowadza ocenę skutków i prowadzi konsultacje zgodnie z art. 56 rozporządzenia (UE) 2019/881.

3. Jeżeli do celów ust. 2 żaden z europejskich programów certyfikacji cyberbezpieczeństwa nie jest odpowiedni, Komisja może – po zasięgnięciu opinii Grupy Współpracy i Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa – zwrócić się do ENISA o przygotowanie propozycji programu zgodnie z art. 48 ust. 2 rozporządzenia (UE) 2019/881."[20]

Definicje (na podstawie art.6 dyrektywy):

- „produkt ICT" oznacza produkt ICT zdefiniowany w art. 2 pkt 12 rozporządzenia (UE) 2019/881;
- „usługa ICT" oznacza usługę ICT zdefiniowaną w art. 2 pkt 13 rozporządzenia (UE) 2019/881;
- „proces ICT" oznacza proces ICT zdefiniowany w art. 2 pkt 14 rozporządzenia (UE) 2019/881;
- „podatność" oznacza słabość, wrażliwość lub wadę produktów ICT lub usług ICT, które to cechy mogą zostać wykorzystane w wyniku cyberzagrożenia;

[19] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

[20] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

✓ ***Normalizacja (Artykuł 25)***

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

2. ENISA we współpracy z państwami członkowskimi i – w stosownych przypadkach – po zasięgnięciu opinii odpowiednich zainteresowanych stron opracowuje porady i wytyczne dotyczące obszarów technicznych, które należy wziąć pod uwagę w związku z ust.1, a także już istniejących norm, w tym norm krajowych, które pozwoliłyby uwzględnić te obszary."[21]

Definicje (na podstawie art.6 dyrektywy):

- „norma" oznacza normę zdefiniowaną w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 (29);
- „specyfikacja techniczna" oznacza specyfikację techniczną zdefiniowaną w art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012;

10. JURYSDYKCJA I REJESTRACJA

ROZDZIAŁ V dyrektywy dotyczy jurysdykcji i rejestracji.

✓ ***Jurysdykcja i terytorialność (Artykuł 26) – najważniejsze informacje w skrócie***

* Podmioty objęte zakresem stosowania niniejszej dyrektywy uznaje się za podlegające jurysdykcji państwa członkowskiego, w którym mają miejsce prowadzenia działalności, z pewnymi ujętymi w dyrektywie wyjątkami.
* Do celów niniejszej dyrektywy uznaje się, że podmiot ma swoje główne miejsce prowadzenia działalności w Unii w tym państwie członkowskim, w którym przeważnie podejmuje decyzje związane ze środkami zarządzania ryzykiem w cyberbezpieczeństwie.
* Jeżeli podmiot nie ma miejsca prowadzenia działalności w Unii, ale oferuje usługiw Unii, wyznacza przedstawiciela w Unii.
* Państwa członkowskie, które otrzymały wniosek o wzajemną pomoc w odniesieniu do podmiotu, o którym mowa w ust. 1 lit. b), mogą – nie wykraczając poza zakres tego wniosku – zastosować odpowiednie środki nadzoru i egzekwowania przepisów w odniesieniu do danego podmiotu świadczącego usługi lub mającego sieć i system informatyczny na ich terytorium.

✓ ***Rejestr podmiotów (Artykuł 27)***

„1. ENISA tworzy i prowadzi rejestr dostawców usługi DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, jak również

[21] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych, na podstawie informacji otrzymanych z pojedynczych punktów kontaktowych, zgodnie z ust. 4. Na wniosek ENISA zezwala właściwym organom na dostęp do rejestru, w stosownych przypadkach zapewniając jednocześnie gwarancje niezbędne do ochrony poufności informacji."[22]

Do 17 stycznia 2025 r. państwa członkowskie wymagają od podmiotów, oby przedłożyły właściwym organom takie informacje, jak m.in.:

- nazwę podmiotu;
- odpowiedni sektor, podsektor i rodzaj podmiotu;
- adres głównego miejsca prowadzenia działalności podmiotu oraz jego innych prawnych miejsc prowadzenia działalności w Unii;
- aktualne dane kontaktowe (adresy poczty elektronicznej, numery telefonów podmiotu);
- państwa członkowskie, w których podmiot świadczy usługi;
- zakresy IP podmiotu.

✓ ***Baza danych dotyczących rejestracji nazw domen (Artykuł 28)***

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

2. Do celów ust. 1 państwa członkowskie wymagają, by baza danych dotycząca rejestracji nazw domen zawierała informacje kluczowe do zidentyfikowania posiadaczy nazw domen i punktów kontaktowych zarządzających nazwami domen TLD oraz do skontaktowania się z nimi. Informacje te obejmują:
a) nazwę domeny;
b) datę rejestracji;
c) imię i nazwisko lub nazwę osoby rejestrującej oraz adres poczty elektronicznej i numer telefonu;
d) adres poczty elektronicznej i numer telefonu, pod którymi można skontaktować się z punktem kontaktowym zarządzającym nazwą domeny, w przypadku gdy różnią się od adresu poczty elektronicznej i numeru telefonu osoby rejestrującej.

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

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

5. Państwa członkowskie wymagają, by rejestry nazw TLD i podmioty świadczące usługi rejestracji nazw domen na zgodny z prawem i należycie uzasadniony wniosek o prawnie uzasadniony dostęp udzielały

[22] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

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

6. Wypełnianie obowiązków określonych w ust. 1–5 nie prowadzi do powielania gromadzenia danych dotyczących rejestracji nazw domen. W tym celu państwa członkowskie wymagają wzajemnej współpracy od rejestrów nazw TLD i podmiotów świadczących usługi rejestracji nazw domen."[23]

11. WYMIANA INFORMACJI

ROZDZIAŁ VI dyrektywy dotyczy wymiany informacji.

✓ ***Mechanizmy wymiany informacji na temat cyberbezpieczeństwa (Artykuł 29)***

„1. Państwa członkowskie zapewniają, aby podmioty objęte zakresem stosowania niniejszej dyrektywy, a w stosownych przypadkach również inne podmioty nieobjęte zakresem niniejszej dyrektywy mogły dobrowolnie wymieniać się odpowiednimi informacjami na temat cyberbezpieczeństwa, w tym informacjami o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacjami o grupach przestępczych, ostrzeżeniami dotyczącymi cyberbezpieczeństwa i zaleceniami dotyczącymi konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki, jeżeli wymiana takich informacji:
a) ma na celu zapobieganie incydentom, ich wykrywanie, reagowanie na nie, przywracanie normalnego działania po incydentach lub łagodzenie ich skutków;
b) zwiększa poziom cyberbezpieczeństwa, zwłaszcza przez podnoszenie świadomości na temat cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się cyberzagrożeń, wspieranie różnorodnych zdolności do obrony przed nimi, eliminowanie i ujawnianie podatności, techniki wykrywania zagrożeń, ograniczania ich zasięgu i zapobiegania im, strategie ograniczania ryzyka, etapy reagowania i przywracania normalnego działania lub sprzyjanie współpracy między podmiotami publicznymi i prywatnymi w badaniach nad cyberzagrożeniami.

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

3. Państwa członkowskie ułatwiają tworzenie mechanizmów wymiany informacji o cyberbezpieczeństwie, o których mowa w ust. 2 niniejszego artykułu. W mechanizmach tych można określić elementy operacyjne, w tym korzystanie ze specjalnych platform ICT i narzędzi automatyzacji, a także treści i warunki funkcjonowania mechanizmów wymiany informacji. Określając szczegóły udziału organów publicznych w tych mechanizmach, państwa członkowskie mogą ustalać warunki udostępniania informacji

[23] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

przez właściwe organy lub CSIRT. Państwa członkowskie oferują pomoc w stosowaniu takich mechanizmów zgodnie ze swoją polityką, o której mowa w art. 7 ust. 2 lit. h).

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

5. ENISA pomaga w tworzeniu mechanizmów wymiany informacji na temat cyberbezpieczeństwa, o których mowa w ust. 2, przez wymianę najlepszych praktyk i udzielanie wskazówek."[24]

Definicje (na podstawie art.6 dyrektywy):

- „system nazw domen" lub „DNS" oznacza hierarchiczny rozproszony system nazw, który umożliwia identyfikację usług i zasobów internetowych, pozwalając urządzeniom użytkowników końcowych na korzystanie z usług routingu internetowego i usług łączności w celu dotarcia do tych usług i zasobów;
- „dostawca usług DNS" oznacza podmiot świadczący:
  a) dostępne publicznie rekurencyjne usługi rozpoznawania nazw domen na rzecz użytkowników końcowych internetu; lub
  b) autorytatywne usługi rozpoznawania nazw domen do użytku osób trzecich, z wyjątkiem głównych serwerów nazw;
- „rejestr nazw domen najwyższego poziomu" lub „rejestr nazw TLD" oznacza podmiot, któremu powierzono konkretną domenę najwyższego poziomu (TLD) i który odpowiada za zarządzanie nią, w tym za rejestrację nazw domen w ramach TLD oraz za jej techniczne funkcjonowanie, w tym za obsługę jej serwerów nazw, utrzymanie jej baz danych oraz dystrybucję plików strefowych TLD we wszystkich serwerach nazw, bez względu na to, czy którekolwiek z tych działań jest wykonywane przez sam podmiot czy zlecane na zewnątrz, ale z wyłączeniem sytuacji, w których rejestr wykorzystuje nazwy TDL wyłącznie do własnego użytku;
- „podmiot świadczący usługi rejestracji nazw domen" oznacza rejestratora lub agenta działającego w imieniu rejestratorów, np. dostawcę lub odsprzedawcę usług w zakresie rejestracji prywatności lub serwerów proxy;
- „usługa cyfrowa" oznacza usługę zdefiniowaną w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady

∗ Dobrowolne zgłaszanie ważnych informacji (Artykuł 30)

12. NADZÓR I EGZEKWOWANIE PRZEPISÓW

ROZDZIAŁ VII dyrektywy dotyczy nadzoru i egzekwowania przepisów.

✓ ***Ogólne aspekty nadzoru i egzekwowania przepisów (Artykuł 31)***

Najważniejsze informacje:

[24] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

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

* Państwa członkowskie mogą zezwolić ich właściwym organom na wprowadzenie hierarchii priorytetów w odniesieniu do zadań nadzorczych. Taka hierarchia priorytetów bazuje na podejściu uwzględniającym analizę ryzyka.

* Państwa członkowskie zapewniają, aby nadzorując przestrzeganie niniejszej dyrektywy przez podmioty administracji publicznej oraz nakładając środki egzekwowania przepisów w odniesieniu do naruszeń niniejszej dyrektywy, właściwe organy posiadały odpowiednie uprawnienia do podejmowania takich zadań w sposób niezależny pod względem operacyjnym wobec nadzorowanych podmiotów administracji publicznej.

* Państwa członkowskie mogą podjąć decyzję o nałożeniu na te podmioty odpowiednich, proporcjonalnych i skutecznych środków nadzoru i egzekwowania przepisów zgodnie z krajowymi ramami ustawodawczymi i instytucjonalnymi.

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

✓ ***Środki nadzoru i egzekwowania przepisów dla podmiotów kluczowych (Artykuł 32)***

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

2. Państwa członkowskie zapewniają, by wykonując uprawnienia nadzorcze wobec podmiotów kluczowych, właściwe organy były uprawnione do objęcia tych podmiotów co najmniej:
a) kontrolami na miejscu i nadzorem zdalnym, w tym wyrywkowymi kontrolami prowadzonymi przez przeszkolonych specjalistów;
b) regularnymi ukierunkowanymi audytami bezpieczeństwa prowadzonymi przez niezależną instytucję lub właściwy organ;
c) audytami doraźnymi, w tym w uzasadnionych przypadkach w związku z wystąpieniem poważnego incydentu lub z naruszeniem niniejszej dyrektywy przez podmiot kluczowy;
d) skanami bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów szacowania ryzyka, w razie potrzeby we współpracy z danym podmiotem;
e) wnioskami o udzielenie informacji niezbędnych do oceny środków zarządzania ryzykiem w cyberbezpieczeństwie przyjętych przez dany podmiot, w tym udokumentowanej polityki cyberbezpieczeństwa, a także zgodności z obowiązkiem przedkładania informacji właściwym organom zgodnie z art. 27;
f) wnioskami o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania ich zadań nadzorczych;
g) wnioskami o przedstawienie dowodów realizacji polityki cyberbezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora oraz odpowiednie dowody.

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

Ukierunkowane audyty bezpieczeństwa, o których mowa w akapicie pierwszym lit. b), opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot bądź na innych dostępnych informacjach dotyczących ryzyka. Wyniki ukierunkowanych audytów bezpieczeństwa udostępnia się właściwemu organowi. Koszty takiego ukierunkowanego audytu bezpieczeństwa prowadzonego przez niezależną instytucję pokrywa podmiot poddawany audytowi, z wyjątkiem należycie uzasadnionych przypadków, gdy właściwy organ postanowi inaczej.

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

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

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

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

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

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

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

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

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

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

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

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

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

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

b) zwrócenia się do właściwych instytucji lub sądów, zgodnie z prawem krajowym, o nałożenie tymczasowego zakazu pełnienia funkcji zarządczych w tym podmiocie kluczowym na osobę fizyczną wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela prawnego w tym podmiocie. Tymczasowe zawieszenie lub zakaz pełnienia funkcji na podstawie niniejszego ustępu stosuje się tylko do czasu, gdy dany podmiot podejmie działania niezbędne do usunięcia uchybień lub spełnienia wymogów właściwego organu, w związku z którymi nałożono na niego środki egzekwowania przepisów. Takie tymczasowe zawieszenie lub zakaz stosuje się z zastrzeżeniem odpowiednich gwarancji proceduralnych zgodnych z ogólnymi zasadami prawa Unii i z Kartą, w tym prawa do skutecznej ochrony prawnej i do rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony. Środki egzekwowania przepisów określone w niniejszym ustępie nie mają zastosowania do podmiotów administracji publicznej objętych zakresem niniejszej dyrektywy.

6. Państwa członkowskie zapewniają, aby każda osoba fizyczna odpowiedzialna za podmiot kluczowy lub działająca w charakterze przedstawiciela prawnego tego podmiotu na podstawie uprawnienia do jego reprezentowania, podejmowania decyzji w jego imieniu lub sprawowania nad nim kontroli była uprawniona do zapewnienia przestrzegania przez ten podmiot niniejszej dyrektywy. Państwa członkowskie zapewniają, by te osoby fizyczne mogły być pociągnięte do odpowiedzialności za niewywiązanie się z obowiązku zapewnienia przestrzegania niniejszej dyrektywy. W odniesieniu do podmiotów administracji publicznej niniejszy ustęp pozostaje bez uszczerbku dla przepisów krajowych dotyczących odpowiedzialności urzędników publicznych oraz osób pełniących funkcję z wyboru lub powołania.

7. Przyjmując środki egzekwowania przepisów, o których mowa w ust. 4 lub 5, właściwe organy przestrzegają prawa doobrony oraz biorą pod uwagę okoliczności każdego indywidualnego przypadku i należycie uwzględniają co najmniej:
a) wagę naruszenia i znaczenie naruszonych przepisów, przy czym za poważne należy uznać w każdym przypadku m.in. następujące naruszenia:
(I) powtarzające się naruszenia;
(II) niezgłoszenie lub nieusunięcie poważnych incydentów;
(III) nieusunięcie uchybień zgodnie z wiążącymi nakazami właściwych organów;
(IV) utrudnianie prowadzenia audytów lub działań monitorujących nakazanych przez właściwy organ po stwierdzeniu naruszenia;
(V) dostarczanie nieprawdziwych lub rażąco niedokładnych informacji w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków zgłaszania incydentów ustanowionych w art. 21 i 23;
b) czas trwania naruszenia;
c) istotne wcześniejsze naruszenia ze strony danego podmiotu;
d) spowodowane szkody majątkowe i niemajątkowe, w tym straty finansowe lub gospodarcze, wpływ na inne usługi i liczbę użytkowników, których dotyka incydent;
e) umyślny lub nieumyślny charakter czynu ze strony sprawcy naruszenia;
f) środki zastosowane przez podmiot, aby zapobiec szkodom majątkowym i niemajątkowym lub je ograniczyć;
g) stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji;
h) stopień współpracy odpowiedzialnych osób fizycznych lub prawnych z właściwymi organami.

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

8. Właściwe organy przedstawiają szczegółowe uzasadnienie zastosowanych środków z zakresu egzekwowania przepisów. Zanim zastosują takie środki, właściwe organy powiadamiają dane podmioty o swoich wstępnych ustaleniach. Dają im one też rozsądny czas na przedstawienie uwag, z wyjątkiem należycie uzasadnionych przypadków, gdy utrudniłoby to natychmiastowe działanie w celu zapobieżenia incydentom lub reakcji na nie.(…)"[25]

✓ ***Środki nadzoru i egzekwowania przepisów dla podmiotów ważnych (Artykuł 33)***

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

2. Państwa członkowskie zapewniają, by wykonując zadania nadzorcze wobec podmiotów ważnych, właściwe organy były uprawnione do objęcia tych podmiotów co najmniej:
a) kontrolami na miejscu i nadzorem zdalnym *ex post* prowadzonymi przez przeszkolonych specjalistów;
b) ukierunkowanymi audytami bezpieczeństwa prowadzonymi przez niezależną instytucję lub właściwy organ;
c) skanami bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów szacowania ryzyka, w razie potrzeby we współpracy z danym podmiotem;
d) wnioskami o udzielenie informacji niezbędnych do oceny *ex post* środków zarządzania ryzykiem w cyberbezpieczeństwie przyjętych przez dany podmiot, w tym udokumentowanej polityki Cyberbezpieczeństwa, a także wypełnienia obowiązku przedłożenia informacji właściwym organom zgodnie z art. 27;
e) wnioskami o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania ich zadań nadzorczych;
f) wnioskami o przedstawienie dowodów realizacji polityki cyberbezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora oraz odpowiednie dowody. Ukierunkowane audyty bezpieczeństwa, o których mowa w akapicie pierwszym lit. b), opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot bądź na innych dostępnych informacjach o ryzyku. Wyniki ukierunkowanych audytów bezpieczeństwa udostępnia się właściwemu organowi. Koszty takiego ukierunkowanego audytu bezpieczeństwa prowadzonego przez niezależną instytucję pokrywa podmiot poddany audytowi, z wyjątkiem należycie uzasadnionych przypadków, gdy właściwy organ postanowi inaczej.

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

4. Państwa członkowskie zapewniają, by wykonując uprawnienia w zakresie egzekwowania przepisów wobec podmiotów ważnych, właściwe organy były uprawnione co najmniej do:
a) wydawania ostrzeżeń dotyczących naruszania przez dane podmioty niniejszej dyrektywy;
b) przyjmowania wiążących poleceń lub nakazów zobowiązujących dane podmioty do naprawienia stwierdzonych uchybień lub usunięcia naruszenia niniejszej dyrektywy;

[25] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

c) nakazania danym podmiotom, by zaniechały postępowania, które narusza niniejszą dyrektywę i nie powtarzały tego postępowania;
d) nakazania danym podmiotom, by w określony sposób i w określonym terminie zapewniły zgodność swoich środków zarządzania ryzykiem w cyberbezpieczeństwie z art. 21 lub wypełniły obowiązki zgłaszania incydentów określone w art. 23;
e) nakazania danym podmiotom, by poinformowały osoby fizyczne lub prawne, w odniesieniu do których świadczą usługi lub prowadzą działania, a których potencjalnie dotyczy poważne cyberzagrożenie, o charakterze tego zagrożenia, a także o możliwych środkach ochronnych lub naprawczych, jakie te osoby fizyczne lub prawne mogą zastosować w reakcji na to zagrożenie;
f) nakazania danym podmiotom, by w rozsądnym terminie wdrożyły zalecenia wydane w wyniku audytu bezpieczeństwa;
g) nakazania danym podmiotom, by w określony sposób podały do wiadomości publicznej informacje o naruszeniach przez nie niniejszej dyrektywy;
h) zastosowania lub zwrócenia się o zastosowanie przez właściwe organy lub sądy, zgodnie z prawem krajowym, administracyjnej kary pieniężnej na podstawie art. 34 oprócz środków, o których mowa w lit. a)–g) niniejszego ustępu.
5. Art. 32 ust. 6, 7 i 8 stosuje się odpowiednio do środków nadzoru i egzekwowania przepisów określonych w niniejszym artykule w odniesieniu do podmiotów ważnych.
6. Państwa członkowskie zapewniają, by ich właściwe organy zgodnie z niniejszą dyrektywą współpracowały z odpowiednimi właściwymi organami zainteresowanego państwa członkowskiego zgodnie z rozporządzeniem (UE) 2022/2554. W szczególności państwa członkowskie zapewniają, by ich właściwe organy na mocy niniejszej dyrektywy informowały forum nadzoru, ustanowione zgodnie z art. 32 ust. 1 rozporządzenia (UE) 2022/2554, gdy wykonują uprawnienia w zakresie nadzoru i egzekwowania przepisów, by zapewnić przestrzeganie niniejszej dyrektywy przez podmiot ważny, wyznaczony jako kluczowy dostawca usług ICT będący osobą trzecią zgodnie z art. 31 rozporządzenia (UE) 2022/2554."[26]

- ✓ ***Ogólne warunki nakładania administracyjnych kar pieniężnych na podmioty kluczowe i ważne (Artykuł 34)***

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

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

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

4. Państwa członkowskie zapewniają, by podmioty kluczowe dokonujące naruszeń art. 21 lub 23 podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej 10 000 000 EUR lub co najmniej 2 % łącznego rocznego światowego obrotu w

[26] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot kluczowy, przy czym zastosowanie ma kwota wyższa.

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

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

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

8. Jeżeli system prawny danego państwa członkowskiego nie przewiduje administracyjnych kar pieniężnych, to państwo członkowskie zapewnia takie stosowanie niniejszego artykułu, by o nałożenie kary pieniężnej wnosił właściwy organ, a nakładał ją właściwy sąd krajowy, przy zapewnieniu skuteczności tych rozwiązań prawnych i równoważności ich skutku względem administracyjnej kary pieniężnej nakładanej przez właściwe organy. W każdym przypadku nakładane kary pieniężne muszą być skuteczne, proporcjonalne i odstraszające. Do dnia 17 października 2024 r. państwo członkowskie powiadamia Komisję o przepisach, które przyjęło zgodnie z niniejszym ustępem, oraz niezwłocznie powiadamia o późniejszych przepisach zmieniających lub zmianach mających na nie wpływ."[27]

Naruszenia pociągające za sobą naruszenie ochrony danych osobowych (Artykuł 35)

- ✓ ***Kary (Artykuł 36)***

„Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń przepisów i środków krajowych przyjętych na podstawie niniejszej dyrektywy i wprowadzają wszelkie środki niezbędne do zapewnieniawykonywania tych sankcji. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie najpóźniej do dnia 17 stycznia 2025 r. powiadamiają Komisję o tych przepisach i środkach, a następnie niezwłocznie powiadamiają ją o zmianach mających na nie wpływ."[28]

- ✓ ***Wzajemna pomoc (Artykuł 37)***

„1. Jeżeli podmiot świadczy usługi w więcej niż jednym państwie członkowskim lub świadczy usługi w co najmniej jednym państwie członkowskim, a jego sieć i systemy informatyczne są zlokalizowane w co najmniej jednym innym państwie członkowskim, właściwe organy zainteresowanych państw członkowskich współpracują ze sobą i udzielają sobie wzajemnie pomocy, odpowiednio do potrzeb. (…)"[29]

[27] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

[28] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

[29] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl

13. PRZEPISY KOŃCOWE

Najważniejsze informacje:

* Do dnia 17 października 2027 r., a następnie co 36 miesięcy Komisja przeprowadza przegląd funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu Radzie sprawozdanie na ten temat.
* Do dnia 17 października 2024 r. państwa członkowskie przyjmują i publikują przepisy niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają one o tym Komisję. Państwa członkowskie stosują te przepisy od dnia 18 października 2024 r.
* Dyrektywa (UE) 2016/1148 (NIS1) traci moc ze skutkiem od dnia 18 października 2024 r.
* Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.
* Niniejsza dyrektywa skierowana jest do państw członkowskich.

ARKANET Wojciech Oleś Stanisław Zygor Spółka Jawna
ul. Porcelanowa 19, 40-246 Katowice
Tel: +48 327821400
biuro@arkanet.pl
www.arkanet.pl