Paweł Pelc*

Zasada proporcjonalności w DORA

Streszczenie

DORA zakresem swoim obejmuje szeroki krąg podmiotów finansowych o zróżnicowanej wielkości, skali i przedmiocie działania. W efekcie szczególnie istotne jest uwzględnienie zasady proporcjonalności, wynikającej z Traktatu o Unii Europejskiej, w jej regulacji. Zasada ta ma zastosowanie zarówno do zakresu podmiotowego, jak i przedmiotowego DORA. W efekcie jej zastosowanie pozwala instytucjom finansowym dostosować sposób stosowania DORA do ich skali i charakteru działania, jednocześnie umożliwiając powszechne stosowanie DORA, ze względu na ryzyko zarażania. Pozytywnie należy też ocenić uproszczone zasady dla najmniejszych podmiotów lub podmiotów prowadzących ograniczoną działalność. Wadliwa jest jedynie regulacja dotycząca instytucji zwolnionych na podstawie dyrektywy bankowej – ich sytuację uregulowano bowiem z pominięciem tego, że są one wyłączone spod zakresu rozporządzenia CRR, w którym zawarta jest definicja instytucji kredytowej, do której odsyła DORA określając zakres podmiotowy.

Słowa kluczowe: DORA, proporcjonalność, instytucje finansowe, cyberbezpieczeństwo

* Paweł Pelc, Akademia Sztuki Wojennej, Warszawa, Akademickie Centrum Polityki Cyberbezpieczeństwa, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

14 grudnia 2022 roku zostało przyjęte rozporządzenie Parlamentu Europejskiego i Rady (UE) 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[1] (Digital Operational Resilience Act – DORA).

Jest to pierwsza próba kompleksowego uregulowania kwestii dotyczących odporności cyfrowej i bezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (Information and communication technology – ICT) instytucji finansowych. DORA to element przyjętego przez Komisję Europejską we wrześniu 2020 roku pakietu dotyczącego finansów cyfrowych, zawierającego m.in. komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 24 września 2020 r. w sprawie strategii dla UE w zakresie finansów cyfrowych (COM(2020) 591 final)[2] – jednym z czterech priorytetów zawartych w tej strategii był ten, który dotyczy sprostania wyzwaniom i zagrożeniom związanym z transformacją cyfrową[3]. Realizując ten priorytet, ustawodawca europejski postanowił objąć zakresem regulacji DORA bardzo duży krąg podmiotów określony w jej art. 2 ust. 1[4].

Stanął on na stanowisku, że „Większy zakres cyfryzacji i wzajemnych powiązań zwiększa również ryzyko związane z ICT, przez co całe społeczeństwo – i w szczególności system finansowy – staje się bardziej podatne na cyberzagrożenia lub zakłócenia w funkcjonowaniu ICT"[5]. W związku z tym podjęto próbę wyważenia konieczności zasady jednolitego podejścia z zasadą proporcjonalności: „Podmioty finansowe powinny przyjąć to samo podejście i stosować się do tych samych, opartych na zasadach przepisów podczas zwalczania ryzyka związanego z ICT, uwzględniając przy tym swoją wielkość i ogólny profil ryzyka oraz charakter, skalę i stopień złożoności realizowanych usług, działań i operacji. Spójność przyczynia się do wzmocnienia zaufania do systemu

1 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, Dz. Urz. UE 2022, L 333, s. 1 9 (dalej: DORA).

2 https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0591&fro- m=EN [dostęp: 15.03.2024].

3 P. Pelc, *Wpływ planowanych przez UE działań i regulacji na instytucje finansowe w Polsce*, „Cybersecurity and Law" 2021, nr 1, s. 31–42.

4 Idem, *Cyberbezpieczeństwo instytucji finansowych w wymiarze krajowym i międzynarodowym* [w:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, red. M. Karpiuk, Warszawa 2024, s. 39.

5 DORA, motyw 1.

finansowego oraz ochrony jego stabilności, zwłaszcza w czasach dużej zależności od systemów, platform i infrastruktur ICT, co powoduje większe ryzyko cyfrowe. Przestrzeganie zasad podstawowej higieny cyberbezpieczeństwa powinno również pozwolić uniknąć obciążania gospodarki znacznymi kosztami dzięki zminimalizowaniu wpływu i kosztów zakłóceń funkcjonowania ICT"[6]. Zasada proporcjonalności jest określona w art. 5 Traktatu o Unii Europejskiej podpisanego w Maastricht 7 lutego 1992 roku[7]. Zgodnie z nim wykonywanie zadań i uprawnień UE podlega m.in. zasadzie pomocniczości, zgodnie z którą zakres i forma działania Unii nie wykraczają poza to, co jest konieczne do osiągnięcia celów traktatów. Wymaga ona, żeby środek unijny nie nakładał niepotrzebnych ciężarów na państwo członkowskie lub jednostki, a jeżeli istnieje wybór między środkami, które nadają się do osiągnięcia danego celu, to należy wybierać środki najmniej restrykcyjne[8]. W pełni należy podzielić pogląd Małgorzaty Urban-Theocharkis dotyczący stosowania zasady proporcjonalności do sektora finansowego: „Odnosząc się do stanowiska prezentowanego przez naukę i praktykę, należy podzielić pogląd, że sektor finansowy jest wyjątkowo zróżnicowany w odniesieniu do działalności, ryzyka generowanego dla klientów i systemu finansowego, skali działania firm i stopnia ich powiązań. Zastosowanie zróżnicowanego podejścia do regulacji, zwłaszcza mniejszych firm i reprezentujących mniejszy stopień złożoności, może spowodować, że byłyby one bardziej skuteczne w realizacji celów w zarządzaniu specyficznymi rodzajami ryzyka i potrzebami"[9].

W związku z tym zasada proporcjonalności została wzięta pod uwagę w procesie pracy nad DORA, na co w szczególności wskazują następujące jej motywy: „Niezależnie od szerokiego zakresu stosowania przewidzianego w niniejszym rozporządzeniu, stosując zasady dotyczące operacyjnej odporności cyfrowej, należy uwzględniać istotne różnice między podmiotami finansowymi pod względem ich wielkości i ogólnego profilu ryzyka. Co do zasady, rozdzielając zasoby i zdolności na wdrażanie ram zarządzania ryzykiem związanym z ICT, podmioty finansowe powinny należycie dostosować swoje potrzeby związane z ICT do swojej wielkości i ogólnego profilu ryzyka oraz charakteru, skali i stopnia złożoności realizowanych usług, działań i operacji,

6 Ibidem, motyw 13.
7 Dz. U. 2004, nr 90, poz. 864.
8 Por. R. Grzeszczak, *Komentarz do art. 5* [w:] *Traktat o Unii Europejskiej. Komentarz*, red. D. Kornobis-Romanowska, Warszawa 2023.
9 M. Urban-Theocharakis, *Pakiet CRRII/ CRD V a wzmocnienie zasady proporcjonalności*, LEX/el. 2019.

natomiast właściwe organy powinny nadal oceniać i weryfikować podejście do takiego rozdziału”[10]. „Ponieważ większe podmioty finansowe mogą korzystać z większych zasobów i są w stanie szybko przeznaczyć środki finansowe na opracowanie struktur zarządzania i stworzenie szeregu strategii korporacyjnych, wymóg tworzenia bardziej złożonych rozwiązań w zakresie zarządzania należy nałożyć wyłącznie na podmioty finansowe, które nie są mikroprzedsiębiorstwami w rozumieniu niniejszego rozporządzenia. Podmioty takie są lepiej przygotowane w szczególności do ustanowienia specjalnych stanowisk w strukturach zarządzania w celu nadzorowania ustaleń umownych z zewnętrznymi dostawcami usług ICT lub w celu zarządzania kryzysowego, do organizowania zarządzania w zakresie ryzyka związanego z ICT zgodnie z modelem trzech linii obrony lub do ustanowienia wewnętrznego modelu zarządzania ryzykiem i kontroli ryzyka oraz do poddania swoich ram zarządzania ryzykiem związanym z ICT audytowi wewnętrznemu”[11]. „Niektóre podmioty finansowe korzystają ze zwolnień lub są objęte bardzo łagodnymi ramami regulacyjnymi na mocy odpowiednich przepisów sektorowych prawa Unii. Takie podmioty finansowe obejmują zarządzających alternatywnymi funduszami inwestycyjnymi, o których mowa w art. 3 ust. 2 dyrektywy Parlamentu Europejskiego i Rady 2011/61/UE 17, zakłady ubezpieczeń i zakłady reasekuracji, o których mowa w art. 4 dyrektywy Parlamentu Europejskiego i Rady 2009/138/WE 18, oraz instytucje pracowniczych programów emerytalnych, które obsługują programy emerytalne liczące łącznie nie więcej niż 15 uczestników. W świetle tych zwolnień włączenie takich podmiotów finansowych do zakresu stosowania niniejszego rozporządzenia nie byłoby proporcjonalne. Dodatkowo w niniejszym rozporządzeniu uznaje się specyfikę struktury rynku pośrednictwa ubezpieczeniowego, w związku z czym pośrednicy ubezpieczeniowi, pośrednicy reasekuracyjni i pośrednicy oferujący ubezpieczenia uzupełniające kwalifikujący się jako mikroprzedsiębiorstwa, czy małe lub średnie przedsiębiorstwa, nie powinni podlegać niniejszemu rozporządzeniu”[12]. „Ponieważ podmioty, o których mowa w art. 2 ust. 5 pkt 4–23 dyrektywy 2013/36/UE, są wyłączone z zakresu stosowania tej dyrektywy, państwa członkowskie powinny w związku z tym mieć możliwość podjęcia decyzji o zwolnieniu takich podmiotów mających siedzibę na ich odpowiednich terytoriach z zakresu stosowania

10 DORA, motyw 36.
11 Ibidem, motyw 38.
12 Ibidem, motyw 39.

niniejszego rozporządzenia”[13]. „Analogicznie, aby dostosować niniejsze rozporządzenie do zakresu stosowania dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE 19, z zakresu stosowania niniejszego rozporządzenia należy wyłączyć osoby fizyczne i prawne, o których mowa w art. 2 i 3 tej dyrektywy, które posiadają zezwolenie na świadczenie usług inwestycyjnych bez konieczności uzyskiwania zezwolenia na mocy dyrektywy 2014/65/UE. Niemniej jednak w art. 2 dyrektywy 2014/65/UE wyłącza się z zakresu stosowania tej dyrektywy podmioty, które kwalifikują się jako podmioty finansowe do celów niniejszego rozporządzenia, takie jak centralne depozyty papierów wartościowych, przedsiębiorstwa zbiorowego inwestowania lub zakłady ubezpieczeń i zakłady reasekuracji. Wyłączenie osób i podmiotów, o których mowa w art. 2 i 3 tej dyrektywy, z zakresu stosowania niniejszego rozporządzenia nie powinno obejmować tych centralnych depozytów papierów wartościowych, przedsiębiorstw zbiorowego inwestowania ani zakładów ubezpieczeń czy reasekuracji”[14]. Na zasadę proporcjonalności wskazuje się także w motywie 42 i 43 DORA dotyczących mniejszych instytucji o ograniczonej skali i przedmiocie świadczonych usług finansowych, a także w motywie 105. Do specyfiki działalności poszczególnych instytucji finansowych nawiązuje też motyw 53 DORA, a w motywie 64 wskazano, że „Podmioty finansowe powinny stosować proporcjonalne podejście do monitorowania zagrożeń występujących na poziomie zewnętrznego dostawcy usług ICT i odpowiednio uwzględnić charakter, skalę, stopień złożoności i znaczenie swoich zależności w zakresie ICT, krytyczność lub znaczenie usług, procesów lub funkcji objętych ustaleniami umownymi, a ostatecznie na podstawie starannej oceny wszelkiego potencjalnego wpływu na ciągłość i jakość usług finansowych na szczeblu indywidualnym i grupowym, w zależności od przypadku”[15].

Zasadę proporcjonalności zastosowano w DORA zarówno w odniesieniu do zakresu podmiotowego regulacji (poprzez wyłączenie części instytucji finansowych spod zakresu DORA), jak i przedmiotowego, nakazując podmiotom nią objętym stosowanie jej zgodnie z zasadą proporcjonalności. To ostatnie zostało wyrażone w art. 4, zgodnie z którym podmioty finansowe stosują przepisy dotyczące zarządzania ryzykiem związanym z ICT zgodnie z zasadą proporcjonalności, biorąc pod uwagę swoją wielkość i ogólny profil ryzyka oraz charakter, skalę i stopień złożoności swoich usług, działań i operacji.

13 Ibidem, motyw 40.
14 Ibidem, motyw 41.
15 Ibidem, motyw 64.

Dodatkowo podmioty finansowe stosują regulację DORA dotyczącą zarządzania incydentami związanymi z ICT, testowania operacyjnej odporności cyfrowej oraz najważniejszych zasad prawidłowego zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT w sposób proporcjonalny do swojej wielkości i ogólnego profilu ryzyka oraz charakteru, skali i stopnia złożoności swoich usług, działań i operacji, jak szczegółowo przewidziano w odpowiednich przepisach tych rozdziałów. Ponadto stworzono mechanizm monitorowania stosowania zasady proporcjonalności, przewidując, że właściwe organy analizują stosowanie zasady proporcjonalności przez podmioty finansowe podczas dokonywania przeglądu spójności ram zarządzania ryzykiem związanym z ICT na podstawie sprawozdań przedkładanych na żądanie właściwych organów. Uzupełnieniem podejścia do zasady proporcjonalności wyrażonej w art. 4 DORA jest jej art. 7 lit. a przewidujący wykorzystywanie przez podmioty finansowe i utrzymywanie zaktualizowanych systemów, protokołów i narzędzi ICT, które są odpowiednie do skali operacji wspierających prowadzenie ich działalności, zgodnie z zasadą proporcjonalności, a także jej art. 28 ust. 1 lit. b przewidujący, że zarządzanie przez podmioty finansowe ryzykiem ze strony zewnętrznych dostawców usług ICT odbywa się zgodnie z zasadą proporcjonalności, z uwzględnieniem charakteru, skali, stopnia złożoności i znaczenia zależności w zakresie ICT, a także ryzyka wynikającego z ustaleń umownych dotyczących korzystania z usług ICT zawartych z zewnętrznymi dostawcami tych usług, biorąc pod uwagę krytyczność lub istotność danej usługi, procesu lub funkcji oraz potencjalny wpływ na ciągłość i dostępność usług finansowych i działalności finansowej na poziomie indywidualnym i grupowym.

Innym przejawem zastosowania w DORA zasady proporcjonalności jest jej art. 16, który przewiduje w stosunku do wskazanych w nim podmiotów stosowanie uproszczonych ram zarządzania ryzykiem związanym z ICT, ale ze względu na jego podmiotowy charakter (nie stosuje się go do wszystkich instytucji finansowych, a jedynie do określonych w nim wąskich kategorii podmiotów) zostanie on omówiony odrębnie w dalszej części.

W konsekwencji wyżej opisanego określonego podejścia do zasady proporcjonalności od strony podmiotowej w art. 2 ust. 3 DORA wyłączono z zakresu regulacji DORA następujące podmioty: zarządzających alternatywnymi funduszami inwestycyjnymi (ZAFI), zarządzających portfelami alternatywnych funduszy inwestycyjnych (AFI) (bezpośrednio albo za pośrednictwem przedsiębiorstwa, z którym ZAFI jest powiązany poprzez wspólne zarządzanie lub kontrolę albo poprzez znaczny, posiadany bezpośrednio bądź pośrednio pakiet akcji), gdy łączna wartość zarządzanych aktywów, w tym aktywów

nabytych za pomocą dźwigni finansowej, ogółem nie przekracza progu 100 mln EUR; lub ZAFI zarządzających portfelami AFI (bezpośrednio albo za pośrednictwem przedsiębiorstwa, z którym ZAFI jest powiązany poprzez wspólne zarządzanie lub kontrolę albo poprzez znaczny, posiadany bezpośrednio bądź pośrednio, pakiet akcji), gdy łączna wartość zarządzanych aktywów nie przekracza progu 500 mln EUR, gdy portfele AFI składają się z AFI, które nie stosują dźwigni finansowej i w których prawa do umorzenia nie mogą być wykonywane przez okres 5 lat od daty początkowej inwestycji w każdy AFI, ponadto zakłady ubezpieczeń i zakłady reasekuracji, w których roczna składka przypisana brutto zakładu nie przekracza 5 mln EUR; łączne rezerwy techniczno-ubezpieczeniowe brutto zakładu (z uwzględnieniem udziału reasekuratorów i spółek celowych) nie przekraczają 25 mln EUR, a jeżeli zakład należy do grupy, to łączne rezerwy techniczno-ubezpieczeniowe grupy (z uwzględnieniem udziału reasekuratorów i spółek celowych) nie przekraczają 25 mln EUR, ponadto działalność zakładu nie obejmuje ubezpieczania lub reasekuracji oraz ryzyka kredytów i poręczeń, chyba że stanowią one ryzyka dodatkowe; a także działalność zakładu w ramach reasekuracji czynnej nie przekracza 0,5 mln EUR składki przypisanej brutto ani 2,5 mln EUR rezerw techniczno-ubezpieczeniowych brutto, z uwzględnieniem udziału reasekuratorów i spółek celowych, ani składka przypisana brutto zakładu reasekuracji czynnej nie przekracza 10% składki przypisanej brutto, ani 10% rezerw techniczno-ubezpieczeniowych brutto, z uwzględnieniem udziału reasekuratorów i spółek celowych; dodatkowo instytucje pracowniczych programów emerytalnych, które obsługują programy emerytalne liczące łącznie nie więcej niż 15 uczestników; a także osoby fizyczne lub prawne zwolnione zgodnie z art. 2 i 3 dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 roku w sprawie rynków instrumentów finansowych oraz zmieniającej dyrektywę 2002/92/WE i dyrektywą 2011/61/UE[16], pośredników ubezpieczeniowych, pośredników reasekuracyjnych i pośredników oferujących ubezpieczenia uzupełniające będących mikroprzedsiębiorstwami, małymi lub średnimi przedsiębiorstwami, a także instytucje świadczące żyro pocztowe.

W art. 2 ust. 4 DORA wprowadzono opcję narodową. Zgodnie z nią państwa członkowskie mogą wyłączyć z zakresu stosowania DORA podmioty, o których mowa w art. 2 ust. 5 pkt 4–23[17] dyrektywy Parlamentu Europejskiego

16 Dz. Urz. UE 2014, L 173, s. 349.

17 Dotyczy to w poszczególnych krajach członkowskich odpowiednio: „4) w Danii: »Eksport Kredit Fonden«, »Eksport Kredit Fonden A/S«, »Danmarks Skibskredit A/S« oraz

i Rady 2013/36/UE z dnia 26 czerwca 2013 roku w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi, zmieniającej dyrektywę 2002/87/WE i uchylającej dyrektywy 2006/48/WE oraz 2006/49/WE[18] (zwana dyrektywą bankową), mające siedzibę na ich odpowiednich terytoriach. Jeżeli państwo członkowskie korzysta z takiej możliwości, to informuje o tym Komisję oraz o wszelkich późniejszych zmianach w tym względzie. Komisja podaje te informacje do wiadomości publicznej na swojej stronie internetowej lub za pomocą innych łatwo dostępnych środków. Opcja ta rodzi istotne problemy interpretacyjne w kontekście relacji art. 2 ust. 4 z art. 2 ust. 1 DORA. Artykuł 2 ust. 4 DORA ma zastosowanie do podmiotów wyłączonych w poszczególnych

»KommuneKredit«; 5) w Niemczech: »Kreditanstalt für Wiederaufbau«, »Landwirtschaftliche Rentenbank«, »Bremer Aufbau-Bank GmbH«, »Hamburgische Investitions- und Förderbank«, »Investitionsbank Berlin«, »Investitionsbank des Landes Brandenburg«, »Investitionsbank Schleswig-Holstein«, »Investitions- und Förderbank Niedersachsen – NBank«, »Investitions- und Strukturbank Rheinland-Pfalz«, »Landeskreditbank Baden-Württemberg – Förderbank«, »LfA Förderbank Bayern«, »NRW.BANK«, »Saarländische Investitionskreditbank AG«, »Sächsische Aufbaubank – Förderbank«, »Thüringer Aufbaubank«, przedsiębiorstw uznanych na podstawie »Wohnungsgemeinnützigkeits-gesetz« za organy realizujące politykę mieszkaniową państwa, których główną działalnością nie są operacje bankowe, oraz przedsiębiorstw uznanych w tej ustawie za niekomercyjne przedsiębiorstwa mieszkaniowe; 6) w Estonii: »hoiu-laenuühistud« jako przedsiębiorstwa spółdzielcze, które są uznane w ramach »hoiu-laenuühistu seadus«; 7) w Irlandii: »the Strategic Banking Corporation of Ireland«, »credit unions« i »friendly societies«; 8) w Grecji: »Ταμείο Παρακαταθηκών και Δανείων« (Tamio Parakatathikon kai Danion); 9) w Hiszpanii: »Instituto de Crédito Oficial«; 10) we Francji: »Caisse des dépôts et consignations«; 11) w Chorwacji: »kreditne unije« oraz »Hrvatska banka za obnovu i razvitak«; 12) we Włoszech: »Cassa depositi e prestiti«; 13) na Łotwie: »krājaizdevu sabiedrības«, przedsiębiorstw uznanych w ramach »krājaizdevu sabiedrību likums« za przedsiębiorstwa spółdzielcze świadczące usługi finansowe wyłącznie na rzecz swoich członków; 14) na Litwie: »kredito unijos« innych niż »centrinės kredito unijos«; 15) na Węgrzech: »MFB Magyar Fejlesztési Bank Zártkörűen Működő Részvénytársaság« oraz »Magyar ExportImport Bank Zártkörűen Működő Részvénytársaság«; 16) na Malcie: »The Malta Development Bank«; 17) w Niderlandach: »Nederlandse Investeringsbank voor Ontwikkelingslanden NV«, »NV Noordelijke Ontwikkeling-smaatschappij«, »NV Limburgs Instituut voor Ontwikkeling en Financiering«, »Ontwikkelingsmaatschappij Oost-Nederland NV« oraz »kredietunies«; 18) w Austrii: przedsiębiorstw uznanych za towarzystwa mieszkaniowe działające w interesie publicznym oraz »Österreichische Kontrollbank AG«; 19) w Polsce: Spółdzielczych Kas Oszczędnościowo-Kredytowych oraz Banku Gospodarstwa Krajowego; 20) w Portugalii: »Caixas Económicas« istniejących w dniu 1 stycznia 1986 r., z wyjątkiem tych, które zostały założone jako spółki z ograniczoną odpowiedzialnością, i z wyjątkiem »Caixa Económica Montepio Geral«; 21) w Słowenii: »SID – Slovenska izvozna in razvojna banka, d.d. Ljubljana«; 22) w Finlandii: »Teollisen yhteistyön rahasto Oy/Fonden för industriellt samarbete AB« oraz »Finnvera Oyj/Finnvera Abp«; 23) w Szwecji: »Svenska Skeppshypotekskassan«".

18 Dz. Urz. UE 2013, L 176, s. 338.

krajach spod regulacji dyrektywy bankowej. Jednakże, żeby móc te podmioty wyłączyć decyzją państwa członkowskiego spod zakresu obowiązywania DORA, powinny one być wcześniej objęte jej zakresem zgodnie z art. 2 ust. 1 DORA. W art. 3 pkt 32 DORA instytucje te zostały zdefiniowane jako instytucje zwolnione zgodnie z dyrektywą 2013/36/UE (czyli zgodnie z dyrektywą bankową). Natomiast art. 2 ust. 1 DORA nie obejmuje instytucji zwolnionych zgodnie z dyrektywą bankową jako instytucje finansowe objęte zakresem DORA. Co prawda zgodnie z art. 2 ust. 1 lit. a DORA ma ona zastosowanie do instytucji kredytowych, ale art. 3 pkt 31 DORA definiuje instytucję kredytową jako instytucję kredytową zdefiniowaną w art. 4 ust. 1 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 roku w sprawie wymogów ostrożnościowych dla instytucji kredytowych, zmieniającego rozporządzenie (UE) nr 648/2012[19] (zwane CRR). Natomiast zgodnie z art. 1 CRR rozporządzenie to wprowadza jednolity zbiór przepisów dla wymienionych w nim podmiotów objętych nadzorem na podstawie dyrektywy bankowej. W konsekwencji jeżeli CRR dotyczy wyłącznie podmiotów objętych nadzorem na podstawie dyrektywy bankowej, to również definicja zawarta w jego art. 1 ust. 1 pkt 1 dotyczy wyłącznie tych podmiotów, zatem *a contrario* – nie dotyczy podmiotów, o których mowa w art. 2 ust. 5 dyrektywy bankowej, w tym w poszczególnych krajach podmiotów wymienionych w art. 2 ust. 5 pkt 4–23 dyrektywy bankowej[20]. W efekcie dotychczas w przypadku podmiotów, o których mowa w art. 2 ust. 5 pkt 4–23 dyrektywy bankowej konsekwentnie nie stosowano przepisów mających zastosowanie właśnie do instytucji kredytowych zdefiniowanych w art. 4 ust. 1 pkt 1 CRR[21]. Taka sytuacja ma np. miejsce w odniesieniu do dyrektywy Parlamentu Europejskiego i Rady (UE) 2021/2167z dnia 24 listopada 2021 roku w sprawie podmiotów obsługujących kredyty i nabywców kredytów oraz w sprawie zmiany dyrektyw 2008/48/WE i 2014/17/UE[22], która ma zastosowanie do kredytodawców będących instytucjami kredytowymi zgodnie z definicją w art. 4 ust. 1 pkt 1

19 Ibidem, s. 1.

20 Zgodnie z art. 2 ust. 5 pkt 19 dyrektywy bankowej w Polsce wyłączenie to dotyczy spółdzielczych kas oszczędnościowo-kredytowych oraz Banku Gospodarstwa Krajowego.

21 Por.: A. Jurkowska-Zeidler, *Komentarz do art. 2* [w:] *Prawo bankowe. Komentarz*, red. A. Miko-Sitek, P. Zapadka, Warszawa 2022, s. 26–27; P. Pelc, *Nadzór Komisji Nadzoru Finansowego nad spółdzielczymi kasami oszczędnościowo-kredytowymi a nadzór nad otwartymi funduszami emerytalnymi* [w:] *Prawo prywatne w służbie społeczeństwu. Księga poświęcona pamięci Profesora Adama Jedlińskiego*, red. P. Zakrzewski, D. Bierecki, Sopot 2019, s. 235.

22 Dz. Urz. UE 2021, L 438, s. 1.

CRR, a nie ma zastosowania do kredytodawców, o których mowa w art. 2 ust. 5 pkt 4–23 dyrektywy bankowej. W związku z powyższym negatywnie należy ocenić sposób określenia zakresu podmiotowego DORA, gdyż w konsekwencji może to w przyszłości prowadzić do problemów interpretacyjnych w odniesieniu do innych unijnych aktów prawnych zawierających odwołania do definicji instytucji kredytowej zawartej w art. 4 ust. 1 pkt 1 CRR.

Jeżeli państwo członkowskie nie skorzysta z opcji narodowej określonej w art. 2 ust. 4 DORA, to do instytucji zwolnionych zgodnie z dyrektywą bankową będzie miał zastosowanie wspominany wyżej art. 16 DORA. Ponadto będzie miał on zastosowanie do instytucji płatniczych zwolnionych przez państwa członkowskie ze stosowania części regulacji dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 roku w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającej dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE[23] (PSD2)[24], instytucji pieniądza elektronicznego zwolnionych w ramach opcji narodowych przez państwa członkowskie ze stosowania części obowiązków wynikających z dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 roku w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniającej dyrektywy 2005/60/WE i 2006/48/WE oraz uchylającej dyrektywę 2000/46/WE[25] oraz małych instytucji pracowniczych programów emerytalnych. Do wszystkich tych instytucji będą miały zastosowanie zgodnie z art. 16 DORA uproszczone ramy zarządzania ryzykiem związanym z ICT. Oznacza to, że nie będą do nich miały zastosowania zasady zarządzania ryzykiem związanym z ICT określone w art. 5–15 DORA, a zamiast tego ustawodawca europejski oczekuje, że instytucje te: wprowadzają i utrzymują prawidłowe i udokumentowane ramy zarządzania ryzykiem związanym z ICT, które wyszczególniają mechanizmy i środki mające na celu szybkie, skuteczne i kompleksowe zarządzanie ryzykiem związanym z ICT, w tym w celu ochrony odpowiednich elementów fizycznych i infrastruktury, stale monitorują bezpieczeństwo i funkcjonowanie wszystkich

23 Ibidem, 2015, L 337, s. 35.

24 W przypadku tych instytucji nie powstaje problem opisany w odniesieniu do instytucji kredytowych zwolnionych na podstawie dyrektywy bankowej, dlatego że są one instytucjami płatniczymi, a jedynie w ramach opcji narodowych państwa w stosunku do nich wyłączyły stosowanie części regulacji PSD2.

25 Ibidem 2009, L 267, s. 7.

systemów ICT, 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, umożliwiają szybką identyfikację i wykrywanie źródeł ryzyka związanego z ICT i nieprawidłowości w sieci i systemach informatycznych oraz szybkie reagowanie na incydenty związane z ICT, określają kluczowe zależności od zewnętrznych dostawców usług ICT, zapewniają ciągłość krytycznych lub istotnych funkcji poprzez plany ciągłości działania oraz środki reagowania i przywracania sprawności, które obejmują co najmniej środki zarządzania kopiami zapasowymi i środki odtwarzania; regularnie testują powyższe plany i środki oraz skuteczność działań wdrożonych w ramach stawianych im wymogów, a także wdrażają, stosownie do przypadku, odpowiednie wnioski operacyjne wynikające z testów oraz wnioski z analiz przeprowadzonych po wystąpieniu incydentu do procesu oceny ryzyka związanego z ICT i opracowują, stosownie do potrzeb i profilu ryzyka związanego z ICT, programy zwiększania świadomości w zakresie bezpieczeństwa ICT oraz szkoleń z operacyjnej odporności cyfrowej dla pracowników i kadry zarządzającej. Oczekuje się także od nich stosownego dokumentowania i poddawania okresowym przeglądom ram zarządzania ryzykiem związanym z ICT przez te instytucje.

Zasada proporcjonalności prowadzi także do wyłączenia podmiotów określonych w art. 16 DORA spod ogólnych regulacyjnych standardów technicznych (RTS) opracowywanych przez Europejskie Urzędu Nadzoru na podstawie art. 15 DORA i poddanie ich RTS adresowanym specjalnie do tych podmiotów (art. 16 ust. 3 DORA), a także spod obowiązku prowadzenia testów penetracyjnych (art. 26 ust. 1 DORA – wyłączenie to dotyczy dodatkowo także mikroprzedsiębiorstw) i strategii dotyczącej ryzyka ze strony zewnętrznych dostawców usług ICT (art. 28 ust. 2 DORA – wyłączenie to dotyczy dodatkowo także mikroprzedsiębiorstw).

Należy, co do zasady, pozytywnie ocenić sposób, w jaki DORA wprowadza zasadę proporcjonalności – pozwala ona bowiem instytucjom finansowym dopasować sposób stosowania DORA zarówno do ich skali działania, jak i charakteru działalności, jednocześnie umożliwia powszechne stosowanie DORA, ze względu na ryzyko zarażania. Pozytywnie należy też ocenić uproszczone zasady dla najmniejszych podmiotów lub podmiotów prowadzących ograniczoną działalność. Natomiast negatywnie należy ocenić sposób uregulowania sytuacji instytucji wyłączonych zgodnie z dyrektywą bankową. W tym

zakresie wyraźnie zabrakło precyzji – podmiotów tych wprost nie włączono do art. 2 ust. 1 DORA określającego zakres podmiotowy regulacji, a mimo to uznano, że do tego żeby jej nie podlegały, konieczne jest wyłączenie ich w ramach opcji narodowych przez państwa członkowskie.

Bibliografia

Grzeszczak R., *Komentarz do art. 5* [w:] *Traktat o Unii Europejskiej. Komentarz*, red. D. Kornobis-Romanowska, Warszawa 2023.

Jurkowska-Zeidler A., *Komentarz do art. 2* [w:] *Prawo bankowe. Komentarz*, red. A. Miko-Sitek, P. Zapadka, Warszawa 2022.

Pelc P., *Cyberbezpieczeństwo instytucji finansowych w wymiarze krajowym i międzynarodowym* [w:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, red. M. Karpiuk, Warszawa 2024.

Pelc P., *Nadzór Komisji Nadzoru Finansowego nad spółdzielczymi kasami oszczędnościowo-kredytowymi a nadzór nad otwartymi funduszami emerytalnymi* [w:] *Prawo prywatne w służbie społeczeństwu. Księga poświęcona pamięci Profesora Adama Jedlińskiego*, red. P. Zakrzewski, D. Bierecki, Sopot 2019.

Pelc P., *Wpływ planowanych przez UE działań i regulacji na instytucje finansowe w Polsce*, „Cybersecurity and Law" 2021, nr 1.

Urban-Theocharakis M., *Pakiet CRRII/ CRD V a wzmocnienie zasady proporcjonalności*, LEX/el. 2019.

Proportionality Rule in DORA

Abstract

DORA covers a wide range of financial entities of varying size, scale and subject of action. As a result, it is particularly important to include the principle of proportionality, resulting from the Treaty on European Union, in its regulation. This principle applies to both the subjective and the objective scope of DORA. As a result, its use allows financial institutions to adapt the use of DORA to both their scale of operation and the nature of their business, while allowing widespread use of DORA, due to the risk of contagion. Simplified rules should also be assessed positively for the smallest operators or entities with limited activities. Only the regulation concerning institutions exempted under the banking directive is flawed – their situation is regulated without taking into consideration that such institutions are excluded from the scope of the CRR regulation, which contains the definition of a credit institution, to which DORA refers specifying the subjective scope.

Key words: DORA, proportionality, financial institutions, cybersecurity