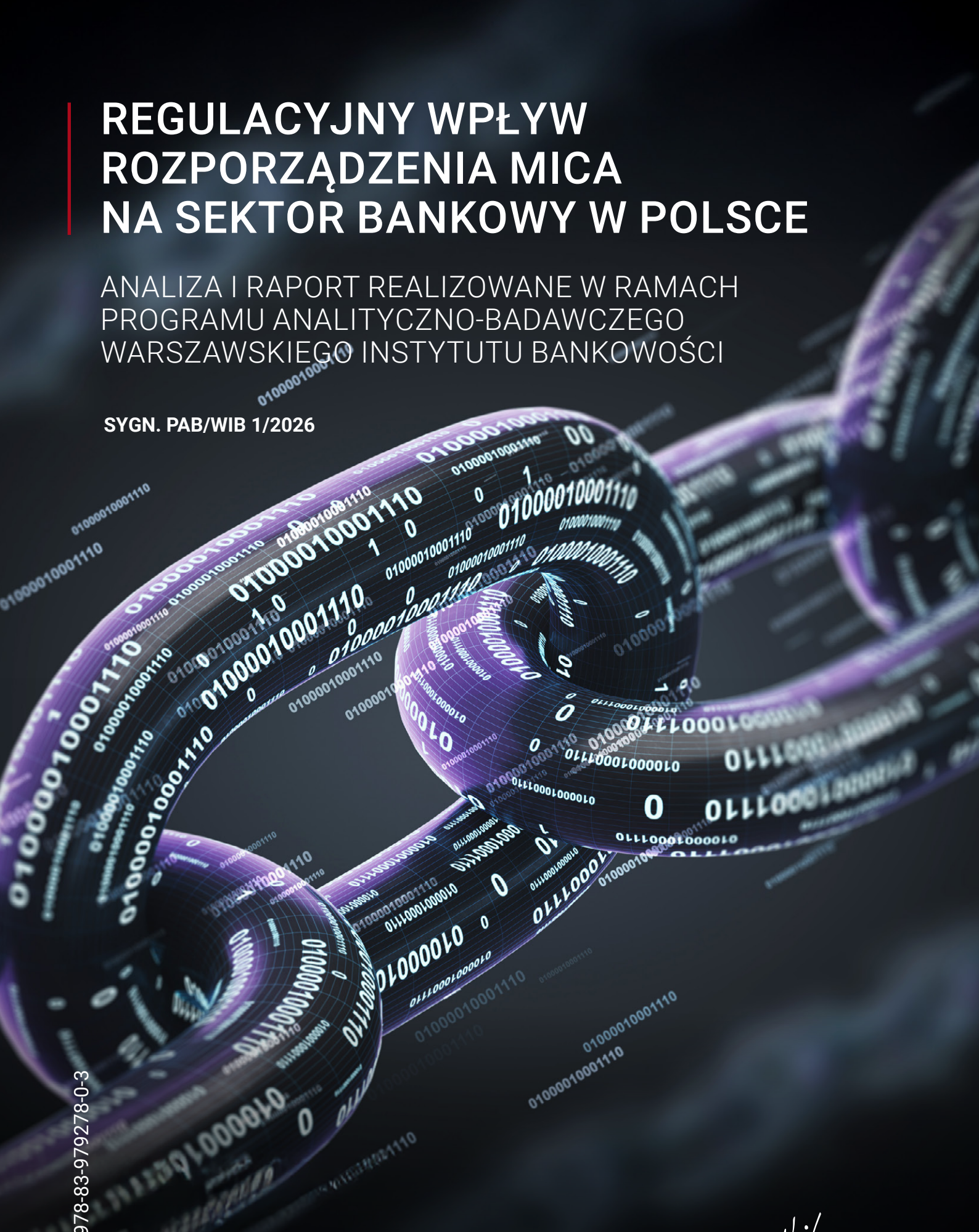
REGULACYJNY WPŁYW ROZPORZĄDZENIA MICA NA SEKTOR BANKOWY W POLSCE

ANALIZA I RAPORT REALIZOWANE W RAMACH PROGRAMU ANALITYCZNO-BADAWCZEGO WARSZAWSKIEGO INSTYTUTU BANKOWOŚCI

SYGN. PAB/WIB 1/2026



ISBN 978-83-979278-0-3

Raport opracowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

PROGRAM ANALITYCZNO BADAWCZY

Warszawa, 15 grudnia 2025 r.

O raporcie

Raport **„Regulacyjny wpływ rozporządzenia MiCA na sektor bankowy w Polsce”** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.

Projekt badawczy został przygotowany zgodnie z umową pomiędzy Wydziałem Prawa i Administracji Uniwersytetu Warszawskiego a Warszawskim Instytutem Bankowości.

Autorzy

Raport przygotowany przez zespół badawczy w składzie:

dr hab. Sławomir Żółtek, prof. ucz. Dziekan Wydziału Prawa i Administracji UW na kadencję 2024–2028. Współzałożyciel i pierwszy kierownik Centrum Badań nad Prawnymi Aspektami Technologii Blockchain działającego na WPiA UW. Wieloletni pracownik centralnych organów wymiaru sprawiedliwości, w tym Sądu Najwyższego oraz Biura Studiów i Analiz Sądu Najwyższego. Był wpisany na listy adwokatów oraz radców prawnych. Członek Głównej Komisji Orzekającej w Sprawach o Naruszenie Dyscypliny Finansów Publicznych. Uczestnik wielu konferencji i seminariów, a także autor publikacji naukowych z zakresu nowych technologii.

dr Jakub Grygutis Adiunkt w Katedrze Prawa Ubezpieczeń na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego oraz sędzia w Sądzie Rejonowym dla m.st. Warszawy. Autor licznych publikacji naukowych, w swojej pracy badawczej porusza takie zagadnienia jak dopuszczalność wypłaty wynagrodzenia w kryptowalucie w świetle polskiego prawa pracy. Aktywny uczestnik konferencji naukowych oraz współpracownik różnych ośrodków badawczych, w tym Centrum Badań nad Prawnymi Aspektami Technologii Blockchain.

r.pr. Michał Dymiński Radca prawny związany z Wydziałem Prawa i Administracji Uniwersytetu Warszawskiego, gdzie pełni funkcję Dyrektora Administracyjnego. Doradca prawny w Centrum Wsparcia Dydaktyki Uniwersytetu Warszawskiego. Współzałożyciel i kierownik Centrum Badań nad Prawnymi Aspektami Technologii Blockchain. Wieloletni pracownik sądów powszechnych i Sądu Najwyższego. Brał udział w pracach mających na celu wdrożenie technologii blockchain na uczelni. Zajmuje się przede wszystkim zastosowaniem nowych technologii w sektorze publicznym; uczestnik wielu konferencji i seminariów, a także autor publikacji naukowych z zakresu nowych technologii.

Raport wykonany w ramach Centrum Badań Nad Prawnymi Aspektami Technologii Blockchain działającego na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego

CENTRUM BADAŃ
NAD PRAWNYMI ASPEKTAMI TECHNOLOGII
BLOCKCHAIN

Odbiorcy raportu

Raport adresowany jest do:

- podmiotów rynku finansowego (banki, ale też towarzystwa ubezpieczeń czy towarzystwa emerytalne);
- zainteresowanych organów władzy publicznej (m.in. Urząd Komisji Nadzoru Finansowego, Rzecznik Finansowy, Narodowy Bank Polski, Urząd Ochrony Konkurencji i Konsumentów);
- instytucji nauki i szkolnictwa wyższego (m.in. uniwersytety, szkoły handlowe, Polska Akademia Nauk);
- mediów i komentatorów;
- organów stosujących (sądy, organy administracji publicznej) oraz stanowiących prawo (Sejm, Senat, administracja rządowa, grupy parlamentarne i partie polityczne);
- organizacji pozarządowych, szczególnie think-tanki aktywne w obszarze prawa i gospodarki oraz fundacje będące zapleczem intelektualno-eksperckim;
- kancelarii prawnych, firm doradczych lub pośrednictwa finansowego.

Raport ma na celu przedstawić rzetelną i aktualną wiedzę oraz jej popularyzację wśród decydentów odpowiedzialnych za tworzenie i interpretację prawa – m.in. w sporach sądowych pomiędzy bankami a klientami czy postępowaniach kontrolnych i nadzorczych.

O programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 r. jako odpowiedź na potrzeby sektora bankowego w zakresie wysokiej jakości analiz i badań z obszaru cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz – w ostateczności – kreowania wartości dla klientów – końcowych użytkowników bankowości.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- **Nowe technologie w sektorze bankowym, cyberbezpieczeństwo banków i systemy płatnicze**
- **Ekonomiczna analiza rozwoju sektora bankowego, stabilności banków, otoczenia makroekonomicznego**
- **Prawno-regulacyjne i legislacyjne uwarunkowania działalności sektora bankowego oraz wyzwania wynikające z orzecznictwa sądów krajowych i europejskich**
- **ESG i sustainable finance**
- **Prace analityczno-badawcze w zakresie poszczególnych obszarów funkcjonowania banków oraz w zakresie funkcjonowania wskaźników referencyjnych**

Więcej na temat działalności programu na stronie **www.pabwib.pl**

Kontakt

dr Tomasz Pawlonka
Dyrektor Programu
m: 505 917 778
e: tpawlonka@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Agnieszka Wicha
m: 661 646 474
e: agnieszka.wicha@zbp.pl

Bartosz Przyborowski
m: 795 933 104
e: bartosz.przyborowski@zbp.pl

Spis treści

Wykaz skrótów

CRD IV – dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi (Dz.Urz. UE L z 2013 r. 176/338 ze zm.)

DLT – Distributed Ledger Technology

DORA – 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 L z 2022 r. 333/1 ze zm.)

EBA – European Banking Authority

ECON – Komisja Gospodarcza i Monetarna Parlamentu Europejskiego

EMD2 – dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE (Dz.Urz. UE L z 2009 r. 267/7 ze zm.)

ESMA – European Securities and Markets Authority

HSM – Hardware Security Module

ICT – Information and Communication Technology

IOSCO – International Organization of Securities Commissions

k.c. – ustawa z 23 kwietnia 1964 r. – Kodeks cywilny (tekst jedn. Dz.U. z 2025 r. poz. 1071 ze zm.)

MiCA – rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz.Urz. UE L z 2023 r. 150/40 ze zm.)

MiFID II – dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.Urz. UE L z 2014 r. 173/349 ze zm.)

MPB – Monitor Prawa Bankowego

MTF – Multilateral Trading Facility

OTF – Organised Trading Facility

PPH – Przegląd Prawa Handlowego

PPP – Przegląd Prawa Publicznego

Pr. bank. – ustawa z 29 sierpnia 1997 r. – Prawo bankowe (tekst jedn. Dz.U. z 2024 r. poz. 1646 ze zm.)

PSD2 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.Urz. UE L z 2015 r. 337/35 ze zm.)

TUE – Traktat o Unii Europejskiej

PROGRAM ANALITYCZNO BADAWCZY

Streszczenie kierownicze

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 w sprawie rynków kryptoaktywów (MiCA) stanowi pierwszy w Unii Europejskiej kompleksowy akt prawny regulujący emisję kryptoaktywów oraz świadczenie usług z nimi związanych. Jego przyjęcie oznacza zasadniczą zmianę podejścia prawodawcy unijnego do technologii blockchain oraz rynków aktywów cyfrowych, które dotychczas funkcjonowały w dużej mierze poza ramami jednolitej regulacji sektorowej.

MiCA nie jest regulacją o charakterze marginalnym ani przejściowym. W praktyce rozporządzenie redefiniuje granice działalności bankowej, włączając do jego potencjalnego zakresu tokenizowane środki pieniężne, nowe formy rozliczeń płatniczych, usługi powiernicze oparte na technologii DLT oraz elementy infrastruktury rynków kryptoaktywów.

Celem niniejszego raportu jest kompleksowa analiza wpływu rozporządzenia MiCA na sektor bankowy w Polsce. Opracowanie koncentruje się na identyfikacji zakresu podmiotowego i przedmiotowego MiCA wobec banków, ocenie konsekwencji prawnych i organizacyjnych wynikających z nowych regulacji, a także na analizie ryzyk regulacyjnych i reputacyjnych związanych z oferowaniem produktów i usług opartych na kryptoaktywach. Raport zmierza do wykazania, że MiCA nie stanowi regulacji proinnowacyjnej w sensie deregulacyjnym; jest to akt stabilizujący i instytucjonalizujący rynek kryptoaktywów, który w sposób świadomy przesuwa ciężar ryzyka z podmiotów technologicznych na instytucje finansowe o najwyższej wiarygodności systemowej, w tym w szczególności na banki.

Banki, jako instytucje kredytowe, nie zostały wyłączone spod stosowania MiCA. Przeciwnie, rozporządzenie przewiduje wobec nich szczególny reżim regulacyjny, oparty przede wszystkim na art. 60 MiCA. Przepis ten umożliwia bankom świadczenie usług w zakresie kryptoaktywów bez konieczności uzyskiwania odrębnego zezwolenia właściwego dla dostawców usług w zakresie kryptoaktywów (CASP), zastępując je obowiązkiem notyfikacji działalności oraz spełnienia rozbudowanych wymogów materialnych. Szczególny reżim przewidziany dla banków nie oznacza jednak uproszczenia regulacyjnego. W praktyce prowadzi on do przesunięcia ciężaru regulacyjnego z etapu licencyjnego na etap bieżącego nadzoru, odpowiedzialności organizacyjnej oraz oceny adekwatności zarządzania ryzykiem.

Przeprowadzona w Raporcie analiza wskazuje, że MiCA może obejmować szeroki zakres produktów i usług bankowych, w szczególności:

- tokenizowane depozyty i środki pieniężne,
- tokeny będące pieniądzem elektronicznym (bankowe stablecoiny),
- emisję i obrót stokenizowanymi instrumentami dłużnymi,
- usługi przechowywania kryptoaktywów (custody),
- prowadzenie platform obrotu kryptoaktywami,
- rozliczenia transgraniczne i transfery oparte na technologii rozproszonego rejestru.

Oznacza to, że MiCA bezpośrednio oddziałuje na klasyczne obszary działalności bankowej, takie jak płatności, depozyty, obrót instrumentami finansowymi oraz usługi powiernicze, wprowadzając do nich elementy technologii blockchain.

Jednym z kluczowych ustaleń Raportu (zob. w szczególności część druga) jest brak autonomii MiCA względem pozostałych regulacji finansowych. MiCA funkcjonuje równolegle z innymi reżimami prawnymi, w szczególności:

- regulacjami ostrożnościowymi CRD/CRR,
- dyrektywą MiFID II,
- dyrektywą PSD2,
- rozporządzeniem DORA,
- regulacjami AML/CFT.

W konsekwencji banki podejmujące działalność w obszarze kryptoaktywów będą funkcjonować w wielowarstwowym systemie zgodności regulacyjnej, w którym to samo zdarzenie może generować obowiązki na gruncie kilku aktów prawnych jednocześnie. Taki model znacząco zwiększa zaś złożoność zarządzania ryzykiem regulacyjnym oraz podnosi koszty operacyjne działalności.

Raport identyfikuje także istotne bariery związane z wdrażaniem MiCA w strukturach bankowych. Obejmują one w szczególności:

- integrację technologii blockchain z istniejącymi systemami legacy,
- zapewnienie bezpiecznego przechowywania kryptoaktywów i zarządzania kluczami kryptograficznymi,
- spełnienie wymogów segregacji aktywów klientów,
- zapewnienie odporności operacyjnej i cyberbezpieczeństwa zgodnie z DORA,
- deficyt wyspecjalizowanych kompetencji technologicznych i prawnych.

Dla wielu banków barierą nie jest zatem brak możliwości prawnych, lecz brak gotowości organizacyjnej i technologicznej do prowadzenia działalności w tym obszarze.

MiCA znacząco wzmacnia mechanizmy ochrony konsumenta, co prowadzi do rozszerzenia zakresu odpowiedzialności banków za utratę kryptoaktywów, niewłaściwe wykonanie usług lub niewystarczające obowiązki informacyjne. Ryzyko to ma charakter nie tylko prawny, lecz również reputacyjny. Incydenty w obszarze kryptoaktywów mogą podważać zaufanie do banku jako instytucji stabilnej i bezpiecznej, a w konsekwencji wpływać na jego ocenę nadzorczą oraz pozycję rynkową. Ryzyko reputacyjne w tym obszarze ma zatem charakter systemowy, a nie wyłącznie wizerunkowy.

Ponadto MiCA wymusza na bankach podejmowanie długofalowych decyzji strategicznych dotyczących zakresu i modelu zaangażowania w rynek kryptoaktywów. Raport wskazuje, że najbardziej racjonalnym kierunkiem dla banków jest selektywne i ostrożne wejście w obszary takie jak:

- usługi custody,
- emisja i obsługa tokenów będących pieniądzem elektronicznym,
- infrastruktura rozliczeniowa i płatnicza oparta na DLT.

Jednocześnie MiCA sprzyja rozwojowi modelu bankowości infrastrukturalnej, w którym bank nie tyle oferuje kryptoaktywa jako produkt inwestycyjny, ile zapewnia bezpieczną, regulacyjnie zgodną infrastrukturę dla tokenizowanej gospodarki.

Na podstawie analizy regulacyjnej i rynkowej raport wyróżnia trzy realistyczne scenariusze rozwoju:

- ograniczenie działalności do usług custody i infrastruktury rozliczeniowej,
- rozwój custody, tokenizacji wybranych instrumentów oraz rozliczeń transgranicznych,
- pełne wejście w rynek kryptoaktywów, w tym prowadzenie platform obrotu i emisja własnych tokenów.

Raport wskazuje, że najbardziej adekwatny dla dużych banków uniwersalnych jest scenariusz rozwoju custody, tokenizacji wybranych instrumentów oraz rozliczeń transgranicznych, natomiast pełne wejście w rynek kryptoaktywów wiąże się z najwyższym poziomem ryzyka regulacyjnego i reputacyjnego.

MiCA nie jest regulacją przejściową ani eksperymentalną. Jest to akt systemowy, którego celem jest trwałe włączenie rynku kryptoaktywów w ramy stabilności finansowej Unii Europejskiej. Dla sektora bankowego oznacza to zarówno nowe możliwości rozwoju, jak i istotne wyzwania regulacyjne, technologiczne oraz reputacyjne. To z kolei powoduje, że odpowiedź banków na MiCA nie powinna sprowadzać się do pytania, czy angażować się w rynek kryptoaktywów, lecz w jaki sposób i w jakim zakresie czynić to w sposób bezpieczny, zgodny z regulacjami i długofalowo opłacalny.

PROGRAM ANALITYCZNO BADAWCZY

1. Zakres przedmiotowy MICA

1.1. Czym są kryptoaktywa

1.1.1. Wprowadzenie

Technologia blockchain oraz proces tokenizacji aktywów stały się przedmiotem zainteresowania tradycyjnych rynków finansowych. Z perspektywy sektora bankowego zastosowanie technologii blockchain w prowadzonej działalności bankowej mogłoby przynieść wiele wymiernych korzyści.

Po pierwsze, technologia blockchain gwarantuje większą przejrzystość i bezpieczeństwo danych. Wskazana przejrzystość wiąże się z cechą tej technologii, jaką jest niezmienność, stąd raz dokonanych transakcji nie da się odwrócić ani też usunąć z historii – na zawsze pozostanie o nich zapis w łańcuchach bloków. Ponadto, taka technologia – z uwagi na rozproszony model uwierzytelniania danych – jest znacznie bardziej odporna na ataki, gdyż możliwość włamania w ramach *single point of failure* jest praktycznie niemożliwe.

Po drugie, transakcje dokonywane poprzez blockchain (zwłaszcza przelewy transgraniczne) co do zasady mogą być szybsze i tańsze. Transakcje mogą być bowiem rozliczane w ciągu kilku minut, w przeciwieństwie do obecnej infrastruktury, jaką jest system SWIFT, gdzie rozliczenia trwają od 2 do 5 dni. Co więcej, koszty takich operacji będą stanowiły niewielkie opłaty transakcyjne, które wynikają z kosztów obsługi transakcji (*gas fee*) na wybranym blockchainie, niezbędne do wykonania transakcji. Nie będzie zatem konieczności uiszczania prowizji dla pośrednika.

Po trzecie, równolegle możliwe jest zmniejszenie kosztów operacyjnych, dzięki samowykonywalnym umowom, czyli *smart contracts*, które mogą zostać zaprogramowane do automatycznego wykonywania rozliczeń, co z kolei wyeliminować może izby rozliczeniowe oraz centra przetwarzania danych.

Po czwarte, już w tej chwili fintechy coraz częściej korzystają z technologii blockchain do rozliczeń z klientami. Brak zainteresowania sektora bankowego tą technologią może sprawić, że banki przestaną być konkurencyjne wobec ich konkurentów. Przykładem takiego fintechu może być revolut, który świadczy usługi związane z kryptoaktywami[1].

Jak wskazuje IOSCO, istnieje kilka cech, które tokenizacja może umożliwić lub usprawnić:

- **fractionalizacja (ułamek własności)** – możliwość dzielenia aktywu na mniejsze części, co ułatwia inwestowanie nawet mniejszym inwestorom;
- **programowalność** – tokeny mogą zawierać kod (smart kontrakty), który wykonuje określone akcje przy spełnieniu warunków (np. płatność dywidendy, warunkowe transfery);
- **kompozycja (*composability*)** – tokeny mogą być łączone lub wykorzystywane w strukturach finansowych (np. jako część innego produktu);
- **atomowość (*atomicity*)** – możliwość wykonania wielu kroków transakcyjnych (np. kupno + rozliczenie) w jednym niepodzielnym kroku[2].

Wskazane cechy mogą prowadzić do zwiększenia adopcji kryptoaktywów w finansach tradycyjnych, jak również w sektorze bankowym.

W niniejszej części podjęta zostanie próba wyjaśnienia, jaka jest definicja kryptoaktywów w świetle MiCA oraz jakie rodzaje kryptoaktywów wyróżnia unijny akt prawny. Istotne jest omówienie, czym są poszczególne rodzaje tokenów i odpowiedzenie na pytania, jakie aktualne i przyszłe produkty bankowe będą objęte regulacją MiCA.

1.1.2. Pojęcie kryptoaktywów i tokenizacji

Z perspektywy MiCA, kluczowa jest definicja kryptoaktywa, gdyż to właśnie emisja i świadczenie usług związanych z tymi dobrami jest przedmiotem tego aktu prawnego. Artykuł 3 ust. 1 pkt 5 MiCA definiuje kryptoaktywo jako cyfrowe odzwierciedlenie wartości lub prawa, które da się przenosić i przechowywać w formie elektronicznej z wykorzystaniem technologii rozproszonego rejestru lub podobnej technologii.

Pojęcie tokenizacji nie ma swojej definicji legalnej w MiCA. Jak wskazuje W. Szpringer, tokenizacja to forma cyfryzacji biznesu oparta na zdecentralizowanej technologii blockchain. Polega na tworzeniu

1 *The role of banking. Future prospects for cross-border payments*, https://www.omfif.org/wp-content/uploads/2020/05/The-role-of-blockchain-in-banking.pdf (dostęp: 29 listopada 2025 r.).

2 IOSCO, *Tokenization of financial assets*, s. 8, dostęp: 29 listopada 2025 r.).

tokenów i przypisywaniu ich do konkretnego projektu, firmy lub osoby. Wraz z rozwojem technologii blockchain, a także otoczenia instytucjonalnego, w szczególności infrastruktury rynku finansowego, potencjał tokenizacji rośnie dzięki inteligentnym kontraktom i pozwala tokenizować wszelkiego rodzaju aktywa, jednocześnie obniżając koszty transakcyjne[3]. Tokenizacja więc odnosi się do procesu reprezentacji aktywów jako zapisu cyfrowego (tokenu) na wspólnej, programowalnej platformie, z wykorzystaniem technologii rozproszonego rejestru (DLT) lub podobnej technologii. DLT to technologia, która umożliwia obsługę i wykorzystanie rozproszonych rejestrów. Każdy „rozproszony rejestr" stanowi repozytorium informacji, które przechowuje zapisy transakcji i jest współdzielone oraz synchronizowane między zestawem węzłów sieci DLT za pomocą mechanizmu konsensusu (art. 3 ust. 1 pkt 1 i 2 MiCA). Rozproszone rejestry mogą obsługiwać inteligentne kontrakty, które są samoczynnie uruchamianymi programami, po spełnieniu zestawu predefiniowanych warunków i umożliwiającymi automatyzację transakcji/zdarzeń[4].

MiCA wymienia cztery rodzaje kryptoaktywów, które podlegają jej regulacji:

- kryptoaktywa powiązane z aktywami,
- kryptoaktywa będące pieniądzem elektronicznym,
- tokeny użytkowe,
- inne kryptoaktywa.

Jeszcze przed uchwaleniem rozporządzenia MiCA istniał rodzaj kryptoaktywów nazywany **stablecoinami** (z ang. *stablecoins*, od połączenia słów *stable*, czyli stabilny, oraz *coin*, czyli moneta). Pojęcie to odnosi się do tokenów, które w odróżnieniu od większości kryptoaktywów, zachowują stabilny kurs względem którejś z walut fiducjarnych (najczęściej jest to dolar amerykański). Stabilność ta może być zapewniana na różne sposoby, np. dzięki utrzymywaniu przez emitenta rezerw walutowych albo zabezpieczenia kryptowaluty innymi aktywami, np. amerykańskimi obligacjami skarbowymi. Istnieją też stablecoiny algorytmiczne, które wykorzystują skomplikowane algorytmy mające za zadanie utrzymać stabilną wartość takiego aktywa względem waluty fiducjarnej. Wskazany rodzaj stablecoinów był podatny na wahania rynkowe, które prowadziły do utraty zaufania do danego stablecoina i finalnie do całkowitej utraty wartości.

To, co jest potocznie nazywane stablecoinami, podlega najdalej idącej regulacji MiCA. Stablecoiny w istocie zostały podzielone na dwie kategorie kryptoaktywów podlegających regulacji: kryptoaktywa powiązane z aktywami oraz kryptoaktywa będące pieniądzem elektronicznym.

1.1.3. Tokeny powiązane z aktywami

W pierwszej kolejności, w art. 3 ust. 1 pkt 6 MiCA wskazano: „token powiązany z aktywami" oznacza rodzaj kryptoaktywa, który nie jest tokenem będącym pieniądzem elektronicznym i który ma utrzymywać stabilną wartość dzięki temu, że jest powiązany z inną wartością lub prawem bądź ich kombinacją, w tym z co najmniej jedną walutą urzędową. Nazwa ta koresponduje z angielskim określeniem *stablecoin* i wzięła się z powiązania wartości tokenu z innym aktywem, do którego jest utrzymywana wartość. Zgodnie z motywem 41 MiCA, zakresem definicji kryptoaktywów powiązanych z aktywami są te kryptoaktywa, które mają utrzymywać stabilną wartość względem co najmniej jednego aktywa, dzięki wykorzystaniu protokołów umożliwiających zwiększenie lub zmniejszenie podaży takich kryptoaktywów w reakcji na zmiany popytu.

Z kolei w motywie 41 MiCA możemy przeczytać, że „aby zmniejszyć ryzyko, że tokeny powiązane z aktywami są wykorzystywane jako środek przechowywania wartości, emitenci tokenów powiązanych z aktywami oraz wszyscy dostawcy usług w zakresie kryptoaktywów nie powinni przyznawać odsetek użytkownikom tokenów powiązanych z aktywami przez okres, w którym użytkownicy ci są posiadaczami tych tokenów powiązanych z aktywami". Wskazany motyw może prowadzić do wniosku, że rolą wskazanej grupy kryptoaktywów nie powinno być pełnienie funkcji tezauryzacji, tylko środka wymiany[5].

Wskazana definicja wyłącza z zakresu aktywów powiązanych z aktywami te kryptoaktywa, które są

3 W. Szpringer, *Ocena skutków regulacji w obszarze nowych technologii. Doświadczenia i wyzwania,* PPP 2024, nr 7–8, s. 7–21.

4 M. Wnęk, *Natura prawna kryptowaluty*, Warszawa 2023, s. 113.

5 T. Tomczak, *Ewolucja definicji kryptoaktywów w projekcie rozporządzenia MiCA*, PPH 2023, nr 3, s. 37–44.

pieniądzem elektronicznym, co jest spowodowane wyodrębnieniem tego rodzaju aktywów w rozporządzeniu jako odrębnej grupy rodzajowej kryptoaktywów. Nie oznacza to jednak, że wybrane stablecoiny powiązane z jedną walutą urzędową nie będą zaliczone do tej grupy kryptoaktywów[6]. Ocena, do której kategorii zostanie przypisane konkretne kryptoaktywo zależy od konkretnych cech danego tokenu, o czym będzie mowa dalej. W praktyce tokenami powiązanymi z aktywami mogą być te, które odwzorowują wartość zarówno: jednej waluty, koszyka walut, surowców czy innych aktywów, które odwzorowują rzeczy oznaczone co do gatunku. Token powiązany z aktywami może też odwzorowywać wartość koszyka, określonych aktywów. W nauce stawia się zatem bardzo ważne pytanie: jak coś ma utrzymywać stabilną wartość, skoro stabilna wartość ma być skutkiem powiązania z czymś, co ze swej natury jest/może być niestabilne? Zgodzić należy się w związku z tym z tezą, że stabilność różnych tokenów powiązanych z aktywami będzie się mocno między sobą różnić. Cecha stabilności jest względna. Ocena stabilności będzie musiała być zatem dokonywana przez inwestora osobno w odniesieniu do każdego tokenu na podstawie obligatoryjnego dokumentu informacyjnego (ang. *white paper*), zatwierdzonego przez właściwy organ[7].

Na koniec warto podkreślić, że emitenci tokenów powiązanych z aktywami są zobowiązani utworzyć i utrzymywać rezerwę aktywów zabezpieczających roszczenia posiadaczy tych tokenów wobec ich emitenta. Posiadaczom tokenów powiązanych z aktywami przysługuje w każdym momencie uprawnienie do żądania wykupu (poprzez zapłatę w środkach pieniężnych) wobec emitentów takich tokenów.

1.1.4. Tokeny będące pieniądzem elektronicznym

Drugą grupą kryptoaktywów, wskazanych w art. 3 ust. 1 pkt 7 MiCA, a podlegających najdalej idącej regulacji, są tokeny będące „pieniądzem elektronicznym" lub „tokeny będące e-pieniądzem", które oznaczają rodzaj kryptoaktywa, które mają utrzymywać stabilną wartość dzięki temu, że jest powiązany z jedną walutą urzędową. Wskazana nazwa jest używana zamiennie. Z kolei w świetle art. 3 ust. 1 pkt 8 MiCA waluta urzędowa oznacza walutę urzędową państwa, która jest wyemitowana przez bank centralny lub inny organ kształtujący politykę pieniężną. Oznacza to, że wskazane kryptoaktywo cechuje się stabilizacją ceny poprzez odniesienie do waluty urzędowej. Co więcej, w tej definicji wprost zostało wskazane, że chodzi o walutę wyemitowaną przez bank centralny, co skutkuje wyłączeniem z definicji tokenów syntetycznych powiązanych z bitcoinem, który jest walutą urzędową w Salwadorze i Republice Środkowoafrykańskiej.

Jak wynika, z motywu 9 MiCA, podstawową funkcją tego rodzaju kryptoaktywa jest funkcja płatnicza. Powołany motyw wskazuje, że token ten powinien być elektronicznym substytutem monet i banknotów, służącym dokonywaniu płatności. Co istotne, miała to być jedynie jego **główna** funkcja.

Warto w tym miejscu podkreślić podstawową zasadę dotyczącą emitentów wskazanych tokenów, która w istocie jest służebna dla pełnienia przez nich funkcji płatniczej. Emitenci takich tokenów emitują je według **wartości nominalnej po otrzymaniu środków pieniężnych**. Przykładowo, po wpłacie 100 zł podmiot powinien otrzymać 100 tokenów będących e-pieniądzem. Brak takiego stuprocentowego „pokrycia" tokenu będzie sprawiał, że potrzebna będzie analiza, czy nie jest to token powiązany z aktywami, który obecnie również może odsyłać do jednej waluty urzędowej, ale nie może być jednocześnie zakwalifikowany jako token będący pieniądzem elektronicznym (zob. art. 3 ust. 1 pkt 3 obowiązującej wersji MiCA). To właśnie takie rozróżnienie zakreśla sztywny podział na stablecoiny, które albo są pieniądzem elektronicznym albo tokenami powiązanymi z aktywami[8].W tym kontekście warto wskazać przykład stablecoina: usdc (USD CIRCLE). Utrzymuje peg: 1 usd do 1 usdc. Jest w całości zabezpieczony poprzez środki pieniężne oraz obligacje amerykańskie, jego emitent posiada licencję instytucji pieniądza elektronicznego i podlega regularnym audytom oraz podlega wykupowi. Aktualnie usdc w świetle MiCA jest uznane za token stanowiący pieniądz elektroniczny[9], natomiast – jak wynika ze strony ESMA – nie ma zarejestrowanych tokenów powiązanych z aktywami[10].

6 T. Tomczak, *Ewolucja definicji kryptoaktywów*….

7 T. Tomczak, *Ewolucja definicji kryptoaktywów*…

8 T. Tomczak, *Ewolucja definicji kryptoaktywów w projekcie rozporządzenia MiCA*, PPH 2023, nr 3, s. 37–44.

9 Https://cointelegraph.com/news/circle-first-licensed-stablecoin-issuer-mica (dostęp: 7 grudnia 2025 r.).

10 https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica#InterimMiCARegister (dostęp: 7 grudnia 2025 r.).

Token będący pieniądzem elektronicznym pojawia się tylko w słowniczku definicyjnym, ponieważ poprzez zrównanie tokenów będących e-pieniądzem (*stablecoin*) z pieniądzem elektronicznym (art. 48 ust. 2 MiCA), tokeny te zostały częściowo wyłączone z reżimu wymogów regulacyjnych dedykowanych dla pieniądza elektronicznego[11]. W literaturze można dostrzec poglądy, że ze względu na nieostrą delimitację przepisów odnoszących się do tokenów stanowiących pieniądz elektroniczny, a tradycyjnych pieniądzy elektronicznych w wersji niestokenizowanej, należy stosować kumulatywnie przepisy MiCA oraz EMD212. Tokeny te stały się tym samym pieniądzem elektronicznym albo – mówiąc precyzyjnie – ich ztokenizowaną wersją.

1.1.5. Tokeny użytkowe

Rozporządzenie MiCA zdefiniowało token użytkowy (ang. *utility tokens*) jako rodzaj kryptoaktywa, który ma jedynie zapewnić dostęp do danego towaru lub usługi dostarczanych przez jego emitenta. Są one tworzone w celu ułatwionego obrotu określonymi dobrami lub produktami. Przykładowo możliwe jest stworzenie tokena, który reprezentuje godzinę czyjejś pracy (np. programisty). Następnie taki programista może przeprowadzić aukcję takich tokenów w celu lepszego wycenienia swojej pracy i uzyskania optymalnego wynagrodzenia[13]. Po analizie dwóch poprzednich definicji widać, że jest to jedyny zdefiniowany w MiCA token, który nie musi utrzymywać stabilnej wartości.

1.1.6. Inne rodzaje kryptoaktywów

Na koniec warto wskazać, że MiCA nie tylko reguluje kwestię emisji i świadczenia usług w zakresie trzech wyodrębnionych wcześniej typów kryptoaktywów, ale także w odniesieniu do innych ich rodzajów. Taki wniosek wynika z redakcji art. 1 ust. 1 MiCA, zgodnie z którym „w niniejszym rozporządzeniu ustanawia się jednolite wymogi dotyczące oferty publicznej i dopuszczania do obrotu na platformie obrotu kryptoaktywów innych niż tokeny powiązane z aktywami i tokeny będące e-pieniądzem […]". Wskazana redakcja wprost stanowi ogólnie o kategorii kryptoaktywów, jednak z uwagi na regulacje szczególne w odniesieniu do trzech wyodrębnionych grup kryptoaktywów doszło do ich wyodrębnienia jako odrębnych kategorii tokenów.

W ramach wskazanej grupy kryptoaktywów znajdują się wszystkie najpopularniejsze kryptowaluty, jak: bitcoin, ether, binancecoin i inne, pod warunkiem, że nie podlegają wyłączeniu w art. 2 ust. 3 i 4 MiCA. Stąd świadczenie usług związanych z kryptoaktywami, których przedmiotem są *de facto* wszystkie kryptowaluty niewyłączone z przepisów rozporządzenia wymaga spełnienia wymogów regulacyjnych zawartych w MiCA.

1.1.7. Kryptoaktywa wyłączone z regulacji MiCA

W rozporządzeniu zostały także wyróżnione kategorie instrumentów, które nie są uznawane za kryptoaktywa dla celów MiCA. Zostały one wskazane w art. 2 ust. 3 i 4 MiCA. Są nimi:

a) instrumenty finansowe;

b) depozyty, w tym lokaty strukturyzowane;

c) środki pieniężne, chyba że kwalifikują się one jako tokeny będące e-pieniądzem;

d) pozycje sekurytyzacyjne w kontekście sekurytyzacji zgodnie z definicją zawartą w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/2402;

e) ubezpieczenia na życie lub ubezpieczenia inne niż ubezpieczenia na życie, należące do grup ubezpieczeń wymienionych w załącznikach I i II do dyrektywy Parlamentu Europejskiego i Rady 2009/138/WE lub umowy reasekuracji i retrocesji, o których mowa w tej dyrektywie;

f) produkty emerytalne uznane w prawie krajowym za mające za główny cel zapewnienie inwestorowi dochodu na emeryturze i uprawniające inwestora do określonych świadczeń;

g) oficjalnie uznane pracownicze programy emerytalne objęte zakresem stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/2341 lub dyrektywy 2009/138/WE;

11 M. Rypina, M. Wierzbowski [w:] M. Rypina, M. Wierzbowski (red.), *Rozporządzenie w sprawie rynków kryptoaktywów. Komentarz* [w:] *Rozporządzenie w sprawie rynków kryptoaktywów (MiCA) i rozporządzenie pilotażowe DLT (DLT Pilot Regime). Komentarz*, Warszawa 2025, art. 3.

12 R. Włoczka, *Pieniądz elektroniczny a tokeny będące pieniądzem elektronicznym – próba delimitacji*, Monitor Prawniczy 2025, nr 8, s. 95–100.

13 A. Bilski, R. Kiełbus, *Kryptoaktywa i blockchain. Technologia, prawo, biznes*, Warszawa 2024, s. 24–25.

h) indywidualne produkty emerytalne, w przypadku których prawo krajowe wymaga wkładu finansowego od pracodawcy, a pracodawca lub pracownik nie ma możliwości wyboru produktu emerytalnego lub jego dostawcy;

i) ogólnoeuropejski indywidualny produkt emerytalny zgodnie z definicją zawartą w art. 2 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1238;

j) systemy zabezpieczenia społecznego objęte rozporządzeniami Parlamentu Europejskiego i Rady (WE) nr 883/2004 i (WE) nr 987/2009.

Z uwagi na obszerny katalog wyłączeń, w dalszych rozważaniach skupiono się na omówieniu czterech z nich, które mogą mieć znaczenie dla oceny produktów bankowych opartych o technologię rozproszonego rejestru (tokeny NFT, instrumenty finansowe, depozyty oraz środki pieniężne).

1.1.7.1. Tokeny NFT

Wskazane kryptoaktywa są określane jako tokeny NFT (z ang. *non-fungible token*, czyli token niewymienialny) – są to tokeny niezamienne o unikalnym charakterze. Ich wyjątkowość może przejawiać się w szczególnych cechach technologicznych (zwykle reprezentowanych jako ciąg cyfr) i przypisanych im wartościach, przez co żaden token NFT nie jest identyczny[14]. Tokeny te mogą stanowić formę stokenizowanego dzieła sztuki albo być narzędziem do weryfikacji tożsamości.

W tym miejscu podkreślić należy, że sama specyfika techniczna nie decyduje o uznaniu za token NFT. Token unikalny powinien być niezastępowalny. W przedmiocie uznania tokenu NFT za podlegający MiCA wydane zostały wytyczne ESMA, w których wskazano, że „właściwe organy krajowe powinny opierać swoją ocenę tego, czy kryptoaktywo jest niewymienialne i unikalne na podstawie: wartości wewnętrznej i rzadkości (np. czy kryptoaktywa posiadają unikalne cechy, które przyczyniają się do ich wartości wewnętrznej i rzadkości, co sprawia, że są one odrębne od innych aktywów); własność i prawa (np. wyłączne prawa do dostępu lub użytkowania, które są unikalne dla posiadacza), użyteczności i funkcjonalności”[15]. ESMA wyjaśnia, że brak podlegania tokenów NFT pod regulację MiCA nie wyłącza tokenów NFT spod innych reżimów regulacyjnych. W ramach wytycznych ESMA, ustalenie czy token jest niewymienialny, może opierać się na teście „współzależnego testu wartości”. W ramach testu pod uwagę brane są trzy elementy oceny kryptoaktywa:

- czy wartość kryptoaktywów wynika przede wszystkim z unikalnych cech lub użyteczności/korzyści, jakie emitent oferuje posiadaczowi (np. konkretny niewymienialny token powiązany z ograniczoną edycją cyfrowego dzieła sztuki autorstwa renomowanego artysty);

- zakres, w jakim wzajemne powiązanie różnych rodzajów kryptoaktywów wpływa na ich wartość w taki sposób, że niewymienialny token nie ma sam w sobie żadnej wartości, która nie byłaby powiązana z innymi niewymienialnymi tokenami w serii lub zbiorze (np. istnienie wspólnej ceny transakcyjnej dla serii tokenów) oraz

- unikalne cechy charakterystyczne, które odróżniają te kryptoaktywa od innych[16]. Na przykład jeśli niewymienialne tokeny spełniają kryteria instrumentów finansowych zostaną objęte MiFID II i innymi odpowiednimi rozporządzeniami UE[17].

1.1.7.2. Instrumenty finansowe

W odniesieniu do kryptoaktywów, które są równocześnie instrumentami finansowymi, mogą zachodzić problemy kwalifikacyjne, które będą miały zasadnicze znaczenie dla późniejszej oceny spełnienia wymogów regulacyjnych. Uznanie kryptoaktywa za instrument finansowy prowadzi do wyłączenia stosowania do emisji oraz usług związanych z tym kryptoaktywem rozporządzenia MiCA i stosowania MiFID II.

W pierwszej kolejności należy wskazać, iż zgodnie z wytycznymi ESMA, **właściwe organy krajowe i uczestnicy rynku finansowego nie powinni uznawać formatu**

14 A. Bilski, *Rodzaje kryptoaktywów* [w:] A. Bilski, R. Kiełbus, *Kryptoaktywa i blockchain. Technologia, prawo, biznes*, Warszawa 2024, s. 25.

15 Wytyczne dotyczące klasyfikacji kryptoaktywów jako instrumentów finansowych, https://www.esma.europa.eu/sites/default/files/2025-03/ESMA75453128700-1323_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs_PL.pdf, (dostęp: 7 grudnia 2025 r., pkt 68).

16 ESMA, pkt 70.

17 ESMA, pkt 66.

technologicznego kryptoaktywów za czynnik decydujący przy ocenie ich kwalifikacji jako instrumentów finansowych. W związku z tym proces tokenizacji instrumentów finansowych nie powinien mieć wpływu na klasyfikację takich aktywów[18]. Powyższa zasada jest określana jako zasada neutralności technologicznej. Oznacza to, że przykładowo: akcje albo obligacje stanowią taki sam instrument finansowy, jeśli ich zdematerializowana forma posiada zapis zarówno oparty o technologię rozproszonego rejestru, jak i o inną technologię, tak jak jest to obecnie powszechne.

Kryptoaktywo kwalifikuje się jako instrument finansowy, jeśli mieści się w definicji zbywalnego papieru wartościowego, określonej w art. 4 ust. 1 pkt 44 MiFID II. Zdefiniowano w niej zbywalne papiery wartościowe, które „oznaczają rodzaje papierów wartościowych, które są zbywalne na rynku kapitałowym – z wyłączeniem instrumentów płatniczych" i obejmują akcje spółek, obligacje i sekurytyzowane wierzytelności, a także „wszelkie inne papiery wartościowe":

- dające prawo nabycia lub zbycia jakichkolwiek zbywalnych papierów wartościowych; lub
- „powodujące rozliczenie w środkach pieniężnych określane w odniesieniu do zbywalnych papierów wartościowych, walut, stóp procentowych lub stóp zwrotu, towarów i innych wskaźników lub mierników". Mogą one obejmować opcje, warranty i obligacje strukturyzowane, w przypadku których odsetki są powiązane z dowolnym instrumentem pochodnym (np. wybranym indeksem giełdowym, stopą procentową, innymi instrumentami pochodnymi lub kombinacją instrumentów pochodnych).

W takim przypadku kryptoaktywa powinny podlegać dokładnie tym samym przepisom, co tradycyjne instrumenty finansowe. **W celu ustalenia, czy kryptoaktywa kwalifikują się jako instrumenty finansowe, należy przyjąć podejście oparte na przewadze treści nad formą[19].**

W związku z tym właściwe organy krajowe i uczestnicy rynku finansowego powinni uznać, że wiarygodne kryteria klasyfikacji kryptoaktywa jako zbywalnego papieru wartościowego mogą obejmować:

- możliwość transferu i zamienność (zbywalność i przynależność do danej klasy) oraz
- posiadanie praw podobnych do praw dotyczących innych papierów wartościowych. Zgodnie z definicją zbywalnych papierów wartościowych zawartą w MiFID II, wszystkie wyżej wymienione kryteria muszą być spełnione, aby kryptoaktywo mogło zostać zakwalifikowane jako zbywalne papiery wartościowe[20].

W praktyce nierzadko kryptoaktywo daje prawo głosu w ramach tzw. DAO, w ramach którego są podejmowane decyzje przez posiadaczy tokenów o dalszym rozwoju projektu technologicznego albo o dalszym losie tokenów, które jeszcze nie zostały nabyte przez żaden podmiot. Takie tokeny wobec tego nie dość, że są zbywalne, to zaczynają przypominać w zakresie uprawnień akcje. W takich sytuacjach nasuwa się pytanie, czy tego typu tokeny nie prowadzą w istocie do nadawania uprawnień przypominających uprawnienia korporacyjne związane z głosem wspólnika na walnym zgromadzeniu udziałowców albo akcjonariuszy?

W zakresie oceny tego typu aktywów ESMA rozróżnia kryptoaktywa dające prawa głosu typowo związane z akcjami (np. prawa głosu w procesie decyzyjnym spółki), a tymi dającymi prawa do zarządzania, które są bardziej powiązane z decyzjami technicznymi lub operacyjnymi i które nie zapewniają posiadaczom żadnego wpływu na kwestie ładu korporacyjnego. Na przykład kryptoaktywa przyznające prawa głosu w procesie decyzyjnym spółki, umożliwiające posiadaczom udział w decyzjach dotyczących zarządzania (takich jak wybór członków zarządu, zatwierdzanie fuzji i przejęć) należy uznać za przyznające prawa głosu równoważne akcjom. Natomiast kryptoaktywa, które przyznawałyby prawa do zarządzania wyłącznie w odniesieniu do kwestii technicznych lub zmian operacyjnych, takich jak aktualizacje protokołów i korekty opłat, nie zapewniając posiadaczom żadnego wpływu na decyzje dotyczące zarządzania, nie powinny przyznawać praw równoważnych akcjom i należy je odróżnić od papierów wartościowych zapewniających tradycyjne uprawnienia akcjonariuszy. Nie zmienia to jednak

18 Wytyczne dotyczące klasyfikacji kryptoaktywów jako instrumentów finansowych, https://www.esma.europa.eu/sites/default/files/2025-03/ESMA75453128700-1323_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs_PL.pdf (dostęp: 16 listopada 2025 r., pkt 11).

19 Wytyczne dotyczące klasyfikacji kryptoaktywów jako instrumentów finansowych, pkt 13.

20 Wytyczne dotyczące klasyfikacji kryptoaktywów jako instrumentów finansowych, pkt 30.

faktu, że projekty kryptowalutowe są, co do zasady, projektami technologicznymi i niektóre decyzje związane ze zmianami technicznymi mogą bezpośrednio wpływać także na przychody, np. tokenariuszy, którzy uwierzytelniają sieć w ramach tzw. Stakingu, i tego typu rozróżnienie jest nieostre. Każda ocena tokenu powinna być dokonywana indywidualnie.

W odniesieniu do instrumentów pochodnych i kryptoaktywów właściwe organy krajowe i uczestnicy rynku finansowego powinni rozróżnić dwie sytuacje. W pierwszym przypadku, którego nie przewidziano w rozporządzeniu MiCA, kryptoaktywa służą jako aktywa bazowe na potrzeby instrumentów pochodnych. W drugim przypadku same kryptoaktywa można zakwalifikować jako instrumenty pochodne.

W pierwszym przypadku właściwe organy krajowe i uczestnicy rynku finansowego powinni rozważyć możliwość, aby kryptoaktywa były kwalifikowanymi aktywami bazowymi w instrumentach pochodnych. Właściwe organy krajowe i uczestnicy rynku finansowego powinny dopilnować, aby ich podejście do oceny takich instrumentów pochodnych było zgodne z kategoriami określonymi w sekcji C pkt 4-10 załącznika I do MiFID II.

Druga grupa dotyczy warunków i kryteriów kwalifikowania kryptoaktywów jako instrumentów pochodnych. Właściwe organy krajowe i uczestnicy rynku finansowego powinny w ramach swojej oceny rozważyć, czy:

- prawa posiadaczy kryptoaktywów są uzależnione od kontraktu opartego na przyszłym zobowiązaniu (które może mieć postać kontraktu terminowego typu forward, transakcji opcyjnych, swapu lub kontraktu terminowego typu future), tworzącego odstęp czasowy między zawarciem a wykonaniem zobowiązań wynikających z takiego kontraktu;

- wartość kryptoaktywów wywodzi się z wartości aktywów bazowych oraz

- podlega metodom rozrachunku, o których mowa w sekcji C pkt 4-10 załącznika I do MiFID II[21].

1.1.7.3. Kryptoaktywa stanowiące depozyty

Depozyt w podstawowym ujęciu to usługa finansowa, w której dostawca przyjmuje tytułem zwrotnym środki pieniężne od użytkowników[22].

Do celów wyłączenia z MiCA „depozyt" definiuje się poprzez odniesienie do art. 2 ust. 1 pkt 3 dyrektywy 2014/49/UE (dyrektywy w sprawie systemów gwarantowania depozytów; DGSD): „depozyt" oznacza saldo dodatnie wynikające ze środków pozostawionych na rachunku lub z sytuacji przejściowych wynikających ze zwykłych transakcji bankowych, które instytucja kredytowa jest zobowiązana spłacić zgodnie z obowiązującymi warunkami prawnymi i umownymi, w tym depozyt terminowy i depozyt oszczędnościowy, z wyłączeniem salda dodatniego, jeżeli:

a) jego istnienie może być udowodnione wyłącznie za pomocą instrumentu finansowego zdefiniowanego w art. 4 pkt 17 dyrektywy 2004/39/WE Parlamentu Europejskiego i Rady, chyba że jest to produkt oszczędnościowy, którego potwierdzeniem jest certyfikat depozytowy wystawiony na osobę wskazaną i istniejący w państwie członkowskim w dniu 2 lipca 2014 r.;

b) jego kapitał nie podlega spłacie według wartości nominalnej;

c) jego kapitał jest spłacany wyłącznie po wartości nominalnej na podstawie określonej gwarancji lub umowy udzielonej przez instytucję kredytową lub osobę trzecią.

Oznacza to, że depozyty, o których mowa w DGSD, w formie kryptoaktywów, nie są regulowane w ramach MiCA. Zamiast tego działalność polegająca na przyjmowaniu depozytów od osób prywatnych nadal podlega regulacjom CRD.

1.1.7.4. Kryptoaktywa hybrydowe

Pod wskazanym pojęciem rozumiane są kryptoaktywa, które wykazują cechy wspólne z przedmiotami wyłączonymi z regulacji MiCA. Aby ustalić, czy kryptoaktywa mają cechy hybrydowe, w pierwszej kolejności należy ocenić, czy spełniają one kryteria

21 Wytyczne dotyczące klasyfikacji kryptoaktywów jako instrumentów finansowych, pkt 44, 45, 46.

22 K. Korus, *Zakres przedmiotowy pojęcia kryptoaktywa w Rozporządzeniu MiCA*, MPB 2014, Nr 7–8, s. 33.

instrumentu finansowego. Jeżeli token hybrydowy wykazuje cechy instrumentu finansowego albo depozytu bankowego, taki charakter powinien mieć pierwszeństwo w jego klasyfikacji. Właściwe organy krajowe i uczestnicy rynku finansowego powinny wziąć pod uwagę, czy kryptoaktywa posiadają szereg cech, które komplikują ich klasyfikację (np. czy kryptoaktywa spełniają wiele ról lub łączą różne atrybuty, takie jak aspekty instrumentu finansowego, płatności i użyteczności; zakres, w jakim występowanie tych różnorodnych cech i funkcji przyczynia się do ogólnej definicji kryptoaktywa)[23].

1.2. Usługa w zakresie kryptoaktywów

1.2.1. Wprowadzenie

Aby móc wyjaśnić, jakie produkty bankowe podlegają regulacji MiCA (produkt bankowy na gruncie niniejszego opracowania rozumiany jest jako każda usługa świadczona przez bank), konieczne jest wyjaśnienie, jakie rodzajowo usługi mieszczą się w pojęciu usługi w zakresie kryptoaktywów. Wskazane pojęcie zostało zdefiniowane w art. 3 ust. 1 pkt 16 MiCA.

Zgodnie z przywołanym przepisem, „usługa w zakresie kryptoaktywów" jest rozumiana jako jedna z następujących usług lub rodzajów działalności związanej z kryptoaktywami:

- zapewnianie przechowywania kryptoaktywów i administrowania nimi w imieniu klientów;
- prowadzenie platformy obrotu kryptoaktywami;
- wymiana kryptoaktywów na środki pieniężne;
- wymiana kryptoaktywów na inne kryptoaktywa;
- wykonywanie zleceń związanych z kryptoaktywami w imieniu klientów;
- plasowanie kryptoaktywów;
- przyjmowanie i przekazywanie zleceń związanych z kryptoaktywami w imieniu klientów;
- doradztwo w zakresie kryptoaktywów;
- zarządzanie portfelem kryptoaktywów;
- świadczenie usług transferu kryptoaktywów w imieniu klientów.

Każda z wyżej wymienionych usług posiada definicję legalną. Jest to spowodowane z jednej strony wolą usunięcia wątpliwości interpretacyjnych w zakresie wykładni poszczególnych pojęć, z drugiej zaś potrzebą delimitacji poszczególnych rodzajów usług, z uwagi na różnice w wymaganiach regulacyjnych między nimi. Jak wskazuje się w literaturze, odniesienie do „rodzajów działalności" zawartych w definicji wydaje się mieć na celu jedynie podkreślenie, że omawiany, zbiorczy termin „usługi w zakresie kryptoaktywów" może być użyty zarówno w kontekście relacji pomiędzy dostawą usług a jego klientem, jak i w kontekście wewnątrzorganizacyjnych lub kontraktowych rozwiązań służących świadczeniu usług, lecz nieodnoszących się bezpośrednio do relacji z klientem[24]. Warte podkreślenia jest podobieństwo pomiędzy definicjami poszczególnych usług w zakresie kryptoaktywów do ich odpowiedników w Załączniku I do rozporządzenia MiFID II. W powołanym katalogu nie ma jedynie usługi transferu kryptoaktywów w imieniu klienta.

1.2.2. Zapewnianie przechowywania kryptoaktywów i administrowanie nimi w imieniu klientów

Pierwszą usługą jest „zapewnianie przechowywania kryptoaktywów i administrowanie nimi w imieniu klientów", potocznie nazywana custody, które oznacza sprawowanie pieczy nad kryptoaktywami lub kluczami dostępu do takich kryptoaktywów, w stosownych przypadkach w postaci prywatnych kluczy kryptograficznych, lub sprawowanie nad nimi kontroli w imieniu klientów. Usługa ta obejmuje każdy przypadek, gdy dostawca usług uzyskuje kontrolę nad kryptoaktywami klienta, z wyłączeniem innych osób. Uzyskanie takiej kontroli ma miejsce poprzez przejęcie danych dostępowych do powierzonych kryptoaktywów poprzez posiadanie prywatnych kluczy kryptograficznych. Z jednej strony wskazana usługa może służyć jedynie bezpiecznemu przechowywaniu kryptoaktywów; potocznie jest nazy-

23 Wytyczne dotyczące klasyfikacji kryptoaktywów jako instrumentów finansowych, pkt 74 i 76.

24 M. Rypina, M. Wierzbowski [w:] M. Rypina, M. Wierzbowski (red.), *Rozporządzenie w sprawie rynków kryptoaktywów. Komentarz* [w:] *Rozporządzenie w sprawie rynków kryptoaktywów (MiCA) i rozporządzenie pilotażowe DLT (DLT Pilot Regime). Komentarz*, Warszawa 2025, art. 3, Nb 18.

wana zimnym portfelem. Celem takiej usługi jest zabezpieczenie środków klienta przed wykonaniem błędnej lub nieautoryzowanej transakcji albo oszustwami prowadzącymi do utraty środków. Wskazana usługa może też być świadczona jako usługa dodatkowa do innych usług, np. wykonywanie zleceń nabycia lub zbycia kryptoaktywów – usługa jest wówczas związana z obrotem kryptoaktywami przez klienta (tzw. gorący portfel). Obecnie praktycznie każda scentralizowana giełda kryptowalutowa (np.: Binance, Kraken, KuCoin) świadczy wskazaną usługę w powiązaniu z innymi usługami.

1.2.3. Prowadzenie platformy obrotu kryptoaktywami

Kolejnym rodzajem usługi w zakresie kryptoaktywów jest „prowadzenie platformy obrotu kryptoaktywami", co oznacza zarządzanie co najmniej jednym systemem wielostronnym, który skupia interesy wielu stron trzecich, związane z nabywaniem i sprzedażą kryptoaktywów, lub który ułatwia skupianie takich interesów – w ramach tego systemu i zgodnie z jego zasadami – w sposób skutkujący zawarciem umowy, albo w drodze wymiany kryptoaktywów na środki pieniężne albo w drodze wymiany kryptoaktywów na inne kryptoaktywa. Potocznie ta usługa odpowiada głównej usłudze, jaką świadczą scentralizowane giełdy kryptowalutowe. Wskazana usługa w pierwszej kolejności zakłada istnienie „systemu obrotu kryptoaktywami", w dalszej czynności są przeprowadzane za pomocą platformy.

Rolą wskazanego systemu jest zwolnienie klienta z samodzielnego poszukiwania potencjalnego nabywcy na jego kryptoaktywa, gdyż czynią to za niego algorytmy platformy. Zasady systemu mogą przewidywać łączenie zleceń nabycia lub zbycia kryptoaktywów pochodzących od wielu stron jednocześnie. Dopuszczalne jest ustalenie zasad przewidujących umowy wielostronne, na przykład wówczas, gdy trzy strony mogą zrealizować swoje interesy wymiany kryptoaktywów, chociaż brak jest wzajemności tych interesów w ich bilateralnym zestawieniu (każda ze stron przekazuje lub otrzymuje aktywa od pozostałych dwóch stron trójstronnej umowy). W literaturze wyrażany jest pogląd, że prowadzenie usługi w zakresie platformy (systemu) obejmuje także platformy zdecentralizowane, które działają za pomocą smart contraktów[25].

1.2.4. Wymiana kryptoaktywów na środki pieniężne

Kolejną usługą jest wymiana kryptoaktywów na środki pieniężne, która oznacza zawieranie z klientami umów nabycia lub sprzedaży kryptoaktywów w zamian za środki pieniężne, z wykorzystaniem własnego kapitału.

Przedmiotowa działalność polega na nabywaniu lub zbywaniu kryptoaktywów na rachunek własny. W istocie przedmiotem transakcji jest kupno albo sprzedaż kryptoaktywów za pośrednictwem walut fiducjarnych albo kryptoaktywów uznanych za pieniądz elektroniczny. Podmioty, z którymi dostawca będzie zawierał transakcje, powinny być przez niego traktowane jako klienci. Podobnie jak w przypadku usługi wymiany walut, dostawca przedmiotowej usługi może samodzielnie ustalać kurs wymiany. W tym miejscu podkreślić należy, że zakresem usługi jest objęty tylko dostawca, który wskazaną działalność świadczy w sposób stały i zorganizowany. Takiej definicji nie będzie spełniał podmiot wymieniający co pewien czas znaczące środki na własne potrzeby, lecz nie prowadząc wskazanej działalności. Wskazana transakcja stanowi typową transakcję kantoru kryptowalutowego, która zarówno może polegać na ustawieniu stacjonarnego urządzenia do wymiany kryptoaktywów, jak również na usłudze świadczonej mobilnie lub stacjonarnie z udziałem osób.

1.2.5. Wymiana kryptoaktywów na inne kryptoaktywa

Następną usługą, podobną w swojej konstrukcji do wcześniej omówionej, jest „wymiana kryptoaktywów na inne kryptoaktywa". Oznacza to zawieranie z klientami umów nabycia lub sprzedaży kryptoaktywów w zamian za inne kryptoaktywa, z użyciem własnego kapitału, na rachunek własny. Warto podkreślić, że przedmiotem wymiany mogą też być stablecoiny niespełniające definicji pieniądza elektronicznego, lecz będące kryptoaktywami powiązanymi z aktywami. Cena za takie wymiany jest swobodnie ustalana przez dostawcę usług w zakresie kryptoaktywów. Omawiana usługa umożliwia wymianę kryptoaktywów na dowolne inne kryptoaktywa, niezależnie od ich płynności oraz ceny rynkowej i możliwości jej ustalenia.

25 M. Rypina, M. Wierzbowski [w:] M. Rypina, M. Wierzbowski (red.), *Rozporządzenie w sprawie rynków kryptoaktywów. Komentarz* [w:] *Rozporządzenie w sprawie rynków kryptoaktywów (MiCA) i rozporządzenie pilotażowe DLT (DLT Pilot Regime). Komentarz*, Warszawa 2025, art. 3, Nb 20.

1.2.6. Wykonywanie zleceń związanych z kryptoaktywami w imieniu klientów

Wykonywanie zleceń związanych z kryptoaktywami w imieniu klientów oznacza zawieranie w ich imieniu umów nabycia lub sprzedaży co najmniej jednego kryptoaktywa lub umów subskrypcji w imieniu klientów co najmniej jednego kryptoaktywa i obejmuje zawieranie umów sprzedaży kryptoaktywów w momencie ich oferty publicznej lub dopuszczenia do obrotu. Wskazana usługa sprowadza się do wykonywania czynności prowadzących do tego, aby klient nabył lub sprzedał kryptoaktywa. W tej relacji dostawca usług w ramach tej usługi jest pośrednikiem pomiędzy nabywcą i zbywcą. Świadczenie wskazanej usługi może dotyczyć zarówno rynku pierwotnego, jak i wtórnego.

1.2.7. Plasowanie kryptoaktywów

Plasowanie kryptoaktywów oznacza oferowanie kryptoaktywów nabywcom w imieniu lub na rachunek oferującego bądź osoby powiązanej z oferującym. Usługa ta polega na prezentowaniu oferty potencjalnym nabywcom i może obejmować szeroki zakres czynności marketingowych i dystrybucyjnych, pod warunkiem, że nie są to ogólne kampanie, ale kierowane do określonego grona potencjalnych inwestorów. Jednak gdy w wyniku plasowania dochodzi do transakcji kupna oferowanych kryptoaktywów przez inwestorów za pośrednictwem dostawcy, stanowi to usługę wykonywania zleceń związanych z kryptoaktywami.

1.2.8. Przyjmowanie i przekazywanie zleceń związanych z kryptoaktywami w imieniu klientów

Usługa „przyjmowania i przekazywania zleceń związanych z kryptoaktywami w imieniu klientów" oznacza przyjmowanie od danej osoby zleceń kupna lub sprzedaży co najmniej jednego kryptoaktywa bądź subskrypcji co najmniej jednego kryptoaktywa oraz przekazywanie takiego zlecenia do wykonania osobie trzeciej.

Przedmiotowa usługa jest rodzajem pośrednictwa, gdzie dostawca ją wykonujący nie jest tym dostawcą, który finalnie zrealizuje zlecenie klienta dotyczące zbycia lub nabycia kryptoaktywów, lecz jest jednym z usługodawców w łańcuchu pośredników występujących w ramach przyjętego modelu.

1.2.9. Doradztwo w zakresie kryptoaktywów

Doradztwo w zakresie kryptoaktywów oznacza oferowanie, udzielanie lub zgodę na udzielanie klientowi spersonalizowanych zaleceń – na żądanie klienta albo z własnej inicjatywy dostawcy usług w zakresie kryptoaktywów świadczącego doradztwo – w odniesieniu do co najmniej jednej transakcji związanej z kryptoaktywami lub korzystania z usług w zakresie kryptoaktywów. Rozpoczęcie świadczenia tej usługi następuje już od momentu udzielenia przez dostawcę zgody na udzielenie klientowi spersonalizowanych zaleceń dotyczących transakcji związanych z kryptoaktywami lub korzystania z usług w zakresie kryptoaktywów. Przedmiotowe doradztwo obejmuje również doradzanie w kwestii usług w zakresie kryptoaktywów, z których klient powinien skorzystać. W tym miejscu wskazać należy, że kluczowy jest termin „spersonalizowane", bowiem ogólna informacja kierowana do klientów nie stanowi spersonalizowanego doradztwa. Dla kwalifikacji usługi nie ma jednocześnie znaczenia, czy ostatecznie dostawca w sposób profesjonalny spersonalizował zalecenia na podstawie zgromadzonych informacji o kliencie, tj. czy trafnie ocenił odpowiedniość zalecanych kryptoaktywów dla danego klienta.

1.2.10. Zarządzanie portfelem kryptoaktywów

Zarządzanie portfelem kryptoaktywów oznacza zarządzanie portfelami zgodnie z upoważnieniami udzielonymi przez klientów wedle swobodnego uznania poszczególnych klientów, w przypadku gdy portfele te obejmują co najmniej jedno kryptoaktywo.

Powyższa definicja wskazuje, że uzyskane od klienta upoważnienie do zarządzania portfelem kryptoaktywów jest upoważnieniem do podejmowania decyzji w zakresie transakcji dotyczących kryptoaktywów oraz do podejmowania czynności zmierzających do realizacji tych decyzji w imieniu i na rachunek klienta. Termin „portfel" nie powinien być rozumiany równoznacznie z portfelami kryptograficznymi służącymi do przechowywania kryptoaktywów, lecz potocznie jako zbiór aktywów, w którym znajduje się co najmniej jedno kryptoaktywo[26].

26 M. Rypina, M. Wierzbowski [w:] M. Rypina, M. Wierzbowski (red.), *Rozporządzenie w sprawie rynków kryptoaktywów. Komentarz* [w:] *Rozporządzenie w sprawie rynków kryptoaktywów (MiCA) i rozporządzenie pilotażowe DLT (DLT Pilot Regime). Komentarz*, Warszawa 2025, art. 3, Nb 27.

1.2.11. Świadczenie usług transferu kryptoaktywów w imieniu klientów

Świadczenie usług transferu kryptoaktywów w imieniu klientów oznacza świadczenie, w imieniu osoby fizycznej lub prawnej, usług transferu kryptoaktywów z jednego adresu lub rachunku w rozproszonym rejestrze do innego.

Wskazana usługa sprowadza się do przesłania kryptoaktywa z jednego adresu portfela albo rachunku na inny. Usługa transferu może więc mieć charakter samoistny albo być elementem innej usługi w zakresie kryptoaktywów, jeżeli jest ona funkcjonalnie powiązana z daną usługą. W tym miejscu należy podkreślić, że samo stworzenie infrastruktury w postaci portfela walut wirtualnych (EVM), z którego każdy posiadacz może wykonać transfer, jeszcze nie stanowi świadczenia usług, gdyż transferu dokonuje dysponent portfela, a nie podmiot, który go stworzył. Transakcje są realizowane na blockchainie, nie zaś poprzez podmiot trzeci. To z kolei sprawia, że podmioty, które są twórcami portfeli, nie podlegają pod MiCA.

W literaturze wskazano, że usługą transferu nie powinny być kwalifikowane czynności podmiotów zatwierdzających, węzłów ani „górników", którzy mogą być częścią procesu zatwierdzania transakcji i aktualizacji stanu rozproszonego rejestru[27].

1.3. Produkty bankowe, które mogą podlegać Regulacji MiCA

Pytanie dotyczy tego, które z oferowanych przez bank produktów mogą podlegać Regulacji MiCA. Ponieważ produkt bankowy rozumiany jest jako każda usługa świadczona przez bank, odpowiedź wymaga odwołania się do ustaleń przedstawionych w poprzednich partiach opracowania.

1.3.1. Tokeny depozytowe i stokenizowane depozyty

Na wstępie warto rozróżnić tokeny depozytowe od stokenizowanych depozytów. Tokeny depozytów bankowych (*deposit tokens*) stanowią nową formę pieniądza bankowego, w której depozyt bankowy jest reprezentowany jako token na blockchainie, ale token istnieje jako odrębny instrument cyfrowy, emitowany przez bank w miejsce tradycyjnego depozytu. W ramach wskazanego produktu bank reprezentuje depozyt klientów jako token (zwykle na *permissioned chain*) umożliwiający szybkie rozliczenia i płatności wewnątrz sieci. Wskazane depozyty są pieniądzem bankowym w formie cyfrowej, a nie klasycznym depozytem. Natomiast sam token stanowi nowy instrument emitowany w oparciu o depozyt: może być zbywalny (transferowalny) między użytkownikami blockchain albo też nie posiadać takiej właściwości.

Wskazane produkty bankowe mogą funkcjonalnie przypominać stablecoiny, ale różnią się brakiem ryzyka emitenta i pełnym pokryciem depozytowym. Przykładem może być JPM Coin (JP Morgan) – token reprezentujący depozyt w USD, służący do rozliczeń instytucjonalnych. Takie tokeny, w świetle rozporządzenia MiCA, mogą nie być objęte jego zakresem, jeśli nie są transferowalne, jednak jeśli można je przenosić, to podlegają pod MiCA, przy czym wtedy mogą być uznane za token powiązany z aktywami albo za token będący pieniądzem elektronicznym.

Inną kategorię stanowią stokenizowane depozyty bankowe (*tokenized deposits*). To tradycyjny depozyt bankowy, który pozostaje depozytem w sensie prawnym, ale jest zapisywany, przenoszony lub rozliczany za pomocą technologii DLT/blockchain. Wskazane depozyty stanowią w istocie zapis środków pieniężnych znajdujących się w depozycie za pomocą technologii blockchain. Z perspektywy prawnej jest to zwykły depozyt. Token jest tylko technicznym odwzorowaniem zapisów księgowych. W ramach takiego depozytu nie tworzy się odrębnych pieniędzy elektronicznych. Takie depozyty nie są regulowane przepisami MiCA[28].

Podsumowując, jak wskazuje K. Korus, oceniając kryptoaktywa pod kątem depozytu należy szczegółowo oceniać właściwe prawa i obowiązki. Nabycie kryptoaktywa i następnie jego zbycie w trybie normalnego obrotu kryptoaktywem nie stanowi *per se* depozytu tylko dlatego, że może się zdarzyć, że jego

27 M. Rypina, M. Wierzbowski [w:] M. Rypina, M. Wierzbowski (red.), *Rozporządzenie w sprawie rynków kryptoaktywów. Komentarz* [w:] *Rozporządzenie w sprawie rynków kryptoaktywów (MiCA) i rozporządzenie pilotażowe DLT (DLT Pilot Regime). Komentarz*, Warszawa 2025, art. 3, Nb 28.

28 https://www.eba.europa.eu/sites/default/files/2024-12/4b294386-1235-463f-b9b5-08f255160435/Report%20on%20Tokenised%20deposits.pdf (dostęp: 30 listopada 2025 r.).

posiadacz przekazuje na końcu kryptoaktywo podmiotowi będącemu jego wydawcą i odzyskuje kwotę, którą zapłacił przy nabyciu. W obecnym stanie prawnym działalność depozytowa obejmuje przyjmowanie pod tytułem zwrotnym środków pieniężnych, a nie dowolnych aktywów. Rozporządzenie MiCA nie ma więc zastosowania do tokenów depozytowych za środki pieniężne. Nie ma przy tym znaczenia, czy zostaje wydana określona pula tokenów czy jeden token odpowiadający wartości depozytu29. Istotne jest to, aby depozytariusz otrzymał dokładną sumę środków pieniężnych o wartości nominalnej w zamian za tokeny.

1.3.2. Bank-issued stablecoins oraz rozrachunki do płatności w oparciu o e-money

Bank-issued stablecoiny stanowią stablecoiny wydawane albo współwydawane przez banki lub konsorcja banków, przeznaczone do płatności i rozliczeń. To obszar, w którym MiCA ma bezpośrednie znaczenie; bank może być emitentem tokenów stanowiących pieniądz elektroniczny oraz tokenów powiązanych z aktywami.

O przesądzeniu, czy istnieje e-money, w pierwszej kolejności należy zbadać, czy wskazane stablecoiny mają swoje cyfrowe odwzorowanie w ramach technologii rozproszonego rejestru i mieszczą się w definicji tokenów stanowiących pieniądz elektroniczny. Najważniejszą konsekwencją jest to, czy posiadacz tokenu musi posiadać roszczenie do wymiany jednego tokenu na jednostkę waluty fiducjarnej.

Celem oceny, czy dane aktywo stanowi e-money, do którego ma zastosowanie rozporządzenie MiCA należy odpowiedzieć na poniższe pytania:

- Czy token jest wydawany i zapisany na DLT/rejestrze rozproszonym (*on-chain*)?
- Czy token posiada referencję do **jednej z** oficjalnych walut (np. EUR albo USD) i deklaruje utrzymanie wartości?
- Czy token daje posiadaczowi prawo do **bezwarunkowego wykupu 1:1** w tej walucie?
- Czy token jest **transferowalny** między użytkownikami?
- Czy produkt ma cechy usługi płatniczej (przyjmowanie płatności, realizacja przelewów)?

Pozytywna odpowiedź na powyższe pytania oznacza, że dany token i usługi na nim oparte stanowią e-money (emisji, prowadzenia rachunku, transferu środków), a w związku z tym będzie podlegał regulacji MiCA, jak i EMD2. Możliwe jest także stosowanie PSD2.

1.3.3. Emisja i obrót stokenizowanymi obligacjami

W odniesieniu do tego typu produktów bank może występować w kilku rolach: może być agentem emisji, pośrednikiem w obrocie wskazanymi instrumentami lub emitentem. Dla rozstrzygnięcia, czy rozporządzenie MiCA ma zastosowanie do powyższego produktu bankowego, wystarczające jest przesądzenie o charakterze prawnym samej tokenizowanej obligacji. Wskazane obligacje dają możliwość automatyzacji wykupu obligacji oraz wypłat odsetek przez smart kontrakty.

W tym miejscu podkreślić należy, że w przypadku, kiedy wskazane produkty stanowią instrument finansowy w rozumieniu MIFID II, zastosowania nie będzie miało MiCA. Jak wskazuje ESMA*:* „W odniesieniu do klasy „obligacje i inne formy sekurytyzowanych wierzytelności", pod warunkiem że instrumenty te są *zbywalne na rynku kapitałowym,* właściwe organy krajowe i uczestnicy rynku finansowego powinni zauważyć*,* że kryptoaktywa, które reprezentowałyby dług podobny do długu pieniężnego, taki jak część pożyczki należnej od emitenta posiadaczowi kryptoaktywów, należy uznać *za papiery* wartościowe o cechach charakterystycznych dla obligacji. To samo dotyczy długu, który zostałby włączony do papieru wartościowego, z wyłączeniem obligacji lub instrumentów rynku pieniężnego. Jako przykład właściwe organy krajowe i uczestnicy rynku finansowego mogą rozważyć *przypadek* spółki, która wyemitowałaby kryptoaktywa zapewniające ich posiadaczom regularne płatności odsetek lub obiecujące spłatę *kwoty* głównej w przyszłości. Takie tokeny należy uznać *za* należące do klasy papierów wartościowych podobnych do obligacji ze względu na ich cechy reprezentujące *dług"*[30].

29 T. Korus, *Zakres przedmiotowy pojęcia kryptoaktywa w Rozporządzeniu MiCA*, MPB 2014, Nr 7–8, s. 33–34.

30 https://www.esma.europa.eu/sites/default/files/2025-03/ESMA75453128700-1323_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs_PL.pdf, pkt 25,26.

Można zaobserwować, że już w tej chwili dochodzi do emisji stokenizowanych obligacji, a emitentami są zarówno komercyjne banki oraz firmy inwestycyjne, jak i Europejski Bank Inwestycyjny. Przykładem może być emisja obligacji w pełni stokenizowanych na blockchainie ethereum w 2019 roku przez Bank Santander[31]. Z kolei w kwietniu 2021 roku Europejski Bank Inwestycyjny wyemitował tzw. „*digital bond*" o wartości 100 mln EUR na publicznej sieci Ethereum. Był to pierwszy przypadek, w którym instytucja UE zdecydowała się na dług tokenizowany, a emisja była „*multi-dealer led*" (współpraca z wieloma bankami – koordynatorami, m.in. Goldman Sachs, Société Générale oraz Santander). W komunikacie Europejskiego Banku Inwestycyjnego wskazano, że celem było pokazanie, iż rynki kapitałowe są gotowe na blockchainowe emisje, co ma przynieść oszczędności, większą transparentność i sprawniejsze rozliczenia[32].

1.3.4. Usługa powiernicza (crypto custody)

Usługa powiernicza, określona w MiCA jako „*custody and administration of crypto-assets on behalf of clients*", polega na przechowywaniu oraz administrowaniu kryptoaktywów klienta. Usługa ta dotyczy wszystkich rodzajów kryptoaktywów, a jej głównym celem jest zabezpieczenie kryptoaktywów klienta. W istocie każdy klient mógłby sam zainstalować portfel sprzętowy na telefonie i sam za niego brać odpowiedzialność, ponosząc ryzyko utraty środków, co w przypadku rynku kryptowalut nierzadko ma miejsce. Wskazana usługa jest bezwarunkowo regulowana przepisami rozporządzenia MiCA. Składa się na nią wiele elementów, choć nie wszystkie muszą wystąpić łącznie, to w praktyce powinno tak być, aby usługa odpowiadała przepisom prawa.

Po pierwsze, w ramach usługi *custody* podmiot świadczący usługę (custodian) zapewnia faktyczną i techniczną kontrolę nad kluczami prywatnymi umożliwiającymi dysponowanie kryptoaktywami klienta. To oznacza, że klient powierza swoje kryptoaktywa bankowi, zamiast samodzielnie zabezpieczać klucze. Równocześnie klient, co do zasady, nie zna swojego klucza prywatnego, a zna go tylko bank lub inny podmiot świadczący usługę custody.

Po drugie, dostawca usługi (*custodian*) prowadzi rejestr praw klienta i odpowiada za odwzorowanie ich pozycji na odpowiednich adresach blockchain lub w portfelach wewnętrznych. Obejmuje to między innymi: aktualizację sald, obsługę zdarzeń łańcucha bloków (forki, airdropy, migracje tokenów), czy przyjmowanie i wykonywanie zleceń transferu aktywów. Zgodnie z wyjaśnieniami ESMA, podmiot świadczący usługę custody musi niezwłocznie odzwierciedlać wszelkie zdarzenia na DLT, które tworzą lub modyfikują prawa klienta. Usługobiorca ma prawo do aktywów utworzonych w wyniku takiego zdarzenia, chyba że umowa stanowi inaczej[33]. Ten ostatni element będzie stanowił element innej usługi w postaci transferu kryptoaktywów.

Po trzecie, podmiot świadczący wskazaną usługę zapewnia zabezpieczenie aktywów, co może nastąpić między innymi poprzez:

1) zabezpieczenia kryptograficzne (HSM, multisig),
2) polityki bezpieczeństwa i kontroli dostępu,
3) segmentację portfeli (cold/warm/hot),
4) procedury odzyskiwania kluczy.

Jest to kluczowa część usługi i jej sens polega na profesjonalnym i regulowanym zabezpieczeniu majątku klienta. Warto także wskazać, że MiCA wymaga prowadzenia rejestru pozycji, który ukazuje, jakie aktywa *custodian* posiada w imieniu każdego klienta oraz na których portfelach są one przechowywane. Rejestr musi być stale aktualizowany i przejrzysty, aby w razie upadłości lub sporu możliwe było szybkie i jednoznaczne ustalenie własności.

1.3.5. Systemy rozliczeń oraz rozrachunku oparte o technologię rozproszonego rejestru wraz usługą transferu aktywów

Jest to infrastruktura (platformy, systemy), które wykorzystują rozproszony rejestr (blockchain/DLT) do prowadzenia handlu, rozliczania i/lub rozrachunku transakcji instrumentów finansowych lub tokenów, którymi mogą być np.: DLT-MTF (platforma obrotu), DLT-SS (system rozrachunku) lub połączone DLT-TSS (*trading + settlement*). Funkcje obejmują

31 https://www.santander.com/en/press-room/press-releases/santander-launches-the-first-end-to-end-blockchain-bond (dostęp: 29 listopada 2025 r.).

32 https://www.eib.org/en/stories/cryptocurrency-blockchain-bonds (dostęp: 29 listopada 2025 r.).

33 https://www.esma.europa.eu/publications-data/questions-answers/2290, (dostęp: 7 grudnia 2025 r.).

księgowanie transferów, rejestrowanie własności tokenów, *settlement* (przeniesienie prawa własności i/lub płatności) oraz czasem *custody* kluczy/*asset-management*.

Przykładowo DLT settlement to proces **finalizacji transakcji finansowej w rozproszonej bazie danych (blockchain/*distributed ledger*)**, gdzie aktywa (np. tokeny, papiery wartościowe, stablecoiny) są przenoszone między stronami w sposób trwały i nieodwracalny.

DvP (*Delivery versus Payment*) oznacza mechanizm, w którym **dostawa aktywów odbywa się jednocześnie z płatnością** – gwarantując, że transfer aktywów nie nastąpi, jeśli nie zostanie równocześnie dokonana zapłata.

***Atomic settlement* oznacza** pojedynczą, niepodzielną transakcję, w której przelew i płatność są rozliczane w tym samym momencie, minimalizując ryzyko kontrahenta (*counterparty risk*).

Wskazane modele transakcyjne mogą być atrakcyjne, gdyż prowadzą do redukcji ryzyka kontrahenta i operacyjnego, skrócenia cyklu rozliczenia, przejrzystość i audytowalność.

W kontekście prawnym warto wskazać, że MiCA znajdzie zastosowanie, jeśli system obsługuje crypto-assets, które nie kwalifikują się jako „*financial instruments*" (tj. typowe tokeny/coiny objęte MiCA). MiCA może mieć zastosowanie do: emitentów tokenów, w e-money tokens, asset-referenced tokens, innych crypto-assets) oraz dostawców usług związanych z tymi tokenami (CASP). Jeżeli jednak infrastruktura i oferowane usługi dotyczą tylko tokenów, stanowiących instrumenty finansowe w rozumieniu MiFID II, to zastosowanie znajdzie to rozporządzenie. Jeśli zaś jedno i drugie, to wtedy obie regulacje będą miały zastosowanie. Warto wskazać, że w tej sytuacji znajdą zastosowanie również inne akty unijne, takie jak DORA.

1.3.6. Cross-border payments w oparciu o stablecoin rails

Płatności transgraniczne w oparciu o *stablecoin rails* to wykorzystanie stablecoinów (tokenów o stabilnej wartości powiązanej z walutą fiat) i infrastruktury DLT jako „torów rozliczeniowych" do przesyłania wartości między podmiotami i jurysdykcjami. Zamiast tradycyjnego łańcucha korespondentów i systemów rozliczeniowych, płatność jest zamieniana na stablecoina po stronie nadawcy, przesyłana on-chain i zamieniana z powrotem na walutę lokalną u odbiorcy – skracając czas rozliczenia i redukując koszty. Usługa ta umożliwia przesył płatności, który odbywa się w sekundach albo minutach oraz daje możliwość śledzenia transakcji[34].

Wskazana usługa stanowi transfer kryptoaktywów i bezwzględnie podlega pod przepisy MiCA w zakresie usługi transferu kryptoaktywów, albowiem dochodzi do zamiany waluty urzędowej na tokeny stanowiące pieniądz elektroniczny albo tokeny powiązane z aktywami.

34 https://www.bis.org/cpmi/publ/d220.pdf (dostęp: 30 listopada 2025 r.).

PROGRAM ANALITYCZNO BADAWCZY

2. Działalność banków w branży kryptoaktywów

2.1. Geneza art. 60 MiCA

Analizując obecną treść art. 60 ust. 1 MiCA, zwrócić należy uwagę na istotną różnicę względem wcześniejszych wersji projektu MiCA z 2020 r., które zawierały sformułowanie *„may provide crypto-asset services without obtaining authorisation"*. W wersji ostatecznej z 2023 r. legislator dodał konkretne terminy proceduralne i wymogi informacyjne.

W pierwotnym projekcie rozporządzenia *Markets in Crypto-Assets* przedstawionym przez Komisję Europejską we wrześniu 2020 r., art. 53 (odpowiednik obecnego art. 60) brzmiał nieco inaczej[35]. Oznaczało to, że banki – jako instytucje kredytowe w rozumieniu CRD IV – automatycznie nabywały status CASP (*Crypto-Asset Service Provider*), bez żadnego wymogu notyfikacyjnego czy kontrolnego. Ta wersja była szeroko krytykowana w toku konsultacji publicznych przez EBA, ESMA oraz Europejski Bank Centralny, które wskazywały, że całkowite zwolnienie banków z obowiązku informacyjnego pozbawia organy nadzoru wiedzy o zakresie działalności kryptoaktywnej36.

W toku prac Rady UE (tzw. *Council General Approach*, listopad 2021 r.) oraz Parlamentu Europejskiego (sprawozdanie ECON z marca 2022 r.) wprowadzono zasadniczą modyfikację:

- zamiast pełnego zwolnienia z autoryzacji, dodano obowiązek uprzedniego powiadomienia właściwego organu (*notification procedure*),
- wprowadzono minimalny termin 40 dni roboczych,
- oraz obowiązek przekazania zestawu informacji określonych w ust. 7 – czyli planu działalności, procedur AML, IT, governance i ochrony klienta[37].

Uzasadnieniem tych zmian było „zapewnienie właściwego nadzoru nad działalnością instytucji kredytowych w zakresie kryptoaktywów, przy jednoczesnym uniknięciu podwójnej autoryzacji"[38].

W finalnym tekście przyjętym przez Parlament Europejski i Radę (Regulation (EU) 2023/1114, OJ L 150, 9 June 202339) art. 60 ust. 1 otrzymał następujące brzmienie:

„Instytucja kredytowa może świadczyć usługi w zakresie kryptoaktywów, jeżeli co najmniej 40 dni roboczych przed rozpoczęciem świadczenia tych usług przekaże właściwemu organowi macierzystego państwa członkowskiego informacje, o których mowa w ust. 7".

Opisana wyżej zmiana ma kluczowe znaczenie normatywne. Wersja końcowa:

- zachowuje wyjątek od obowiązku licencyjnego CASP (banki nie potrzebują nowego zezwolenia),
- wprowadza obowiązek proceduralny i informacyjny, stanowiący formę *ex ante* nadzoru.

W praktyce zmiana ta przekształciła mechanizm z czysto deklaratywnego (*ex lege authorisation*) w model „notyfikacji warunkowej", w którym rozpoczęcie działalności jest dopuszczalne dopiero po spełnieniu wymogów formalnych i upływie terminu 40 dni.

Europejski Urząd Nadzoru Bankowego (EBA) w swoim stanowisku z 2021 r. (EBA Response to MiCA Proposal) podkreślił, że *„the absence of a notification requirement for credit institutions could undermine the objective of supervisory convergence across Member States"*[40]. Podobne stanowisko zajął Europejski Bank Centralny, wskazując, że brak obowiązku informacyjnego utrudni monitorowanie ekspozycji banków na ryzyka kryptowalutowe i może „prowadzić do asymetrii informacyjnej między nadzorcami bankowymi a rynkiem finansowym"41.

Włączenie 40-dniowego okresu i obowiązkowych informacji z ust. 7 art. 60 jest więc kompromisem legislacyjnym – uznaniem, że banki nie potrzebują drugiej licencji, ale powinny działać w reżimie transparentnego nadzoru informacyjnego.

35 *Credit institutions authorised under Directive 2013/36/EU may provide crypto-asset services without obtaining an authorisation as a crypto-asset service provider under this Regulation.*

36 European Banking Authority, *Opinion on the European Commission's Proposal for MiCA* (EBA 2021), p. 3–5.

37 Council of the EU, General Approach on MiCA, Council Document 13590/21, November 2021, Annex p. 54–56.

38 Regulation (EU) 2023/1114 (MiCA), Recital (99).

39 Regulation (EU) 2023/1114, OJ L 150, 9 June 2023.

40 European Banking Authority, Consultation Paper on Draft Regulatory Technical Standards under MiCA (EBA/CP/2023/09), p. 4.2.1.

41 European Central Bank, Opinion on the Proposal for a Regulation on Markets in Crypto-assets (CON/2021/4), p. 6–7.

Z perspektywy praktyki nadzorczej i bankowej zmiana redakcyjna oznacza, że:

- status CASP nie powstaje już automatycznie, lecz dopiero po notyfikacji i braku sprzeciwu;
- organ nadzoru (KNF) zyskuje realny instrument kontroli *ex ante* nad działalnością banku w sektorze krypto;
- ESMA otrzymuje lepsze dane o strukturze rynku i może prowadzić centralny rejestr usług CASP;
- cała procedura wpisuje się w zasady proporcjonalności (art. 5 TUE) oraz subsydiarności – pozwala nadzorować rynek bez tworzenia nowych, dublujących licencji.

2.2. Zagadnienia wstępne

Jak już wskazano, rozporządzenie MiCA stworzyło pierwszy w Unii Europejskiej spójny i kompleksowy system regulacyjny, dotyczący kryptoaktywów oraz podmiotów świadczących usługi w tym obszarze. Regulacja obejmuje zarówno zasady emisji tokenów (w tym tokenów powiązanych z aktywami oraz tokenów będących e-pieniądzem), jak i reżim działalności usługowej, definiując szczegółowo kategorię dostawców usług w zakresie kryptoaktywów (CASP). Co do zasady, świadczenie usług takich jak przechowywanie kryptoaktywów, prowadzenie platform obrotu, wykonywanie zleceń, wymiana czy doradztwo, wymaga uzyskania zezwolenia właściwego organu nadzoru oraz spełnienia szerokiego katalogu wymogów ostrożnościowych, operacyjnych i technologicznych. W odniesieniu do instytucji kredytowych, MiCA wprowadza jednak rozwiązanie szczególne. Zgodnie bowiem z art. 60 rozporządzenia, banki mogą świadczyć usługi w zakresie kryptoaktywów bez konieczności uzyskania zezwolenia CASP, pod warunkiem uprzedniego przekazania właściwemu organowi – w Polsce Komisji Nadzoru Finansowego – kompletu informacji dotyczących planowanej działalności, struktury operacyjnej, systemów ICT, procedur AML oraz zasad ochrony aktywów klientów. Artykuł 60 MICA nie tworzy z banków CASP „z mocy prawa", lecz przyznaje im możliwość wejścia na rynek kryptoaktywów w trybie notyfikacyjnym, z zachowaniem pełnej odpowiedzialności za zgodność działalności z wymogami MiCA, DORA, CRR/CRD oraz krajowych regulacji nadzorczych.

Znaczenie art. 60 wykracza poza samą procedurę. Regulacja ta *de facto* uznaje, że banki – jako podmioty o wysokim poziomie regulacyjnym i nadzorczym – mogą świadczyć usługi krypto „wewnątrz" istniejących ram prudencyjnych, o ile potrafią wykazać odpowiedni poziom bezpieczeństwa technologicznego, odporności operacyjnej i zarządzania ryzykiem. Jednocześnie wejście banków w sektor kryptoaktywów rodzi szereg pytań praktycznych i strategicznych:

- czy konieczne jest wydzielenie działalności krypto w strukturze organizacyjnej banku?
- jakie są minimalne wymogi kapitałowe i technologiczne?
- jak wygląda ocena ryzyk operacyjnych, rynkowych i reputacyjnych?
- oraz jakie standardy nadzorcze będą stosowane przez KNF w procesie oceny notyfikacji?

W związku z powyższym, niniejszy rozdział ma na celu przedstawienie roli banków w reżimie MiCA oraz identyfikację konsekwencji regulacyjnych wynikających z wejścia instytucji kredytowych w sektor kryptoaktywów. Analiza koncentruje się na trzech kluczowych zagadnieniach:

- Jakie obowiązki MiCA nakłada na banki oferujące produkty oparte o kryptoaktywa?
- Czy banki muszą składać odrębny wniosek o licencję CASP, czy wystarczająca jest licencja bankowa?
- Które produkty bankowe podlegają MiCA i jak klasyfikować produkty hybrydowe?

Nie sposób tym samym pominąć wymogów dotyczących notyfikacji działalności na podstawie art. 60 MiCA, wymogów organizacyjnych, operacyjnych i technologicznych, zasad ochrony aktywów klientów, a także obowiązków w zakresie AML/CFT, przejrzystości czy cyberbezpieczeństwa.

Niezbędne jest także podjęcie próby wyjaśnienia różnicy między standardowym reżimem licencyjnym CASP a szczególną ścieżką przewidzianą dla instytucji kredytowych. W szczególności, o ile zostanie wykazane, że banki nie muszą uzyskiwać licencji CASP, to jednak muszą spełnić pełen katalog wymogów merytorycznych MiCA oraz przygotować dokumentację opisującą sposób świadczenia usług.

Ponadto przedstawiona zostanie klasyfikacja produktów, które mogą zostać uznane za kryptoaktywa lub usługi w zakresie kryptoaktywów, a także granice pomiędzy MiCA a regulacjami dotyczącymi instrumentów finansowych i pieniądza elektronicznego.

Połączenie powyższych zagadnień ma w założeniu pozwolić na ocenę, w jakim zakresie banki mogą rozwijać innowacyjne produkty cyfrowe oparte na technologii DLT (*Distributed Ledger Technology*), jakie obowiązki regulacyjne wiążą się z ich oferowaniem oraz jakie ryzyka należy uwzględnić przy projektowaniu i wdrażaniu takich usług.

2.3. Obowiązki wynikające z MiCA dla banków oferujących produkty oparte o kryptoaktywa – szczególny reżim art. 60

Artykuł 60 ust. 1 MiCA umożliwia instytucjom kredytowym rozpoczęcie świadczenia usług w zakresie kryptoaktywów na podstawie samej notyfikacji, składanej co najmniej 40 dni roboczych przed rozpoczęciem działalności[42]. Wprowadza on szczególny, uproszczony tryb, który umożliwia bankom rozpoczęcie świadczenia usług w zakresie kryptoaktywów bez konieczności uzyskania odrębnej licencji CASP, o ile instytucja złoży właściwemu organowi – w Polsce Komisji Nadzoru Finansowego – kompletną notyfikację o planowanej działalności. Konstrukcja tego przepisu odzwierciedla podejście ustawodawcy unijnego, który przyjmuje, że banki jako podmioty o najwyższym stopniu regulacji i nadzoru powinny mieć możliwość wejścia na rynek krypto w sposób mniej obciążający administracyjnie niż standardowi dostawcy usług krypto.

Opisywane uprawnienie obejmuje cztery fundamentalne elementy.

1. Rezygnacja z procedury licencyjnej, ale nie ze standardów regulacyjnych.

Instytucje kredytowe nie muszą uzyskiwać licencji CASP, ale podlegają wszystkim materialnym wymogom MiCA stosowanym do dostawców usług krypto, w tym:

- wymogom dotyczącym przechowywania i administrowania kryptoaktywami,
- zasadom realizacji zleceń i prowadzenia platformy obrotu,
- wymogom technologicznym, cyberbezpieczeństwa i odporności operacyjnej (powiązanie z DORA),
- wymogom informacyjnym i ochrony klienta,
- wymogom AML/CFT, obejmującym ocenę ryzyka oraz monitoring transakcji on-chain.

Jedynymi obszarami, z których banki są zwolnione, są:

- obowiązek uzyskania licencji CASP,
- wymogi funduszy własnych właściwe dla CASP,
- procedura zatwierdzania znaczących akcjonariuszy przewidziana dla CASP.

Wszystkie te elementy są już regulowane w ramach CRD/CRR i nadzoru bankowego.

2. Uprawnienie banków do świadczenia pełnego katalogu usług CASP.

Artykuł 60 MiCA nadaje instytucjom kredytowym generalne uprawnienie do świadczenia wszystkich usług w zakresie kryptoaktywów, które zdefiniowano w MiCA, pod warunkiem skutecznego dokonania notyfikacji. Oznacza to, że w teorii bank może świadczyć każdy rodzaj usług CASP, w tym:

- przechowywanie i administrowanie kryptoaktywami,
- wymianę kryptoaktywów,
- wykonywanie zleceń,
- prowadzenie platformy obrotu,
- doradztwo i zarządzanie portfelem krypto,
- plasowanie kryptoaktywów,
- transfer kryptoaktywów,
- usługi związane z wyceną, ustalaniem cen, politykami handlowymi.

42 Art. 60. 1. Instytucja kredytowa może świadczyć usługi w zakresie kryptoaktywów, jeżeli co najmniej 40 dni roboczych przed rozpoczęciem świadczenia tych usług przekaże właściwemu organowi macierzystego państwa członkowskiego informacje, o których mowa w ust. 7.

Zakres ten jest szerszy niż w przypadku firm inwestycyjnych, które mogą korzystać z procedury notyfikacji tylko w odniesieniu do usług uznanych za „równoważne" usługom MiFID II (art. 60 ust. 3). W odniesieniu do banków ustawodawca unijny zdecydował się tym samym na rozwiązanie maksymalnie elastyczne.

Motyw 78 MiCA wskazuje jednak, że uprawnienie to nie uchyla przepisów krajowych transponujących CRD IV. Oznacza to, że:

- bank może świadczyć dane usługi krypto tylko w zakresie, w jakim pozwala na to jego statut,
- rozpoczęcie świadczenia określonej kategorii usług wymaga zapewnienia zgodności również z krajowym prawem bankowym.

W zależności od losów uchwalonej ustawy o kryptoaktywach, w Polsce będzie to zapewne wymagało zmiany statutu banku za zgodą KNF, zgodnie z projektowaną nowelizacją Prawa bankowego[43]. Artykuł 34 Pr. bank. stanowi bowiem, że w zezwoleniu na utworzenie banku Komisja Nadzoru Finansowego określa: firmę banku, jego siedzibę, nazwy (nazwiska) założycieli i obejmowane przez nich akcje, wysokość kapitału założycielskiego, przedmiot działalności, do wykonywania którego bank jest upoważniony, oraz warunki, po spełnieniu których Komisja Nadzoru Finansowego zezwoli na rozpoczęcie przez bank działalności, a także zatwierdza projekt statutu banku oraz skład pierwszego zarządu banku, a zmiana statutu banku wymaga zezwolenia Komisji Nadzoru Finansowego. Zezwolenie na zmianę statutu może określać termin, do którego powinna być podjęta uchwała. W przypadku niepodjęcia uchwały we wskazanym terminie decyzja wygasa.

3. Charakter notyfikacji – funkcjonalny odpowiednik licencji CASP.

Choć procedura notyfikacyjna banków nie ma charakteru licencyjnego, jej funkcja jest zbliżona do procesu „autoryzacyjnego":

- organ nadzoru (KNF) ocenia kompletność dokumentacji,
- w przypadku braków formalnych termin 40 dni roboczych ulega zawieszeniu,
- bank nie może rozpocząć świadczenia usług przed potwierdzeniem kompletności.

Notyfikacja ma charakter rozbudowany i obejmuje pełną dokumentację techniczną, organizacyjną, AML, ICT oraz operacyjną. W praktyce wymagania te mogą być porównywalne lub bardziej wymagające niż standardowe wnioski licencyjne w innych sektorach.

4. Charakter uprawnienia dla banków w kontekście jednolitego rynku krypto.

Uprawnienie banków do świadczenia usług krypto na podstawie art. 60 MiCA wpisuje się w szerszy cel MiCA – budowę jednolitego rynku usług krypto w UE. Instytucje kredytowe są traktowane jako podmioty o szczególnej wiarygodności i stabilności, co w założeniu na pozwolić:

- ograniczyć koszt regulacyjny wejścia na rynek,
- przyspieszyć budowę infrastruktury krypto w ramach sektora bankowego,
- zapewnić wysoki poziom bezpieczeństwa poprzez przeniesienie działalności krypto do instytucji o solidnych strukturach nadzorczych.

Jednocześnie MiCA zapewnia, że bank, mimo uproszczeń proceduralnych, nie może prowadzić działalności krypto w sposób mniej bezpieczny niż podmiot licencjonowany jako CASP. O ile więc w założeniu bank może wejść w rynek krypto łatwiej (notyfikacja), to musi działać równie bezpiecznie (pełne wymogi materialne MiCA) – bez żadnych taryf ulgowych.

2.4. Zakres notyfikacji

Artykuł 60 ust. 7 MiCA określa szczegółowy katalog informacji, jakie instytucja kredytowa musi przekazać właściwemu organowi nadzorczemu co najmniej 40 dni roboczych przed rozpoczęciem świadczenia usług w zakresie kryptoaktywów. Notyfikacja ta nie ma charakteru uproszczonego zgłoszenia – stanowi ona w praktyce rozbudowaną dokumentację operacyjną, technologiczną i organizacyjną, której celem jest umożliwienie organowi nadzoru oceny, czy bank jest zdolny do bezpiecznego, zgodnego i stabilnego

43 M. Rypina, M. Wierzbowski (red.), *Rozporządzenie w sprawie rynków kryptoaktywów. Komentarz* [w:] *Rozporządzenie w sprawie rynków kryptoaktywów (MiCA) i rozporządzenie pilotażowe DLT (DLT Pilot Regime). Komentarz*, wyd. 1, 2025, art. 60, nt 2.

świadczenia usług krypto. Wymogi te stanowią funkcjonalny odpowiednik materiałów analizowanych w procedurze autoryzacyjnej dla CASP[44].

Zakres notyfikacji obejmuje następujące elementy:

- program działania i opis usług,
- mechanizmy kontroli wewnętrznej oraz procedury AML/CFT,
- dokumentację techniczną i cyberbezpieczeństwo (ICT),
- procedury zapewniające wyodrębnienie aktywów klientów,
- politykę przechowywania i administrowania kryptoaktywami,
- jeżeli dotyczy – regulamin działania platformy obrotu,
- politykę realizacji zleceń i model ustalania cen,
- dowody kwalifikacji personelu,
- informację o kategorii kryptoaktywa,
- modelu świadczenia usług transferu kryptoaktywów.

Przede wszystkim bank musi przedstawić szczegółowy opis: kategorii usług krypto, które zamierza świadczyć; modelu świadczenia usług (własna infrastruktura, usługi podmiotów trzecich, outsourcing); grup docelowych klientów; przewidywanego wolumenu działalności i struktury przychodowej; geograficznego zakresu działania (Polska/UE/świadczenie transgraniczne).

Program działania musi odpowiadać strukturze i logice RTS 2025/303[45], co oznacza konieczność przedstawienia informacji w sposób ujednolicony na poziomie UE.

Ponadto bank przedstawia: polityki zgodności w zakresie krypto, procedury AML/CFT dostosowane do ryzyka kryptoaktywów, metody identyfikacji i monitorowania transakcji on-chain, opis ram oceny ryzyka działalności krypto, zasady eskalacji i przeciwdziałania nadużyciom. Organ nadzoru weryfikuje natomiast, czy bank wprowadza kontrole jakościowo równoważne tym, których wymaga się od CASP.

Do kolejnych obowiązków banku należy: przedstawienie opisu architektury systemowej i technologicznej, stosowanych rozwiązań kryptograficznych (klucze, HSM, *multi-signature*), mechanizmów zarządzania kluczami prywatnymi, systemów monitorowania integralności sieci blockchain, zasad backupu i odzyskiwania danych, planu ciągłości działania i odzyskiwania po awarii. Dokumentacja ICT musi być sporządzona zarówno w formie technicznej, jak i w tzw. wersji „niespecjalistycznej", przewidzianej w MiCA.

44 Art. 60. 7. Do celów ust. 1–6 przekazuje się powiadomienie zawierające następujące informacje:
a) program działania określający rodzaje usług w zakresie kryptoaktywów, które dostawca usług w zakresie kryptoaktywów ubiegający się o zezwolenie zamierza świadczyć, w tym miejsce i sposób świadczenia tych usług;
b) opis:
(i) mechanizmów kontroli wewnętrznej, polityk i procedur służących zapewnieniu zgodności z przepisami prawa krajowego transponującymi dyrektywę (UE) 2015/849;
(ii) ram oceny ryzyka na potrzeby zarządzania ryzykiem związanym z praniem pieniędzy i finansowaniem terroryzmu; oraz
(iii) planu ciągłości działania;
c) dokumentację techniczną systemów ICT i rozwiązań w zakresie bezpieczeństwa oraz ich opis w języku niespecjalistycznym;
d) opis procedury wyodrębnienia kryptoaktywów i środków pieniężnych klienta;
e) opis polityki w zakresie przechowywania i administrowania w przypadku zamiaru świadczenia usług w zakresie przechowywania kryptoaktywów i administrowania nimi w imieniu klientów;
f) opis przepisów operacyjnych platformy obrotu oraz procedur i systemu wykrywania nadużyć na rynku w przypadku zamiaru prowadzenia platformy obrotu kryptoaktywami;
g) opis niedyskryminacyjnej polityki handlowej regulującej stosunki z klientami oraz opis metody określania ceny kryptoaktywów, które dany podmiot oferuje do wymiany na środki pieniężne lub inne kryptoaktywa w przypadku zamiaru wymiany kryptoaktywów na środki pieniężne lub na inne kryptoaktywa;
h) opis polityki realizowania zleceń w przypadku zamiaru realizowania zleceń dotyczących kryptoaktywów w imieniu klientów;
i) dowody potwierdzające, że osoby fizyczne świadczące usługi doradztwa w imieniu dostawcy usług w zakresie kryptoaktywów ubiegającego się o zezwolenie lub zarządzające portfelami w imieniu dostawcy usług w zakresie kryptoaktywów ubiegającego się o zezwolenie posiadają wiedzę ogólną i fachową niezbędne do wywiązania się ze swoich obowiązków w przypadku zamiaru świadczenia usług doradztwa w zakresie kryptoaktywów lub zarządzania portfelem kryptoaktywów;
j) czy usługa w zakresie kryptoaktywów dotyczy tokenów powiązanych z aktywami, tokenów będących e-pieniądzem czy innych kryptoaktywów;
k) informacje na temat sposobu świadczenia usług transferu kryptoaktywów w imieniu klientów w przypadku zamiaru świadczenia takich usług transferu.

45 Rozporządzenie delegowane Komisji (UE) 2025/303 z dnia 31 października 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 w odniesieniu do regulacyjnych standardów technicznych określających informacje, które mają być przekazywane przez niektóre podmioty finansowe w powiadomieniu o zamiarze świadczenia usług w zakresie kryptoaktywów (Dz.Urz. UE L z 2025 r. poz. 303).

Bank zobowiązany jest do wykazania, że: aktywa klientów są zawsze oddzielone od aktywów własnych, bank stosuje wymagane polityki bezpieczeństwa depozytów krypto oraz posiada narzędzia do ochrony przed utratą kluczy lub nieautoryzowanymi transakcjami. Organ nadzoru analizuje w tym zakresie skuteczność segregacji zarówno na poziomie prawnym, jak i technologicznym.

Polityka przechowywania i administrowania kryptoaktywami dotyczy usług custody, w ramach których bank: opisuje techniczne i organizacyjne procedury przechowywania aktywów, przedstawia zasady wyboru infrastruktury blockchain, przedstawia zasady audytu, testów penetracyjnych i kontroli wewnętrznej, przedstawia strukturę odpowiedzialności w operacjach custody.

Niezależnie od powyższego, w przypadku, gdy bank zamierza prowadzić platformę obrotu kryptoaktywami, musi przedstawić: zasady dopuszczania aktywów do obrotu, zasady niedyskryminacyjnego dostępu, procedury zapobiegania nadużyciom rynkowym, systemy zapewniające integralność i płynność rynku. W tym zakresie regulacje te są zbliżone do wymogów dla MTF/OTF w MiFID II.

Jeżeli bank będzie wykonywał zlecenia w imieniu klientów lub prowadził działalność wymiany, musi przedstawić: kryteria realizacji zleceń, model określania cen kryptoaktywów, zasady przedstawiania klientom informacji o ryzyku cenowym i płynnościowym, a także opis struktury danych rynkowych wykorzystywanych do wyceny.

Do katalogu kolejnych nałożonych na bank obowiązków należy zaliczyć wymóg przedstawienia dowodów kompetencji pracowników świadczących usługi doradztwa w zakresie kryptoaktywów, a także zarządzających portfelami krypto oraz strukturę organizacyjną i plan odpowiedzialności. MiCA traktuje bowiem doradztwo i *asset management* w obszarze krypto analogicznie, jak doradztwo inwestycyjne dotyczące tradycyjnych instrumentów finansowych.

Dla oceny zgodności z innymi regulacjami: PSD2, EMD2, CRD/CRR istotne znaczenie ma informacja o kategorii kryptoaktywa. Bank musi bowiem określić, czy planowane usługi dotyczą: tokenów powiązanych z aktywami (ART), tokenów będących e-pieniądzem (EMT), innych kryptoaktywów.

Wreszcie w przypadku usług transferu (*transfer services*) notyfikacja musi zawierać: zasady identyfikacji i autentykacji nadawcy i odbiorcy, zasady bezpieczeństwa transakcji, interoperacyjność systemów blockchain i systemów bankowych oraz gwarancję zgodności z przepisami AML i *travel rule*.

Jak można zatem zauważyć, przewidziany w art. 60 MiCA obowiązek notyfikacji ma charakter znacznie szerszy niż zwykłe zgłoszenie administracyjne. W istocie stanowi on mechanizm pełniący funkcję zbliżoną do procedury licencyjnej, choć formalnie uproszczoną. Rozpoczęcie jakiejkolwiek działalności w zakresie kryptoaktywów przez bank jest dopuszczalne dopiero po złożeniu notyfikacji i potwierdzeniu jej kompletności przez właściwy organ nadzoru. Do czasu tego potwierdzenia świadczenie usług krypto jest niedopuszczalne, a w sytuacji stwierdzenia braków dokumentacyjnych, bieg terminu przewidziany w MiCA ulega zawieszeniu. Oznacza to, że notyfikacja staje się bezpośrednim warunkiem legalności działalności krypto prowadzonej przez instytucję kredytową.

Znaczenie notyfikacji wykracza poza aspekt formalny i spełnia funkcję kontroli *ex ante*, która w odniesieniu do banków zastępuje klasyczną procedurę udzielania zezwolenia CASP. Organ nadzoru, analizując dokumentację przekazaną wraz z notyfikacją, weryfikuje przygotowanie banku do świadczenia usług krypto pod względem technologii, bezpieczeństwa, przejrzystości, procedur AML/CFT, sposobu realizacji zleceń oraz ochrony aktywów klientów. W praktyce oznacza to, że kontrola prowadzona na etapie notyfikacji jest jakościowo zbliżona do oceny, jaką organ przeprowadza wobec podmiotów wnioskujących o licencję CASP. Uproszczenie proceduralne nie oznacza więc obniżenia standardów, lecz jedynie ominięcie jednego z etapów formalnych, przy zachowaniu pełnej merytorycznej oceny zdolności banku do prowadzenia działalności w sposób bezpieczny i zgodny z MiCA.

Notyfikacja odgrywa również istotną rolę w zapewnieniu jednolitych standardów bezpieczeństwa w całej Unii Europejskiej. Ustawodawca unijny zakłada, że banki, które tradycyjnie działają w silnie regulowanym środowisku, nie mogą uzyskać przewagi konkurencyjnej wynikającej z mniej rygorystycznych wymogów przy świadczeniu usług krypto. Dlatego dokumentacja składana w ramach notyfikacji musi w pełni odwzorowywać standardy stosowane wobec licencjonowanych CASP, co eliminuje ryzyko arbitrażu regulacyjnego i utrzymuje spójność reżimu MiCA w całej Unii Europejskiej.

Notyfikacja wzmacnia także narzędzia nadzorcze państwa członkowskiego. Dzięki niej organ nadzoru może żądać wyjaśnień, uzupełnień lub modyfikacji planowanego modelu działania banku w zakresie usług krypto. Choć formalnie w art. 60 MiCA nie przewidziano procedury zatwierdzenia w sensie decyzyjnym, to w praktyce bank nie może rozpocząć działalności do czasu akceptacji kompletności dokumentacji, a organ ma możliwość wpływania na zakres i strukturę usług poprzez ocenę prawidłowości wdrożonych polityk, procedur oraz infrastruktury ICT. Zapewnia to realny nadzór nad wejściem banków na rynek krypto bez konieczności wprowadzania dodatkowej procedury licencyjnej.

Obowiązek notyfikacji pełni również funkcję integracyjną, łącząc reżim MiCA z dotychczasowym nadzorem bankowym opartym na CRD/CRR, EMD2, PSD2 oraz innych regulacjach sektorowych. Dzięki temu organ nadzoru uzyskuje kompleksowy obraz działalności banku w kontekście całego profilu ryzyka, co jest konieczne ze względu na możliwość wzajemnego oddziaływania ryzyka krypto i ryzyk tradycyjnych. Notyfikacja zmusza również bank do wcześniejszego przeprowadzenia pełnej analizy ryzyka, dostosowania procedur AML/CFT, wdrożenia odpowiednich mechanizmów governance oraz zapewnienia właściwej struktury odpowiedzialności za działalność krypto.

Istotnym elementem notyfikacji jest także jej wymiar europejski. Po potwierdzeniu kompletności dokumentacji krajowy organ nadzoru przekazuje informacje do ESMA, która umieszcza bank w publicznym rejestrze podmiotów świadczących usługi krypto w UE. Z punktu widzenia jednolitego rynku finansowego, oznacza to formalne uznanie banku jako uczestnika rynku krypto na terenie Unii oraz umożliwia korzystanie z paszportowania usług w modelu transgranicznym.

W rezultacie notyfikacja stanowi narzędzie gwarantujące, że bank – mimo korzystania z uproszczonego trybu proceduralnego – wchodzi na rynek krypto wyłącznie po wykazaniu zgodności z pełnym zakresem wymogów materialnych MiCA. Jest to zatem mechanizm równoważący efektywność wejścia na rynek z koniecznością zapewnienia stabilności i bezpieczeństwa sektora finansowego.

2.5. Obowiązki materialne banków

Chociaż instytucje kredytowe wchodzące w sektor kryptoaktywów korzystają z uproszczonej procedury notyfikacyjnej przewidzianej w art. 60 MiCA, to jednak – o czym była już mowa powyżej – nie są zwolnione z żadnych wymogów materialnych, które nakładane są na licencjonowanych dostawców usług w zakresie kryptoaktywów (CASP). Ustawodawca unijny przyjmuje zasadę równoważności standardów: bank może wejść na rynek krypto szybciej i bez odrębnej procedury autoryzacyjnej, lecz musi świadczyć usługi w modelu zapewniającym poziom bezpieczeństwa, przejrzystości, stabilności i zgodności regulacyjnej identyczny z tym, którego wymaga się od CASP. W konsekwencji banki podlegają pełnemu katalogowi obowiązków dotyczących ochrony klientów, zarządzania ryzykiem, bezpieczeństwa technologicznego i przeciwdziałania nadużyciom.

Obowiązki te można podzielić na kilka głównych obszarów.

Ochrona aktywów klientów i polityki *custody*. Bank świadczący usługi przechowywania i administrowania kryptoaktywami musi zapewnić pełną segregację aktywów klientów od aktywów własnych oraz zagwarantować, że środki klientów nie będą wykorzystywane do celów innych niż wynikające z ich dyspozycji. MiCA wprowadza rygorystyczne zasady dotyczące bezpieczeństwa kluczy kryptograficznych, przechowywania aktywów w środowiskach o wysokiej odporności technologicznej oraz ochrony przed nieautoryzowanymi transakcjami. Wymogi te nakładają na bank obowiązek wdrożenia wyraźnie oddzielonych struktur operacyjnych i systemowych, nawet jeśli działalność krypto nie stanowi odrębnej jednostki organizacyjnej banku.

Przejrzystość, informowanie klientów i ochrona inwestorów. MiCA nakłada na bank szerokie obowiązki informacyjne, w tym konieczność przedstawienia klientom jasnych, zrozumiałych i niewprowadzających w błąd informacji dotyczących charakteru kryptoaktywów, ryzyk związanych z inwestowaniem, sposobu ustalania cen oraz potencjalnej zmienności rynkowej. Przejrzystość obejmuje również obowiązek ujawniania konfliktów interesów, zasad realizacji zleceń oraz ryzyk specyficznych dla aktywów cyfrowych, które różnią się od ryzyk właściwych instrumentom finansowym. Bank musi zapewnić klientom poziom ochrony przewidziany w MiCA, niezależnie od tego, czy usługi krypto są świadczone na rzecz klientów detalicznych, profesjonalnych czy instytucjonalnych.

Wymogi AML/CFT dostosowane do specyfiki kryptoaktywów. Usługi kryptoaktywów generują

ryzyka związane z praniem pieniędzy i finansowaniem terroryzmu, które różnią się od ryzyk charakterystycznych dla tradycyjnych usług bankowych. W związku z tym MiCA wymaga, aby bank rozszerzył swoje procedury AML/CFT o mechanizmy umożliwiające monitorowanie transakcji on-chain, ocenę ryzyka adresów i kontraktów inteligentnych oraz stosowanie narzędzi analizy blockchain. Procedury AML muszą obejmować identyfikację beneficjentów rzeczywistych transakcji krypto, ocenę źródła pochodzenia aktywów oraz monitorowanie podejrzanych schematów transferów w czasie rzeczywistym. MiCA wymaga również zgodności z zasadą *travel rule*, zgodnie z którą informacje towarzyszące transferom krypto muszą być przekazywane pomiędzy instytucjami zaangażowanymi w transakcję.

Governance, zarządzanie ryzykiem i kompetencje personelu. Bank musi wykazać, że posiada adekwatną strukturę zarządczą, umożliwiającą bezpieczne świadczenie usług krypto. Oznacza to konieczność wyznaczenia kierownictwa odpowiedzialnego za działalność krypto, zapewnienia niezależności funkcji kontroli (*compliance*, zarządzanie ryzykiem, audyt wewnętrzny) oraz wdrożenia procedur eskalacji ryzyka. Osoby odpowiedzialne za doradztwo w zakresie kryptoaktywów lub zarządzanie portfelami krypto muszą posiadać kwalifikacje potwierdzające ich kompetencje, a bank ma obowiązek udokumentować te kompetencje w procesie notyfikacyjnym. ESMA podkreśla, że ryzyko związane z aktywami cyfrowymi wymaga od instytucji finansowych stosowania niezależnych modeli oceny ryzyka, które uwzględniają specyficzne zagrożenia dla aktywów opartych na technologii blockchain.

Bezpieczeństwo technologiczne, cyberbezpieczeństwo i odporność operacyjna. MiCA, w powiązaniu z rozporządzeniem DORA, nakłada na bank obowiązek wdrożenia infrastruktury technologicznej zapewniającej wysoki poziom odporności operacyjnej. Bank musi wykazać, że systemy ICT służące do świadczenia usług krypto spełniają rygorystyczne wymogi dotyczące bezpieczeństwa kryptograficznego, kontroli dostępu, przechowywania kluczy prywatnych, monitorowania transakcji oraz zarządzania incydentami. Wymagane jest również wdrożenie planów ciągłości działania i procedur odzyskiwania danych, w tym rozwiązań na wypadek utraty kluczy kryptograficznych. Organ nadzoru analizuje adekwatność stosowanych technologii w kontekście poziomu ryzyka właściwego dla planowanej działalności.

Zapobieganie nadużyciom rynkowym i zapewnienie integralności obrotu. W przypadku świadczenia usług związanych z obrotem kryptoaktywami bank jest zobowiązany do stosowania procedur wykrywania i przeciwdziałania nadużyciom rynkowym, takich jak manipulacja cenami, *insider trading* czy *wash trading*. MiCA wymaga, aby bank implementował systemy monitorowania rynku zbliżone do tych stosowanych na rynkach regulowanych lub platformach MTF/OTF. Bank musi także zapewnić niedyskryminacyjny dostęp klientów do oferowanych usług oraz stosować procedury dotyczące dopuszczania aktywów do obrotu na platformie krypto prowadzonej przez instytucję.

Konsekwencja regulacyjna: brak taryf ulgowych mimo uproszczonego wejścia na rynek. Obowiązki materialne nakładane na bank w praktyce zrównują jego pozycję regulacyjną z licencjonowanym CASP. Mimo że art. 60 MiCA pozwala bankowi na pominięcie procedury licencyjnej, rozporządzenie nie przewiduje żadnych obniżonych standardów dotyczących bezpieczeństwa technologicznego, governance, zarządzania ryzykiem, AML/CFT czy przejrzystości. Oznacza to, że bank, aby wejść na rynek krypto, musi spełnić wszystkie wymogi, które w innym przypadku byłyby badane w ramach procesu licencyjnego CASP.

2.6. Relacja art. 60 MiCA do CRD/CRR, MiFID II, PSD2 i prawa krajowego

Artykuł 60 MiCA funkcjonuje w ścisłej relacji z istniejącym systemem regulacyjnym instytucji finansowych. Przepis ten nie wprowadza pełnej autonomii regulacyjnej w zakresie działalności kryptoaktywów, lecz buduje konstrukt, w którym wejście banków i innych instytucji finansowych w sektor krypto następuje w sposób komplementarny wobec obowiązujących reżimów licencyjnych i nadzorczych. W praktyce art. 60 MiCA integruje wymogi właściwe dla rynku krypto z zestawem regulacji tradycyjnego systemu finansowego, co ma na celu ograniczenie ryzyka systemowego i zapobieganie powstawaniu luk regulacyjnych.

Relacja między MiCA a CRD/CRR ma przede wszystkim znaczenie w zakresie zezwoleń i funduszy własnych. MiCA jednoznacznie wskazuje, że instytucje kredytowe, które uzyskały zezwolenie na prowadzenie działalności bankowej zgodnie z CRD IV, nie muszą poddawać się procedurze licencyjnej CASP. Wynika to z założenia, że ocena nadzorcza, jakiej podlegają banki w ramach CRD/CRR, obejmuje klu-

czowe aspekty stabilności finansowej, kwalifikacji zarządu, ładu korporacyjnego i adekwatności kapitałowej. MiCA nie powiela tych wymogów, lecz nakazuje organom nadzoru uwzględniać je przy ocenie zdolności banku do świadczenia usług krypto na podstawie wspomnianego art. 60. Jednocześnie w motywie 78 MiCA podkreślono, że notyfikacja usług krypto przez bank powinna odbywać się z poszanowaniem procedur wynikających z regulacji CRD, w tym przepisów dotyczących zmiany zakresu czynności bankowych wymagających zmiany statutu i zgody organu nadzoru krajowego.

MiCA pozostaje także ściśle powiązana z MiFID II w odniesieniu do firm inwestycyjnych. Artykuł 60 MiCA identyfikuje, które usługi krypto mają charakter równoważny wobec usług inwestycyjnych regulowanych w MiFID II, co pozwala firmom inwestycyjnym rozszerzać działalność o kryptoaktywa bez konieczności uzyskiwania licencji CASP, o ile dana czynność odpowiada zakresowi usług, na które posiadają dotychczasowe zezwolenie. Relacja ta opiera się na zasadzie funkcjonalnej analogii: prowadzenie platformy obrotu krypto jest traktowane jako odpowiednik MTF/OTF, przechowywanie krypto jako odpowiednik usług powierniczych, a doradztwo krypto jako odpowiednik doradztwa inwestycyjnego. MiCA zdejmuje z firm inwestycyjnych obowiązek licencyjny, lecz wymaga pełnej zgodności z wymogami materialnymi CASP, co powoduje, że reżimy MiFID II i MiCA funkcjonują w modelu nakładających się obowiązków, a nie wzajemnych wyłączeń.

W odniesieniu do PSD2 i EMD2 relacja art. 60 MiCA ma szczególne znaczenie dla instytucji pieniądza elektronicznego oraz dla usług transferu kryptoaktywów. Instytucje te mogą świadczyć usługi dotyczące tokenów będących e-pieniądzem (EMT) wyłącznie wówczas, gdy spełniają równocześnie wymogi MiCA oraz wymogi dotyczące emisji pieniądza elektronicznego. Oznacza to, że choć MiCA klasyfikuje EMT jako szczególną kategorię kryptoaktywa, to jednak nie usuwa regulacji sektorowych wynikających z EMD2, a wprost przeciwnie – nakłada wymóg kumulatywnego stosowania regulacji. W przypadku usług transferu MiCA przewiduje obowiązki dostosowane do zasady *travel rule*, które zbliżają się do obowiązków charakterystycznych dla dostawców usług płatniczych podlegających PSD2. Dla banków oznacza to konieczność operacyjnego połączenia procedur właściwych dla przelewów tradycyjnych i transakcji blockchain.

Istotna jest również relacja z prawem krajowym. W polskim porządku prawnym wejście banków w sektor krypto wymaga dostosowania przepisów ustawy Pr. bank. poprzez dodanie nowych względnych czynności bankowych, obejmujących emisję określonych kategorii tokenów oraz świadczenie usług w zakresie kryptoaktywów. Zmiana taka wymaga zgody KNF na zmianę statutu banku. Oznacza to, że mimo unijnej podstawy prawnej działalności krypto, procedura notyfikacji MiCA musi być uzupełniona o wymogi krajowe dotyczące zakresu czynności bankowych i ich zgodności z krajowym nadzorem. Relacja art. 60 MiCA do prawa krajowego polega więc na tym, że MiCA wyznacza ramy minimalne, lecz nie zwalnia instytucji kredytowych z przestrzegania wymogów właściwych dla rynku krajowego, w tym wymogów dotyczących organizacji banku, zakresu działalności statutowej, odpowiedzialności zarządu oraz krajowych zasad dotyczących outsourcingu, bezpieczeństwa ICT czy raportowania.

W rezultacie art. 60 MiCA funkcjonuje jako przepis o charakterze intersektorowym. Integruje on zasady właściwe dla rynku krypto z dotychczasowymi reżimami nadzorczymi, nie znosząc ich, lecz tworząc spójną konstrukcję, w której bank wchodzący w sektor krypto podlega jednocześnie: wymogom MiCA, wymogom prudencyjnym CRR/CRD, wymogom organizacyjnym i informacyjnym MiFID II (w zakresie usług analogicznych), regulacjom PSD2 i EMD2 (w zakresie EMT i usług transferu), a także krajowym przepisom definiującym zakres dozwolonej działalności bankowej. Model ten zapobiega powstawaniu luk regulacyjnych, a jednocześnie gwarantuje, że działalność banków w sektorze krypto będzie prowadzona z zachowaniem standardów charakterystycznych dla podmiotów o znaczeniu systemowym.

2.7. Praktyka nadzorcza i standardy interpretacyjne (ESMA/EBA/ECB/KNF) oraz implikacje dla banków

W ostatnich latach ukształtował się dość spójny kanon interpretacyjny, dotyczący stosowania art. 60 MiCA wobec banków. Największy ciężar wytycznych spoczywa na ESMA, która – obok przepisów wykonawczych Komisji – dostarczyła nadzorcom i uczestnikom rynku praktyczny „podręcznik" autoryzacyjno-notyfikacyjny. Kluczowym dokumentem jest Supervisory Briefing on the Authorisation of CASPs under MiCA (31.01.2025). ESMA wskazuje w nim m.in. na oczekiwany „*risk-based approach*" do oceny wniosków/notyfikacji, wymóg realnej substancji w UE (governance, zasoby, decyzyjność), a także na konieczność zrównania jakości kontroli banków

z jakością kontroli nad licencjonowanymi CASP. W praktyce briefing przesądza, że ułatwienie proceduralne z art. 60 nie może skutkować obniżeniem standardów bezpieczeństwa, ciągłości działania czy ochrony klienta. Tym samym działalność krypto prowadzona przez bank ma być co najmniej tak bezpieczna, jak działalność podmiotów posiadających licencję CASP[46].

Na poziomie „twardego" prawa wtórnego, mechanika notyfikacji została doprecyzowana przez rozporządzenie delegowane (UE) 2025/303 (RTS) oraz rozporządzenie wykonawcze (UE) 2025/304 (ITS). Pierwsze z powołanych precyzuje zakres informacji, jakie bank musi złożyć (program działania, mechanizmy AML/CFT, architektura ICT, zasady segregacji aktywów itd.), drugie ustanawia zaś ujednolicone formularze i procedury. Te akty kończą spór, czy notyfikacja banku to „proste zgłoszenie" – z ich treści wynika, że jest to de *facto* pełna dokumentacja operacyjno-techniczna, umożliwiająca nadzorcy kontrolę *ex ante*, zanim bank uruchomi usługę krypto[47].

Dalszą warstwę wykładni dostarczają Q&A ESMA. Odpowiedzi nr 2143 zakazują konstruowania przez CASP (a zatem i przez bank działający jak CASP) sieci „agentów" na wzór agentów z MiFID II, chyba że dany podmiot działający „dla" CASP sam posiada status CASP. To istotne przy planowaniu dystrybucji usług krypto w grupie kapitałowej banku czy przy modelach „white-label". Z kolei 2125 przypomina firmom inwestycyjnym (i w praktyce również bankom prowadzącym działalność maklerską), że usługi wykraczające poza katalog równoważności z art. 60 wymagają licencji CASP na zasadach ogólnych. Wreszcie Q&A nr 2342 precyzuje status podmiotowy dostawców (np. wykluczając osoby fizyczne/powierników jako CASP). Te odpowiedzi wzmacniają tezę o braku „taryf ulgowych" dla banków w warstwie materialnej świadczenia usług[48].

Z perspektywy ostrożnościowej i płynnościowej na działalność banków w krypto wpływa standard Bazylejski dotyczący ekspozycji na kryptoaktywa (SCO60), finalizowany w grudniu 2022 r. i przeznaczony do wdrożenia od 1 stycznia 2025 r., a także towarzyszące mu szablony ujawnień (decyzja o publikacji ekspozycji od 2026 r.). W praktyce oznacza to, że banki, planując modele custody/market-making/tokenizacji, muszą łączyć reżim MiCA z wymogami kapitałowymi i ujawnieniowymi Bazylei. Wprost podkreślono też, że „tokenised deposits" rozpatrywane są w reżimie bankowym, przy braku planów dodatkowych reguł kapitałowych na dziś – co jednak nie zwalnia z rygorystycznego zarządzania ryzykiem operacyjnym i stron trzecich (np. cloud)[49].

Po stronie EBA widać dwa ważne wątki. Po pierwsze, EBA od lat zwraca uwagę, że brak obowiązku informacyjnego wobec nadzorców dla banków w krypto osłabiałby konwergencję nadzorczą (co historycznie uzasadniało odejście od wersji „automatic status" w pierwotnym projekcie MiCA). Po drugie, świeże Opinie EBA z 10.10.2025 r. w sprawie zmian KE do projektów RTS o rezerwach aktywów (dla ART/EMT) pokazują, że nadzór bankowy jest gotów blokować rozwiązania osłabiające ramy ostrożnościowe MiCA. Uzupełniająco, Opinia EBA (10.06.2025 r.) o interakcji PSD2–MiCA systematyzuje granice między usługami płatniczymi a transferem krypto w rozumieniu MiCA — kluczowe przy projektowaniu przepływów „on/off-ramp" w bankach[50].

W tle pozostaje także ECB (opinie do projektu MiCA), który akcentował, że brak obowiązków informacyjnych dla banków utrudniałby monitorowanie ryzyk — rekomendując podejście bardziej zbliżone do obecnej notyfikacji warunkowej (40 dni + zakres z ust. 7). To wsparło finalny kształt art. 60[51].

Wreszcie, w warstwie krajowej warto odnotować stanowiska UKNF dotyczące kryptoaktywów (2020 r.)., które wyznaczały linie ocenne co do charakteru prawnego tokenów, ryzyk AML/CFT i oczekiwanych standardów informacyjnych. W zestawieniu z pla-

46 ESMA, *Supervisory Briefing Authorisation of CASPs under MiCA*, ESMA75-453128700-1263, 31.01.2025.

47 Komisja Europejska, *Rozporządzenie delegowane (UE) 2025/303 z 31.10.2024 r. (RTS w sprawie informacji do notyfikacji)*; Komisja Europejska, *Rozporządzenie wykonawcze (UE) 2025/304 z 31.10.2024 r. (ITS — formularze/wzory/procedury notyfikacji)*.

48 ESMA Q&A – MiCA: ID 2143 (agenci), ID 2125 (zakres równoważności i konieczność licencji CASP na „dodatkowe" usługi) https://www.esma.europa.eu/publications-data/questions-answers/

49 Basel Committee on Banking Supervision, *Prudential treatment of cryptoasset exposures* (SCO60), 16.12.2022; oraz materiały dot. ujawnień od 2026 r.

50 *Opinion of the European Banking Authority on the interplay between Directive EU 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens, https://www.eba.europa.eu/, 10.06.2025; The EBA responds to Commission's proposed changes to the technical standards on liquidity requirements of the reserve of assets under MiCA*, https://www.eba.europa.eu/ (dostęp: 10 października 2025 r.).

51 Opinion of the European Central Bank of 30 November 2021 on a proposal for a regulation to extend traceability requirements to transfers of crypto-assets (CON/2021/37)

nowaną krajową implementacją (zmiany w Pr. bank. – rozszerzenie czynności bankowych) tworzy to logiczny „pomost" między unijną notyfikacją a krajowym zatwierdzaniem zmian statutowych[52].

W konkluzji stwierdzić można, co następuje:

- notyfikacja z art. 60 jest procedurą materialnie równoważną weryfikacji licencyjnej CASP – różni ją tylko brak nowej decyzji „zezwalającej", nie zaś luźniejsze standardy;
- ocena KNF prawdopodobnie będzie prowadzona w duchu dokumentów ESMA/RTS/ITS, z silnym naciskiem na substancję operacyjną, DORA/ICT i segregację aktywów;
- wymogi bazylejskie i oczekiwania EBA/ECB zmuszają banki do integralnego ujęcia ryzyk krypto w ICAAP/ILAAP, testach odporności i ujawnieniach – a więc do potraktowania działalności krypto jako pełnoprawnego komponentu profilu ryzyka banku, nie zaś „pilotażu technologicznego".

2.8. Wymogi materialne dla banków świadczących usługi w zakresie kryptoaktywów

2.8.1. Wymogi organizacyjne i governance (art. 61–63 MiCA)

W art. 61–63 MiCA ustanowiono ogólne wymogi organizacyjne dla podmiotów świadczących usługi w zakresie kryptoaktywów, które obowiązują również instytucje kredytowe działające na podstawie art. 60. MiCA posługuje się podejściem funkcjonalnym: bank, mimo że nie potrzebuje odrębnej licencji CASP, musi spełniać wszystkie wymogi materialne dotyczące governance, kontroli wewnętrznej i operacyjnej, tak jak podmiot licencjonowany.

MiCA wymaga w szczególności, aby instytucje świadczące usługi krypto:

- posiadały skuteczny system zarządzania obejmujący strategię, procesy i mechanizmy kontroli ryzyka;
- wdrożyły struktury zapewniające niezależność funkcji kontroli (compliance, risk management, audyt);
- zapewniły rozdzielenie funkcji kluczowych oraz odpowiednią ciągłość działania.

Standardy te są tożsame z wymogami znanymi z CRD IV, EBA Guidelines on Internal Governance[53] oraz EBA Guidelines on ICT and Security Risk Management[54]). Oznacza to, że bank wchodzący w działalność krypto musi jedynie rozszerzyć istniejące ramy governance na nowe obszary ryzyka, zamiast budować je od początku.

W odniesieniu do banków szczególne znaczenie ma obowiązek wykazania realnej substancji operacyjnej w UE. ESMA wskazuje[55], że:

- co najmniej jeden członek zarządu powinien mieć miejsce zamieszkania w państwie, w którym dokonywana jest notyfikacja (z wyjątkami dla małych państw);
- zarząd musi realnie nadzorować działalność krypto, a nie delegować ją w całości do podmiotów trzecich;
- organ nadzoru nie powinien akceptować modelu „letterbox entity" ani nadmiernej zależności od outsourcingu lub partnerów technologicznych.

2.8.2. Wymogi dotyczące segregacji aktywów i ochrony klienta (art. 67–69 MiCA)

MiCA nakłada na banki obowiązek ochrony aktywów klientów w sposób równoważny ochronie zapewnianej przez licencjonowanych CASP.

Przede wszystkim zwrócić należy tutaj uwagę na konieczność segregacji aktywów klientów. Artykuł 67 MiCA wymaga bowiem oddzielenia kryptoaktywów klientów od aktywów własnych banku, prowadzenia precyzyjnych zapisów i rejestrów, a także wprowadzenia mechanizmów ochronnych w przypadku niewypłacalności i restrukturyzacji.

52 UKNF, *Stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami*, 16.07.2020 r.

53 EBA/GL/2021/05.

54 EBA/GL/2019/04.

55 Supervisory Briefing on Authorisation of CASPs under MiCA (31.01.2025 r.).

Przepisy te są zbliżone do zasad segregacji instytucji inwestycyjnych wynikających z MiFID II, a także do polityk ochrony środków klientów w dyrektywie BRRD i częściowo do regulacji art. 73 CRR (ryzyko operacyjne).

Ponadto MiCA nie narzuca jednego modelu przechowywania kryptoaktywów, ale bank musi wykazać w notyfikacji:

- sposób przechowywania kluczy kryptograficznych, w tym politykę generowania, rotacji i przechowywania;
- zastosowanie wieloskładnikowych systemów podpisu (np. MPC, multisig);
- plan odzyskiwania dostępu (key recovery);
- środki redundancji i kontroli wewnętrznej,
- procedury zapobiegania konfliktom interesów w przypadku modeli omnibus.

MiCA dopuszcza zarówno custody wewnętrzne (self-hosted), jak i zewnętrzne, o ile nie narusza to art. 62–63 MiCA.

2.8.3. Wymogi ICT i cyberbezpieczeństwa dla banków świadczących usługi w zakresie kryptoaktywów (art. 60 ust. 7 lit. c, art. 62–63 MiCA + DORA)

MiCA wprowadza istotny zestaw wymogów technologicznych wobec podmiotów świadczących usługi w zakresie kryptoaktywów, obejmujący zarówno infrastrukturę ICT, jak i systemy bezpieczeństwa, procesy operacyjne oraz procedury reagowania na incydenty. Choć MiCA nie tworzy pełnego i autonomicznego reżimu cyberbezpieczeństwa, to w przypadku banków podstawowym źródłem obowiązków jest art. 60 ust. 7 lit. c, który wymaga przedłożenia „dokumentacji technicznej systemów ICT i rozwiązań w zakresie bezpieczeństwa", oraz przepisy art. 62–63 dotyczące governance i kontroli operacyjnej. Całość musi być interpretowana łącznie z rozporządzeniem DORA (Regulation (EU) 2022/2554), które ma pełne zastosowanie do instytucji kredytowych i w praktyce stanowi główną podstawę nadzoru ICT nad działalnością krypto w bankach.

Artykuł 60 ust. 7 lit. c MiCA nakłada obowiązek przedłożenia szczegółowego opisu infrastruktury technologicznej, obejmującej zarówno systemy własne banku, jak i elementy dostarczane przez strony trzecie (np. dostawców rozwiązań custody, technologii multisig/MPC, dostawców API do wymiany kryptoaktywów, weryfikatorów adresów blockchain czy dostawców analiz on-chain). Dokumentacja ta musi obejmować:

- strukturę architektury IT, obejmującą środowiska produkcyjne, testowe, chmurowe oraz integracje z blockchainami publicznymi i prywatnymi;
- szczegółowy opis wykorzystywanych modułów kryptograficznych, w tym metod generowania i przechowywania kluczy prywatnych;
- procesy autoryzacji dostępu i logowania zdarzeń;
- systemy wykrywania incydentów oraz narzędzia monitorujące ruch on-chain;
- procedury Disaster Recovery i Business Continuity (BCP/DRP).

Wymogi te zostały rozwinięte w Delegowanym Rozporządzeniu Komisji (UE) 2025/303 (RTS), które wprowadza standardowe formularze i wymogi dotyczące dokumentacji ICT dołączanej do notyfikacji.

Podczas gdy MiCA określa wymagania informacyjne i podstawowe standardy bezpieczeństwa, to DORA określa pełny reżim zarządzania ryzykiem ICT, obowiązkowy dla banków również w odniesieniu do działalności krypto. Obejmuje to m.in.:

- systematyczne zarządzanie ryzykami ICT (art. 5–15 DORA), w tym model ryzyk specyficznych dla blockchain, smart contracts i technologii zdecentralizowanych;
- obowiązki w zakresie zgłaszania poważnych incydentów ICT organom nadzoru (art. 17–20 DORA);
- obowiązki w zakresie testów odporności cyfrowej, w tym procedury TLPT – Threat-Led Penetration Testing (art. 21–27 DORA);
- obowiązki dotyczące nadzoru nad outsourcingiem ICT i dostawcami usług technologicznych (art. 28–40 DORA).

MiCA i DORA wspólnie ustanawiają standard, w którym bank musi udowodnić zdolność do obsługi kryptoakty-

wów z wykorzystaniem rozwiązań o wysokim poziomie odporności technologicznej, porównywalnym z infrastrukturą płatniczą i systemami rozrachunku.

Ponadto MiCA nakłada obowiązek wykazania kontroli nad ryzykiem operacyjnym i technologicznym, wynikającym z działań w środowisku blockchain. W praktyce oznacza to konieczność uwzględnienia:

- ryzyk związanych z **publicznymi blockchainami** (reorgs, finalność probabilistyczna, ataki 51%);
- ryzyk **MEV (Maximal Extractable Value)** oraz front-runningu, szczególnie istotnych dla banków prowadzących platformy obrotu lub usługi wymiany;
- ryzyk związanych z inteligentnymi kontraktami, w tym błędów kodu, exploitów oraz konieczności zapewnienia audytu smart contracts;
- ryzyk związanych z mostami międzyłańcuchowymi (bridge exploits), będących jednym z najczęściej wykorzystywanych wektorów ataku;
- ryzyk kryptograficznych związanych z przechowywaniem kluczy prywatnych oraz kompromitacją metod podpisu wieloskładnikowego (MPC).

W ocenie zgodności MiCA kładzie nacisk na wykazanie, że bank posiada program monitorowania transakcji on-chain oraz zdolność wykrywania anomalii w czasie rzeczywistym.

Artykuł 63 MiCA oraz art. 28–40 DORA wyraźnie ograniczają możliwość przeniesienia odpowiedzialności na dostawców zewnętrznych. Bank może wykorzystywać podmioty trzecie (np. dostawcę infrastruktury MPC), ale:

- nadal pozostaje w pełni odpowiedzialny za wykonanie usługi zgodnie z MiCA;
- musi posiadać realną zdolność nadzorczą nad dostawcą;
- musi zagwarantować, że outsourcing nie prowadzi do powstania „podmiotu skrzynkowego" (letterbox entity), co jest zakazane według ESMA Supervisory Briefing (2025);
- musi zapewnić, że umowa outsourcingu obejmuje zapisy dotyczące audytu, dostępności danych, szyfrowania oraz wymogów DORA.

MiCA nakłada obowiązek posiadania planu reagowania na incydenty, a DORA szczegółowo określa wymogi raportowania. Banki muszą:

- posiadać 24/7 monitoring infrastruktury on-chain i off-chain;
- klasyfikować incydenty zgodnie z kategoriami DORA;
- raportować incydenty ICT odpowiednim organom w terminach określonych w DORA;
- prowadzić okresowe testy skuteczności planów BCP/DRP.

W kontekście kryptoaktywów dodatkowo wymagane jest opracowanie scenariuszy awaryjnych dla sytuacji, w których dochodzi do utraty klucza prywatnego, degradacji sieci blockchain lub awarii mostów komunikacyjnych łączących sieci zdecentralizowane.

Artykuł 64 MiCA nakłada na banki wymogi dotyczące systemów informatycznych oraz zarządzania bezpieczeństwem ICT. Przepisy te są komplementarne względem rozporządzenia DORA (Regulation (EU) 2022/2554), które ma zastosowanie pełne – DORA obejmuje banki bez wyjątków.

Na banku spoczywa obowiązek przedstawienia: dokumentacji architektury ICT (hardware, software, integracje API, infrastruktura chmurowa, smart contracts); analizy ryzyk technologicznych; opisu procesów monitorowania on-chain; polityki dostępu i autoryzacji; scenariuszy awaryjnych. Wymogi te zostały szczegółowo rozwinięte w Delegowanym Rozporządzeniu Komisji (UE) 2025/303 (RTS, sekcja 2).

2.8.4. Obowiązek uczciwego, rzetelnego i profesjonalnego działania zgodnie z interesem klienta (art. 66 MiCA)

Artykuł 66 MiCA ustanawia podstawową zasadę ochrony klientów w relacji z dostawcami usług w zakresie kryptoaktywów. Przepis ten ma zastosowanie również do instytucji kredytowych, które rozpoczynają działalność krypto na podstawie art. 60, ponieważ zgodnie z ust. 10 tego przepisu banki są zobowiązane do przestrzegania wszystkich wymogów materialnych MiCA (poza procedurą licencyjną). W efekcie reżim ochrony klienta jest dla banków identyczny jak dla pełnoprawnych CASP.

Po pierwsze, na mocy art. 66 ust. 1 bank świadczący usługi krypto musi działać: uczciwie, rzetelnie, profesjonalnie, zgodnie z najlepiej pojętym interesem klienta.

Zasada ta odwołuje się do standardu znanego z MiFID II oraz CRD/CRR i pełni funkcję normy generalnej, na podstawie której organy nadzoru oceniają zachowania rynkowe. W praktyce oznacza to, że bank musi unikać jakichkolwiek modeli działania, które mogłyby narażać klienta na nieuzasadnione ryzyko, asymetrię informacji lub niezrozumienie oferowanej usługi.

Ponadto bank musi zapewnić, że każdy rodzaj komunikacji jest: uczciwy, jasny, rzetelny, niewprowadzający w błąd, odpowiednio oznaczony jako materiał marketingowy. Zakazane są zatem wszelkie praktyki, które mogłyby sugerować domniemane korzyści lub bezpieczeństwo kryptoaktywów bez uwzględnienia ryzyk. W szczególności bank nie może: sugerować gwarantowanej wartości, pomijać istotnych ryzyk technologicznych, ukrywać opłat lub mechanizmów ustalania cen, eksponować wyłącznie zalet produktu. Dla banków ma to szczególne znaczenie, ponieważ klienci często utożsamiają markę bankową z bezpieczeństwem i stabilnością, co może wywołać mylne oczekiwania dotyczące usług krypto.

Zgodnie z art. 66 ust. 3 MiCA banki muszą przekazywać klientom przejrzyste ostrzeżenia dotyczące ryzyk związanych z transakcjami na kryptoaktywach, obejmujące: zmienność cen, ryzyko utraty całości środków, ryzyko technologiczne, w tym utratę klucza lub błędne transfery, ryzyka właściwe blockchainom (atak 51%, reorganizacje bloków), – podatność smart contracts na błędy lub exploity.

Dodatkowo banki świadczące usługi prowadzenia platformy obrotu, wymiany kryptoaktywów, doradztwa kryptowalutowego, zarządzania portfelem krypto, muszą udostępniać klientom hiperłącza do dokumentów informacyjnych dotyczących danego kryptoaktywa (white papers lub inne dokumenty informacyjne zależne od typu tokena).

Na podstawie art. 66 ust. 4 MiCA bank zobowiązany jest do: podawania do publicznej wiadomości polityki cenowej, publikowania kosztów i opłat w widocznym miejscu na stronie internetowej, przedstawienia metod ustalania spreadów i opłat transakcyjnych. Wymóg ten wspiera zasadę przejrzystości kosztów i minimalizuje asymetrię informacji między bankiem a klientem.

W art. 66 ust. 5–6 MiCA wprowadza dodatkowy, nowatorski obowiązek informacyjny. Mianowicie bank, który świadczy usługi związane z danym kryptoaktywem, musi:

- publikować informacje o negatywnych skutkach środowiskowych mechanizmu konsensusu używanego przez to kryptoaktywo,
- przedstawiać je w widocznym miejscu na stronie internetowej,
- korzystać z danych zawartych w dokumentach informacyjnych emitenta, o ile są dostępne.

Informacje te dotyczą w szczególności: zużycia energii, udziału energii odnawialnej, emisji gazów cieplarnianych, produkcji odpadów elektronicznych.

Z perspektywy banków art. 66 MiCA tworzy zestaw obowiązków, które łączą elementy: standardów MiFID II (uczciwa komunikacja, ochrona klienta), standardów z PSD2 i CRD IV (rzetelność i profesjonalizm), zasad przejrzystości właściwych dla rynków krypto (dokumenty informacyjne, white papers).

2.8.5. Wymogi AML/CFT i *Travel Rule*

Działalność banków w zakresie kryptoaktywów podlega pełnemu reżimowi przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT), wynikającemu zarówno z MiCA, jak i równoległych regulacji sektorowych. MiCA nie tworzy samodzielnego reżimu AML, lecz w art. 60 ust. 7 lit. b nakłada na banki obowiązek wykazania, że posiadają mechanizmy kontroli wewnętrznej, polityki AML/CFT i ramy oceny ryzyka, które obejmują również usługi oparte na kryptoaktywach. Oznacza to konieczność rozszerzenia istniejących procedur AML banku na specyfikę technologii blockchain oraz transakcji on-chain.

W odniesieniu do banków kluczowe jest, że regulacje AML obowiązują je w całości niezależnie od MiCA. Jednak działalność kryptoaktywowa pociąga za sobą nowe ryzyka, które muszą zostać uwzględnione w:

- procedurach identyfikacji i weryfikacji klientów (KYC),
- ocenie ryzyka klienta i transakcji,
- monitorowaniu transakcji i przepływów on-chain,

- analizie adresów kryptowalutowych i ich ryzyka,
- procedurach sankcyjnych i kontroli kontrahentów,
- raportowaniu transakcji podejrzanych do GIIF (w Polsce),
- szkoleniach pracowników mających styczność z usługami krypto.

Bank musi dostosować swoje procedury AML do narzędzi i praktyk właściwych dla blockchain, w tym analizy adresów, oceny ryzyka protokołów i identyfikacji transakcji wysokiego ryzyka.

Z dniem 30 grudnia 2024 r. weszło w życie rozporządzenie w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849 (rozporządzenie TFR), które nakłada obowiązki dotyczące gromadzenia i przekazywania informacji o inicjatorach i beneficjentach transferów kryptoaktywów. Akt ten rozszerza tzw. *Travel Rule* na transfery kryptoaktywów. Zgodnie z nim bank wykonujący usługę transferu kryptoaktywów musi przekazywać instytucji odbierającej:

- dane nadawcy,
- dane beneficjenta,
- numer konta lub adres portfela,
- dodatkowe informacje wymagane dla transakcji wysokiego ryzyka.

Co istotne, obowiązek ten dotyczy wszystkich transakcji, niezależnie od kwoty, nie istnieje próg minimalny (np. 100 EUR), a dane muszą zostać przekazane przed lub równocześnie z transakcją.

W konsekwencji bank musi wdrożyć system zdolny do automatycznego pobierania danych nadawcy i odbiorcy, odrzucenia transferu przy braku wymaganych informacji, współpracy z systemami międzynarodowymi stosującymi *Travel Rule* oraz mapowania adresów blockchain na konta klientów lub wallet ID.

Standardy AML dla usług krypto wymagają stosowania specjalistycznych narzędzi, takich jak:

- systemy wykrywania złośliwych adresów,
- analiza ryzyka adresów (risk scoring),
- wykrywanie schematów mieszania środków (mixers, tumblers),
- wykrywanie powiązań z hackami i atakami na protokoły,
- analiza ryzyka geograficznego (jurysdykcje wysokiego ryzyka),
- analizę ryzyk związanych z DeFi (brak KYC po stronie kontrahentów).

Obecnie standardem rynkowym jest korzystanie z narzędzi typu Chainalysis, TRM Labs, Elliptic lub ich odpowiedników. Bank musi posiadać wewnętrzne procedury oceny ryzyka on-chain i integrować je z systemem AML.

2.8.6. Wymogi dotyczące prowadzenia platformy obrotu kryptoaktywów przez banki (art. 76–83 MiCA)

MiCA ustanawia pełny reżim prowadzenia platformy obrotu kryptoaktywami (*trading venue* dla krypto), który zawarty jest w art. 76–83. Bank, który zamierza prowadzić taką platformę w modelu z art. 60 MiCA (notyfikacja zamiast licencji CASP), korzysta z uproszczenia proceduralnego, ale materialnie podlega tym samym standardom co licencjonowany CASP: od zasad dopuszczania aktywów i uczestników, przez wymogi rynkowej przejrzystości i zapobieganie nadużyciom, po odporność systemów i zasady rozrachunku. MiCA wyraźnie zakazuje „taryf ulgowych": bank nie może prowadzić platformy „mniej bezpiecznie" niż standardowy CASP, a notyfikacja jest narzędziem kontroli *ex ante*, a nie „wolną kartą" wobec wymogów merytorycznych.

Operator platformy musi przyjąć jasne, przejrzyste reguły funkcjonowania (*rules of operation*). Reguły te co najmniej: opisują procesy zatwierdzania/dopuszczania kryptoaktywów (w tym due diligence proporcjonalne do ryzyka AML/CFT), definiują kategorie wykluczeń, kryteria uczestnictwa (obiektywne, niedyskryminacyjne), zasady „*fair and orderly trading*", warunki pozostawania aktywów w obrocie (progi płynności, ujawnienia) oraz warunki zawieszeń, a także procedury skutecznego rozrachunku aktywów i środków pieniężnych. Dopuszczenie jest niedopuszczalne bez wymaganego dokumentu informacyjnego (tam, gdzie MiCA go wymaga). Po-

nadto operator ocenia „odpowiedniość" (*suitability*) aktywów, w tym wiarygodność rozwiązań technologicznych i potencjalne powiązania z działaniami nielegalnymi; MiCA *expressis verbis* zakazuje dopuszczania aktywów z wbudowaną funkcją anonimizacji, chyba że identyfikacja posiadaczy i historii transakcji jest możliwa. Wymagany jest też językowy wymóg publikacyjny (język państwa macierzystego albo zwyczajowo używany w finansach).

Operator platformy nie może zawierać transakcji na własny rachunek na prowadzonej przez siebie platformie (w tym, gdy świadczy wymianę). Obrót polegający na „zestawianiu zleceń" (principal/ matched principal) dopuszczalny jest tylko za zgodą klienta i podlega ścisłemu monitorowaniu przez organ, aby nie generował konfliktów interesów. To ograniczenie funkcjonalnie zbliża platformy krypto do standardów MTF/OTF w MiFID II, gdzie również obowiązują rygory bezstronności, rozdziału ról i nadzoru nad konfliktami.

MiCA nakazuje, aby systemy obrotu były: odporne, o przepustowości adekwatnej do szczytowych wolumenów, zdolne do „orderly trading" w warunkach skrajnych, wyposażone w filtry odrzucające błędne/ponadprogowe zlecenia oraz objęte kompleksowymi testami i planami ciągłości działania. Operator musi posiadać mechanizmy wykrywania i zapobiegania nadużyciom rynkowym oraz wykorzystywaniu do prania pieniędzy/finansowania terroryzmu, a także obowiązek niezwłocznego raportowania wykrytych nadużyć do właściwego organu. Dodatkowo wprowadzono obowiązek inicjowania ostatecznego rozrachunku transakcji w rejestrze rozproszonym w ciągu 24 godzin od realizacji na platformie (lub – dla rozliczeń poza DLT – najpóźniej do zamknięcia sesji danego dnia).

Operator ma obowiązek bieżącej publikacji cen kupna/sprzedaży i poziomów zainteresowania (pre-trade transparency) w godzinach obrotu oraz publikacji ceny, wolumenu i czasu transakcji „tak szybko, jak technicznie możliwe" (post-trade transparency). Dane te muszą być udostępniane na rozsądnych warunkach, nieodpłatnie po 15 minutach i w formacie maszynowym przez co najmniej 2 lata. Operator przechowuje – lub zapewnia wgląd organowi do danych arkusza zleceń przez co najmniej 5 lat (specyfikacja treści/formatu ma charakter level-2).

Poza samym prowadzeniem venue MiCA reguluje też powiązane usługi. „Best execution" przy wykonywaniu zleceń (art. 78) wymaga polityki zapewniającej najlepszy dla klienta wynik oraz uzyskania zgody na wykonywanie poza platformą. Przy „przyjmowaniu/przekazywaniu zleceń" (art. 80) zakazane są wynagrodzenia/korzyści za kierowanie zleceń (unikanie „payment for order flow") i nieuprawnione użycie informacji o zleceniach. „Plasowanie kryptoaktywów" (art. 79) nakłada obowiązki informacyjne wobec emitenta oraz rygorystyczne zarządzanie konfliktami (np. przy plasowaniu do własnej bazy klientów).

Wymogi regulaminowe i systemowe operatora platformy sprzęgają się z reżimem AML/CFT, w tym z unijną „Travel Rule" (TFR) dotyczącą informacji towarzyszących transferom kryptoaktywów. Polityki dopuszczania aktywów i uczestników muszą być spójne z identyfikacją i przekazywaniem danych nadawcy/odbiorcy w łańcuchu (VASP-to-VASP), a systemy monitoringu powinny wykrywać aktywa/kontrakty i adresy o podwyższonym ryzyku. W praktyce oznacza to operacyjne połączenie reguł MiCA (market integrity) z obowiązkami wynikającymi z rozporządzenia 2023/1113 (TFR).

Wszystkie powyższe obowiązki „informatyczne" MiCA są komplementarne względem DORA: bank-operator platformy musi wykazać zarządzanie ryzykiem ICT, monitoring incydentów, testy TLPT, ład dostawców zewnętrznych (w tym chmury/HSM), a także zgodność z nadzorem trzecich dostawców krytycznych (CTPPs).

2.8.7. Rekomendacje wstępne

Powyższe ustalenia pozwalają na przedstawienie następujących rekomendacji wstępnych dla banków planujących świadczenie usług w zakresie kryptoaktywów. Bank powinien:

- Opracować i wdrożyć spójne polityki komunikacyjne dotyczące usług krypto, obejmujące zasady przygotowywania, akceptacji, publikacji oraz cyklicznej weryfikacji treści kierowanych do klientów.
- Przygotować jednolite, zgodne z MiCA szablony ostrzeżeń o ryzyku, obejmujące ryzyka technologiczne, rynkowe, operacyjne i środowiskowe właściwe dla usług opartych na kryptoaktywach.
- Wprowadzić procedury systematycznej weryfikacji materiałów marketingowych pod kątem zgodności z art. 66 MiCA, zapewniające eliminowanie treści mogących wprowadzać klientów

w błąd, w tym mechanizmy weryfikacji *ex ante* oraz okresowych przeglądów *ex post*.

- Zagwarantować pełną zgodność języka komunikacji – marketingowej, sprzedażowej i edukacyjnej – z zasadami uczciwości, jasności i rzetelności określonymi w art. 66 MiCA, w tym zasadą niedobierania lub pomijania informacji w sposób zniekształcający obraz ryzyka.

- Ustanowić proces raportowania informacji środowiskowych dotyczących kryptoaktywów, zgodny z art. 66 ust. 5–6 MiCA, obejmujący m.in. dane o zużyciu energii, emisjach oraz innych wskaźnikach wpływu środowiskowego aktywów objętych usługami banku.

- Wprowadzić formalny proces wewnętrznej akceptacji nowych usług krypto oraz zmian w istniejących usługach, obejmujący ocenę ryzyka operacyjnego, technologicznego, AML/CFT, zgodności z MiCA oraz wpływu zmian na sposób komunikacji z klientami; proces ten powinien być zgodny z wymogami MiCA i DORA dotyczącymi kontroli zmian oraz zarządzania ryzykiem ICT.

- Zapewnić regularne szkolenia pracowników zaangażowanych w świadczenie, sprzedaż lub promocję usług krypto (AML/CFT, ICT, operacje, sprzedaż, marketing), tak aby posiadali aktualną wiedzę dotyczącą ryzyk, obowiązków regulacyjnych i standardów komunikacji wynikających z MiCA.

2.9. Ryzyko utraty reputacji

Wejście banków w sektor kryptoaktywów niewątpliwie wiąże się z istotnym ryzykiem reputacyjnym, które może materializować się szybciej niż tradycyjne ryzyka rynkowe czy kredytowe. Wynika to zarówno z dynamiki rynku krypto, jego podatności na nadużycia oraz silnej wrażliwości opinii publicznej i nadzorców. Badania, raporty nadzorcze oraz doświadczenia rynków międzynarodowych potwierdzają, że ekspozycja banku na sektor krypto może tworzyć trzy zasadnicze źródła ryzyka reputacji:

- powiązanie z incydentami rynkowymi,

- ryzyka AML/ICT pochodzące od partnerów,

- niespójność regulacyjną skutkującą brakiem jasnego komunikatu do rynku.

Dlatego banki nie są traktowane przez MiCA jako podmioty wymagające nowej, autonomicznej autoryzacji, lecz jako instytucje kredytowe o rozszerzonym zakresie usług.

Przykłady rynku amerykańskiego wskazują, że nawet ograniczone ekspozycje na podmioty krypto mogą stać się katalizatorem gwałtownych zmian reputacyjnych. Raport Federal Deposit Insurance Corporation (FDIC) dotyczący upadku Signature Bank potwierdza, że negatywna narracja medialna dotycząca ekspozycji banku na sektor krypto – mimo że była tylko jednym z elementów sytuacji – przyczyniła się do narastającego odpływu nieubezpieczonych depozytów oraz pogorszenia zaufania rynku („negative press concerning crypto-related deposits contributed to heightened liquidity stress")[56].

Podobnie w przypadku Silvergate Bank, amerykańska SEC w pozwie z grudnia 2024 r. wskazała, że nieprawidłowości AML w relacjach z podmiotami krypto oraz brak właściwej reakcji zarządu stały się jednym z kluczowych czynników reputacyjnych, prowadząc do utraty zaufania rynku i paraliżu finansowania[57].

Europejski Urząd Nadzoru Bankowego (EBA) wskazał, że instytucje finansowe wchodzące w usługi krypto często nie zapewniają „*sufficient blockchain analytics, counterparty verification and travel rule compliance*". Braki te – nawet jeśli dotyczą partnerów zewnętrznych, a nie samego banku – mogą przenosić się na reputację instytucji kredytowej, jeżeli zostanie ona powiązana z incydentem o charakterze ML/TF[58].

Podobne wnioski przedstawia Financial Action Task Force (FATF), wskazując, że globalna implementacja „Travel Rule" jest nadal niepełna, a podmioty współpracujące z CASP z państw trzecich pozostają szczególnie narażone na ryzyka reputacyjne wynikające z „*regulatory arbitrage*"[59].

Komitet Bazylejski ds. Nadzoru Bankowego (BCBS) łączy aktywa krypto z podwyższonym ryzykiem re-

56 FDIC, *Material Loss Review – Signature Bank, New York* (April 2023), s. 14–18.

57 U.S. Securities and Exchange Commission, *SEC v. Silvergate Capital Corporation et al.*, Civil Action No. 23-cv-01502 (2024).

58 EBA, *Report on ML/TF risks associated with crypto-asset service providers* (January 2025).

59 FATF, *Targeted Update on Implementation of the Travel Rule*, June 2023.

putacyjnym, wskazując, że w przypadku aktywów z grupy 2 (cryptoassets with high risk) konieczne jest ujawnianie szczegółowych ekspozycji oraz stosowanie rygorystycznych zasad zarządzania ryzykiem. Standard BCBS „Prudential treatment of cryptoasset exposures" (December 2022) wskazuje, że w kontekście reputacji szczególne znaczenie ma *„market perception of insufficient governance around crypto activity"*[60].

Z kolei Financial Stability Board (FSB) w raporcie z października 2023 r. ostrzega, że *„regulatory gaps and cross-border inconsistencies create uncertainty that can amplify reputational risk for regulated financial institutions"*, zwłaszcza w przypadkach dynamicznych zmian rynkowych[61].

MiCA nakłada na dostawców usług krypto (w tym banki) obowiązek transparentnej komunikacji i rzetelnych ostrzeżeń. Naruszenie art. 66 MiCA może prowadzić do reputacyjnych zarzutów niewłaściwego oferowania produktów.

W świetle międzynarodowych doświadczeń takie zarzuty mają dużą wagę: UK Financial Conduct Authority wskazywała wielokrotnie, że niewłaściwa komunikacja w sektorze krypto prowadzi do utraty reputacji instytucji finansowych i ryzyk prawnych[62].

Jak widać, banki wchodzące w sektor krypto są obarczone podwyższonym ryzykiem reputacji, wynikającym zarówno z dynamiki rynku krypto, jak i ze wzmocnionej presji nadzorów. Ryzyko to materializuje się szybciej niż tradycyjne ryzyka bankowe i często pochodzi z incydentów u partnerów zewnętrznych. Minimalizowanie tego ryzyka wymaga zintegrowanego podejścia do governance, AML/CFT, DORA, zgodności informacyjnej z MiCA oraz przejrzystej komunikacji z rynkiem.

2.10. Wdrożenia usług kryptoaktywów w bankach europejskich

2.10.1. Santander UK – infrastruktura do custody i rozliczeń aktywów cyfrowych

Santander UK w 2023 r. rozpoczął projekt pilotażowy dotyczący infrastruktury przechowywania aktywów cyfrowych dla klientów instytucjonalnych. Z opublikowanych informacji wynika, że celem projektu było:

- opracowanie bezpiecznego systemu przechowywania kluczy prywatnych,
- testowanie rozwiązań klasy instytucjonalnej dla custody,
- weryfikacja zgodności z unijnym rozporządzeniem DORA (Regulation (EU) 2022/2554).

Santander wskazał, iż pilotaż „ma przygotować bank do rygorów wynikających z regulacji MiCA, w szczególności w zakresie custody i przejrzystości informacji dla klientów"[63]).

Rozwiązanie to stanowi przykład implementacji wymogów art. 75 MiCA, dotyczącego ochrony aktywów klientów, oraz art. 60 – wymogu przedstawienia organowi nadzoru szczegółowej dokumentacji techniczno-organizacyjnej.

2.10.2. BBVA Switzerland – pełne wdrożenie custody i tradingu

BBVA Switzerland jest jednym z pierwszych banków w Europie, oferujących klientom prywatnym usługi:

- custody Bitcoin i Ethereum,
- kupna i sprzedaży kryptoaktywów,
- integracji aktywów cyfrowych z klasyczną bankowością prywatną[64].

Bank opracował model przechowywania aktywów zgodny z wymogami FINMA, a w 2023 r. ogłosił dostosowanie dokumentacji i procedur do struktury

60 Basel Committee on Banking Supervision, *Prudential treatment of cryptoasset exposures*, Dec 2022.

61 FSB, *Global Regulatory Framework for Crypto-Asset Activities* (October 2023).

62 FCA, *Cryptoasset promotions – Warning on misleading claims*, October 2023.

63 Santander UK, *Institutional Digital Asset Custody Pilot*, 2023.

64 BBVA Switzerland, *Crypto Asset Services Overview*, 2023.

MiCA, wskazując, że kluczowe będą:

- art. 63 MiCA (informacje przekazywane klientom),
- art. 75 MiCA (obowiązki dostawców custody),
- art. 76 MiCA (segregacja aktywów).

BBVA już dziś implementuje wszystkie elementy wymagane w art. 60 ust. 7 MiCA, w tym procedury ryzyka operacyjnego, AML i zarządzania incydentami ICT – co czyni z niego modelowy przykład banku zgodnego z MiCA.

2.10.3. Deutsche Bank AG – licencjonowany custody provider

Deutsche Bank ogłosił w 2023 r. uzyskanie zgody BaFin na prowadzenie usług crypto custody na podstawie §1(1a) nr 6 KWG[65].

Wdrożenie obejmuje:

- system zarządzania kluczami o podwyższonym standardzie,
- politykę outsourcingu zgodną z BaFin Merkblatt (2023),
- pełną zgodność z cyberwymogami DORA.

Rozwiązanie to praktycznie odpowiada wymogom art. 75–76 MiCA, a Deutsche Bank już zapowiedział, że po wejściu MiCA przejdzie na reżim art. 60 (notyfikacja, brak potrzeby uzyskania nowej licencji).

BaFin wskazuje wprost, że: „banki posiadające doświadczenie w custody mogą być traktowane jako podmioty spełniające większość wymogów art. 60 ust. 7 MiCA"[66].

2.10.4. ING (Holandia) – zaawansowane prace nad tokenizacją i bezpieczeństwem kryptograficznym

Holenderski ING prowadzi badania nad infrastrukturą aktywów cyfrowych od 2018 r., publikując m.in. rozwiązania oparte na tzw. *Zero-Knowledge Range Proofs*[67]). Wdrożenia obejmują:

- prototypowy system custody,
- rozwiązania dla handlu aktywami tokenizowanymi,
- model bezpieczeństwa zgodny z DORA i wymogami EBA.

ING wskazuje, że prace te prowadzi „w kierunku zgodności z europejskimi regulacjami dotyczącymi aktywów cyfrowych, w tym MiCA"[68].

2.10.5. SEB (Szwecja) – platforma DLT do emisji tokenizowanych instrumentów

SEB wraz z Nasdaq Sweden wdrożył platformę DLT dla emisji obligacji i papierów wartościowych[69] (Nasdaq–SEB, *DLT Digital Bond Platform Launch*, 2022).

W praktyce jest to implementacja obowiązków z art. 79–83 MiCA dotyczących prowadzenia platform obrotu kryptoaktywami. Bank rozwija:

- system rejestru rozproszonego,
- połączenie z tradycyjnym rynkiem regulowanym,
- narzędzia do zgodności z governance określonym w MiCA art. 62.

2.10.6. Wdrożenia poza UE jako modele referencyjne dla MiCA

JPMorgan, poprzez projekt *Onyx*, wdrożył platformę blockchainową dla rozliczeń aktywów tokenizowanych[70] (JPMorgan, *Onyx Digital Assets Whitepaper*, 2023). Platforma ta:

- umożliwia tokenizację zobowiązań,
- wykorzystuje atomic settlement,

65 Deutsche Bank, *BaFin Approval for Digital Asset Custody*, 2023.

66 BaFin, *Hinweisschreiben zur MiCA-Umsetzung*, 2024.

67 ING, *ZKRP Technical Paper*, 2022.

68 ING Digital Assets Initiative, 2022.

69 Nasdaq–SEB, *DLT Digital Bond Platform Launch*, 2022.

70 JPMorgan, *Onyx Digital Assets Whitepaper*, 2023.

- jest zgodna z modelami regulacyjnymi przewidywanymi w MiCA dla usług tradingowych.

ESMA w dokumencie „MiCA Level 2 Technical Standards" (2024) wskazuje Onyx jako przykład „industry-leading institutional architecture", mogącej stanowić wzorzec dla implementacji wymogów art. 75 i 83 MiCA.

Standard Chartered, poprzez SC Ventures, uruchomił dwa serwisy instytucjonalne:

- Zodia Custody – przechowywanie aktywów,
- Zodia Markets – działalność transakcyjna.

Zodia Custody jest jednym z pierwszych światowych podmiotów wdrażających standardy identyczne z art. 75–76 MiCA[71]. ESMA oraz EBA wskazują Zodię jako przykład „segregacji aktywów, która w pełni odpowiada modelowi proponowanemu w MiCA"[72].

BNY Mellon od 2022 r. oferuje custody Bitcoin i Ethereum, integrując je z systemami bankowymi depozytów i funduszy powierniczych[73]. EBA i ESMA w konsultacjach z 2023 r. wskazały BNY Mellon jako przykład wdrożenia spełniającego:

- bezpieczeństwo operacyjne,
- integralność danych,
- segregację aktywów klientów.

2.11. Konkluzje

Z powyższych rozważań wynika, że nie tylko banki europejskie, ale także i światowe organizacje kredytowe wdrożyły liczne elementy przewidziane w MiCA, zanim regulacja weszła w życie. Większość wdrożeń dotyczy obszarów „wysokiego ryzyka" regulacyjnego: custody, AML, tokenizacja, cyberbezpieczeństwo. Praktyka rynkowa banków tworzy standard, który regulatorzy (EBA, ESMA, BaFin, CSSF) traktują jako benchmark. Można zatem z pełna odpowiedzialnością stwierdzić, że art. 60 MiCA nie stanowi bariery wejścia dla banków – przeciwnie, tworzy ścieżkę „notyfikacji zamiast licencji", z której banki mogą korzystać, wykorzystując istniejące wdrożenia.

Analiza wdrożeń pokazuje, że banki w praktyce przygotowały już:

Wymóg art. 60 ust. 7 MiCA	Wdrożenia bankowe
model operacyjny usług	BBVA, Santander, Deutsche Bank
governance i compliance	ING, SEB, BNY Mellon
custody i segregacja aktywów	Zodia, Deutsche Bank, BBVA
zarządzanie ICT i DORA	Santander, ING
AML/CFT specyficzne dla krypto	Standard Chartered, BBVA

71 Zodia Custody, *Service Overview*, 2022.

72 EBA, *RTS under MiCA*, 2023.

73 BNY Mellon, *Digital Asset Custody Announcement*, 2022.

3. Bariery techniczne i prawne w implementacji MiCA w strukturach bankowych

3.1. Zagadnienia wstępne

Jak już wskazywano, regulacja MiCA wprowadza jednolity system regulacji usług kryptoaktywów na rynku europejskim, a jej stosowanie w bankach odbywa się w oparciu o szczególny mechanizm z art. 60. Banki nie muszą uzyskiwać licencji CASP, ale są zobowiązane do notyfikacji działalności i przedstawienia dokumentów z art. 60 ust. 7, obejmujących m.in. systemy ICT, procedury AML, governance i polityki ochrony aktywów.

Implementacja MiCA w bankach wymaga dostosowania wielowarstwowych systemów organizacyjnych, ryzyka i zgodności. W praktyce banki mierzą i będą mierzyć się z następującymi barierami:

- **technicznymi** (IT, cyberbezpieczeństwo, integracja DLT),
- **prawnymi** (compliance, AML/CFT, outsourcing),
- **operacyjnymi** (custody, segregacja aktywów),
- **konsumenckimi** (informowanie klientów, ochrona inwestorów).

3.2. Bariery techniczne

3.2.1. Integracja kryptowalut z systemami legacy

Banki komercyjne i instytucje kredytowe w Unii Europejskiej funkcjonują w oparciu o rozbudowane systemy informatyczne typu core banking, które stanowią centralny element ich infrastruktury technologicznej i operacyjnej. Systemy te, często rozwijane od kilkunastu lub kilkudziesięciu lat, są zoptymalizowane pod kątem obsługi tradycyjnych produktów finansowych – kredytów, rachunków depozytowych, płatności międzybankowych czy instrumentów pochodnych – ale nie zostały zaprojektowane z myślą o technologii blockchain ani o kryptoaktywach. **Jak zauważa Europejski Urząd Nadzoru Bankowego (EBA),** „systemy instytucji kredytowych nie są z natury kompatybilne z mechanizmami blockchain i wymagają implementacji nowych modułów bezpieczeństwa, interoperacyjności i raportowania”[74].

W kontekście MiCA, integracja kryptoaktywów z infrastrukturą bankową oznacza zatem nie tylko dostosowanie organizacyjne, ale i głęboką modernizację architektury IT zgodnie z zasadami odporności cyfrowej (digital operational resilience) określonymi w rozporządzeniu (UE) 2022/2554 (DORA).

Systemy *legacy core banking* są z reguły monolityczne i scentralizowane, co oznacza, że dane klientów, transakcje i księgi rachunkowe są przetwarzane w ramach jednej, zamkniętej platformy. Integracja z technologią blockchain, która operuje w środowisku rozproszonym i kryptograficznie zabezpieczonym, powoduje szereg problemów architektonicznych:

- brak natywnego wsparcia dla przechowywania kluczy kryptograficznych i mechanizmów podpisu cyfrowego,
- brak funkcji umożliwiających transakcje on-chain (tj. rejestrowane bezpośrednio w łańcuchu bloków),
- brak infrastruktury pozwalającej na tokenizację aktywów (*asset tokenisation*),
- brak możliwości zastosowania tzw. *atomic settlement*, czyli natychmiastowego rozliczenia transakcji w ramach jednego procesu kryptograficznego.

Te ograniczenia sprawiają, że banki muszą wdrożyć tzw. warstwę integracyjną *(middleware)*, która umożliwia komunikację między systemem centralnym banku a blockchainem. Takie rozwiązania wprowadzają jednak dodatkową złożoność, opóźnienia i ryzyka cybernetyczne[75].

Rozporządzenie DORA (UE 2022/2554) w art. 9–12 nakłada na instytucje finansowe obowiązek wdrożenia systemów zapewniających odporność cyfrową, czyli zdolność do utrzymania ciągłości działania i bezpieczeństwa danych w środowisku wieloplatformowym. W odniesieniu do kryptoaktywów wymaga to m.in.:

- wdrożenia mechanizmów ochrony kluczy kryptograficznych (np. Hardware Security Modules – HSM),
- wprowadzenia monitoringu transakcji blockchainowych w czasie rzeczywistym,
- ustanowienia planów reagowania na incydenty ICT (art. 17 DORA),

74 European Banking Authority, *ICT and Security Risk Management under MiCA*, (EBA/CP/2023/11) p. 3.2.1.

75 Jak wskazuje ESMA, brak jednolitego standardu integracji z DLT „utrudnia zapewnienie spójności danych między księgą blockchain a systemem rachunkowym banku” – European Securities and Markets Authority, *MiCA Level 2 Technical Standards* (2024) section 5.1.

- zapewnienia zgodności z zasadą *segregation of duties* między systemem bankowym a platformą kryptoaktywną.

MiCA z kolei wymaga, aby instytucje świadczące usługi w zakresie kryptoaktywów zapewniły odpowiednie systemy techniczne, organizacyjne i bezpieczeństwa, umożliwiające przechowywanie aktywów klientów w sposób odseparowany i odporny na cyberzagrożenia. W praktyce oznacza to, że modernizacja systemów legacy jest warunkiem niezbędnym, by bank mógł skutecznie złożyć notyfikację zgodnie z art. 60 MiCA.

Integracja z systemami *core banking* wiąże się z następującymi wyzwaniami:

- niespójność formatów danych – blockchain przechowuje dane w formacie kryptograficznych hashy, podczas gdy systemy legacy wykorzystują relacyjne bazy danych (SQL). Konwersja między tymi strukturami jest kosztowna i ryzykowna;
- brak standardów API – brak wspólnego interfejsu programistycznego między dostawcami technologii DLT a systemami bankowymi utrudnia automatyzację;
- ryzyko operacyjne – dodanie kolejnych warstw integracyjnych zwiększa powierzchnię ataku i wymaga nowych procedur bezpieczeństwa;
- zgodność z zasadami audytu – blockchain wymaga nowego podejścia do audytu, ponieważ dane są nieusuwalne i przechowywane w sposób rozproszony.

Banki funkcjonują w oparciu o wieloletnie systemy *core banking*. Systemy te nie zostały zaprojektowane dla: przechowywania kluczy kryptograficznych, transakcji on-chain, tokenizacji aktywów, czy mechanizmów „atomic settlement". Integracja wymaga zatem modernizacji architektury IT zgodnie z DORA (Regulation (EU) 2022/2554). Jak bowiem wskazuje EBA: „systemy instytucji kredytowych nie są z natury kompatybilne z mechanizmami blockchain i wymagają implementacji nowych modułów bezpieczeństwa"[76].

W tym zakresie jedynie przykładowo wskazać należy, że Santander UK testuje tzw. Digital Assets Gateway – platformę pośredniczącą między systemem bankowym a blockchainem, opartą na standardzie ISO 20022. System umożliwia natychmiastowe rozliczenia (*atomic settlement*) i raportowanie zgodne z art. 63 MiCA[77].

Z kolei ING Bank N.V. w ramach projektu Pyctor opracował rozwiązanie multi-party custody, które łączy system legacy banku z blockchainem przy użyciu kryptograficznej technologii Multi-Party Computation (MPC). Projekt został zaprezentowany w ramach inicjatywy EBA FinTech Roadmap 2023 jako model zgodny z MiCA i DORA[78].[7]

W 2024 r. Deutsche Bank we współpracy ze szwajcarską firmą Taurus wdrożył moduł Taurus Custody, integrujący zarządzanie kluczami prywatnymi z infrastrukturą compliance banku. Projekt został zatwierdzony przez BaFin jako zgodny z art. 75 MiCA i art. 16 DORA[79].

W konsekwencji stwierdzić należy, że integracja technologii blockchain i kryptoaktywów z systemami bankowymi typu legacy jest jednym z najbardziej wymagających etapów wdrażania MiCA. Proces ten wymaga: przebudowy architektury IT i zapewnienia interoperacyjności, zastosowania nowych standardów bezpieczeństwa kryptograficznego, dostosowania systemów do zasad DORA i MiCA w zakresie odporności cyfrowej, wprowadzenia nowych polityk audytu i compliance. Bez spełnienia tych warunków banki nie będą w stanie skutecznie realizować usług kryptoaktywnych w zgodzie z prawem unijnym.

3.2.2. Ochrona klienta i przechowywanie aktywów (custody)

Ochrona klienta w zakresie przechowywania kryptoaktywów stanowi jedno z kluczowych zagadnień regulowanych przez MiCA. Artykuł 75 rozporządzenia określa kompleksowe obowiązki dostawców usług w zakresie przechowywania kryptoaktywów i administrowania nimi w imieniu klientów. W praktyce – w świetle art. 60 MiCA – przepisy te dotyczą również banków, które zamierzają świadczyć usługi custody w trybie notyfikacji, bez konieczności uzyskiwania licencji CASP (o ile spełnią wszystkie wymogi organizacyjne i technologiczne).

76 EBA, *RTS under MiCA*, 2023, p. 4.2.3.

77 Santander UK, *Digital Assets Gateway Pilot Documentation* (2023).

78 ING Bank N.V., *Pyctor Whitepaper: Institutional Digital Asset Custody* (2023).

79 Deutsche Bank AG and Taurus SA, *Integrated Custody Platform Launch Report* (2024).

Wprowadzenie art. 75 do systemu prawa UE oznacza, że banki wchodzące w obszar usług kryptoaktywnych muszą wdrożyć nowy, wysoce restrykcyjny standard ochrony aktywów klientów, porównywalny do obowiązków depozytariuszy instrumentów finansowych na gruncie MiFID II, UCITS V i AIFMD – ale dostosowany do specyfiki technologii DLT.

Art. 75 ust. 1 MiCA wymaga, aby dostawca usług custody – w tym bank działający na podstawie art. 60 – zawarł z klientem pisemną, sformalizowaną umowę, szczegółowo określającą zakres obowiązków i odpowiedzialności stron. Jest to element fundamentalny, ponieważ przechowywanie kryptoaktywów nie sprowadza się wyłącznie do funkcji technicznej. Dostawca staje się powiernikiem środków dostępu (kluczy prywatnych), a więc przyjmuje rolę zbliżoną do opiekuna majątku klientów.

Umowa musi obejmować m.in.: precyzyjną identyfikację dostawcy i klienta, szczegółowy opis rodzaju świadczonych usług i ich parametrów technicznych, politykę przechowywania, metody komunikacji, procedury uwierzytelniania i bezpieczeństwa, opłaty i koszty, wybór prawa właściwego. W praktyce umowa taka staje się instrumentem regulacyjnym i operacyjnym — bank musi wskazać, jakie rodzaje portfeli stosuje, jakie środki kryptograficzne chronią klucze klientów oraz jakie procedury obowiązują w przypadku awarii blockchaina lub ataku hakerskiego.

MiCA w art. 75 ust. 2 nakłada na banki obowiązek prowadzenia odrębnego, elektronicznego rejestru pozycji każdego klienta, który odzwierciedla stan i wszelkie operacje dotyczące jego kryptoaktywów. Jest to odpowiednik rachunku papierów wartościowych, lecz dostosowany do struktury aktywów cyfrowych.

Rejestr taki pełni funkcję dowodową, ewidencyjną i ochronną.

Zgodnie z art. 75 ust. 3 bank musi ustanowić formalną politykę przechowywania, obejmującą wewnętrzne zasady, procedury, kontrole i modele bezpieczeństwa. Polityka ta powinna minimalizować ryzyka związane z: utratą kluczy prywatnych, cyberatakami, błędami operacyjnymi, dostępem nieuprawnionych pracowników, awariami infrastruktury DLT.

Artykuł 75 ust. 4 nakłada na dostawców usług obowiązek aktywnego wspierania klientów w wykonywaniu praw wynikających z posiadanych kryptoaktywów. Oznacza to, że bank nie tylko przechowuje tokeny, lecz musi także: rejestrować wszelkie zmiany praw klienta w wyniku forków, airdropów, stakingu, tokenizacji lub migracji łańcucha, zapewnić klientom dostęp do nowych aktywów powstałych w wyniku zdarzeń technologicznych, aktualizować rejestr pozycji w sposób natychmiastowy.

Ten element ma ogromne znaczenie dla praktyki — w dotychczasowych modelach giełdowych wiele platform prywatnych nie przekazywało klientom nowych tokenów w wyniku forków. MiCA nakłada obowiązek ich wydania, chyba że klient wyraził zgodę na odstępstwo w umowie.

CASP ma obowiązek przekazywania klientom co najmniej co trzy miesiące informację o stanie aktywów, obejmującą: dane kryptoaktywa, saldo, wartość, przeniesienia dokonane w danym okresie. Praktyka bankowa będzie wymagała integracji systemów raportowych zgodnych z MiCA z dotychczasowymi systemami sprawozdawczymi (np. FINREP, COREP). ESMA w 2024 r. wskazała, że raporty custody powinny być „jasne, przejrzyste i zrozumiałe dla klientów detalicznych”[80].

Bank musi ponadto zapewnić możliwość szybkiego zwrotu aktywów klientów, także w sytuacjach awaryjnych. Dla tradycyjnych banków oznacza to konieczność integracji custody z procedurami BCP/DRP (Business Continuity Plan, Disaster Recovery Plan) zgodnie z DORA.

Jedną z najważniejszych norm MiCA jest art. 75 ust. 7, który stanowi o segregacji aktywów i ochronną przed niewypłacalnością. CASP musi: oddzielić aktywa klientów od aktywów własnych; wyraźnie oznaczyć klucze i pakiety kryptoaktywów; prowadzić oddzielne rejestry on-chain i off-chain; zapewnić prawne wydzielenie aktywów w razie niewypłacalności. W praktyce oznacza to, że wierzyciele banku nie mogą zaspokajać się z aktywów klientów, co jest zbieżne z konstrukcją depozytariusza UCITS i AIF. Dla banków jest to ogromne wyzwanie organizacyjne i prawne – zwłaszcza w zakresie nadzoru nad kluczami.

Artykuł 75 ust. 8 MiCA wprowadza quasi-obiektywną odpowiedzialność CASP: bank odpowiada za każdą utratę aktywów lub kluczy, o ile nie wykaże, że incydent był całkowicie niezależny od jego działania oraz od sposobu świadczenia usługi. Domniemanie winy nakłada na banki bardzo wysokie standardy bez-

80 ESMA, *Investor Protection Requirements for Crypto-Asset Services* (2024) 22.

pieczeństwa. EBA ocenia, że ten przepis „zmienia punkt odniesienia dla instytucji finansowych: odpowiedzialność nie wynika tylko z naruszenia umowy, ale z samego faktu prowadzenia usługi custody”[81].

3.3. Bariery prawne

3.3.1. Relacja MiCA do prawa krajowego i ryzyko „podwójnej regulacji”

Rozporządzenie MiCA – pomimo jego bezpośredniego stosowania – nie zastępuje wielu kluczowych aktów unijnego i krajowego prawa finansowego. Dla banków oznacza to konieczność równoczesnego stosowania CRR/CRD, PSD2, EMD2, TFR, DORA oraz przepisów krajowych – w szczególności Pr. bank., ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[82], ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (ustawa AML)[83] czy ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi[84]. W praktyce powoduje to powstanie szeregu punktów kolizji, niejasności i nakładania się obowiązków.

Po pierwsze, MiCA nie zmienia katalogu czynności bankowych określonych w Pr. bank. Dopóki ustawodawca nie znowelizuje art. 5 i 6 Pr. bank. (dodając np. świadczenie usług w zakresie kryptoaktywów jako względnej czynności bankowej), każda próba wejścia w rynek krypto – np. w obszarze emisji tokenów powiązanych z aktywami, custody czy prowadzenia platformy obrotu – będzie powodować wątpliwości, czy mieści się w granicach dotychczasowego zezwolenia KNF. Wymóg zmiany statutu za zgodą KNF (art. 34 Pr. bank.) staje się faktyczną barierą wejścia: bank – o czym była już mowa – musi zsynchronizować procedurę krajową z notyfikacją z art. 60 MiCA, co nie tylko wydłuży proces, ale i wprowadzi ryzyko rozbieżnych ocen materialnych.

Po drugie, ustawa o usługach płatniczych, implementująca dyrektywę PSD2, zdefiniowała „usługi płatnicze” oraz „instrument płatniczy” w oparciu o pojęcie środków pieniężnych. Transfer kryptoaktywów w rozumieniu MiCA nie jest usługą płatniczą *sensu stricto*, ale w praktyce granica między przelewem pieniężnym a transferem krypto może się zacierać. Brak jasnych wytycznych może tym samym powodować:

- ryzyko „podwójnej regulacji” (ta sama czynność kwalifikowana jako usługa płatnicza i usługa krypto);
- lub odwrotnie – powstanie luk regulacyjnych, gdy element pieniężny i krypto są rozdzielane pomiędzy podmioty z grupy.

Po trzecie, pamiętać należy, że wciąż w mocy pozostają ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi oraz dyrektywa MiFID II, zaś MiCA wprost wyłącza ze swojego zakresu kryptoaktywa będące instrumentami finansowymi. Banki projektujące produkty oparte na tokenizacji (np. cyfrowe obligacje, tokenizowane udziały w funduszach) każdorazowo będą zatem musiały przeprowadzić kwalifikację, czy dany token:

- jest instrumentem finansowym (wówczas zastosowanie mają MiFID II / MiFIR, a nie MiCA),
- czy „innym kryptoaktywem” podlegającym MiCA.

Niewątpliwie zaistnieje w związku z powyższym ryzyko prawne, że ocena dokonana przez bank może zostać zakwestionowana przez KNF lub ESMA – z konsekwencją konieczności dostosowania produktu do odmiennych wymogów prospektowych, informacyjnych i ostrożnościowych.

Po czwarte wreszcie, ustawa AML nakłada na banki obowiązki związane z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu. MiCA oraz rozporządzenie (UE) 2023/1113 (tzw. Transfer of Funds Regulation – TFR) dodają do tego specyficzne wymogi dla transferów kryptoaktywów („travel rule” dla krypto). Dopóki ustawa AML nie zostanie zaktualizowana w sposób odzwierciedlający nową architekturę MiCA/TFR, banki będą musiały na własny rachunek „scalać” dwa zestawy wymogów, co zapewne zwiększy zagrożenie niekomplementarności.

3.3.2. Procedura notyfikacji z art. 60 MiCA a krajowe procedury nadzorcze

Problematyka notyfikacji została już szeroko poruszona w innym miejscu niniejszego opracowania, przy czym konieczne jest ponowne zwrócenie uwa-

81 EBA, *Legal Risks in Crypto-Asset Custody* (2024) 5.

82 Tekst jedn. Dz.U. z 2025 r. poz. 611 ze zm.

83 Tekst jedn. Dz.U. z 2025 r. poz. 644.

84 Tekst jedn. Dz.U. z 2024 r. poz. 722 ze zm.

gi, że art. 60 MiCA wprowadza 40-dniowy termin na notyfikację planowanej działalności kryptoaktywnej, obejmującej m.in. program działania, systemy ICT, procedury AML/CFT, governance i polityki ochrony aktywów. Rozporządzenie zakłada, że po upływie tego terminu – przy braku sprzeciwu – bank może rozpocząć świadczenie usług. W polskim porządku prawnym ten mechanizm musi jednak zostać pogodzony z:

- procedurą zmiany statutu banku za zgodą KNF (art. 34 Pr. bank.),
- krajowymi wymogami dotyczącymi outsourcingu, chmury obliczeniowej i bezpieczeństwa ICT (m.in. „Komunikat chmurowy" UKNF),
- istniejącymi procedurami zatwierdzania nowych produktów i obszarów działalności.

Obecnie brak jednoznacznej sekwencji („najpierw" zmiana statutu i zgoda KNF, czy „najpierw" notyfikacja MiCA) tworzy barierę formalną:

- bank nie ma pewności, czy KNF będzie dokonywać oceny planowanej działalności krypto w ramach procedury statutowej, czy w ramach analizy notyfikacji MiCA, czy w obu równolegle;
- istnieje ryzyko podwójnego badania tych samych dokumentów (ICT, AML, governance) według odmiennych kryteriów;
- 40-dniowy termin MiCA może w praktyce zostać „rozciągnięty" przez konieczność uzupełniania dokumentacji pod kątem wymogów prawa krajowego.

Na dzień dzisiejszy brak jest także szczegółowych wytycznych KNF co do oczekiwanej zawartości dokumentacji notyfikacyjnej. Banki muszą więc w tym względzie opierać się na wytycznych ESMA/EBA, interpretując je przez pryzmat polskiej praktyki nadzorczej. To zaś ma wpływ nie tylko na potencjalnie zaistniałe ryzyko konieczności wielokrotnego uzupełniania notyfikacji, ale i zwiększa koszt przygotowania notyfikacji.

3.3.3. Outsourcing, chmura i dostawcy technologiczni

Rozporządzenie MiCA dopuszcza outsourcing, ale wymaga, aby dostawca usług w zakresie kryptoaktywów (w tym bank działający na podstawie art. 60) zachował pełną odpowiedzialność za zgodność usługi z rozporządzeniem. Jednocześnie DORA (rozporządzenie (UE) 2022/2554) wprowadza szczegółowy reżim zarządzania ryzykiem ICT oraz nadzoru nad dostawcami usług ICT trzeciej strony, w tym nad chmurą obliczeniową i dostawcami krytycznych usług ICT. W polskich realiach regulacyjnych dochodzi do tego „Komunikat chmurowy" UKNF, który:

- zawęża listę akceptowalnych lokalizacji danych,
- nakłada wymogi co do struktury umów chmurowych,
- wymaga zapewnienia KNF prawa audytu i wglądu do środowiska IT.

Dla banków planujących korzystanie z zewnętrznych HSM zlokalizowanych poza UE czy rozwiązań MPC działających w publicznej chmurze, a także dla podmiotów świadczących usługi on-chain analytics spoza Europejskiego Obszaru Gospodarczego, powstaje napięcie między efektywnością operacyjną a zgodnością regulacyjną. Konieczne jest zawieranie skomplikowanych umów trójstronnych (bank – dostawca – poddostawca), zapewnianie praw nadzorczych dla KNF i innych organów oraz rozwiązywanie problemu transgranicznego przekazywania danych (RODO, tajemnica bankowa). Brak precyzyjnych, sektorowych wytycznych zwiększa ponadto ryzyko, że dany model outsourcingowy zostanie *ex post* uznany przez nadzorcę za nieakceptowalny.

3.3.4. Ochrona konsumenta i odpowiedzialność cywilna banków

W MiCA zawarto szereg przepisów dotyczących ochrony klienta, w tym np. quasi-obiektywną odpowiedzialność za utratę kryptoaktywów w usługach custody (art. 75 ust. 8), obowiązki informacyjne (art. 66), segregację aktywów (art. 67) oraz wymogi przejrzystości kosztów. Na rynku polskim może to powodować kolizję z prawem krajowym: Kodeks cywilny oraz orzecznictwo krajowe dopuszczają w określonych granicach modyfikację odpowiedzialności kontraktowej, podczas gdy MiCA ustanawia domniemanie odpowiedzialności CASP/banku za utratę aktywów, które może być bardzo trudno wyłączyć w relacji z klientem detalicznym.

Zauważyć w tym miejscu należy, że ustawa z 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego, o Rzeczniku Finanso-

wym i o Funduszu Edukacji Finansowej[85] przewiduje określone standardy obsługi reklamacji. W przypadku nieodwracalnych transakcji on-chain, bank może nie mieć faktycznej możliwości „naprawienia" skutków błędu klienta, mimo potencjalnego oczekiwania wynikającego z praktyki rynku usług płatniczych.

Ponadto, ustawa z 16.02.2007 r. o ochronie konkurencji i konsumentów[86] oraz praktyka Prezesa UOKiK w zakresie klauzul abuzywnych mogą prowadzić do zakwestionowania części postanowień ograniczających odpowiedzialność banku za ryzyka technologiczne (np. ataki na sieć blockchain, forki, błędy smart kontraktów), nawet jeśli MiCA pozostawia tu pewien margines kontraktowy.

W praktyce banki staną więc przed koniecznością:

- przeprojektowania wzorców umownych i regulaminów tak, aby jednocześnie spełniały wymogi MiCA, były zgodne z prawem krajowym i nie naruszały standardów ochrony konsumenta;
- wdrożenia nowych procedur reklamacyjnych uwzględniających specyfikę nieodwracalności transakcji;
- opracowania strategii procesowej na wypadek sporów sądowych dotyczących usług krypto, które będą toczone przed sądami krajowymi stosującymi jednocześnie MiCA i prawo polskie.

3.4. Bariery operacyjne i organizacyjne

3.4.1. Struktura organizacyjna i governance

Zarówno rozporządzenie MiCA jak i DORA zakładają, że usługi w zakresie kryptoaktywów nie są „pilotażem technologicznym", lecz pełnoprawną częścią działalności regulowanej. ESMA i EBA podkreślają konieczność realnej substancji operacyjnej w UE, niezależności funkcji kontrolnych oraz spójności z istniejącymi ramami zarządzania ryzykiem. Dla banków oznacza to konieczność dokonania szeregu zmian organizacyjnych:

- wyznaczenia członka zarządu odpowiedzialnego za obszar kryptoaktywów;
- zdefiniowania ról i odpowiedzialności w pierwszej, drugiej i trzeciej linii obrony (business, risk/compliance, audyt),
- włączenia ryzyk krypto do komitetów ryzyka, komitetów produktowych oraz ICAAP/ILAAP.

Bariery operacyjne ujawniają się tam, gdzie dotychczasowe procesy banku zostały zaprojektowane wyłącznie z myślą o produktach tradycyjnych (kredyty, depozyty, instrumenty finansowe), a nie o aktywach on-chain. Dotyczy to w szczególności:

- procedur „new product approval", które nie uwzględniają oceny ryzyk specyficznych dla DLT (finalność probabilistyczna, reorgi, MEV, ataki na mosty międzyłańcuchowe);
- roli departamentu IT jako „dostawcy usług" vs. roli właścicieli biznesowych rozwiązań krypto;
- konieczności zbudowania kompetencji w zakresie audytu IT i audytu smart kontraktów.

Banki, które traktują kryptoaktywa wyłącznie jako rozszerzenie oferty inwestycyjnej, bez adekwatnego wpięcia w governance, narażają się na ryzyko negatywnej oceny nadzorczej, w tym zarzutów braku „tone from the top" lub nadmiernego polegania na podmiotach zewnętrznych.

3.4.2. Ryzyko operacyjne, ICAAP/ILAAP i testy odporności

Ekspozycja na kryptoaktywa generuje także specyficzne ryzyka operacyjne, które muszą zostać odzwierciedlone w ramach zarządzania ryzykiem operacyjnym, procesach wewnętrznej oceny adekwatności kapitałowej (ICAAP), procesach oceny adekwatności płynnościowej (ILAAP) i scenariuszach testów warunków skrajnych.

Do szczególnie istotnych należą:

- ryzyko utraty kluczy kryptograficznych lub kompromitacji systemów MPC/HSM;
- ryzyko błędów operacyjnych w obsłudze adresów krypto (np. wysyłka na błędny adres, niewłaściwy blockchain, brak memo/tagu);
- ryzyko przerw w działaniu sieci blockchain lub mostów (bridge outages), skutkujących zawieszeniem wypłat;

85 Tekst jedn. Dz.U. z 2024 r. poz. 1109 ze zm.

86 Tekst jedn. Dz.U. z 2024 r. poz. 1616 ze zm.

- ryzyko awarii lub utraty dostępności zewnętrznych dostawców ICT kluczowych dla usług krypto.

W praktyce banki muszą opracować nowe scenariusze testów odporności, które odzwierciedlają te ryzyka, oraz przypisać im odpowiednie bufory kapitałowe. Brak wypracowanego standardu rynkowego powoduje, że każdy bank jest zmuszony budować takie scenariusze autonomicznie, co zwiększa koszty i ryzyko rozbieżności z późniejszymi oczekiwaniami nadzorczymi.

3.4.3. Integracja procesów AML/CFT i narzędzi on-chain analytics

MiCA i TFR zakładają, że monitoring AML/CFT będzie obejmował nie tylko przepływy pieniężne, lecz także transakcje on-chain. Dla banków oznacza to konieczność:

- zakupu i integracji narzędzi typu Chainalysis lub odpowiedników;
- zbudowania reguł detekcyjnych właściwych dla aktywności krypto (mixery, tumblery, darknet markets, ransomware, adresy sankcyjne);
- powiązania wyników analiz on-chain z wewnętrznymi systemami scoringowymi i scenariuszami transakcji podejrzanych.

Barierą operacyjną jest tutaj zarówno dostępność kompetencji (specjalistów AML rozumiejących technologię DLT), jak i złożoność integracji danych:

- dane z blockchainu mają inny charakter (publiczność, pseudonimowość, format techniczny) niż tradycyjne dane transakcyjne;
- konieczne jest ustalenie, w jaki sposób wyniki scoringu on-chain wpływają na decyzje w zakresie KYC, EDD czy zamykania relacji.

Brak jednolitych wytycznych regulatorów co do minimalnego standardu stosowania narzędzi on-chain analytics powoduje niepewność co do tego, jaki poziom zaawansowania rozwiązań będzie uważany za wystarczający w świetle kardynalnej zasady „należytej staranności".

3.4.4. Bariery kadrowe i kompetencyjne

Nie sposób nie wspomnieć, że usługi krypto wymagają połączenia kompetencji: technologicznych (kryptografia, DLT, cyberbezpieczeństwo), regulacyjnych (MiCA, DORA, TFR, AML, CRR/CRD), a także biznesowych (projektowanie produktów finansowych, zarządzanie ryzykiem rynkowym).

Rynek pracy oferuje ograniczoną liczbę specjalistów, którzy łączą te obszary. Banki konkurują o tę samą pulę talentów z dużymi giełdami krypto, fintechami oraz firmami doradczymi. Z perspektywy operacyjnej oznacza to:

- wydłużony czas budowy zespołów projektowych;
- konieczność intensywnego programu szkoleń wewnętrznych;
- ryzyko nadmiernego polegania na doradcach zewnętrznych w kluczowych procesach (np. przy projektowaniu modeli custody czy architektury ICT), co może być krytycznie oceniane przez nadzór.

3.5. Bariery konsumenckie i relacja z klientem

3.5.1. Asymetria informacji i zrozumiałość produktów

Kryptoaktywa cechują się wysoką złożonością technologiczną i rynkową. MiCA nakłada na dostawców usług obowiązek przekazywania klientom jasnych, rzetelnych i niewprowadzających w błąd informacji (art. 66), ale nie usuwa fundamentalnej asymetrii informacji między bankiem a klientem detalicznym. W praktyce często zdarza się, że:

- klienci często mylą kryptoaktywa z depozytami bankowymi objętymi gwarancjami Bankowego Funduszu Gwarancyjnego;
- nie rozumieją różnicy między tokenem będącym instrumentem finansowym, e-pieniądzem a „innym kryptoaktywem" podlegającym MiCA;
- nie są świadomi ryzyk technologicznych (utrata klucza, fork, exploit smart kontraktu).

Banki stoją zatem przed zadaniem zaprojektowania materiałów informacyjnych i ostrzeżeń o ryzyku w sposób dalece wykraczający poza standardy znane z MiFID II. Brak dobrze ustrukturyzowanej komunikacji zwiększa ryzyko zarzutów nieuczciwego proponowania produktów finansowych, które nie odpowiadają potrzebom klienta (*misselling*) oraz sporów z klienta-

mi, w których MiCA będzie interpretowana przez sądy w duchu maksymalnej ochrony konsumenta.

3.5.2. Ocena adekwatności i odpowiedniości usług krypto

MiCA nie wprowadza wprost mechanizmu testu odpowiedniości w kształcie znanym z MiFID II, ale wymogi art. 66 oraz przepisy dotyczące doradztwa i zarządzania portfelem kryptoaktywów prowadzą w praktyce do konieczności stosowania zbliżonych standardów. Dla banków oznacza to konieczność podjęcia decyzji, czy:

- traktować usługi krypto skierowane do klientów detalicznych jako obszar wymagający pełnego badania profilu ryzyka, doświadczenia i wiedzy klienta (model „jak w MiFID II"),
- czy ograniczyć się do ostrzeżeń o ryzyku przy założeniu, że klient samodzielnie ocenia adekwatność produktu.

Pierwsze podejście generuje wyższe koszty operacyjne i może ograniczać dostępność usług, drugie – zwiększa ryzyko sporów i zarzutów missellingu. Brak jednoznacznych wytycznych powoduje, że banki kształtują własne modele, które mogą następnie zostać zakwestionowane przez nadzorcę lub sądy. Szczególnym problemem są produkty hybrydowe (np. tokenizowane depozyty, struktury z wbudowaną ekspozycją na krypto), w których element krypto bywa „ukryty" za znanym klientowi opakowaniem produktowym.

3.5.3. Reklamacje, spory i nieodwracalność transakcji on-chain

Tradycyjne usługi płatnicze i depozytowe opierają się na założeniu, że błędna transakcja może zostać skorygowana w drodze tzw. obciążenia zwrotnego (chargebacku), korekty księgowej lub uzgodnienia między bankami. W świecie kryptoaktywów transakcja zapisania w blockchainie jest co do zasady nieodwracalna. MiCA nie wprowadza mechanizmu „odwracania" transferów, a jedynie wymogi ochrony klienta i odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi.

Dla banków oznacza to szereg barier konsumenckich:

- konieczność jasnego komunikowania klientowi, że błędny transfer (np. na niewłaściwy adres) nie może zostać cofnięty w sposób analogiczny do przelewu SEPA;
- konieczność zaprojektowania nowych procedur reklamacyjnych, które skupiają się na analizie, czy błąd wynikał z działania banku (np. wady interfejsu, błędnych instrukcji) czy klienta;
- ryzyko sporów sądowych, w których klienci będą powoływać się na standardy ochrony znane z dyrektywy PSD2 i próbować przenosić je na grunt usług krypto.

Ponadto, w przypadku sporów transgranicznych (klient z innego państwa UE, usługa świadczona w trybie paszportowym) powstają dodatkowe bariery związane z kolizją jurysdykcji, prawem właściwym i sposobem wykonywania wyroków dotyczących zwrotu kryptoaktywów.

3.5.4. Wymiar reputacyjny i oczekiwania społeczne

Rynek kryptoaktywów jest silnie wrażliwy na incydenty medialne (upadki giełd, kradzieże, ataki hakerskie). Wejście banków w ten sektor powoduje, że negatywne zdarzenia – nawet jeśli dotyczą podmiotów trzecich – mogą być postrzegane przez opinię publiczną jako „wina banku", który zaoferował klientom ekspozycję na krypto.

MiCA nie reguluje wprost ryzyka reputacyjnego, ale raporty EBA, ESMA i EBC podkreślają konieczność jego uwzględnienia w strategii banku. Bariery konsumenckie mają tu charakter miękki, ale bardzo realny:

- część klientów i interesariuszy (np. organizacje konsumenckie) może postrzegać wejście banku w krypto jako sprzeczne z rolą instytucji zaufania publicznego;
- bank musi prowadzić komunikację z rynkiem w sposób tłumaczący, dlaczego i w jaki sposób wdrożono MiCA (wysokie standardy ochrony klienta, segregacja aktywów, DORA, AML), aby zminimalizować ryzyko utraty reputacji;
- każdy incydent technologiczny lub spór konsumencki w obszarze krypto będzie prawdopodobnie nagłaśniany w mediach w większym stopniu niż analogiczny incydent w tradycyjnej bankowości.

Ostatecznie bariery konsumenckie sprowadzają się do konieczności zbudowania zaufania do usług krypto oferowanych przez bank w środowisku, w którym zaufanie do rynku krypto jako takiego pozostaje ograniczone. Wymaga to długofalowej strategii edukacyjnej, transparentnej polityki informacyjnej oraz bardzo konserwatywnego podejścia do projektowania produktów dla klientów detalicznych.

4. W jaki sposób MiCA wpływa na ryzyko regulacyjne i reputacyjne instytucji finansowych?

4.1. Wprowadzenie

Rozporządzenie **MiCA** wprowadza kompleksowy zestaw mechanizmów ochrony inwestora (klienta), do których zobowiązani są emitenci kryptoaktywów oraz dostawcy usług kryptoaktywowych (CASP). Celem MiCA jest zmniejszenie asymetrii informacyjnej, ograniczenie ryzyka nadużyć oraz zapewnienie bezpieczeństwa środków klientów.

Wyróżnić można następujące główne grupy mechanizmów:

- **środki ochrony informacyjnej,** do których zaliczyć należy: zapewnienie obowiązku informacyjnego, obowiązek publikacji whitepaperu, ograniczenia związane z reklamą kryptoaktywów;
- **mechanizmy ochrony klienta przed utratą środków**, między innymi poprzez segregację środków klienta, odpowiedzialność CASP za utratę środków, wymogi techniczne w zakresie przechowywania środków oraz odrębne regulacje związane z postępowaniem upadłościowym CASP (w przypadku banku – zdaniem autorów – pierwszeństwo ma dyrektywa Parlamentu Europejskiego i Rady 2014/59/UE z dnia 15 maja 2014 r. ustanawiająca ramy na potrzeby prowadzenia działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji w odniesieniu do instytucji kredytowych i firm inwestycyjnych;
- **mechanizmy ochrony w zakresie tokenów**, stanowiących pieniądz elektroniczny oraz tokenów powiązanych z aktywami. Jest to między innymi: obowiązek pełnego pokrycia, obowiązek wykupu, wymogi związane z raportowaniem oraz audytowaniem środków;
- **mechanizmy ochrony przed nadużyciami rynkowymi** obejmują między innymi zakaz manipulacji rynkowej, w tym: *wash trading*, *pump & dump*, *spoofing*, zakaz insider tradingu;
- mechanizmy ochrony klienta w obsłudze i relacji z instytucją, do których zaliczają się procedury reklamacyjne.

W ramach niniejszej części zwrócona zostanie uwaga tylko na wybrane elementy ochrony klienta. Z uwagi na analogiczne regulacje w rozporządzeniu MiFID II, w analizie pominięte zostaną mechanizmy ochrony przed nadużyciami rynkowymi, gdyż są one analogiczne do już istniejących przepisów.

4.2. Mechanizmy informacyjne w odniesieniu do emisji kryptoaktywów na przykładzie tokenów stanowiących pieniądz elektroniczny

Whitepaper stanowi dokument informacyjny, którego rolą jest ochrona inwestora poprzez zapewnienie rzetelnej informacji o danym tokenie, w taki sposób, aby mógł poznać najważniejsze ryzyka związane z konkretnym aktywem. Co do zasady whitepaper ma za zadanie zapewnić transparentność rynku i stabilność sektora. Ponadto taki dokument powinien zawierać też najważniejsze informacje na temat infrastruktury bezpieczeństwa. Wskazany dokument informacyjny jest wymogiem dotyczącym wszystkich kryptoaktywów, przy czym tylko w przypadku tokenów będących pieniądzem elektronicznym oraz powiązanych z aktywami podlega zatwierdzeniu przez krajowy organ regulacyjny. W przypadku innych tokenów wymagana jest tylko autoryzacja, a w przypadku ograniczonych emisji innych tokenów nawet zgłoszenie do krajowego organu regulacyjnego nie jest wymagane.

W niniejszym opracowaniu analiza kwestii whitepaperu zostanie ograniczona do tokenów będących e-pieniądzem, ponieważ mają największe znaczenie dla sektora bankowego.

Na wstępie wskazać należy, że tylko instytucja kredytowa albo instytucja pieniądza elektronicznego może dokonywać oferty publicznej emitowanych tokenów, będących pieniądzem elektronicznym albo ich dopuszczenia do obrotu na platformie na terytorium UE. W tym celu, zgodnie z art. 48 ust. 1 MiCA, muszą zostać spełnione następujące warunki:

posiadanie zezwolenia na prowadzenie działalności jako instytucja kredytowa lub instytucja pieniądza elektronicznego;

sporządzenie, zgodnie z przepisami MiCA, i przekazanie organowi nadzoru projektu dokumentu informacyjnego (tzw. *whitepaper*). Oznacza to, że nie można przeprowadzić legalnej emisji bez opublikowania i zatwierdzenia whitepaperu przez krajowy organ regulacyjny.

Zgodnie z art. 51 ust. 1 MiCA, dokument informacyjny dotyczący kryptoaktywa i sporządzany dla tokena będącego e-pieniądzem zawiera wszystkie następujące informacje, określone szczegółowo w załączniku III. Wśród informacji znajduje się między innymi:

- informacje o emitencie tokena będącego e-pieniądzem;
- informacje na temat tokena będącego e-pieniądzem;
- informacje na temat oferty publicznej tokena będącego e-pieniądzem lub dopuszczenia go do obrotu;
- informacje na temat praw i obowiązków związanych z tokenem będącym e-pieniądzem;
- informacje na temat technologii bazowej;
- informacje na temat ryzyka;
- informacje na temat głównych niekorzystnych skutków dla klimatu i innych niekorzystnych skutków środowiskowych mechanizmu konsensusu stosowanego do emisji tokenów będących e-pieniądzem.

4.3. Wymogi informacyjne

Zgodnie z art. 66 ust. 1 MiCA, dostawcy usług w zakresie kryptoaktywów działają uczciwie, rzetelnie i profesjonalnie zgodnie z najlepiej pojętym interesem swoich klientów i potencjalnych klientów. Z kolei w myśl art. 66 ust. 2 MiCA, dostawcy usług w zakresie kryptoaktywów przekazują swoim klientom uczciwe, jasne i niewprowadzające w błąd informacje, w tym w materiałach marketingowych, które muszą być oznaczone jako takie. Dostawcy usług w zakresie kryptoaktywów nie mogą, umyślnie lub w wyniku zaniedbania, wprowadzać klienta w błąd w odniesieniu do rzeczywistych lub domniemanych korzyści związanych z jakimikolwiek kryptoaktywami. Jak stanowi art. 66 ust. 3 MiCA, dostawcy usług w zakresie kryptoaktywów ostrzegają klientów o ryzyku związanym z transakcjami dotyczącymi kryptoaktywów. Dostawcy usług w zakresie kryptoaktywów, którzy prowadzą platformę obrotu kryptoaktywami, wymieniają kryptoaktywa na środki pieniężne lub inne kryptoaktywa, świadczą doradztwo w zakresie kryptoaktywów lub zarządzają portfelem kryptoaktywów, przekazują swoim klientom hiperłącza do wszelkich dokumentów informacyjnych dotyczących kryptoaktywów, w odniesieniu do których świadczą te usługi. W myśl art. 66 ust. 4 MiCA dostawcy usług w zakresie kryptoaktywów udostępniają publicznie swoje polityki w zakresie cen, kosztów i opłat, zamieszczając ją w widocznym miejscu na swojej stronie internetowej.

Wskazany przepis zawiera obowiązek informacyjny oparty o zasadę zaufania. Oznacza to, że na dostawcy usług ciąży obowiązek przekazywania informacji w oparciu o interes klienta, a nie swój własny. Przepis ten nakłada na dostawcę usług obowiązek działania:

- uczciwie (bez manipulacji, zgodnie z deklaracjami),
- rzetelnie (z należytą starannością profesjonalisty),
- profesjonalnie (zawodowo, zgodnie z najlepszymi praktykami rynku),
- w najlepiej pojętym interesie klienta (klient nie może być narażony na nieuzasadnione ryzyko lub niekorzystne konsekwencje wynikające z działań dostawcy).

Z powyższych przepisów wynika kilka jasnych, niepoddających się dalszym ocenom, obowiązków. Poniżej wskazane obowiązki zostaną poddane wyjaśnieniu wraz z rekomendacjami związanymi ze stosowaniem wskazanego przepisu.

Po pierwsze, materiały marketingowe muszą być oznaczone jako reklama albo materiał marketingowy/ promocyjny. Takie oznaczenie komunikatu pozwala odbiorcy na odbiór konkretnego materiału jako treści, która ma skłonić go do skorzystania z produktu lub usługi.

Po drugie, informacje dla klientów powinny być formułowane w sposób prosty i zrozumiały, bez stosowania zbyt technicznego języka. Zaleca się testy czytelności oraz regularne przeglądy materiałów pod kątem ryzyka wprowadzania w błąd.

Po trzecie, materiał taki nie może wprowadzać w błąd w odniesieniu do rzeczywistych lub potencjalnych korzyści. Wszelkie materiały o charakterze promocyjnym powinny być poddawane uprzedniej kontroli działu zgodności, aby wyeliminować ryzyko nadmiernych obietnic lub sugestii nieadekwatnych korzyści. Naruszeniem powyższego przepisu będzie wskazywanie w takim materiale: „gwarantowanych" zysków, stałych stóp zwrotu, braku ryzyka. W naszej ocenie, najlepiej w materiałach marketingowych nie informować o potencjalnej stopie zwrotu związanej z danym kryptoaktywem, nawet jeśli w ramach stakingu konkretnego kryptoaktywa istnieje stała stopa zwrotu, w tym w aktywie; ewentualnie przedstawiać

dane historyczne, z informacją, iż cena w przyszłości nie jest znana i zachodzi ryzyko jej spadku. Wskazana uwaga odnosi się głównie do tokenów innych niż te będące pieniądzem elektronicznym oraz powiązanych z aktywami.

Po czwarte, istnieje obowiązek informowania o ryzyku. Obowiązek ten należy rozumieć jako zobowiązanie do publicznego przedstawienia informacji o ryzyku adekwatnym do danego rodzaju usługi. Obowiązek ten nie wskazuje konkretnych ryzyk, stąd jego realizacja nie powinna sprowadzać się tylko do wskazania, że korzystanie z konkretnej usługi wiąże się z ryzykiem utraty w całości lub części swoich środków (zarówno w odniesieniu do waluty fiducjarnej, jak i kryptoaktywów). Przykładowo, w przypadku oferowania usługi prowadzenia platformy wymiany zarówno walut urzędowych na kryptoaktywa, jak i kryptoaktywa na inne kryptoaktywa, informacja powinna dotyczyć wszelkich ryzyk związanych z możliwością utraty środków, które towarzyszą usłudze, zarówno: ryzyka rynkowego, jak i braku gwarancji pokrycia środków w przypadku niewypłacalności dostawcy czy ryzyka technicznego. Warto także poinformować o nieodwracalności transakcji w sytuacji przesłania kryptoaktywa do niewłaściwego odbiorcy.

Po piąte, polityka opłat powinna być opublikowana w widocznym miejscu na stronie internetowej oraz być stale aktualizowana. Zaleca się wykorzystywanie tabel, przykładów i kalkulatorów kosztów, by zwiększyć ich zrozumiałość.

Po szóste, platforma powinna udostępniać klientowi hiperłącza do dokumentów informacyjnych każdego kryptoaktywa (whitepaper MiCA) w miejscach, gdzie podejmowane są decyzje inwestycyjne, np. podczas składania zlecenia. Wskazany obowiązek nie dotyczy świadczenia usług typu custody czy przekazu kryptoaktywów.

Po siódme, system powinien rejestrować potwierdzenia zapoznania się przez klienta z ryzykami i dokumentami informacyjnymi. Zalecane jest potwierdzenie zapoznania się klienta z ryzykami i dokumentami przed rozpoczęciem korzystania z usługi, co ułatwi wykazanie zgodności z MiCA w razie kontroli.

Po ósme, treści informacyjne, materiały marketingowe i polityki opłat powinny być aktualizowane równolegle ze zmianami w ofercie, modelu biznesowym, cenach lub warunkach świadczenia usług. Zalecany jest co najmniej coroczny przegląd compliance.

Po dziewiąte, wśród wytycznych ESMA znajduje się następująca: „Właściwe organy powinny również rozważyć włączenie do swoich działań w zakresie monitorowania i nadzoru rynku wszelkiej komunikacji dotyczącej kryptoaktywów, w tym komunikacji odbywającej się na platformach internetowych, mediach społecznościowych i blogach, w biuletynach i podcastach, jeżeli są one wykorzystywane do rozpowszechniania informacji na temat kryptoaktywów, z zastosowaniem podejścia opartego na analizie ryzyka (z uwzględnieniem np. tematów, liczby użytkowników i dostępności). W ramach bieżącego nadzoru nad mediami właściwe organy mogą stosować automatyczne monitorowanie umożliwiające identyfikację wzorców, słów kluczowych i trendów, uzupełnione analizą przeprowadzaną przez ludzi”[87].

W tym miejscu warto zalecić podmiotom świadczącym usługi w zakresie kryptoaktywów, aby w umowach o zatrudnienie z pracownikami, którzy zajmują się tymi usługami, zostało zawarte zobowiązanie do powstrzymania się od wypowiadania się zarówno pod swoim imieniem i nazwiskiem, jak i pod pseudonimem na kanałach grupowej komunikacji internetowej w przedmiocie tematów związanych z kryptoaktywami, niezależnie o tego, czy dotyczą usług świadczonych przez tego konkretnego dostawcę. Takie zobowiązanie może być zabezpieczone karą umowną.

Naruszenie analizowanych przepisów może prowadzić do nałożenia przez właściwy organ kar administracyjnych za niedochowanie obowiązków wynikających z MiCA, a także zastosowania innych środków administracyjnych.

4.4. Mechanizmy ochrony finansowej klienta przed utratą środków

4.4.1. Segregacja aktywów klienta

Podstawowym mechanizmem ochrony środków inwestora przed ewentualną niewypłacalnością jest separacja środków klienta od aktywów instytucji kredytowej lub CASP-u.

87 Wytyczne ESMA dotyczące praktyk nadzorczych właściwych organów mających na celu zapobieganie nadużyciom na rynku i ich wykrywanie na podstawie rozporządzenia w sprawie rynków kryptoaktywów (rozporządzenie MiCA), s. 12, pkt 31, https://www.esma.europa.eu/sites/default/files/2025-07/ESMA75-453128700-1039_Guidelines_on_supervisory_practices_to_prevent_and_detect_market_abuse__MiCA__PL.pdf (dostęp: 30 listopada 2025 r.).

Zgodnie z art. 70 ust. 1 MiCA, dostawcy usług w zakresie kryptoaktywów, którzy posiadają kryptoaktywa należące do klientów lub środki dostępu do takich kryptoaktywów, wprowadzają odpowiednie mechanizmy mające na celu zabezpieczenie praw własności klientów, w szczególności w przypadku niewypłacalności dostawcy usług w zakresie kryptoaktywów, oraz mające na celu zapobieżenie wykorzystywaniu kryptoaktywów należących do klienta na swój własny rachunek. W myśl art. 70 ust. 3 MiCA, do końca dnia roboczego następującego po dniu otrzymania środków pieniężnych klientów innych niż tokeny będące e-pieniądzem dostawcy usług w zakresie kryptoaktywów deponują te środki pieniężne w instytucji kredytowej lub w banku centralnym. Dostawcy usług w zakresie kryptoaktywów podejmują wszelkie niezbędne kroki w celu zapewnienia, aby środki pieniężne klientów inne niż tokeny będące e-pieniądzem, zdeponowane w instytucji kredytowej lub w banku centralnym, były przechowywane na rachunku dającym się wyodrębnić od wszelkich innych rachunków wykorzystywanych do przechowywania środków pieniężnych należących do dostawców usług w zakresie kryptoaktywów.

Wskazany przepis chroni przed:

- ryzykiem niewypłacalności dostawcy/banku (chociaż w tym przypadku istnieją także inne przepisy, w tym np. dyrektywa o przymusowej restrukturyzacji banków – brak ochrony środków klientów w przypadku bankructwa CASP;
- ryzykiem wykorzystywania aktywów klientów przez CASP – np. w transakcjach własnych lub jako zabezpieczenie;
- ryzykiem błędów operacyjnych i braku przejrzystości – pomieszanie aktywów własnych z aktywami klientów.
- W tym zakresie zostały nałożone stosowne obowiązki na CASP oraz instytucje finansowe, które zostaną omówione poniżej.

4.4.2. Oddzielenie środków klientów od aktywów banku

Ochrona własności klientów sprowadza się zapewnienia, że kryptoaktywa lub środki pieniężne nie mogą być używane przez dostawcę na własny rachunek. Podmiot dostarczający usługi w zakresie kryptoaktywów musi wprowadzić mechanizmy zapobiegające wykorzystaniu kryptoaktywów klienta na własny rachunek. Wymóg obejmuje wszystkie aktywa klientów przechowywane przez ten podmiot, w tym tokeny, stablecoiny i inne kryptoaktywa. W tym zakresie bank powinien utworzyć oddzielne rachunki depozytowe klientów, wyodrębnione od środków własnych banku oraz stosować systemy księgowe umożliwiające pełną identyfikowalność aktywów klienta. Ponadto, bank powinien zapewnić, że środki pieniężne wpływają na odpowiedni rachunek w tym samym dniu lub najpóźniej do końca dnia roboczego następującego po wpłacie. Mechanizmy wdrożone przez dostawcę mają chronić aktywa klientów również w sytuacji jego niewypłacalności, tj. zarówno w przypadku egzekucji z majątku dostawcy jako dłużnika, jak i w sytuacji jego upadłości[88].

W tym miejscu warto zarekomendować utworzenie oddzielnych portfeli dla każdego klienta, z wyraźnym oznaczeniem w systemach księgowych i DLT. Podkreślić należy, że stosowanie kombinacji segregacji księgowej i operacyjnej segregacji kluczy (np. *aggregate on-chain* i *ledger off-chain* z ewidencją) w świetle MiCA jest również dopuszczalne, pod warunkiem, że zapewniają pełną identyfikowalność i wydzielenie praw klienta. Wybór rozwiązań technologicznych powinien być oparty na opiniach technicznych, dotyczących bezpieczeństwa cyfrowego. Możliwym, choć droższym, rozwiązaniem będzie zamówienie stworzenia modelu portfela na potrzeby konkretnego banku lub CASP. Zastosowane rozwiązania technologiczne powinny zaś zapewniać mechanizmy techniczne uniemożliwiające użycie aktywów klienta na własny rachunek CASP.

4.4.3. Ograniczenie ryzyka niewypłacalności CASP

W razie upadłości, aktywa klientów pozostają własnością klienta i nie wchodzą do masy upadłościowej. Wskazany mechanizm przypomina znane rozwiązanie w odniesieniu do upadłości banków lub domów maklerskich. Z uwagi na stosowanie do banków dyrektywy o przymusowej restrukturyzacji, przepisy wskazanej dyrektywy będą miały pierwszeństwo. MiCA nakłada obowiązek segregacji i wydzielenia, ale nie zastępuje ani nie rozszerza

88 E. Kniaziowska-Bryk [w:] M. Rypina, M. Wierzbowski (red.), *Rozporządzenie w sprawie rynków kryptoaktywów. Komentarz* [w:] *Rozporządzenie w sprawie rynków kryptoaktywów (MiCA) i rozporządzenie pilotażowe DLT (DLT Pilot Regime). Komentarz*, Warszawa 2025, art. 70, Nb 2.

systemów gwarancji depozytów ani reguł resolution. Stanowi to odrębne ramy regulacyjne.

4.4.4. Separacja środków klientów od środków banku

Środki muszą być umieszczone na oddzielnym rachunku, wyodrębnionym od rachunków instytucji kredytowej i CASP. Środki pieniężne klientów (poza tokenami e-money) należy zdeponować do końca dnia roboczego następującego po dniu otrzymania środków. Depozyt powinien być w instytucji kredytowej lub banku centralnym.

W przypadku, kiedy instytucja kredytowa świadczy usługi w zakresie kryptoaktywów, należy postawić pytanie: Czy środki mogą być zdeponowane w tej samej instytucji? Wydaje się, że odpowiedź na to pytanie jest twierdząca, gdyż instytucja taka wcześniej musiała spełnić wymogi regulacyjne związane z prowadzeniem działalności bankowej, także środki zdeponowane na oddzielnym koncie bankowym. Co więcej, prawodawca unijny nie zakazuje w żadnym przepisie takiej praktyki; ważna jest jednak separacja środków klienta i instytucji finansowej. Skoro więc unijny legislator nie stworzył ograniczenia, to nie sposób dostrzec podstaw do przyjęcia innego stanowiska.

4.4.5. Obowiązki w zakresie przechowywania (*custody*)

Dostawca usług powierniczych musi:

- utrzymywać wysoki poziom bezpieczeństwa kluczy prywatnych,
- prowadzić precyzyjne rejestry aktywów,
- wdrażać procedury ochrony przed cyberzagrożeniami,
- zapewniać, że aktywa klienta są zawsze dostępne i możliwe do zwrotu.

Zgodnie z art. 75 ust. 2 MiCA, dostawcy usług w zakresie kryptoaktywów, którzy zapewniają przechowywanie kryptoaktywów i administrowanie nimi w imieniu klientów, prowadzą otwarty w imieniu każdego klienta rejestr pozycji odpowiadających prawom każdego klienta do kryptoaktywów. W stosownych przypadkach dostawcy usług w zakresie kryptoaktywów rejestrują w tym rejestrze, możliwie jak najszybciej, wszelkie operacje wynikające z dyspozycji ich klientów. W takich przypadkach ich procedury wewnętrzne zapewniają, aby każda operacja mająca wpływ na rejestrację kryptoaktywów była udokumentowana transakcją prawidłowo zarejestrowaną w rejestrze pozycji klienta. W myśl art. 75 ust. 7 MiCA, dostawcy usług w zakresie kryptoaktywów, którzy zapewniają przechowywanie kryptoaktywów i administrowanie nimi w imieniu klientów, oddzielają pakiety kryptoaktywów, które przechowują w imieniu swoich klientów od swoich własnych pakietów i zapewniają, by środki dostępu do kryptoaktywów ich klientów były wyraźnie oznaczone jako takie. Zapewniają oni, aby w rozproszonym rejestrze kryptoaktywa ich klientów były przechowywane oddzielnie od ich własnych kryptoaktywów. Przechowywane kryptoaktywa są prawnie wydzielone z majątku dostawcy usług w zakresie kryptoaktywów w interesie klientów zgodnie z mającym zastosowanie prawem tak, aby wierzyciele dostawcy usług w zakresie kryptoaktywów nie mogli zaspokajać swoich roszczeń z kryptoaktywów przechowywanych przez dostawcę, w szczególności w przypadku jego niewypłacalności. Dostawca usług w zakresie kryptoaktywów zapewnia, aby przechowywane kryptoaktywa były pod względem operacyjnym oddzielone od jego majątku.

W tym zakresie należy zarekomendować:

- wprowadzenie w umowach z klientami postanowienia umownego, które wyraźnie określi wyodrębnienie kryptoaktywów klientów od środków banku;
- prowadzenie dokładnej ewidencji pakietów kryptoaktywów klienta;
- utworzenie systemów audytu umożliwiających weryfikację stanu aktywów w każdej chwili;
- raportowanie do regulatora zgodnie z wymogami MiCA.

Wskazane rozwiązania, związane z zapewnieniem bezpieczeństwa klienta, powinny być określone w regulaminach i materiach informacyjnych dotyczących konkretnego podmiotu, świadczącego usługi w zakresie kryptoaktywów.

4.4.6. Odpowiedzialność za utratę kryptoaktywów

W myśl art. 75 ust. 8 MiCA, dostawcy usług w zakresie kryptoaktywów, którzy zapewniają przechowywa-

nie kryptoaktywów i administrowanie nimi w imieniu klientów, ponoszą wobec swoich klientów odpowiedzialność za utratę kryptoaktywów lub środków dostępu do kryptoaktywów w wyniku incydentu, który można im przypisać. Odpowiedzialność dostawcy usług w zakresie kryptoaktywów jest ograniczona do wartości rynkowej utraconych kryptoaktywów w momencie wystąpienia utraty. Incydenty, których nie można przypisać dostawcy usług w zakresie kryptoaktywów, obejmują wszelkie zdarzenia, w odniesieniu do których dostawca usług w zakresie kryptoaktywów wykaże, że miały miejsce niezależnie od świadczenia odpowiedniej usługi lub niezależnie od operacji dostawcy usług w zakresie kryptoaktywów, takie jak problem nieodłącznie związany z eksploatowaniem rozproszonego rejestru, nad którym dostawca usług w zakresie kryptoaktywów nie sprawuje kontroli.

Wskazany przepis wprowadza odpowiedzialność cywilnoprawną dostawcy usług w zakresie kryptoaktywów oraz instytucji finansowych. Ten zakres podmiotowy wynika z redakcji przepisu i wprost wskazania w nim podmiotu, będącego dostawcą usług w zakresie kryptoaktywów. Dotyczy to też instytucji kredytowej, w tym banku.

Powyższej odpowiedzialności może dochodzić klient, który został poszkodowany na skutek utraty kryptoaktywów. Wskazane prawo dotyczy zarówno klienta, będącego osobą fizyczną, jak i prawną. Nie ma także znaczenia, czy roszczenie ma związek z działalnością gospodarczą. W tym zakresie prawodawca unijny nie rozróżnia klientów w zależności od ich konkretnych cech.

Przepis przewiduje trzy przesłanki odpowiedzialności:

- zajście incydentu;
- utratę kryptoaktywów lub środków dostępu do nich;
- związek przyczynowy pomiędzy incydentem a utratą środków.

Przez zajście incydentu należy rozumieć zdarzenie, które zakłóca świadczenie usług. Przyczyną incydentu może być zarówno działanie, jak i zaniechanie dostawców usług w zakresie kryptoaktywów. Przykładami incydentów mogą być: złośliwe oprogramowanie, błąd w smart kontrakcie, przełamanie zabezpieczenia systemu.

Przez utratę środków należy rozumieć szkodę rzeczywistą, a więc tylko kwotę, którą posiadacz kryptoaktywów utracił w ramach incydentu. Jej wartość jest w ramach odpowiedzialności określana na moment wystąpienia incydentu. Oznacza to, że jeśli klient utraciłby w dniu 20 marca 2025 roku 10 eth, to na potrzeby odpowiedzialności szkoda zostałaby przeliczona po kursie z dnia 20 marca 2025 roku z godziny dokonania incydentu. Wskazane rozwiązanie pozbawia więc dochodzącego swojego roszczenia klienta utraconych korzyści związanych z faktem np. utraty dochodów ze stakingu w czasie od incydentu do otrzymania zwrotu środków albo potencjalnego wzrostu wartości konkretnego kryptoaktywa.

Ostatnią przesłanką odpowiedzialności jest istnienie związku przyczynowego pomiędzy incydentem a szkodą. Związek ten należy rozumieć jako adekwatny związek przyczynowy, analogicznie do prawa cywilnego.

W przepisie została przewidziana także okoliczność egzoneracyjna zajścia incydentu, który to miał miejsce niezależnie od świadczenia odpowiedniej usługi lub niezależnie od operacji dostawcy usług w zakresie kryptoaktywów. Wskazana okoliczność jest wysoce dyskusyjna, gdyż na pierwszy rzut oka mogłoby się wydawać, że zachowanie, którego sprawcą była osoba trzecia, będzie eskulpować bank. Tak jednak nie jest, gdyż bank jest odpowiedzialny zarówno za wybór infrastruktury technicznej, jak i za bezpieczeństwo – w znaczeniu technicznym – środków. Powyższe oznacza, że badanie wskazanej przesłanki powinno opierać się na analizie dopełnienia przez bank obowiązków związanych z zabezpieczeniem środków klientów, zwłaszcza przepisów art. 75 MiCA. W istocie bank powinien zachować szczególną staranność w zakresie wykonywania swoich obowiązków. W literaturze wskazano przykład incydentu, w którym podmiot świadczący usługi w zakresie kryptoaktywów nie sprawuje kontroli, jednak administruje tymi kryptoaktywami na rzecz klienta i wobec tego rejestru rozproszonego dochodzi do ataku z wykorzystaniem luki w jego kodzie źródłowym w celu wytransferowania tychże kryptoaktywów na adres atakującego. Równocześnie wskazano, że optyka odnośnie do odpowiedzialności dostawcy mogłaby być przyjęta w sytuacji, gdyby świadczył on na rzecz klienta usługę zarządzania portfelem kryptoaktywów i to on podjąłby decyzję o zakupie danych kryptoaktywów do portfela klienta[89].

89 E. Kniaziowska-Bryk [w:] M. Rypina, M. Wierzbowski (red.),

Ciężar dowodu w zakresie wykazania: incydentu, szkody oraz związku między szkodą a incydentem ciążą na kliencie. W tym zakresie nie ma jednak potrzeby wykazywania dokładnie od strony technicznej, na czym polegał incydent. Wystarczającym jest wskazanie salda, które było na rachunku klienta przed incydentem i po nim. Nie sposób wymagać od klienta, aby bezpośrednio analizował przyczyny techniczne albo organizacyjne związane z utratą swoich środków, gdyż nie ma dostępu do takich informacji. Informacje takie posiada tylko CASP. Na potrzeby niniejszych rozważań można postawić tezę, że w przypadku utraty środków zdeponowanych w CASP poza wiedzą klienta, należy przyjąć domniemanie faktyczne, iż doszło do incydentu z przyczyn dotyczących CASP.

Ciężar dowodu wykazania, że do incydentu doszło niezależnie od świadczonych usług, ciąży na CASP. W tym przypadku dla oceny odpowiedzialności zasadnicze będzie zbadanie, na czym polegał incydent oraz czy miał on związek z brakiem lub nienależytym wykonaniem obowiązków ciążących na CASP w przepisach MiCA. W tym przypadku można dokonać testu adekwatności, czy gdyby CASP nie naruszył określonej normy, dotyczącej bezpieczeństwa kryptoaktywów, to adekwatnym skutkiem takiego naruszenia mógł być incydent, prowadzący do utraty środków. W przypadku takich postępowań sądowych niewątpliwie konieczne może być przeprowadzenie dowodu z opinii biegłego z zakresu informatyki, aby ten zarówno ustalił, na czym polegał incydent, jak i ocenił istnienie adekwatnego związku przyczynowego.

4.5. Odpowiedzialność podmiotów świadczących usługi z zakresu kryptoaktywów za zmianę cen kryptoaktywów

4.5.1. Odpowiedzialność cywilna

Niezależnie od powyższych przepisów, podmioty, które świadczą usługi z zakresu kryptoaktywów w przypadku naruszenia przepisów MiCA i ustawodawstwa je implementującego będą ponosić odpowiedzialność cywilną na zasadach ogólnych, a więc w oparciu o odpowiedzialność deliktową (art. 415 k.c.) lub kontraktową (471 k.c.). Wskazana odpowiedzialność ma swoje podstawy prawne w polskim prawie krajowym.

Odpowiedzialność deliktowa ma swoje źródło w ogólnych przepisach MiCA lub w ustawodawstwie je implementującym, które w istocie mają charakter publicznoprawny i określają standard szczególnej staranności w zakresie świadczenia wskazanych usług. W ramach tej odpowiedzialności będzie mógł dochodzić swoich roszczeń zarówno klient podmiotu świadczącego usługi, jak i osoba trzecia. W ramach wskazanej odpowiedzialności konieczne jest wykazanie: winy, zdarzenia powodującego szkodę, szkody oraz związku przyczynowego pomiędzy winą a szkodą. W ramach tej odpowiedzialności to na powodzie będzie spoczywał ciężar dowodu.

Obok odpowiedzialności deliktowej, możliwe jest dochodzenie roszczeń odszkodowawczych w reżimie odpowiedzialności kontraktowej, której źródłem jest niewykonanie albo nienależyte wykonanie zobowiązania. Wynika to z faktu, że każdy podmiot świadczący usługi z zakresu kryptoaktywów zawiera umowę z klientem o świadczenie usług. W związku z istnieniem umowy i zobowiązaniem się w niej do przestrzegania MiCA przez dostawcę usług, powstaje stosunek zobowiązaniowy pomiędzy klientem, a dostawcą usługi. Wobec powyższego roszczeń będzie mógł dochodzić tylko podmiot, który zawarł wcześniej umowę z podmiotem świadczącym takie usługi. W kontekście przesłanek odpowiedzialności, są one podobne jak w przypadku odpowiedzialności deliktowej, przy czym konieczne jest wykazanie naruszenia zobowiązania oraz zmianie ulega ciężar dowodu. Na powodzie występuje tylko wykazanie zdarzenia powodującego szkodę, szkody i związku przyczynowego. Istnieje domniemanie zawinienia, które może być obalone przez pozwanego w toku procesu.

Na koniec warto podkreślić, że to podmiot dochodzący odpowiedzialności jest uprawniony do wybrania podstawy jej dochodzenia. W myśl art. 443 k.c. okoliczność, że działanie lub zaniechanie, z którego szkoda wynikła, stanowiło niewykonanie lub nienależyte wykonanie istniejącego uprzednio zobowiązania, nie wyłącza roszczenia o naprawienie szkody z tytułu czynu niedozwolonego, chyba że z treści istniejącego uprzednio zobowiązania wynika co innego. Oznacza to, że powód będzie decydował, na jakiej podstawie będzie dochodził swojego roszczenia.

Rozporządzenie w sprawie rynków kryptoaktywów. Komentarz [w:] Rozporządzenie w sprawie rynków kryptoaktywów (MiCA) i rozporządzenie pilotażowe DLT (DLT Pilot Regime). Komentarz, Warszawa 2025, art. 75, Nb 3.

4.5.2. Odpowiedzialność podmiotów świadczących usługi z zakresu kryptoaktywów za zmianę cen kryptoaktywów

Cechą rynku kryptowalut jest to, że kursy kryptowalut zmieniają się bardzo często, *de facto* z sekundy na sekundę; co więcej jest to rynek, na którym notowania trwają 24 godziny przez siedem dni w tygodniu. Cena danego aktywa zależna jest od rynku, popytu/podaży, wahań globalnych itp. Jeśli CASP lub instytucja kredytowa uczciwie informuje klienta, że kurs jest rynkowy, zmienny i przedstawia aktualny kurs w momencie transakcji – to sama zmiana kursów (np. między momentem oferty a rozliczenia) jest naturalna i zwykle nie stanowi podstawy do odpowiedzialności. Regulacja MiCA nie gwarantuje ustalania stałych kursów kryptoaktywów, a ryzyko kursowe jest naturalnie wpisane w ten rynek.

Odpowiedzialność podmiotów dostarczających kryptoaktywa może jednak zaistnieć w sytuacji naruszenia przepisów MiCA, które będą skutkowały rozliczeniem transakcji klienta po kursach nierynkowych. W tym miejscu warto wskazać sytuacje, w których taka odpowiedzialność może mieć miejsce, w przypadku naruszenia konkretnych przepisów MiCA, w tym art. 68 ust. 2, który zobowiązuje CASP do działania w sposób uczciwy, rzetelny i profesjonalny w najlepiej pojętym interesie klientów. Innym przepisem jest art. 68 ust. 3 MiCA, który nakazuje przekazywanie informacji klientom w sposób rzetelny, jasny i niewprowadzający w błąd. Dalej, art. 72 MiCA nakazuje ujawnianie kosztów, opłat i zasad ustalania ceny, a zwłaszcza w zakresie ostatniego z wymienionych obowiązków niezwykle istotna jest kalkulacja ceny oraz wskazanie spreadu. Naruszenie wskazanych przepisów może skutkować odpowiedzialnością odszkodowawczą. Może to dotyczyć następujących stanów faktycznych:

- **kurs lub spread były przedstawione w sposób wprowadzający w błąd** (naruszenie art. 68 ust. 3 MiCA)
- Przykładowo, CASP pokazuje klientowi: „0% prowizji", ale stosuje wysoki ukryty spread.
- **CASP nie ujawnił zasad ustalania ceny** (naruszenie art. 72 MiCA)
- Przykładowo, CASP stosuje dynamiczny kurs, ale nie wyjaśnia, skąd pochodzi ani jak jest liczony.
- **CASP podał cenę nieaktualną lub nieadekwatną do rynku (***mis-pricing***)**. CASP nie może prezentować kursu „odklejonego" od metodologii, którą deklaruje klientowi.
- **CASP niewłaściwie przeprowadził *best execution* (jeśli dotyczy)** – MiCA przewiduje odpowiednik *best execution* w usługach wykonania zleceń. Jeśli kurs dla klienta był oderwany od deklarowanej metody wykonania, pojawia się odpowiedzialność.

W przypadku powyższych naruszeń przepisów MiCA, ustawodawca unijny nie przewidział odrębnego reżimu odpowiedzialności odszkodowawczej. Wskazana odpowiedzialność będzie ustalana na podstawie przepisów prawa krajowego. W przypadku Polski będzie to odpowiedzialność deliktowa oparta na art. 415 k.c. Oznacza to, że w przypadku CASP albo instytucji kredytowej konieczne jest wykazanie winy, polegającej na niedochowaniu staranności, w tym przypadku będzie to naruszenie obowiązków wynikających z MiCA. Rodzaj winy, umyślna czy nieumyślna, nie ma znaczenia dla odpowiedzialności podmiotu. Ponadto, konieczne jest wykazanie zaistnienia szkody i związku przyczynowego. Wskazana odpowiedzialność może być dochodzona zarówno w postępowaniach indywidualnych, jak i zbiorowych (na skutek wniesienia tzw. pozwu zbiorowego).

Obok odpowiedzialności cywilnej, CASP może odpowiadać za powyższe naruszenia w ramach odpowiedzialności administracyjnoprawnej przed krajowym organem regulacyjnym. Odpowiedzialność ta jest niezależna od powstania szkody po stronie klientów CASP. W ramach wskazanej odpowiedzialności za naruszenie art. 68 i 72 MiCA, krajowy organ regulacyjny może nałożyć karę pieniężną (maksymalna kara: do 5 mln euro albo do 12,5% rocznych przychodów CASP). Ponadto, organ regulacyjny ma kompetencje do cofnięcia licencji w przypadku rażącego naruszenia przepisów MiCA, w tym art. 68 i 72 MiCA. Dodatkowo możliwe jest też zastosowanie sankcji wobec kadry zarządzającej w CASP poprzez nałożenie zakazu pełnienia funkcji kierowniczych do 10 lat lub zakazu sprawowania obowiązków związanych z CASP. Dodatkowo, o naruszeniu organ regulacyjny powinien powiadomić publicznie.

4.6. Procedury skargowe w MiCA a sektor bankowy (analiza art. 70 i 71 MiCA)

4.6.1. Wprowadzenie

Artykuł 71 MiCA wprowadza jednolite wymogi dotyczące przyjmowania i rozpatrywania skarg przez dostawców usług w zakresie kryptoaktywów (CASP). Przepis ten stanowi kluczowy element systemu ochrony użytkowników usług kryptowalutowych, zapewniając odpowiedni standard transparentności, sprawiedliwości i dostępności ścieżki reklamacyjnej. W przypadku banków planujących świadczenie usług objętych MiCA, obowiązki te mają szczególne znaczenie, ze względu na wysokie ryzyko operacyjne i reputacyjne, jakie może wynikać ze zdarzeń związanych z kryptoaktywami[90].

4.6.2. Zakres obowiązków wynikających z art. 71 MiCA

Zgodnie z art. 71 ust. 1 MiCA, CASP zobowiązani są do ustanowienia i utrzymywania skutecznych, przejrzystych, szybkich i sprawiedliwych procedur rozpatrywania skarg klientów oraz do publikacji opisu tych procedur. Oznacza to konieczność opracowania dedykowanego procesu reklamacyjnego, który uwzględnia specyfikę technologii DLT, ryzyko utraty środków oraz charakter nieodwracalnych transakcji blockchain. Wskazany przepis ma zasadnicze znaczenie dla utrzymania dobrego wizerunku CASP. Brak właściwej procedury albo jej nieskuteczność mogą skutkować niezadowoleniem klientów, a co za tym – idzie rozprzestrzenianiem negatywnych opinii w internecie.

W zakresie samej procedury reklamacyjnej przepis art. 70 i 71 MiCA nie precyzuje jej dokładnie. W dniu 25 marca 2024 r. ESMA przyjęła **Regulatory Technical Standards (RTS)** dotyczące procedur rozpatrywania skarg, które po przyjęciu przez Komisję Europejską stanowią wiążące przepisy wykonawcze do art. 71 MiCA. Biorąc pod uwagę treść RTS, można znaleźć odpowiedzi na większość pytań, które mogą nasuwać się po lekturze przepisu.

Po pierwsze, jak należy rozumieć pojęcie „skargi"? W myśl art. 1 ust. 1 RTS, przez „skargę" należy rozumieć skierowane przez klienta do dostawcy usług w zakresie kryptoaktywów oświadczenie, w którym zgłasza swoje zastrzeżenia w związku ze świadczeniem jednej lub większej liczby usług. Skarga może być złożona w formie elektronicznej lub w formie pisemnej. Wskazany przepis w istocie pozwala na przyjęcie, iż istotą skargi jest wskazanie uwag w zakresie świadczonych usług niezależnie od formy.

Po drugie, czy CASP może określić w jakich językach skargi mogą być składane, poprzez ograniczenie na przykład do jednego albo trzech języków urzędowych UE? W tym zakresie wskazać należy, że co do zasady klienci powinni móc składać skargi w językach państw, w których są świadczone usługi[91].

Po trzecie, opracowane przez CASP procedury rozpatrywania reklamacji powinny zostać udostępnione w łatwo dostępnym miejscu na stronie internetowej wraz ze wzorem formularza do składania skarg. Procedura oraz formularz mają być publikowane we wszystkich językach używanych przez CASP do promowania swoich usług lub do komunikowania się z klientami92. W tym zakresie należy rekomendować umieszczenie na stronie internetowej CASP widocznego okna, nazwanego „reklamacje" albo „skargi", aby każdy użytkownik miał możliwość złożenia takiej skargi.

Po czwarte, dostawcy usług w zakresie kryptoaktywów, opracowując procedury rozpatrywania skarg, muszą dbać o to, aby zawierały one szereg szczegółowych informacji, takich jak:

- warunki dopuszczalności wniesienia skargi,
- informację o tym, że wniesienie i rozpatrzenie skargi jest wolne od jakichkolwiek opłat,
- szczegółowy opis procedury wnoszenia skargi, w tym: informację o możliwości skorzystania ze wzoru formularza do wniesienia skargi; informacje, które klient zobligowany jest dostarczyć CASP wraz ze skargą; dane osoby lub działu odpowiedzialnych za przyjmowanie skarg; adres korespondencyjny, adres e-mail, dane platformy elektronicznej lub systemu, za pomocą których można wnosić skargi; informację o językach, w których klient może złożyć skargę; opis proce-

90 Szerzej: P. Dyrduł, *Klient na rynku usług z zakresu kryptoaktywów – perspektywy ochrony w kontekście MiCA i polskiego projektu ustawy o kryptoaktywach*, Palestra 2025, Nr 1, s. 158–175.

91 art. 3 ust. 2 lit. a i b RTS.

92 art. 1 ust. 3 RTS.

su rozpatrywania skargi; harmonogram rozpatrywania skargi (potwierdzenie otrzymania, żądanie dodatkowych informacji, rozpatrywanie, udzielenie odpowiedzi); ustalenia dotyczące rejestrowania i przechowywania rozpatrzonych skarg[93].

Powyższe warunki najlepiej przedstawić w formie formularza, który będzie udostępniony w oknie „skarga".

Po piąte, opublikowany projekt RTS określa procedurę rozpatrywania skarg przez CASP. Wskazana procedura powinna być uregulowana w regulaminie świadczenia usług przez CASP. Także sam dokument określający sposób postępowania może być zamieszczony w widocznym miejscu na stronie internetowej.

W RTS zostało wskazane, że po otrzymaniu skargi dostawca usług w zakresie kryptoaktywów zobowiązany jest bez zbędnej zwłoki potwierdzić klientowi fakt otrzymania skargi wraz z informacją o dopuszczalności skargi. Potwierdzenie otrzymania skargi musi zawierać informacje o danych kontaktowych do osoby lub działu rozpatrujących skargę, datę otrzymania skargi, odniesienie do harmonogramu rozpatrzenia skargi, a także kopię skargi, jeżeli została ona złożona za pomocą elektronicznego formularza[94]. Jeżeli skarga nie spełnia warunków dopuszczalności, o których CASP informował w swojej procedurze, wówczas zobowiązany jest do przekazania skarżącemu niebudzących wątpliwości wyjaśnień powodów jej odrzucenia.

Rozpatrzenie skargi klienta musi nastąpić bez zbędnej zwłoki. Po potwierdzeniu jej otrzymania, właściwa osoba lub dział ze strony CASP ocenia, czy skarga jest zrozumiała i kompletna, tj. czy spełnia warunki określone w przyjętej i opublikowanej przez CASP procedurze. W razie konieczności dodatkowych wyjaśnień, informacji, uzupełnienia braków dostawca usług w zakresie kryptoaktywów ma zwrócić się do klienta (skarżącego) z prośbą o uzupełnienie zidentyfikowanych braków[95]. Sama procedura rozpatrywania skargi ma być jak najmniej uciążliwa dla klienta. Przejawiać ma się to m.in. w tym, że ciężar gromadzenia i oceny informacji stanowiących podstawę skargi ma spoczywać na CASP.

Po szóste, RTS zakazuje dostawcom usług w zakresie kryptoaktywów żądania od klienta informacji, które są lub powinny być w ich posiadaniu[96]. Klient w trakcie rozpatrywania reklamacji ma być należycie informowany przez CASP o stanie rozpatrywania skargi, jak również o wszelkich dodatkowych krokach, które będą podjęte w celu rozpatrzenia skargi. Procedura rozpatrywania wniesionej przez klienta skargi ma zakończyć się decyzją dostawcy usług w zakresie kryptoaktywów.

Po siódme, decyzja ta może odrzucić skargę bądź uwzględnić ją w całości lub w części. W wydawanej decyzji CASP ma się odnieść do wszystkich kwestii podnoszonych przez klienta w skardze, a także uzasadnić swoje stanowisko. W razie nieuwzględnienia w całości lub w części skargi klienta, CASP zobligowany jest do poinformowania klienta o dalszych możliwościach dochodzenia roszczeń, np. na drodze postępowania sądowego[97].

W zakresie czasu rozpoznawania skargi, w art. 6 ust. 2–4 RTS wskazano, że zasadą powinno być rozpoznanie skargi bez zbędnej zwłoki, nie dłużej jednak niż 2 miesiące, a w szczególnie uzasadnionych przypadkach ten czas może zostać wydłużony, przy czym klient powinien zostać poinformowany o terminie ostatecznego rozpoznania skargi.

4.6.3. Rekomendacje dla banków

Ogólne wytyczne, zawarte w RTS, należy dostosować do specyfiki konkretnego podmiotu świadczącego usługi.

Po pierwsze, banki powinny przygotować odrębną procedurę reklamacyjną, adresowaną tylko do usług w zakresie kryptoaktywów, która uwzględnia:

- specyfikę usług custody, tradingu i transferu,
- ryzyka związane z technologią DLT,
- nieodwracalność transakcji blockchain,
- bezpieczeństwo kluczy prywatnych.

Po drugie, w standardowym formularzu skargi, poza elementami wymienionymi powyżej, klient powinien

93 Art. 1 ust. 2 RTS.

94 Art. 4 ust. 3 RTS.

95 Art. 5 ust. 1 RTS.

96 Art. 5 ust. 3 RTS.

97 Art. 6 ust. 4 RTS.

mieć możliwość podania informacji specyficznych dla transakcji blockchain, takich jak:

- identyfikator transakcji (hash),
- adresy portfeli,
- rodzaj tokenu i blockchain,
- opis incydentu technicznego.

Po trzecie, bank powinien przeszkolić zespoły w zakresie: działania blockchain i DLT, analizy transakcji on-chain, interpretacji logów technicznych, identyfikacji incydentów cyber oraz technologicznych oraz funkcjonowania smart kontraktów.

Po czwarte, bank powinien utworzyć zintegrowany rejestr skarg. Wskazany rejestr pozwoli z jednej strony na identyfikowanie podobnych incydentów w przyszłości i zapobieganiu tym incydentom oraz będzie stanowił podstawę do uznania obowiązku w zakresie stworzenia procedury i rejestrowania skarg obowiązku publicznoprawnego przez organ regulacyjny. Rejestr powinien umożliwiać:

- monitorowanie trendów ryzyk,
- raportowanie do organów nadzorczych,
- identyfikację powtarzających się problemów,
- analizę incydentów technologicznych.

Rejestr powinien być powiązany z procesami: zarządzania incydentami (zgodnie z DORA), AML/CFT, monitorowania ryzyka operacyjnego.

Po piąte, bank powinien przyjąć:

- maksymalny czas potwierdzenia skargi (np. 48 godzin),
- maksymalny czas rozpatrzenia skargi (np. 14–30 dni).

Wskazane terminy są krótsze niż znajdujące się w zaleceniach RTS, jednak taka rekomendacja wynika z faktu, że niesprawna procedura skargowa grozi ryzykiem reputacyjnym. Brak szybkiego potwierdzenia przyjęcia skargi może negatywnie odbijać się na wizerunku banku na forach internetowych.

4.7. Nadzór regulacyjny i sankcyjny oraz odpowiedzialność administracyjna

4.7.1 Wprowadzenie

Kolejnym istotnym elementem, związanym z implementacją MiCA, jest nadzór regulacyjny, który jest wykonywany zarówno przez unijne organy nadzorcze, jak i krajowy organ regulacyjny („kompetentny organ" w rozumieniu MiCA; w Polsce tę funkcję miała pełnić Komisja Nadzoru Finansowego). Poniższa analiza ogranicza się do omówienia najważniejszych kompetencji oraz komentarza do najważniejszych ryzyk związanych z kontrolą rynku kryptoaktywów.

4.7.2. Instytucje unijne

4.7.2.1. European Securities and Markets Authority (ESMA)

ESMA to unijna instytucja nadzorcza, powołana w 2011 r. w ramach Europejskiego Systemu Nadzoru Finansowego (ESFS). Jest organem ponadnarodowym, który działa niezależnie, a jego zadaniem jest zapewnienie stabilności i integralności rynków finansowych UE. Głównym zadaniem ESMA jest ochrona jednolitego unijnego rynku kapitałowego. Wskazana instytucja wcześniej uzyskała wiele kompetencji w sprawie prowadzenia działań koordynacyjnych i nadzorczych w zakresie obrotu instrumentami finansowymi.

Do kompetencji ESMA na podstawie MICA należy:

- publikowanie listy kompetentnych organów („*competent authorities*") wyznaczonych w państwach członkowskich zgodnie z art. 93 MiCA[98];
- prowadzenie rejestru („*interim MiCA register*") zgodnie z art. 109–110 MiCA – rejestru *white papers*, wydawców tokenów, usługodawców świadczących usługi związane z kryptoaktywami;

98 https://www.esma.europa.eu/sites/default/files/2024-12/List_of_Competent_Authorities_notified_to_ESMA_under_MiCA.pdf (dostęp: 25 listopada 2025 r.).

- współpraca z organami krajowymi w zakresie harmonizacji nadzoru (*supervisory convergence*), między innymi poprzez wydawanie wytycznych oraz przygotowywanie standardów technicznych (RTS/ITS). RTS to wiążące akty prawne przygotowywane przez ESMA lub EBA, a następnie przyjmowane formalnie przez Komisję Europejską w formie rozporządzeń delegowanych (*delegated acts*). W tym miejscu warto podkreślić, że są one przygotowywane przez ESMA w ścisłej współpracy z European Banking Authority (EBA) i innymi instytucjami UE. Do najważniejszych przepisów upoważniających do wydawania wytycznych należą: art. 4 ust. 7 MiCA, dotyczący wytycznych w zakresie procedur zgłaszania informacji i prowadzenia rejestrów dostawców kryptoaktywów; art. 15 ust. 10 MiCA, który upoważnia do wydania wytycznych w przedmiocie standardów whitepaperu; art. 68 ust. 4 MiCA, dotyczący procedur zatwierdzenia CASP; art. 72 ust. 7 MiCA, dotyczący obowiązków związanych z przechowywaniem i zabezpieczaniem kryptoaktywów klientów; art. 78 ust. 10 MiCA, dotyczący systemów zarządzania ryzykiem operacyjnym i cyberbezpieczeństwa; art. 83 i 84 MiCA, dotyczące przejrzystości handlu i raportowania transakcji.

- pełnienie roli koordynatora w ramach „*supervisory colleges*" lub działań nadzorczych między państwami członkowskimi, w przypadku znacznych dostawców usług w zakresie kryptoaktywów (np. znaczące asset-referenced tokens – ART) lub e-money tokens (EMT). W tym miejscu warto przywołać wytyczne ESMA, określające, w jakich sytuacjach ten nadzór powinien mieć miejsce. Zgodnie z wytycznymi ESMA: „Właściwe organy powinny rozważyć wystąpienie do ESMA o koordynację kontroli lub dochodzeń, zgodnie z 95 ust. 5 rozporządzenia MiCA, zawsze jeżeli w przypadku transgranicznym:

  a) istnieją dowody lub podejrzenie, że w danej sprawie właściwe są więcej niż dwa organy;

  b) nieskoordynowane działania mogą negatywnie wpłynąć na ostateczny wynik dochodzenia; lub

  c) nieskoordynowane działania mogą prowadzić do dodatkowych obciążeń dla uczestników rynku"[99].

Podsumowując powyższe podkreślić należy, że główną rolą wskazanego organu unijnego jest koordynowanie działań państw UE w zakresie nadzoru nad rynkiem, nie zaś sprawowanie bezpośredniego nadzoru nad wszystkimi dostawcami kryptoaktywów w ramach UE. MiCA też nie daje żadnych uprawnień ESMA w zakresie nakładania kar administracyjnych na podmioty świadczące usługi w zakresie kryptoaktywów.

Najistotniejszą rolą ESMA będzie wydawanie wytycznych, które normatywnie stanowią *soft law*, jednak z perspektywy regulatorów mogą stanowić standardy postępowania i oceny przestrzegania przepisów MiCA, stąd wskazane akty wydawane przez ESMA mogą odgrywać równie ważną rolę, jak samo MiCA.

4.7.2.2. European Banking Authority (EBA)

EBA (European Banking Authority) to unijny organ nadzoru, odpowiedzialny za cały sektor bankowy i instytucji kredytowych. Istnieje od 2011 r. i tworzy wraz z ESMA i EIOPA trójfilarowy system nadzoru finansowego UE. Rolą EBA jest ujednolicanie standardów dotyczących banków poprzez wydawanie wytycznych, opinii, standardów technicznych (RTS/ITS). Ponadto pełni rolę w zakresie nadzoru nad unią bankową, w ramach którego współpracuje z Europejskim Bankiem Centralnym oraz koordynuje krajowe organy nadzoru.

Do kompetencji EBA na gruncie MiCA należy zaliczyć: opracowywanie standardów technicznych (RTS/ITS) wraz z ESMA dotyczące governance, rezerw, planów odzyskiwania i wykupu, sytuacji kryzysowych. Przykładem może być art. 61 ust. 11 MiCA, zgodnie z którym ESMA i EUNB wspólnie wydają, zgodnie z odpowiednio art. 16 rozporządzenia (UE) nr 1095/2010 oraz art. 16 rozporządzenia (UE) nr 1093/2010, wytyczne dotyczące oceny odpowiedniości członków organu zarządzającego dostawcy usług w zakresie kryptoaktywów ubiegającego się o zezwolenie oraz akcjonariuszy lub udziałowców – niezależnie od tego, czy bezpośrednich, czy pośrednich – posiadających znaczne pakiety akcji lub znaczne udziały w takim podmiocie.

4.7.3. Instytucje krajowe

Najważniejsze kompetencje, związane z nadzorem nad przestrzeganiem MiCA, pełnią organy krajowe. Zgodnie z art. 93 MiCA, państwa członkowskie wy-

99 https://www.esma.europa.eu/sites/default/files/2024-12/List_of_Competent_Authorities_notified_to_ESMA_under_MiCA.pdf (dostęp: 25 listopada 2025 r.), s. 13

znaczają właściwe organy odpowiedzialne za wykonywanie funkcji i obowiązków przewidzianych w niniejszym rozporządzeniu. Następnie o tym wyborze powinny powiadomić ESMA i EBA. To na organach krajowych spoczywają kompetencje zarówno związane z reglamentacją działalności w zakresie kryptoaktywów, jak również bieżącym nadzorem, w tym kompetencje sankcyjne.

W tym miejscu należy podkreślić, że MiCA dało bardzo daleko ingerujące w działalność podmiotów kompetencje do nakładania sankcji administracyjnych, których nałożenie może skutkować czasową albo trwałą niemożnością prowadzenia dalszej działalności. Wskazane sankcje pełnią rolę zapobiegawczą w zakresie uniknięcia wyrządzenia szkód uczestnikom rynku, w tym konsumentom, oraz naruszenia stabilności systemu finansowego, a także naruszenia zaufania do rynku kryptoaktywów. Stosowanie jednak wskazanych niżej sankcji zwykle jest oparte na ogólnej dyspozycji „naruszenia przepisów Rozporządzenia MiCA", „podejrzenia naruszenia przepisów Rozporządzenia MiCA" lub „zagrożenia naruszeniem przepisów Rozporządzenia w przyszłości". Tak sformułowane dyspozycje przepisów rodzą pytanie, czy naruszenie dowolnego przepisu MiCA może skutkować tak dalece idącymi sankcjami. W istocie dyspozycje norm nie są wyraźnie określone i pozostawiają ustawodawcom krajowym dalece idącą swobodę w zakresie określania potencjalnych sytuacji, kiedy organ krajowy będzie mógł wskazane niżej środki administracyjne stosować.

W naszej ocenie, rolą ustawodawców krajowych jest taka implementacja wskazanych przepisów, aby odnosiły się do konkretnych naruszeń, tak aby przesłanki stosowania administracyjnoprawnych środków były dostatecznie określone przy zachowaniu zasady proporcjonalności oraz celowości stosowania środka w odniesieniu do konkretnego naruszenia. Wszakże zbyt daleko idącym środkiem byłby zakaz prowadzenia usług w zakresie kryptoaktywów, w przypadku naruszenia przepisów określających wymogi reklamowe produktów podmiotu oferującego tego typu usługi. Brak określoności stosowania wskazanych sankcji w przepisach krajowych może skutkować stwierdzeniem ich niekonstytucyjności przez Trybunał Konstytucyjny, w przypadku zainicjowania postępowania przez uprawniony podmiot. Stąd implementacja tych przepisów powinna uwzględniać wagę naruszeń do możliwego zastosowania przez instytucję krajową środka.

Na koniec warto wskazać, że tak ogólne przepisy o środkach administracyjnych stwarzają ryzyko, które może skutkować utratą reputacji banku, nie tylko w zakresie świadczenia usług związanych z kryptoaktywami, ale także w zakresie właściwej działalności bankowej.

4.7.3.1. Kompetencje związane z reglamentacją działalności gospodarczej w odniesieniu do usług w zakresie kryptoaktywów

W zakresie autoryzacji emitentów tokenów powiązanych z aktywami właściwe organy są uprawnione do:

- wydawania decyzji w przedmiocie udzielenia lub cofnięcia zezwolenia na oferowanie tokenów powiązanych z aktywami lub na przyjęcie do obrotu (art. 21 i 24 MiCA);
- przyjmowania od instytucji kredytowych powiadomień i ich kontroli, ewentualnie wstrzymania emisji kryptoaktywów powiązanych z aktywami (art. 17 MiCA).

Instytucja krajowa może cofnąć zezwolenie lub wstrzymać emisję tokenów powiązanych z aktywami, jeżeli:

- emitent nie spełnia warunków udzielenia zezwolenia, np. naruszył wymogi z art. 16–19 MiCA (np. *governance*, rezerwy, *white paper*);
- emitent nie spełnia już wymogów organizacyjnych lub ostrożnościowych, m.in. w zakresie art. 29 MiCA (*governance*), art. 30–38 MiCA (rezerwy, polityka inwestycyjna, zarządzanie ryzykiem);
- emitent narusza obowiązki wobec posiadaczy tokenów, w szczególności brak możliwości wykupu lub nieodpowiednia wartość rezerwy;
- emitent dostarczył nieprawdziwe lub niepełne dane, np. w procesie autoryzacji (art. 17 MiCA);
- dalsza działalność zagraża stabilności finansowej lub ochronie konsumentów;
- token staje się „*significant*" (istotny), a emitent nie spełnia wymogów EBA, co wynika z art. 20 ust. 1 lit. f MiCA w powiązaniu z art. 43–45 MiCA.

W zakresie autoryzacji emitentów tokenów, stanowiących pieniądz elektroniczny, to instytucje kredytowe (banki) lub instytucje pieniądza elektronicznego (e-money institutions) mogą zgłosić krajowej instytucji emisję. W tym zakresie instytucja krajowa sprawdza zgodność z prawem, w tym z MiCA, warunki emisji. Jeżeli wydawca jest instytucją pieniądza elektronicznego – stosuje się procedurę z dyrektywy 2009/110/WE (a nie nową autoryzację pod MiCA). Banki nie otrzymują nowej licencji, ale podlegają nadzorowi zgodności z tytułem IV MiCA.

Instytucja krajowa może **zawiesić oferowanie lub przyjmowanie do obrotu** kryptoaktywów, będących pieniądzem elektronicznym, jeżeli:

- materiały marketingowe są niezgodne z prawem, np. wprowadzają w błąd, są niejasne, nieuczciwe (art. 51 MiCA);
- white paper EMT jest niekompletny lub narusza MiCA (art. 49 ust. 3 i art. 51 MiCA);
- emitent (np. bank) narusza wymogi wykupu (art. 50 ust. 1–2 MiCA);
- istnieje zagrożenie dla stabilności finansowej lub systemu płatniczego (art. 50 ust. 5 lit. d MiCA);
- emitent nie spełnia wymogów segregacji aktywów lub rezerwy (art. 47 MiCA).

4.7.3.2. Stosowanie środków administracyjnych

W związku powyższymi ofertami, krajowy organ może stosować środki administracyjne, które polegają na:

- nałożeniu na oferujących, osoby ubiegające się o dopuszczenie do obrotu kryptoaktywów lub emitentów tokenów powiązanych z aktywami lub tokenów będących e-pieniądzem obowiązku uwzględnienia w ich dokumencie informacyjnym dotyczącym kryptoaktywa dodatkowych informacji, jeżeli to konieczne dla zapewnienia stabilności finansowej lub dla ochrony interesów posiadaczy kryptoaktywów, w szczególności posiadaczy detalicznych;
- zawieszeniu oferty publicznej lub dopuszczeniu do obrotu kryptoaktywów na okres jednorazowo nie dłuższy niż 30 kolejnych dni roboczych, jeżeli istnieją uzasadnione powody, aby podejrzewać, że naruszone zostały przepisy rozporządzenia;
- zakazaniu dokonania oferty publicznej lub zakazaniu dopuszczenia do obrotu kryptoaktywów, w przypadku stwierdzenia, że doszło do naruszenia rozporządzenia, lub w przypadku gdy istnieją uzasadnione powody, aby podejrzewać, że mogło dojść do jego naruszenia.

Wskazane powyżej środki mają charakter władczy i ich stosowanie w realiach prawa polskiego powinno przybrać formę decyzji administracyjnej. Podmiot świadczący usługi w zakresie kryptoaktywów powinien mieć zagwarantowane prawo wniesienia skargi do wojewódzkiego sądu administracyjnego.

4.7.3.3. Autoryzacja podmiotów, będącymi dostawca usług w zakresie kryptoaktywów (CASP)

Instytucja krajowa wydaje zezwolenie CASP albo cofa takie zezwolenia (art. 62 i 64 MiCA). Ponadto instytucja krajowa ma obowiązek zgłosić do ESMA oraz EBUP informacje o powiadomieniu przez CASP albo instytucję finansową o zamiarze prowadzenia działalności w innym państwie (art. 67 MiCA). Wskazana procedura ma charakter autoryzacyjny. Organ krajowy nie może odmówić przekazania takiego zgłoszenia.

Do środków administracyjnych, związanych z ograniczeniem możliwości świadczenia usług, zaliczyć należy:

- zawieszenie świadczenia usług przez dostawcę usług w zakresie kryptoaktywów lub zobowiązanie dostawcy usług w zakresie kryptoaktywów do zawieszenia świadczenia tych usług na okres każdorazowo nie dłuższy niż 30 kolejnych dni roboczych, jeżeli istnieją uzasadnione powody, aby podejrzewać, że doszło do naruszenia rozporządzenia;
- zakazanie świadczenia usług w zakresie kryptoaktywów, w przypadku gdy stwierdzono, że doszło do naruszenia rozporządzenia;
- zawieszenie świadczenia usług przez dostawcę usług w zakresie kryptoaktywów lub zobowiązanie dostawcy usług w zakresie kryptoaktywów do zawieszenia świadczenia tych usług, jeżeli właściwy organ uznaje, że dostawca usług w za-

kresie kryptoaktywów znajduje się w takiej sytuacji, że świadczenie usług w zakresie kryptoaktywów byłoby szkodliwe dla interesów klientów, w szczególności posiadaczy detalicznych;

- nałożenie obowiązku przeniesienia istniejących umów do innego dostawcy usług w zakresie kryptoaktywów w przypadkach cofnięcia zezwolenia na prowadzenie działalności w charakterze dostawcy usług w zakresie kryptoaktywów zgodnie z art. 64, z zastrzeżeniem zgody klientów i dostawcy usług w zakresie kryptoaktywów, do którego umowy te są przenoszone;

- nakazanie natychmiastowego zaprzestania działalności bez uprzedniego ostrzeżenia lub wyznaczenia terminu, jeżeli istnieje powód, aby przypuszczać, że dana osoba świadczy usługi w zakresie kryptoaktywów bez zezwolenia.

4.7.3.4. Nadzór i bieżący monitoring zgodności

Instytucje krajowe monitorują przestrzeganie przepisów MiCA w zakresie wymogów dotyczących m.in.: whitepaperów, przepisów dotyczących zarządzania ryzykiem, wymogów związanych z dopuszczalnością zasiadania w zarządach określonych osób, rezerw aktywów czy wymogów dotyczących obowiązków reklamowych.

W przypadku stwierdzenia przez instytucję krajową naruszenia powyższych wymogów, instytucja krajowa może stosować następujące środki administracyjne:

- zobowiązanie podania do publicznej wiadomości faktu, że dostawca usług w zakresie kryptoaktywów nie spełnia swoich obowiązków;

- zobowiązanie do ujawnienia lub zobowiązania oferującego, osoby ubiegającej się o dopuszczenie do obrotu kryptoaktywa lub emitenta tokena powiązanego z aktywami lub tokena będącego e-pieniądzem do ujawnienia wszystkich istotnych informacji, które mogą mieć wpływ na ocenę kryptoaktywa będącego przedmiotem oferty publicznej lub dopuszczonych do obrotu, aby zapewnić ochronę interesów posiadaczy kryptoaktywów, w szczególności posiadaczy detalicznych, lub zapewnić sprawne działanie rynku;

- do wystąpienia o usunięcie osoby fizycznej z organu zarządzającego emitenta tokena powiązanego z aktywami lub dostawcy usług w zakresie kryptoaktywów;

- i inne.

4.7.3.5. Kontrole, inspekcje, żądanie informacji

Instytucja krajowa na podstawie art. 94 MiCA może m.in.: żądać dokumentów, danych, rejestrów; żądać wyjaśnień od członków zarządu i pracowników; przeprowadzać kontrolę na miejscu; uzyskiwać dostęp do systemów IT; wzywać podmioty do usunięcia naruszeń. Ponadto, instytucja krajowa nabyła uprawnienia do przesłuchania osób; wzywania do dostarczenia informacji; przeszukania pomieszczeń (zgodnie z prawem krajowym). Wskazane uprawnienia mają charakter służebny wobec innych uprawnień instytucji krajowej. Ich celem jest ustalenie stanu faktycznego na potrzeby innych postępowań prowadzonych przez instytucję. Część informacji może także być konieczna do sprawowania bieżącego nadzoru. W istocie bez posiadania przez instytucję krajową powyższych uprawnień, nadzór mógłby stać się iluzoryczny.

4.7.4. Kary administracyjne

Obok środków administracyjnych, które mają charakter zapobiegawczo-naprawczy, MiCA przewiduje także kompetencje do nakładania kar administracyjnych za naruszenie przepisów MiCA oraz innych sankcji o charakterze administracyjnym. Wskazane kary mogą być nakładane równolegle do wcześniej wymienionych sankcji administracyjnych. Środki administracyjne, o których mowa w art. 95 MiCA, mogą być stosowane zarówno w razie stwierdzenia naruszenia, jak i jego uzasadnionego podejrzenia lub ryzyka. Natomiast administracyjne kary pieniężne, o których mowa w art. 111 MiCA, mogą być nakładane wyłącznie za stwierdzone naruszenie. Warto podkreślić, że różnica między karą a stosowaniem środków zapobiegawczo-naprawczych jest taka, że kara ma charakter „odpłaty za naruszenie przepisów Rozporządzenia"; w istocie jest ona formą negatywnej oceny postępowania określonego podmiotu występującego na rynku kryptoaktywów. Z kolei środki administracyjno-naprawcze służą w pierwszej kolejności celom prewencyjnym, a więc zapobiegnięciu wyrządzenia potencjalnych szkód na rynku na skutek naruszania przepisów MiCA.

Stosowanie kar administracyjnych, zgodnie z art. 111 MiCA, może dotyczyć naruszeń następujących przepisów:

- art. 4–14 (przepisy regulujące zasady emisji tokenów innych niż kryptoaktywa powiązane z aktywami lub te będące pieniądzem elektronicznym);
- art. 16, 17, 19, 22, 23 i 25, art. 27–41, art. 46 i 47 (przepisy o dopuszczalności świadczenia usług w zakresie kryptoaktywów oraz przepisy dotyczące rezerwy aktywów);
- art. 48–51, art. 53, 54 i 55;
- art. 59, 60, 64 i art. 65–83;
- art. 88–92;
- brakiem współpracy lub niepoddaniem się czynnościom dochodzeniowym, kontroli lub niezastosowaniem się do żądania, o którym mowa w art. 94 ust. 3.

Wskazane kary, zgodnie z art. 111 ust. 3 MiCA, w odniesieniu do naruszeń popełnianych przez osoby prawne, właściwe krajowe instytucje miały uprawnienia do nakładania administracyjnych kar pieniężnych w maksymalnej wysokości co najmniej:

- 5 000 000 EUR lub w państwach członkowskich, których walutą urzędową nie jest euro, równowartości tej kwoty w walucie urzędowej na dzień 29 czerwca 2023 r. w odniesieniu do naruszeń, o których mowa w ust. 1 akapit pierwszy lit. a–d;
- 3% łącznego rocznego obrotu osoby prawnej ustalonego na podstawie ostatniego dostępnego sprawozdania finansowego zatwierdzonego przez organ zarządzający w odniesieniu do naruszeń, o których mowa w ust. 1 akapit pierwszy lit. a;
- 5% łącznego rocznego obrotu osoby prawnej ustalonego na podstawie ostatniego dostępnego sprawozdania finansowego zatwierdzonego przez organ zarządzający w odniesieniu do naruszeń, o których mowa w ust. 1 akapit pierwszy lit. d;
- 12,5% łącznego rocznego obrotu osoby prawnej ustalonego na podstawie ostatniego dostępnego sprawozdania finansowego zatwierdzonego przez organ zarządzający w odniesieniu do naruszeń, o których mowa w ust. 1 akapit pierwszy lit. b i c.

W przypadku gdy osoba prawna, o której mowa w akapicie pierwszym lit. a–d, jest jednostką dominującą lub jednostką zależną jednostki dominującej, która jest zobowiązana do sporządzenia skonsolidowanego sprawozdania finansowego zgodnie z dyrektywą 2013/34/UE, za stosowny łączny roczny obrót uznaje się łączny roczny obrót lub odpowiadający mu rodzaj dochodu zgodnie z mającymi zastosowanie przepisami prawa Unii w dziedzinie rachunkowości, ustalony na podstawie ostatniego dostępnego skonsolidowanego sprawozdania finansowego zatwierdzonego przez organ zarządzający jednostki dominującej najwyższego szczebla.

Wskazane przepisy określają, jaki maksymalny wymiar kar może przewidzieć ustawodawca krajowy, który będzie implementował przepisy MiCA. Nie określają one jednak minimalnego poziomu tych kar.

W myśl art. 111 ust. 2 MiCA, obok powyższych kar administracyjnych organy krajowe mogą także stosować inne sankcje administracyjne jak:

- w odniesieniu do naruszeń, o których mowa w ust. 1 akapit pierwszy lit. a–d, co najmniej poniższych kar administracyjnych i innych środków administracyjnych:
  a) podania do wiadomości publicznej informacji wskazującej osobę fizyczną lub prawną odpowiedzialną za naruszenie oraz charakter naruszenia;
  b) nakazu zobowiązującego odpowiedzialną osobę fizyczną lub prawną do zaprzestania określonego postępowania stanowiącego naruszenie oraz do powstrzymania się od jego powtarzania;
  c) administracyjnych kar pieniężnych w maksymalnej wysokości co najmniej dwukrotności kwoty korzyści uzyskanych lub strat uniknętych w wyniku naruszenia, o ile można je określić, nawet jeżeli wysokość ta przekracza kwoty maksymalne określone w lit. d niniejszego ustępu w odniesieniu do osób fizycznych lub w ust. 3 w odniesieniu do osób prawnych;
  d) w przypadku osoby fizycznej – administracyjnych kar pieniężnych w maksymalnej

wysokości co najmniej 700 000 EUR lub – w państwach członkowskich, których walutą urzędową nie jest euro – równowartości tej kwoty w walucie urzędowej na dzień 29 czerwca 2023 r.

Z kolei w przypadku naruszeń, o których mowa w lit. e także inne sankcje:

a) podania do wiadomości publicznej informacji wskazującej osobę fizyczną lub prawną odpowiedzialną za naruszenie oraz charakter naruszenia;

b) nakazu zobowiązującego odpowiedzialną osobę fizyczną lub prawną do zaprzestania określonego postępowania stanowiącego naruszenie oraz do powstrzymania się od jego powtarzania;

c) wydania korzyści uzyskanych lub wyrównania strat unikniętych w wyniku naruszenia, o ile możliwe jest ich ustalenie;

d) cofnięcia lub zawieszenia zezwolenia na prowadzenie działalności w charakterze dostawcy usług w zakresie krypto- aktywów;

e) tymczasowego zakazu pełnienia funkcji kierowniczych w przedsiębiorstwach dostawców usług w zakresie kryptoaktywów wobec dowolnego członka organu zarządzającego dostawcy usług w zakresie kryptoaktywów lub dowolnej innej osoby fizycznej, których uznano za odpowiedzialnych za naruszenie;

f) w razie ponownego naruszenia art. 89, 90, 91 lub 92 – co najmniej 10-letniego zakazu pełnienia funkcji kierowniczych w przedsiębiorstwie dostawcy usług w zakresie kryptoaktywów wobec dowolnego członka organu zarządzającego dostawcy usług w zakresie kryptoaktywów lub dowolnej innej osoby fizycznej, których uznano za odpowiedzialnych za naruszenie;

g) tymczasowego zakazu zawierania transakcji na własny rachunek wobec dowolnego członka organu zarządzającego przedsiębiorstwem dostawcy usług w zakresie kryptoaktywów lub wobec dowolnej innej osoby fizycznej, których uznano za odpowiedzialnych za naruszenie;

h) administracyjnych kar pieniężnych w maksymalnej wysokości co najmniej trzykrotności kwoty korzyści uzyskanych lub strat unikniętych w wyniku naruszenia, o ile można je określić, nawet jeżeli wysokość ta przekracza kwoty maksymalne określone, zależnie od przypadku, w lit. i lub j;

i) w przypadku osoby fizycznej – administracyjnych kar pieniężnych w maksymalnej wysokości co najmniej 1 000 000 EUR za naruszenia art. 88 i 5 000 000 EUR za naruszenia art. 89–92 lub – w państwach członkowskich, których walutą urzędową nie jest euro – równowartości tych kwot w walucie urzędowej na dzień 29 czerwca 2023 r.;

j) w przypadku osób prawnych – administracyjnych kar pieniężnych w maksymalnej wysokości co najmniej 2 500 000 EUR za naruszenia art. 88 i 15 000 000 EUR za naruszenia art. 89–92 lub 2% łącznego rocznego obrotu tej osoby prawnej według ostatniego dostępnego sprawozdania finansowego zatwierdzonego przez organ zarządzający za naruszenia art. 88 oraz 15% tej kwoty za naruszenia art. 89–92 lub – w państwach członkowskich, których walutą urzędową nie jest euro – równowartości tych kwot w walucie urzędowej na dzień 29 czerwca 2023 r.

Rozporządzenie MiCA wskazuje na podstawie art. 112 ust. 1 i 2 MiCA następujące dyrektywy wymiaru kar oraz wskazanych sankcji administracyjnych:

a) wagę naruszenia i czas jego trwania;

b) kwestię, czy naruszenie jest wynikiem działania umyślnego czy zaniedbania;

c) stopień odpowiedzialności osoby fizycznej lub prawnej odpowiedzialnej za dane naruszenie;

d) sytuację finansową osoby fizycznej lub prawnej odpowiedzialnej za naruszenie, której wyznacznikiem jest wysokość łącznego obrotu odpowiedzialnej osoby prawnej lub rocznego dochodu oraz aktywów netto odpowiedzialnej osoby fizycznej;

e) skalę korzyści uzyskanych lub strat unikniętych przez osobę fizyczną lub prawną

odpowiedzialną za naruszenie, o ile można je ustalić;

f) straty poniesione przez osoby trzecie w wyniku naruszenia, o ile można je ustalić;

g) poziom współpracy osoby fizycznej lub prawnej odpowiedzialnej za naruszenie z właściwym organem, bez uszczerbku dla konieczności zapewnienia wydania korzyści uzyskanych lub wyrównania strat uniknietych przez tę osobę;

h) poprzednie naruszenia niniejszego rozporządzenia popełnione przez osobę fizyczną lub prawną odpowiedzialną za naruszenie;

i) środki zastosowane przez osobę odpowiedzialną za naruszenie w celu zapobieżenia jego powtórzeniu się;

j) wpływ naruszenia na interesy posiadaczy kryptoaktywów i klientów dostawców usług w zakresie kryptoaktywów, w szczególności posiadaczy detalicznych.

Ponadto, na wymiar kary może mieć wpływ współpracy naruszyciela z organem krajowym.

W myśl art. 114 ust. 1 MiCA, organy krajowe mają obowiązek opublikować informacje o decyzji o sankcjach na stronie internetowej (zasada *„naming and shaming"*), w ramach którego dojdzie do ujawnienia o charakterze naruszenia, podmiot oraz rodzaj środka. Ponadto, organ krajowy jest zobowiązany do informowania ESMA/EBA o zastosowanych sankcjach (114 ust. 4 MiCA).

4.8. Budowanie wiarygodności banków w świecie ryzykownych aktywów

Budowanie wiarygodności powinno zacząć się od wprowadzenia opisanych w niniejszym opracowaniu wymogów regulacyjnych. Bank powinien **ograniczyć działania marketingowe** dotyczące kryptoaktywów do komunikatów informacyjnych oraz promocji produktów, zgodnych ze strategią ryzyka i z wymogami MiCA. Zabronione powinny być reklamy i materiały promocyjne zachęcające do spekulacyjnych inwestycji detalicznych w niestabilne kryptoaktywa. Komunikaty kierowane do klientów detalicznych muszą zawierać jasne ostrzeżenia o ryzyku i informacje o braku gwarancji zwrotu kapitału.

Aktywność banków powinna ograniczyć się do promowania bezpiecznych produktów opartych o kryptoaktywa, jak: usługi custody (przechowywanie i administrowanie kluczami/aktywami), stokenizowane depozyty lub depozyty zapisywane on-chain (jeśli konstrukcja prawna zachowuje status depozytu), rozwiązania płatnicze oparte o e-money tokens (EMT) wydawane zgodnie z MiCA. Wskazane produkty są bezpieczne oraz nie wiążą się dla klienta z ryzykiem związanym z obrotem kryptoaktywami, zwłaszcza, że ryzyko to nie tylko pochodzi ze strony banku, ale wynika z ogólnej sytuacji rynkowej. Stąd, w celu ochrony dobrego imienia banku, biorąc pod uwagę wczesny etap rozwoju rynku kryptoaktywów, to świadczenie usług prowadzenia platform obrotu (giełdy), oferowanie wymiany kryptoaktywów na waluty fiat lub prowadzenie handlu wysokowyczynnościowego należy rozważać ostrożnie ze względu na podwyższone ryzyko operacyjne, prawne i reputacyjne. Wskazana uwaga nie dotyczy jednak wymiany w zakresie tokenów, będących pieniądzem elektronicznym albo tokenów powiązanych z aktywami. Wskazane ryzyko nie bierze się z faktu, że same kryptoaktywa w świecie tradycyjnych finansów posiadają negatywną reputację, ale z faktu ich niestabilności i stawiania ewentualnych zarzutów, które nie muszą być oparte na faktach, iż np. kursy prezentowane przez bank nie w pełni oddają wartość rynkową konkretnej kryptowaluty. Taki zarzut może wystąpić w momentach załamania rynku, kiedy kursy kryptowalut są bardzo dynamiczne. Stąd podstawowe zalecenie jest takie, aby stosować te usługi, które mogą dla tradycyjnego klienta banku być przydatne, np. dzięki przyspieszeniu transakcji czy zapewnieniu bezpiecznych warunków przechowywania konkretnych kryptoaktywów w ramach usługi custody.

Bank, podejmując decyzję o zakresie działalności w sferze kryptoaktywów, powinien rozważyć płaszczyznę organizacyjnoprawną jako podstawę do dalszych działań, tzn. jakie działania na gruncie obecnie istniejącej struktury organizacyjnej banku należy podjąć, aby doszło do minimalizacji ryzyk oraz włączenia się w rynek kryptoaktywów, jako jeden z podmiotów świadczących usługi.

W przypadku świadczenia usług związanych z kryptoaktywami oraz z uwagi na ryzyka wynikające z wyżej opisanych przepisów, warto zalecić stworzenie odrębnej osoby prawnej powiązanej z bankiem, która świadczyłaby usługi z zakresu kryptoaktywów. Wskazany cel może zostać osiągnięty poprzez powołanie nowej spółki akcyjnej, w której to bank będzie 100% akcjonariuszem lub akcjonariuszem więk-

szościowym. Spółka taka może w firmie mieć nazwę banku oraz oznaczenie, że jej celem działalności jest prowadzenie usług w zakresie kryptoaktywów np. [nazwa banku CASP S.A.]. Spółka także może posiadać inną firmę.

Wskazane zalecenie w istocie prowadzi do konieczności uzyskania przez taki nowo powołany podmiot odrębnego zezwolenia CASP na prowadzone w przyszłości określonego rodzaju działalności w zakresie świadczonych usług. Przed utworzeniem spółki należy przeprowadzić: analizę prawną, ocenę kapitałową, plan compliance, plan bezpieczeństwa IT oraz scenariusze ciągłości działania. Nowy podmiot będzie podlegał obowiązkowi uzyskania zezwolenia jako CASP, w związku z czym trzeba zaplanować zasoby na spełnienie wymogów licencyjnych (są to: kapitał, governance, procedury AML/KYC, IT/security, raportowanie).

Może to być proces dłuższy niż procedura notyfikacyjna i wymagający spełnienia dodatkowych wymogów i obowiązków regulacyjnych. Takie rozdzielenie działalności jednak chroni bank w wymiarze zarówno ryzyka prawnego, technicznego, jak i reputacyjnego. To na tę ostatnią sferę warto zwrócić szczególną uwagę, gdyż bank biorąc pod uwagę zaistnienie niepożądanego problemu technicznego lub praktyki w podmiocie świadczącym usługi w zakresie kryptoaktywów, będzie mógł wskazywać na odpowiedzialność podmiotów zarządzających wskazaną spółką.

Kolejne zalecenie dotyczy stworzenia odpowiednio dostosowanych do MiCA regulaminów w zakresie świadczenia usług, AML, ochrony danych osobowych klientów oraz stworzenia skutecznych mechanizmów przestrzegania wskazanych reguł. Wskazane zalecenie sprowadza się do zbadania istniejących w danym banku polityk, regulaminów i procedur pod kątem compliance z przepisami MiCA, z zaleceniami ESMA i EBA, a także krajowych regulatorów, a następnie dostosowania ich do wymogów unijnych.

Brak przyjęcia odpowiednich polityk wewnętrznych może skutkować zarówno nałożeniem kary przez krajowy organ regulacyjny, ale także prowadzić do utraty zaufania klientów banku w przypadku zaistnienia incydentu albo innego zdarzenia niepożądanego.

Po dokonaniu powyższej analizy, bank powinien powołać odrębną jednostkę nadzorczą (funkcję compliance/AML dla krypto) odpowiedzialną za: monitoring przestrzegania MiCA i innych przepisów, raportowanie do zarządu, analizę ryzyk operacyjnych i reputacyjnych oraz współpracę z regulatorami. Jednostka ta powinna mieć bezpośrednią linię raportowania do najwyższego szczebla zarządzania.

Kolejną kwestią jest zintegrowanie systemów AML z narzędziami analizy blockchain. MiCA współdziała z rozporządzeniem TFR (Transfer of Funds Regulation), które wprowadza „Travel Rule" dla kryptoaktywów. Systemy AML powinny zostać zintegrowane z narzędziami analizy blockchain (on-chain analytics) w celu: identyfikowania adresów wysokiego ryzyka, monitorowania przepływów tokenów, generowania alertów oraz automatycznego raportowania. Bank powinien mieć możliwość, aby:

- automatycznie identyfikować adresy wysokiego ryzyka,
- monitorować transakcje i przepływy tokenów,
- spełniać wymogi Travel Rule (identyfikacja nadawcy i odbiorcy),
- generować raporty AML zgodne z MiCA+TFR.

Wskazana kwestia będzie jednym z punktów kontroli regulatorów.

Reasumując, budowanie wiarygodności w obszarze kryptoaktywów wymaga ostrożnego podejścia: selektywnego oferowania produktów, silnego nadzoru compliance, adekwatnej organizacji korporacyjnej oraz inwestycji w narzędzia AML i bezpieczeństwa. Utworzenie odrębnego podmiotu operacyjnego jest rozwiązaniem zmniejszającym ekspozycję banku-matki, ale powinno iść w parze z gruntownym planowaniem regulacyjnym i technicznym.

5. Podsumowanie, wnioski końcowe i rekomendacje

5.1. Znaczenie MiCA w perspektywie systemowej

Przeprowadzona w raporcie analiza potwierdza, że rozporządzenie MiCA stanowi jedną z najistotniejszych zmian regulacyjnych w europejskim prawie finansowym ostatnich lat, porównywalną – pod względem zakresu oddziaływania systemowego – z takimi aktami jak MiFID II, CRD/CRR czy PSD2. Jego znaczenie nie ogranicza się do wprowadzenia ram prawnych dla nowej kategorii aktywów, lecz polega na świadomym i trwałym włączeniu technologii rozproszonego rejestru (DLT) oraz rynku kryptoaktywów do architektury stabilności finansowej Unii Europejskiej. Oznacza to odejście od dotychczasowego podejścia, w którym kryptoaktywa były postrzegane jako zjawisko peryferyjne, funkcjonujące na pograniczu systemu finansowego, w kierunku uznania ich za element infrastrukturalny, wymagający objęcia mechanizmami nadzoru, kontroli ryzyka oraz ochrony uczestników rynku.

MiCA realizuje ten cel poprzez ustanowienie jednolitych standardów dotyczących emisji kryptoaktywów, świadczenia usług w tym zakresie oraz odpowiedzialności podmiotów uczestniczących w rynku, a także poprzez powiązanie tych standardów z istniejącymi reżimami regulacyjnymi prawa finansowego. W rezultacie rynek kryptoaktywów zostaje podporządkowany tym samym fundamentalnym wartościom, które od lat kształtują regulację tradycyjnych rynków finansowych, takim jak stabilność systemowa, ochrona konsumenta, integralność rynku oraz odporność operacyjna infrastruktury finansowej.

Z tego względu MiCA należy postrzegać nie jako regulację sektorową, adresowaną wyłącznie do wyspecjalizowanych podmiotów technologicznych, lecz jako akt o charakterze quasi-ustrojowym dla nowego segmentu rynku finansowego, którego funkcjonowanie ma istotne znaczenie dla całego systemu. Regulacja ta redefiniuje relacje pomiędzy innowacją technologiczną a bezpieczeństwem finansowym, przesuwając punkt ciężkości z nieformalnej samoregulacji rynku na instytucjonalny nadzór i odpowiedzialność regulacyjną.

W tym sensie MiCA oddziałuje bezpośrednio na banki, które – niezależnie od przyjętej strategii biznesowej oraz zakresu faktycznego zaangażowania w obrót kryptoaktywami – pozostają kluczowymi instytucjami systemu finansowego oraz naturalnymi adresatami oczekiwań regulatorów, nadzorców i klientów w zakresie bezpieczeństwa, przejrzystości i ochrony interesów uczestników rynku. Banki, jako podmioty o szczególnym znaczeniu systemowym, są postrzegane jako potencjalni gwaranci stabilności również w obszarach dotychczas zarezerwowanych dla podmiotów nieregulowanych lub słabiej regulowanych, co w praktyce oznacza rozszerzenie ich odpowiedzialności regulacyjnej na nowy, technologicznie złożony segment rynku finansowego.

Jednym z fundamentalnych wniosków raportu jest stwierdzenie, że MiCA świadomie przenosi istotną część ryzyk rynku kryptoaktywów na podmioty regulowane, w tym w szczególności na banki. Dotyczy to nie tylko ryzyka operacyjnego i technologicznego, lecz również ryzyka reputacyjnego, regulacyjnego oraz cywilnoprawnego.

W praktyce oznacza to, że bank, który decyduje się na świadczenie usług w zakresie kryptoaktywów nie występuje w roli neutralnego pośrednika technologicznego, lecz staje się podmiotem gwarantującym określony standard bezpieczeństwa i zgodności regulacyjnej, a w konsekwencji ponosi odpowiedzialność za skutki zdarzeń, które często mają źródło poza jego bezpośrednią kontrolą (np. zmienność rynkowa, podatności protokołów DLT, zachowania klientów). Taki model istotnie zmienia profil ryzyka działalności bankowej w porównaniu z tradycyjnymi usługami finansowymi.

5.2. Kluczowe wyzwania dla banków

Jednym z najpoważniejszych i jednocześnie najbardziej złożonych problemów zidentyfikowanych w niniejszym raporcie jest kumulacja reżimów regulacyjnych, w ramach których banki świadczące usługi w zakresie kryptoaktywów **będą zobowiązane funkcjonować. Rozporządzenie** MiCA nie ustanawia bowiem autonomicznego i wyłącznego systemu regulacyjnego dla tej działalności, lecz działa jako warstwa normatywna nakładająca się na istniejące już reżimy prawa finansowego. W szczególności MiCA nie zastępuje regulacji ostrożnościowych wynikających z CRD/CRR, nie wyłącza stosowania przepisów MiFID II ani PSD2, a jednocześnie pozostaje w ścisłej relacji z regulacjami dotyczącymi odporności cyfrowej (DORA) oraz przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT).

W praktyce oznacza to, że działalność kryptoaktywna banków będzie podlegać wielopoziomowej i skoordynowanej ocenie regulacyjnej, w której to samo

zdarzenie faktyczne może generować skutki prawne na gruncie kilku aktów prawnych jednocześnie. Przykładowo, incydent ICT związany z infrastrukturą custody może rodzić konsekwencje w zakresie obowiązków wynikających z DORA, odpowiedzialności administracyjnej na gruncie MiCA, wymogów ostrożnościowych dotyczących zarządzania ryzykiem operacyjnym oraz potencjalnej odpowiedzialności cywilnoprawnej wobec klientów. Podobnie błąd w zarządzaniu kluczami prywatnymi lub utrata dostępu do kryptoaktywów może prowadzić jednocześnie do naruszenia obowiązków informacyjnych, zasad ochrony aktywów klientów oraz standardów uczciwego i profesjonalnego działania.

Taki model regulacyjny powoduje, że zarządzanie ryzykiem regulacyjnym przestaje mieć charakter wyłącznie operacyjny lub compliance, a staje się jednym z kluczowych wyzwań strategicznych dla banków. Konieczność zapewnienia spójności działań w obszarach prawa bankowego, rynku kapitałowego, usług płatniczych, cyberbezpieczeństwa oraz AML/CFT istotnie zwiększa złożoność organizacyjną działalności kryptoaktywnej. W konsekwencji koszty compliance, wymogi dotyczące governance, systemów kontroli wewnętrznej oraz zasobów kadrowych mogą w praktyce ograniczać skalowalność oferty kryptoaktywnej, zwłaszcza w przypadku banków o mniejszym potencjale organizacyjnym i technologicznym.

Kumulacja reżimów regulacyjnych pozostaje w ścisłym związku z **podwyższonym ryzykiem reputacyjnym oraz odpowiedzialnością banków wobec klientów**. Raport jednoznacznie wskazuje, że ryzyko reputacyjne związane z działalnością kryptoaktywną banków ma charakter systemowy, a nie jedynie komunikacyjny czy wizerunkowy. Banki, jako instytucje zaufania publicznego, podlegają bowiem istotnie wyższym oczekiwaniom klientów niż podmioty technologiczne czy wyspecjalizowani dostawcy usług w zakresie kryptoaktywów. W percepcji klientów zaangażowanie banku w obrót kryptoaktywami oznacza domniemanie podwyższonego poziomu bezpieczeństwa, stabilności oraz ochrony prawnej.

MiCA wzmacnia pozycję klienta poprzez rozbudowane obowiązki informacyjne, mechanizmy odpowiedzialności za utratę kryptoaktywów oraz sformalizowane procedury skargowe i nadzorcze. W efekcie banki muszą liczyć się z istotnym wzrostem ryzyka sporów cywilnych oraz interwencji nadzorczych, zwłaszcza w sytuacjach gwałtownych wahań wartości kryptoaktywów, incydentów technologicznych lub niejasności co do charakteru oferowanych produktów i usług. Ryzyko to jest dodatkowo potęgowane przez specyfikę technologii rozproszonego rejestru, w której wiele zdarzeń ma charakter nieodwracalny, a odpowiedzialność banku może być oceniana niezależnie od faktycznego stopnia jego wpływu na przyczynę szkody.

W konsekwencji **kumulacja reżimów regulacyjnych oraz podwyższone ryzyko reputacyjne i odpowiedzialności wobec klienta** należy uznać za jedno z najpoważniejszych wyzwań stojących przed bankami rozważającymi rozwój działalności w obszarze kryptoaktywów. Wyzwanie to nie dotyczy wyłącznie zgodności formalnoprawnej, lecz wymaga całościowego, strategicznego podejścia do projektowania modeli biznesowych, struktur organizacyjnych oraz systemów zarządzania ryzykiem.

5.3. Stabilność a innowacja

Przeprowadzona w raporcie analiza prowadzi do jednoznacznego wniosku, że działalność banków w obszarze kryptoaktywów – w warunkach regulacyjnych wyznaczonych przez MiCA – wiąże się z jakościowo odmiennym profilem ryzyka niż tradycyjne formy aktywności bankowej. Kluczową rolę odgrywa tu **ryzyko reputacyjne**, które w przypadku banków ma charakter systemowy i strukturalny, a nie jedynie incydentalny czy komunikacyjny. Wynika to z faktu, że banki funkcjonują jako instytucje zaufania publicznego, a ich działalność jest oceniana nie tylko przez pryzmat zgodności formalnoprawnej, lecz również przez oczekiwania społeczne dotyczące stabilności, bezpieczeństwa i odpowiedzialności.

Zaangażowanie banków w rynek kryptoaktywów – nawet w ograniczonym zakresie – prowadzi do przeniesienia tych oczekiwań na nowy, technologicznie złożony i obarczony wysoką zmiennością segment rynku. W percepcji klientów oraz opinii publicznej obecność banku w tym obszarze oznacza **domniemanie podwyższonego poziomu bezpieczeństwa oraz instytucjonalnej kontroli ryzyk**, niezależnie od faktycznego charakteru oferowanej usługi. W rezultacie banki ponoszą reputacyjne konsekwencje zdarzeń, które w przypadku podmiotów technologicznych byłyby postrzegane jako immanentne ryzyko rynku, a nie jako przejaw nienależytego działania instytucji.

Rozporządzenie MiCA wzmacnia tę asymetrię odpowiedzialności poprzez istotne **wzmocnienie pozy-**

cji klienta w relacji z bankiem świadczącym usługi w zakresie kryptoaktywów. Regulacja ta rozszerza zakres obowiązków informacyjnych, nakładając na banki konieczność kompleksowego i zrozumiałego komunikowania nie tylko cech produktu, lecz także ryzyk technologicznych, operacyjnych i rynkowych, w tym ryzyk wynikających z samej architektury technologii rozproszonego rejestru. Jednocześnie MiCA wprowadza mechanizmy odpowiedzialności za utratę kryptoaktywów powierzonych bankowi w ramach usług przechowywania, a także formalizuje procedury skargowe i nadzorcze, które znacząco ułatwiają klientom dochodzenie roszczeń oraz inicjowanie kontroli regulacyjnych.

W praktyce prowadzi to do istotnego wzrostu ekspozycji banków na spory cywilne oraz działania nadzorcze, zwłaszcza w sytuacjach gwałtownych wahań wartości kryptoaktywów, incydentów ICT, problemów z dostępnością infrastruktury lub sporów dotyczących kwalifikacji prawnej danego produktu. Charakterystyczna dla technologii DLT nieodwracalność transakcji dodatkowo potęguje to ryzyko, ponieważ ogranicza możliwości restytucji stanu poprzedniego i sprzyja przenoszeniu odpowiedzialności na podmiot postrzegany jako najsilniejszy ekonomicznie i regulacyjnie, czyli bank.

Jednocześnie MiCA nie zamyka całkowicie przestrzeni dla **innowacyjności bankowej**, lecz radykalnie zmienia jej charakter. Innowacyjność w obszarze kryptoaktywów przestaje mieć wymiar eksperymentalny i rynkowy, a staje się innowacyjnością instytucjonalną, podporządkowaną rygorystycznym wymogom zgodności *ex ante*, rozbudowanym strukturom governance oraz wysokim standardom odporności operacyjnej. Wymaga to od banków znacznych inwestycji organizacyjnych i technologicznych, długiego okresu przygotowawczego oraz zdolności do zarządzania skumulowanymi ryzykami regulacyjnymi, operacyjnymi i reputacyjnymi.

Raport wskazuje, że w tych warunkach najbardziej perspektywiczne obszary aktywności banków to te segmenty rynku kryptoaktywów, które pozostają funkcjonalnie zbliżone do tradycyjnych ról bankowych i pozwalają na wykorzystanie istniejących kompetencji instytucjonalnych. Dotyczy to w szczególności usług przechowywania kryptoaktywów (custody), emisji i obsługi tokenów będących pieniądzem elektronicznym, infrastruktury rozliczeniowej i płatniczej opartej na technologii rozproszonego rejestru oraz tokenizacji wybranych instrumentów finansowych. W tych obszarach banki mogą pełnić rolę dostawców bezpiecznej, regulacyjnie zgodnej infrastruktury, minimalizując jednocześnie ekspozycję na ryzyka spekulacyjne.

Na poziomie strategicznym MiCA wymusza na bankach **zasadniczą zmianę podejścia do innowacji**. Kluczowe staje się nie pytanie, czy angażować się w rynek kryptoaktywów, lecz w jakim zakresie i w jakim modelu organizacyjnym powinno to nastąpić. Brak świadomej i spójnej decyzji strategicznej może w dłuższej perspektywie prowadzić do utraty kompetencji technologicznych, marginalizacji banków w obszarze rozwijającej się tokenizowanej gospodarki oraz przejęcia kluczowych funkcji infrastrukturalnych przez podmioty pozabankowe. Z drugiej strony nadmiernie ofensywne strategie, nieuwzględniające ograniczeń regulacyjnych i reputacyjnych, mogą narazić banki na nieproporcjonalne ryzyka prawne i nadzorcze.

W tym sensie MiCA działa jako **mechanizm dyscyplinujący innowacyjność bankową**, zmuszając banki do równoważenia ambicji technologicznych z podstawowymi zasadami stabilności finansowej, ochrony klienta i odpowiedzialności systemowej. Ostateczny kształt bankowej obecności na rynku kryptoaktywów będzie zatem determinowany nie przez tempo adopcji nowych technologii, lecz przez zdolność instytucjonalną do zarządzania ich konsekwencjami w ramach skumulowanego reżimu regulacyjnego.

5.4. Rekomendacje i wnioski końcowe

Przeprowadzona w raporcie analiza prowadzi do wniosku, że skuteczna i bezpieczna implementacja rozporządzenia MiCA wymaga skoordynowanych działań na kilku poziomach: po stronie banków jako instytucji systemowych, po stronie regulatorów i organów nadzoru, a także na poziomie całego ekosystemu finansowego. Rekomendacje sformułowane poniżej mają charakter komplementarny i powinny być rozpatrywane łącznie, jako element spójnej strategii adaptacji do nowego reżimu regulacyjnego.

Z perspektywy banków kluczowe znaczenie ma **wyniesienie problematyki MiCA na poziom decyzji strategicznej zarządu**. Kwestia zaangażowania w rynek kryptoaktywów nie powinna być postrzegana wyłącznie jako zagadnienie compliance ani delegowana do wyspecjalizowanych jednostek operacyjnych. MiCA oddziałuje bowiem na fundamen-

talne obszary działalności bankowej, takie jak profil ryzyka, reputacja instytucji, struktura organizacyjna, strategia technologiczna oraz relacje z klientami i nadzorem. Brak jednoznacznej decyzji strategicznej w tym zakresie może prowadzić do niespójnych działań, zwiększenia ekspozycji na ryzyka regulacyjne oraz utraty kontroli nad kierunkiem rozwoju oferty.

Jednocześnie raport rekomenduje **selektywny i etapowy model wejścia banków w obszar kryptoaktywów**. W warunkach wysokiej niepewności regulacyjnej, technologicznej i rynkowej najbardziej racjonalnym podejściem jest stopniowe angażowanie się w te segmenty rynku, które charakteryzują się relatywnie niższym profilem ryzyka i pozostają funkcjonalnie zbliżone do tradycyjnych ról bankowych. Dotyczy to w szczególności usług przechowywania kryptoaktywów (custody), emisji i obsługi tokenów będących pieniądzem elektronicznym oraz infrastruktury rozliczeniowej i płatniczej opartej na technologii rozproszonego rejestru. Taki model pozwala bankom budować kompetencje i doświadczenie w sposób kontrolowany, bez nadmiernej ekspozycji na ryzyka spekulacyjne i reputacyjne.

Niezależnie od przyjętego zakresu działalności, konieczne jest **wzmocnienie struktur governance oraz systemów ICT, w tym systemów zarządzania ryzykiem, outsourcingu i cyberbezpieczeństwa.** Specyfika kryptoaktywów oraz technologii DLT wymaga dostosowania istniejących ram organizacyjnych do nowych rodzajów ryzyk, w szczególności ryzyk operacyjnych, technologicznych i związanych z nieodwracalnością transakcji. W tym kontekście kluczowe znaczenie ma również integracja wymogów MiCA z regulacjami DORA oraz AML/CFT, tak aby zapewnić spójność podejścia do zarządzania ryzykiem na poziomie całej organizacji.

Z perspektywy regulatorów i organów nadzoru raport wskazuje na **konieczność wypracowania spójnej praktyki interpretacyjnej w zakresie stosowania MiCA wobec banków**. Szczególnego znaczenia nabiera tu jednolite podejście do art. 60 MiCA, zakresu obowiązków notyfikacyjnych oraz relacji pomiędzy MiCA a innymi reżimami regulacyjnymi. Brak jasnych i spójnych wytycznych interpretacyjnych może prowadzić do rozbieżności w praktyce nadzorczej, zwiększać niepewność prawną po stronie banków oraz hamować rozwój innowacyjnych, lecz regulacyjnie zgodnych modeli biznesowych.

Równocześnie istotne jest **unikanie nadregulacji krajowej w procesie stosowania MiCA**. Nakładanie dodatkowych, krajowych wymogów ponad standardy unijne mogłoby osłabić konkurencyjność polskiego sektora bankowego wobec podmiotów z innych jurysdykcji oraz zniechęcać banki do angażowania się w rynek kryptoaktywów w sposób formalny i przejrzysty.

Na poziomie systemowym raport podkreśla znaczenie **stałego dialogu regulacyjnego pomiędzy bankami, organami nadzoru oraz środowiskiem eksperckim**. Dynamiczny rozwój technologii DLT oraz modeli biznesowych opartych na kryptoaktywach sprawia, że wiele problemów interpretacyjnych i regulacyjnych nie może zostać rozstrzygniętych wyłącznie na poziomie legislacyjnym. Platformy dialogu i wymiany doświadczeń mogą odegrać kluczową rolę w identyfikacji ryzyk systemowych oraz wypracowywaniu dobrych praktyk rynkowych.

Warunkiem powodzenia tego procesu są również **inwestycje w rozwój kompetencji technologicznych i prawnych**, zarówno po stronie sektora bankowego, jak i administracji publicznej. Bez odpowiedniego zaplecza eksperckiego ryzyko błędnej implementacji MiCA oraz nieadekwatnej reakcji na nowe wyzwania technologiczne będzie istotnie wzrastać.

W konkluzji stwierdzić należy, że rozporządzenie MiCA stanowi trwały element europejskiego porządku regulacyjnego i w długiej perspektywie będzie w sposób zasadniczy kształtować rolę banków w ekosystemie aktywów cyfrowych. Regulacja ta nie eliminuje ryzyk związanych z kryptoaktywami, lecz porządkuje je, instytucjonalizuje i przenosi do sektora regulowanego, czyniąc banki jednymi z kluczowych gwarantów bezpieczeństwa i stabilności tego rynku.

Ostatecznie to sposób implementacji MiCA – zarówno po stronie banków, jak i regulatorów – zdecyduje o tym, czy rynek kryptoaktywów stanie się trwałym, bezpiecznym i społecznie akceptowalnym elementem europejskiego systemu finansowego. MiCA tworzy ramy prawne dla takiego rozwoju, lecz ich efektywność zależy od dojrzałości instytucjonalnej, zdolności do zarządzania ryzykiem oraz gotowości do prowadzenia odpowiedzialnej innowacji w granicach wyznaczonych przez stabilność finansową i ochronę klienta.

PROGRAM
ANALITYCZNO
BADAWCZY

Raport opracowany na zlecenie
Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości