**Wskazówki dla podmiotów ubiegających się o zezwolenie na świadczenie usług płatniczych   
w charakterze krajowej instytucji płatniczej w zakresie opracowania wewnętrznej regulacji przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu na potrzeby dokumentacji składanej wraz z wnioskiem o takie zezwolenie**

Stosownie do art. 61 ust. 1 pkt 6 ustawy z dnia 19 sierpnia 2011 r. *o usługach płatniczych* (j.t. Dz. U. z 2024 r. poz. 30.; dalej: u.u.p.), jednym z elementów wniosku podmiotów ubiegających się   
o zezwolenie Komisji Nadzoru Finansowego (KNF) na świadczenie usług płatniczych w charakterze krajowej instytucji płatniczej (KIP) jest **opis systemu zarządzania ryzykiem i kontroli wewnętrznej**, o którym mowa w art. 64 ust. 1 pkt 3 u.u.p., w tym zatwierdzone regulacje wewnętrzne w tym zakresie. Zgodnie z art. 64 ust. 1 pkt 3 u.u.p. zezwolenie może być udzielone, jeżeli dany podmiot zapewnia ostrożne i stabilne zarządzanie działalnością objętą wnioskiem o wydanie zezwolenia, w szczególności przez posiadanie systemu zarządzania ryzykiem i kontroli wewnętrznej odpowiedniego do rodzaju, skali i stopnia złożoności świadczonych usług płatniczych, zapewniającego należyte wypełnianie obowiązków związanych z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu.

Powyższe odnosi się do działalności zarówno instytucji płatniczej, jak również jej agentów.

Ponadto art. 64a ust. 1 u.u.p. wskazuje, że w skład systemu zarządzania ryzykiem i kontroli wewnętrznej w KIP wchodzą m.in. rozwiązania organizacyjne obejmujące zasady i procedury wypełniania obowiązków instytucji obowiązanych w rozumieniu art. 2 ust. 1 ustawy z dnia 1 marca 2018 r. *o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Dz. U. z 2023 r. poz. 1124, z późn. zm.; dalej: ustawa AML), a także kontrola wewnętrzna, która uwzględnia badanie zgodności prowadzonej przez KIP oraz jej agentów działalności z przepisami w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (AML/CFT).

Podmiot, który ubiega się o uzyskanie zezwolenia KNF na świadczenie usług płatniczych   
w charakterze KIP musi tym samym przygotować **procedurę wewnętrzną instytucji obowiązanej**, o której mowa w **art. 50 ustawy AML**.

Celem niniejszego dokumentu jest przedstawienie zbioru dobrych praktyk, które powinny być stosowane przez podmioty zamierzające świadczyć usługi płatnicze w charakterze krajowej instytucji płatniczej przy opracowywaniu regulacji wewnętrznej w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Opisane w niniejszym dokumencie zasady postępowania mogą zostać uwzględnione również przez inne podmioty sektora usług płatniczych oraz ich agentów, które zobligowane do przedstawienia KNF procedury, o której mowa w art. 50 ust. 1 ustawy AML.

Przygotowując Procedurę Przeciwdziałania Praniu Pieniędzy oraz Finansowaniu Terroryzmu (dalej: *Procedura*), instytucja obowiązana (IO) powinna uwzględnić polskie przepisy prawa regulujące przedmiotowe zagadnienie, jak również odpowiednie regulacje unijne oraz wytyczne zawarte w Komunikatach Generalnego Inspektora Informacji Finansowej[[1]](#footnote-1) (GIIF) oraz Stanowiskach Urzędu Komisji Nadzoru Finansowego (UKNF).

Na podstawie art. 65 u.u.p. KNF może odmówić wydania zezwolenia dla KIP, jeżeli procedura wewnętrzna nie będzie regulowała systemu zarządzania ryzykiem i kontroli wewnętrznej w sposób odpowiedni do rodzaju, skali i stopnia złożoności świadczonych usług płatniczych, zapewniający należyte wypełnianie obowiązków związanych z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu.

1. **Osoba odpowiedzialna i AMLRO**

Zgodnie z art. 7 ustawy AML, zarząd lub inny organ zarządzający IO powinien wyznaczyć spośród członków tego organu **osobę odpowiedzialną za wdrażanie obowiązków określonych w ustawie AML**. Powinna ona mieć należytą wiedzę, umiejętności i doświadczenie w zakresie ryzyka prania pieniędzy oraz finansowania terroryzmu (ML/FT) oraz wdrażania polityk, mechanizmów kontrolnych i procedur AML/CFT. Zadania oraz funkcja osoby odpowiedzialnej powinna mieć umocowanie w stosownych dokumentach wewnętrznych (np. uchwałach zarządu, regulaminach).

Niezależnie od obowiązku powołania osoby odpowiedzialnej, na podstawie art. 8 ustawy AML, powinien zostać wyznaczony pracownik zajmujący kierownicze stanowisko, odpowiedzialny za zapewnienie zgodności działalności instytucji obowiązanej oraz jej pracowników i innych osób wykonujących czynności na rzecz IO z przepisami ustawy AML. Wskazany pracownik pełnić będzie rolę tzw. AMLRO (*Anti-Money Laundering Reporting Officer*). AMLRO również powinien m.in. posiadać wystarczającą wiedzę i świadomość ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z modelem biznesowym IO, doświadczenie w zakresie zarządzania tym ryzykiem oraz odpowiedni staż pracy i zakres obowiązków umożliwiający sprawowanie przedmiotowej funkcji   
w sposób skuteczny. Należy wskazać, że taki pracownik powinien mieć zapewnioną niezależność   
w wykonywaniu swojej funkcji, co jest równoznaczne z tym, że osoba wyznaczona spośród członków zarządu IO nie może pełnić roli AMLRO.

Stosownie do dyspozycji art. 154 ust. 1 ustawy AML w przypadku stwierdzenia naruszenia przez IO obowiązków, o których mowa w art. 147 lub art. 148 na osobę odpowiedzialną może zostać nałożona kara pieniężna.

Przy określaniu roli i zadań ww. osób należy uwzględnić wytyczne zawarte w Stanowisku UKNF *dotyczącym AMLRO* z dnia 1 grudnia 2022 r.[[2]](#footnote-2) Obowiązki AMLRO i jego rola muszą być odpowiednio udokumentowane.

1. **Wymogi dotyczące *Procedury***

*Procedura* powinna uwzględniać nie tylko cel jej wprowadzenia, jakim jest ograniczanie   
i zarządzanie rozpoznanym ryzykiem ML/FT, ale również charakter, rodzaj i rozmiar prowadzonej działalności. W konsekwencji *Procedura* powinna odzwierciedlać zasady postępowania stosowane w IO, uwzględniając zarazem określone ramy prawne. W *Procedurze* powinny zostać uregulowane te obszary, w których ustawa AML daje IO swobodę w zakresie sposobu realizacji obowiązków AML/CFT.

*Procedura* powinna stanowić przejrzysty przewodnik dla pracowników IO, w zakresie realizacji obowiązków ustawowych i w szczególności **zawierać** **opis**:

1. **czynności lub działań podejmowanych w celu ograniczenia ryzyka ML/FT i właściwego zarządzania zidentyfikowanym ryzykiem prania pieniędzy lub finansowania terroryzmu;**

W świetle art. 27 ustawy AML, IO **identyfikuje i ocenia ryzyko ML/FT** odnoszące się do jej działalności. Ocena ta powinna wskazywać, w jakim stopniu KIP jest podatna na wykorzystanie   
w procederze prania pieniędzy lub finansowania terroryzmu, co będzie determinowało konieczność zastosowania odpowiednich środków w celu eliminowania tego ryzyka. Ocena ryzyka ML/FT powinna być proporcjonalna do rozmiaru i zakresu działania KIP. Minimalny zakres czynników ryzyka, które muszą zostać wzięte pod uwagę przy przygotowywaniu oceny ryzyka dotyczy:

* klientów,
* państw lub obszarów geograficznych,
* produktów, usług, transakcji lub kanałów ich dostaw.

Należy zauważyć, iż wskazane powyżej czynniki ryzyka są katalogiem podstawowym.   
KNF oczekuje, że w przypadku dużych KIP, oferujących szeroki lub pełen zakres usług płatniczych, działających w wielu państwach Europejskiego Obszaru Gospodarczego powinny być brane pod uwagę dodatkowe obszary ryzyka[[3]](#footnote-3), w szczególności ryzyko w obszarze sankcji międzynarodowych. Prawidłowo sporządzona ocena ryzyka powinna wskazywać obszary działania KIP wymagające poprawy (o ile takie zostaną zidentyfikowane) oraz podjęte działania naprawcze. KIP oceniając ryzyko może uwzględnić obowiązującą, zgodnie z art. 25 ust. 1 ustawy AML, **Krajową Ocenę Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu**[[4]](#footnote-4), jak również sprawozdanie Komisji Europejskiej, o którym mowa w art. 6 ust. 1-3 Dyrektywy 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*. Ustawa AML nakazuje **aktualizację** oceny ryzyka w razie potrzeby, nie rzadziej jednak niż co   
2 lata, szczególnie w związku ze zmianami czynników ryzyka[[5]](#footnote-5) np. zbrojną agresją Federacji Rosyjskiej na Ukrainę. W tym zakresie pomocny może być Komunikat KNF z dnia 10 czerwca 2022 r. *dotyczący sankcji i stosowania przepisów ustawy z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, w przypadku współpracy z podmiotami branży walut wirtualnych*[[6]](#footnote-6)*.* Ocena ryzyka powinna zostać zatwierdzona przez osobę wyznaczoną na podstawie art. 7 ustawy AML lub przez zarząd KIP.

Kwestie związane z oceną ryzyka zostały również przedstawione przez GIIF w *Komunikacie nr 36 w sprawie oceny ryzyka instytucji obowiązanej*[[7]](#footnote-7) oraz w *Stanowisku UKNF dotyczącym oceny ryzyka instytucji obowiązanej* z dnia 15 kwietnia 2020 r.[[8]](#footnote-8)

1. **zasad rozpoznawania i oceny ryzyka ML/FT związanego z danymi stosunkami gospodarczymi lub transakcją okazjonalną, w tym zasad weryfikacji i aktualizacji uprzednio dokonanej oceny ryzyka;**

Zgodnie z przepisami ustawy AML, IO zobligowana jest do rozpoznania i oceny ryzyka ML/FT związanego ze stosunkami gospodarczymi lub transakcją okazjonalną, a zarazem dokonania oceny poziomu rozpoznanego ryzyka. Podstawowymi **kryteriami** przy rozpoznaniu ryzyka są:

* rodzaj klienta,
* obszar geograficzny,
* przeznaczenie rachunku,
* rodzaj produktów, usług i sposobów ich dystrybucji,
* poziom wartości majątkowych deponowanych przez klienta lub wartości przeprowadzonych transakcji,
* cel, regularność lub czas trwania stosunków gospodarczych.

KNF oczekuje, że *Procedura* zawierać będzie opis praktycznego przebiegu procesu klasyfikowania klientów do poszczególnych kategorii ryzyka, czyli opis matrycy ryzyka wraz ze wskazaniem czynników determinujących ocenę ryzyka oraz sposób jego wyliczenia.

Najczęściej stosowanymi kategoriami ryzyka ML/FT są: kategoria ryzyka niskiego, normalnego, wysokiego oraz nieakceptowalnego. Przyznanie ryzyka nieakceptowalnego jest jednoznaczne   
z nienawiązywaniem relacji z klientem lub rozwiązaniem już istniejącej relacji.

## W czasie trwania stosunków gospodarczych z klientem KIP powinna uwzględnić w *Procedurze* konieczność zmiany oceny ryzyka klienta w przypadku ujawnienia okoliczności, które mają na nią wpływ oraz w trakcie okresowej weryfikacji oceny ryzyka, stosownie do wytycznych zawartych w Komunikacie GIIF nr 45 *w sprawie oceniania informacji uzyskiwanych o klientach przez instytucje obowiązane i działań w przypadku braku możliwości zastosowania środków bezpieczeństwa finansowego*[[9]](#footnote-9).

Ustawa AML nie precyzuje jak często ocena ryzyka klienta powinna być aktualizowana,   
w związku z tym przedmiotowy proces powinien wynikać z oceny ryzyka prania pieniędzy   
i finansowania terroryzmu odnoszącego się do działalności KIP oraz jej agentów. Jednak, biorąc pod uwagę praktykę rynkową za zasadne rozwiązanie należy przyjąć, aby okresowa weryfikacja oceny ryzyka odbywała się w odniesieniu do klientów zaklasyfikowanych do:

* niskiego ryzyka – nie rzadziej niż co 4 – 5 lat,
* standardowego ryzyka – nie rzadziej niż co 2-3 lata,
* wysokiego ryzyka – nie rzadziej niż raz do roku.

Proces okresowej weryfikacji klienta powinien być nakierowany na weryfikację wszystkich informacji o kliencie mających wpływ na ocenę jego ryzyka.

KNF oczekuje, że *Procedura* określać będzie czynności, jakie powinny być wykonane   
w ramach weryfikacji oceny ryzyka (np. weryfikacja, czy dokumenty, dane i informacje o kliencie są aktualne, w uzasadnionych przypadkach konieczność pozyskania dokumentów od klienta, weryfikacja transakcji płatniczych realizowanych przez klienta od momentu poprzedniej oceny ryzyka). Wyniki dokonanej analizy oceny ryzyka powinny stanowić uzasadnienie dla nadanej klientowi oceny ryzyka. Wszystkie podejmowane przez KIP działania w tym zakresie powinny być odpowiednio udokumentowane. Dokumentowanie powinno być dokonywane w sposób zapewniający zweryfikowanie informacji i dokumentów będących podstawą oceny ryzyka oraz historii zmian oceny ryzyka.

1. **środków stosowanych w celu właściwego zarządzania rozpoznanym ryzykiem ML/FT związanym z danymi stosunkami gospodarczymi lub transakcją okazjonalną;**

Zgodnie z art. 33 ust. 4 ustawy AML, IO stosują środki bezpieczeństwa finansowego w zakresie i z intensywnością uwzględniającą rozpoznane ryzyko ML/FT związane ze stosunkami gospodarczymi lub transakcją okazjonalną oraz ich ocenę.

Ustawa AML określa **podstawowy** **katalog** **środków** **bezpieczeństwa** **finansowego**, które KIP musi zawsze stosować względem klientów (poza przypadkami określonymi w art. 38 ustawy AML). Ustawa AML przewiduje stosowanie **uproszczonych** lub **wzmożonych** środków bezpieczeństwa finansowego w zależności od wyniku przeprowadzonej oceny ryzyka.   
W związku z tym istnieje możliwość zmiany intensywności i zakresu stosowania środków bezpieczeństwa finansowego. W przypadku relacji obarczonych **niższym** **ryzykiem**, KIP może stosować niektóre środki bezpieczeństwa finansowego z mniejszą częstotliwością (np. ograniczenie bieżącego monitorowania stosunków gospodarczych). Warunkiem stosowania uproszczonych środków bezpieczeństwa finansowego jest potwierdzenie niższego ryzyka w toku oceny ryzyka klienta. W przypadku **ryzyka** **normalnego** muszą zostać zastosowane wszystkie środki bezpieczeństwa finansowego, których minimalny katalog określa art. 34 ust. 1 ustawy AML, z większą intensywnością niż w przypadku ryzyka niskiego. W odniesieniu do **ryzyka** **wysokiego,** ustawa AML nakazuje stosowanie **wzmożonych** środków bezpieczeństwa finansowego. Natomiast w przypadkach określonych w art. 44 - 46 ustawy AML, ustawodawca wprost wskazał, jakie czynności powinny zostać podjęte przez KIP w ramach stosowania wzmożonych środków bezpieczeństwa finansowego. Należy podkreślić, że KIP powinna kierować się zasadą *risk based approach* (podejście oparte na indywidualnie rozumianym ryzyku) przy podejmowaniu działań wobec klienta.

KNF oczekuje, że *Procedura* będzie jednoznacznie wskazywać, jak poziom ryzyka różnicuje stosowanie środków bezpieczeństwa finansowego oraz które z nich i z jaką intensywnością stosowane są względem klientów zaklasyfikowanych do poszczególnych kategorii ryzyka.

W *Procedurze* powinien zostać określony katalog sytuacji – najlepiej poprzez wskazanie konkretnych przypadków – w odniesieniu do których będą miały zastosowanie uproszczone lub wzmożone środki bezpieczeństwa finansowego.

KNF oczekuje, że dla poszczególnych kategorii środków bezpieczeństwa finansowego powinien być wskazany katalog działań w praktyce podejmowanych przez KIP w celu mitygacji danego ryzyka.

Ustawa AML nakłada **bezwzględny** obowiązek stosowania **wzmożonych** środków bezpieczeństwa finansowego w czterech przypadkach:

1. relacji z osobami zajmującymi eksponowane stanowiska polityczne,
2. relacji korespondenckich,
3. relacji z klientami z krajów trzecich wysokiego ryzyka[[10]](#footnote-10),
4. ujawnienia transakcji nietypowych zgodnie z art. 43 ust. 4 ustawy AML.

W odniesieniu do relacji z osobami zajmującymi eksponowane stanowiska polityczne (PEP) ustawa AML nakłada na IO obowiązek wprowadzenia procedury ustalania, czy klient lub beneficjent rzeczywisty jest PEP. Należy podkreślić, że obowiązek przedmiotowej weryfikacji leży po stronie IO. Klient jest jedynie zobowiązany do udzielenia informacji o swoim statusie PEP i może to zrobić w formie oświadczenia pod rygorem odpowiedzialności karnej za składanie fałszywych zeznań. *Procedura* powinna określać procesy (w tym sposób dokumentowania poszczególnych czynności):

* uzyskania akceptacji kadry kierowniczej wyższego szczebla na nawiązanie lub kontynuację stosunków gospodarczych z klientem (np. w formie uchwały zarządu, pisemnej decyzji kadry kierowniczej),
* zastosowania odpowiednich środków celem ustalenia źródła majątku klienta i źródła pochodzenia wartości majątkowych pozostających w dyspozycji klienta w ramach stosunków gospodarczych lub transakcji,
* bieżącego monitorowania stosunków gospodarczych z klientem.

Powyższe działania dotyczą również członków rodziny oraz osób znanych jako bliscy współpracownicy osoby zajmującej eksponowane stanowisko polityczne.

Ustawa AML **nie** **przewiduje** **katalogu** wzmożonych środków bezpieczeństwa finansowego, a zatem ustawodawca pozostawił ich wybór IO. Należy jednak mieć na względzie, że ich celem jest uzyskanie dodatkowych informacji o kliencie i jego beneficjencie rzeczywistym oraz   
o zamierzonym charakterze stosunków gospodarczych.

**Stosowanie** wzmożonych środków bezpieczeństwa finansowego między innymi może polegać na:

* ustaleniu źródła majątku klienta i źródła pochodzenia wartości majątkowych pozostających w jego dyspozycji (np. na podstawie dokumentów potwierdzających źródło majątku oraz źródło pochodzenia środków, faktur, dokumentów podatkowych),
* intensyfikacji stosowania środka bezpieczeństwa finansowego polegającego m.in. na wzmożonym monitoringu stosunków gospodarczych, bieżącej analizie przeprowadzanych przez klienta transakcji (w tym w uzasadnionych przypadkach pozyskanie dodatkowych dokumentów dotyczących realizowanych transakcji),
* częstszej weryfikacji danych zawartych w dokumentacji klienta, w tym weryfikacji tożsamości beneficjenta rzeczywistego (np. na podstawie powszechnie dostępnych źródeł informacji),
* rozszerzeniu zakresu informacji i dokumentów pozyskiwanych od klienta (np. drugi dokument potwierdzający tożsamość klienta, aktualny wyciąg z rachunku bankowego, umowy handlowe, rachunek za czynsz, prąd itp.),
* uzyskaniu dodatkowej zgody na nawiązanie relacji lub kontynuację stosunków gospodarczych z klientem przez kadrę kierowniczą wyższego szczebla.

Dobrą praktyką rynkową jest wdrożenie **programu** **KYC** – **„Poznaj swojego klienta”** („KYC”), regulującego proces zbierania danych i informacji o kliencie w ramach stosowanych środków bezpieczeństwa finansowego, celem identyfikacji i oceny ryzyka klienta.

Ponadto w przypadku współpracy z innymi instytucjami finansowymi, w tym instytucjami sektora usług płatniczych, należy wziąć pod uwagę fakt, iż transakcje realizowane będą na rzecz podmiotów trzecich, co może charakteryzować się wyższym ryzykiem i koniecznością zastosowania wzmożonych środków bezpieczeństwa finansowego, które powinny ograniczyć ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu.

1. **zasad stosowania środków bezpieczeństwa finansowego;**

KNF oczekuje, że *Procedura* będzie wskazywać **przypadki**, w których zachodzi konieczność zastosowania środków bezpieczeństwa finansowego oraz zawierać będzie **opis** **faktycznych** **czynności** wykonywanych przez KIP w zakresie stosowania środków bezpieczeństwa finansowego określonych w art. 34 ust. 1 ustawy AML, w tym:

1. Wytyczne dotyczące procesu identyfikacji klienta i weryfikacji jego tożsamości, stosownie do postanowień art. 37 ustawy AML, w sposób zapewniający prawdziwość i kompletność danych. Kluczowe dla procesu identyfikacji jest pozyskanie i zweryfikowanie danych na podstawie dokumentu stwierdzającego tożsamość klienta (w tym daty ważności dokumentu tożsamości). Dokumentami potwierdzającymi/stwierdzającymi tożsamość są np.: dowód osobisty (polski i obywateli UE), paszport (w tym paszport tymczasowy, dyplomatyczny, służbowy), książeczka żeglarska, żołnierska karta tożsamości, karta pobytu, polski dokument tożsamości cudzoziemca, dokument „zgoda na pobyt tolerowany”, tymczasowe zaświadczenie tożsamości cudzoziemca, dokument podróży przewidziany w konwencji genewskiej dotyczącej statusu uchodźców). KIP powinna wskazać, jakiego rodzaju dokumenty identyfikujące powinny być pozyskiwane od klientów w przypadku osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej, w tym określić wiarygodne i niezależne źródła służące do weryfikacji tożsamości klientów.

W przypadku zawierania relacji na odległość zbiór dobrych praktyk zawiera: Stanowisko UKNF *dotyczące identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji*[[11]](#footnote-11) z dnia 5 czerwca 2019 r. oraz Stanowisko UKNF *dotyczące identyfikacji klienta instytucjonalnego i weryfikacji jego tożsamości w sektorze finansowym podlegającym nadzorowi Komisji Nadzoru Finansowego w oparciu o metodę wideoweryfikacji[[12]](#footnote-12)*z dnia 3 maja 2022 r.

1. Wytyczne dotyczące identyfikacji beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu weryfikacji jego tożsamości, ustalenia struktury własności   
   i kontroli, zgodnie z definicją zawartą w art. 2 ust. 2 pkt 1 ustawy AML. W każdym przypadku, gdy klient jest osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej, KIP powinna ustalić każdą osobę fizyczną, która jest beneficjentem rzeczywistym danego podmiotu w rozumieniu art. 2 ust. 2 pkt 1 ustawy AML. Wobec powyższego należy wskazać, iż pojęcie **beneficjenta** **rzeczywistego** sprowadza się do wskazania osoby/osób, które sprawują kontrolę nad klientem w sposób bezpośredni lub pośredni rozumianej jako możliwość decydowania o czynnościach lub działaniach podejmowanych przez klienta. Czynności podejmowane w celu weryfikacji tożsamości beneficjenta rzeczywistego i ustalenia jego struktury własności mogą polegać np.: na korzystaniu z usług profesjonalnych podmiotów, samodzielnym poszukiwaniu informacji   
   i dokumentów, pozyskaniu od klienta stosownych dokumentów.

W art. 39 ustawy AML został wskazany moment, w którym IO jest obowiązana do weryfikacji tożsamości klienta i beneficjenta rzeczywistego. Ustawa AML dopuszcza zakończenie weryfikacji tożsamości klienta i beneficjenta rzeczywistego podczas nawiązywania stosunków gospodarczych, jeżeli jest to konieczne do zapewnienia ciągłości działalności gospodarczej pod warunkiem, że przeprowadzona pełna ocena ryzyka wskaże na niski poziom ryzyka.

1. Sposób dokonywania oceny stosunków gospodarczych, który powinien bazować na całokształcie posiadanych informacji o kliencie w kontekście usług i produktów, z których klient korzysta. Stosownie do sytuacji, KIP powinna ustalić cel i zamierzony charakter stosunków gospodarczych (na podstawie informacji uzyskanych od klienta, z zewnętrznych baz danych, ze stron internetowych, na podstawie przeprowadzanych transakcji oraz innych wiarygodnych informacji).
2. Wytyczne dotyczące sposobu wykonywania środka bezpieczeństwa finansowego polegającego na bieżącym monitorowaniu stosunków gospodarczych klienta. KNF oczekuje, że *Procedura* zawierać będzie opis procesów monitorowania transakcji poprzez wykonywanie podstawowych obowiązków, takich jak:

* analiza transakcji przeprowadzanych w ramach stosunków gospodarczych,
* bieżąca analiza transakcji,
* wzmożona analiza w przypadku transakcji nietypowych, złożonych, wysokokwotowych i osób zajmujących eksponowane stanowiska polityczne.

W ramach stosowania tego środka bezpieczeństwa KIP powinna mieć możliwość wykrycia transakcji potencjalnie podejrzanych, mogących mieć związek z przestępstwem prania pieniędzy bądź finansowania terroryzmu.

W KIP realizujących znaczną liczbę transakcji, bieżąca ich analiza powinna odbywać się   
z wykorzystaniem przeznaczonych do tego celu programów informatycznych stosujących odpowiednie reguły wyszukujące transakcje potencjalnie podejrzane. Źródłem określenia tych reguł mogą być typologie udostępniane przez np. GIIF, FATF[[13]](#footnote-13) lub wiedza własna KIP. Reguły powinny być na bieżąco aktualizowanie, co podyktowane jest ciągłymi zmianami otoczenia lub pojawieniem się nowych schematów prania pieniędzy lub finansowania terroryzmu. Przy wykorzystywaniu programów analizujących transakcje istotna jest **częstotliwość**, z jaką reguły wyszukują transakcje potencjalnie podejrzane oraz **parametryzacja** **reguł**, która nie powinna pomijać istotnych kryteriów. Każda analiza alertu zgłoszonego przez system, jak i same alerty, powinny podlegać archiwizacji. Właściwym rozwiązaniem jest również nadzorowanie zamkniętych alertów przez osobę kierującą komórką AML/CFT.

W KIP przeprowadzających niewielką liczbę transakcji płatniczych ich analiza może odbywać się manualnie. W zależności od wielkości i skomplikowania (złożoności) procesów i produktów analiza może obejmować różne okresy.

Wynikiem przeprowadzonej analizy transakcji powinno być rozstrzygnięcie, czy transakcje klienta są zgodne z wiedzą KIP o nim i jego działalności. W swoich działaniach KIP powinna uwzględnić wytyczne zawarte w Komunikacie GIIF nr 31 *w sprawie działań podejmowanych przez instytucje obowiązane w przypadku realizacji przez klienta transakcji niezgodnych   
z wiedzą tej instytucji o kliencie, rodzaju i zakresie prowadzonej przez niego działalności*[[14]](#footnote-14).

Należy również uwzględnić szczegółowe wymogi zawarte w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r. *w sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia rozporządzenia (WE) nr 1781/2006* (*Rozporządzenie 2015/847*) oraz w Wspólnych wytycznych wydanych na mocy art. 25 rozporządzenia (UE) 2015/847 dotyczących środków, które dostawcy usług płatniczych powinni podjąć w celu wykrycia brakujących lub niekompletnych informacji   
o płatniku lub odbiorcy, oraz procedur, które powinni wprowadzić w celu zarządzania transferem środków pieniężnych, w przypadku którego brakuje wymaganych informacji (JC/GL/2017/16), w tym wdrożenie skutecznych procedur pozwalających na wykrycie brakujących informacji o płatniku lub odbiorcy[[15]](#footnote-15). Rekomendacje dotyczące informacji towarzyszących transferom środków pieniężnych zostały zawarte w *Stanowisku Urzędu Komisji Nadzoru Finansowego dotyczącym informacji towarzyszących transferom środków pieniężnych*[[16]](#footnote-16)z dnia 8 listopada 2022 r*.*

1. Wskazanie działań podejmowanych, w celu badania źródła pochodzenia wartości majątkowych będących w dyspozycji klienta (np. uzyskanie informacji i dokumentów od klienta, identyfikacja instytucji z której środki przychodzą). Za stosowne rozwiązanie należy uznać podejmowanie przedmiotowych czynności w przypadku klientów zaklasyfikowanych do wysokiej kategorii ryzyka, w tym zwłaszcza klienta o statusie PEP,   
   w przypadku transakcji nietypowych dla danego klienta oraz okoliczności świadczących   
   o podejrzeniu prania pieniędzy lub finansowania terroryzmu.
2. Działania podejmowane celem zapewnienia, że posiadane dane oraz informacje o kliencie są aktualne. W ramach tego procesu KIP powinna wprowadzić periodyczne przeglądy informacji o kliencie uzależnione od poziomu ryzyka przez niego generowanego.   
   W przypadku osób fizycznych powinna być monitorowana data ważności dokumentu tożsamości. Ustawa AML nakazuje **aktywne podejmowanie działań** mających na celu realizację przedmiotowego środka bezpieczeństwa finansowego. W związku z tym nie jest wystarczające zawarcie w regulacjach wewnętrznych postanowień nakazujących klientowi informowanie o każdej zmianie danych. W odniesieniu do klientów wysokiego ryzyka proces ten powinien być bardziej szczegółowy i zindywidualizowany oraz nakierowany na weryfikację wszystkich informacji o kliencie mających wpływ na ocenę ryzyka.
3. Sposób identyfikowania osób upoważnionych do działania w imieniu klienta oraz weryfikacji ich tożsamości, w tym weryfikacja prawidłowości umocowania do działania w imieniu klienta pod kątem, czy jest to dokument wiarygodny, czy zakres upoważnienia uprawnia do wykonywania określonych czynności etc.
4. Sposób dokumentowania stosowania środków bezpieczeństwa finansowego oraz wyników analiz transakcji. Każda czynność podjęta w ramach realizacji środków bezpieczeństwa finansowego powinna być formalnie udokumentowana w formie papierowej czy też elektronicznej pozwalającej na udowodnienie, że obowiązki ustawowe w tym zakresie zostały wykonane. Wyniki analiz transakcji powinny w sposób jednoznaczny wskazywać na powody uznania danej transakcji klienta za potencjalnie podejrzaną lub nie.

KIP na potrzeby stosowania środków bezpieczeństwa finansowego **może przetwarzać informacje** zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania   
w jego imieniu oraz sporządzać ich kopie, przy czym KIP ma obowiązek **poinformować klienta** o powyższym, zarówno przed nawiązaniem relacji, jak i przed przeprowadzeniem transakcji okazjonalnej. KNF przypomina o obowiązku przestrzegania przepisów dotyczących ochrony danych osobowych obowiązujących w Polsce jak i w Unii Europejskiej zgodnie   
z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r.   
*w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz.Urz. UE L119, s.1)[[17]](#footnote-17).

Przesłanki do stosowania środków bezpieczeństwa finansowego zostały wskazane w art. 35 ustawy AML.

Ponadto art. 41 ustawy AML nakłada na IO **obowiązek podjęcia określonych działań   
w przypadku niemożności wykonania któregokolwiek ze środków bezpieczeństwa finansowego**. W praktyce, w przypadku braku możliwości wykonania jednego dowolnego środka ze środków bezpieczeństwa finansowego, KIP powinna podjąć działania wskazane w art. 41 ust. 1 ustawy AML. Wytyczne w tym zakresie zostały określone w Komunikacie GIIF nr 45 *w sprawie oceniania informacji uzyskiwanych o klientach przez instytucje obowiązane i działań w przypadku braku możliwości zastosowania środków bezpieczeństwa finansowego*[[18]](#footnote-18)*.*   
W przypadku wystąpienia okoliczności wskazanych w art. 74, art. 86 lub art. 90 ustawy AML, KIP powinna skierować zawiadomienie do GIIF.

W *Procedurze* należy uwzględnić postanowienia art. 47 ustawy AML, **w przypadku korzystania przez IO z usług podmiotu trzeciego przy stosowaniu środków bezpieczeństwa finansowego** oraz art. 48 ustawy AML, w przypadku **powierzenia** stosowania środków bezpieczeństwa finansowego **innemu podmiotowi działającego w imieniu i na rzecz IO** (np. za pośrednictwem sieci agencyjnej). KNF oczekuje, że *Procedura* będzie zawierała szczegółowe informacje w celu potwierdzenia, że proces jest właściwie zorganizowany i kontrolowany przez KIP, gdyż odpowiedzialność za stosowanie środków bezpieczeństwa finansowego obciąża KIP.

1. **zasad przechowywania dokumentów oraz informacji;**

*Procedura* powinna określać zakres, sposób i długość przechowywania informacji i dokumentów związanych z procesem AML/CFT. Zgodnie z postanowieniami art. 49 ustawy AML, IO zobowiązane są do przechowywania przez okres **5 lat**:

* kopii dokumentów i informacji uzyskanych w wyniku stosowania środków bezpieczeństwa finansowego, w tym informacji uzyskanych za pomocą środków identyfikacji elektronicznej oraz usług zaufania umożliwiających identyfikację elektroniczną w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 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*, licząc od dnia zakończenia stosunków gospodarczych z klientem lub od dnia przeprowadzenia transakcji okazjonalnej,
* dowodów potwierdzających przeprowadzone transakcje i ewidencje transakcji (w oryginale lub kopii) konieczne do identyfikacji transakcji, licząc od dnia zakończenia stosunków gospodarczych z klientem lub od dnia przeprowadzenia transakcji okazjonalnej,
* wyników bieżących analiz przeprowadzonych transakcji, o których mowa w art. 34 ust. 3 ustawy AML, przez okres 5 lat**,** licząc od dnia ich przeprowadzenia.

W szczególnych sytuacjach, GIIF może zażądać, przed upływem ww. terminów, przechowywania przedmiotowej dokumentacji przez kolejny okres nie dłuższy niż 5 lat, licząc od dnia, w którym upływa okres ustawowy.

1. **zasad wykonywania obowiązków obejmujących przekazywanie GIIF informacji o transakcjach oraz zawiadomieniach;**

Obowiązki informacyjne związane z przekazywaniem i gromadzeniem informacji reguluje Rozdział 7, natomiast wstrzymanie transakcji i blokowanie rachunku reguluje Rozdział 8 ustawy AML.

KNF oczekuje, że *Procedura* będzie określać:

* sposób postępowania w przypadku zidentyfikowania transakcji, o których mowa w art. 43 ust. 4 ustawy AML,
* zakres i rodzaj gromadzonych informacji o transakcjach, stosownie do oferowanych produktów i usług przez KIP oraz przekazywanie ich do GIIF w trybie art. 72 ustawy AML. Ustawa AML przewiduje termin **7** **dni** na ich przekazanie od dnia wykonania czynności wskazanych w ust. 5 tego przepisu. Wytyczne w tym zakresie zostały wskazane w Komunikacie GIIF nr 11 *w sprawie raportowania do GIIF informacji o transakcjach ponadprogowych, o których mowa w art. 72 ust. 1 pkt 1 i 2 Ustawy AML, tj. przyjętej wpłacie lub dokonanej wypłacie środków pieniężnych oraz wykonanym transferze środków pieniężnych[[19]](#footnote-19),*
* sposób sporządzania zawiadomień w trybie art. 74 ustawy AML do GIIF o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu. Dotyczy to okoliczności, które nie budzą uzasadnionego podejrzenia. Zawiadomienie jest przekazywane niezwłocznie, jednak nie później niż   
  w terminie do 2 dni roboczych od dnia potwierdzenia przez KIP podejrzenia,
* sposób sporządzania zawiadomień w trybie art. 86 ustawy AML do GIIF o przypadku powzięcia uzasadnionego podejrzenia, że określona transakcja lub określone wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu oraz dalszego jego procesowania. Przepis art. 86 ustawy AML odnosi się do transakcji planowanych. W przypadku, gdy zawiadomienie GIIF nie było możliwe przed przeprowadzeniem transakcji, KIP przekazuje zawiadomienie w trybie art. 90 ustawy AML, uzasadniając przyczyny braku wcześniejszego zawiadomienia.

Wytyczne w tym zakresie zostały wskazane w Komunikacie GIIF nr 22 *w sprawie praktycznych aspektów stosowania środków bezpieczeństwa finansowego oraz przekazywania zawiadomień, o których mowa w art. 74 i art. 86 ustawy AML*[[20]](#footnote-20)*,*

* proces postępowania KIP w przypadku wstrzymania transakcji lub blokady rachunku,
* tryb postępowania w przypadku zawiadomienia prokuratora o podejrzeniu pochodzenia wartości majątkowych z przestępstwa innego niż przestępstwo prania pieniędzy lub finansowania terroryzmu na podstawie art. 89 ustawy AML, w tym niezwłocznego przekazania do GIIF kopii zawiadomień oraz postanowień prokuratury.

Ustawa AML w art. 76 nakłada obowiązek przekazywania informacji lub dokumentów   
w przypadku żądania wystosowanego przez GIIF. Wszelkie czynności podejmowane   
w celu realizacji przedmiotowego obowiązku powinny być udokumentowane np. data i wynik weryfikacji bazy klientów pod kątem podmiotów lub osób fizycznych wskazanych w żądaniu GIIF.

*Procedura* powinna uwzględniać postanowienia art. 54 ustawy AML dotyczącego obowiązku **zachowania tajemnicy** przez IO, jej pracowników oraz osoby działające w imieniu i na jej rzecz w zakresie przekazywania informacji do GIIF oraz planowaniu wszczęcia oraz o prowadzeniu analizy dotyczącej ML/FT.

1. **zasad upowszechniania wśród pracowników KIP oraz jej agentów wiedzy z zakresu przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu;**

Zgodnie z postanowieniami art. 52 ust. 1 ustawy AML, KIP ma obowiązek zapewnienia udziału osób wykonujących czynności związane z przeciwdziałaniem ML/FT w programach szkoleniowych dotyczących realizacji tych obowiązków. Programy szkoleniowe powinny uwzględniać charakter, rodzaj i rozmiar prowadzonej działalności.

Opracowując postanowienia *Procedury* należy uwzględnić Komunikat GIIF z dnia 19 czerwca 2018 r. *dotyczący obowiązku szkoleniowego z przepisów ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*[[21]](#footnote-21)*.*

Zgodnie z praktyką rynkową *Procedura* powinna określać:

* obowiązek ukończenia szkolenia w odniesieniu do nowo zatrudnionych pracowników przed samodzielnym przystąpieniem do czynności merytorycznych,
* częstotliwość przeprowadzania aktualizujących szkoleń AML/CFT (dla dotychczasowych pracowników), jak również konieczność odbycia szkoleń w przypadku zmian przepisów prawa bądź w przypadku stwierdzenia istotnych nieprawidłowości w wyniku przeprowadzonych kontroli zewnętrznych, wewnętrznych lub audytu,
* jednostki organizacyjne, stanowiska, pracowników oraz agentów, którzy podlegają obowiązkowi szkoleniowemu w zakresie AML/CFT,
* osobę/osoby odpowiedzialne za zapewnienie pracownikom szkolenia w zakresie AML/CFT,
* sposób dokumentowania/potwierdzania udziału w szkoleniu, w tym nowo przyjętych pracowników przed przystąpieniem do czynności merytorycznych,
* sposób prowadzenia monitoringu/kontroli wykonywania obowiązku szkoleniowego przez pracowników i osoby współpracujące (przedstawicieli, agentów) oraz działań podejmowanych w stosunku do osób, które nie wzięły udziału w szkoleniu,
* sposób raportowania wykonania obowiązku szkoleniowego (statystyki oraz podejmowane działania) do osób nadzorujących proces AML/CFT lub organów statutowych KIP.

1. **zasad zgłaszania przez pracowników rzeczywistych lub potencjalnych naruszeń przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;**

Zgodnie z art. 53 ustawy AML, IO opracowują i wdrażają wewnętrzną procedurę anonimowego zgłaszania przez pracowników lub inne osoby i podmioty wykonujące czynności na rzecz instytucji obowiązanej rzeczywistych lub potencjalnych naruszeń przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu – *Procedura whistleblowing*.

Procedura ta powinna określać w szczególności:

1. osobę odpowiedzialną za odbieranie zgłoszeń (może to być konkretna osoba lub stanowisko). Osoba, która przetwarza zgłoszenia nie powinna być AMLRO, ani osobą zaangażowaną   
   w przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu, aby uniknąć sytuacji,   
   w której będzie ona rozpatrywać ewentualne skargi na własne działanie,
2. sposób odbierania zgłoszeń (wskazanie kanałów, jakimi zgłoszenie może być dokonane tak, aby osobie zgłaszającej zapewnić anonimowość),
3. sposób ochrony pracownika lub innej osoby wykonującej czynności na rzecz KIP dokonujących zgłoszeń, zapewniający co najmniej ochronę przed działaniami o charakterze represyjnym lub wpływającymi na pogorszenie ich sytuacji prawnej lub faktycznej, lub polegającymi na kierowaniu gróźb (wskazanie w jaki sposób instytucja obowiązana zamierza chronić osoby dokonujące zgłoszenia),
4. sposób ochrony danych osobowych pracownika lub innej osoby wykonującej czynności na rzecz instytucji obowiązanej dokonujących zgłoszenia oraz osoby, której zarzuca się dokonanie naruszenia, zgodnie z przepisami o ochronie danych osobowych (określenie podstawy prawnej przetwarzania danych osobowych, wskazanie sposobu postępowania   
   z danymi, sposobu ich przechowywania),
5. zasady zachowania poufności w przypadku ujawnienia tożsamości osób, o których mowa w pkt 4, lub gdy ich tożsamość jest możliwa do ustalenia (taki sposób postępowania   
   z dokonanym zgłoszeniem, aby pozostawało ono oraz dane osobowe w nim zawarte, poufne poprzez zawężenie kręgu osób uprawnionych do dostępu do treści zgłoszeń, jak   
   i zabezpieczenie dostępu do kanałów odbierania zgłoszeń),
6. rodzaj i charakter działań następczych podejmowanych po odebraniu zgłoszenia (w tym określenie dalszych działań podejmowanych w związku ze zgłoszeniem, wskazanie osób, które ustalą zasadność zgłoszenia, terminów, w jakich poszczególne etapy postępowania powinny być realizowane. Wynik przeprowadzonych działań w formie pisemnej powinien zostać przekazany do organów KIP, które podejmą decyzje o powiadomieniu odpowiednich organów lub GIIF),
7. termin usunięcia przez instytucje obowiązane danych osobowych zawartych w zgłoszeniach (określenie, zgodnie z przepisami dotyczącymi ochrony danych osobowych, czasu, po jakim dane osobowe przetwarzane w związku z dokonanym zgłoszeniem oraz przeprowadzonym postępowaniem wyjaśniającym, zostaną usunięte).

Do *Procedury whistleblowing* powinny mieć zastosowanie przepisy art. 53a ust. 1 i 2 ustawy AML, które mają zagwarantować pracownikom bezpośrednio odpowiedzialnym za przygotowanie zgłoszeń o transakcjach podejrzanych ochronę przed działaniami wymuszającymi nieprawidłową realizację zadań w tym zakresie lub ich karanie. Zgodnie z art. 53a ust. 3 ustawy AML, osoby te w przypadku zetknięcia się z działaniami o charakterze represyjnym lub wpływających na pogorszenie ich sytuacji prawnej lub faktycznej, lub polegających na kierowaniu gróźb mogą poinformować o takich przypadkach GIIF.

*Procedura whistleblowing* może być elementem *Procedury,* jak również może stanowić oddzielną regulację wewnętrzną. W przypadku, gdy KIP posiada oddzielną *Procedurę whistleblowing*, powinna ona zawierać wskazane powyżej elementy i jednoznacznie określać, że odnosi się również do obszaru AML/CFT. Regulacja ta powinna być załączona do wniosku o wydanie zezwolenia.

1. **kontroli wewnętrznej lub nadzoru zgodności działalności KIP z przepisami o przeciwdziałaniu ML/FT oraz zasadami postępowania określonymi w wewnętrznej procedurze;**

Ustawa AML zobowiązuje IO do określenia zasad kontroli wewnętrznej lub nadzoru zgodności działalności IO z przepisami AML/CFT oraz zasadami postępowania.

W zależności od wielkości i charakteru działalności KIP, *Procedura* powinna określać sposób, termin oraz zakres czynności kontrolnych (w tym kontroli agentów) przeprowadzanych przez IO w zakresie zapewnienia:

* prawidłowości procedur oraz rzetelnego raportowania wewnętrznego i zewnętrznego,
* skuteczności i efektywności działania oraz zgodności działania z przepisami prawa   
  i regulacjami wewnętrznymi z uwzględnieniem rekomendacji nadzorczych i standardów rynkowych, przestrzegania zasad zarządzania ryzykiem.

Zakres kontroli, w zależności od rozmiaru prowadzonej działalności, powinien obejmować wszystkie poziomy w strukturze organizacyjnej KIP (w tym agentów i oddziały).

Biorąc pod uwagę stosowane praktyki rynkowe, zasadne jest, aby podstawą funkcjonowania systemu kontroli wewnętrznej było określenie obszarów zwiększonego ryzyka ML/FT w danym **procesie**. Na podstawie określonego w ten sposób obszaru zwiększonego ryzyka możliwe jest racjonalne określenie:

* zakresu kontroli, z uwzględnieniem stopnia złożoności procesów funkcjonujących w KIP, przypadków zaistnienia nieprawidłowości w przeszłości oraz ryzyka zaistnienia nieprawidłowości w przyszłości,
* optymalnej częstotliwości (planu) kontroli, uzależnionej od powyższych czynników ryzyka   
  i stopnia złożoności procesów funkcjonujących w KIP oraz rodzaju kluczowych mechanizmów kontrolnych.

KIP powinna opracować zasady kategoryzacji, dokumentowania i raportowania   
o nieprawidłowościach wykrytych przez kontrolę oraz o statusie realizacji środków naprawczych i dyscyplinujących.

W przypadku KIP posiadających sformalizowany system kontroli i audytu w obszarze AML/CFT, w *Procedurze* wystarczy odesłanie do regulacji wewnętrznych w tym zakresie. Jednakże regulacje te powinny być także załączone do wniosku o wydanie zezwolenia na świadczenie usług płatniczych w charakterze krajowej instytucji płatniczej.

1. **zasad odnotowywania rozbieżności między informacjami w Centralnym Rejestrze Beneficjentów Rzeczywistych (CRBR) a informacjami o beneficjentach rzeczywistych klienta ustalonymi w związku ze stosowaniem ustawy AML;**

IO, zgodnie z art. 61a ust. 1 ustawy AML, odnotowuje rozbieżności między informacjami zgromadzonymi w CRBR a ustalonymi przez nią informacjami o beneficjencie rzeczywistym klienta i podejmuje czynności w celu wyjaśnienia przyczyn tych rozbieżności.

Kwestie w tym zakresie zostały omówione w Komunikacie nr 37 *w sprawie zasad odnotowywania rozbieżności między informacjami zgromadzonymi w CRBR a ustalonymi przez instytucję obowiązaną o beneficjencie rzeczywistym*[[22]](#footnote-22)*.*

Zasady odnotowywania rozbieżności między informacjami zgromadzonymi w CRBR   
a ustalonymi o beneficjencie rzeczywistym powinny określać:

* jakiego rodzaju czynności powinny zostać podjęte w celu wyjaśnienia rozbieżności (np. kontakt z klientem, wyjaśnienie sposobu ustalenia struktury własności i kontroli przez klienta, wyjaśnienie, czy sposób ustalenia beneficjenta rzeczywistego przez instytucję obowiązaną był prawidłowy, wyjaśnienie z jakiego powodu klient uznał daną osobę za beneficjenta rzeczywistego, wskazanie terminu, w jakim powinny być podjęte i zakończone czynności   
  w celu wyjaśnienia przyczyn rozbieżności oraz osoby odpowiedzialne),
* sposób potwierdzenia odnotowywania rozbieżności (np. potwierdzenie, że KIP nie popełniła błędu podczas ustalania beneficjenta rzeczywistego, że informacja zawarta w CRBR nie jest prawidłowa, ustalenie czy rozbieżność ma charakter pozorny czy faktyczny),
* sposób sporządzenia uzasadnienia rozbieżności (np. udokumentowanie czynności podejmowanych przez KIP, wskazanie jakie informacje i dokumenty były podstawą do ustalenia beneficjenta rzeczywistego, z jakich powodów uznała ona, że rozbieżności mają charakter faktyczny).

W przypadku potwierdzenia odnotowanych rozbieżności KIP przekazuje do organu właściwego w sprawach CRBR, wskazanego w art. 56 ustawy AML, zweryfikowaną informację o tych rozbieżnościach wraz z uzasadnieniem i dokumentacją dotyczącą odnotowanych rozbieżności.

1. **zasad dokumentowania utrudnień stwierdzonych w związku z weryfikacją tożsamości beneficjenta rzeczywistego orasz czynności podejmowanych w związku z identyfikacją jako beneficjenta rzeczywistego osoby fizycznej zajmującej wyższe stanowisko kierownicze;**

W świetle przepisów ustawy AML, w przypadku identyfikacji beneficjenta rzeczywistego będącego osobą, o której mowa w art. 2 ust. 2 pkt 1 lit. a) tiret 5, IO dokumentuje:

* wszystkie utrudnienia powodujące brak możliwości ustalenia lub wątpliwości co do tożsamości osób fizycznych określone w art. 2 ust. 2 pkt 1 lit. a) tiret od pierwszego do czwartego ustawy AML,
* wszystkie utrudnienia związane z uzasadnionymi czynnościami podejmowanymi w celu weryfikacji tożsamości beneficjenta rzeczywistego.

Bez względu na to, jak bardzo skomplikowana i wielopoziomowa jest struktura własności klienta, występują czy brakuje publicznych informacji o strukturze własności klienta –KIP jest zobligowana do podjęcia działań zmierzających do **identyfikacji beneficjenta rzeczywistego, weryfikacji jego tożsamości oraz ustalenia struktury własności   
i kontroli klienta**. Dopiero, gdy z analizy struktury własności klienta wynika, iż brak jest możliwości ustalenia lub istnieją wątpliwości co do tożsamości osób fizycznych określonych w art. 2 ust. 2 pkt 1 lit. a) tiret od pierwszego do czwartego ustawy AML, możliwe jest ustalenie jako beneficjenta rzeczywistego osoby fizycznej zajmującej wyższe stanowisko kierownicze.

Dodatkowo powyższe obowiązki w przypadku współpracy z agentami powinny mieć tożsame zastosowanie z uwzględnieniem procesu kontroli przez KIP.

W sytuacji gdy KIP ustaliła jako beneficjenta rzeczywistego osobę fizyczną zajmującą wyższe stanowisko kierownicze, to *Procedura* powinna zawierać opis sposobu dokumentowania wszystkich:

* podjętych czynności zmierzających do ustalenia tożsamości osób fizycznych określonych w art. 2 ust. 2 pkt 1 lit. a) tiret od pierwszego do czwartego ustawy AML (np. pozyskanie odpisu z rejestru przedsiębiorców Krajowego Rejestru Sądowego klienta, umowy spółki klienta, umowy przeniesienia własności udziałów klienta, spisanie przez pracownika notatki z rozmowy telefonicznej z przedstawicielem klienta),
* okoliczności, które zostały uznane przez KIP jako powodujące brak możliwości ustalenia lub wątpliwości co do tożsamości osób fizycznych określonych w art. 2 ust. 2 pkt 1 lit. a) tiret od pierwszego do czwartego ustawy AML (np. ustalenie, że każdy wspólnik klienta – osoba fizyczna – posiada 20% udziałów),
* utrudnień związanych z uzasadnionymi czynnościami podejmowanymi w celu weryfikacji tożsamości beneficjenta rzeczywistego tj. osoby fizycznej zajmującej wyższe stanowisko kierownicze (np. brak zgłoszenia informacji o beneficjencie rzeczywistym do CRBR, utrudnienia związane z brakiem fizycznej obecności beneficjenta, utrudnienia związane z wideoweryfikacją).

Rekomendacje w powyższym zakresie zawiera Komunikat nr 38 GIIF *w sprawie braku możliwości ustalenia lub wątpliwości co do tożsamości osób fizycznych określonych w art. 2 ust.2 pkt.1 lit a tiret pierwszym –czwartym ustawy AML*[[23]](#footnote-23).

1. **zasad stosowania szczególnych środków ograniczających, o których mowa w art. 117 ustawy AML;**

Na mocy art. 118 ustawy AML, IO zobligowana jest do stosowania szczególnych środków ograniczających wobec osób i podmiotów wskazanych w rezolucjach Rady Bezpieczeństwa ONZ, oraz na liście prowadzonej przez GIIF na podstawie art. 120 ust. 1 ustawy AML. Szczególne środki ograniczające, zgodnie z art. 117 ust. 2 ustawy AML, polegają na zamrożeniu wartości majątkowych tych osób i podmiotów lub ich nieudostępnianiu.

Ponadto, KIP ma również obowiązek stosowania środków ograniczających wobec osób   
i podmiotów wskazanych na listach sankcyjnych określonych w rozporządzeniach Rady Unii Europejskiej oraz na liście, o której mowa w art. 2 ust. 1 ustawy z dnia 13 kwietnia 2022 r.   
*o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (Dz. U. z 2023 r. poz. 1497 ze zm.).

Mając na względzie powyższe wymogi, KNF oczekuje, że *Procedura* będzie określała m.in.:

* zasady weryfikacji nowych i istniejących klientów KIP pod kątem występowania na listach sankcyjnych,
* listy sankcyjne wykorzystywane przez KIP i sposób ich aktualizacji,
* zasady postępowania w przypadku zidentyfikowania klienta na liście sankcyjnej, w szczególności zasady zamrażania wartości majątkowych,
* zasady przekazywania informacji do GIIF lub Szefa Krajowej Administracji Skarbowej w związku z zastosowaniem przez KIP odpowiednich środków wobec osób i podmiotów wskazanych na listach sankcyjnych.

1. **Podsumowanie**

Należy wskazać, iż powyższe wskazówki określają **minimalny zakres zagadnień i obowiązków, które uwzględnić powinna instytucja płatnicza w swoich regulacjach wewnętrznych z zakresu przestrzegania przepisów wynikających z ustawy AML**. Każda *Procedura* powinna regulować wykonywanie ustawowych obowiązków w praktyce z uwzględnieniem skali i rodzaju prowadzonej działalności oraz obsługiwanych przez KIP klientów oraz jej agentów. Ponadto dokument ten, jak również jego aktualizacje, powinien być formalnie przyjęty co najmniej przez organ zarządzający KIP.

1. **Sankcja karno-administracyjna za brak *Procedury***

KNF wskazuje, że zgodnie z art. 147 pkt 7 ustawy AML, IO, która nie dopełnia obowiązku wprowadzenia wewnętrznej procedury, o której mowa w art. 50 ustawy AML, podlega karze administracyjnej. Oznacza to, że *Procedura* musi spełniać **wszystkie wymogi** wskazane w art. 50 ust. 2 ustawy AML, aby można było potwierdzić, że KIP posiada *Procedurę*.

1. **Informacja dodatkowa**

Jednocześnie podmioty ubiegające się o uzyskanie statusu KIP powinny być świadome, iż ze względu na charakter relacji instytucji płatniczej z instytucjami sektora bankowego, konieczne może być przekazanie przez instytucję płatniczą szerszego zakresu informacji dotyczącego działalności płatniczej niezbędnego do właściwego oszacowania ryzyka ML/FT oraz zastosowania właściwych środków bezpieczeństwa finansowego przez instytucje sektora bankowego. Przykładowy zakres dodatkowych informacji wskazany został w Stanowisku UKNF z dnia 2 czerwca 2020 r. *dotyczącym stosowania kwestionariusza ankietowego przez banki wobec instytucji sektora usług płatniczych[[24]](#footnote-24)* oraz informacji uzupełniającej z dnia 26 września 2022 r. do ww. Stanowiska[[25]](#footnote-25).

1. <https://www.gov.pl/web/finanse/komunikaty-giif> [↑](#footnote-ref-1)
2. <https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_AMLRO_80468.pdf> [↑](#footnote-ref-2)
3. Dodatkowymi czynnikami ryzyka mogą być np.: narzędzia i systemy informatyczne wykorzystywane przez IO, stopień uzależnienia w obszarze AML/CFTod dostawców zewnętrznych, outsourcing procesów, struktura organizacyjna, efektywność systemu kontroli wewnętrznej, dostępność i efektywność szkoleń. [↑](#footnote-ref-3)
4. https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu [↑](#footnote-ref-4)
5. Takim czynnikiem ryzyka w latach 2020-2022 była pandemia COVID-19 [↑](#footnote-ref-5)
6. https://www.knf.gov.pl/komunikacja/komunikaty?articleId=78557&p\_id=18 [↑](#footnote-ref-6)
7. <https://www.gov.pl/web/finanse/komunikat-nr-36-w-sprawie-oceny-ryzyka-instytucji-obowiazanej> [↑](#footnote-ref-7)
8. <https://www.knf.gov.pl/komunikacja/komunikaty?articleId=69504&p_id=18> [↑](#footnote-ref-8)
9. https://www.gov.pl/web/finanse/komunikat-nr-45-w-sprawie-oceniania-informacji-uzyskiwanych-o-klientach-przez-instytucje-obowiazane-i-dzialan-w-przypadku-braku-mozliwosci-zastosowania-srodkow-bezpieczenstwa-finansowego [↑](#footnote-ref-9)
10. Państwem trzecim wysokiego ryzyka są państwa wskazane w rozporządzeniu delegowanym Komisji (UE) 2016/1675 z 14.07.2016 r. uzupełniającym dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/849 przez wskazanie państw trzecich wysokiego ryzyka mających strategiczne braki. [↑](#footnote-ref-10)
11. 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 [↑](#footnote-ref-11)
12. www.knf.gov.pl/aktualnosci?articleId=77311&p\_id=18 [↑](#footnote-ref-12)
13. *Financial Action Task Force*. [↑](#footnote-ref-13)
14. https://www.gov.pl/web/finanse/komunikat-nr-31-w-sprawie-dzialan-podejmowanych-przez-instytucje-obowiazane-w-przypadku-realizacji-przez-klienta-transakcji-niezgodnych-z-wiedza-tej-instytucji-o-kliencie-rodzaju-i-zakresie-prowadzonej-przez-niego-dzialalnosci [↑](#footnote-ref-14)
15. <https://www.eba.europa.eu/sites/default/documents/files/document_library/About%20Us/Governance%20structure/JC/Publications/Guidelines/1050460/Joint%20Guidelines%20to%20prevent%20TF%20and%20ML%20in%20electronic%20fund%20transfers_PL_16-01-2018.pdf?retry=1> [↑](#footnote-ref-15)
16. https://[www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko\_UKNF\_dot\_informacji\_towarzyszacych\_transferom\_srodkow\_pienieznych\_80201.pdf](http://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_informacji_towarzyszacych_transferom_srodkow_pienieznych_80201.pdf) [↑](#footnote-ref-16)
17. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679 [↑](#footnote-ref-17)
18. https://www.gov.pl/web/finanse/komunikat-nr-45-w-sprawie-oceniania-informacji-uzyskiwanych-o-klientach-przez-instytucje-obowiazane-i-dzialan-w-przypadku-braku-mozliwosci-zastosowania-srodkow-bezpieczenstwa-finansowego [↑](#footnote-ref-18)
19. https://www.gov.pl/web/finanse/komunikat-nr-11-w-sprawie-raportowania-do-giif-informacji-o-transakcjach-ponadprogowych-o-ktorych-mowa-w-art-72-ust-1-pkt-1-i-2-ustawy-aml [↑](#footnote-ref-19)
20. https://ww]w.gov.pl/web/finanse/komunikat-nr-22-w-sprawie-praktycznych-aspektow-stosowania-srodkow-bezpieczenstwa-finansowego-oraz-przekazywania-zawiadomien-o-ktorych-mowa-w-art-74-i-art-86-ustawy-aml2 [↑](#footnote-ref-20)
21. <https://mf-arch2.mf.gov.pl/ministerstwo-finansow/dzialalnosc/giif/aktualnosci/-/asset_publisher/SVp7/content/komunikat-dotyczacy-obowiazku-szkoleniowego-z-przepisow-ustawy-z-dnia-1-marca-2018-r-o-przeciwdzialaniu-praniu-pieniedzy-oraz-finansowaniu-terroryzmu/pop_up?_101_INSTANCE_SVp7_viewMode=print>. [↑](#footnote-ref-21)
22. <https://www.gov.pl/web/finanse/komunikat-nr-37-w-sprawie-zasad-odnotowywania-rozbieznosci-miedzy-informacjami-zgromadzonymi-w-crbr-a-ustalonymi-przez-instytucje-obowiazana-informacjami-o-beneficjencie-rzeczywistym-klienta> [↑](#footnote-ref-22)
23. https://www.gov.pl/web/finanse/komunikat-nr-38-w-sprawie-braku-mozliwosci-ustalenia-lub-watpliwosci-co-do-tozsamosci-osob-fizycznych-okreslonych-w-art-2-ust-2-pkt-1-lit-a-tiret-pierwszymczwartym-ustawy-aml. [↑](#footnote-ref-23)
24. <https://www.knf.gov.pl/aktualnosci?articleId=69893&p_id=18> [↑](#footnote-ref-24)
25. <https://www.knf.gov.pl/knf/pl/komponenty/img/Informacja_uzupe%C5%82niaj%C4%85ca_do_Stanowiska_UKNF_z_2_czerwca_2020%20r..pdf> [↑](#footnote-ref-25)