

LIDIA MALINOWSKA*

Regulacyjne uwarunkowania zdalnego onboardingu klienta (AML)

Streszczenie

Celem artykułu jest przedstawienie założeń regulacyjnych z zakresu przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu (*anti-money laundering*; AML) dotyczących zdalnego onboardingu klienta przeprowadzanego przez podmioty działające na rynku finansowym oraz obecnie obowiązujących regulacji składających się zarówno z przepisów prawa, jak i stanowisk regulatorów, które są kluczowe z perspektywy sektora finansowego, w tym branży FinTech. W ocenie autorki artykułu regulacyjne uwarunkowania AML tworzą dla sektora FinTech szansę, ale i wyzwanie w zakresie tworzenia nowych rozwiązań technologicznych. W artykule zostały użyte metody badawcze obejmujące analizę unijnych i polskich przepisów, w tym projektowanych zmian regulacyjnych poprzez wykładnię literalną oraz celowościową, jak również analizę treści publikacji właściwych organów krajowych i unijnych dotyczących zdalnego onboardingu AML.

Słowa kluczowe: zdalny onboarding, AML, FinTech, regulacje.

JEL: K20

Regulatory Conditions for Remote Onboarding of Customers (AML)

Abstract

The purpose of this article is to present anti-money laundering (AML) regulatory objectives regarding remote customer onboarding carried out by financial market entities and current regulations consisting of both law provisions and regulators' positions, which are the key from the perspective of the financial sector, including the FinTech industry. According to the author, the regulatory environment of AML creates both an opportunity and a challenge for the FinTech sector to develop new technological solutions. Research methods used in the article involve the analysis of EU and Polish regulations, including the proposed regulatory

* mgr Lidia Malinowska – Uniwersytet Warszawski, Wydział Prawa i Administracji, Administracji, ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa, Polska. ORCID: 0000-0003-4111-7785.

changes, by literal and purposive interpretation, as well as content analysis of publications of relevant national and EU authorities regarding AML remote onboarding.

Keywords: Remote onboarding, AML, FinTech, regulations.

Wprowadzenie

Celem artykułu jest przedstawienie założeń regulacyjnych z zakresu przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu (*anti-money laundering*; AML) dotyczących zdalnego onboardingu klienta przeprowadzanego przez podmioty działające na rynku finansowym oraz obecnie obowiązujących regulacji składających się zarówno z przepisów prawa, jak i stanowisk regulatorów, które są kluczowe z perspektywy sektora FinTech.

W artykule zostały użyte metody badawcze obejmujące analizę unijnych i polskich przepisów, w tym projektowanych zmian regulacyjnych poprzez wykładnię literalną oraz celowościową, jak również analizę treści publikacji właściwych organów krajowych i unijnych dotyczących zdalnego onboardingu AML.

W poszczególnych częściach artykułu zostały omówione regulacyjne uwarunkowania zdalnego onboardingu, w tym obowiązujące ramy prawne, projektowane ramy prawne, oczekiwania regulacyjne wynikające z *soft law* o zasięgu zarówno krajowym, jak i unijnym, które razem tworzą szansę, ale i wyzwanie dla sektora FinTech w obszarze zdalnego onboardingu.

Artykuł składa się z wprowadzenia oraz rozwinięcia, w ramach którego w punkcie 1. została omówiona kwestia zdalnego onboardingu z perspektywy szansy dla sektora FinTech, która wynika w dużej mierze ze skutków pandemii COVID-19 oraz wyzwania związanego z konieczności dostosowania się do regulacyjnych oczekiwań. Kolejne punkty omawiają regulacyjne uwarunkowania, w tym obowiązujące ramy prawne zdalnego onboardingu (punkt 2) czy projektowane zmiany prawne i ich wpływ na zdalny onboarding (punkt 3). Następnie omówione zostały oczekiwania regulacyjne wynikające z *soft law*, w tym krajowe wynikające z działalności Generalnego Inspektora Informacji Finansowej (dalej GIIF) oraz Komisji Nadzoru Finansowego (dalej KNF) oraz międzynarodowe, głównie unijne, związane z działalnością European Supervisory Authorities (dalej ESA), European Banking Authority (dalej EBA), Financial Action Task Force (dalej FATF) oraz Komisji Europejskiej (dalej KE).

1. Szansa i wyzwanie dla sektora FinTech

Pandemia COVID-19 wymusiła na sektorze finansowym zintensyfikowanie działań ukierunkowanych na funkcjonowanie zdalnych modeli zawierania

umów. Sektor finansowy stanął przed wyzwaniem stworzenia lub skorzystania z dostarczanego z zewnątrz systemu zapewniającego bezpieczne oraz w pełni zgodne z wymogami i oczekiwaniami regulacyjnymi zdalne nawiązywanie relacji z nowymi klientami (tzw. zdalny onboarding).

W rezultacie wyzwanie, przed którym stanął sektor finansowy stało się jednocześnie ogromną szansą dla sektora FinTech. Jak wskazują wyniki badań przeprowadzonych przez EBA, pandemia COVID-19 i bezpośrednio związane z nią przejście na korzystanie ze zdalnych rozwiązań spowodowały szczególnie rozwój branży FinTech właśnie w zakresie zdalnego onboardingu AML (European Banking Authority, 2021, 16–18). Również Cambridge Centre for Alternative Finance, World Group Bank i World Economic Forum wskazały w swoim opracowaniu badań na temat rynku FinTech w dobie pandemii COVID-19, że okres pandemii znacząco zwiększył wykorzystanie technologii FinTech, ponieważ ułatwiają one świadczenie usług finansowych na odległość (CCAF i in., 2020, s. 8).

Pomimo sprzyjających okoliczności, które przyczyniły się do rozwoju sektora FinTech w obszarze AML, dostawcy rozwiązań technologicznych wskazują, że uwarunkowania prawne są jednym z największych wyzwań, które ograniczają szersze wykorzystanie ich produktów na rynku finansowym. Jako bariery rozwojowe są postrzegane w szczególności złożone i stale ewoluujące ramy krajowych i międzynarodowych regulacji oraz brak zharmonizowanych wymogów regulacyjnych (CCAF i in., 2020, s. 35–36).

W kontekście wskazanych barier, jeżeli chodzi o polski rynek finansowy, należy uznać, że obowiązujące ramy prawne – tak krajowe, jak i europejskie – mają charakter stosunkowo elastyczny i są oparte na koncepcji neutralności technologicznej, dzięki czemu zdalny onboarding może stanowić istotny obszar rozwoju dla sektora FinTech. Jednocześnie praktycznym utrudnieniem dla sektora FinTech jest *soft law*, wynikające z o wiele bardziej precyzyjnych niż przepisy prawa stanowisk krajowych oraz międzynarodowych organów regulacyjnych. W szczególności lokalne oczekiwania regulacyjne nie są zharmonizowane, co stanowi utrudnienie dla sektora FinTech w kontekście opracowywania uniwersalnych modeli zdalnego onboardingu.

Również w publikacjach branżowych wskazuje się na trudności wynikające z braku ujednoczonego podejścia i wspólnych ram prawnych w zakresie zdalnej weryfikacji tożsamości, co doprowadziło do tego, że w poszczególnych krajach pojawiają się różne inicjatywy, które mają pewne wspólne elementy, ale także liczne różnice. W konsekwencji, mimo że technologie zdalnej weryfikacji tożsamości stają się coraz bardziej popularne, to m.in. ujednoczenie ustawodawstwa w poszczególnych krajach może przyczynić się do wzmocnienia i przyspieszenia rozwoju zsynchronizowanych i bezpiecznych rozwiązań w zakresie zdalnej weryfikacji tożsamości (Laas-Mikko i in., 2022, s. 445–446).

Badania dotyczące wpływu pandemii Covid-19 na rynek FinTech również wskazują na konkretne działania regulacyjne, które firmy FinTech uważają za niezbędne dla swojego rozwoju w obszarze zdalnego onboardingu AML, tj. elektroniczny proces identyfikacji i weryfikacji klienta (e-KYC) czy uproszczone zasady stosowania środków bezpieczeństwa finansowego wobec klienta (CCAF i in., 2020, s. 8).

Już w 2020 r. na potrzebę harmonizacji przepisów AML z zakresu zdalnego onboardingu zwróciła uwagę KE, wskazując w komunikacie w sprawie planu działania na rzecz kompleksowej unijnej polityki zapobiegania praniu pieniędzy i finansowaniu terroryzmu na konieczność ułatwienia korzystania z identyfikacji cyfrowej¹. Natomiast w komunikacie w sprawie strategii dla Unii Europejskiej (UE) w zakresie finansów cyfrowych KE wskazała, że do 2024 r. UE powinna wdrożyć solidne i zharmonizowane ramy prawne umożliwiające stosowanie interoperacyjnych rozwiązań w zakresie tożsamości cyfrowej, które pozwolą nowym klientom na szybki i łatwy dostęp do usług finansowych w ramach zdalnego onboardingu².

Zmiana uwarunkowań i będąca jej konsekwencją popularyzacja systemów zdalnego nawiązywania relacji gospodarczych spowodowały, że zdalny onboarding jest obecnie przedmiotem nowych wytycznych EBA wydanych 22 listopada 2022 r. (2022) oraz unijnego pakietu AML³, które mogą znacząco wpłynąć na oczekiwania sektora finansowego co do rozwiązań technologicznych wykorzystywanych przy zdalnym zawieraniu umów.

2. Regulacyjne uwarunkowania zdalnego onboardingu – obowiązujące ramy prawne

W polskim sektorze finansowym stanowiącym element unijnego systemu podstawowe ramy prawne dla zdalnego onboardingu, które są również istotne z perspektywy dostawców rozwiązań FinTech, tworzą obecnie dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu,

¹ Komunikat w sprawie planu działania na rzecz kompleksowej unijnej polityki zapobiegania praniu pieniędzy i finansowaniu terroryzmu, 2020/C 164/06, 13 maja 2020 r., s. 5. Pozyskano z <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0513%2803%29> (pobrano: 29.03.2022).

² Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii dla UE w zakresie finansów cyfrowych, COM(2020) 591, 24 września 2020 r., s. 6. Pozyskano z [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2020\)591&lang=pl](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)591&lang=pl) (pobrano: 29.03.2022).

³ Rozporządzenie Parlamentu Europejskiego i Rady w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy lub finansowania terroryzmu, Wniosek COM/2021/420 final (20.07.2021) (EU).

zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE zmieniona dyrektywą Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniającą dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (dalej AMLD IV) oraz implementowana w ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu zmienionej ustawą z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (dalej ustawa AML).

AMLD IV i ustawa AML zawierają wyłącznie ogólne przepisy określające obowiązki związane z nawiązywaniem stosunków gospodarczych z nowymi klientami, które mają zastosowanie zarówno w przypadku fizycznej obecności klienta, jak i przy wykorzystaniu zdalnych metod. W ramach ogólnych wymogów związanych z nawiązywaniem stosunków gospodarczych, podmioty sektora finansowego rozpoznają i oceniają poziom ryzyka prania pieniędzy oraz finansowania terroryzmu, związanego z danym stosunkiem gospodarczym, z klientem, w tym m.in. poprzez określenie czy klient bądź jego beneficjent rzeczywisty mają status osoby zajmującej eksponowane stanowisko polityczne lub związek z państwem trzecim wysokiego ryzyka (art. 33 ust. 2 ustawy AML) oraz czy stosują środki bezpieczeństwa finansowego, takie jak: identyfikacja klienta oraz weryfikacja jego tożsamości, identyfikacja osoby upoważnionej do działania w imieniu klienta oraz weryfikacja jej tożsamości i umocowania do działania w imieniu klienta, identyfikacja beneficjenta rzeczywistego i podejmowanie uzasadnionych czynności w celu weryfikacji jego tożsamości oraz ustalenia struktury własności i kontroli, ocena stosunków gospodarczych, a także – stosownie do sytuacji – uzyskanie informacji na temat ich celu i zamierzonego charakteru (art. 35 ust. 1 pkt 1 w zw. z art. 34 ust. 1 ustawy AML).

Chociaż przepisy z zakresu AML nie przewidują odrębnej procedury zdalnego nawiązywania stosunków gospodarczych, to zdalny onboarding został bezpośrednio wskazany w przepisach dotyczących wzmoczonych środków bezpieczeństwa finansowego. Zgodnie z art. 43 ust. 2 pkt 7 ustawy AML nawiązywanie stosunków gospodarczych bez fizycznej obecności klienta może świadczyć o wyższym ryzyku prania pieniędzy oraz finansowania terroryzmu (art. 43 ust. 2 pkt 7 ustawy AML). Regulacja ta nie ma jednak charakteru bezwzględnie, ponieważ wyższe ryzyko prania pieniędzy oraz finansowania terroryzmu występuje w przypadku zdalnych relacji, o ile nie zostało ono ograniczone, w tym przez użycie środków identyfikacji elektronicznej oraz usług zaufania umożliwiających identyfikację elektroniczną w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającą dyrektywę 1999/93/WE (dalej rozporzą-

dzenie eIDAS). W konsekwencji sam fakt wystąpienia zdalnego onboardingu nie powoduje automatycznie przypisania relacji gospodarczej wyższego ryzyka i konieczności zastosowania wzmożonych środków bezpieczeństwa finansowego.

W ramach zdalnego onboardingu zastosowanie mają zatem te same przepisy, które podmioty finansowe stosują również podczas nawiązywania stosunków gospodarczych przy jednoczesnej fizycznej obecności dwóch stron. Niemniej w praktyce, pomimo zastosowania tych samych ram prawnych, zdalne modele różnią się od klasycznych trybów nawiązywania stosunków gospodarczych. Co więcej, specyfika przepisów AML kreuje również dużą elastyczność w zakresie tworzenia i funkcjonowania zdalnych modeli, dlatego mogą się one opierać na różnorodnych rozwiązaniach technologicznych.

Odwołując się bezpośrednio do przepisów, które gwarantują elastyczność procedur onboardingowych, należy wskazać na obowiązek stosowania środków bezpieczeństwa finansowego, obejmujący m.in. KYC (*know your customer*), czyli procedurę identyfikacji oraz weryfikacji (art. 35 ust. 1 pkt 1, art. 36, art. 37 ustawy AML).

W zakresie identyfikacji przepisy precyzyjnie wskazują zakres danych, które muszą być pozyskane przez podmiot sektora finansowego, jednocześnie zupełnie nie regulując metod ich pozyskiwania (art. 36 ustawy AML). W konsekwencji, w przypadku zdalnego onboardingu może to nastąpić np. mailowo bądź poprzez wypełnienie danych na stronie internetowej.

Natomiast w ramach weryfikacji mającej charakter następczy i polegającej na potwierdzeniu ustalonych danych identyfikacyjnych, podmiot sektora finansowego może wykorzystać jako materiał weryfikacyjny dokument stwierdzający tożsamość osoby fizycznej, dokument zawierający aktualne dane z wyciągu z właściwego rejestru lub inny dokument, dane lub informacje pochodzące z wiarygodnego i niezależnego źródła w tym, o ile są dostępne, środki identyfikacji elektronicznej lub odpowiednie usługi zaufania określone w rozporządzeniu eIDAS (art. 37 ust. 1 ustawy AML). Doprecyzowujące odwołanie do środków identyfikacji elektronicznej oraz odpowiednich usług zaufania zostało dodane w 2021 r. w ramach nowelizacji ustawy AML⁴ i ma szczególne znaczenie w kontekście modeli zdalnego onboardingu. Ze względu na możliwość zastosowania jako materiału weryfikacyjnego każdego dokumentu, danych lub informacji pochodzących z wiarygodnego i niezależnego źródła, katalog materiałów weryfikacyjnych ma charakter otwarty. Natomiast użycie spójnika „lub” w kontekście zasad logiki oraz wykładni literalnej pozwala m.in. na stwierdzenie, że wystarczający jest jeden materiał weryfikacyjny, a w przypadku osób fizycznych dokument stwierdzający tożsamość nie jest obligatoryjnym materiałem weryfikacyjnym. W rezultacie należy uznać, że proces dokonywania weryfikacji

⁴ Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. poz. 815 z późn. zm.).

w zakresie doboru materiałów jest odformalizowany i pozwala na stosunkowo dużą dowolność w ramach kształtowania modelu onboardingowego.

Opisana powyżej elastyczność weryfikacji jest również odzwierciedleniem wynikającej z przepisów AML zasady *risk based approach*, która pozwala na stosowanie środków bezpieczeństwa finansowego w zakresie i z intensywnością uwzględniającą rozpoznane ryzyko prania pieniędzy oraz finansowania terroryzmu (art. 33 ust. 3 ustawy AML). Przyjmuje się, że zasada ta nie ma zastosowania do identyfikacji, ponieważ ustawa AML wskazuje minimalny katalog danych, których pozyskanie ma charakter obligatoryjny. Ma ona natomiast szczególne znaczenie w procesie weryfikacji, ponieważ umożliwia dobór materiałów weryfikacyjnych oraz zakres danych podlegających weryfikacji w zależności od rozpoznanego ryzyka prania pieniędzy oraz finansowania terroryzmu.

3. Regulacyjne uwarunkowania – projektowane zmiany prawne i ich wpływ na zdalny onboarding

Natomiast w kontekście procedowanych obecnie zmian prawnych oraz zdalnego onboardingu należy zwrócić uwagę na projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy lub finansowania terroryzmu, 2021/0239. Projekt dotyczy m.in. zasad stosowania środków bezpieczeństwa finansowego wobec klienta w przypadkach zdalnego onboardingu, które są spójne z proponowaną przez KE zmianą rozporządzenia eIDAS w odniesieniu do ram europejskiej tożsamości cyfrowej, w tym europejskich portfeli tożsamości cyfrowej i odpowiednich usług zaufania. W projektowanych rozporządzeniu AML zawarta jest również kompetencja do wydania regulacyjnych standardów technicznych, które mają umożliwić uczestnikom rynku finansowego opracowanie bezpiecznych, dostępnych i innowacyjnych środków weryfikacji tożsamości klientów i przeprowadzania analizy klienta, również zdalnie, przy jednoczesnym poszanowaniu zasady neutralności technologicznej. Ponadto w kontekście omówionych powyżej, obecnie obowiązujących, regulacji dotyczących zasad weryfikacji danych, należy wskazać na projektowany art. 18 ust. 4 rozporządzenia AML, który posługuje się koniunkcją i w konsekwencji przewiduje konieczność stosowania co najmniej dwóch materiałów weryfikacyjnych, w tym dokumentu tożsamości, paszportu lub jego odpowiednika. Wykładnia literalna tego przepisu pozwala jednak jednocześnie na przyjęcie, że wykorzystanie do weryfikacji tożsamości środków identyfikacji elektronicznej i odpowiednich usług zaufania z rozporządzenia eIDAS zastępuje weryfikację w oparciu o dokument tożsamości, paszport lub jego odpowiednik oraz informacje z wiarygodnych i niezależnych źródeł, do których dostęp uzyskano bezpośrednio lub które zostały dostarczone przez klienta.

4. Oczekiwania regulacyjne wynikające z *soft law*

Pomimo stosunkowo elastycznych ram prawnych, problematyczne z perspektywy tworzenia onboardingowych rozwiązań technologicznych jest w praktyce sprostanie bardziej precyzyjnym oczekiwaniom regulacyjnym wynikającym z *soft law*.

4.1. Krajowe oczekiwania regulacyjne

Z perspektywy polskiego sektora finansowego szczególnie istotne są wytyczne i komunikat GIIF⁵ oraz stanowiska Urzędu KNF (dalej UKNF)⁶. Chociaż nie mają one charakteru bezwzględnie wiążącego, tak jak przepisy prawa, to mając na uwadze, że podmioty sektora finansowego podlegają nadzorowi, to w praktyce zapewniają zgodność swojej działalności również z *soft law*, traktując je na równi z powszechnie obowiązującym prawem.

Zarówno GIIF, jak i UKNF podkreślają, że w zakresie weryfikowania tożsamości klienta bez jego fizycznej obecności instrumentami najbardziej bezpiecznymi w zastosowaniu są środki identyfikacji elektronicznej, o których mowa w rozporządzeniu eIDAS, w tym w szczególności kwalifikowany podpis elektroniczny. Podejście to jest spójne z założeniami ustawodawcy, który bezpośrednio w art. 43 ustawy AML wskazał na ograniczanie ryzyka prania pieniędzy i finansowania terroryzmu poprzez zastosowanie środków identyfikacji elektronicznej oraz usług zaufania umożliwiających identyfikację elektroniczną w rozumieniu rozporządzenia eIDAS oraz doprecyzował w ostatniej nowelizacji ustawy AML katalog materiałów weryfikacyjnych zawarty w art. 37 ust. 1 ustawy AML wska-

⁵ Wytyczne z dnia 22 sierpnia 2018 r. w sprawie identyfikacji klienta instytucji obowiązanej i weryfikacji jego tożsamości w sytuacji braku jego fizycznej obecności. Pozyskano z: https://mf-arch2.mf.gov.pl/web/bip/ministerstwo-finansow/dzialalnosc/giif/komunikaty/-/asset_publisher/8KnM/content/id/6480692 (20 marca. 2022); Komunikat nr 4 z dnia 18 kwietnia 2019 r. w sprawie korekty komunikatu Generalnego Inspektora Informacji Finansowej z dnia 22 sierpnia 2018 r. w sprawie identyfikacji klienta instytucji obowiązanej i weryfikacji jego tożsamości. Pozyskano z: <https://www.gov.pl/web/finanse/komunikat-nr-4-w-sprawie-korekty-komunikatu-generalnego-inspektora-informacji-finansowej-z-dnia-22-sierpnia-2018-r-w-sprawie-identyfikacji-klienta-instytucji-obowiazanej-i-weryfikacji-jego-tozsamosci> (pobrano: 20.03.2022).

⁶ Stanowisko z dnia 5 czerwca 2019 r. dotyczące identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji. Pozyskano z: https://www.knf.gov.pl/knf/pl/komponenty/img/Stowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf (pobrano: 29.03.2022); Stanowisko z dnia 3 marca 2022 r. dotyczące identyfikacji klienta instytucjonalnego1 i weryfikacji jego tożsamości w sektorze finansowym podlegającym nadzorowi Komisji Nadzoru Finansowego w oparciu o metodę wideoweryfikacji. Pozyskano z: https://www.knf.gov.pl/knf/pl/komponenty/img/Stowisko_UKNF_dot_wideoweryfikacji_klientow_instytucjonalnych.pdf (pobrano: 29.03.2022).

zując wprost na środki identyfikacji elektronicznej i odpowiednie usługi zaufania określone w rozporządzeniu eIDAS.

Zasadniczo zarówno UKNF, jak i GIIF bezpośrednio odwołują się do stosowania zasady *risk based approach* w ramach przeprowadzenia zdalnego onboardingu klienta. Jednocześnie zgodnie z oczekiwaniami GIIF oraz UKNF podmioty sektora finansowego, przeprowadzając zdalny onboarding, powinny stosować co najmniej dwa materiały weryfikacyjne, w tym w przypadku osób fizycznych dowód tożsamości⁷, co stoi w sprzeczności z literalnym brzmieniem art. 37 ust. 1 ustawy AML oraz wyklucza zastosowanie zasady *risk based approach* w tym zakresie. Natomiast drugie stanowisko UKNF z dnia 3 marca 2022 r. wskazuje, że podmiot nadzorowany powinien rozważyć posłużenie się różnymi materiałami weryfikacyjnymi pochodzącymi z wiarygodnych i niezależnych źródeł, co teoretycznie mogłoby wskazywać na uelastycznienie tej kwestii. Jednak we fragmencie dotyczącym materiałów weryfikacyjnych dotyczących osób prawnych została użyta koniunkcja, co zgodnie z zasadami logiki i wykładnią literalną wskazuje na konieczność użycia co najmniej dwóch materiałów weryfikacyjnych. Ponadto w drugim stanowisku wprost zostało wskazane, że poprzednie stanowisko pozostaje nadal utrzymane, w tym w zakresie materiałów weryfikacyjnych. Dodatkowo GIIF wskazuje na konieczność doboru materiałów umożliwiających dokonanie dokładnej weryfikacji tożsamości. Sformułowanie odwołujące do dokładnej weryfikacji może oznaczać, że zdaniem GIIF istnieje konieczność weryfikacji wszystkich danych zebranych w ramach identyfikacji, co również wykluczałoby zastosowanie zasady *risk based approach* co do zakresu weryfikowanych danych. Mając na uwadze złożony katalog danych podlegających identyfikacji w przypadku osoby fizycznej należy wskazać, że w ramach dokładnej weryfikacji⁸ w praktyce nie jest możliwe skorzystanie wyłącznie z jednego materiału weryfikacyjnego. Przykładowo adres jest daną, która nie występuje obecnie wśród danych zawartych w dowodzie tożsamości, dlatego UKNF wskazał, że rachunki za media mogą stanowić materiał umożliwiający weryfikację tej informacji.

Ponadto organy stoją na stanowisku, że istnieje konieczność minimalizowania ryzyka związanego z wprowadzeniem w błąd co do prawdziwości materiałów weryfikacyjnych, np. poprzez zastosowanie dodatkowego środka w postaci przelewu weryfikacyjnego z rachunku klienta (prowadzonego w innej instytucji) na rzecz podmiotu przeprowadzającego weryfikację. Jednocześnie GIIF oraz UKNF ze względu na minimalny zakres danych osobowych zawartych w informacji o przelewie jednoznacznie wskazują na subsydiarny charakter przelewu jako materiału weryfikacyjnego.

⁷ Przy czym wymaga podkreślenia, że prawo jazdy według UKNF może stanowić wyłącznie dodatkowy materiał weryfikacyjny, ponieważ nie stanowi oficjalnego dokumentu tożsamości.

⁸ Wytyczne z dnia 22 sierpnia 2018 r., op. cit.

W konsekwencji należy stwierdzić, że stanowiska regulatorów ograniczają zastosowanie zasady *risk based approach* zarówno co do doboru materiałów weryfikacyjnych, jak i zakresu danych identyfikacyjnych, które podlegają weryfikacji, przez co znacząco wpływają na konstruowanie modelowych rozwiązań technologicznych służących do zawierania umów z klientami bez fizycznej obecności. Ma to szczególnie negatywny wpływ na tworzenie rozwiązań onboardingowych uwzględniających aspekty biznesowe ściśle powiązane z równie istotnymi doświadczeniami użytkowników (*user experience*).

Poza ogólnymi odniesieniami do zdalnego onboardingu stanowiska UKNF zawierają głównie omówienie wytycznych dotyczących wideoweryfikacji, które powinny zostać uwzględnione w zdalnych rozwiązaniach opartych na takim modelu weryfikacji. Wideoweryfikacja ma szczególne znaczenie, ponieważ jest jedynym modelem zdalnego zawierania relacji, który najbardziej odwzorowuje tradycyjną, fizyczną obecność stron i umożliwia dokonanie oceny behawioralnej klienta, co nie jest możliwe w przypadku korzystania z pozostałych rozwiązań technologicznych. Zasadniczo jednak liczne wytyczne UKNF mają charakter uniwersalny, dlatego ze względów ostrożnościowych powinny być uwzględniane też w zdalnych modelach, które nie zawierają elementu wideoweryfikacji.

4.2. Międzynarodowe oczekiwania regulacyjne

Kwestia zdalnego onboardingu stanowiła dotychczas również przedmiot rozważań i działań na poziomie międzynarodowym, głównie w obrębie Unii Europejskiej, tj. ESA⁹, EBA¹⁰, FATF¹¹ oraz KE¹².

⁹ Opinia z dnia 23 stycznia 2018 r. w sprawie stosowania innowacyjnych rozwiązań przez instytucje kredytowe i finansowe w procesie należytej staranności wobec klienta, JC 2017 81. Pozyskano z: [https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20\(JC-2017-81\).pdf](https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf) (pobrano: 29.03.2022).

¹⁰ Dokument konsultacyjny, projekt wytycznych dotyczących korzystania z rozwiązań do zdalnego przyjmowania klientów na podstawie art. 13 ust. 1 dyrektywy (UE) 2015/849, EBA/CP/2021/40, 10 grudnia 2021 r. Pozyskano z: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2022/Consultation%20on%20draft%20Guidelines%20on%20the%20use%20of%20remote%20customer%20onboarding%20solutions/1025218/CP%20on%20draft%20GLs%20on%20remote%20customer%20onboarding.pdf (pobrano: 29.03.2022).

¹¹ Wytyczne dotyczące identyfikacji cyfrowej, marzec 2020 r. Pozyskano z: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf> (29 marca 2022); *Możliwości i wyzwania związane z nowymi technologiami dla AML/CTF*, lipiec 2021 r. Pozyskano z: <https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf> (pobrano: 29.03.2022).

¹² Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions. <https://www.google>.

Z perspektywy sektora FinTech istotne są stanowiska europejskie szczegółowo poruszające tematykę rozwiązań technologicznych, które mogą być wykorzystywane w ramach realizacji obowiązków AML przez podmioty finansowe działające na terenie UE. W tym zakresie należy zwrócić uwagę na raport KE¹³, który zawiera opis różnych istniejących modeli zdalnego onboardingu wraz z ich oceną co do zagrożeń oraz sposobów ich ograniczania, a także odnosi się do perspektywy interoperacyjności i ogólnej funkcjonalności. Raport KE wskazuje na bardzo szczegółowe aspekty, m.in. w jaki sposób należy weryfikować dokument tożsamości zarówno w sposób techniczny (np. okazywanie pod wieloma kątami, ocena hologramu), jak i poprzez walidację w odpowiednich bazach danych. Dodatkowo KE zwraca uwagę chociażby na konieczność przeprowadzenia testu żywotności (*proof of liveness*), np. poprzez wymóg poruszania przez klienta głową od lewej do prawej podczas nagrywania wideo selfie oraz zmianę wyrazu twarzy, co ma zapewnić, że osoba, z którą nawiązywana jest relacja jest żywa i w konsekwencji ograniczyć ryzyko spoofingu polegającego na wykorzystaniu zdjęcia, filmu, maski lub innego substytutu twarzy klienta. Natomiast w zakresie standardów technologicznych KE wskazuje na konieczność korzystania z rozwiązań posiadających uznane standardy rynkowe (np. ISO). Również FATF opublikował w 2021 r. specjalne opracowanie na temat szans i wyzwań związanych z nowymi technologiami w obszarze AML¹⁴, które ma na celu podniesienie świadomości o istotnych postępach w zakresie innowacji konkretnych rozwiązań oraz zawiera ocenę utrzymujących się wyzwań i przeszkód w ich wdrażaniu. Zdaniem FATF wiele wyzwań wynika z istniejących ograniczeń regulacyjnych, takich jak dotychczasowe systemy zgodności z przepisami AML oraz tradycyjne ramy regulacyjne i mechanizmy nadzoru. Z przeprowadzonych przez FATF badań wynika również, że zauważalna jest na rynku potrzeba wyraźnego wsparcia ze strony właściwych organów krajowych, co zwiększyłyby zainteresowanie, liczbę inwestycji i zaufanie do nowych technologii.

Wydaje się, że obecnie najistotniejsze znaczenie w UE w zakresie zdalnego onboardingu zarówno dla podmiotów sektora finansowego, jak i dla branży

com/url?sa=t&rc=tj&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiyw9OExK37AhVCmosKHWkxB0YQFnoECBMQAQ&url=https%3A%2F%2Fec.europa.eu%2Finfo%2Fsites%2Fdefault%2Ffiles%2Fbusiness_economy_euro%2Fbanking_and_finance%2Fdocuments%2Freport-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf&usg=AOvVaw2JOVSsKzd2U4h02_ptuWJ.

¹³ Ibidem.

¹⁴ Opportunities and Challenges of New Technologies for AML/CFT. Pozyskano z: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.html> (pobrano: 29.03.2022).

FinTech, mają opublikowane przez EBA (2022) wytyczne¹⁵. Działania EBA w tym zakresie są odpowiedzią na wniosek KE realizującej założenia strategii dla UE w zakresie finansów cyfrowych. Zdaniem KE przepisy dotyczące środków bezpieczeństwa finansowego zawarte w AMLD IV nie zapewniają wystarczającej jasności i zbieżności w zakresie tego co jest, a co nie jest dozwolone w kontekście zdalnym i cyfrowym, czego rezultatem są rozbieżne w skali europejskiej oczekiwania organów nadzoru oraz działania podejmowane przez podmioty sektora finansowego w celu zapewnienia zgodności. EBA w swoich pracach potwierdza, że państwa członkowskie mają różne poglądy na temat tego, co jest dopuszczalne w odniesieniu do zdalnego onboardingu klientów, a rozbieżności te mogą stanowić przeszkodę we wspieraniu innowacji. EBA zauważa również, że rośnie niezawodność rozwiązań technologicznych służących do identyfikacji i weryfikacji czy klient jest osobą, za którą się podaje, aczkolwiek podkreśla też potrzebę zapewnienia, aby podmioty sektora finansowego wprowadziły zabezpieczenia ograniczające ryzyko prania pieniędzy oraz finansowania terroryzmu oraz ryzyko oszustw polegających na podszywaniu się pod inne osoby. W konsekwencji wytyczne EBA mają na celu określenie wspólnych standardów UE w zakresie opracowywania i wdrażania solidnych, uwzględniających ryzyko procesów stosowania środków bezpieczeństwa finansowego w kontekście zdalnego onboardingu. Wytyczne określają kroki, jakie podmioty sektora finansowego powinny podjąć przy wyborze narzędzi do zdalnego przyjmowania klientów, a także czynności, jakie powinny podjąć, aby upewnić się, że wybrane narzędzie jest odpowiednie i rzetelne w ramach bieżącego stosowania oraz że pozwala im skutecznie wypełniać ich wstępne obowiązki w zakresie środków bezpieczeństwa finansowego. Wytyczne wprost wskazują, że wybór indywidualnych rozwiązań technologicznych należy do podmiotów sektora finansowego, w zakresie dozwolonym przez prawo krajowe.

Podsumowanie

Podsumowując, szeroko rozumiane regulacyjne uwarunkowania zdalnego onboardingu obejmujące zarówno obowiązujące regulacje prawne, jak i regulacyjne stanowiska organów przybierające m.in. formy stanowisk, wytycznych (*soft law*), stanowią ramy działalności podmiotów sektora finansowego, które

¹⁵ PaperFinal Report. Draft Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849. (EBA/GLCP/20221/1540). Pozyskano z: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-15%20GL%20on%20remote%20customer%20onboarding/1043884/Guidelines%20on%20the%20use%20of%20Remote%20Customer%20Onboarding%20Solutions.pdf (pobrano: 29.03.2022).

jednocześnie determinują tworzenie rozwiązań technologicznych przez sektor FinTech. Chociaż z przeprowadzonych i omówionych w artykule badań wynika, że regulacyjne wymogi uznawane są za wyzwanie, a wręcz przeszkodę w tworzeniu modeli onboardingowych bądź ich elementów, to należy podkreślić, że jednocześnie dzięki swojej elastyczności i oparciu na zasadzie neutralności technologicznej umożliwiają branży FinTech skorzystanie z szansy na zaspokojenie zapotrzebowania podmiotów finansowych w tym obszarze. Zapotrzebowanie obejmuje nie tylko implementację, lecz także bieżące korzystanie z rozwiązań onboardingowych, które w związku z ciągle ewoluującymi ramami regulacyjnymi, postępem technologicznym oraz zmieniającą się rzeczywistością nie mogą zostać zaspokojone jednorazowo, co gwarantuje sektorowi FinTech długofalową możliwość korzystania z szans występujących w obszarze AML.

Bibliografia

- CCAF, World Bank & World Economic Forum. (2020). *The Global Covid-19 FinTech Market Rapid Assessment Report*. University of Cambridge; World Bank Group and the World Economic Forum.
- Departament Informacji Finansowej. (2018, 22 sierpnia). *Wytyczne Generalnego Inspektora Informacji Finansowej w sprawie identyfikacji klienta instytucji obowiązanej i weryfikacji jego tożsamości w sytuacji braku jego fizycznej obecności*. Archiwalna strona MF.gov.pl. https://mf-arch2.mf.gov.pl/web/bip/ministerstwo-finansow/dzialalnosc/giif/komunikaty/-/asset_publisher/8KnM/content/id/6480692.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE, L 141/73 (05.06.2015) (UE). <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32015L0849>.
- European Banking Authority. (2018). *Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process*. (JC 2017 81). https://www.eba.europa.eu/sites/default/documents/files/document_library/930583/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20%28JC-2017-81%29.pdf.
- European Banking Authority. (2022). *Final Report. Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849*. (EBA/GL/2022/15). https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-15%20GL%20on%20remote%20customer%20onboarding/1043884/Guidelines%20on%20the%20use%20of%20Remote%20Customer%20Onboarding%20Solutions.pdf.
- European Banking Authority. (2021b). *EBA Analysis of Regtech in the EU financial sector*. (EBA/REP/2021/17). <https://www.eba.europa.eu/sites/default/documents/>

- files/document_Slibrary/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf.
- FATF. (2020). *Guidance on Digital Identity*. www.fatf-gafi.org/publications/documents/digital-identity-guidance.html.
- FATF. (2021). *Opportunities and Challenges of New Technologies for AML/CFT*. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.html>.
- GIIF. (2019, 18 kwietnia). *Komunikat nr 4 w sprawie korekty komunikatu Generalnego Inspektora Informacji Finansowej z dnia 22 sierpnia 2018 r. w sprawie identyfikacji klienta instytucji obowiązanej i weryfikacji jego tożsamości*. Gov.pl. <https://www.gov.pl/web/finanse/komunikat-nr-4-w-sprawie-korekty-komunikatu-generalnego-inspektora-informacji-finansowej-z-dnia-22-sierpnia-2018-r-w-sprawie-identyfikacji-klienta-instytucji-obowiazanej-i-weryfikacji-jego-tozsamosci>.
- Laas-Mikko, K., Kalvet, T., Derevski, R. & Tiits, M. (2022). Promises, Social, and Ethical Challenges with Biometrics in Remote Identity Onboarding. W C. Rathgeb, R. Tolosana, R. Vera-Rodriguez & C. Busch (red.), *Handbook of Digital Face Manipulation and Detection From Deep Fakes to Morphing Attacks* (s. 437–463). Springer.
- Komisja Europejska. (2019). *Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions*. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiyw9OExK37AhVCmosKHwKxB0YQFnoECBMQAQ&url=https%3A%2F%2Fec.europa.eu%2Finfo%2Fsites%2Fdefault%2Ffiles%2Fbusiness_economy_euro%2Fbanking_and_finance%2Fdocuments%2Freport-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf&usq=AOvVaw2JOVSsKzdz2U4h02_ptuWJ.
- Komisja Europejska. (2020a). *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii dla UE w zakresie finansów cyfrowych*, COM(2020)591 (24/09/2020) [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2020\)591&lang=pl](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)591&lang=pl).
- Komisja Europejska. (2020b). *Komunikat w sprawie planu działania na rzecz kompleksowej unijnej polityki zapobiegania praniu pieniędzy i finansowaniu terroryzmu* (2020/C 164/06), C 164/21 (13.05.2020). [https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020XC0513\(03\)](https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020XC0513(03)).
- Rozporządzenie Parlamentu Europejskiego i Rady w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy lub finansowania terroryzmu, Wniosek COM/2021/420 final (20.07.2021) (EU). <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52021PC0420>.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, Rozporządzenie L 257/73 (28.8.2014) (UE). <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32014R0910>.
- UKNF, (2019). *Stanowisko UKNF dotyczące identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji*. https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf.

UKNF. (2022). *Stanowisko Urzędu Komisji Nadzoru Finansowego dotyczące identyfikacji klienta instytucjonalnego i weryfikacji jego tożsamości w sektorze finansowym podlegającym nadzorowi Komisji Nadzoru Finansowego w oparciu o metodę wideoweryfikacji*. https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_wideoweryfikacji_klientow_instytucjonalnych.pdf.

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. 2018 poz. 723. <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000723>.

Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw, Dz.U. 2021 poz. 815. <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210000815>.