Komunikat nr 114 skierowany do instytucji obowiązanych, o których mowa w art. 2 ust. 1 pkt 15, 15a oraz 17 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Status instytucji obowiązanych

Zgodnie z art. 2 ust. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[1] (dalej jako: Ustawa), instytucjami obowiązanymi są m.in.:

1) doradcy podatkowi w zakresie, w jakim świadczą na rzecz klienta pomoc prawną lub czynności doradztwa podatkowego dotyczące:

a) kupna lub sprzedaży nieruchomości, przedsiębiorstwa lub zorganizowanej części przedsiębiorstwa;
b) zarządzania środkami pieniężnymi, instrumentami finansowymi lub innymi aktywami klienta;
c) zawierania umowy o prowadzenie rachunku bankowego, rachunku papierów wartościowych lub wykonywania czynności związanych z prowadzeniem tych rachunków;
d) wnoszenia wkładu do spółki kapitałowej lub podwyższenia kapitału zakładowego spółki kapitałowej;
e) tworzenia, prowadzenia działalności lub zarządzania spółkami kapitałowymi lub trustami

- z wyjątkiem doradców podatkowych wykonujących zawód w ramach stosunku pracy w podmiotach innych niż te, o których mowa w art. 4 ust. 1 pkt 1 i 3 ustawy o doradztwie podatkowym[2];

2) doradcy podatkowi w zakresie czynności doradztwa podatkowego innych niż wymienione w art. 2 ust. 1 pkt 14;

3) biegli rewidenci;

4) podmioty prowadzące działalność w zakresie usługowego prowadzenia ksiąg rachunkowych[3];

[1] T.j. Dz. U. z 2025 r. poz. 644

[2] Ustawa z dnia 5 lipca 1996 r. o doradztwie podatkowym (t.j. Dz. U. z 2021 r. poz. 2117).

[3] Mając na uwadze art. 76a ust 3 ustawy z dnia 29 września1994 r. o rachunkowości (Dz. U. z 2002 r. nr 76, poz. 694, ze zm.), do tej kategorii instytucji obowiązanych zaliczają się zarówno księgowi tj. osoby fizyczne prowadzące działalność polegającą na usługowym prowadzeniu ksiąg rachunkowych na podstawie posiadanych uprawnień, jak i podmioty gospodarcze (spółki cywilne, spółki prawa handlowego), oferujące takie usługi, zatrudniające pracowników posiadających odpowiednie uprawnienia do usługowego prowadzenia ksiąg.

5) przedsiębiorcy w rozumieniu ustawy Prawo przedsiębiorców[4], których podstawową działalnością gospodarczą jest świadczenie usług polegających na sporządzaniu deklaracji, prowadzeniu ksiąg podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego, niebędący innymi instytucjami obowiązanymi.

Na ww. instytucjach obowiązanych spoczywają wskazane poniżej obowiązki.

I. Wyznaczenie pracownika odpowiedzialnego za wykonanie obowiązków ustawowych[5]

Instytucje obowiązane wyznaczają pracownika zajmującego kierownicze stanowisko, odpowiedzialnego za zapewnienie zgodności działalności instytucji obowiązanej oraz jej pracowników i innych osób wykonujących czynności na rzecz tej instytucji obowiązanej, z przepisami w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Wyznaczony pracownik jest również odpowiedzialny za przekazywanie, w imieniu instytucji obowiązanej, zawiadomień o których mowa w art. 74 ust. 1, art. 86 ust. 1, art. 89 ust. 1 i art. 90 Ustawy.

W przypadku instytucji obowiązanych prowadzących działalność jednoosobowo, zadania kadry kierowniczej wyższego szczebla (art. 6 Ustawy) oraz zadania pracownika, o którym mowa w art. 8 Ustawy, wykonuje osoba prowadząca tę działalność.

Właściwe wykonywanie zadań przez osobę odpowiedzialną za wykonywanie obowiązków wynikających z Ustawy, jest niezwykle ważne z perspektywy funkcjonowania całego systemu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Prawidłowa realizacja tych obowiązków jest kluczowa dla zgodności działalności instytucji obowiązanej z przepisami Ustawy, a także zwiększa bezpieczeństwo finansowe firmy.

W przypadku instytucji obowiązanych o złożonej strukturze organizacyjnej, konieczne jest wyznaczenie pracownika zajmującego kierownicze stanowisko jako osobę odpowiedzialną za zapewnienie zgodności działań instytucji, jej pracowników i współpracowników z przepisami Ustawy.

Osoba taka jest nazywana AMLRO, czyli *Anti Money Laundering Reporting Officer*.

[4] Ustawa z dnia 6 marca 2018 r. - Prawo przedsiębiorców (t.j. Dz. U. z 2025 r. poz. 1480).
[5] Art. 6- 9 Ustawy.

Osoba na stanowisku AMLRO powinna m.in.:

a) mieć odpowiednią wiedzę i doświadczenie w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;
b) mieć wiedzę dotyczącą specyfiki działalności danej instytucji obowiązanej, aby prawidłowo ocenić ryzyka związane z prowadzeniem tej działalności;
c) nadzorować, analizować i aktualizować wewnętrzne regulacje dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, takie jak analiza oceny ryzyka instytucji obowiązanej, wewnętrzne procedury, procedury dotyczące sygnalistów;
d) zachowywać niezależność;
e) mieć nieograniczony dostęp do informacji niezbędnych do realizacji swoich zadań;
f) monitorować nieprawidłowości występujące w instytucji obowiązanej i wprowadzać działania naprawcze;
g) przekazywać w imieniu instytucji obowiązanej zawiadomienia, o których mowa
w art. 74 ust. 1, art. 86 ust. 1, art. 89 ust. 1 i art. 90. Ustawy.

Wyznaczenie osoby odpowiedzialnej za realizację obowiązków w wynikających z Ustawy, powinno, dla celów dowodowych, mieć formę pisemną lub wynikać z akt osobowych pracownika np. zakresu obowiązków.

II. Ocena ryzyka dokonywana przez instytucje obowiązane

Art. 27 ust. 1 Ustawy nakłada na instytucje obowiązane obowiązek identyfikacji i oceny ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, odnoszącego się do ich działalności, z uwzględnieniem czynników ryzyka dotyczących klientów, państw lub obszarów geograficznych, produktów, usług, transakcji lub kanałów ich dostaw.
Działania te są proporcjonalne do charakteru i wielkości instytucji obowiązanej.

Należy podkreślić, że art. 27 ust. 1 Ustawy dotyczy identyfikacji i oceny ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu odnoszącego się do ogólnej działalności instytucji obowiązanej, tzn. w oderwaniu od konkretnego i indywidualnego stosunku gospodarczego oraz konkretnej i indywidualnej transakcji okazjonalnej (tzw. „ogólna ocena ryzyka").

Natomiast art. 33 ust. 2 i 3 Ustawy dotyczy rozpoznania i oceny ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z konkretnym i indywidualnym stosunkiem gospodarczym nawiązanym przez instytucję

obowiązaną z klientem, lub związanego z konkretną i indywidualną transakcją okazjonalną (tzw. „indywidualna ocena ryzyka").

Nie można jednak zapominać, iż ogólna ocena ryzyka wpływa również na indywidualną ocenę ryzyka i na odwrót. Instytucje obowiązane, podczas rozpoznawania i dokonywania oceny ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z konkretnym stosunkiem gospodarczym lub z transakcją okazjonalną, powinny wykorzystywać informacje i wnioski wynikające z ogólnej oceny ryzyka.

Należy przy tym uwzględnić, że działania w zakresie identyfikacji i oceny ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu odnoszące się do działalności instytucji obowiązanej mają być proporcjonalne do jej charakteru i wielkości. Wnioski wynikające z przeprowadzania indywidualnych ocen ryzyka powinny wpływać na bieżące aktualizacje ogólnej oceny ryzyka.

Każda instytucja obowiązana powinna znać i rozumieć ryzyko prania pieniędzy i finansowania terroryzmu, na jakie jest narażona w związku z charakterem oraz zakresem prowadzonej przez siebie działalności gospodarczej. Należy podkreślić, że ogólna ocena ryzyka musi być bezwzględnie dostosowana do charakteru i zakresu działalności prowadzonej przez instytucję obowiązaną. Generalny Inspektor Informacji Finansowej (dalej jako: Generalny Inspektor) zaznacza, iż stosowanie wzorów ogólnych ocen ryzyka (np. dostępnych w otwartych źródłach danych) bez dokładnego dostosowania ich do konkretnego i indywidualnego charakteru i zakresu działalności, naraża instytucję obowiązaną na zarzut niedopełnienia obowiązku ustawowego. Warto podkreślić, iż nawet w przypadku instytucji obowiązanych prowadzących działalność w zbliżonym zakresie, możliwe jest zidentyfikowanie całkowicie odmiennych ryzyk związanych z praniem pieniędzy i finansowaniem terroryzmu.

Efektem końcowym dokonania ogólnej oceny ryzyka instytucji obowiązanej, powinno być określenie poziomu ryzyka prania pieniędzy oraz finasowania terroryzmu, na jaki dana instytucja jest narażona prowadząc działalność gospodarczą.

Generalny Inspektor podkreśla, że ocena ryzyka instytucji obowiązanej jest jednym z najważniejszych dokumentów w instytucji obowiązanej, ponieważ określa ona czynności i działania, jakie instytucja obowiązana podejmuje w celu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.[6] [7]

[6] Komunikat nr 36 Generalnego Inspektora w sprawie oceny ryzyka instytucji obowiązanej:

https://www.gov.pl/web/finanse/komunikat-nr-36-w-sprawie-oceny-ryzyka-instytucji-obowiazanej

[7] Urząd Komisji Nadzoru Finansowego opublikował w dniu 15 kwietnia 2020 r. „Stanowisko UKNF dotyczące oceny ryzyka instytucji obowiązanej". Wprawdzie powyższy dokument skierowany został do instytucji obowiązanych podlegających

III. Analiza i ocena ryzyka związanego ze stosunkiem gospodarczym bądź transakcją okazjonalną

Zgodnie z art. 33 Ustawy:

1) instytucje obowiązane stosują wobec swoich klientów środki bezpieczeństwa finansowego;

2) instytucje obowiązane rozpoznają ryzyko prania pieniędzy oraz finansowania terroryzmu związane ze stosunkami gospodarczymi lub z transakcją okazjonalną oraz oceniają poziom rozpoznanego ryzyka;

3) instytucje obowiązane dokumentują rozpoznane ryzyko prania pieniędzy oraz finansowania terroryzmu związane ze stosunkami gospodarczymi lub z transakcją okazjonalną oraz jego ocenę, uwzględniając w szczególności czynniki dotyczące:

a) rodzaju klienta;

b) obszaru geograficznego;

c) przeznaczenia rachunku;

d) rodzaju produktów, usług i sposobów ich dystrybucji;

e) poziomu wartości majątkowych deponowanych przez klienta lub wartości przeprowadzonych transakcji;

f) celu, regularności lub czasu trwania stosunków gospodarczych;

4) instytucje obowiązane stosują środki bezpieczeństwa finansowego w zakresie i z intensywnością uwzględniającymi rozpoznane ryzyko prania pieniędzy oraz finansowania terroryzmu związane ze stosunkami gospodarczymi lub z transakcją okazjonalną, oraz jego ocenę.

Obowiązek, o którym mowa w art. 33 Ustawy, dotyczy rozpoznania i oceny ryzyka konkretnej relacji gospodarczej czy konkretnej transakcji okazjonalnej. Na podstawie oceny, określa się klasy ryzyka, najczęściej według podziału na ryzyko niskie, standardowe i wysokie.

Przeprowadzenie oceny ryzyka jest wstępnym etapem jakiejkolwiek relacji z klientem, to od przypisanego poziomu zależy rodzaj środków bezpieczeństwa, jakie zostaną zastosowane, i częstotliwość monitorowania operacji.

---

nadzorowi KNF (podmiotów rynku finansowego - np. banków), jednak przedstawione w nim dobre praktyki można odnieść do wszystkich instytucji obowiązanych. Stanowisko to dostępne jest pod poniższym linkiem:

https://www.knf.gov.pl/komunikacja/komunikaty?articleId=69504&p_id=18

W pierwszej kolejności należy rozpoznać ryzyko prania pieniędzy oraz finansowania terroryzmu, co oznacza ogólną analizę ryzyka, na podstawie wiedzy i doświadczenia osoby wypełniającej obowiązki w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, jakie stosunek gospodarczy czy transakcja okazjonalna mogą wywołać dla instytucji obowiązanej. Dopiero na podstawie rozpoznanego ryzyka, instytucja dokonuje oceny ryzyka z uwzględnieniem zasad wynikających z wewnętrznej procedury instytucji obowiązanej.

Należy pamiętać, że dokonana ocena ryzyka powinna być weryfikowana i aktualizowana. Częstotliwość aktualizacji powinna wynikać z uprzednio przypisanego poziomu ryzyka.

Wymienione w art. 33 ust. 3 Ustawy czynników, jakie powinna uwzględnić instytucja obowiązana, są wyliczeniem przykładowym, aczkolwiek zasługującym na szczególną uwagę przy dokonywaniu oceny ryzyka stosunku gospodarczego bądź transakcji okazjonalnej. W przypadku klientów o szerszym profilu działalności, rekomendowane jest poszerzenie katalogu czynników w oparciu, o które będzie dokonywana ocena ryzyka.

W zakresie czynnika dotyczącego rodzaju klienta, instytucja obowiązana powinna wziąć pod uwagę m.in. to, czy klient jest osobą fizyczną, czy osobą prawną, formę organizacyjną osoby prawnej oraz profil działalności klienta.

W odniesieniu do czynnika dotyczącego obszaru geograficznego, instytucja obowiązana powinna uwzględnić m.in. miejsce siedziby klienta, obszar geograficzny jego działalności, miejsce urodzenia, miejsce zamieszkania, obywatelstwo, itp., przy czym szczególną uwagę powinny zwrócić kraje wysokiego ryzyka.

W zakresie czynnika dotyczącego rodzaju produktów, usług i sposobów ich dystrybucji, należy wziąć pod uwagę np. typy oferowanych przez klienta produktów czy usług oraz to, czy są one oferowane zdalnie czy stacjonarnie, przy założeniu, że zdalny sposób dystrybucji stwarza wyższe ryzyko, niż dystrybucja stacjonarna.

Rozpoznane ryzyko i przeprowadzoną ocenę ryzyka należy zawsze udokumentować w taki sposób, aby można było zidentyfikować tok przeprowadzonego rozumowania i składowe wpływające na ostateczną ocenę ryzyka przypisaną danemu stosunkowi gospodarczemu.

IV. Stosowanie środków bezpieczeństwa finansowego

Zgodnie z art. 33 Ustawy, instytucje obowiązane stosują środki bezpieczeństwa z intensywnością wynikającą z ryzyka przypisanego konkretnemu stosunkowi

gospodarczemu, czy transakcji okazjonalnej. Oznacza to, że im wyższe ryzyko, tym intensywniejsze stosowanie środków bezpieczeństwa finansowego. Ponadto, nie ma możliwości całkowitego odstąpienia od stosowania środków bezpieczeństwa finansowego w sytuacjach, w których ustawa nakłada obowiązek ich stosowania.

Art. 34 Ustawy zawiera katalog środków bezpieczeństwa finansowego. Zgodnie z nim, środki bezpieczeństwa finansowego obejmują:

1) identyfikację klienta oraz weryfikację jego tożsamości;

2) identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu:

a) weryfikacji jego tożsamości,

b) ustalenia struktury własności i kontroli, w przypadku klienta będącego osobą prawną, jednostką organizacyjną nieposiadającą osobowości prawnej lub trustem,

3) ocenę stosunków gospodarczych i, stosownie do sytuacji, uzyskanie informacji na temat ich celu i zamierzonego charakteru;

4) bieżące monitorowanie stosunków gospodarczych klienta, w tym:

a) analizę transakcji przeprowadzanych w ramach stosunków gospodarczych w celu zapewnienia, że transakcje te są zgodne z wiedzą instytucji obowiązanej o kliencie, rodzaju i zakresie prowadzonej przez niego działalności oraz zgodne z ryzykiem prania pieniędzy oraz finansowania terroryzmu związanym z tym klientem,

b) badanie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta, w przypadkach uzasadnionych okolicznościami,

c) zapewnienie, że posiadane dokumenty, dane lub informacje dotyczące stosunków gospodarczych są na bieżąco aktualizowane.

Zgodnie z art. 35 Ustawy, stosowanie środków bezpieczeństwa jest obowiązkowe
w przypadku:

1) nawiązywania stosunków gospodarczych;

2) przeprowadzania transakcji okazjonalnej:

a) o równowartości 15 000 euro lub większej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane,

lub

b) która stanowi transfer środków pieniężnych na kwotę przekraczającą równowartość 1000 euro,

c) z wykorzystaniem waluty wirtualnej o równowartości 1000 euro lub większej, w przypadku instytucji obowiązanych, o których mowa w art. 2 ust. 1 pkt 12 Ustawy;

3) przeprowadzania gotówkowej transakcji okazjonalnej o równowartości 10 000 euro lub większej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane, w przypadku instytucji obowiązanych, o których mowa w art. 2 ust. 1 pkt 21-23 Ustawy;

4) obstawiania stawek oraz odbioru wygranych o równowartości 2000 euro lub większej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane - w przypadku instytucji obowiązanych, o których mowa w art. 2 ust. 1 pkt 20 Ustawy;

5) podejrzenia prania pieniędzy lub finansowania terroryzmu;

6) wątpliwości co do prawdziwości lub kompletności dotychczas uzyskanych danych identyfikacyjnych klienta.

Ponadto, instytucje obowiązane stosują środki bezpieczeństwa finansowego również w odniesieniu do klientów, z którymi utrzymują stosunki gospodarcze, z uwzględnieniem rozpoznanego ryzyka prania pieniędzy oraz finansowania terroryzmu, w szczególności gdy:

1) doszło do zmiany uprzednio ustalonego charakteru lub okoliczności stosunków gospodarczych;

2) doszło do zmiany uprzednio ustalonych danych dotyczących klienta lub beneficjenta rzeczywistego;

3) instytucja obowiązana była w ciągu danego roku kalendarzowego zobowiązana, na podstawie przepisów prawa, do skontaktowania się z klientem w celu weryfikacji informacji dotyczących beneficjentów rzeczywistych, w szczególności gdy obowiązek taki wynikał z przepisów ustawy o wymianie informacji podatkowych z innymi państwami[8].

Art. 36 i 37 Ustawy szczegółowo wyjaśniają na czym polega identyfikacja i weryfikacja klienta oraz beneficjenta rzeczywistego. Identyfikacja klienta i weryfikacja jego tożsamości jest podstawowym i niezbędnym środkiem

[8] Ustawa z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami (Dz.U. z 2024 r. poz. 1588 i 1685).

bezpieczeństwa finansowego, bez którego nie jest możliwe nawiązanie jakiejkolwiek relacji z klientem.

Identyfikacja klienta polega na ustaleniu:

1) w przypadku osoby fizycznej:

a) imienia i nazwiska;

b) obywatelstwa;

c) numeru Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub daty urodzenia w przypadku gdy nie nadano numeru PESEL, oraz państwa urodzenia;

d) serii i numeru dokumentu stwierdzającego tożsamość osoby;

e) adresu zamieszkania, w przypadku posiadania tej informacji przez instytucję obowiązaną;

f) nazwy (firmy), numeru identyfikacji podatkowej (NIP) oraz adresu głównego miejsca wykonywania działalności gospodarczej - w przypadku osoby fizycznej prowadzącej działalność gospodarczą;

2) w przypadku osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej:

a) nazwy (firmy);

b) formy organizacyjnej;

c) adresu siedziby lub adresu prowadzenia działalności;

d) NIP, a w przypadku braku takiego numeru - państwa rejestracji, nazwy właściwego rejestru oraz numeru i daty rejestracji;

e) danych identyfikacyjnych, o których mowa w art. 36 ust. 1 pkt 1 lit. a i c, osoby reprezentującej tę osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej.

W przypadku klienta będącego osobą fizyczną, wymagane jest pozyskanie wszystkich danych, o których mowa w art. 36 ust. 1 pkt 1 Ustawy.

Identyfikacja osoby upoważnionej do działania w imieniu klienta, obejmuje ustalenie danych, o których mowa w art. 36 ust. 1 pkt 1 lit. a-d Ustawy.

W każdym przypadku, gdy klientem jest osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, poza zakresem danych wskazanych
w art. 36 ust. 1 pkt 2 Ustawy, należy ustalić, kto jest jej beneficjentem rzeczywistym. W przypadkach klientów, którymi są osoby fizyczne i osoby

fizyczne prowadzące działalność gospodarczą, należy przyjąć, że to one są beneficjentami rzeczywistymi, chyba że okoliczności zaobserwowane przez instytucję obowiązaną, wskazują na to, że beneficjentem jest ktoś inny.

W zakresie identyfikacji beneficjenta rzeczywistego, wystarczające jest pozyskanie imienia i nazwiska, niemniej jednak, jeżeli jest to możliwe, zaleca się pozyskanie dodatkowych informacji.

Osobą upoważnioną do działania w imieniu klienta, będzie każda osoba, która nie tylko ma prawo do takiej reprezentacji, ale również faktycznie wykorzystuje swoje szczególne prawne umocowanie i działa przed daną instytucją obowiązaną.

Zgodnie z art. 37 ust. 1 Ustawy, weryfikacja tożsamości klienta, osoby upoważnionej do działania w jego imieniu oraz beneficjenta rzeczywistego, polega na potwierdzeniu ustalonych danych identyfikacyjnych na podstawie dokumentu stwierdzającego tożsamość osoby fizycznej, dokumentu zawierającego aktualne dane z wyciągu z właściwego rejestru lub innych dokumentów, danych lub informacji pochodzących z wiarygodnego i niezależnego źródła, w tym, o ile są dostępne, ze środków identyfikacji elektronicznej lub pozyskanych za pośrednictwem odpowiednich usług zaufania określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym[9].

Dokument stwierdzający tożsamość, to każdy dokument, który jest za taki uznawany
w przepisach polskiego prawa. Do takich dokumentów można zaliczyć: dowód osobisty, dokument paszportowy (paszport, paszport tymczasowy, paszport dyplomatyczny, paszport służbowy Ministerstwa Spraw Zagranicznych), wizę, dokument podróży, kartę pobytu, polski dokument podróży dla cudzoziemca, tymczasowy polski dokument podróży dla cudzoziemca, polski dokument tożsamości cudzoziemca, dokument „zgoda na pobyt tolerowany", książeczkę żeglarską, kartę tożsamości, dokument podróży przewidziany w Konwencji genewskiej dotyczącej statusu uchodźców[10], jak też książeczkę wojskową.

W ustawie nie ma definicji wiarygodnych i niezależnych źródeł informacji, jednak za przykład takiego źródła można uznać rejestr PESEL. Należy jednak pamiętać, że bezpośredni dostęp do tego rejestru mają wyłącznie podmioty uprawnione,

[9] 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 (Dz.U.UE.L.2014.257.73).

[10] Konwencja dotycząca statusu uchodźców, sporządzona w Genewie dnia 28 lipca 1951 r. (Dz.U.1991.119.515).

takie jak policja czy organy administracji publicznej. Pozostałe podmioty, aby uzyskać dostęp do rejestru, muszą wykazać swój interes prawny.

W przypadku identyfikacji osób fizycznych ważne jest, aby w miarę możliwości, ustalić wszystkie posiadane przez klienta obywatelstwa.

W zakresie stosunków gospodarczych, należy zawsze stosować środek bezpieczeństwa finansowego wymieniony w art. 34 ust. 1 pkt 3 Ustawy tj. ocenę stosunków gospodarczych i, stosownie do sytuacji, uzyskać informację na temat ich celu i zamierzonego charakteru. Środek ten należy stosować każdorazowo przy nawiązywaniu stosunków gospodarczych, a także przy okresowym stosowaniu środków bezpieczeństwa, w związku z utrzymywanymi stosunkami gospodarczymi.
W ramach stosowania tego środka należy zbudować kompleksowy profil klienta. Należy dokładnie ustalić, w jaki sposób klient zamierza wykorzystywać relację z instytucją obowiązaną, jakimi kwotami zamierza operować, z jakich produktów czy usług korzystać.

Zbudowanie takiego profilu klienta jest niezbędne do późniejszego porównywania z ewentualnymi odstępstwami, które mogłyby wzbudzać podejrzenia[11].

W zakresie środka bezpieczeństwa finansowego, o którym mowa w art. 34 ust. 1 pkt 4 Ustawy, należy zapewnić bieżące monitorowanie stosunków gospodarczych klienta, w tym:

W celu zapewnienia zgodności transakcji z wiedzą instytucji obowiązanej o kliencie, rodzajem i zakresem prowadzonej przez niego działalności oraz uwzględnienia ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z tym klientem, niezbędne jest bieżące analizowanie wszelkich aktywności klienta i porównywanie ich do ustalonego profilu klienta, w zakresie środka bezpieczeństwa finansowego, o którym mowa w art. 34 ust. 1 pkt 3 Ustawy.

W przypadku wystąpienia rozbieżności, instytucja obowiązana powinna wystąpić do klienta, w celu uzyskania dodatkowych wyjaśnień.

Analizy transakcji należy odpowiednio dokumentować. Notatki z analiz transakcji, powinny zawierać wszystkie elementy zawarte w art. 34 ust. 1 pkt 4 lit. a Ustawy, oraz powinny być rozbudowane na tyle, aby opisywały działania

[11] Więcej informacji na ten temat można znaleźć w Komunikacie nr 31 Generalnego Inspektora: 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

podejmowane w ramach danej analizy oraz aby wyjaśniały, dlaczego akurat takie kroki i decyzje zostały podjęte.

W treści notatki powinny być zawarte takie dane, jak m.in. profil klienta, poziom ryzyka prania pieniędzy lub finansowania terroryzmu dla tego klienta, informacje o wszystkich analizowanych transakcjach, dane z teczki klienta, do których odnosi się analityk, wynik analizy.

Analizy transakcji powinny być przeprowadzane na bieżąco, od momentu nawiązania stosunków gospodarczych i rozpoczęcia dokonywania przez klienta transakcji.

W uzasadnionych okolicznościach, należy stosować środek bezpieczeństwa finansowego, o którym mowa w art. 34 ust. 1 pkt 4 lit. b Ustawy tj. badanie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta.

Instytucja obowiązana powinna określić w wewnętrznych procedurach, czym są uzasadnione okoliczności w przypadku jej klientów. Definicja uzasadnionych okoliczności powinna być aktualizowana i modyfikowana tak, aby uwzględniała aktualny poziom ryzyka, z którym mierzy się dana instytucja obowiązana.

W zakresie badania źródła pochodzenia wartości majątkowych, instytucja obowiązana powinna zwracać się do klientów o wyjaśnienia i wiarygodne dokumenty dotyczące źródła pochodzenia środków i źródła pochodzenia majątku, a następnie powinna poddać je analizie. Badanie źródła wartości majątkowych nie powinno ograniczać się do informacji dostępnych publicznie. *Open Source Intelligence* (OSINT) może być stosowany jedynie pomocniczo, do oceny informacji i dokumentów od klienta. Badanie źródła wartości majątkowych powinno zawsze obejmować uzyskiwanie wyjaśnień i dokumentów od klienta.

Posiadane dokumenty, dane lub informacje dotyczące stosunków gospodarczych powinny być na bieżąco aktualizowane. Częstotliwość aktualizacji zależy od poziomu ryzyka przypisanego danemu klientowi. Instytucja obowiązana powinna odnotowywać każdorazowo w teczce klienta daty aktualizacji zgromadzonych dokumentów dotyczących klienta, tak aby było wiadomo kiedy i jakie dane pojawiały się w teczce. Każdorazowa aktualizacja danych powinna być dokładnie dokumentowana, tak aby była widoczna historia zmian. Proces ten powinien obejmować daty aktualizacji oraz szczegółowy opis wprowadzonych zmian.

Zgodnie z art. 43 Ustawy, instytucje obowiązane stosują wzmożone środki bezpieczeństwa finansowego w przypadkach wyższego ryzyka prania pieniędzy lub finansowania terroryzmu, a także w przypadkach, o których mowa w art. 44-46 Ustawy. W pozostałych przypadkach, ich stosowanie zależy od ustalonego

przez instytucję obowiązaną poziomu ryzyka prania pieniędzy oraz finansowania terroryzmu.

W art. 43 Ustawy zostały wymienione przypadki, które mogą wskazywać na wyższe ryzyko prania pieniędzy oraz finansowania terroryzmu.

O wyższym ryzyku prania pieniędzy oraz finansowania terroryzmu może świadczyć w szczególności:

1) nawiązywanie stosunków gospodarczych w nietypowych okolicznościach;

2) fakt, że klient jest:

a) osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej, których działalność służy do przechowywania aktywów osobistych,

b) spółką, w której wydano akcje na okaziciela, której papiery wartościowe nie są dopuszczone do obrotu zorganizowanego, lub spółką, w której prawa z akcji lub udziałów są wykonywane przez podmioty inne niż akcjonariusze lub udziałowcy,

c) rezydentem państwa, o którym mowa w pkt 10;

3) przedmiot prowadzonej przez klienta działalności gospodarczej obejmujący przeprowadzanie znacznej liczby lub opiewających na wysokie kwoty transakcji gotówkowych;

4) nietypowa lub nadmiernie złożona struktura własnościowa klienta, biorąc pod uwagę rodzaj i zakres prowadzonej przez niego działalności gospodarczej;

5) korzystanie przez klienta z usług lub produktów oferowanych w ramach bankowości prywatnej;

6) korzystanie przez klienta z usług lub produktów sprzyjających anonimowości lub utrudniających jego identyfikację, w tym z usługi polegającej na tworzeniu dodatkowych numerów rachunków oznaczanych zgodnie z przepisami wydanymi na podstawie art. 68 pkt 3 i 4 ustawy Prawo bankowe[12] oraz art. 4a ust. 5 ustawy. o usługach płatniczych[13], powiązanych z posiadanym rachunkiem, w celu ich udostępniania innym podmiotom do identyfikacji płatności lub zleceniodawców tych płatności;

7) nawiązywanie albo utrzymywanie stosunków gospodarczych lub przeprowadzanie transakcji okazjonalnej bez fizycznej obecności klienta, w przypadku gdy związane z tym wyższe ryzyko prania pieniędzy lub

[12] Ustawa z dnia 29 sierpnia 1997 r. - Prawo bankowe (t.j. Dz.U. z 2026 poz. 38).

[13] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. z 2025 poz.611).

finansowania terroryzmu nie zostało ograniczone w inny sposób, w tym przez użycie środków identyfikacji elektronicznej oraz usług zaufania umożliwiających identyfikację elektroniczną w rozumieniu rozporządzenia w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym[14].

8) zlecanie przez nieznane lub niepowiązane z klientem podmioty trzecie transakcji, których beneficjentem jest klient;

9) objęcie stosunkami gospodarczymi lub transakcjami nowych produktów lub usług albo oferowanie produktów lub usług przy wykorzystaniu nowych kanałów dystrybucji lub nowych rozwiązań technologicznych;

10) powiązanie stosunków gospodarczych lub transakcji okazjonalnej z:

a) państwem trzecim wysokiego ryzyka,

b) państwem określanym przez wiarygodne źródła jako państwo o wysokim poziomie korupcji lub innego rodzaju działalności przestępczej, państwo finansujące lub wspierające popełnianie czynów o charakterze terrorystycznym, lub z którym łączona jest działalność organizacji o charakterze terrorystycznym,

c) państwem, w stosunku do którego Organizacja Narodów Zjednoczonych lub Unia Europejska podjęły decyzję o nałożeniu sankcji lub szczególnych środków ograniczających;

11) powiązanie stosunków gospodarczych lub transakcji okazjonalnej z ropą naftową, bronią, metalami szlachetnymi, produktami tytoniowymi, artefaktami kulturowymi, kością słoniową, gatunkami chronionymi lub innymi przedmiotami o znaczeniu archeologicznym, historycznym, kulturowym i religijnym lub o szczególnej wartości naukowej;

12) powiązanie stosunków gospodarczych lub transakcji okazjonalnej z klientem będącym obywatelem państwa trzeciego i ubiegającym się o prawo pobytu lub obywatelstwo w państwie członkowskim w zamian za transfery kapitałowe, nabycie nieruchomości lub obligacji skarbowych lub inwestycje w podmioty o charakterze korporacyjnym w danym państwie członkowskim.

Bieżąca analiza transakcji, o której mowa w art. 43 ust. 3 Ustawy, powinna być kompletna i uwzględniać wszystkie elementy, o których mowa w art. 43 ust. 4 Ustawy, tzn. powinno się zwracać na te okoliczności szczególną uwagę.

[14] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014…

Pomocny może być również, wspomniany wcześniej, Komunikat nr 31 Generalnego Inspektora[15] .

Zgodnie z art. 43 ust. 4 Ustawy, w przypadku ujawnienia transakcji:

1) skomplikowanych lub

2) opiewających na wysokie kwoty, które nie są uzasadnione okolicznościami przeprowadzenia transakcji lub

3) przeprowadzanych w nietypowy sposób lub

4) wydających się nie mieć uzasadnienia prawnego lub gospodarczego

- instytucje obowiązane podejmują działania w celu wyjaśnienia okoliczności, w jakich przeprowadzono te transakcje oraz, w przypadku transakcji przeprowadzanych w ramach stosunków gospodarczych, intensyfikują stosowanie środka bezpieczeństwa finansowego, o którym mowa w art. 34 ust. 1 pkt 4 Ustawy, w odniesieniu do stosunków gospodarczych, w ramach których te transakcje zostały przeprowadzone.

Podkreślić należy, że w powyższych sytuacjach, podjęcie działań w celu wyjaśnienia okoliczności oraz zintensyfikowanie bieżącego monitorowania stosunków gospodarczych klienta, jest obligatoryjne.

Ustawa nie wskazuje jakie działania ma podjąć instytucja obowiązana, zatem mogą to być zarówno działania własne instytucji, jak i kontakt z klientem.

Zgodnie z art. 41 Ustawy, w przypadku gdy instytucja obowiązana nie może zastosować jednego ze środków bezpieczeństwa finansowego, o których mowa w art. 34 ust. 1 Ustawy:

a) nie nawiązuje stosunków gospodarczych;
b) nie przeprowadza transakcji okazjonalnej;
c) nie przeprowadza transakcji za pośrednictwem rachunku bankowego;
d) rozwiązuje stosunki gospodarcze.

V. Osoby zajmujące eksponowane stanowiska polityczne

Zgodnie z art. 46 Ustawy, instytucje obowiązane mają obowiązek ustalenia, czy klient lub beneficjent rzeczywisty jest osobą zajmującą eksponowane stanowisko polityczne (ang. politically exposed person, dalej jako: PEP) .

[15] Link do Komunikatu: 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

Na podstawie art. 46 ust. 6 Ustawy, przepisy dotyczące PEP stosuje się odpowiednio do członków rodziny osoby zajmującej eksponowane stanowisko polityczne oraz osób znanych jako bliscy współpracownicy takiej osoby.

Zgodnie z art. 2 ust. 2 pkt 11 Ustawy, przez PEP rozumie się, z wyłączeniem grup stanowisk średniego i niższego szczebla, osoby zajmujące znaczące stanowiska publiczne lub pełniące znaczące funkcje publiczne, w tym:

a) szefów państw, szefów rządów, ministrów, wiceministrów oraz sekretarzy stanu;

b) członków parlamentu lub podobnych organów ustawodawczych;

c) członków organów zarządzających partii politycznych;

d) członków sądów najwyższych, trybunałów konstytucyjnych oraz innych organów sądowych wysokiego szczebla, których decyzje nie podlegają zaskarżeniu, z wyjątkiem trybów nadzwyczajnych;

e) członków trybunałów obrachunkowych lub zarządów banków centralnych;

f) ambasadorów, chargés d'affaires oraz wyższych oficerów sił zbrojnych;

g) członków organów administracyjnych, zarządczych lub nadzorczych przedsiębiorstw państwowych, spółek z udziałem Skarbu Państwa, w których ponad połowa akcji albo udziałów należy do Skarbu Państwa lub innych państwowych osób prawnych;

h) dyrektorów, zastępców dyrektorów oraz członków organów organizacji międzynarodowych lub osoby pełniące równoważne funkcje w tych organizacjach;

i) dyrektorów generalnych w urzędach naczelnych i centralnych organów państwowych oraz dyrektorów generalnych urzędów wojewódzkich.

Zgodnie z art. 2 ust. 2 pkt 12 Ustawy, przez osoby znane jako bliscy współpracownicy osoby zajmującej eksponowane stanowisko polityczne rozumie się:

a) osoby fizyczne będące beneficjentami rzeczywistymi osób prawnych, jednostek organizacyjnych nieposiadających osobowości prawnej lub trustów wspólnie z osobą zajmującą eksponowane stanowisko polityczne lub utrzymujące z taką osobą inne bliskie stosunki związane z prowadzoną działalnością gospodarczą;

b) osoby fizyczne będące jedynym beneficjentem rzeczywistym osób prawnych, jednostek organizacyjnych nieposiadających osobowości prawnej lub trustu, o

których wiadomo, że zostały utworzone w celu uzyskania faktycznej korzyści przez osobę zajmującą eksponowane stanowisko polityczne.

Krajowy wykaz stanowisk i funkcji publicznych będących eksponowanymi stanowiskami politycznymi określa rozporządzenie ministra właściwego do spraw finansów publicznych, wydane na podstawie art. 46c Ustawy[16]. Instytucje obowiązane powinny każdorazowo weryfikować aktualne brzmienie tego aktu prawnego i niezwłocznie odzwierciedlać wszelkie zmiany w procedurach i narzędziach weryfikacyjnych.

Ustawa nie narzuca konkretnego sposobu identyfikacji PEP przez instytucje obowiązane, jednakże wymaga wprowadzenia odpowiednich procedur opartych na analizie ryzyka. Ustalony sposób postępowania powinien być zatem dostosowany do charakteru prowadzonej działalności, kategorii instytucji obowiązanej i oparty na zasadzie *risk based approach* (RBA), tzn. identyfikacji, ocenie
i zrozumieniu ryzyka prania pieniędzy i finansowania terroryzmu, na które instytucja jest narażona oraz na podejmowaniu odpowiednich środków ograniczających, zgodnie z poziomem ryzyka.

Ustawa dopuszcza przyjmowanie od klienta oświadczenia w formie pisemnej lub dokumentowej, składanego pod rygorem odpowiedzialności karnej, wraz z wymaganą klauzulą. Oświadczenie klienta nie zwalnia jednak z obowiązku zastosowania, odpowiednio do poziomu ryzyka, niezależnych źródeł weryfikacyjnych, takich jak informacje dostępne publicznie, w tym krajowy wykaz stanowisk PEP oraz wiarygodne komercyjne bazy danych.

W przypadku większych instytucji obowiązanych, zalecane jest stosowanie bardziej zaawansowanych sposobów weryfikacji PEP. Z kolei np. dla instytucji prowadzącej jednoosobową działalność gospodarczą, uzyskanie oświadczenia i sprawdzenie w informacjach dostępnych publicznie, może okazać się wystarczające. W każdym przypadku ważne jest stosowanie metod odpowiednich do poziomu ryzyka danej instytucji obowiązanej.

W przypadku, gdy klient bądź beneficjent rzeczywisty jest PEP (bądź jest współpracownikiem, bądź osobą z rodziny PEP), stosowanie wzmożonych środków bezpieczeństwa finansowego przez instytucję obowiązaną jest obowiązkowe.

Jeżeli ustalono, że klient jest PEP, decyzję o nawiązaniu lub kontynuowaniu stosunków gospodarczych podejmuje, zgodnie z art. 46 ust. 2 pkt 1 Ustawy, kadra kierownicza wyższego szczebla, a następnie instytucja odpowiednio,

[16] Na dzień wydania niniejszych wytycznych, obowiązuje rozporządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 27 lipca 2021 r. w sprawie wykazu krajowych stanowisk i funkcji publicznych będących eksponowanymi stanowiskami politycznymi (t.j. Dz. U. z 2025 r. poz. 502).

zgodnie z art. 46 ust. 2 pkt 2 i 3 Ustawy, ustala źródło majątku i pochodzenia środków oraz stosuje zintensyfikowany monitoring transakcji.

Przy ustalaniu źródła majątku oraz źródła pochodzenia środków, dopuszczalne są oświadczenia i dokumenty klienta oraz publiczne źródła (np. oświadczenia majątkowe, rejestry), przy czym zakres i intensywność weryfikacji wynikają z poziomu ryzyka ustalonego zgodnie z art. 33 Ustawy.

Instytucja obowiązana stosuje wobec osoby, która przestała zajmować eksponowane stanowisko polityczne, środki uwzględniające podwyższone ryzyko jeszcze przez okres co najmniej 12 miesięcy (art. 46 ust. 5 Ustawy). Po upływie tego okresu, instytucja obowiązana dokonuje ponownego rozpoznania i oceny ryzyka prania pieniędzy oraz finansowania terroryzmu związanego ze stosunkami gospodarczymi z tym klientem, dokumentuje wynik tej oceny oraz dostosowuje zakres i intensywność środków bezpieczeństwa finansowego do wyniku oceny(art. 33 ust. 2–4 Ustawy).

Dalsze stosowanie działań właściwych dla PEP, po upływie 12 miesięcy, jest dopuszczalne wyłącznie w przypadku utrzymywania się podwyższonego ryzyka wykazanego tą oceną. Brak przeprowadzenia oceny albo brak stwierdzenia podwyższonego ryzyka, wyklucza kontynuowanie stosowania środków przewidzianych dla PEP.

VI. Centralny Rejestr Beneficjentów Rzeczywistych (CRBR)

Przepisy Unii Europejskiej zobowiązują państwa członkowskie do przechowywania informacji na temat beneficjentów rzeczywistych w centralnym rejestrze oraz do udostępniania tych informacji właściwym organom i jednostkom analityki finansowej, a także podmiotom zobowiązanym (w ramach stosowania środków należytej staranności wobec klienta).

W Polsce, CRBR funkcjonuje na podstawie Ustawy, zgodnie z którą organem właściwym w sprawach CRBR, jest minister właściwy do spraw finansów publicznych, natomiast do wykonywania zadań organu właściwego w sprawach CRBR, został wyznaczony Dyrektor Izby Administracji Skarbowej w Bydgoszczy (art. 55 w zw. z art. 71a Ustawy).

Stosownie do definicji znajdującej się w art. 2 ust. 2 pkt 1 w zw. z art. 58 Ustawy, beneficjent rzeczywisty to każda osoba fizyczna sprawująca bezpośrednio lub pośrednio kontrolę nad podmiotem poprzez posiadane uprawnienia, które wynikają z okoliczności prawnych lub faktycznych, umożliwiające wywieranie decydującego wpływu na czynności lub działania podejmowane przez podmiot, lub w imieniu której są nawiązywane stosunki gospodarcze lub jest przeprowadzana transakcja okazjonalna.

Pełna definicja beneficjenta rzeczywistego znajduje się w art. 2 ust. 2 pkt 1 Ustawy.

Natomiast szczegółowe wyjaśnienia dotyczące CRBR, znajdują się pod adresem: https://www.gov.pl/web/finanse/centralny-rejestr-beneficjentow-rzeczywistych

Instytucje obowiązane, na podstawie art. 34 w zw. z art. 61a Ustawy, dokonują identyfikacji klienta oraz weryfikacji jego tożsamości, a także odnotowują rozbieżności między informacjami zgromadzonymi w CRBR, a ustalonymi przez nią informacjami o beneficjencie rzeczywistym klienta. Należy również pamiętać, że sama weryfikacja, czy dana osoba widnieje w CRBR, jako beneficjent rzeczywisty danego podmiotu, nie jest wystarczająca do dokonania identyfikacji klienta.

Nie ma jednego, powszechnie obowiązującego, wzorca czynności jakie należy wykonać w celu ustalenia kto jest beneficjentem rzeczywistym danego podmiotu. W tym celu pomocne mogą być np. oświadczenia zebrane w ramach stosowania środków bezpieczeństwa finansowego, aktualne umowy, a przede wszystkim inne zgromadzone przez instytucję obowiązaną na rzecz danego klienta informacje, np. wskazanie kto jest faktycznym dysponentem rachunków bankowych prowadzonych na rzecz danego podmiotu, na czyje zlecenie dokonywane są transakcje.

Zawsze należy badać ogół okoliczności, a nie jedynie pojedyncze elementy mogące wskazywać, czy dana osoba jest beneficjentem rzeczywistym danego podmiotu.

Instytucja obowiązana, w przypadku wykrycia i potwierdzenia odnotowanych rozbieżności w CRBR, przekazuje zweryfikowaną informację o tych rozbieżnościach, wraz z uzasadnieniem i dokumentacją dotyczącą odnotowanych rozbieżności. Informacje te mogą być przekazywane za pośrednictwem systemu teleinformatycznego, przy użyciu którego prowadzony jest CRBR (art. 61a Ustawy), jako zgłoszenie pojedynczej albo zbiorowej rozbieżności (dotyczącej dwóch albo więcej podmiotów).

Zasady odnotowywania rozbieżności między informacjami zgromadzonymi w CRBR a ustalonymi przez instytucję obowiązaną informacjami o beneficjencie rzeczywistym klienta, zostały określone w Komunikacje nr 37 Generalnego Inspektora.[17]

[17] Komunikat nr 37 Generalnego Inspektora:

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

Treść wytycznych w zakresie realizacji obowiązku, o którym mowa w art. 61a ust. 1 Ustawy, jest dostępna dla wszystkich instytucji obowiązanych zarejestrowanych w systemie SI*GIIF.

VII. Dokumentowanie działań w zakresie AML

Artykuł 33 ust. 2 i 3 Ustawy wskazuje, że instytucja obowiązana ocenia poziom rozpoznanego ryzyka i dokumentuje czynniki brane pod uwagę przy tej ocenie. Zatem zastosowane przez instytucję obowiązaną środki bezpieczeństwa finansowego, powinny zostać odpowiednio udokumentowane.

Dokumenty uzyskane w związku ze stosowaniem środków bezpieczeństwa finansowego muszą być przechowywane przynajmniej przez okres 5 lat, licząc od dnia zakończenia stosunków gospodarczych z klientem lub od dnia przeprowadzenia transakcji okazjonalnej.

W instytucji obowiązanej powinny funkcjonować procesy analizy i przechowywania każdej otrzymanej informacji o kliencie, uzyskanej w ramach aktualizacji oceny ryzyka prania pieniędzy oraz finansowania terroryzmu, w tym informacji od klienta. Informacje te są uzyskiwane zarówno przy nawiązywaniu relacji, jak i w toku utrzymywania relacji.

Instytucja obowiązana zawsze bierze pod uwagę i dokumentuje wszystkie czynniki określone w art. 33 ust. 3 pkt 1-6 Ustawy, przy czym czynności te nie stanowią katalogu zamkniętego. Instytucja obowiązana powinna dokonać oceny specyfiki swojej działalności i na jej podstawie rozbudowywać listę czynników branych pod uwagę przy ocenie ryzyka.

Instytucja obowiązana nie powinna opierać się wyłącznie na informacjach uzyskiwanych od klienta, ale powinna gromadzić informacje także z innych źródeł, w tym ogólnodostępnych, oraz otrzymanych np. od organów ścigania lub GIIF.

Informacje z innych źródeł powinny służyć także do weryfikowania informacji otrzymywanych od klienta. Instytucja obowiązana, świadcząc usługi w zakresie usługowego prowadzenia ksiąg rachunkowych, ujmuje w księgach rachunkowych i wykazuje w sprawozdaniu finansowym wydarzenia i operacje ekonomiczne, zgodnie ze stanem faktycznym funkcjonowania gospodarczego podmiotu.

Nie jest dopuszczalna sytuacja, w której instytucja obowiązana uzyskując informację o kliencie, umieszcza ją w swojej bazie danych nie oceniając jej pod kątem potencjalnego wpływu na poziom ryzyka prania pieniędzy oraz finansowania terroryzmu, związany z tym klientem.

Oznacza to, że gromadzenie informacji o kliencie przez instytucję obowiązaną, nie może funkcjonować w oderwaniu od obowiązku oceny takiej informacji pod kątem tego, czy wpływa ona na ryzyko prania pieniędzy oraz finansowania terroryzmu.

W sprawie oceniania informacji uzyskiwanych o klientach przez instytucje obowiązane i działań w przypadku braku możliwości zastosowania środków bezpieczeństwa finansowego, Generalny Inspektor wydał Komunikat nr 45[18].

VIII. Wewnętrzna procedura w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu

Instytucje obowiązane wprowadzają wewnętrzną procedurę w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, zwaną dalej "wewnętrzną procedurą". Wewnętrzna procedura podlega bieżącej weryfikacji oraz, w razie potrzeby, aktualizacji.

Wewnętrzna procedura określa, z uwzględnieniem charakteru, rodzaju i rozmiaru prowadzonej działalności, zasady postępowania stosowane w instytucji obowiązanej i obejmuje w szczególności określenie:

a) czynności lub działań podejmowanych w celu ograniczenia ryzyka prania pieniędzy oraz finansowania terroryzmu i właściwego zarządzania zidentyfikowanym ryzykiem prania pieniędzy lub finansowania terroryzmu;

b) zasad rozpoznawania i oceny ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z danymi stosunkami gospodarczymi lub transakcją okazjonalną, w tym zasad weryfikacji i aktualizacji uprzednio dokonanej oceny ryzyka prania pieniędzy oraz finansowania terroryzmu;

c) środków stosowanych w celu właściwego zarządzania rozpoznanym ryzykiem prania pieniędzy lub finansowania terroryzmu związanym z danymi stosunkami gospodarczymi lub transakcją okazjonalną;

d) zasad stosowania środków bezpieczeństwa finansowego;

e) zasad przechowywania dokumentów oraz informacji;

[18] Komunikat nr 45 Generalnego Inspektora: 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.

f) zasad wykonywania obowiązków obejmujących przekazywanie Generalnemu Inspektorowi informacji o transakcjach oraz zawiadomieniach;

g) zasad upowszechniania wśród pracowników instytucji obowiązanej wiedzy z zakresu przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu;

h) zasad zgłaszania przez pracowników rzeczywistych lub potencjalnych naruszeń przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;

i) zasad kontroli wewnętrznej lub nadzoru zgodności działalności instytucji obowiązanej z przepisami o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz zasadami postępowania określonymi w wewnętrznej procedurze;

j) zasad odnotowywania rozbieżności między informacjami zgromadzonymi w Centralnym Rejestrze Beneficjentów Rzeczywistych a informacjami o beneficjentach rzeczywistych klienta ustalonymi w związku ze stosowaniem ustawy;

k) zasad dokumentowania utrudnień stwierdzonych w związku z weryfikacją tożsamości beneficjenta rzeczywistego oraz czynności podejmowanych w związku z identyfikacją jako beneficjenta rzeczywistego osoby fizycznej zajmującej wyższe stanowisko kierownicze.

Wewnętrzna procedura lub jej aktualizacja, przed wprowadzeniem do stosowania, podlega akceptacji przez kadrę kierowniczą wyższego szczebla.

Wewnętrzna procedura powinna zawierać konkretne zapisy działań podejmowanych przez instytucję obowiązaną w zakresie przeciwdziałania praniu pieniędzy oraz finasowaniu terroryzmu. Wewnętrzna procedura powinna być spójna z oceną ryzyka instytucji obowiązanej oraz podejmowanymi przez instytucję działaniami w obszarze przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Celem wewnętrznej procedury jest podniesienie poziomu bezpieczeństwa finansowego i zminimalizowania ryzyka oszustw, prania pieniędzy i finansowania terroryzmu, a także ich wykrywanie poprzez identyfikowanie nietypowych zachowań klientów instytucji obowiązanej oraz monitorowanie podejrzanych transakcji i zachowań klientów instytucji obowiązanej.

Wszyscy pracownicy instytucji obowiązanej powinni zapoznać się z wewnętrzną procedurą, a fakt ten powinien być udokumentowany.

IX. Szkolenie pracowników

W ramach realizacji obowiązku szkoleniowego, określonego w art. 52 Ustawy, instytucja obowiązana powinna zapewnić udział osób wykonujących obowiązki związane z przeciwdziałaniem praniu pieniędzy i finansowaniem terroryzmu (AML / CFT) w szkoleniach dotyczących realizacji tych obowiązków, z uwzględnieniem tematyki ochrony danych osobowych.

Ważne jest, żeby wdrażanie programów szkoleniowych i podnoszenie kompetencji ww. osób było ciągłym procesem, a nie tylko jednorazowym działaniem.

Szkolenia powinny być dopasowane do charakteru, rodzaju i rozmiaru działalności instytucji obowiązanej i koncentrować się przede wszystkim na aspektach praktycznych.

W przypadku instytucji obowiązanej działającej jako osoba fizyczna prowadząca jednoosobową działalność gospodarczą, wypełnienie ustawowego obowiązku szkoleniowego jest możliwe wyłącznie poprzez udział w szkoleniach realizowanych przez podmiot zewnętrzny.

Szkolenia osób wykonujących zadania z zakresu przeciwdziałania praniu pieniędzy i finansowania terroryzmu mogą odbywać się wewnątrz instytucji obowiązanej oraz w ramach zewnętrznych programów szkoleniowych, zarówno w formie stacjonarnej, jak i online.

Realizacja obowiązku szkoleniowego powinna być rzetelnie udokumentowana. Z dokumentów potwierdzających udział w szkoleniu powinno jednoznacznie wynikać, kto, kiedy, w jakim zakresie i przez kogo został przeszkolony.

Generalny Inspektor wydał komunikat dotyczący realizacji obowiązku szkoleniowego[19].

X. Informacje przekazywane przez instytucje obowiązane na podstawie art. 72 Ustawy

Instytucje obowiązane przekazują Generalnemu Inspektorowi informacje m.in. o:

1. przyjętej wpłacie lub dokonanej wypłacie środków pieniężnych o równowartości przekraczającej 15 000 euro;

[19] Komunikat nr 92 Generalnego Inspektora:

https://www.gov.pl/web/finanse/komunikat-nr-92-w-sprawie-obowiazku-szkoleniowego-okreslonego-w-ustawie-aml--komunikat-giif-uknf-i-nbp

2. wykonanym transferze środków pieniężnych o równowartości przekraczającej 15 000 euro.

W przypadku określonym w art. 72 ust. 1 pkt 1 Ustawy, instytucje obowiązane raportują do Generalnego Inspektora informacje o przyjętej wpłacie lub dokonanej wypłacie środków pieniężnych o równowartości przekraczającej 15 000 euro tj. o wpłacie gotówki przyjętej od klienta przez ww. instytucję obowiązaną lub wypłacie gotówki dokonanej przez ww. instytucję obowiązaną na rzecz klienta. W przypadku gdy instytucja obowiązana dokonała wpłaty albo wypłaty, jest zobowiązana do raportowania transakcji.

W przypadku wskazanym w art. 72 ust.1 pkt 2 Ustawy, należy w pierwszej kolejności ustalić, czy instytucje obowiązane, o których mowa w art. 2 ust. 1 pkt 17 Ustawy, wykonują transfery środków pieniężnych.

Zgodnie z zawartą w art. 2 ust. 2 pkt 23 Ustawy definicją, transferem środków pieniężnych jest transfer środków pieniężnych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1113 ws. informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów (…) [20].

Instytucje obowiązane, o których mowa w art. 2 ust. 1 pkt 14, 15, 15a i 17 Ustawy, nie są dostawcami usług płatniczych w rozumieniu przepisów ww. rozporządzenia 2015/847. Zatem nie mogą one realizować transferów środków pieniężnych.

W konsekwencji, instytucje obowiązane, o których mowa w art. 2 ust. 1 pkt 14, 15, 15a i 17 Ustawy, które z założenia nie dokonują transakcji wpłaty i wypłaty gotówki, a także nie wykonują transferów środków pieniężnych (choć mogą mieć o nich wiedzę w związku z wykonywaniem usług na rzecz swoich klientów), nie są zobowiązane do raportowania[21] do Generalnego Inspektora informacji, o którym mowa w art. 72 ust. 1 pkt 1 i 2 ww. Ustawy.

XI. Rozpoznawanie i zgłaszanie transakcji podejrzanych do GIIF

Definicję transakcji zawiera art. 2 pkt 21 Ustawy, zgodnie z którym „transakcja" to czynność prawna lub faktyczna, na podstawie której dokonuje się przeniesienia własności lub posiadania wartości majątkowych, lub czynność prawna lub faktyczna dokonywana w celu przeniesienia własności lub posiadania wartości majątkowych.

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849 (Dz.U.UE.L.2023.150.1).

[21] Dodatkowe informacje dotyczące raportowania transakcji można znaleźć w Komunikacie nr 11 Generalnego Inspektora:

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.

Identyfikacja transakcji nietypowych lub transakcji, których okoliczności wskazują, że mogą mieć one związek z praniem pieniędzy lub finansowaniem terroryzmu, nie jest objęta konkretnym wzorcem. Podejrzenie co do przestępczego charakteru danej transakcji, musi mieć uzasadniony charakter, np. gdy transakcja jest niespójna z dotychczasowym sposobem działania klienta, źródło przychodów jest nietypowe, wartość obrotów jest nieproporcjonalnie wysoka w stosunku do zaplecza finansowego, jakim dysponuje dany podmiot, lub gdy częstotliwość danego działania nagle wzrasta.

Należy też zwrócić uwagę na transakcje, które są często realizowane przez dany podmiot, np. przyjmowana jest duża ilość gotówki, występują przelewy przychodzące od podmiotów lub są zlecane na rzecz podmiotów, co do których nie ma uzasadnienia ekonomicznego w zakresie dokonywania z nimi transakcji.

Należy też zwrócić szczególną uwagę na transakcje realizowane wbrew przepisom obowiązującego prawa, np. wbrew przepisom ustawy Prawo bankowe. Przykładem takiej transakcji jest sytuacja, w której z rachunku VAT[22] podmiotu dokonywane są płatności kwot netto za poszczególne faktury, czy też transferowane są środki w ramach pożyczek, a także gdy celowo dzielone są zapłaty za faktury. W ostatnim przypadku chodzi o faktyczne zlecanie lub przyjmowanie kilku przelewów dotyczących zapłaty za jedną fakturę, przy czym przelewy te są wykonywane w taki sposób, że łącznie z rachunku VAT jest płacona inna kwota, niż wynikająca z faktury kwota podatku.

W celu zobrazowania występowania ryzyka prania pieniędzy i finansowania terroryzmu w przypadku transakcji, mogą być pomocne poniższe przykłady.

<u>Przykład nr 1</u>

Transakcje realizowane z naruszeniem art. 62b ust. 1 i 2 ustawy Prawo bankowe (uznanie i obciążenie rachunku VAT).

Załóżmy sytuację w której przelewy realizowane przez podmiot A za faktury, powinny być realizowane z zastosowaniem mechanizmu podzielonej płatności (MPP, split payment).
Zarówno podmiot A, jak i jego dostawcy są czynnymi podatnikami VAT, a zakupy służą czynnościom opodatkowanym, przy czym na rachunkach prowadzonych na rzecz podmiotu A odnotowano przelewy realizowane z zachowaniem mechanizmu MPP, ale także, np.:

a. transakcje realizowane z pominięciem metody split-payment,

[22] Objaśnienia co do transakcji, jakie powinny być realizowane w ramach rachunku VAT, można znaleźć pod adresem: https://www.podatki.gov.pl/podatki-firmowe/vat/poradniki-i-informatory/mechanizm-podzielonej-platnosci-mpp/

b. dzielenie płatności za daną fakturę na kilka części, co znacznie utrudnia analizę prawidłowości zapłat realizowanych z udziałem rachunków VAT podmiotu A,

c. realizację przelewów za fakturę, w których kwoty jakie wskazywano jako podatek VAT w związku z płaconymi fakturami, nie odpowiadały kwotom wskazanym na tych fakturach, np. w skutek dzielenia zapłaty za jedną fakturę, łącznie przekazywana jest kwota np. 126 690,00 PLN, z czego z rachunku VAT 108 300,00 PLN, co stanowi 85,3 % całości zapłaty,

d. transakcje realizowane z zastosowaniem metody split-payment, przy czym 100% zapłaty pochodzi z rachunku VAT, jako zapłata zobowiązań w postaci zawartych umów np. spłaty pożyczek.

Finalnie, deklarowani dostawcy podmiotu A otrzymywali płatności w zw. z wystawianymi dokumentami, jednakże środki z rachunku VAT podmiotu A nie powinny być przeznaczone na zapłatę kwot netto faktur lub na płatność w związku z realizowanymi umowami. Ten sposób realizowania płatności pozwala na wykorzystanie środków zgromadzonych na rachunku VAT w sposób niezgodny z art. 62b ust. 2 pkt 1 ustawy Prawo bankowe.

Powyższe może świadczyć o wyprowadzaniu środków z rachunku VAT prowadzonego na rzecz podmiotu A poprzez mechanizm split payment, tj. „uwolnienie" środków z rachunku VAT kupującego (A), i przekazaniu tak uwolnionej części tych środków (w ww. przykładzie na rzecz dostawcy) do dowolnej dyspozycji, już bez nałożenia ograniczeń wynikających z ustawy Prawo bankowe dotyczących realizacji płatności z rachunku VAT.
W takim przypadku, istnieje wysokie prawdopodobieństwo prania pieniędzy za pośrednictwem rachunków bankowych prowadzonych na rzecz podmiotu A, a także podmiotów na rzecz których podmiot A transferuje „uwolnione" w ten sposób środki pieniężne.

<u>Przykład nr 2</u>

Transakcje realizowane przelewami zlecanymi, poza zwykłymi sesjami określonymi przez dany bank.

W tym przypadku chodzi o przelewy, które są realizowane natychmiastowo, w wyniku czego środki pieniężne są transferowane na rzecz innych podmiotów. Takie działania zazwyczaj nie są wyjątkiem, a regułą, pomimo że wymagają one dodatkowej zapłaty prowizji i opłat bankowych. Faktycznym celem takich transakcji nie jest zapłata za rzeczywiste zdarzenie gospodarcze, a przerzut

środków pieniężnych pomiędzy rachunkami w celu prania pieniędzy lub finansowania terroryzmu.

Instytucje obowiązane, które zidentyfikowały podejrzane transakcje u swoich klientów, zobowiązane są do ich zaraportowania do Generalnego Inspektora za pośrednictwem:

1) systemu teleinformatycznego Generalnego Inspektora (SI*GIIF), dostępnego pod adresem: www.giif.mofnet.gov.pl

   lub

2) poczty, na adres:

   Departament Informacji Finansowej
   Ministerstwo Finansów
   ul. Świętokrzyska 12
   00-916 Warszawa.

W Ustawie wyróżniono 3 tryby raportowania transakcji do Generalnego Inspektora – na podstawie art. 74, art. 86 i art. 90.

1) Zawiadomienie w trybie art. 74 dotyczy transakcji, co do których instytucja obowiązana powzięła uzasadnione podejrzenie, że są one przeprowadzane w okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu.

W zawiadomieniu podaje się:

a) dane identyfikacyjne, o których mowa w art. 36 ust. 1 Ustawy, klienta instytucji obowiązanej przekazującej zawiadomienie;

b) posiadane dane identyfikacyjne, o których mowa w art. 36 ust. 1 Ustawy, osób fizycznych, osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej, niebędących klientami instytucji obowiązanej przekazującej zawiadomienie;

c) rodzaj i wielkość wartości majątkowych oraz miejsce ich przechowywania;

d) numer rachunku prowadzonego dla klienta instytucji obowiązanej przekazującej zawiadomienie, oznaczony identyfikatorem IBAN lub identyfikatorem zawierającym kod kraju oraz numer rachunku w przypadku rachunków nieoznaczonych IBAN;

e) posiadane informacje, o których mowa w art. 72 ust. 6 Ustawy, w odniesieniu do transakcji lub prób ich przeprowadzenia;

f) wskazanie państwa Europejskiego Obszaru Gospodarczego, z którym jest powiązana transakcja, jeżeli została przeprowadzona w ramach działalności transgranicznej;

g) posiadane informacje o rozpoznanym ryzyku prania pieniędzy lub finansowania terroryzmu oraz o czynie zabronionym, z którego mogą pochodzić wartości majątkowe;

h) uzasadnienie przekazania zawiadomienia.

2) Zawiadomienie w trybie art. 86 dotyczy transakcji wstrzymanych przez instytucję obowiązaną, co do których powzięła ona uzasadnione podejrzenie, że określona transakcja lub określone wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu.

W zawiadomieniu instytucja obowiązana przekazuje pozostające w jej posiadaniu informacje związane z powziętym podejrzeniem oraz informację o przewidywanym terminie przeprowadzenia transakcji.

3) Zawiadomienie w trybie art. 90 zawiera informację o przeprowadzeniu transakcji, o której mowa w art. 86 Ustawy, w przypadku gdy przekazanie zawiadomienia było niemożliwe przed jej przeprowadzeniem.

W tym przypadku, instytucja obowiązana uzasadnia w zawiadomieniu przyczyny nieprzekazania wcześniej zawiadomienia oraz przekazuje pozostające w jej posiadaniu informacje potwierdzające powzięcie podejrzenia, o którym mowa w art. 86 Ustawy, przy czym zawiadomienie to zawiera analogiczne elementy jak w przypadku zawiadomienia z art. 74 Ustawy.

XII. Szczególne środki ograniczające i sankcje międzynarodowe[23]

Obowiązek stosowania szczególnych środków ograniczających wobec osób i podmiotów znajdujących się na listach ogłaszanych przez GIIF na podstawie rezolucji Rady Bezpieczeństwa ONZ oraz na liście sankcyjnej prowadzonej przez GIIF, spoczywa na każdej instytucji obowiązanej.

Listy te są dostępne na stronie internetowej GIIF, w zakładce „sankcje międzynarodowe”.

[23] Więcej informacji nt. zasad dot. stosowania szczególnych środków ograniczających, w szczególności w kontekście sankcji międzynarodowych, można znaleźć m.in. w Komunikacie Generalnego Inspektora ws. nowych zasad stosowania szczególnych środków ograniczających:

file:///d:/HXPY/Downloads/komunikat_w_sprawie_nowych_zasad_stosowania_sankcji-1.pdf.

Szczególne środki ograniczające polegają na zamrażaniu wartości majątkowych oraz nieudostępnianiu ich osobom i podmiotom wskazanym na ww. liście lub listach.

Zamrożenie wartości majątkowych dotyczy wartości będących własnością, posiadanych, kontrolowanych pośrednio oraz bezpośrednio przez osoby i podmioty wskazane na liście lub listach, a także korzyści pochodzących z tych wartości.

Natomiast zakaz udostępniania wartości majątkowych obejmuje także zakaz pośredniego ich udostępniania osobom wskazanym na liście lub listach (w szczególności m.in. niedokonywanie płatności za towary lub usługi oraz niedokonywanie darowizn).

W przypadku zastosowania szczególnych środków ograniczających, instytucje obowiązane zobligowane są przekazać stosowną informację do GIIF niezwłocznie, jednak nie później niż w terminie 2 dni roboczych od ich zastosowania.

Instytucja obowiązana powinna sprawdzać swoich klientów również na liście osób i podmiotów objętych sankcjami w związku z wojną na Ukrainie, opublikowanej na stronie internetowej Ministerstwa Spraw Wewnętrznych i Administracji.

Sprawdzanie klientów na listach sankcyjnych powinno być dokonywane przed nawiązaniem stosunków gospodarczych oraz okresowo, z częstotliwością uwzględniającą rodzaj prowadzonej działalności, strukturę klientów, oraz przypisany poziom ryzyka, a także zgodnie z zasadami określonymi w wewnętrznej procedurze danej instytucji obowiązanej.