Wpływ DORA na wybrane wymogi związane z outsourcingiem bankowym

dr *Michał Synowiec**

Z dniem 27.12.2022 r. w Dzienniku Urzędowym Unii Europejskiej opublikowano rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego[1]. Akt ten statuuje jednolite wymogi prawne w zakresie bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w działalności podmiotów finansowych[2]. W niedalekiej perspektywie będzie on mieć niebagatelne znaczenie nie tylko dla instytucjonalnych uczestników rynku, ale również dostawców szeroko pojmowanych technologii informatycznych (IT[3]), którzy wspierają swoją działalnością procesy biznesowe wielu instytucji finansowych. Celem niniejszego artykułu jest przeanalizowanie wpływu DORA na część obowiązków banku związanych z planowanym powierzeniem podmiotowi trzeciemu wykonania czynności z obszaru IT oraz omówienie pojawiających się na tym tle wątpliwości interpretacyjnych wynikających z praktycznej aplikacji przepisów rozporządzenia, których stosowanie formalnie rozpocznie się od 17.1.2025 r. Prowadzone rozważania zmierzają przy tym do ustalenia normatywnych konsekwencji uchwalenia DORA oraz oddziaływania tego rozporządzenia na dotychczasowy reżim prawny outsourcingu bankowego. Z uwagi na ograniczony charakter niniejszego opracowania wywód skupia się na zagadnieniach podoutsourcingu, odpowiedzialności insourcera oraz outsourcingu zagranicznym, wyłączając z zakresu dyskursu problematykę dotyczącą *stricte* umowy outsourcingu.

Cel oraz zakres stosowania przepisów DORA

Zasadniczym celem przyjęcia DORA jest **osiągnięcie wysokiego wspólnego poziomu operacyjnej odporności cyfrowej** (ang. *digital resilience*)[4] **przez podmioty finansowe, o których mowa w art. 2 ust. 1 DORA**. Katalog takich jednostek jest niezwykle rozbudowany. Ujęto w nim bowiem podmioty prowadzące działalność w rozmaitych segmentach rynku finansowego, a w szczególności dostawców usług o charakterze bankowym, płatniczym, ubezpieczeniowym, inwestycyjnym oraz emerytalnym, bez względu na poziom wykorzystywanych przez nich rozwiązań technologicznych.

Nowe wymogi prawne obejmą przede wszystkim podmioty pokroju instytucji kredytowych, instytucji płatniczych, instytucji pieniądza elektronicznego, zakładów ubezpieczeń, firm inwestycyjnych oraz instytucji pracowniczych programów emerytalnych[5]. DORA znajdzie zastosowanie również do innych podmiotów rynku finansowego, niejednokrotnie prowadzących działalność na znacznie mniejszą skalę (np. dostawców świadczących wyłącznie usługę dostępu do informacji o rachunku, pośredników ubezpieczeniowych, reasekuracyjnych i oferujących ubezpieczenia uzupełniające[6] oraz dostawców usług finansowania społecznościowego)[7].

Spoza zakresu podmiotowego rozporządzenia *explicite* **wyłączono** natomiast takie jednostki jak zarządzających alternatywnymi funduszami inwestycyjnymi, tzw. małe zakłady ubezpieczeń[8], osoby fizyczne lub prawne, o których mowa w art. 2 i 3 dyrektywy 2014/65/UE[9] oraz instytucje świadczące żyro pocztowe. **Opcja narodowa** przewidziana w art. 2 ust. 4 DORA dodatkowo uprawnia polskiego ustawodawcę do wyłączenia stosowania rozporządzenia względem spółdzielczych kas oszczędnościowo-kredytowych oraz Banku Gospodarstwa Krajowego.

Z perspektywy formalnej nowe regulacje znajdą zastosowanie do wszystkich kategorii podmiotów finansowych, o których mowa w art. 2 ust. 2 DORA. Z pola widzenia nie można jednak tracić, że prawodawca unijny zdecydował się na wprowadzenie **zasady proporcjonalności** w zakresie aplikacji poszczególnych przepisów, uzależniając ich stosowanie od wielkości i profilu ryzyka danego podmiotu oraz charakteru, skali i stopnia złożoności świadczonych usług, a także prowadzonej

* Adwokat, Counsel w kancelarii Traple Konarski Podrecki i Wspólnicy; ORCID: 0000-0001-6621-8406.

[1] Zob. rozporządzenie Parlamentu Europejskiego i Rady z 14.12.2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenie (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014; Dz.Urz. L Nr 331 z 27.12.2022 r., s. 1; dalej jako: DORA.

[2] Zgodnie z art. 2 ust. 2 DORA, przez „podmioty finansowe" rozumieć należy adresatów rozporządzenia, z wyjątkiem zewnętrznych dostawców usług ICT. Szerzej na temat desygnatów pojęcia „podmiotów finansowych" zob. uwagi poniżej.

[3] Od ang. *information technology*.

[4] Zob. motyw 105 preambuły DORA.

[5] Dotyczy to wyłącznie instytucji pracowniczych programów emerytalnych, które obsługują programy emerytalne liczące łącznie więcej niż 15 uczestników (*argumentum ex* art. 2 ust. 3 lit. c DORA).

[6] Z zakresu podmiotowego DORA wyłączono jednak pośredników ubezpieczeniowych, reasekuracyjnych i oferujących ubezpieczenia uzupełniające, którzy nie są mikroprzedsiębiorcami lub małymi lub średnimi przedsiębiorcami; zob. art. 2 ust. 3 lit. e DORA.

[7] Co ciekawe, niejako wyprzedzająco – jeszcze przed formalnym przyjęciem oraz opublikowaniem w Dzienniku Urzędowym Unii Europejskiej rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów oraz zmieniającego rozporządzenia (UE) nr – przepisami DORA objętego również dostawców usług w zakresie kryptoaktywów oraz emitentów tokenów powiązanych z aktywami.

[8] Chodzi o podmioty, o których mowa w art. 4 dyrektywy Parlamentu Europejskiego i Rady 2009/138/WE z 25.11.2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II), Dz.Urz. L Nr 335 z 17.12.2009 r., s. 1.

[9] Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z 15.5.2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE, Dz.Urz. Nr 173 z 12.6.2014 r., s. 1.

działalności[10]. Podmioty finansowe działające na polskim rynku tego rodzaju podejście kojarzyć mogą chociażby z modelu referencyjnego przyjętego w tzw. Komunikacie chmurowym UKNF[11] (pkt IV.2.).

Zakres podmiotowy rozporządzenia nie odnosi się przy tym wyłącznie do podmiotów finansowych, ale także do **zewnętrznych dostawców technologii informacyjno-komunikacyjnych** (ang. *information and communication technology* – ICT), ze szczególnym uwzględnieniem tzw. **dostawców kluczowych**. Tym samym rozporządzenie w pewien sposób prowadzi do zmiany dotychczasowego kierunku regulacji, koncentrując się nie tylko na działalności uczestników rynku finansowego, ale także ich partnerach technologicznych, których część objęta zostanie publicznoprawnym nadzorem właściwych organów (art. 31 i n. DORA).

Jeżeli chodzi o **zakres przedmiotowy** rozporządzenia to dotyczy on **czterech grup zagadnień**. **Pierwsza** z nich odnosi się do wymogów stawianych podmiotom finansowym i obejmuje zarządzanie ryzykiem związanym z korzystaniem z technologii ICT (w tym wdrażanych środków zarządczych), monitorowanie i raportowanie incydentów ICT, testowanie operacyjnej odporności cyfrowej oraz wymianę informacji i analiz w związku ze zidentyfikowanymi podatnościami i cyberzagrożeniami. **Druga** grupa dotyczy wymogów regulacyjnych z obszaru kontraktowego, związanego z nawiązywaniem relacji umownych[12] pomiędzy podmiotami finansowymi a zewnętrznymi dostawcami usług ICT. **Trzecia** grupa odnosi się do zasad objęcia nadzorem kluczowych zewnętrznych dostawców usług ICT. Z kolei ostatnia, **czwarta** grupa, nawiązuje do współpracy właściwych organów w zakresie przestrzegania DORA[13].

Zagadnienia kolizyjnoprawne na tle reżimu outsourcingu bankowego

Problematyka powierzenia podmiotom trzecim wykonywania czynności z zakresu szeroko pojmowanych technologii informatycznych (IT) niejednokrotnie stanowiła przedmiot dyskusji doktrynalnych odnośnie do zasad wykonywania działalności bankowej. Charakter niniejszego opracowania nie pozwala na szczegółowe przedstawienie sformułowanych dotychczas poglądów, niemniej na potrzeby prowadzonego wywodu wystarczające powinno być zwrócenie uwagi, że klasyczny outsourcing IT, co do zasady, kwalifikuje się jako **powierzenie wykonywania czynności faktycznych związanych z działalnością bankową w rozumieniu art. 6a ust. 1 pkt 2 PrBank**[14]. Wniosek ten dotyczy przypadków realizacji czynności będących w bezpośrednim związku z działalnością bankową, tj. stanowiących części składowe czynności wskazanych w art. 5 i 6 ust. 1 PrBank lub bez których realizacji nie jest możliwe właściwe wykonanie umowy dotyczącej czynności wskazanej w art. 5 lub 6 ust. 1 PrBank[15]. W literaturze przyjmuje się przy tym (w ślad za pismem GINB), iż na ogół dotyczy to przypadków zagwarantowania insourcerowi dostępu do informacji objętych tajemnicą bankową (niemniej, w mojej ocenie, dostęp do informacji objętych tajemnicą bankową nie stanowi samodzielnej przesłanki decydującej o kwalifikacji danej relacji jako outsourcingu podlegającego reżimowi PrBank[16]) lub wykonywania przez podmiot trzeci czynności zmierzających do zapewnienia ciągłego i niezakłóconego działania systemów informatycznych, które wykorzystywane są bezpośrednio w działalności bankowej[17].

Z perspektywy kwalifikacji outsourcingu IT na gruncie DORA kwestią kluczową pozostaje ustalenie **charakteru usług świadczonych przez danego dostawcę podmiotu finansowego** (np. banku). Zakresem przedmiotowym outsourcingu w świetle rozporządzenia objęte jest bowiem świadczenie tych usług z obszaru technologii informatycznych, które spełniają definicję „usługi ICT" w rozumieniu art. 3 pkt 21 DORA (ustalenie charakteru świadczonej usługi wpływa przy tym na możliwość przypisania konkretnemu podmiotowi statusu dostawcy usług ICT). Co jednak istotne, wymogi wprowadzone przez DORA dotyczą bezpieczeństwa sieci i systemów informatycznych, które wspierają biznesowe procesy podmiotów finansowych (art. 1 ust. 1 *in principio* DORA). Wymogów tych nie sposób zatem odnosić do świadczenia usług nieobejmujących biznesowych obszarów działalności podmiotów finansowych (np. wykorzystywanych przez bank wyłącznie na wewnętrzne potrzeby kadrowe).

[10] Zob. art. 4 DORA.

[11] Komunikat Urzędu Komisji Nadzoru Finansowego z 23.1.2020 r. dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej; dalej jako: Komunikat UKNF ws. chmury obliczeniowej.

[12] Jedynie na marginesie wypada zwrócić uwagę, że polska wersja językowa DORA posługuje się nie do końca fortunnym sformułowaniem „ustaleń umownych" zamiast po prostu „umowy". Wykładając całokształt przepisów rozporządzenia nie powinno jednak budzić wątpliwości, że pojęcie to rozumieć należy jako kontrakt będący źródłem zobowiązania łączącego podmiot finansowy z dostawcą usług ICT. Podobnie *M. Kulesza*, *P. Filipowski*, Ryzyko wykorzystywania usług ICT w sektorze finansowym – Omówienie wybranych wymogów projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA), dodatek specjalny do MoP Nr 15/2022, s. 40–41.

[13] Szerzej na temat zakresu przedmiotowego stosowania DORA zob. *D. Clausmeier*, Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA), „International Cybersecurity Law Review" Nr 4/2023, s. 79–90.

[14] Ustawa z 29.8.1997 r. – Prawo bankowe, t. jedn.: Dz.U. z 2023 r. poz. 2488; dalej jako: PrBank.

[15] Tak pismo Generalnego Inspektoratu Nadzoru Bankowego z 21.12.2004 r. ws. outsourcingu (sygn. NB-BPN-I-022-70/04); dalej jako: Pismo GINB, którego zasadniczą aktualność potwierdzono w ramach Stanowiska UKNF z 16.9.2019 r. dotyczącego wybranych zagadnień związanych z wejściem w życie Wytycznych EBA w sprawie outsourcingu i ich uwzględnianiem w działalności banków – dalej jako: Stanowisko UKNF ws. outsourcingu. Por. również *J. Ząbczyk*, Korzystanie przez banki z usług dostawców wykonujących swoje czynności z wykorzystaniem chmury obliczeniowej w świetle przepisów o podoutsourcingu bankowym, „Monitor Prawa Bankowego" Nr 3/2023, s. 98.

[16] Podobnie *T. Czech*, Ujawnienie tajemnicy prawnie chronionej jako przesłanka outsourcingu bankowego, „Monitor Prawa Bankowego" Nr 10/2012, s. 80–89; *J. Ząbczyk*, Korzystanie…, s. 99–100.

[17] Tak m.in.: *A. Żygadło*, Outsourcing bankowy po zmianach w prawie [w:] Problemy współczesnej bankowości – zagadnienia prawne, pod red. *W. Góralczyka*, Warszawa 2014, s. 72–75; *taż*, Usługa cloud computingu jako czynność faktyczna związana z działalnością bankową, „Monitor Prawa Bankowego" Nr 7–8/2013, s. 85–87; *B. Bajor* [w:] *B. Bajor*, *L. Kociucki*, *K. Królikowska*, *J.M. Kondek*, Prawo bankowe. Komentarz do przepisów cywilnoprawnych, Lex/el. 2022, kom. do art. 6a PrBank, teza 4. Odmiennie natomiast *T. Dukiet-Nagórska*, Rodzaje umów outsourcingowych zawieranych przez banki, „Prawo Bankowe" Nr 11/2004, s. 48. Pośrednie stanowisko zdaje się z kolei zajmować *J. Byrski*, którego zdaniem wyróżnić należy trzy sytuacje powierzania przez bank czynności faktycznych związanych z działalnością bankową. Pierwsza dotyczy dostępu do informacji objętych tajemnicą bankową, która, zdaniem wspomnianego Autora, powinna być kwalifikowana jako wykonywanie czynności faktycznych związanych z działalnością bankową. Druga odnosi się do przypadków braku dostępu do informacji objętych tajemnicą bankową, ale mieszczących się w zakresie wykonywania czynności zapewniających ciągłe i niezakłócone funkcjonowanie systemów informatycznych bezpośrednio służących do wykonywania działalności bankowej – w tym przypadku, w ocenie *J. Byrskiego*, podmiot realizujący powierzone czynności działa w charakterze tzw. przedsiębiorstwa pomocniczych usług bankowych, które podlega nadzorowi KNF, niemniej stosunek ten nie mieści się w reżimie outsourcingu bankowego. Trzecia wreszcie obejmuje stany faktyczne niezwiązane z dostępem do informacji objętych tajemnicą bankową, czy też wykonywaniem czynności zapewniających ciągłe i niezakłócone działanie systemów informatycznych bezpośrednio służących do wykonywania działalności bankowej – takie przypadki mają nie mieścić się w granicach outsourcingu bankowego, ani innych obostrzeniach znajdujących podstawę w przepisach PrBank. Szerzej zob. *J. Byrski*, Outsourcing w działalności dostawców usług płatniczych, Warszawa 2018, s. 139–147.

Mając na uwadze zakres zastosowania rozporządzenia konsekwentnie należy zauważyć, że powierzenie podmiotowi trzeciemu wykonywania czynności mieszczących się w granicach definicji „usługi ICT" (w świetle DORA), co do zasady, objęte będzie reżimem outsourcingu bankowego jako stanowiące wykonywanie czynności faktycznych związanych z działalnością bankową na podstawie art. 6a ust. 1 pkt 1 PrBank[18].

Przepisy PrBank oraz DORA to jednak nie jedyne regulacje jakie w najbliższym czasie kształtować będą reżim prawny outsourcingu IT w działalności bankowej. Przykładowo, w zakresie w jakim dojdzie do powierzenia przetwarzania danych osobowych przez bank na rzecz zewnętrznego dostawcy usług ICT zastosowanie znajdą również **przepisy RODO**[19]. Niezależnie reżim takiego outsourcingu symultanicznie uzupełniany będzie również przez szereg aktów prawa miękkiego (ang. *soft law*), które wydane zostały zarówno na szczeblu prawodawstwa krajowego, jak i unijnego. Na tym tle w szczególności należy wspomnieć o:

1) Piśmie GINB;
2) Rekomendacji D[20];
3) Rekomendacji M[21];
4) Wytycznych EBA ws. outsourcingu[22];
5) Wytycznych EBA ws. ICT i zarządzania ryzykiem bezpieczeństwa[23];
6) Stanowisku UKNF ws. outsourcingu;
7) Komunikacie UKNF ws. chmury obliczeniowej oraz module Q&A w zakresie stosowania Komunikatu UKNF ws. chmury obliczeniowej[24].

Z pola widzenia nie można przy tym tracić, że w niedalekiej przyszłości do grona regulacji znajdujących (w mniejszym lub większym stopniu) zastosowanie do outsourcingu IT w działalności bankowej dołączą również regulacje wprowadzane na podstawie wykonawczych standardów technicznych oraz regulacyjnych standardów technicznych, których opracowaniem zajmują się europejskie urzędy nadzoru (EBA[25], ESMA[26] i EIOPA[27]), niekiedy przy współpracy z innymi podmiotami. W przepisach DORA zawarto aż dziesięć delegacji do wydania tego rodzaju aktów.

Niejako naturalną konsekwencją funkcjonowania w systemie prawnym złożonego reżimu outsourcingu IT w działalności bankowej jest **ryzyko występowania rozmaitych przypadków kolizji, w szczególności sprzeczności, norm znajdujących swoje źródło w poszczególnych regulacjach**. W tym kontekście przede wszystkim zwrócić należy uwagę, że DORA jest aktem o randze rozporządzenia unijnego, bezpośrednio skutecznym w porządkach prawnych państw członkowskich. Z tego faktu wynikają z kolei dwie podstawowe konsekwencje. Po pierwsze, w toku stosowania prawa zarówno organy krajowe, jak również jednostki będą mogły powoływać się na normy zawarte w DORA, jeżeli będą one wywodzone z przepisów uznawanych za bezpośrednio skuteczne[28]. Po drugie, normy wynikające z DORA (jako normy rozporządzenia) w przypadku ich sprzeczności z regulacjami krajowymi znajdą zastosowanie na zasadzie **pierwszeństwa przed normami krajowymi**[29]. Zabieg stosowania w pierwszej kolejności norm prawa unijnego zasadny będzie przy tym za każdym razem, gdy w systemie prawa (rozumianym jako prawo krajowe oraz prawo unijne) obowiązywać będą i znajdą zastosowanie do tego samego stanu faktycznego dwie normy, których aplikacja w istocie doprowadzi do przeciwnych rezultatów[30]. Rozwiązaniu tego impasu służy **odmowa skorzystania z przepisu krajowego pozostającego w sprzeczności z prawem unijnym** (tzw. reguła *Simmenthal*), która stanowi podstawową konsekwencję obowiązywania zasady pierwszeństwa[31].

Stosunkowo najmniejsze problemy w kontekście ustalenia zasad stosowania konkretnych norm pojawiają się w przypadkach sprzeczności zachodzącej pomiędzy przepisami DORA a unormowaniami wy-

[18] Na marginesie wypada jednocześnie zasygnalizować, że kwestią dyskusyjną może wydawać się kwalifikowanie świadczenia wszystkich usług ICT jako powierzenia wykonywania pewnych czynności w rozumieniu art. 6a–6d PrBank. Legalna definicja „usług ICT" swoim zakresem obejmuje bowiem także sprzęt komputerowy jako usługę oraz usługi w zakresie sprzętu komputerowego dotyczące zapewnienia wsparcia technicznego za pośrednictwem aktualizacji oprogramowania lub oprogramowania układowego przez dostawcę sprzętu. Jak wynika przy tym z Pisma GINB, nieuzasadnione jest kwalifikowanie jako outsourcingu bankowego wykonywania takich czynności, które polegają m.in. na nabywaniu sprzętu komputerowego, nabywaniu i instalacji oprogramowania, tworzeniu, rozwoju i modyfikacji licencjonowanego oprogramowania oraz serwisu sprzętu komputerowego. Na tym tle odrębnym wątkiem jest ponadto przyjmowanie niezwykle szerokiej interpretacji pojęcia „usług ICT" na gruncie projektu wykonawczych standardów technicznych opracowywanych przez europejskie urzędy nadzoru na podstawie art. 28 ust. 9 DORA [projekt dostępny jest pod następującym adresem: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Consultations/2023/Consultation%20Papers%20on%20DORA/1056507/CP%20-%20Draft%20ITS%20on%20register%20of%20information.pdf (dostęp: 12.1.2024 r.)]. Projektodawcy wstępnie przyjęli wszak, że usługami ICT są także m.in. usługi w zakresie licencjonowania oprogramowania *on premises*, testowanie oprogramowania, wynajem obiektów, w których znajduje się infrastruktura ICT, wynajem sprzętu wykorzystywanego w ramach wewnętrznych sieci ICT oraz usługi konsultacyjne z obszaru ICT. Takie rozumowanie może natomiast budzić wątpliwości w kontekście przyjętej na gruncie DORA legalnej definicji „usług ICT", która wskazuje, iż z założenia chodzi o usługi cyfrowe (ang. *digital services*) oraz usługi w zakresie danych (ang. *data services*), świadczone w sposób ciągły za pośrednictwem systemów ICT. Szczegółowe omówienie zasygnalizowanego tutaj zagadnienia wykracza jednak poza ramy niniejszego opracowania.

[19] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych); Dz.Urz. L Nr 119 z 4.5.2016 r., s. 1; dalej jako: RODO.

[20] Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, wydana w styczniu 2013 r. przez Komisję Nadzoru Finansowego; dalej jako: KNF.

[21] Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach, wydana przez KNF w styczniu 2013 r.

[22] Wytyczne Europejskiego Urzędu Nadzoru Bankowego z 25.2.2019 r. w sprawie outsourcingu (EBA/GL/2019/02); dalej jako: Wytyczne EBA ws. outsourcingu.

[23] Wytyczne Europejskiego Urzędu Nadzoru Bankowego z 28.11.2019 r. w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT.

[24] Moduł Q&A (pytania i odpowiedzi) dotyczący stosowania Komunikatu UKNF ws. chmury obliczeniowej dostępny jest pod następującym adresem: https://www.knf.gov.pl/dla_rynku/fin_tech/chmura_obliczeniowa/Q&A (dostęp: 12.1.2024 r.).

[25] Europejski Urząd Nadzoru Bankowego (ang. *European Banking Authority*).

[26] Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ang. *European Securities and Markets Authority*).

[27] Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (ang. *European Insurance and Occupational Pensions Authority*).

[28] Na temat zasad uznawania przepisów unijnych za bezpośrednio skuteczne zob. *M. Baran*, Rozporządzenie [w:] System Prawa Unii Europejskiej. T. 1. Podstawy i źródła prawa Unii Europejskiej, pod red. *S. Biernata*, Warszawa 2020, s. 966–971.

[29] Zob. *ibidem*, s. 984. Zdaniem *M. Barana*, w przypadku sprzeczności zachodzącej pomiędzy przepisami krajowymi i przepisami rozporządzenia zasada pierwszeństwa wyprzedzać będzie nawet obowiązek wykładni prounijnej (zob. *M. Baran*, *op. cit.*, s. 986). Inaczej natomiast *D. Miąsik*, który twierdzi, iż z metodologicznego punktu widzenia w przypadku sprzeczności norm prawa krajowego z prawem unijnym w pierwszej kolejności zasadne jest sięgnięcie do wykładni przepisów krajowych w zgodzie z prawem UE, a dopiero kolejno – jeżeli wystąpią stosowne przesłanki – skorzystanie z zasady pierwszeństwa (prymatu) prawa UE; zob. *D. Miąsik* [w:] System Prawa Unii Europejskiej. T. 2. Zasady i prawa podstawowe, pod red. *D. Miąsika*, Warszawa 2022, s. 136.

[30] *D. Miąsik*, *op. cit.*, s. 141.

[31] Szerzej na temat zasady pierwszeństwa w prawie UE zob. *D. Miąsik* [w:] System…, T. 2, *op. cit.*, s. 116–157.