

INSTRUKCJA PRZECIWDZIAŁANIA PRANIU PIENIĘDZY ORAZ FINANSOWANIU TERRORYZMU

I. POSTANOWIENIA OGÓLNE

1. Cel i podstawy prawne Instrukcji

1) Celem Instrukcji jest określenie i sprecyzowanie przyjętych przez **Instytucję obowiązaną/ Przedsiębiorcę** zasad wewnętrznych działań, ukierunkowanych na przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Ilekroć w niniejszej Instrukcji jest mowa o przeciwdziałaniu praniu pieniędzy, jej zapisy odnoszą się również do przeciwdziałania finansowaniu terroryzmu.

2) Postanowienia Instrukcji oparte są o obowiązujące uregulowania prawne:

- ustawy z dnia 01 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2018 r. poz. 723), dalej zwanej **USTAWĄ**, która stanowi załącznik nr 1 do niniejszej Instrukcji;
- art. 299 ustawy z dnia 6 czerwca 1997 roku - Kodeks karny (Dz. U. Nr 88, poz. 553 z późn. zm.);
- rozporządzenia Ministra Finansów z dnia 21 września 2001 r. w sprawie określenia wzoru rejestru transakcji, sposobu jego prowadzenia oraz trybu dostarczania danych z rejestru Generalnemu Inspektorowi Informacji Finansowej (Dz. U. Nr 113, poz. 1210), zwane dalej **ROZPORZĄDZENIEM**, które stanowi załącznik nr 2 do niniejszej Instrukcji,
- rozporządzenia Ministra Finansów z dnia 16 maja 2005 r. w sprawie określenia krajów i terytoriów stosujących szkodliwą konkurencję podatkową;
- rozporządzenia (WE) Nr 1781/2006 Parlamentu Europejskiego i Rady z dnia 15 listopada 2006r. w sprawie informacji o zleceniodawcach, które towarzyszą przekazom pieniężnym (Dz. U. UE nr L345 z dnia 08.12.2006 r.),
- dyrektywy 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu oraz przepisów ustanawiających środki wykonawcze do tej Dyrektywy.

2. Przez użyte w niniejszej Instrukcji określenia należy rozumieć:

- 1) **bank fikcyjny** – rozumie się przez to podmiot świadczący usługi finansowe lub prowadzący równoważną działalność, utworzony na terytorium państwa, w którym nie posiada siedziby, w taki sposób, aby występowało rzeczywiste zarządzanie nim i kierowanie oraz który to podmiot nie jest stowarzyszony z grupą finansową działającą w sposób prawnie,
- 2) **beneficjent transakcji** – podmiot, na rzecz którego następuje przysporzenie majątkowe,
- 3) **beneficjent rzeczywisty** - rozumie się przez to:
 - a. osobę fizyczną lub osoby fizyczne, które są właścicielami osoby prawnej lub sprawują kontrolę nad klientem albo mają wpływ na osobę fizyczną, w imieniu której przeprowadzana jest transakcja lub prowadzona jest działalność,
 - b. osobę fizyczną lub osoby fizyczne, które są udziałowcami lub akcjonariuszami lub posiadają prawo głosu na zgromadzeniu wspólników w wysokości powyżej 25 % w tej osobie prawnej, w tym za pomocą pakietów akcji na okaziciela, z wyjątkiem spółek, których papiery wartościowe są w obrocie zorganizowanym, podlegających lub stosujących przepisy prawa Unii Europejskiej w zakresie ujawniania

informacji, a także podmiotów świadczących usługi finansowe na terytorium państwa członkowskiego Unii Europejskiej albo państwa równoważnego - w przypadku osób prawnych,

c. osobę fizyczną lub osoby fizyczne, które sprawują kontrolę nad co najmniej 25 % majątku - w przypadku podmiotów, którym powierzono administrowanie wartościami majątkowymi oraz rozdzielanie takich wartości, z wyjątkiem podmiotów wykonujących czynności, o których mowa w art. 69 ust. 2 pkt. 4 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi;

4) **blokada rachunku** – czasowe uniemożliwienie dysponowania i korzystania ze wszystkich wartości majątkowych zgromadzonych na rachunku, w tym również przez instytucję obowiązana,

5) **Instytucja obowiązana** - instytucje płatnicze, biura usług płatniczych oraz ich agenci w rozumieniu ustawy o usługach płatniczych,

6) **Koordynator** - osoba odpowiedzialna za koordynację całości zadań związanych z zapobieganiem praniu pieniędzy oraz przeciwdziałaniem finansowaniu terroryzmu w instytucji obowiązanej.

7) **osoby zajmujące eksponowane stanowiska polityczne (PEP)** – rozumie się przez to osoby fizyczne:

a. szefów państw, szefów rządów, ministrów, wiceministrów lub zastępców ministrów, członków parlamentu, sędziów sądów najwyższych, trybunałów konstytucyjnych oraz innych organów sądowych, których orzeczenia nie podlegają zaskarżeniu, z wyjątkiem trybów nadzwyczajnych, członków trybunałów obrachunkowych, członków zarządów banków centralnych, ambasadorów, *chargés d'affaires* oraz wyższych oficerów sił zbrojnych, członków organów zarządzających lub nadzorczych przedsiębiorstw państwowych – którzy sprawują lub sprawowali te funkcje publiczne w okresie roku od dnia zaprzestania spełniania przesłanek określonych w tych przepisach,

b. małżonków osób, o których mowa w lit. a, lub osoby pozostające z nimi we wspólnym pożyciu, rodziców i dzieci osób, o których mowa w lit. a, małżonków tych rodziców i dzieci lub osoby pozostające z nimi we wspólnym pożyciu,

c. które pozostają lub pozostawały z osobami, o których mowa w lit. a, w ścisłej współpracy zawodowej lub gospodarczej lub są współwłaścicielami podmiotów prawa, a także jedynymi uprawnionymi do majątku podmiotów prawa, jeżeli zostały one założone na rzecz tych osób

- **mające miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej;**

8) **pranie pieniędzy** - rozumie się przez to zamierzone postępowanie polegające na:

a. zamianie lub przekazaniu wartości majątkowych pochodzących z działalności o charakterze przestępczym lub z udziału w takiej działalności, w celu ukrycia lub zatajenia bezprawnego pochodzenia tych wartości majątkowych albo udzieleniu pomocy osobie, która bierze udział w takiej działalności w celu uniknięcia przez nią prawnych konsekwencji tych działań,

b. ukryciu lub zatajeniu prawdziwego charakteru wartości majątkowych lub praw związanych z nimi, ich źródła, miejsca przechowywania, rozporządzania, faktu ich przemieszczania, ze świadomością, że wartości te pochodzą z działalności o charakterze przestępczym lub udziału w takiej działalności,

c. nabyciu, objęciu w posiadanie albo używaniu wartości majątkowych pochodzących z działalności o charakterze przestępczym lub udziału w takiej działalności,

- d. współdziałaniu, usiłowaniu popełnienia, pomocnictwie lub podżeganiu w przypadkach zachowań określonych w lit. a-c - również jeżeli działania, w ramach których uzyskano wartości majątkowe, były prowadzone na terytorium innego państwa niż Rzeczpospolita Polska;
- 9) **przekaz pieniężny** - oznacza transakcję realizowaną drogą elektroniczną przez dostawcę usług płatniczych w imieniu zleceniodawcy, w celu udostępnienia środków odbiorcy obsługiwaneemu przez dostawcę usług płatniczych, bez względu na to, czy zleceniodawca i odbiorca jest tą samą osobą.
- 10) **rejestr Prania** - rejestr transakcji w kwotach powyżej równowartości 15.000 Euro, transakcji powiązanych oraz transakcji podejrzanych, dokonywanych przez klientów,
- 11) **transakcje** - dokonywane we własnym jak i cudzym imieniu, na własny jak i cudzy rachunek:
- a. wpłaty i wypłaty w formie gotówkowej lub bezgotówkowej, w tym także przekazy pieniężne, zleczone zarówno na obszarze Rzeczypospolitej Polskiej jak i poza nim,
- b. kupno i sprzedaż wartości dewizowych,
- c. przeniesienie własności lub posiadania wartości majątkowych, w tym oddanie w komis lub pod zastaw takich wartości oraz przeniesienie wartości majątkowych pomiędzy rachunkami należącymi do tego samego Klienta,
- d. zamianę wierzytelności na akcje lub udziały.
- 12) **wartości majątkowe** – środki płatnicze, instrumenty finansowe, w rozumieniu art. 2 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, a także inne papiery wartościowe lub wartości dewizowe, prawa majątkowe, rzeczy ruchome oraz nieruchomości,
- 13) **wstrzymanie transakcji** – czasowe ograniczenie dysponowania i korzystania z wartości majątkowych, polegające na uniemożliwieniu dokonania określonej transakcji przez instytucję obowiązaną,
- 14) **zamrażanie** – rozumie się przez to zapobieganie przenoszeniu, zmianie, wykorzystaniu wartości majątkowych lub przeprowadzaniu transakcji w jakikolwiek sposób, który może spowodować zmianę ich wielkości, wartości, miejsca, własności, posiadania, charakteru, przeznaczenia lub jakąkolwiek inną zmianę, która może umożliwić korzystanie z wartości majątkowych.

II. FUNKCJE I ZADANIA OSÓB WYZNACZONYCH DO REALIZACJI PROGRAMU

1. Dla uniknięcia wykorzystania Przedsiębiorcy w procederze prania pieniędzy i finansowania terroryzmu jak również w celu realizacji obowiązków wynikających z obowiązujących przepisów, dokonuje się w szczególności następujących czynności, opisanych w dalszej części Instrukcji:
- 1) wyznaczenie osoby odpowiedzialnej (Koordynatora) za wykonywanie obowiązków określonych w Ustawie i Instrukcji, w tym w szczególności:
- identyfikację klientów,
 - prowadzenie rejestru transakcji i rejestrowanie transakcji,
 - monitorowanie transakcji, analizę ryzyka transakcji i typowanie transakcji podejrzanych,
 - przekazywanie do GIFF informacji o zarejestrowanych transakcjach,

- zgłaszanie do GIIF transakcji podejrzanych oraz tam, gdzie zachodzi taka konieczność wstrzymywanie realizacji transakcji podejrzanych,
- współpraca z GIIF w zakresie prowadzonej korespondencji dotyczącej w szczególności kierowanych do Przedsiębiorcy zapytań o klientów, a także w ramach uprawnień kontrolnych GIIF,

2) szkolenia osób odpowiedzialnych za przeciwdziałanie praniu pieniędzy.

2. W celu właściwej realizacji obowiązków wyznaczony członek Zarządu/ właściciel firmy w drodze uchwały może wyznaczyć spośród podległych sobie pracowników **analityka** odpowiedzialnego za prowadzenie cyklicznych analiz oraz wprowadzających dane do rejestru transakcji.
3. Koordynator kontroluje realizację przepisów Instrukcji i co najmniej raz w roku informuje wyznaczonego członka Zarządu o wynikach przeprowadzonej przez siebie kontroli.

III. ZASADY REJESTRACJI TRANSAKCJI I PROWADZENIA REJESTRU

1. Obowiązek identyfikacji i rejestracji dotyczy transakcji, których wartość przekracza równowartości 15 tys. Euro oraz transakcji podejrzanych i powiązanych.

2. Zasady rejestracji transakcji

Pracownik jednostki operacyjnej przeprowadzający transakcję:

- a. której równowartość przekracza 15 000 Euro,
- b. w drodze więcej niż jednej operacji, których okoliczności wskazują, że są one ze sobą powiązane,
- c. której okoliczności wskazują, że może ona mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, bez względu na jej wartość i charakter –

ma obowiązek zarejestrować taką transakcję w rejestrze w momencie jej przeprowadzenia, najpóźniej następnego dnia roboczego.

3. Przy ustalaniu równowartości w Euro, stosuje się średni kurs Narodowego Banku Polskiego dla danej waluty, obowiązujący w dniu dokonywania transakcji lub w dniu złożenia dyspozycji (zlecenia) przeprowadzenia transakcji.
4. Rejestr składa się z zapisów elektronicznych sporządzanych oddzielnie dla każdej rejestrowanej transakcji. Prowadzony jest w systemie informatycznym, umożliwiającym niezwłoczny odczyt lub wydruk całości lub części zapisanych danych. Raz wprowadzonych zapisów nie można zlikwidować, a ewentualne błędy poprawiane są za pomocą zapisu korygującego.
5. Informacje o transakcjach zarejestrowanych powinny zawierać w szczególności następujące dane:

- datę przeprowadzenia transakcji;
- dane identyfikacyjne stron transakcji, o których mowa w rozdziale VIII ust.4 niniejszej Instrukcji;
- kwotę, walutę i rodzaj transakcji;
- numery rachunków, które zostały wykorzystane do przeprowadzenia transakcji, w przypadku transakcji z udziałem takich rachunków;
- uzasadnienie oraz miejsce, datę i sposób złożenia dyspozycji w przypadku przekazywania informacji o transakcji podejrzanej.

IV. ZASADY PRZEKAZYWANIA INFORMACJI DO GIIF

1. Koordynator przekazuje informacje o zarejestrowanych transakcjach do GIIF, wykorzystując elektroniczne nośniki informacji. Przekazywane dane opatrzone są bezpiecznym podpisem elektronicznym.
2. Informacje o transakcjach zarejestrowanych w rejestrze przekazywane są do GIIF:
 - a. w terminie 14 dni po upływie każdego miesiąca kalendarzowego – w przypadku transakcji powyżej równowartości 15.000 Euro oraz powiązanych,
 - b. niezwłocznie - w przypadku transakcji podejrzanych.
3. W przypadku stwierdzenia błędów w dostarczonych informacjach z rejestru, Koordynator przekazuje GIIF, w terminie 7 dni od dnia ich ujawnienia, skorygowane dane.
4. GIIF może zażądać ponownego przekazania danych w przypadku, gdy stwierdzi, że otrzymana przesyłka jest uszkodzona lub dane z rejestru zostały przekazane z naruszeniem trybu ustalonego w Rozporządzeniu. W takim przypadku analityk przekazuje niezwłocznie żądane informacje nie później niż w ciągu 3 dni roboczych od daty wpływu żądania.

V. TYPOWANIE TRANSAKЦИИ PODEJRZANYCH

1. Przez obowiązek typowania transakcji podejrzanych należy rozumieć obowiązek zwracania uwagi przez Koordynatora lub Analityka i informowania Koordynatora o transakcjach, których cechy świadczą o tym, że transakcje te mogą zostać uznane za nietypowe, niestandardowe dla klienta – transakcje niespójne z znanym i ustalonym profilem transakcyjnym klienta biorąc pod uwagę np. wartość przeprowadzanej transakcji, kierunek transferu, czy częstotliwość.
2. Szczególny obowiązek typowania oraz stosowania metod typowania transakcji podejrzanych ciąży na Koordynatorze lub Kontrolerze.

VI. POSTĘPOWANIE W PRZYPADKU WYKRYCIA TRANSAKЦИИ PODEJRZANEJ

1. Każdy pracownik Przedsiębiorcy w przypadku powzięcia podejrzenia, iż planowana, realizowana bądź zrealizowana transakcja ma na celu pranie pieniędzy, ma bezwzględny obowiązek bezwzględnego zgłoszenia tego faktu na piśmie, w formie notatki służbowej Koordynatorowi.
2. Notatka służbowa, o której mowa w ust.1, winna zawierać opis transakcji pozwalający na jej identyfikację oraz wskazanie uzasadnionego podejrzenia transakcji wraz z uzasadnieniem.
3. Koordynator w porozumieniu z członkiem Zarządu/właścicielem, podejmuje decyzję co do uznania transakcji za podejrzaną i przekazania stosownej informacji do GIIF.
4. Pozytywna decyzja, co do uznania transakcji za podejrzaną, skutkuje koniecznością dokonania przez Koordynatora odpowiednich wpisów dotyczących przedmiotowej transakcji w rejestrze i powiadomienia GIIF.
5. Ujawnienie osobom nieuprawnionym, w tym także stronom transakcji lub posiadaczom rachunku, faktu poinformowania Generalnego Inspektora o transakcjach, których okoliczności wskazują, że wartości majątkowe mogą pochodzić z prania pieniędzy albo o rachunkach podmiotów, co do których zachodzi uzasadnione podejrzenie, że mają związek z finansowaniem terroryzmu oraz o transakcjach dokonywanych przez te podmioty, jest zabronione.

6. W przypadku podjętej decyzji przez Koordynatora po ewentualnych uzgodnieniach z członkiem Zarządu/właścicielem co do uznania transakcji za podejrzaną Koordynator niezwłocznie przekazuje informacje o tym fakcie do GIIF.

VII. PROCEDURA WSTRZYMANIA TRANSAKCJI I ZAMROŻENIA TRANSAKCJI

1. Pracownik Instytucji obowiązanej/Przedsiębiorcy, który otrzymał dyspozycję lub zlecenie przeprowadzenia transakcji, mający przeprowadzić transakcję lub posiadający informacje o zamiarze przeprowadzenia transakcji, co do której zachodzi uzasadnione podejrzenie, że może ona mieć związek z popełnieniem przestępstwa, o którym mowa w art. 165a (finansowanie terroryzmu) lub art. 299 (pranie pieniędzy) Kodeksu karnego, ma obowiązek niezwłocznie zawiadomić Koordynatora, wraz ze wskazaniem planowanego terminu jej realizacji i wskazaniem przesłanek uzasadnionego podejrzenia.
2. W przypadku braku uzasadnienia zgłoszenia zlecenia przeprowadzenia transakcji jako podejrzanego o pranie pieniędzy lub finansowanie terroryzmu, Koordynator, sporządza odpowiednie uzasadnienie, które dołącza do dokumentacji i nie dokonuje zgłoszenia do GIIF. W przeciwnym przypadku informacja o transakcji natychmiast jest przekazywana do GIIF.
3. W przypadku wysłania zawiadomienia do GIIF, potwierdza on niezwłocznie jego odbiór - w formie pisemnej podając datę i godzinę przyjęcia zawiadomienia.
4. GIIF może w ciągu 24 godzin liczonych od daty i godziny wskazanych w potwierdzeniu, o którym mowa w ust. 4, przekazać do instytucji obowiązanej/Przedsiębiorcy pisemne żądanie wstrzymania transakcji lub blokady rachunku na okres nie dłuższy niż 72 godziny od daty i godziny wskazanych w tym potwierdzeniu. Równocześnie GIIF zawiadamia właściwego prokuratora o podejrzeniu popełnienia przestępstwa i przekazuje mu informacje i dokumenty dotyczące wstrzymywanej transakcji lub blokowanego rachunku. Do liczenia terminów, o których mowa powyżej, nie wlicza się sobót, niedziel i dni ustawowo wolnych od pracy.
5. Do czasu otrzymania żądania, o którym mowa w ust. 4, nie dłużej niż 24 godziny, od momentu potwierdzenia przyjęcia zawiadomienia, o którym mowa w ust. 4, Instytucji obowiązana/Przedsiębiorca nie wykonuje transakcji, której dotyczy zawiadomienie oraz nie może poinformować klienta, że transakcja przez niego zapowiedziana została zgłoszona do GIIF.
6. Instytucja obowiązana/Przedsiębiorca wstrzymuje transakcję lub dokonuje blokady rachunku z momentem otrzymania pisemnego żądania wstrzymania transakcji lub blokady rachunku przez GIIF lub łącznie dwie upoważnione przez niego na piśmie.
7. Jeżeli zawiadomienia do GIIF nie można było dokonać przed wykonaniem albo podczas wykonywania dyspozycji (zlecenia) przeprowadzenia transakcji, Koordynator przekazuje do GIIF informację o transakcji niezwłocznie po jej przeprowadzeniu, równocześnie podając przyczyny braku wcześniejszego zawiadomienia.
8. GIIF może przekazać do Instytucji obowiązanej/Przedsiębiorcy pisemne żądanie wstrzymania transakcji lub blokady rachunku bez uprzedniego otrzymania od niego zawiadomienia, jeżeli posiadane przez GIIF informacje wskazują na prowadzenie działań mających na celu pranie pieniędzy lub finansowanie terroryzmu.
9. Po otrzymaniu zawiadomienia od GIIF, o którym mowa w ust. 4, Prokurator może postanowieniem wstrzymać transakcję lub dokonać blokady rachunku na czas oznaczony, nie dłuższy jednak niż 3 miesiące

od otrzymania tego zawiadomienia. Wstrzymanie transakcji lub blokada rachunku upada, jeżeli przed upływem tego terminu nie zostanie wydane postanowienie o zabezpieczeniu majątkowym.

10. Instytucja obowiązana/Przedsiębiorca na żądanie zlecającego transakcję lub posiadacza rachunku, może poinformować go o wstrzymaniu transakcji lub o blokadzie rachunku i wskazać organ, który zażądał wstrzymania transakcji lub blokady rachunku.
11. Instytucja obowiązana/Przedsiębiorca dokonuje **zamrożenia** wartości majątkowych, z zachowaniem należytej staranności, z wyłączeniem rzeczy ruchomych i nieruchomości, na podstawie:
 - 1) prawa Unii Europejskiej wprowadzającego szczególne środki ograniczające przeciwko niektórym osobom, grupom lub podmiotom oraz
 - 2) przepisów wydanych na podstawie art. 20d ust. 4 ustawy przez Ministra właściwego do spraw instytucji finansowych w porozumieniu z ministrem właściwym do spraw zagranicznych, w drodze rozporządzenia, określających listę osób, grup lub podmiotów, w stosunku do których dokonuje się zamrożenia, o którym mowa w ust. 1, z uwzględnieniem konieczności wykonania zobowiązań wynikających z wiążących Rzeczpospolitą Polską umów międzynarodowych lub wiążących uchwał organizacji międzynarodowych, oraz mając na uwadze konieczność zwalczania terroryzmu i przeciwdziałania finansowaniu terroryzmu.
12. Zamrożenie polega na przeciwdziałaniu przenoszeniu, zmianie, wykorzystaniu wartości majątkowych lub przeprowadzaniu transakcji w jakikolwiek sposób, który może spowodować zmianę ich wielkości, wartości, miejsca, własności, posiadania, charakteru, przeznaczenia lub jakąkolwiek inną zmianę, która może umożliwić korzystanie z wartości majątkowych.

VIII. ŚRODKI BEZPIECZEŃSTWA FINANSOWEGO

1. Proces stosowania środków bezpieczeństwa finansowego jest procesem rozpoznawania nowych i okresowej weryfikacji istniejących Klientów, ich tożsamości, celu współpracy z Instytucją obowiązana/Przedsiębiorcą, zgodności przeprowadzanej transakcji z profilem transakcyjnym Klienta oraz z ryzykiem.
2. Instytucja obowiązana/Przedsiębiorca stosuje wobec swoich Klientów środki bezpieczeństwa finansowego, których zakres stosowania uzależniony jest od oceny Klienta dokonanej w wyniku analizy ryzyka prania pieniędzy i finansowania terroryzmu z nim związanego, z uwzględnieniem w szczególności rodzaju Klienta, stosunków gospodarczych, rodzaju produktów lub transakcji.
3. Środki bezpieczeństwa finansowego są stosowane w szczególności w następujących przypadkach:
 - 1) przy zawieraniu umowy z klientem;
 - 2) przy przeprowadzaniu transakcji z klientem, z którym instytucja obowiązana nie zawarła uprzednio umowy, której równowartość przekracza 15 000 euro, bez względu na to czy transakcja jest przeprowadzana jako pojedyncza operacja czy kilka operacji, których okoliczności wskazują, że są one ze sobą powiązane;
 - 3) gdy istnieje uzasadnione podejrzenie prania pieniędzy lub finansowania terroryzmu bez względu na wartość transakcji, formę organizacyjną oraz rodzaj Klienta;
 - 4) gdy zachodzi wątpliwość czy otrzymane wcześniej dane identyfikacyjne są prawdziwe lub pełne, tzn. gdy istnieją wątpliwości co do prawdziwości, zupełności lub wiarygodności wcześniej otrzymanych danych dotyczących identyfikacji Klienta, charakteru jego działalności, czy innych elementów znanego i udokumentowanego profilu transakcyjnego Klienta.

4. Środki bezpieczeństwa polegają na:

- 1) identyfikacji klienta i weryfikacji (sprawdzeniu i potwierdzeniu uzyskanych danych identyfikacyjnych) jego tożsamości na podstawie dokumentów lub informacji publicznie dostępnych.

Identyfikacja obejmuje:

- **w przypadku osób fizycznych i ich przedstawicieli** - ustalenie i zapisanie cech dokumentu stwierdzającego na podstawie odrębnych przepisów tożsamość osoby, a także imienia, nazwiska, obywatelstwa oraz adresu osoby dokonującej transakcji, a ponadto numeru PESEL lub daty urodzenia w przypadku osoby nieposiadającej numeru PESEL lub numeru dokumentu stwierdzającego tożsamość cudzoziemca, lub kodu kraju w przypadku przedstawienia paszportu,
- **w przypadku osób prawnych** - zapisanie aktualnych danych z wyciągu z rejestru sądowego lub innego dokumentu, wskazującego nazwę (firmę), formę organizacyjną osoby prawnej, siedzibę i jej adres, numer identyfikacji podatkowej, a także imienia, nazwiska i numeru PESEL lub daty urodzenia w przypadku osoby nieposiadającej numeru PESEL, osoby reprezentującej tę osobę prawną,
- **w przypadku jednostek organizacyjnych niemających osobowości prawnej** – zapisanie aktualnych danych z dokumentu wskazującego nazwę, formę organizacyjną, siedzibę i jej adres, numer identyfikacji podatkowej, a także imienia, nazwiska i numeru PESEL lub daty urodzenia w przypadku osoby nieposiadającej numeru PESEL, osoby reprezentującej tę jednostkę.

Identyfikacja, o której mowa powyżej, dotyczy także stron transakcji niebędących klientami i obejmuje ustalenie i zapisanie ich nazwy (firmy) lub imienia i nazwiska oraz adresu, w zakresie, w jakim dane te można ustalić przy zachowaniu należytej staranności.

- 2) podejmowaniu czynności, z zachowaniem należytej staranności, w celu identyfikacji beneficjenta rzeczywistego i stosowaniu uzależnionych od oceny ryzyka odpowiednich środków weryfikacji jego tożsamości w celu uzyskania

danych dotyczących tożsamości beneficjenta rzeczywistego, w tym ustalaniu struktury własności i zależności klienta; identyfikacja w takim wypadku obejmuje ustalenie i zapisanie imienia, nazwiska i adresu oraz dodatkowo innych danych identyfikacyjnych, o których mowa powyżej w pkt. 1 w zakresie, w jakim można je ustalić.

- 3) uzyskiwaniu informacji dotyczących celu i zamierzonego przez klienta charakteru stosunków gospodarczych,
- 4) bieżącym monitorowaniu stosunków gospodarczych z klientem, w tym badaniu przeprowadzanych transakcji w celu zapewnienia, że przeprowadzane transakcje są zgodne z wiedzą instytucji obowiązanej o kliencie i profilu jego działalności oraz z ryzykiem, a także, w miarę możliwości, badaniu źródła pochodzenia wartości majątkowych oraz bieżącym aktualizowaniu posiadanych dokumentów i informacji.

5. W przypadku gdy nie jest możliwe wykonanie obowiązków, o których mowa w ust. 4 pkt. 1-3 Instytucja obowiązana/Przedsiębiorca nie przeprowadza transakcji oraz przekazuje GIIF, w uzasadnionych przypadkach z uwzględnieniem ryzyka prania pieniędzy oraz finansowania terroryzmu, informacje o danym kliencie wraz z posiadanymi informacjami o planowanej przez niego transakcji.

6. Pracownicy przeprowadzający transakcję stosują, na podstawie analizy ryzyka, wzmożone środki bezpieczeństwa finansowego wobec klienta w przypadkach, które mogą wiązać się z wyższym ryzykiem prania pieniędzy, a w szczególności w przypadkach wymienionych poniżej.
- 1) W przypadku, gdy klient nie jest obecny, dla celów identyfikacji stosuje się, w celu zmniejszenia ryzyka, co najmniej jeden z następujących środków: ustalenie tożsamości klienta na podstawie dodatkowych dokumentów lub informacji; dodatkową weryfikację autentyczności przedstawionych dokumentów lub poświadczenie ich zgodności z oryginałem przez notariusza, organ administracji rządowej, organ samorządu terytorialnego lub podmiot świadczący usługi finansowe; ustalenie, że pierwsza transakcja została przeprowadzona za pośrednictwem rachunku klienta w podmiocie świadczącym usługi finansowe.
 - 2) W odniesieniu do osób zajmujących eksponowane stanowiska polityczne Koordynator lub Analityk kierując się podejściem opartym na ocenie ryzyka, ustala czy dany Klient jest osobą zajmującą eksponowane stanowiska polityczne, członkiem najbliższej rodziny tej osoby lub osobą będącą jej bliskim współpracownikiem, tylko w stosunku do osób fizycznych mających miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej. Ustalenie, czy dany Klient jest osobą zajmującą eksponowane stanowisko polityczne lub osobą z nią związaną, następuje poprzez przyjęcie od takiego Klienta oświadczenia na piśmie, czy jest osobą zajmującą eksponowane stanowisko polityczne lub osobą z nią związaną, pod rygorem odpowiedzialności karnej za podanie danych niezgodnych ze stanem faktycznym /następuje poprzez sprawdzenie w odpowiednich bazach PEP's-ów do których Instytucja obowiązana posiada dostęp.
 - 3) Przed zawarciem jakiegokolwiek transakcji lub nawiązaniem stosunków gospodarczych z podmiotem, klasyfikowanym jako osoba na eksponowanym stanowisku politycznym, należy ze szczególną starannością przeanalizować, źródło finansowania transakcji oraz źródło pochodzenia kapitału takiego podmiotu. W przypadku nawiązania trwałych stosunków gospodarczych z takim podmiotem, należy na bieżąco monitorować źródła pochodzenia wartości majątkowych.
 - 4) Decyzja o zawarciu umowy z osobą zajmującą eksponowane stanowisko politycznie zapada po uprzednim uzyskaniu zgody członka zarządu odpowiedzialnego za obszar przeciwdziałania praniu pieniędzy lub właściciela (przedsiębiorcy).
7. Na zasadzie wyjątku od standardowych środków bezpieczeństwa finansowego wobec Klienta, Instytucja obowiązana/Przedsiębiorca może odstąpić od stosowania, przy uwzględnieniu ryzyka, środków bezpieczeństwa finansowego określonych w ust. 4 pkt. 1-3 niniejszego rozdziału:
- 1) gdy Klient jest podmiotem świadczącym usługi finansowe, mającym siedzibę na terytorium państwa członkowskiego Unii Europejskiej albo państwa równoważnego;
 - 2) w stosunku do organów administracji rządowej, organów samorządu terytorialnego oraz organów egzekucyjnych.
8. W przypadku gdy Klient jest spółką, której papiery wartościowe są dopuszczone do publicznego obrotu na rynku regulowanym w co najmniej jednym państwie członkowskim Unii Europejskiej lub w państwie równoważnym, instytucja obowiązana przy uwzględnieniu ryzyka prania pieniędzy lub finansowania terroryzmu, może ograniczyć stosowanie środków bezpieczeństwa finansowego do identyfikacji i weryfikacji jego tożsamości przy zawieraniu umowy z Klientem oraz gdy istnieje podejrzenie prania pieniędzy.

IX. ANALIZA TRANSAKCJI I OCENA RYZYKA KLIENTÓW

1. Wymagane standardy i zakres stosowanych środków bezpieczeństwa finansowego różnią się w zależności od prawdopodobieństwa zaistnienia sytuacji prania pieniędzy, które Instytucja obowiązana/Przedsiębiorca szacuje na podstawie analizy ryzyka, w szczególności z uwzględnieniem rodzaju Klienta, stosunków gospodarczych łączących go z Klientem, produktów lub transakcji.
2. Zakres stosowanych środków bezpieczeństwa finansowego ustala się w oparciu o analizę ryzyka: im wyższe ryzyko wystąpienia prania pieniędzy lub finansowania terroryzmu, tym zakres stosowanych środków bezpieczeństwa finansowego powinien być szerszy, celem minimalizacji możliwości wystąpienia tego procederu.
3. W celu systematycznego prowadzenia analiz transakcji i oceny ryzyka Klienta Koordynator lub Analityk dokonują analizy przeprowadzanych transakcji, biorąc w szczególności pod uwagę przy dokonywaniu analizy i oceny następujące kryteria:
 - 1) ekonomiczne - polegające na ocenie transakcji klienta pod względem celu prowadzonej przez niego działalności gospodarczej;
 - 2) geograficzne - polegające na dokonywaniu transakcji nieuzasadnionych charakterem działalności gospodarczej zawieranych z podmiotami z państw, w których występuje wysokie zagrożenie prania pieniędzy i finansowania terroryzmu;
 - 3) przedmiotowe - polegające na prowadzeniu przez klienta działalności gospodarczej wysokiego ryzyka z punktu widzenia podatności na pranie pieniędzy i finansowanie terroryzmu;
 - 4) behawioralne - polegające na nietypowym, w danej sytuacji, zachowaniu klienta.
4. W wyniku analizy ryzyka każdy Klient zostaje zaklasyfikowany do właściwej mu klasy ryzyka.
 - 1) Klienci charakteryzujący się niskim ryzykiem, z którymi związane jest niewielkie ryzyko prania pieniędzy (np. organ egzekucyjny, organy samorządowe). Wyłącznie do tej grupy Klientów pracownik Instytucji obowiązanej może stosować uproszczone środki bezpieczeństwa finansowego.
 - 2) Klienci charakteryzujący się standardowym ryzykiem, z którymi związane jest normalne/naturalne ryzyko prania pieniędzy. Do tej grupy Klientów pracownik Instytucji obowiązanej stosuje standardowe środki bezpieczeństwa finansowego.
 - 3) Klienci charakteryzujący się podwyższonym ryzykiem, z którymi związane jest wysokie ryzyko prania pieniędzy (np. z uwagi na branżę w której działa Klient, status PEP's, czy przeprowadzanie transakcji nietypowych). Do tej grupy Klientów pracownik Instytucji obowiązanej stosuje wzmożone środki bezpieczeństwa finansowego.
 - 4) Klienci charakteryzujący się nieakceptowanym poziomem ryzyka - osoba lub podmiot stwarzający nieakceptowane ryzyko prawne lub reputacyjne nie może zostać zaakceptowany jako Klient, w szczególności, gdy:
 - a) wpisany jest na aktualną listę sankcyjną;
 - b) ma siedzibę w kraju nieakceptowalnego ryzyka lub prowadzi działalność w takim kraju;
 - c) klient prowadzi działalność w branży nieakceptowalnego ryzyka – dopalacze,
 - d) Instytucja obowiązana posiada wiedzę, iż wartości majątkowe Klienta pochodzą z nielegalnych lub nieujawnionych źródeł/mają związek z praniem pieniędzy lub finansowaniem terroryzmu.

e) Klient odmawia udzielenia informacji w akceptowalnym zakresie.

5. Instytucja obowiązana/Przedsiębiorca prowadzi także bieżącą analizę przeprowadzanych transakcji.

X. PRZEPISY KOŃCOWE

1. Informacje uzyskane w wyniku stosowania środków bezpieczeństwa finansowego oraz wyniki analiz są przechowywane przez okres 5 lat, licząc od pierwszego dnia roku następującego po roku, w którym przeprowadzono transakcję z klientem. W przypadku likwidacji, połączenia, podziału lub przekształcenia instytucji obowiązanej, do przechowywania dokumentacji stosuje się przepisy art. 76 ustawy z dnia 29 września 1994 r. o rachunkowości.
 2. Pracownicy mający dostęp do danych osobowych klientów, rejestru transakcji, jak również wszelkiej dokumentacji związanej z przeciwdziałaniem praniu pieniędzy zobowiązani są do przestrzegania tajemnicy zawodowej, także po ustaniu zatrudnienia.
 3. Instytucja obowiązana/Przedsiębiorca zapewnia udział pracowników w programach szkoleniowych dotyczących realizacji zadań związanych z przeciwdziałaniem praniu pieniędzy oraz finansowania terroryzmu, w tym w szczególności identyfikacji transakcji mogących mieć związek z przestępstwem, o którym mowa w art. 299 Kodeksu karnego. Szkolenia zewnętrzne w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu organizowane są cyklicznie.
 4. Pracownicy, którzy nie dopełniają obowiązków nałożonych przepisami Ustawy, a w szczególności: nie zarejestrowali transakcji podlegającej rejestracji, nie zachowali środków bezpieczeństwa finansowego, zgodnie z procedurą, nie zrealizowali żądania wstrzymania transakcji lub blokady rachunku, ujawnili informacje osobom nieuprawnionym, przekazali nieprawdziwe dane lub je zataili oraz odmówili przekazania dokumentów do GIIF
- Podlegają odpowiedzialności karnej na zasadach określonych w ustawie