Europejski Przegląd Prawa i Stosunków Międzynarodowych
Europejska Wyższa Szkoła Prawa i Administracji w Warszawie
nr 3/2024/71

Dominik Bierecki*

Zasada proporcjonalności w stosowaniu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act – DORA)

[Principle of Proportionality in the Application of the Digital Operational Resilience Act (DORA)]

Abstract

The Digital Operational Resilience Act (DORA) – Regulation of the European Parliament and of the Council imposes a number of obligations on financial entities related to information and communication technology (ICT) security. However, some of these entities are excluded from the scope of DORA, e.g. due to the size of their capital or assets under management. Others may be excluded from the scope of DORA by a Member State under a national option. In addition, the legal standards of DORA express the principle of proportionality and indicate which characteristics of a financial entity are to be taken into account in fulfilling the obligations under DORA. The aim of the article is to present these obligations and the rationale under which the principle of proportionality applies to the entities regulated by this legal act. The research thesis of the article is that the principle of proportionality is regulated in DORA in a multifaceted manner. The article uses the dogmatic-legal method.

Keywords: DORA, principle of proportionality, credit unions.

Cel i teza badawcza

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14 grudnia 2022 roku 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], zwane DORA (Digital Opera-

* **Dominik Bierecki** – dr hab. nauk prawnych, profesor uczelni, Uniwersytet Pomorski w Słupsku (afiliacja) / PhD in Legal Sciences, Associate Professor, Pomeranian University in Słupsk (affiliation); https://orcid.org/0000-0001-6993-3974; dominik.bierecki@upsl.edu.pl.

tional Resiliance Act), ma na celu zabezpieczenie podmiotów rynku finansowego przed zagrożeniami, jakie wynikają z rozwoju nowych technologii informacyjno-komunikacyjnych (ICT – Information and Communication Technology). Realizacja tego celu ma nastąpić przez ustanowienie jednolitych wymogów bezpieczeństwa sieci i systemów teleinformatycznych wspierających procesy biznesowe podmiotów finansowych. Celem tych wymogów jest osiągnięcie wysokiego i wspólnego poziomu operacyjnej odporności cyfrowej (art. 1 ust. 1 DORA). Przez operacyjną odporność cyfrową należy rozumieć umiejętność podmiotu finansowego[2] do budowania, gwarantowania i weryfikowania swojej operacyjnej integralności i niezawodności przez bezpośrednie lub pośrednie zapewnianie pełnego zakresu zdolności w obszarze technologii informacyjno-komunikacyjnych (ICT) do zapewniania bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy w celu wspierania ciągłości świadczenia usług finansowych i ich jakości (art. 3 pkt 1 DORA). We wniosku Komisji Europejskiej z 24 września 2020 r.[3] dotyczącym DORA wskazano, że cyfryzacja i odporność operacyjna podmiotów finansowych są ze sobą związane, gdyż z technologiami informacyjno-komunikacyjnymi wiążą się jednocześnie szanse i zagrożenia. DORA nakłada na podmioty finansowe szereg obowiązków, których wykonanie ma doprowadzić do wzmocnienia operacyjnej odporności cyfrowej tych podmiotów. Obowiązki te są zawarte w rozdziałach II–V DORA, które obejmują regulacje:

1. Zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (rozdział II),
2. Zarządzania incydentami związanymi z technologiami informacyjno-komunikacyjnymi (rozdział III),
3. Testowania operacyjnej odporności cyfrowej (rozdział IV),
4. Zarządzania ryzykiem ze strony zewnętrznych dostawców usług technologii informacyjno-komunikacyjnej (rozdział V).

Niektóre z podmiotów finansowych w rozumieniu DORA są wyłączone z zakresu obowiązywania tego rozporządzenia. Jednocześnie art. 4 DORA wyraża zasadę proporcjonalności w stosowaniu przepisów tego rozporządzenia (proporcjonalność w stosowaniu DORA została także zaznaczona w motywach 42, 43, 53, 64 i 105 DORA). Prowadzi to do dostosowania realizacji obowiązku nałożonego przez przepis DORA do skali podmiotu finansowego ze względu na jego wielkość i ogólny profil ryzyka oraz charakter, skalę oraz stopień złożoności wykonywanych przez podmiot finansowy usług, działań i operacji. Celem artykułu jest omówienie przesłanek stosowania zasady proporcjonalności na

[1] Dz. Urz. UE z 27 grudnia 2022 r., L 333/1.

[2] Zgodnie z art. 2 ust. 2 DORA podmiotami finansowymi w rozumieniu DORA są podmioty wymienione w art. 2 ust. 1 lit. a–t tego rozporządzenia.

[3] Wniosek rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014, COM/2020/595 final.

gruncie DORA i ustalenie, w jaki sposób zasada proporcjonalności wpływa na ograniczenie stosowania norm prawnych DORA. Teza badawcza artykułu stanowi, że proporcjonalność w stosowaniu DORA jest uregulowana wielopłaszczyznowo: przez wyłączenie podmiotu finansowego z zakresu regulacji przepisów DORA lub przez wyłączenie zastosowania obowiązku wynikającego z normy DORA w stosunku do danego podmiotu finansowego ze względu na jego konkretne cechy. Artykuł został przygotowany z wykorzystaniem metody dogmatycznoprawnej.

Wyłączenie z zakresu regulacji DORA

Zasada proporcjonalności wiąże się z podmiotowym zakresem stosowania DORA. Zgodnie z art. 2 ust. 1 DORA rozporządzenie to ma zastosowanie do różnych podmiotów rynku finansowego, np. instytucji kredytowych i firm inwestycyjnych w rozumieniu prawa UE[4], zakładów ubezpieczeń, pośredników ubezpieczeniowych i reasekuracyjnych oraz podmiotów zarządzających alternatywnymi funduszami inwestycyjnymi (ZAFI). Jednak zgodnie z art. 2 ust. 3 DORA podmiotów tych dotyczą różne wyłączenia przedmiotowe z zastosowania DORA, np. ze względu na wartość ich kapitału (zakłady ubezpieczeń – art. 4 dyrektywy 2009/138/WE[5]) albo zarządzanych aktywów (ZAIF – art. 3 ust. 2 dyrektywy 2011/61/UE[6]), a także status mikroprzedsiębiorcy, małego przedsiębiorcy bądź średniego przedsiębiorcy (pośrednicy ubezpieczeniowi lub reasekuracyjni – art. 2 ust. 3 lit. e DORA). Poza tym prawodawca UE pozostawia państwom członkowskim możliwość wyłączenia z zakresu stosowania DORA unii kredytowych (*credit unions*), którymi w Polsce są spółdzielcze kasy oszczędnościowo-kredytowe, czyli SKOK (opcja narodowa). Zgodnie bowiem z art. 2 ust. 4 DORA państwa członkowskie mogą wyłączyć z zakresu stosowania niniejszego rozporządzenia podmioty, o których mowa w art. 2 ust. 5 pkt 4–23 dyrektywy 2013/36/UE[7], mające siedzibę na ich odpowiednich

[4] Definicja instytucji kredytowej zawarta jest w art. 4 ust. 1 pkt 1 CRR (rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z 26 czerwca 2013 roku w sprawie wymogów ostrożnościowych dla instytucji kredytowych, zmieniającego rozporządzenie (UE) nr 648/2012, Dz. Urz. UE z 27 czerwca 2013 r., L 176, 1. Definicję firmy inwestycyjnej wyraża natomiast art. 4 ust. 1 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE z 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniający dyrektywę 2002/92/WE i dyrektywę 2011/61/UE, Dz. Urz. UE z 12 czerwca 2014 r., L 173, 349.

[5] Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II), Dz. Urz. UE z 17 grudnia 2009 r., L 335, 1.

[6] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2011/61/UE z 8 czerwca 2011 r. w sprawie zarządzających alternatywnymi funduszami inwestycyjnymi i zmiany dyrektyw 2003/41/WE i 2009/65/WE oraz rozporządzeń (WE) nr 1060/2009 i (UE) nr 1095/2010, Dz. Urz. UE z 1 lipca 2011 r., L 174, 1.

[7] Dyrektywa 2013/36/UE w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrek-

terytoriach (w Polsce SKOK, a także Bank Gospodarstwa Krajowego – art. 2 ust. 5 pkt 19 dyrektywy 2013/36/UE)[8]. Pojęcie „unia kredytowa" jest używane do zbiorczego określenia podmiotów, które są demokratycznie kontrolowane przez swoich członków i prowadzą działalność *not for profit*[9] – polegającą na świadczeniu wyłącznie na rzecz swoich członków usług finansowych w postaci udzielania pożyczek i przyjmowania depozytów na prowadzone przez unię rachunki[10]. Polskie ustawodawstwo dopuszcza używanie przez SKOK nazwy unia kredytowa dla określenia swojej działalności lub reklamy (art. 5 ust. 2 ustawy z 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych[11]). Natomiast w projekcie ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego[12] (wdrażającej DORA[13]) ustawodawca polski nie korzysta z opcji narodowej wyłączenia unii kredytowych (SKOK), a także Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej (Kasy Krajowej)[14] z zakresu DORA. Projekt ten przewiduje bowiem nadanie KNF kompetencji przeprowadzenia w SKOK i Kasie Krajowej kontroli zgodności działalności z przepisami rozporządzenia 2022/2554 w zakresie zapewnienia operacyjnej odporności cyfrowej sektora finansowego (art. 5 pkt 6 projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego).

Prawodawca europejski odwołuje się więc do traktatowej zasady proporcjonalności (art. 5 TUE[15]) – uznając, że bezwzględne stosowanie DORA może być nieodpowiednie w stosunku do niektórych podmiotów finansowych. Wydaje się, że występuje tu przejaw charakteru zasady proporcjonalności polegającego na wyznaczaniu granic ingerencji unijnych i krajowych władz publicznych w sferę wolności jednostki[16]. We wniosku Komisji Europejskiej z 24 września 2020 r.[17] zaznaczono, że pod względem zakresu proporcjonalność DORA polega

---

tywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE, Dz. Urz. UE z 27 czerwca 2013 r., L 176/338.

[8] Zob. P. Pelc, *Zasada proporcjonalności w* DORA, „Cybersecurity and Law" 2024, 2, 12, ss. 207–218.

[9] Działalność *not for profit* polega na uzyskiwaniu zysku (nadwyżki bilansowej) z prowadzonej działalności gospodarczej i obligatoryjnym jego przeznaczaniu na dalszą działalność przedsiębiorcy, bez możliwości podziału dywidendy. Zob. B. Bátiz-Lazo, M. Billings, *New perspectives on not-for-profit financial institutions: Organizational form, performance and governance*, „Business History" 2012, 3, 54, s. 311; D. Bierecki, *Konsekwencje prawne uzyskania przez spółdzielnię statusu przedsiębiorstwa społecznego*, „Krytyka Prawa" 2023, 15, 3, ss. 197–202.

[10] Taka definicja unii kredytowej jest przyjęta w statucie Światowej Rady Związków Kredytowych (*World Council of Credit Unions*). Zob. art. II. 2.3. Bylaws of World Council of Credit Unions Inc. https://www.woccu.org/member_services/our_network/membership/join [dostęp: 17.03.2024].

[11] Tekst jedn. Dz.U. 2024, poz. 512 ze zm., dalej: ustawa o SKOK.

[12] https://legislacja.gov.pl/projekt/12384252/katalog/13053516#13053516 [dostęp: 7.06.2024].

[13] Stosowanie DORA rozpocznie się 17 stycznia 2025 r. (art. 64 DORA).

[14] Kasa Krajowa to spółdzielnia osób prawnych, w której obligatoryjnie zrzeszają się wszystkie SKOK (art. 41 ust. 1 i 2 ustawy o SKOK). Zob. D. Bierecki [w:] System prawa prywatnego, tom 21, Prawo spółdzielcze, red. K. Pietrzykowski, Warszawa 2020, ss. 995–1038.

[15] Traktat o Unii Europejskiej podpisany w Maastricht 7 lutego 1992 r., Dz.U. 2004, nr 90, poz. 864.

[16] Zob. D. Miąsik, System prawa Unii Europejskiej, tom 2, Zasady i prawa podstawowe, Warszawa 2022, s. 187.

[17] Wniosek rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sek-

na kryteriach oceny jakościowej i ilościowej oraz dostosowuje przepisy DORA do ryzyka oraz potrzeb wynikających z właściwości podmiotów finansowych z punktu widzenia ich rozmiaru i profilu działalności. Dla przykładu, w wypadku unii kredytowych (SKOK) należy wziąć pod uwagę, że świadczą one ograniczone w stosunku do banków rodzaje usług finansowych jedynie dla określonej grupy osób – członków unii (art. 3 ust. 1 i 1a ustawy o SKOK)[18].

Wyłączenie obowiązków z DORA

Z drugiej strony art. 4 ust. 1 i 2 DORA wyraża zasadę proporcjonalności w stosowaniu przepisów tego rozporządzenia. Przepis ten nie wiąże proporcjonalnego stosowania DORA z rodzajem podmiotu finansowego, ale z jego cechami. Wystąpienie tych cech może powodować, że realizacja obowiązków z DORA nie będzie konieczna do zachowania operacyjnej odporności cyfrowej danego podmiotu finansowego. Chodzi tu o cechy konkretnego podmiotu, niepowiązane z jego rodzajem ani charakterem prawnym. Do tych cech art. 4 ust. 1 i 2 DORA zalicza: wielkość i ogólny profil ryzyka podmiotu, charakter, skalę oraz stopień złożoności jego usług, działań i operacji.

Należy zauważyć, że stosowanie DORA wiązać się będzie z wykonywaniem kompetencji organów nadzoru w stosunku do podmiotów finansowych. W stosunku do spółdzielczych kas oszczędnościowo-kredytowych (unii kredytowych) już z ustawy o SKOK wynika obowiązek Komisji Nadzoru Finansowego (KNF) stosowania środków nadzorczych adekwatnie do stopnia skomplikowania prowadzonej przez SKOK działalności i występującej w tej działalności skali ryzyka. Skalę tę ustala się według zakresu działalności SKOK ustalonego na podstawie sumy bilansowej i liczby członków. W taki sposób ustala się status małej kasy (art. 1a pkt 5 ustawy o SKOK). Jednak obowiązek zachowania adekwatności środków nadzoru KNF nad SKOK-ami nie ogranicza się wyłącznie do małych kas. Podobnie, proporcjonalne stosowanie DORA nie powinno doznać takich ograniczeń.

Na podstawie art. 4 ust. 1 i 2 DORA proporcjonalne stosowanie przepisów tego rozporządzenia dotyczy rozdziału II o zarządzaniu ryzykiem związanym z technologiami informacyjno-komunikacyjnymi, rozdziału III o zarządzaniu incydentami związanymi z tymi technologiami, rozdziału IV o testowaniu operacyjnej odporności cyfrowej i sekcji 1 rozdziału V o zarządzaniu ryzykiem ze strony zewnętrznych dostawców usług technologii informacyjno-komunikacyjnych.

tora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014, COM/2020/595 final, s. 4.

[18] Zob. P. Zakrzewski [w:] A. Herbet, S. Pawłowski, P. Zakrzewski, Spółdzielcze kasy oszczędnościowo-kredytowej, Komentarz, Warszawa 2024, ss. 26–42.

Proporcjonalne stosowanie przepisów rozdziału II DORA oznacza ustalenie wystarczającego spełnienia wymogów tego rozporządzenia w stosunku do konkretnego podmiotu finansowego ze względu na jego wielkość, ogólny profil ryzyka, charakter, skalę oraz stopień złożoności jego usług, działań i operacji. Normy prawne rozdziału II DORA pozostawiają ocenie podmiotów finansowych i organów nadzoru skalę wykonania obowiązków dotyczących zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi. Przeniesienie ciężaru oceny na adresatów norm prawnych polega na obłożeniu ich obowiązkiem opracowania wewnętrznych ram zarządzania i kontroli oraz procedur wraz z określeniem celu ich wdrażania, ale bez wymienienia ich obligatoryjnej treści.

Wyłączenie natomiast w regulacji rozdziału II DORA o zarządzaniu ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (art. 5–15 DORA) dotyczy unii kredytowych, gdy państwo członkowskie nie skorzysta z możliwości wyłączenia tych podmiotów z zakresu zastosowania DORA. Dotyczy to także rodzajów podmiotów finansowych, które obligatoryjnie stosują DORA, ale które w konkretnym przypadku spełniają warunki wyłączenia na gruncie przepisów pierwotnie je regulujących. Chodzi o małe i niepowiązane wzajemnie firmy inwestycyjne, instytucje płatnicze, instytucje pieniądza elektronicznego i małe instytucje pracowniczych programów emerytalnych (art. 16 ust. 1 DORA). Wymienione podmioty i unie kredytowe mają obowiązek stosowania uproszczonych ram zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (art. 16 ust. 1 lit. a–h DORA). Należy jednak zauważyć, że nie następuje w tym przypadku wyłączenie zastosowania art. 4 DORA. Wydaje się więc, że proporcjonalność stosowania DORA ze względu na cechy danego podmiotu, takie jak: wielkość, ogólny profil ryzyka, charakter, skala oraz stopień złożoności usług, działań i operacji dotyczy także stosowania wymogów uproszczonych.

Z kolei według art. 4 ust. 2 DORA proporcjonalność w stosowaniu rozdziału III, IV i sekcji 1 rozdziału V ma następować tak, jak szczegółowo przewidziano w odpowiednich przepisach tych rozdziałów. Przepisy te nie odnoszą się do proporcjonalności wprost, lecz do cech stanowiących podstawę proporcjonalnego stosowania DORA według art. 4. Przepisy te wskazują na przykład, że mając na uwadze skalę działalności podmiotu finansowego, należy określić wpływ incydentu technologii informacyjno-komunikacyjnej na jego działalność (art. 18 ust. 1 i 2 DORA).

Następnie należy zauważyć, że w przepisach rozdziału IV DORA bierze się pod uwagę, że przeprowadzenie testu podatności, wydajności, kompatybilności programu testowania operacyjnej odporności cyfrowej przez mikroprzedsiębiorcę powinno nastąpić z uwzględnieniem utrzymania równowagi między skalą zasobów i czasem, który należy przeznaczyć na testy, a pilnością, rodzajem ryzyka, krytycznością zasobów informacyjnych

i świadczonych usług (art. 25 ust. 3 DORA). Należy się tutaj doszukiwać proporcjonalności *sensu stricto* – ustaliwszy, czy koszty testu: zasoby i czas nie doprowadzą do nadmiernego obciążenia podmiotu finansowego w stosunku do pilności testu, rodzaju występującego ryzyka, krytyczności zasobów informacyjnych i świadczonych usług[19]. Ten stosunek należy ustalić z uwzględnieniem charakteru, skali oraz stopnia złożoności usług podmiotu finansowego, jego działań i operacji – czyli w świetle cech wymienionych przez art. 4 DORA.

Przepisy rozdziału IV DORA nakazują również podmiotom finansowym określać częstotliwość audytów i kontroli u zewnętrznych dostawców usług technologii informacyjno-kumunikacyjnej – z podejściem opartym na analizie ryzyka. Taka analiza może być przeprowadzona z uwzględnieniem ogólnego profilu ryzyka podmiotu finansowego (art. 25 ust. 3 DORA). Przepisy rozdziału IV DORA nadają także kompetencję do zmniejszenia lub zwiększenia częstotliwości przeprowadzania testów penetracyjnych pod kątem wyszukiwania zagrożeń (TLPT), które według DORA powinny być przeprowadzane nie rzadziej niż co trzy lata, mając na uwadze konieczność przeprowadzania tych testów ze względu na profil ryzyka danego podmiotu finansowego (art. 26 ust. 1 DORA).

Ponadto należy zauważyć, że przepisy rozdziału V DORA nakazują podmiotom finansowym zarządzać ryzykiem ze strony zewnętrznych dostawców usług technologii informacyjno-komunikacyjnej zgodnie z zasadą proporcjonalności, z uwzględnieniem charakteru, skali, stopnia złożoności i znaczenia zależności w zakresie technologii informacyjno-komunikacyjnej (art. 28 ust. 1 lit. b pkt i DORA).

Także w ramach regulacji zawartych w rozdziałach III i V, podobnie jak w przypadku rozdziału II, dochodzi do wyłączenia zastosowania norm DORA wobec: unii kredytowych, małych i niepowiązanych wzajemnie firm inwestycyjnych, instytucji płatniczych, instytucji pieniądza elektronicznego oraz małych instytucji pracowniczych programów emerytalnych. W tym przypadku wyłączenie zastosowania DORA obejmuje również mikroprzedsiębiorców. Wyłączenia te odnoszą się do obowiązku przeprowadzania testów penetracyjnych pod kątem wyszukiwania zagrożeń (TLPT) i przyjęcia strategii dotyczącej ryzyka ze strony zewnętrznych dostawców usług technologii informacyjno-komunikacyjnej (art. 26 ust. 1 i art. 28 ust. 2 DORA).

Pochodną zasady proporcjonalności z art. 4 DORA jest regulacja art. 28 ust. 10 DORA. Przepis ten nakłada na europejskie urzędy nadzoru obowiązek opracowania projektów standardów technicznych polityki korzystania z usług ICT od zewnętrznych dostawców. Projekty te powinny być opracowane z uwzględ-

[19] Na temat proporcjonalności *sensu stricto* jako elementu zasady proporcjonalności zob. J. Maliszewska-Nienartowicz, Zasada proporcjonalności jako podstawa oceny legalności ograniczeń swobód rynku wewnętrznego Unii Europejskiej, Toruń 2020, ss. 77–84.

nieniem wielkości i ogólnego profilu ryzyka podmiotu finansowego oraz charakteru, skali oraz stopnia złożoności jego usług, działań i operacji.

Wnioski

Przeprowadzona w artykule analiza potwierdza tezę badawczą o wielopłaszczyznowym uregulowaniu zasady proporcjonalności w stosowaniu DORA. Po pierwsze, proporcjonalność ta wynika z bezwzględnego wyłączenia zastosowania DORA do niektórych rodzajów podmiotów ryku finansowego. Po drugie, przejawem proporcjonalności w stosowaniu DORA jest przyznanie kompetencji państwom członkowskim do wyłączenia zastosowania DORA w stosunku do niektórych podmiotów, w tym unii kredytowych (SKOK). W przypadku nieskorzystania z tej kompetencji następuje wyłączenie zastosowania do tych podmiotów niektórych przepisów DORA i nałożenie uproszczonych norm zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (art. 16 ust. 1 DORA). Po trzecie, stosowanie DORA proporcjonalnie w stosunku do każdego rodzaju podmiotu finansowego powinno następować ze względu na jego konkretne cechy wymienione w art. 4 ust. 1 i 2 DORA. Dotyczy to nawet tych podmiotów finansowych, które stosują uproszczone normy zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi.

Trzeba mieć ponadto na uwadze dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2556 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii. Należy zauważyć, że zgodnie z art. 2 ust. 10 dyrektywy 2022/2555 nie będzie ona miała zastosowania do unii kredytowych (SKOK), jeżeli państwo członkowskie wyłączy te podmioty z zastosowania DORA (art. 2 ust. 4 DORA). Regulacja ta koresponduje z motywem 16 DORA, według którego rozporządzenie to jest *lex specialis* w stosunku do dyrektywy 2022/2555.

Abstrakt
Rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej (*Digital Operational Resilience Act* – DORA) nakłada na podmioty finansowe szereg obowiązków związanych z bezpieczeństwem technologii informacyjno-komunikacyjnych (ICT). Niektóre z tych podmiotów są jednak wyłączone z zakresu obowiązywania DORA, np. ze względu na wielkość posiadanego kapitału lub zarządzanych aktywów. Inne mogą zostać wyłączone z zakresu zastosowania DORA przez państwo członkowskie w ramach opcji narodowej. Poza tym normy prawne DORA wyrażają zasadę proporcjo-

nalności i wskazują, jakie cechy podmiotu finansowego należy uwzględnić przy wypełnianiu obowiązków wynikających z DORA. Celem artykułu jest przedstawienie tych obowiązków oraz przesłanek, zgodnie z którymi zasada proporcjonalności ma zastosowanie do podmiotów wskazanych w tym akcie prawnym. Teza badawcza artykułu stanowi, że zasada proporcjonalności została uregulowana w DORA wielopłaszczyznowo. W artykule posłużono się metodą dogmatycznoprawną.

Słowa kluczowe: DORA, zasada proporcjonalności, unie kredytowe.

BIBLIOGRAFIA

Bátiz-Lazo B., Billings M., *New perspectives on not-for-profit financial institutions: Organizational form, performance and governance*, „Business History" 2012, 3, 54, https://doi.org/10.1080/00076791.2011.638480.

Bierecki D., *Konsekwencje prawne uzyskania przez spółdzielnię statusu przedsiębiorstwa społecznego*, „Krytyka Prawa" 2023, 15, 3. DOI 10.7206/kp.2080-1084.628.

Herbet A., Pawłowski S., Zakrzewski P., Spółdzielcze kasy oszczędnościowo-kredytowe, Komentarz, Warszawa 2024.

Maliszewska-Nienartowicz J., Zasada proporcjonalności jako podstawa oceny legalności ograniczeń swobód rynku wewnętrznego Unii Europejskiej, Toruń 2020.

Miąsik D., System prawa Unii Europejskiej, tom 2, Zasady i prawa podstawowe, Warszawa 2022.

Pelc P., *Zasada proporcjonalności w* DORA, „Cybersecurity and Law" 2024, 2, 12.

Pietrzykowski K. (red.), System prawa prywatnego, tom 21, Prawo spółdzielcze, Warszawa 2020.

Wniosek rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014, COM/2020/595 final.