Cybersecurity and Law

2026 Nr 1(15)

DOI: 10.35467/cal/221059

DORA jako regulacja sektorowa w rozumieniu dyrektywy NIS2

DORA as a sectoral regulation within the meaning of the NIS2 directive

Paweł PELC
Kancelaria Radcy Prawnego Pawła Pelca, Warszawa
ORCID: 0000-0002-5007-568X
E-mail: pawel.pelc@kancelariapelc.com

Streszczenie

Dyrektywa NIS2 przewiduje możliwość stosowania zamiast jej regulacji – regulacji sektorowych aktów prawnych Unii Europejskiej jeśli wymagają one od podmiotów kluczowych lub ważnych przyjęcia środków zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania poważnych incydentów i w przypadku gdy wymogi te są co najmniej równoważne pod względem skutku obowiązkom określonym w dyrektywnie NIS2. Komisja Europejska wydała komunikat, w których uznała, że DORA jest sektorowym aktem Unii w stosunku do podmiotów finansowych będących podmiotami kluczowymi lub ważnymi. W związku z powyższym zamiast przepisów dyrektywy NIS2 zastosowanie powinny mieć przepisy DORA dotyczące zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (ICT). Zdaniem Komisji Europejskiej do podmiotów finansowych objętych DORA państwa członkowskie nie powinny zatem stosować przepisów dyrektywy NIS2 dotyczących zarządzania ryzykiem w cyberbezpieczeństwie i obowiązków w zakresie zgłaszania incydentów oraz nadzoru i egzekwowania przepisów. Jest to zgodne także z regulacją DORA oraz motywami preambuł zarówno DORA jak i NIS2. Należy uznać, że ustawodawca europejski uznał jednoznacznie, że w stosunku do podmiotów finansowych, do których stosuje się DORA, nie ma zastosowania NIS2.

Słowa kluczowe

DORA, NIS2, cyberbezpieczeństwo, instytucje finansowe, podmioty finansowe

Abstract

The NIS2 Directive provides for the possibility of using instead of its regulation – regulations of sectoral legal acts of the European Union if they require key or important entities to adopt cybersecurity risk management measures or report serious incidents and where these requirements are at least equivalent in effect to the obligations set out in the NIS2 Directive. The European Commission issued a communication recognizing

that DORA is a sectoral act of the Union for financial entities that are key or important entities. Therefore, instead of the provisions of the NIS2 Directive, the provisions of the DORA on information and communication technology (ICT) risk management (Articles 6 et seq.), ICT incident management and, in particular, reporting serious ICT incidents According to the European Commission, Member States should therefore not apply the provisions of the NIS2 Directive on cybersecurity risk management and incident reporting, surveillance and enforcement obligations to financial entities covered by the DORA. This is also in line with the DORA regulation and the preamble recitals of both DORA and NIS2. It should be considered that the European legislator has clearly recognized that NIS2 does not apply to financial entities to which DORA applies.

Keywords
DORA, NIS2, Cybersecurity, financial institutions, financial entities

Wprowadzenie

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)[1] w art. 4 wskazuje, że w przypadku, gdy na podstawie sektorowych aktów prawnych Unii Europejskiej (UE) wymaga się od podmiotów kluczowych lub ważnych przyjęcia środków zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania poważnych incydentów i w przypadku, gdy wymogi te są co najmniej równoważne pod względem skutku obowiązkom określonym w dyrektywie NIS2, nie stosuje się do takich podmiotów odpowiednich przepisów dyrektywy NIS2, w tym przepisów dotyczących nadzoru i egzekwowania przepisów określonych w rozdziale VII dyrektywy NIS2. Jeżeli sektorowe akty prawne UE nie obejmują wszystkich podmiotów w konkretnym sektorze, objętych zakresem stosowania niniejszej dyrektywy, odpowiednie przepisy niniejszej dyrektywy nadal mają zastosowanie do podmiotów nieobjętych tymi sektorowymi aktami prawnymi UE. Zgodnie z tą regulacją, wymogi uznaje się za równoważne pod względem skutku obowiązkom określonym w dyrektywie NIS2, jeżeli środki zarządzania ryzykiem w cyberbezpieczeństwie są co najmniej równoważne pod względem skutku środkom określonym w art. 21 ust. 1 i 2 dyrektywy NIS2, lub jeżeli sektorowy akt prawny UE przewiduje natychmiastowy dostęp CSIRT, właściwych organów lub pojedynczych punktów kontaktowych na mocy niniejszej dyrektywy do zgłoszeń incydentów.

W związku z powyższym przedmiotem niniejszego tekstu jest przeprowadzenie analizy, czy regulacja dotycząca operacyjnej odporności cyfrowej sektora finansowego może być uznana za akt sektorowy w rozumieniu art. 4 dyrektywy NIS2. Ze względu na charakter powyższych rozważań podstawową metodą badawczą jest metoda dogmatyczno-prawna, gdyż w celu przeprowadzenia analizy w tym zakresie niezbędna jest przede wszystkim wykładania regulacji i wzajemnych relacji między tymi aktami prawnymi oraz opisanego dalej komunikatu Komisji Europejskiej (KE) wydanego na podstawie art. 4 ust. 3 dyrektywy NIS2. W procesie tym istotne znacznie będzie miało także wykorzystanie motywów do preambuł obu wskazanych wyżej aktów prawa unijnego. Temat jest ważki ze względu na rolę cyberbezpieczeństwa w funkcjonowaniu współczesnych społeczeństw i konieczność stworzenia przez państwa członkowskie UE z jednej

[1] Dz. U. UE z 2022 r. nr 333 s. 80.

strony spójnych krajowych systemów cyberbezpieczeństwa, a z drugiej strony spójnego systemu cyberbezpieczeństwa na poziomie UE. Działania te muszą jednak uwzględniać także dostępne zasoby i unikać dublowania regulacji służących osiąganiu tych samych celów[2].

Komunikat Komisji Europejskiej z art. 4 Dyrektywy NIS2

Na podstawie art. 4 ust. 3 dyrektywy NIS2 KE była obowiązana do podania wytycznych wyjaśniających stosowanie tych regulacji. Ponadto jest ona obowiązana do dokonywania regularnego przeglądu tych wytycznych. Na podstawie tego upoważnienia wydany został Komunikat Komisji Europejskiej w sprawie Wytycznych dotyczących stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS 2)[3]. W komunikacie tym potwierdzono pierwszeństwo stosowania do podmiotów kluczowych lub ważnych - sektorowych aktów prawnych wymagających przyjecia przez nie środków zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania incydentów co najmniej równoważnych pod względem skutku obowiązkom określonym w dyrektywie NIS 2.[4] W ocenie KE z art. 21 ust. 1 akapit pierwszy dyrektywy NIS2 wynika obowiązek zapewnienia przez państwa członkowskie wprowadzenia przez podmioty kluczowe i ważne odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług[5] Zdaniem KE przy ocenie równoważności należy zwrócić szczególną uwagę na to, czy obowiązki w zakresie bezpieczeństwa przewidziane w danym akcie prawnym obejmują środki zapewniające bezpieczeństwo sieci i systemów informatycznych w rozumieniu art. 6 pkt 2 dyrektywy NIS 2. Środki bezpieczeństwa, których wprowadzenia wymaga sektorowy akt prawny UE, powinny również obejmować sprzęt, oprogramowanie układowe i oprogramowanie komputerowe wykorzystywane w działalności podmiotu.[6] Kolejnym kryterium oceny równoważności w zakresie art. 21 ust. 1 i 2 dyrektywy NIS2 określonym przez KE, jest wymóg, by środki zarządzania ryzykiem w cyberbezpieczeństwie opierały się na podejściu uwzględniającym wszystkie zagrożenia, które mogą mieć różne źródła potencjalnie prowadzące do incydentu. Środki zarządzania ryzykiem w cyberbezpieczeństwie stosowane przez podmiot powinny służyć ochronie nie tylko sieci i systemów informatycznych podmiotu, ale także środowiska fizycznego tych systemów przed jakimkolwiek zdarzeniem, takim

[2] Zob. D. Tylawa, Cyberbezpieczeństwo a globalne prawo adminsitracyjne [w:] M. Karpiuk (red.), Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe, Warszawa 2024, s. 45-46; C. Banasiński, Podstawowe pojęcia i podstawy prawne cyberbezpieczeństwa [w:] C. Banasiński (red.), Cyberbezpieczeństwo. Zarys wykładu, Warszawa 2023, s. 31-37; K. Mączka, Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji, „Ochrona Ludności i Dziedzictwa Kulturowego" 2024, nr 5, s. 111-124; B. Głowacki, D. Grzybowska-Ganszczyk, Dyrektywa NIS2 jako narzędzie wzmacniania bezpieczeństwa lokalnego i narodowego w obszarze cyberzagrożeń, dot.pl 2025, nr 1, s. 82-83; D. Skoczylas, Dyrektywa NIS 2 a cyberbezpieczeństwa administracji publicznej, „Dyskurs Prawniczy i Administracyjny" 2025, nr 1, s. 229; T. Zawadzki, Analiza wpływu regulacji na zagrożenia w cyberprzestrzeni, „Cybersecurity and Law" 2025, nr 2, s. 93-109; Ch. Gaie, M. Karpiuk, N. Strizzolo, Cybersecurity of Public Sector Institutions, „Prawo i Więź" 2024, nr 6, s. 347-362; M. Karpiuk, The Legal Status of Digital Service Providers in the Sphere of Cybersecurity, „Studia Iuridica Lublinensia" 2023, nr 2, s. 189-201.

[3] Dz. U. UE z 2023 r. nr 328 s. 2.

[4] Tamże, pkt 5.

[5] Tamże, pkt 7.

[6] Tamże pkt 8.

jak np. sabotaż czy kradzież[7]. Ponadto w zakresie równoważności z wymogami art. 21 ust. 2 dyrektywy NIS 2 środki zarządzania ryzykiem w cyberbezpieczeństwie muszą również obejmować szczególne wymogi w zakresie bezpieczeństwa obejmujące: politykę analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługę incydentu, ciągłość działania, zarządzanie kryzysowe, bezpieczeństwo łańcucha dostaw. Komunikat wskazuje także na akty delegowane KE w tym zakresie.[8] KE dokonała także interpretacji w zakresie równoważności wymogów dotyczących zgłaszania incydentów określonych w art. 4 ust. 2 lit. b dyrektywy NIS 2 i uznała je za równoważne pod względem skutku obowiązkom określonym w tej dyrektywie, jeżeli sektorowy akt prawny UE przewiduje natychmiastowy dostęp CSIRT, właściwych organów lub pojedynczych punktów kontaktowych do zgłoszeń incydentów[9] KE wskazała na konieczność równoważności pod względem skutku, co najmniej z wymogami art. 23 ust. 106 dyrektywy NIS 2, w tym w zakresie rodzajów incydentów, podmiotu któremu należy zgłaszać incydent oraz terminów zgłaszania tych incydentów.[10] KE zwróciła także uwagę na określony w art. 23 ust. 1 dyrektywy NIS 2 obowiązek zgłaszania przez podmioty kluczowe i ważne właściwemu CSIRT lub swojemu właściwemu organowi każdego poważnego incydentu oraz powiadamiania w stosownych przypadkach bez zbędnej zwłoki odbiorców ich usług[11]. W ocenie KE, incydent jest poważny, jeżeli spowodował lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu lub wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe[12]. Powołując się na motyw 101 preambuły do dyrektywy NIS 2, KE wskazała w swoim komunikacie także na konieczność zgłaszania incydentów na podstawie wstępnej oceny dokonanej przez podmiot, którego dotyczy incydent[13]. KE odniosła się także do przewidzianego w NIS 2 wieloetapowego podejścia do zgłaszania poważnych incydentów, celu tego podejścia, jak również do terminów[14].

KE, powołując się na art. 4 ust. 2 lit. b dyrektywy NIS 2, uznała, że aby sektorowy akt prawny Unii miał zastosowanie do wymogów w zakresie zgłaszania incydentów zamiast tej dyrektywy, musi on zapewniać CSIRT, właściwym organom lub SPOC natychmiastowy dostęp do zgłoszeń incydentów dokonywanych zgodnie z sektorowym aktem prawnym Unii. Zgodnie z motywem 24 preambuły dyrektywy NIS 2, taki natychmiastowy dostęp można zapewnić w szczególności, jeżeli zgłoszenia incydentów są przekazywane bez zbędnej zwłoki CSIRT, właściwemu organowi lub SPOC.[15] Przy czym, zdaniem KE, natychmiastowy dostęp może być zapewniony za pomocą środków automatycznych i bezpośrednich wdrożonych przez państwa członkowskie, można w tym celu wykorzystać także pojedynczy punkt zgłaszania incydentów, który jednak musi być zgodny z sektorowym aktem prawnym UE.[16]

KE dokonała także interpretacji w zakresie konsekwencji równoważności aktu sektorowego z dyrektywą NIS 2 w zakresie określonym w jej art. 4 ust. 1 i 2 uznając, że w takim przypadku nie stosuje się odpowiednich przepisów dyrektywy

[7] Tamże, pkt 9.
[8] Tamże, pkt 10.
[9] Tamże, pkt 11.
[10] Tamże, pkt 12.
[11] Tamże, pkt 13.
[12] Tamże, pkt 14.
[13] Tamże, pkt 15.
[14] Tamże, pkt 17-20.
[15] Tamże, pkt 25.
[16] Tamże, pkt 26.

NIS 2 dotyczących przyjęcia środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa, zgłaszania poważnych incydentów oraz nadzoru i egzekwowania przepisów (rozdział VII dyrektywy NIS 2)[17]. Z powołaniem się na motyw 25 preambuły dyrektywy NIS 2, KE podreśliła możliwość przewidywania przez sektorowe akty prawne Unii, które są co najmniej równoważne pod względem skutku, że właściwe organy wyznaczone na ich podstawie wykonują swoje uprawnienia dotyczące nadzoru i egzekwowania przepisów w odniesieniu do obowiązków w zakresie zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków w zakresie zgłaszania incydentów z pomocą właściwych organów wyznaczonych na podstawie dyrektywy NIS 2. Mogą one w tym celu przyjąć ustalenia dotyczące współpracy, w tym procedury dotyczące koordynacji działań nadzorczych procedury dochodzeń i kontroli na miejscu zgodnie z prawem krajowym[18].

Zdaniem KE, sektorowe akty prawne UE mogą określać szczególne zadania CSIRT, a w razie braku ich określenia w tych aktach – wykonują one zadania określone w art. 11 ust. 3 dyrektywy NIS 2[19]. Ponadto w odniesieniu do krajowych ram zarządzania kryzysowego oraz EU-CyCLONe, KE uznała, że art. 9 i 16 dyrektywy NIS 2 powinny w całości mieć zastosowanie do sektorów, nawet jeżeli istnieją sektorowe akty prawne Unii w rozumieniu jej art. 4. Państwo członkowskie musi wyznaczyć lub ustanowić co najmniej jeden organ ds. zarządzania kryzysowego w cyberbezpieczeństwie odpowiedzialny za zarządzanie incydentami i sytuacjami kryzysowymi w cyberbezpieczeństwie na dużą skalę w sektorach objętych zakresem stosowania sektorowych aktów prawnych UE. Sektorów tych nie należy także pomijać przy przyjmowaniu krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę[20]

Dodatek do komunikatu KE odnosi się do jedynego aktu sektorowego - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/ 1011[21] (dalej: DORA)

Art. 1 ust. 2 DORA stanowi, że w odniesieniu do podmiotów finansowych objętych zakresem stosowania dyrektywy NIS 2 oraz odpowiednich krajowych przepisów transponujących tę dyrektywę, DORA uznaje się za sektorowy akt prawny Unii do celów art. 4 dyrektywy NIS 2. W związku z powyższym zamiast przepisów dyrektywy NIS 2 zastosowanie powinny mieć przepisy DORA dotyczące zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (dalej: ICT) (art. 6 i nast. DORA), zarządzania incydentami związanymi z ICT, a w szczególności zgłaszania poważnych incydentów związanych z ICT (art. 17), a także testowania operacyjnej odporności cyfrowej (art. 24), mechanizmów wymiany informacji (art. 25) oraz ryzyka związanego z zewnętrznymi dostawcami ICT (art. 28). Do podmiotów finansowych objętych DORA państwa członkowskie nie powinny zatem stosować przepisów dyrektywy NIS 2 dotyczących zarządzania ryzykiem w cyberbezpieczeństwie i obowiązków w zakresie zgłaszania incydentów oraz nadzoru i egzekwowania przepisów.

Zgodnie z nim podmioty finansowe uznaje się za podmioty, o których mowa w art. 2 ust. 1 lit. a)–t) DORA. Rodzaje podmiotów, które wchodzą w zakres

[17] Tamże, pkt 28.
[18] Tamże, pkt 29.
[19] Tamże, pkt 33.
[20] Tamże, pkt 36.
[21] Dz.U. L 333 z 27.12.2022, s. 1.

stosowania DORA, jako podmioty finansowe, jak również dyrektywy NIS 2, jako podmioty kluczowe lub ważne, obejmują instytucje kredytowe, systemy obrotu i kontrahentów centralnych. Ponieważ ważne jest utrzymanie silnych relacji i wymiany informacji z sektorem finansowym, zgodnie z dyrektywą NIS 2, DORA umożliwia Europejskim Urzędom Nadzoru oraz właściwym organom wyznaczonym na podstawie tego rozporządzenia ubieganie się o udział w działaniach Grupy Współpracy oraz wymianę informacji i współpracę z SPOC, a także z CSIRT i właściwymi organami wyznaczonymi na podstawie dyrektywyNIS 2. Państwa członkowskie powinny w dalszym ciągu uwzględniać sektor finansowy w swoich strategiach cyberbezpieczeństwa. Przepisy dotyczące krajowych ram zarządzania kryzysowego w cyberbezpieczeństwie (art. 9 dyrektywy NIS 2), jak również dotyczące EU-CyCLONe (art. 16 dyrektywy NIS 2) powinny nadal mieć zastosowanie do podmiotów objętych zakresem DORA[22]

DORA a Dyrektywa NIS 2

Należy uznać, że KE jednoznacznie uznała DORA za sektorowy akt prawny UE dla celów art. 4 dyrektywy NIS 2. W konsekwencji powyższego, zdaniem KE do podmiotów finansowych w rozumieniu DORA, zamiast przepisów dyrektywy NIS2 powinny mieć zastosowanie przepisy DORA dotyczące zarządzenia ryzykiem związanym z technologiami informacyjno-komunikacyjnymi, zarządzania incydentami z nimi związanymi testowania operacyjnej odporności cyfrowej, mechanizmów wymiany informacji oraz ryzyka związanego z zewnętrznymi dostawcami tych technologii. Ponadto do podmiotów finansowych objętych DORA państwa członkowskie nie powinny stosować przepisów dyrektywy NIS 2 dotyczących zarządzania ryzykiem w cyberbezpieczeństwie i obowiązków w zakresie zgłaszania incydentów oraz nadzoru i egzekwowania przepisów[23].

Stanowisko KE jest w pełni zgodne z regulacją art. 1 ust. 2 DORA, zgodnie z którą w odniesieniu do podmiotów finansowych, zidentyfikowanych jako podmioty kluczowe lub ważne[24] zgodnie z przepisami krajowymi transponującymi art. 3 dyrektywy NIS 2, DORA uznaje się za sektorowy akt prawny UE do celów art. 4 dyrektywy NIS 2. Z motywu 15 preambuły DORA wynika, że dyrektywa NIS 2 ustanawia jednolite kryterium określania podmiotów objętych jej zakresem stosowania (zasada limitu wielkości), przy czym obejmuje nim też instytucje kredytowe, systemów obrotu i kontrahentów centralnych.[25] Relację między dyrektywą NIS 2 a DORA określa motyw 16 preambuły DORA. Zgodnie z tym zapisem, ze względu na zwiększenie przez DORA poziomu harmonizacji różnych elementów odporności cyfrowej poprzez wprowadzenie bardziej rygorystycznych wymogów w zakresie zarządzania ryzykiem związanym z ICT i zgłaszania

[22] Komunikat KE w sprawie Wytycznych dotyczących stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS 2) – Dodatek – Sektorowe akty prawne Unii - Rozporządzenie (UE) 2022/2554 (rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego).
[23] Tamże, pkt 1. Por. także Ch. Rupp. Navigating the EU Cybersecurity Policy Ecosystem, A Comprehensive Overview of Legislation, Policies and Actors, June 27, 2024. https://www.interface-eu.org/publications/download/navigating-the-eu-cybersecurity-policy-ecosystem [dostęp 20.08.2025], s. 66.
[24] Por. E. Chronowska-Sioła, Unijna Dyrektywa NIS 2 w obszarze cyberbezpieczeństwa – analiza podmiotów kluczowych i podmiotów ważnych, Cybersecurity and Law 2025, nr 2, s. 14-29, https://www.cybersecurityandlaw.pl/nr-2/2.pdf [dostęp 9.04.2026 r.]; K. Chałubińska-Jentkiewicz, M. Nowikowska, Entities Involved in the Policy and Information Systems in the Light of the NIS 2 Directive (Part 1), Cybersecurity and Law 2024, nr 1, s. 8-10.
[25] DORA, motyw 15.

incydentów związanych z ICT, wyższy poziom zapewnia zwiększoną harmonizację również w porównaniu z wymogami określonymi w dyrektywie NIS 2. W związku z tym DORA stanowi *lex specialis* względem dyrektywy NIS 2. Jednocześnie, utrzymanie silnego związku między sektorem finansowym a unijnymi horyzontalnymi ramami w zakresie cyberbezpieczeństwa, określonymi obecnie w dyrektywie NIS 2, ma zasadnicze znaczenie dla zapewnienia spójności z przyjętymi przez państwa członkowskie strategiami w zakresie cyberbezpieczeństwa[26].

Wzajemne relacje między dyrektywą NIS 2 a DORA zostały opisane także w motywie 18 preambuły DORA, zgodnie z którym podmioty finansowe powinny pozostać częścią „ekosystemu" dyrektywy NIS 2, m.in. w celu współpracy międzysektorowej. Właściwe organy zgodnie z DORA powinny również prowadzić konsultacje i współpracować z CSIRT.[27]

Analogiczne zapisy zawarte są także w motywie 28 preambuły dyrektywy NIS 2, zgodnie z którym DORA należy uznać za sektorowy akt prawny UE powiązany z dyrektywą NIS 2 w odniesieniu do podmiotów finansowych. Zamiast przepisów dyrektywy NIS 2 zastosowanie powinny mieć przepisy DORA dotyczące zarządzania ryzykiem związanym z ICT, zarządzania incydentami związanymi z ICT, a w szczególności zgłaszania poważnych incydentów związanych z ICT. Do podmiotów finansowych objętych DORA państwa członkowskie nie powinny stosować przepisów dyrektywy NIS 2 dotyczących zarządzania ryzykiem w cyberbezpieczeństwie i obowiązków w zakresie zgłaszania incydentów oraz nadzoru i egzekwowania prawa. Istotne jest utrzymywanie silnych relacji i skutecznej wymiany informacji z sektorem finansowym na podstawie dyrektywy NIS 2. W tym celu DORA umożliwia Europejskim Urzędom Nadzoru oraz właściwym organom na podstawie tego rozporządzenia udział w działaniach Grupy Współpracy oraz wymianę informacji i współpracę z pojedynczymi punktami kontaktowymi, a także z CSIRT i właściwymi organami na podstawie dyrektywy NIS 2. Właściwe organy na podstawie DORA powinny także przekazywać dane na temat poważnych incydentów związanych z ICT i, w odpowiednich przypadkach, poważnych cyberzagrożeń także CSIRT, właściwym organom lub pojedynczym punktom kontaktowym na podstawie dyrektywy NIS 2. Można to osiągnąć przez zapewnienie natychmiastowego dostępu do zgłoszeń incydentów i ich bezpośrednie przekazywanie bezpośrednio lub za pośrednictwem pojedynczego punktu[28] Podkreślić należy, że motyw 28 preambuły dyrektywy NIS 2 jest bardzo szczegółowy i odnosi się do konkretnego aktu prawnego UE – DORA. Ogólny charakter w zakresie sektorowych aktów prawnych mają motywy 23 – 27 preambuły dyrektywy NIS2[29].

Zgodnie z art. 2 ust. 4 DORA, państwa członkowskie mogą wyłączyć z zakresu stosowania DORA podmioty, o których mowa w art. 2 ust. 5 pkt 4-23 dyrektywy 2013/36/UE, mające siedzibę na ich odpowiednich terytoriach. Jeżeli państwo członkowskie korzysta z takiej możliwości, informuje o tym KE oraz o wszelkich późniejszych zmianach w tym względzie. KE podaje te informacje do wiadomości publicznej na swojej stronie internetowej lub za pomocą innych łatwo

[26] DORA, motyw 16.
[27] DORA, motyw 18.
[28] Dyrektywa NIS2, motyw 28.
[29] Odnoszą się one m.in. do podmiotowego zakresu sektorowego aktu UE, obowiązków związanych ze zgłaszaniem incydentów, współpracy organów przy obsłudze incydentów oraz roli CSIRT, właściwych organów i pojedynczych punktów kontaktowych. Przyszłe akty sektorowe powinny uwzględniać definicje zawarte w dyrektywie NIS 2.

dostępnych środków. W Polsce do kręgu tych podmiotów należy Bank Gospodarstwa Krajowego, spółdzielcze kasy oszczędnościowo-kredytowe[30] oraz Krajową Spółdzielczą Kasę Oszczędnościowo-Kredytową. Zgodnie z art. 2 ust. 10 dyrektywa NIS 2 nie ma zastosowania do podmiotów, które państwa członkowskie zwolniły z zakresu stosowania DORA na podstawie art. 2 ust. 4 DORA. W Polsce nie zdecydowano się na zwolnienie z zakresu stosowania DORA na podstawie art. 2 ust. 4 DORA żadnego z podmiotów[31].

Krąg podmiotów finansowych, których dotyczy DORA, został określony bardzo szeroko i obejmuje podmioty, o których mowa w art. 2 ust. 1 lit. a-t DORA. DORA przewiduje dwa reżimy obowiązywania – pełny oraz uproszczony. Reżim uproszczony DORA ma zastosowanie do małych i niepowiązanych wzajemnie firm inwestycyjnych, zwolnionych instytucji płatniczych, zwolnionych instytucji kredytowych, co do których państwo członkowskie nie skorzystało z opcji narodowej określonej w art. 2 ust. 4 DORA. Brak jest uzasadnienia do ewentualnego różnicowania w kontekście zastosowania art. 4 dyrektywy NIS 2 sytuacji podmiotu finansowego podlegającego DORA ze względu na to czy ma do niego zastosowanie art. 16 DORA, czy też nie. Jednocześnie podkreślić należy, że państwa członkowskie nie mają możliwości wyłączenia stosowania art. 16 DORA do objętych nim podmiotów finansowych, gdyż w artykule tym nie przewidziano opcji narodowej. W tym kontekście regulacja art. 4 i 9 ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji wyłączającą stosowanie art. 16 DORA do części podmiotów nim objętych stanowi oczywiste naruszenie art. 16 oraz 64 DORA, a w konsekwencji także art. 288 Traktatu o funkcjonowaniu Unii Europejskiej[32] oraz art. 91 ust. 3 w zw. z art. 9 i art. 87 ust. 1 oraz art. 90 ust. 1 Konstytucji RP[33].

Kwestia tzw. Gold Platingu

Dyrektywa NIS 2 nie jest dyrektywą maksymalnej harmonizacji, a jedynie dyrektywą minimalnej harmonizacji, zatem, co do zasady państwo członkowskie może objąć regulacją krajową także podmioty wyłączone spod zakresu obowiązywania dyrektywy. Należy zwrócić uwagę na to, DORA nie jest dyrektywą, ale rozporządzeniem, zatem obowiązuje bezpośrednio i w całości na obszarze wszystkich państw członkowskich[34]. Zgodnie z powołanym wyżej art. 1 ust. 2 DORA, w odniesieniu do podmiotów finansowych zidentyfikowanych jako podmioty kluczowe lub ważne zgodnie z przepisami krajowymi transponującymi art. 3 dyrektywy NIS 2, DORA uznaje się za sektorowy akt prawny UE do celów art. 4 tej dyrektywy. Każde państwo członkowskie zobowiązane jest zatem do stosowania tej normy. Jej cel należy interpretować zgodnie z motywem 16 preambuły DORA, który nakazuje by DORA potraktować jako *lex specialis* do NIS 2 w odniesieniu do

[30] Ustawa z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (tj. Dz. U z 2026 r. poz. 595).
[31] Ustawa z dnia 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji (Dz. U. 2025 r. poz. 1069), por. także Sejm RP X kadencji. Druk Sejmowy nr 1262, uzasadnienie s. 19 i 55-56.
[32] Dz. U. z 2004 r. nr 90 poz. 864
[33] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. nr 78, poz. 483).
[34] Por art. 64 DORA.

podmiotów finansowych, a także wskazuje, że DORA zapewnia zwiększoną harmonizację również w porównaniu z wymogami określonymi w dyrektywie NIS 2. W tym kontekście można uznać implementację dyrektywy NIS 2 do krajowego porządku prawnego włączającą do podmiotowego zakresu regulacji także podmioty finansowe podlegające DORA nie tylko jako tzw. *Gold plating*[35], ale także jako naruszenie art. 1 ust. 2 w zw. z art. 64 DORA ze względu na brzmienie motywu 16 preambuły DORA.

Kwestia równoważności DORA

W oparciu o treść omówionego wyżej komunikatu KE wydanego na podstawie art. 4 ust. 3 dyrektywy NIS 2, należy uznać DORA za sektorowy akt równoważny wymogom art. 21 ust. 1 i 2 DORA zarówno do podmiotów finansowych objętych pełną regulacją, jak i w odniesieniu do podmiotów finansowych, do których zastosowanie mają uproszczone ramy zarządzania ryzykiem ICT określone w art. 16 DORA.

Kluczowe jest po pierwsze wskazanie, że DORA przewiduje mechanizm zarządzania incydentami związanymi z ICT, ich klasyfikacji i zgłaszania. Regulacje te mają zastosowanie także do podmiotów finansowych stosujących uproszczone zasady zarządzania ryzykiem ICT na podstawie art. 16 DORA. Należy uznać, że także w odniesieniu do tych podmiotów, sektorowy akt prawny UE przewiduje natychmiastowy dostęp CSIRT, właściwych organów lub pojedynczych punktów kontaktowych na mocy niniejszej dyrektywy do zgłoszeń incydentów.

Istotne jest wskazanie, że art. 4 ust. 1 dyrektywy NIS 2 wymaga co najmniej równoważności pod względem skutku. Nie chodzi zatem o porównywanie treści poszczególnych zapisów, lecz ich skutku. Obowiązek wprowadzania odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez 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 wynikający z art. 21 ust. 1 dyrektywy NIS 2, realizowany jest w przypadku podmiotów objętych uproszczonym reżimem w pełni przez art. 16 ust. 1 DORA. Wprowadza on bowiem m.in. obowiązek wprowadzania i utrzymywania prawidłowych i udokumentowanych ram zarządzania ryzykiem związanym z ICT. Środki te są zatem w pełni równoważne pod względem skutku z wymogami określonymi w art. 21 ust. 1 dyrektywy NIS 2. Zasada proporcjonalności jest wprost wyrażona w art. 21 ust. 1 dyrektywy NIS 2, zgodnie z którym, oceniając proporcjonalność tych środków, uwzględnia się stopień narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze.

Analiza oceny równoważności skutków zawartych w art. 21 ust. 2 dyrektywy NIS 2 wymaga wykazania, że skutki wynikające z DORA, są co najmniej równoważne ze skutkami określonym w art. 21 ust. 2 dyrektywy NIS 2.

Skutek bazowania na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska

[35] Por. K. Kaczor, *Gold-plating* – problem nadtraspozycji dyrektyw unijnych do krajowego porządku prawnego, Folia Iuridica Universitatis Wratislaviensis 2022, vol. 11 (1), s. 76-98; M. Marciniak, Nadmierna implementacja dyrektyw unijnych do krajowego systemu prawnego, Lublin 2024, s. 199-278.

fizyczne tych systemów przed incydentami wynika w szczególności z art. 16 ust. 1 lit. a DORA.

Jeśli chodzi o poszczególne elementy tego podejścia określone w art. 21 ust. 2 lit a-j dyrektywy NIS 2 to skutek równoważności wynika z następujących uregulowań:

- art. 21 ust. 2 lit. a dyrektywy NIS2 polityka analizy ryzyka i bezpieczeństwa systemów informatycznych – art. 16 ust. 1 lit. a w zw. z ust. 2 DORA (udokumentowane ramy zarządzania ryzykiem wywołują skutek co najmniej równoważny z polityką analizy ryzyka i bezpieczeństwa systemów informatycznych)[36],
- art. 21 ust. 2 lit. b dyrektywy NIS 2 – obsługa incydentu – art. 16 ust. 1 lit. a, b oraz art. 16 ust. 1 lit. d, art. 17 i nast. DORA;
- art. 21 ust. 2 lit. c dyrektywy NIS 2 – ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej – art. 16 ust. 1 lit. b, c oraz f DORA;
- art. 21 ust. 2 lit. d dyrektywy NIS 2 – bezpieczeństwo łańcucha dostaw – art. 16 ust. 1 lit. e DORA zgodnie z którym podmioty finansowe określają kluczowe zależności od zewnętrznych dostawców usług ICT;
- art. 21 ust. 2 lit. e dyrektywy NIS 2 – bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie – art. 16 ust. 1 lit. d, e DORA;
- art. 21 ust. 2 lit. f dyrektywy NIS 2 – polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie – art. 16 ust. 1 lit. b, g oraz h DORA;
- art. 21 ust. 2 lit. g dyrektywy NIS 2 – podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa – art. 16 ust. 1 i 2 DORA;
- art. 21 ust. 1 lit. h dyrektywy NIS 2 – polityki i procedury stosowania kryptografii – art. 16 ust. 1 lit. c DORA
- art. 21 ust. 1 lit. h dyrektywy NIS 2 – bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami – art. 16 ust. 1 i 2 DORA;
- art. 21 ust. 1 lit. j dyrektywy NIS 2 – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych. W odniesieniu do podmiotów finansowych równoważny skutek jest osiągany przez art. 16 ust. 1 lit. c DORA, zgodnie z którym podmioty finansowe minimalizują wpływ ryzyka związanego z ICT poprzez stosowanie prawidłowych, odpornych i zaktualizowanych systemów, protokołów i narzędzi ICT, które są odpowiednie do wspierania realizacji ich działań i świadczenia usług i odpowiednio chronią dostępność, autentyczność, integralność oraz poufność danych w sieci i systemach informatycznych.

Podsumowanie

Podsumowując przeprowadzone rozważania można stwierdzić, że zarówno w świetle analizy komunikatu KE wydanego na podstawie art. 4 ust. 3 dyrektywy NIS 2, treści dyrektywy NIS 2 i DORA oraz motywów preambuł do tych aktów prawnych należy uznać, że regulacja DORA powinna być uznana za co najmniej równoważną

[36] Dz. U. UE z 2024 r. nr 1774.

w odniesieniu do skutku z regulacją określoną w art. 4 ust. 1 i 2 dyrektywy NIS 2. Wynika z tego, że DORA powinna mieć dla podlegających jej podmiotów finansowych pierwszeństwo i wyłączać w zakresie w niej uregulowanym stosowanie regulacji implementujących dyrektywę NIS 2 do porządku krajowego w państwach członkowskich. Osiągnięcie skutku równoważnego nie oznacza, że DORA musi posługiwać się dokładnie tymi samymi narzędziami co dyrektywa NIS 2. W przypadku podmiotów finansowych podlegających DORA będących podmiotami kluczowymi lub ważnymi w rozumieniu dyrektywy NIS 2, zamiast przepisów dyrektywy NIS 2 zastosowanie powinny mieć przepisy DORA dotyczące zarządzania ryzykiem związanym z technologiami ICT (art. 6 i nast.), zarządzania incydentami związanymi z ICT, a w szczególności zgłaszania poważnych incydentów związanych z ICT (art. 17 i nast.), a także testowania operacyjnej odporności cyfrowej (art. 24 i nast.), mechanizmów wymiany informacji (art. 25) oraz ryzyka związanego z zewnętrznymi dostawcami ICT (art. 28 i nast.). W tym zakresie zastosowanie będzie miało stosowane wprost prawo unijne (DORA), a nie regulacja dyrektywy NIS 2 implementowana do porządku prawnego państw członkowskich przez ich ustawodawstwo krajowe. Podkreślić należy, że dotychczas jedynie DORA została uznana przez KE za sektorowy akt prawny UE, którego wymogi są co najmniej równoważne pod względem skutku obowiązkom określonym w dyrektywnie NIS 2.

Bibliografia

Banasiński C., Podstawowe pojęcia i podstawy prawne cyberbezpieczeństwa [w:] Banasiński C. (red.), Cyberbezpieczeństwo. Zarys wykładu, Warszawa 2023.

Chałubińska-Jentkiewicz K., Nowikowska M., Entities Involved in the Policy and Information Systems in the Light of the NIS 2 Directive (Part 1), „Cybersecurity and Law" 2024, nr 1.

Chronowska-Sioła E., Unijna Dyrektywa NIS 2 w obszarze cyberbezpieczeństwa – analiza podmiotów kluczowych i podmiotów ważnych, „Cybersecurity and Law" 2025, nr 2.

Gaie Ch., Karpiuk M., Strizzolo N., Cybersecurity of Public Sector Institutions, „Prawo I Więź" 2024, nr 6.

Głowacki B., Grzybowska-Ganszczyk D., Dyrektywa NIS2 jako narzędzie wzmacniania bezpieczeństwa lokalnego i narodowego w obszarze cyberzagrożeń, journaldot.pl.

Kaczor K., Gold-plating – problem nadtraspozycji dyrektyw unijnych do krajowego porządku prawnego, „Folia Iuridica Universitatis Wratislaviensis" 2022, vol. 11 (1).

Karpiuk M., The Legal Status of Digital Service Providers in the Sphere of Cybersecurity, „Studia Iuridica Lublinensia" 2023, nr 2.

Mączka K., Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji, „Ochrona Ludności i Dziedzictwa Kulturowego" 2024, nr 5.

Rupp Ch., Navigating the EU Cybersecurity Policy Ecosystem. A Comprehensive Overview of Legislation, „Policies and Actors" 2024.

Skoczylas D., Dyrektywa NIS 2 a cyberbezpieczeństwa administracji publicznej, „Dyskurs Prawniczy i Administracyjny" 2025, nr 1.

Tylawa D., Cyberbezpieczeństwo a globalne prawo adminsitracyjne [w:] Karpiuk M. (red.), Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe, Warszawa 2024.

Zawadzki T., Analiza wpływu regulacji na zagrożenia w cyberprzestrzeni, „Cybersecurity and Law" 2025, nr 2.

Komisja Europejska, Wysoki Przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, Bruksela 16.12.2020, JOIN(2020) 18 final.

Traktat o funkcjonowaniu Unii Europejskiej (Dz. U. z 2004 r. nr 90 poz. 864.).

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

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE z 2022 r. nr 333).

Rozporządzanie delegowane Komisji (UE) 2024/1774 z dnia 13 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT oraz uproszczone ramy zarządzania ryzykiem związanym z ICT (Dz. U. UE z 2024 r. nr 1774).

Komunikat Komisji Europejskiej w sprawie Wytycznych dotyczących stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS 2), (Dz. U. UE z 2023 r. nr 328 str. 2)

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. nr 78, poz. 483)

Ustawa z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (tj. Dz. U z 2024 r. poz. 512).

Ustawa z dnia 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji (Dz. U. 2025 r. poz. 1069).