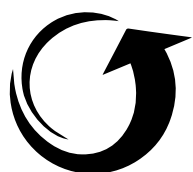


Wojciech Kapica
Marta Wysocka-Fronczek

AML w biurze rachunkowym wszystko co musisz wiedzieć



| C.H.BECK

AML w biurze rachunkowym – wszystko co musisz wiedzieć

Stan prawny: czerwiec 2021

Autorzy:

Wojciech Kapica, Marta Wysocka-Fronczek

Wydawca: Anna Mięso

Korekta: Sylwia Pańków

Projekt okładki: Rafał Kowalczyk



© Wydawnictwo C.H.Beck 2021

Wszelkie prawa zastrzeżone.

Opinie zawarte w niniejszej publikacji wyrażają osobisty punkt widzenia Autora.
Wydawnictwo C.H.Beck nie ponosi odpowiedzialności za zawarte w niej informacje.

Wydawnictwo C.H.Beck Sp. z o.o.
ul. Bonifraterska 17, 00-203 Warszawa
tel.: 22 33 77 600
www.beckinfobiznes.pl

Skład i łamanie: Wydawnictwo C.H.Beck



ISBN 978-83-8158-000-7

Spis treści

O autorach	VII
Wykaz skrótów	IX
Wprowadzenie	XI
1. Obowiązki biur rachunkowych	1
1.1. Osoba odpowiedzialna	2
1.2. Wdrożenie wewnętrznych regulacji	3
1.3. Obowiązek szkoleniowy	3
1.4. Analiza oceny ryzyka	4
1.5. Identyfikacja klienta	4
1.6. Beneficjent rzeczywisty	5
1.7. Identyfikacja PEP	5
1.8. Szczególne środki ograniczające	6
1.9. Monitorowanie transakcji	7
1.10. Transakcje podejrzane	7
1.11. Przekazywanie informacji do GIIF	8
1.12. Termin przechowywania danych	11
2. Kary dla biura rachunkowego za naruszenie ustawy	13
3. Kontrola GIIF	15
4. Wzory dokumentów	17
4.1. Wzór uchwały zarządu	17
4.2. Wzór powierzenia obowiązków z zakresu AML	18
4.3. Wewnętrzna regulacja o przeciwdziałaniu praniu brudnych pieniędzy	19
4.4. Analiza oceny ryzyka AML	29
4.5. Oświadczenie o beneficjencie rzeczywistym	31
4.6. Oświadczenie PEP	35
4.7. Rejestr transakcji podejrzanych	36
4.8. Zawiadomienie odnośnie transakcji podejrzanej	36

0 autorach

Wojciech Kapica – ekspert w zakresie regulacji sektora finansowego, systemów zgodności (compliance) oraz etyki w działalności instytucji finansowych; współkierujący departamentem prawa rynku finansowego w kancelarii SMM LEGAL Maciak Mataczyński Adwokaci sp.k.; specjalizuje się w prawie bankowym, rynku kapitałowego i ubezpieczeń, polityce nadzorczej i ładzie korporacyjnym w podmiotach nadzorowanych; autor kilkudziesięciu publikacji i twórca wielu autorskich szkoleń dotyczących regulacji bankowych, ubezpieczeniowych i przeciwdziałania praniu pieniędzy; redaktor i współautor książki Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Praktyczny przewodnik (2018) oraz Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz (2019).

Marta Wysocka-Fronczek – prawnik, certyfikowany compliance officer, ekspert w dziedzinie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, praktyk z wieloletnim doświadczeniem zawodowym w obszarze przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i compliance w instytucjach finansowych. Specjalizuje się w zagadnieniach corporate governance, kontroli wewnętrznej, compliance, audytu wewnętrznego, zarządzania ryzykiem i whistleblowingu.

Wykaz skrótów

1. Akty prawne

ZmTerroryzmU21	ustawa z 30.3.2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. z 2021 r. poz. 815)
TerroryzmU	ustawa z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2020 r. poz. 971 ze zm.)
RachunkU	ustawa z 29.9.1994 r. o rachunkowości (t.j. Dz.U. z 2021 r. poz. 217 ze zm.)
KK	ustawa z 6.6.1997 r. – Kodeks karny (t.j. Dz.U. z 2020 r. poz. 1444)

2. Organy i instytucje

ONZ	Organizacja Narodów Zjednoczonych
UE	Unia Europejska
GIIF	Generalny Inspektor Informacji Finansowej
UKNF	Urząd Komisji Nadzoru Finansowego
NBP	Narodowy Bank Polski

3. Inne skróty

art.	artykuł
ds.	do spraw
itp.	i tym podobne
lit.	litera
m.in.	między innymi
w zw.	w związku
np.	na przykład
pkt.	punkt (-u)
t.j.	tekst jednolity
tzw.	tak zwany
ust.	ustęp
§	paragraf

PKPiR	Podatkowa Księga Przychodów i Rozchodów
AML	(ang. <i>Anti-Money Laundering</i>)
PEP	(ang. <i>Politically Exposed Persons</i>)
PESEL	Powszechny Elektroniczny System Ewidencji Ludności
NIP	Numer Identyfikacji Podatkowej
CBR	Centralny Rejestr Beneficjentów Rzeczywistych
IBAN	(ang. <i>International Bank Account Number</i>)

Marta Wysocka-Fronczek

Wprowadzenie

Nowelizacja ustawy z 30.3.2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz.U. z 2021 r. poz. 815; dalej: ZmTerroryzmU21) rozszerza katalog podmiotów zobowiązanych do realizacji obowiązków w zakresie AML, w ten sposób, iż do tej grupy dołączono również **osoby świadczące usługi sporządzania deklaracji, prowadzenia ksiąg podatkowych, udzielania porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego**.

Do tej pory obowiązane do wypełniania wszystkich obowiązków wynikających z tej ustawy były podmioty prowadzące działalność w zakresie usługowego prowadzenia ksiąg rachunkowych, a zatem wyłączone z tego obowiązku były biura księgowe prowadzące działalność jedynie w zakresie rozliczeń osób fizycznych prowadzących działalność gospodarczą, objętych uproszczoną ewidencją podatkową (PKPiR).

Na mocy ZmTerroryzmU21 do art. 2 w ust. 1 ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2020 r. poz. 971 ze zm.; dalej: TerroryzmU) dodano pkt 15a o treści: „przedsiębiorcy w rozumieniu ustawy z dnia 6.3.2018 r. – Prawo przedsiębiorców (Dz.U. z 2021 r. poz. 162), 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 obowiązany”.

W związku z powyższym również małe biura księgowe czy rachunkowe, które świadczą usługi sporządzania deklaracji, prowadzenia ksiąg podatkowych, udzielania porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego, będą musiały, jako instytucje obowiązane, stosować wszystkie obowiązki wskazane w TerroryzmU.

1. Obowiązki biur rachunkowych

Ustawa z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2020 r. poz. 971 ze zm.; dalej: *TerroryzmU*) w art. 33 w zw. z art. 2 ust. 1 pkt 17 nakłada na biura rachunkowe obowiązek bezwzględnego stosowania środków bezpieczeństwa finansowego (których katalog wskazano poniżej) względem wszystkich klientów. W przypadku każdego stosunku gospodarczego lub transakcji okazjonalnej należy przeprowadzić analizę ryzyka i jego ocenę, przy uwzględnieniu czynników dotyczących rodzaju klienta, obszaru geograficznego, rodzaju usług i sposobów ich dystrybucji, a także wartości przeprowadzonej transakcji, jej celu, regularności i czasu trwania. Środki bezpieczeństwa finansowego stosuje się w różnym zakresie (z różną intensywnością), zależnie od stopnia zidentyfikowanego ryzyka dotyczącego klienta lub transakcji. Ustawodawca wskazuje, że biura rachunkowe mogą moderować częstotliwość i zakres stosowania podstawowego katalogu środków bezpieczeństwa finansowego, zabraniając jednocześnie odstępowań od stosowania któregokolwiek z nich.

Przesłanki niższego ryzyka prania pieniędzy i finansowania terroryzmu zostały wskazane w art. 42 *TerroryzmU*. Stosunkowo bliski charakter relacji biznesowych pomiędzy biurami rachunkowymi a ich klientami również może być traktowany jako jeden z czynników, który może potencjalnie wpływać na możliwość stosowania uproszczonych środków bezpieczeństwa. Warunkiem zastosowania uproszczonych środków bezpieczeństwa finansowego, czyli *de facto* zarządzania częstotliwością i dokładnością wykonywania wszystkich środków wskazanych w art. 34 *TerroryzmU*, jest potwierdzenie niższego ryzyka w toku oceny ryzyka klienta bądź transakcji okazjonalnej. Każdorazowe stosowanie uproszczonych środków bezpieczeństwa finansowego musi być poprzedzone ocenieniem ryzyka klienta bądź transakcji okazjonalnej jako niskiego.

W art. 43 *TerroryzmU* wskazano natomiast przesłanki powodujące konieczność stosowania wzmożonych środków bezpieczeństwa finansowego. Odwrotnie niż przy uproszczonych środkach bezpieczeństwa finansowego, których zastosowanie było jedynie opcjonalne, tak w tym przepisie ustawodawca wyraźnie stwierdza, że zawsze w przypadkach wyższego ryzyka prania pieniędzy lub finansowania terroryzmu należy stosować wzmo-

żone środki bezpieczeństwa finansowego. Wśród sytuacji mogących powodować podwyższone ryzyko znalazło się m.in. nawiązywanie stosunków gospodarczych w nietypowych okolicznościach; działalność klienta służąca do przechowywania aktywów osobistych; nawiązywanie relacji ze spółką, w której wydano akcje na okaziciela, której papiery wartościowe nie są dopuszczone do obrotu zorganizowanego; nietypowa lub nadmiernie złożona struktura własnościowa klienta; powiązanie stosunków gospodarczych lub transakcji okazjonalnej z państwem trzecim wysokiego ryzyka lub państwem, w stosunku do którego ONZ lub UE nałożyły szczególne środki ograniczające. W przypadku wystąpienia wyższego ryzyka prania pieniędzy lub finansowania terroryzmu biura rachunkowe stosują wzmożone środki bezpieczeństwa finansowego, polegające co najmniej na:

- 1) podejmowaniu działania w celu wyjaśnienia okoliczności, w jakich przeprowadzono te transakcje;
- 2) intensyfikowaniu bieżącego monitorowania stosunków gospodarczych, w ramach których te transakcje zostały przeprowadzone. Nie ogranicza to oczywiście biura rachunkowego w stosowaniu dodatkowych środków, natomiast oblige je do wykonania środków wskazanych w art. 43 TerroryzmU.

Art. 35 TerroryzmU zawiera katalog przypadków, w których środki bezpieczeństwa finansowego powinny być każdorazowo stosowane. Należą do nich:

- 1) nawiązywanie stosunków gospodarczych;
- 2) przeprowadzanie transakcji okazjonalnej o równowartości 15 000 euro lub większej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się być ze sobą powiązane;
- 3) przeprowadzanie transakcji okazjonalnej, stanowiącej transfer środków pieniężnych na kwotę przekraczającą równowartość 1000 euro;
- 4) podejrzenie prania pieniędzy lub finansowania terroryzmu;
- 5) wątpliwości co do prawdziwości lub kompletności dotychczas uzyskanych danych identyfikacyjnych klienta;
- 6) zmiana uprzednio ustalonego charakteru lub okoliczności stosunków gospodarczych.

1.1. Osoba odpowiedzialna

Biura rachunkowe wyznaczają (np. w formie uchwały zarządu):

- 1) przedstawicieli kadry kierowniczej wyższego szczebla odpowiedzialnych za wykonywanie obowiązków określonych w TerroryzmU (art. 6 TerroryzmU);
- 2) w biurach rachunkowych, w których działa zarząd lub inny organ zarządzający – jednego spośród członków zarządu jako osobę odpowiedzialną za wdrażanie obowiązków określonych w TerroryzmU (art. 7 TerroryzmU);
- 3) pracownika zajmującego kierownicze stanowisko odpowiedzialnego za zapewnienie zgodności działalności biura rachunkowego oraz jego pracowników i innych osób wykonujących czynności na rzecz tego biura rachunkowego z przepisami TerroryzmU (art. 8 TerroryzmU). Wyznaczony pracownik jest również odpowiedzialny za przekazywanie w imieniu biura rachunkowego zawiadomień o podejrzeniu popełnienia przestępstwa.

W małych biurach rachunkowych wystarczy wyznaczenie jednej osoby, odpowiedzialnej za wdrożenie obowiązków z zakresu AML i realizację obowiązków z zakresu AML (np. wyrażanie zgody na stosunek gospodarczy z PEP, obowiązki raportowe do GIIF).

1.2. Wdrożenie wewnętrznych regulacji

Zgodnie z art. 50 TerroryzmuU biuro rachunkowe jako instytucja obowiązana powinno posiadać swoją własną procedurę wewnętrzną przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

Wewnętrzna procedura stanowić ma akt, w którym sprecyzowane zostaną zasady postępowania stosowane w danym biurze rachunkowym, w celu właściwego wywiązania się z nałożonych na to biuro obowiązków z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Szczegółowe elementy procedury zostały wskazane przez ustawodawcę w art. 50 ust. 2 TerroryzmuU i uwzględniono wśród nich m.in. zasady rozpoznawania i oceny ryzyka, zasady stosowania środków bezpieczeństwa finansowego oraz zasady dot. raportowania transakcji do GIIF. Katalog ten ma charakter otwarty, biorąc pod uwagę użyte w tekście sformułowanie „w szczególności”. Przy wprowadzaniu procedury należy zastosować zasadę proporcjonalności, tj. procedura ta powinna uwzględniać charakter i wielkość podmiotu zobowiązanego.

Ponadto biuro rachunkowe powinno posiadać procedurę anonimowego zgłaszania naruszeń ustawy, która umożliwiać ma dokonywanie zgłoszeń w ramach danego biura rachunkowego zarówno przez pracowników, jak i inne osoby realizujące czynności na rzecz biura rachunkowego. Wymogi dotyczące procedury anonimowego zgłaszania naruszeń zawarte zostały w art. 53 ust. 2 TerroryzmuU. Dla rzeczonyj procedury nie zastrzeżono wprost formy – wydaje się, że procedura powinna być opracowana i utrzymywana na trwałym nośniku danych. Tym samym może to być zarówno wersja elektroniczna, jak i dokument w formie papierowej. Procedura powinna być prawidłowo wdrożona (na przykład poprzez uchwałę zarządu).

1.3. Obowiązek szkoleniowy

Art. 52 TerroryzmuU nakłada obowiązek przeprowadzania szkoleń, których celem jest podnoszenie poziomu wiedzy oraz świadomości osób wykonujących obowiązki związane z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu. Celem takich szkoleń może być również szybkie reagowanie na zidentyfikowane nowe zjawiska przestępcze. Należy zatem przyjąć, że biuro rachunkowe powinno szkolić wskazane wyżej osoby regularnie, a nie jedynie jednorazowo. Szkolenia nie powinny obejmować całej materii przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, a jedynie część, która w praktyce będzie miała zastosowanie do charakteru, skali i rozmiaru działalności prowadzonej przez biuro rachunkowe.

Ważne

Art. 52 ust. 3 Terroryzmu precyzuje, że przepis ma zastosowanie także odpowiednio do biura rachunkowego prowadzonego w formie działalności jednoosobowej – w takim zakresie przedsiębiorca będzie musiał jednak korzystać z zewnętrznego programu szkoleń.

1.4. Analiza oceny ryzyka

Obowiązek identyfikacji i oceny ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu wynika z art. 27 Terroryzmu, zgodnie z którym ustawodawca wymaga, aby biuro rachunkowe podjęło, proporcjonalnie do charakteru wykonywanej przez siebie działalności, odpowiednie działania w celu zidentyfikowania i oceniania ryzyka prania pieniędzy i finansowania terroryzmu z tą działalnością związanego, z uwzględnieniem czynników ryzyka dotyczących klientów, państw lub obszarów geograficznych, usług i transakcji. Biorąc jednak pod uwagę fakt, że biura rachunkowe dostosowują poziom szczegółowości przeprowadzanej przez siebie oceny ryzyka do swojej działalności, w przypadku biur mniejszych czy prowadzących mniej narażoną na ryzyko działalność proces ten może być znacznie mniej skomplikowany.

Przy ocenie ryzyka biuro rachunkowe może brać pod uwagę zarówno Krajową Ocenę Ryzyka publikowaną przez Generalnego Inspektora Informacji Finansowej, jak też ocenę ryzyka przeprowadzoną przez Komisję Europejską. Zgodnie z art. 27 ust. 3 Terroryzmu przeprowadzona ocena ryzyka powinna być udokumentowana i aktualizowana nie rzadziej niż co dwa lata, a także w przypadku zmiany istotnych czynników ryzyka lub aktualizacji ww. dokumentów GIIF lub Komisji Europejskiej.

1.5. Identyfikacja klienta

Identyfikacja osoby fizycznej polega na ustaleniu danych wskazanych w art. 36 ust. 1 Terroryzmu (imienia i nazwiska, obywatelstwa, państwa urodzenia, numeru PESEL lub daty urodzenia w przypadku braku numeru PESEL, serii i numeru dowodu osobistego, NIP).

W przypadku osoby prawnej należy podać ww. dane dotyczące osoby uprawnionej do reprezentowania osoby prawnej, a także dodatkowo firmę osoby prawnej, jej formę organizacyjną, adres siedziby lub miejsca prowadzenia działalności oraz numer NIP.

Pozyskane dane ww. podmiotów podlegają weryfikacji zgodnie z art. 37 Terroryzmu na podstawie dokumentu tożsamości, danych z odpowiedniego rejestru lub innych wiarygodnych i niezależnych źródeł. Przykłady źródeł, które uznawane są za wiarygodne i niezależne, można znaleźć w Komunikacie UKNF z 5.6.2019 r. dot. identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji.

Obowiązek identyfikacji i weryfikacji odnosi się również do osób działających w imieniu klienta, a dodatkowo TerroryzmU nakłada obowiązek weryfikacji prawidłowości umocowania tych osób do reprezentacji.

Ponadto podczas nawiązywania relacji z klientem wymagane jest pozyskanie informacji na temat celu i zamierzonego charakteru stosunków gospodarczych z danym klientem.

Identyfikacja i weryfikacja tożsamości klienta powinna nastąpić przed nawiązaniem z nim stosunków gospodarczych (art. 39 ust. 1 TerroryzmU). Może być ona zakończona po rozpoczęciu stosunków gospodarczych tylko w uzasadnionych przypadkach.

1.6. Beneficjent rzeczywisty

W przypadku beneficjenta rzeczywistego, czyli osoby sprawującej bezpośrednią lub pośrednią kontrolę nad klientem (pojęcie zdefiniowane w art. 2 ust. 2 pkt 1 TerroryzmU), również przewidziano w TerroryzmU obowiązek ustalenia przynajmniej jego imienia i nazwiska oraz obywatelstwa. W tym celu biuro rachunkowe musi każdorazowo zweryfikować dane zawarte w Centralnym Rejestrze Beneficjentów Rzeczywistych (wpisowi podlegają spółki, ale także fundacje, stowarzyszenia rejestrowe czy spółdzielnie), a także potwierdzić dane zawarte w CRBR w inny sposób (przykładowo – odbierając oświadczenie).

Ważne

Odpis wygenerowany z CRBR należy zachować na wypadek kontroli GIIF.

W przypadku klienta będącego osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej niezbędne jest także ustalenie struktury własności i kontroli u klienta, co zmierzać ma do prawidłowego określenia osoby beneficjenta rzeczywistego.

Weryfikacja pozyskanych danych przebiega analogicznie jak w przypadku klientów biura rachunkowego.

1.7. Identyfikacja PEP

Nawiązywanie i utrzymywanie stosunków gospodarczych, zdefiniowanych w art. 2 ust. 2 pkt 20 ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2020 r. poz. 971 ze zm.; dalej: TerroryzmU) jako „stosunki biura rachunkowego z klientem związane z działalnością zawodową instytucji obowiązanej, które w chwili ich nawiązywania wykazują cechę trwałości”, z osobami zajmującymi eksponowane stanowisko polityczne (PEP), ich członkami rodziny lub osobami znanymi jako ich bliscy współpracownicy wymaga od biura rachunkowego stosowania szczególnie rygorystycznych procedur identyfikacji i weryfikacji tożsamości klienta oraz zastosowania względem klienta wzmożonych środków bezpieczeństwa finansowego. Decyzja o sposobie przeprowadzania weryfikacji klientów pod kątem statusu PEP zależy od moż-

liwości biura rachunkowego, może odbywać się manualnie (np. w formie odbierania od klienta oświadczenia o jego statusie PEP) lub w sposób zautomatyzowany.

Ustalenie statusu PEP jest wymagane dla każdego klienta i beneficjenta rzeczywistego. Zidentyfikowanie PEP oznacza konieczność zastosowania względem klienta środków bezpieczeństwa finansowego, podjęcia działań określonych w punktach 1 i 2 ust. 2 art. 46 TerroryzmU (uzyskanie akceptacji kadry kierowniczej wyższego szczebla na nawiązanie lub kontynuację stosunków gospodarczych z osobą posiadającą status PEP, ustalenie źródła majątku klienta i źródła pochodzenia wartości majątkowych pozostających do dyspozycji klienta) oraz intensyfikacji bieżącego monitorowania stosunków gospodarczych z tym podmiotem. Oznacza to, że posiadanie przez klienta statusu osoby zajmującej eksponowane stanowisko polityczne determinuje wystąpienie wysokiego ryzyka prania pieniędzy i finansowania terroryzmu i wyklucza możliwość odstąpienia od zastosowania wzmożonych środków bezpieczeństwa finansowego.

1.8. Szczególne środki ograniczające

Obowiązek stosowania sankcji międzynarodowych względem osób znajdujących się na listach sankcyjnych ogłaszanych przez GIIF na podstawie rezolucji Rady Bezpieczeństwa ONZ oraz na liście GIIF osób i podmiotów, wobec których stosuje się szczególne środki ograniczające, spoczywa na każdym z biur rachunkowych.

Sankcje międzynarodowe polegają na:

- 1) zamrożeniu wartości majątkowych będących własnością osób i podmiotów, kontrolowanych pośrednio oraz bezpośrednio przez osoby i podmioty, a także korzyści pochodzących z tych wartości majątkowych;
- 2) nieudostępnianiu wartości majątkowych bezpośrednio ani pośrednio osobom i podmiotom ani na ich rzecz, przez co rozumie się w szczególności nieudzielanie pożyczek, kredytu konsumenckiego lub kredytu hipotecznego, niedokonywanie darowizn, niedokonywanie płatności za towary lub usługi.

Wszystkie informacje związane z zamrożeniem wartości majątkowych lub ich nieudostępnieniem są przekazywane przez biura rachunkowe do GIIF niezwłocznie, jednak nie później niż w terminie 2 dni roboczych od zastosowania szczególnych środków ograniczających.

Weryfikacja z listą sankcyjną powinna być dokonywana:

- 1) przed nawiązaniem stosunków gospodarczych;
- 2) okresowo w terminach:
 - a) dwa razy w roku dla klientów wysokiego ryzyka;
 - b) raz do roku dla klientów standardowego ryzyka;
 - c) raz na dwa lata dla klientów niskiego ryzyka.

Weryfikacja, czy klient, jego beneficjent lub członek zarządu jest na liście sankcyjnej, dokonywana jest za pośrednictwem strony internetowej:

- 1) http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm,
- 2) http://www.un.org/sc/committees/list_compend.shtml,

po wprowadzeniu w polu „nazwa”: imienia, nazwiska lub nazwy firmy oraz daty urodzenia – w przypadku jej posiadania (dot. osób fizycznych). W przypadku braku dopasowania – można kontynuować czynności związane z obsługą klienta.

1.9. Monitorowanie transakcji

Monitorowanie stosunków gospodarczych polega na bieżącej analizie transakcji i weryfikacji, czy zidentyfikowane przepływy są zgodne z wiedzą biura rachunkowego dotyczącą klienta i przeprowadzanych przez niego transakcji oraz czy odpowiadają przeprowadzonej wcześniej ocenie ryzyka. W przypadkach uzasadnionych okolicznościami biuro rachunkowe zobowiązane jest do badania źródła pochodzenia wartości majątkowych będących w dyspozycji klienta.

Przykładem takich okoliczności będzie wystąpienie czynników ryzyka dotyczących klienta powodujących podwyższone ryzyko lub wszelkie wątpliwości dotyczące charakteru działalności prowadzonej przez klienta.

Dodatkowo biuro rachunkowe musi zapewnić aktualność danych dotyczących klientów, posiadanych dokumentów i informacji dotyczących stosunków gospodarczych. W tym celu powinny być przeprowadzane okresowe przeglądy informacji o klientach, których częstotliwość będzie odpowiednio dostosowana do poziomu zidentyfikowanego ryzyka.

1.10. Transakcje podejrzane

Obowiązek ciągłego monitorowania transakcji przez biuro rachunkowe odnosi się do obserwacji stosunków gospodarczych z klientem i oceny transakcji przez niego wykonywanych w dłuższym czasie.

Zadaniem biura rachunkowego jest typowanie transakcji nietypowych na etapie oceny zawieranych przez klientów biura rachunkowego umów, jak również na etapie księgowania określonych przychodów lub wydatków. Analiza dokonywana jest w odniesieniu do klientów biura rachunkowego.

Tego typu analiza powinna się odbywać na etapie:

- 1) opiniowania umowy pod względem finansowo-księgowo-podatkowym;
- 2) weryfikacji przez biuro rachunkowe faktur zakupowych:
 - a) gdy faktura nie wynika z zapisów umownych/posiada inną kwotę niż wskazana w umowie, lub
 - b) gdy umowa nie była opiniowana przez biuro rachunkowe przed wystawieniem faktury, lub
 - c) gdy faktura jest wystawiona na podstawie zamówienia, lub
 - d) gdy faktura nie wynika z umowy/zamówienia/innego dokumentu merytorycznego;
- 3) możliwej dodatkowej weryfikacji podczas akceptacji przelewów;
- 4) rozliczenia wydatków ze służbowych kart płatniczych;
- 5) rozliczania podatku dochodowego od osób prawnych.

Przy czym wystarczająca jest jedna analiza dokonana na jak najwcześniejszym etapie.

Ważne

W przypadku transakcji okresowych wynikających z wcześniej zawartych umów raz dokonana analiza, jeśli okoliczności faktyczne lub prawne nie uległy zmianie, jest wystarczająca i nie ma potrzeby ponawiania jej przy kolejnych płatnościach.

Symptomami wskazującymi, że biuro rachunkowe ma do czynienia z transakcjami nietypowymi, są następujące sytuacje:

- 1) istnieją wątpliwości co do informacji, które biuro rachunkowe otrzymało – transakcja, która podlega analizie, nie ma uzasadnienia gospodarczego lub prawnego. Znaczaco odbiega od dotychczasowego profilu transakcji danego klienta;
- 2) transakcje są bardzo skomplikowane w porównaniu z innymi podobnymi transakcjami powiązanymi z podobnego rodzaju klientami, produktami lub usługami;
- 3) sposób przeprowadzenia transakcji jest nietypowy lub nieoczekiwany – w porównaniu do tego samego rodzaju klientów, produktów lub usług;
- 4) transakcje opiewają na wysokie kwoty, nieadekwatne do wiedzy instytucji o danym kliencie biura rachunkowego;
- 5) transakcja jest dokonywana bez zawartej umowy, w tym bez pisemnego zamówienia;
- 6) transakcja nie może być kwalifikowana jako koszt uzyskania przychodu klienta (za wyjątkiem transakcji, które nie stanowią kosztu uzyskania przychodu w rozumieniu odnośnych przychodów);
- 7) w transakcje zaangażowani są klienci z krajów wysokiego ryzyka (spoza UE).

Powyższe sytuacje wskazują na nietypowość transakcji – wątpliwości w tym zakresie powinny zostać wyjaśnione poprzez kontakt biura rachunkowego z klientem. W przypadku dobrego kontaktu z klientem w większości przypadków jest to proces prosty i zazwyczaj kończy się wyjaśnieniem sytuacji.

Ważne

W przypadku natomiast braku kontaktu z klientem, niechęci klienta do udzielenia jakiejkolwiek informacji lub odmowy podania informacji transakcja powinna być traktowana przez biuro rachunkowe jako podejrzana.

1.11. Przekazywanie informacji do GIIF

Zgodnie z art. 74 ust. 2 TerroryzmuU zawiadomienie o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, przekazuje się do Generalnego Inspektora niezwłocznie, nie później jednak niż w terminie 2 dni roboczych od dnia potwierdzenia przez biuro rachunkowe tego podejrzenia.

W związku z tym, po ustaleniu okoliczności mogących wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, a przed przekazaniem Generalnemu Inspektorowi zawiadomienia, biuro rachunkowe w zależności

od konkretnego stanu faktycznego powinno zastosować wzmożone środki bezpieczeństwa finansowego lub zintensyfikować bieżące monitorowanie stosunków gospodarczych klienta, poprzez podjęcie przynajmniej jednej lub kilku czynności w celu potwierdzenia podejrzenia, przykładowo:

- 1) przeprowadzenie badania źródła pochodzenia wartości majątkowych (np. poprzez zwrócenie się do klienta z wnioskiem o przedłożenie wyjaśnień lub dokumentów dotyczących źródła pochodzenia środków),
- 2) ustalenie celu i okoliczności, w jakich klient dokonuje płatności na rzecz wybranych adresatów (np. poprzez wystąpienie do klienta z wnioskiem o udostępnienie dokumentów związanych z realizowanymi transakcjami).

W sytuacji gdy złożone przez klienta wyjaśnienia i dostarczone dokumenty nie budzą istotnych wątpliwości w zakresie źródła pochodzenia wartości majątkowych, a także celu i zamierzonego charakteru realizowanych transakcji biuro rachunkowe może wznowić realizowanie transakcji.

W sytuacji gdy klient nie przekaze żądanych informacji i dokumentów (np. unika kontaktu i pojawienia się w biurze rachunkowym, odmawia przedstawienia źródeł pochodzenia wartości majątkowych lub nie przedstawia stosownych dokumentów związanych z realizowanymi transakcjami) albo okażą się one niewystarczające lub niewiarygodne, biuro rachunkowe ma obowiązek rozważyć:

- 1) zawiadomienie Generalnego Inspektora o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu (zgodnie z art. 74 ust. 1–3 TerroryzmU), lub
- 2) zawiadomienie Generalnego Inspektora o podejrzeniu, że określona transakcja lub określone wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu (zgodnie z art. 86 ust. 1–2 TerroryzmU).

Zarówno zawiadomienie przekazywane zgodnie z art. 74, jak i art. 86 TerroryzmU powinno zawierać:

- 1) dane identyfikacyjne, o których mowa w art. 36 ust. 1 TerroryzmU, klienta biura rachunkowego przekazującego zawiadomienie;
- 2) posiadane dane identyfikacyjne, o których mowa w art. 36 ust. 1 TerroryzmU, osób fizycznych, osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej niebędących klientami biura rachunkowego przekazującego zawiadomienie;
- 3) rodzaj i wielkość wartości majątkowych oraz miejsce ich przechowywania;
- 4) numer rachunku prowadzonego dla klienta biura rachunkowego przekazującego zawiadomienie, oznaczony identyfikatorem IBAN lub identyfikatorem zawierającym kod kraju, oraz numer rachunku w przypadku rachunków nieoznaczonych IBAN;
- 5) posiadane informacje, o których mowa w art. 72 ust. 6 TerroryzmU, w odniesieniu do transakcji lub prób ich przeprowadzenia;
- 6) wskazanie państwa Europejskiego Obszaru Gospodarczego, z którym jest powiązana transakcja, jeżeli została przeprowadzona w ramach działalności transgranicznej;

- 7) posiadane informacje o rozpoznanym ryzyku prania pieniędzy lub finansowania terroryzmu oraz o czynie zabronionym, z którego mogą pochodzić wartości majątkowe;
- 8) uzasadnienie przekazania zawiadomienia.

Przy tym nie ma określonych na dzisiaj wzorów takich zawiadomień.

Zgodnie z art. 74 ust. 3 pkt 8 oraz z art. 86 ust. 2 zdanie 2 w zw. z art. 74 ust. 3 pkt 8 Terroryzmu powyższe zawiadomienia powinny zawierać m.in. uzasadnienie. Oznacza to, że biuro rachunkowe, w kontekście ustalenia okoliczności mogących wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, opisuje m.in.:

- 1) jakie informacje i dokumenty zostały zebrane przed nawiązaniem stosunków gospodarczych (np. jaki ustalono profil działalności gospodarczej klienta, jaka została zadeklarowana częstotliwość transakcji, jakie zostało wskazane źródło pochodzenia wartości majątkowych);
- 2) jakie informacje biuro rachunkowe zebrało w trakcie trwania stosunków gospodarczych (np. czy uzyskiwane wartości majątkowe oraz wykonywane transakcje były zgodne z ustalonym profilem działalności gospodarczej, czy dochodziło do zmian właścicielskich, czy jakiegokolwiek okoliczności wpłynęły na zmianę ryzyka przypisanego klientowi);
- 3) jakie środki bezpieczeństwa finansowego zostały zastosowane po ustaleniu okoliczności mogących wskazywać na podejrzenie popełnienia przestępstwa oraz jaki był ich wynik (np. czy dokonano analizy transakcji klienta z wybranymi kontrahentami i wytypowano konkretne przypadki do dalszej pogłębionej analizy);
- 4) jakie czynności w stosunku do klienta zostały podjęte po ustaleniu okoliczności mogących wskazywać na podejrzenie popełnienia przestępstwa oraz jaki był efekt (np. czy podjęto kontakt telefoniczny z klientem lub zobowiązano klienta do przedstawienia umów i faktur, czy klient przedstawił wnioskowaną dokumentację w całości lub części);
- 5) jakie informacje i dokumenty zostały przeanalizowane po ustaleniu okoliczności mogących wskazywać na podejrzenie popełnienia przestępstwa oraz jaki był efekt (np. czy wykryto niejasności w przedstawionych przez klienta umowach i fakturach);
- 6) jaki był wpływ ustalenia okoliczności mogących wskazywać na podejrzenie popełnienia przestępstwa na stosunki gospodarcze (np. czy wskutek braku przedstawienia dokumentów przez klienta biuro rachunkowe podjęło decyzję o nieprzeprowadzaniu transakcji lub o rozwiązaniu stosunków gospodarczych).

Zgodnie z art. 76 ust. 1 Terroryzmu biuro rachunkowe na żądanie Generalnego Inspektora niezwłocznie przekazuje lub udostępnia posiadane informacje lub dokumenty niezbędne do realizacji zadań Generalnego Inspektora określonych w ustawie. W takim przypadku biuro rachunkowe jest zobligowane przekazać między innymi pełne i wyczerpujące informacje i kopie dokumentów uzyskanych w wyniku stosowania środków bezpieczeństwa finansowego (przykładowo wszystkie dokumenty będące podstawą do złożenia zawiadomienia, o którym mowa w art. 74 lub art. 86 Terroryzmu).

W celu realizacji po raz pierwszy obowiązków, o których mowa w art. 74 lub art. 86 TerroryzmU, biuro rachunkowe przekazuje do Generalnego Inspektora formularz identyfikujący biuro rachunkowe. Wzór formularza określa rozporządzenie Ministra Finansów z 4.10.2018 r. w sprawie przekazywania informacji o transakcjach oraz formularza identyfikującego instytucję obowiązującą (Dz.U. z 2018 r. poz. 1946).

Formularz składa się elektronicznie na stronie <https://www.giif.mofnet.gov.pl/>.

Ważne

Z chwilą przekazania zawiadomienia dotyczącego uzasadnionego podejrzenia prania pieniędzy i finansowania terroryzmu biuro rachunkowe nie może przeprowadzić transakcji, której ono dotyczy.

Po otrzymaniu takiego zawiadomienia GIIF niezwłocznie dokonuje potwierdzenia jego przyjęcia, w postaci urzędowego poświadczenia odbioru, zawierającego w szczególności datę i godzinę przyjęcia zawiadomienia. Czynność ta ma istotne znaczenie dla dalszego trybu postępowania, bowiem **od tego momentu rozpoczyna bieg 24 godzinny okres, w którym GIIF może podjąć decyzję o wstrzymaniu transakcji lub blokadzie rachunku.**

GIIF w przypadku uznania, że transakcja może mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, przekazuje biurowi rachunkowemu żądanie wstrzymania transakcji lub blokady rachunku na okres nie dłuższy niż **96 godzin**, licząc od daty i godziny wskazanych w potwierdzeniu. Niezwłocznie po otrzymaniu tego żądania biuro rachunkowe wstrzymuje transakcję lub blokuje rachunek. W żądaniu GIIF określa wartości majątkowe objęte żądaniem.

1.12. Termin przechowywania danych

Zastosowane przez biura rachunkowe środki bezpieczeństwa powinny zostać odpowiednio udokumentowane (art. 34 ust. 3 TerroryzmU). Dokumenty uzyskane w trakcie stosowania środków bezpieczeństwa finansowego podlegają archiwizacji i muszą być przechowywane przynajmniej przez **okres 5 lat**, licząc od pierwszego dnia roku następującego po roku, w którym dany środek bezpieczeństwa został zastosowany (art. 49 ust. 1 TerroryzmU).

Podstawa prawna:

- art. 2, art. 6–8, art. 27, art. 33–37, art. 39, art. 42, art. 43, art. 46, art. 74, art. 49, art. 50, art. 52, art. 53 ust. 2, art. 74, art. 76 ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2020 r. poz. 971 ze zm.)
- rozporządzenie Ministra Finansów z 4.10.2018 r. w sprawie przekazywania informacji o transakcjach oraz formularza identyfikującego instytucję obowiązującą (Dz.U. z 2018 r. poz. 1946)

2. Kary dla biura rachunkowego za naruszenie ustawy

Niewykonanie lub nieprawidłowe wykonanie przez biuro rachunkowe obowiązków nałożonych na nie przez TerroryzmU podlega karom administracyjnym. Do katalogu kar administracyjnych przewidzianych ustawą zalicza się:

- 1) publikację informacji o biurze rachunkowym oraz zakresie naruszenia w BIP;
- 2) nakaz zaprzestania podejmowania przez biuro rachunkowe określonych czynności;
- 3) cofnięcie koncesji lub zezwolenia albo wykreślenie z rejestru działalności regulowanej;
- 4) zakaz pełnienia obowiązków na stanowisku kierowniczym przez osobę odpowiedzialną za naruszenie przez biuro rachunkowe przepisów ustawy przez okres nie dłuższy niż rok;
- 5) karę pieniężną (w wysokości dwukrotności osiągniętej korzyści lub unikniętej straty lub w wypadku gdy kwoty tej nie da się ustalić – do 1 000 000 euro).

Podstawa prawna:

- art. 150 ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2020 r. poz. 971 ze zm.)

3. Kontrola GIIF

GIIF sprawuje kontrolę wykonywania przez biuro rachunkowe obowiązków w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Biuro rachunkowe jest zobligowane, na gruncie art. 137 TerroryzmU, do zapewnienia kontrolerowi warunków i środków niezbędnych do sprawnego przeprowadzenia kontroli, w szczególności do przedstawienia w wyznaczonym terminie żądanych dokumentów i materiałów, zapewnienia terminowego udzielania informacji, udostępnienia w niezbędnym zakresie środków łączności, a także innych urządzeń technicznych, umożliwienia sporządzania kopii, filmowania, fotografowania, dokonywania nagrań dźwiękowych oraz przedłożenia urzędowego tłumaczenia na język polski sporządzonych w języku obcym dokumentów mających znaczenie dla kontroli. Biuro rachunkowe pokrywa również koszty wykonania ww. obowiązków.

Podstawa prawna:

- art. 137 ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2020 r. poz. 971 ze zm.)

Marta Wysocka-Fronczek

4. Wzory dokumentów

Niniejszy rozdział zawiera 8 gotowych wzorów, które zostały przygotowane przez autorkę w celu ułatwienia wdrożenia w biurze rachunkowym przepisów o AML.

4.1. Wzór uchwały zarządu

Uchwała Zarządu nr /.....

z dnia

§ 1

Zarząd Spółki pod firmą na podstawie art. 6 ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wyznacza Pana/Panią jako przedstawiciela kadry kierowniczej wyższego szczebla odpowiedzialnego za wykonywanie obowiązków określonych w tej ustawie.

§ 2

Zarząd Spółki pod firmą na podstawie art. 7 ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wyznacza Pana/Panią jako członka zarządu odpowiedzialnego za wdrażanie obowiązków określonych w tej ustawie.

§ 3

Zarząd Spółki pod firmą na podstawie art. 8 ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wyznacza Pana/Panią jako pracownika zajmującego kierownicze stanowisko odpowiedzialnego za zapewnienie zgodności działalności biura rachun-

kowego oraz jego pracowników i innych osób wykonujących czynności na rzecz tego biura rachunkowego z przepisami tej ustawy.

§ 4

Uchwała została podjęta jednomyślnie.

§ 5

Niniejsza uchwała wchodzi w życie z dniem jej uchwalenia.

Zarząd Spółki

.....

[Prezes zarządu]

.....

[Wiceprezes zarządu]

4.2. Wzór powierzenia obowiązków z zakresu AML

Zakres obowiązków związanych z ustawą z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu

- opracowanie regulacji wewnętrznych oraz wytycznych i standardów dotyczących AML,
- monitorowanie i weryfikacja transakcji klientów pod kątem podejrzeń prania pieniędzy lub finansowania terroryzmu,
- sporządzanie zawiadomień do GIIF dotyczących podejrzeń prania pieniędzy lub finansowania terroryzmu,
- opracowywanie i aktualizacja analizy oceny ryzyka,
- przeprowadzanie szkoleń wewnętrznych z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu,
- współpraca z organami nadzoru i instytucjami upoważnionymi do kontroli w zakresie przeciwdziałania praniu pieniędzy.

4.3. Wewnętrzna regulacja o przeciwdziałaniu praniu brudnych pieniędzy

Wewnętrzna instrukcja w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu

§ 1

Postanowienia ogólne

1. Niniejsza Instrukcja określa sposób postępowania w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.
2. Obowiązek ustanowienia i stosowania instrukcji wynika z art. 50 ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (dalej jako Ustawa).
3. Instrukcja opisuje sposoby identyfikacji i weryfikacji tożsamości Klienta, oceny stosunków gospodarczych, identyfikacji Klientów o statusie PEP, identyfikacji i weryfikacji tożsamości beneficjenta rzeczywistego oraz przeprowadzania oceny ryzyka prania pieniędzy w Spółce.

§ 2

Ilekcioć w niniejszej instrukcji mowa jest o:

Beneficjencie rzeczywistym – rozumie się przez to każdą osobę fizyczną sprawującą bezpośrednio lub pośrednio kontrolę nad klientem poprzez posiadane uprawnienia, które wynikają z okoliczności prawnych lub faktycznych, umożliwiające wywieranie decydującego wpływu na czynności lub działania podejmowane przez klienta, lub każdą osobę fizyczną, w imieniu której są nawiązywane stosunki gospodarcze lub jest przeprowadzana transakcja okazjonalna, w tym:

- a) w przypadku osoby prawnej innej niż spółka, której papiery wartościowe są dopuszczone do obrotu na rynku regulowanym podlegającym wymogom ujawniania informacji wynikającym z przepisów prawa Unii Europejskiej lub odpowiadających im przepisów prawa państwa trzeciego:
 - osobę fizyczną będącą udziałowcem lub akcjonariuszem, której przysługuje prawo własności więcej niż 25% ogólnej liczby udziałów lub akcji tej osoby prawnej,
 - osobę fizyczną dysponującą więcej niż 25% ogólnej liczby głosów w organie stanowiącym tej osoby prawnej, także jako zastawnik albo użytkownik, lub na podstawie porozumień z innymi uprawnionymi do głosu,
 - osobę fizyczną sprawującą kontrolę nad osobą prawną lub osobami prawnymi, którym łącznie przysługuje prawo własności więcej niż 25% ogólnej liczby udziałów lub akcji lub które łącznie dysponują więcej niż 25% ogólnej liczby głosów w organie stanowiącym tej osoby prawnej, także jako zastawnik albo użytkownik, lub na podstawie porozumień z innymi uprawnionymi do głosu,
 - osobę fizyczną sprawującą kontrolę nad osobą prawną poprzez posiadanie uprawnień, o których mowa w art. 3 ust. 1 pkt 37 ustawy z dnia 29.4.1994 r. o rachunkowości (Dz.U. z 2021 r. poz. 217), lub
 - osobę fizyczną zajmującą wyższe stanowisko kierownicze w przypadku udokumentowanego braku możliwości ustalenia lub wątpliwości co do tożsamości osób fizycznych określonych w tiret pierwsze–czwarte oraz w przypadku niestwierdzenia podejrzenia prania pieniędzy lub finansowania terroryzmu,

- b) w przypadku trustu:
 - założyciela,
 - powiernika,
 - nadzorcę, jeżeli został ustanowiony,
 - beneficjenta lub – w przypadku gdy osoby fizyczne czerpiące korzyści z danego trustu nie zostały jeszcze określone – grupę osób, w których głównym interesie powstał lub działa trust,
 - inną osobę sprawującą kontrolę nad trustem,
 - inną osobę fizyczną posiadającą uprawnienia lub wykonującą obowiązki równoważne z określonymi w tiret pierwsze–piąte,
- c) w przypadku osoby fizycznej prowadzącej działalność gospodarczą, wobec której nie stwierdzono przesłanek lub okoliczności mogących wskazywać na fakt sprawowania kontroli nad nią przez inną osobę fizyczną lub osoby fizyczne, przyjmuje się, że taka osoba fizyczna jest jednocześnie beneficjentem rzeczywistym.

Członkowie rodziny osoby zajmującej eksponowane stanowisko polityczne (PEP) – rozumie się przez nich:

- a) małżonka lub osobę pozostającą we wspólnym pożyciu z osobą zajmującą eksponowane stanowisko polityczne,
- b) dziecko osoby zajmującej eksponowane stanowisko polityczne i jego małżonka lub osoby pozostającej we wspólnym pożyciu,
- c) rodziców osoby zajmującej eksponowane stanowisko polityczne.

Finansowanie terroryzmu – czyn określony w art. 165a ustawy z 6.6.1997 r. – Kodeks karny (t.j. Dz.U. z 2020 r. poz. 1444 ze zm.; dalej: KK).

GIIF – Generalny Inspektor Informacji Finansowej.

Kadra kierownicza wyższego szczebla – rozumie się przez to członka zarządu, dyrektora lub pracownika instytucji obowiązanej, posiadającego wiedzę z zakresu ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z działalnością instytucji obowiązanej oraz podejmującego decyzje mające wpływ na to ryzyko.

Klient – rozumie się przez to osobę fizyczną, osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, której instytucja obowiązana świadczy usługi lub dla której wykonuje czynności wchodzące w zakres prowadzonej przez nią działalności zawodowej, w tym z którą instytucja obowiązana nawiązuje stosunki gospodarcze lub na zlecenie której przeprowadza transakcję okazjonalną.

Koordynator ds. AML – osoba, o której mowa w art. 6 Ustawy.

Listy sankcyjne – listy osób i podmiotów publikowane w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Finansów, o których mowa w art. 118 ust. 1 Ustawy, oraz wykazy osób, grup i podmiotów, przeciwko którym wprowadzone zostały w prawodawstwie Unii Europejskiej szczególne środki ograniczające stosowane wprost na terenie wspólnoty.

Nieudostępnianie wartości majątkowych – szczególny środek ograniczający, który polega na nieudostępnianiu wartości majątkowych bezpośrednio ani pośrednio osobom i podmiotom wpisanym na listy sankcyjne ani na ich rzecz, w szczególności polega na nieudzielaniu pożyczek, kredytu konsumenckiego lub kredytu hipotecznego, niedokonywaniu darowizn, niedokonywaniu płatności za towary lub usługi.

Osoba zajmująca eksponowane stanowisko polityczne (PEP) – rozumie się przez to, z wyłączeniem grup stanowisk średniego i niższego szczebla, osoby zajmujące znaczące stanowiska publiczne lub pełniące znaczące funkcje publiczne, w tym:

- szefów państw, szefów rządów, ministrów, wiceministrów oraz sekretarzy stanu,
- członków parlamentu lub podobnych organów ustawodawczych,
- członków organów zarządzających partii politycznych,
- członków sądów najwyższych, trybunałów konstytucyjnych oraz innych organów sądowych wysokiego szczebla, których decyzje nie podlegają zaskarżeniu, z wyjątkiem trybów nadzwyczajnych,
- członków trybunałów obrachunkowych lub zarządów banków centralnych,
- ambasadorów, *chargés d'affaires* oraz wyższych oficerów sił zbrojnych,
- 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,
- dyrektorów, zastępców dyrektorów oraz członków organów organizacji międzynarodowych lub osoby pełniące równoważne funkcje w tych organizacjach,
- dyrektorów generalnych w urzędach naczelnych i centralnych organów państwowych oraz dyrektorów generalnych urzędów wojewódzkich,
- inne osoby zajmujące stanowiska publiczne lub pełniące funkcje publiczne w organach państwa lub centralnych organach administracji rządowej.

Osoby znane jako bliscy współpracownicy osoby zajmującej eksponowane stanowisko polityczne – rozumie się przez to:

- 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.

Pranie pieniędzy – czyn określony w art. 299 KK.

Przeprowadzanie transakcji – rozumie się przez to wykonanie przez instytucję obowiązaną zlecenia lub dyspozycji wydanej przez Klienta lub osobę działającą w jego imieniu.

Realizator ds. AML – osoba zajmująca kierownicze stanowisko, o której mowa w art. 8 Ustawy, odpowiedzialna za zapewnienie zgodności działalności, jej pracowników oraz innych osób wykonujących na jej rzecz czynności z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, wykonująca, na podstawie umocowania, wskazane obowiązki określone w instrukcji.

Stosunki gospodarcze – rozumie się przez to stosunki instytucji obowiązanej z klientem związane z działalnością zawodową instytucji obowiązanej, które w chwili ich nawiązywania wykazują cechę trwałości.

Transakcja – 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.

Transakcja okazjonalna – transakcja, która nie jest przeprowadzana w ramach stosunków gospodarczych.

Transakcja powiązana – to co najmniej dwie lub więcej transakcji jednostkowych o wartości każdej z nich poniżej 15 000 euro, jeżeli ich łączna wartość przekracza 15 000 euro, a okoliczności ich dokonywania wskazują, że posłużono się więcej niż jedną transakcją w celu uniknięcia ujawnienia wobec instytucji obowiązanej przekroczenia wartości 15 000 euro, jako kwoty progowej, powodującej rejestrację transakcji. Powiązanie transakcji jednostkowych może być:

- 1) podmiotowe – w szczególności gdy występuje tożsamość zlecającego lub beneficjenta (a także ich pełnomocników, w przypadku osób prawnych także składu ich organów) lub identyczność numerów rachunków bankowych,
- 2) przedmiotowe – zbieżność deklarowanej ekonomicznej treści transakcji lub jej podstawy prawnej.

Transakcja powiązana może być realizowana jednym zleceniem zbiorczym albo, co jest regułą, serią zleceń (dyspozycji). Nie ustala się okresu, w którym seria zleceń może stanowić o uznaniu transakcji jednostkowych za transakcję powiązaną.

Transakcja podejrzana – transakcja, której okoliczności wskazują, że może ona mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, bez względu na jej wartość i charakter.

Transfer środków pieniężnych – dowolna transakcja przynajmniej częściowo realizowana drogą elektroniczną w imieniu płatnika za pośrednictwem dostawcy usług płatniczych (np. banku) w celu udostępnienia środków pieniężnych odbiorcy za pośrednictwem dostawcy usług płatniczych, bez względu na to, czy płatnik i odbiorca są tą samą osobą (np. przelew między własnymi rachunkami), i niezależnie od tego, czy dostawca usług płatniczych płatnika jest tożsamy z dostawcą usług płatniczych odbiorcy (np. przelew w ramach jednego banku). W szczególności transferami środków pieniężnych będą spełniające powyższe warunki: polecenie przelewu, polecenie zapłaty, przekaz pieniężny czy transfery wykonywane przy wykorzystaniu karty płatniczej.

Trust – rozumie się przez to regulowany przepisami prawa obcego stosunek prawny wynikający ze zdarzenia prawnego, umowy lub porozumienia, w tym zespołu takich zdarzeń lub czynności prawnych, na podstawie którego dokonuje się przeniesienia własności lub posiadania wartości majątkowych na powiernika w celu sprawowania zarządu powierniczego oraz udostępniania tych wartości beneficjentom tego stosunku.

Ustawa – ustawa z 1.3.2018 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wraz z nowelizacjami.

Wartości majątkowe – prawa majątkowe lub inne mienie ruchome lub nieruchomości, środki płatnicze, instrumenty finansowe w rozumieniu ustawy z 29.7.2005 r. o obrocie instrumentami finansowymi, inne papiery wartościowe, wartości dewizowe oraz waluty wirtualne.

§ 3

Pranie pieniędzy – to podejmowanie działań (czynności) mających na celu ukrycie korzyści majątkowych uzyskanych z popełnionych przestępstw (bez względu na to, czy były one popełniane przez ukrywającego czy przez osoby trzecie) i nadanie im znamion legalnego pochodzenia, poprzez znalezienie (stworzenie) podstaw prawnych uzasadniających posiadanie tych korzyści majątkowych. Brudne pieniądze pochodzą z działalności przestępczej, przynoszącej dochody, których nie można zaksięgować i zapłacić za nie podatku, dlatego też zostają wprowadzane do obiegu w sposób zamaskowany z wykorzystaniem legalnych transakcji. Proceder Prania pieniędzy ma umożliwić sprawcom swobodne korzystanie z brudnych pieniędzy, w taki sposób, by nie wzbudzić zainteresowania organów kontroli i ścigania.

1. Najczęstsze źródła brudnych pieniędzy to:

- 1) Tzw. szara strefa, czyli środki pochodzące z unikania płacenia podatków.

- 2) Produkcja, handel i przemysł narkotyków.
- 3) Zakup dzieł sztuki.
- 4) Nielegalny handel bronią.
- 5) Przestępstwa przeciwko życiu i zdrowiu, m.in. zabójstwa na zlecenie, przestępstwa porachunkowe.
- 6) Przestępstwa przeciwko mieniu, np. napady na instytucje finansowe, egzekwowanie długów, wymuszanie za ochronę, kradzieże i przemysł samochodów, kradzieże i przemysł dzieł sztuki oraz antyków.
- 7) Przemysł różnych atrakcyjnych towarów, np. sprzętu audio-video, papierosów, alkoholu.
- 8) Fałszerstwa: pieniędzy, papierów wartościowych, faktur, czeków, kart kredytowych i dokumentów bankowych (polecenia przelewu/wypłaty), stempli dziennych, a także dokumentów tożsamości.
- 9) Defraudacje i wyprowadzanie środków finansowych z rachunków bankowych, np. phishing, fraudy.

§ 4

1. **Terroryzm** – jest formą przemocy politycznej, jego najważniejszą cechą jest stosowanie przemocy lub groźby jej użycia, przy czym jest to przemoc nieprzewidywalna, drastyczna i spektakularna. Efekt zastraszania osiągany jest m.in. przez wykorzystanie w zamachach niewinnych, przypadkowych ofiar.

2. Najczęstsze źródła Finansowania terroryzmu to:

- 1) Wykorzystywanie instytucji typu non profit: organizacji charytatywnych, fundacji, kościołów i związków wyznaniowych, np. organizacja taka prowadzi samodzielną działalność, ale część zbieranych środków przekazuje terrorystom lub też organizacja działa wyłącznie fikcyjnie, jako „przykrywką” i wszystkie zbierane środki trafiają w ręce terrorystów. Terrorysty wykorzystują również takie podmioty w celach propagandowych i rekrutacyjnych, poprzez ich faktyczne sponsorowanie własnymi środkami i świadczenie pomocy finansowej potrzebującym, aby mieli oni wrażenie, że otrzymują pomoc od terrorystów.
- 2) Dochody uzyskiwane z legalnej działalności gospodarczej osób powiązanych z terroryzmem. Wykorzystywane są tu głównie drobne podmioty prowadzące działalność związaną z obrotem gotówkowym, stosujące uproszczoną księgowość. Mogą one łatwo ukryć mieszanie dochodów, gdy część środków przekazywana jest członkom organizacji terrorystycznych, np. restauracje, warsztaty rzemieślnicze, sklepy. Często są to podmioty prowadzone przez członków jednej grupy etnicznej lub religijnej.
- 3) Dochody z działalności przestępczej – pochodzące z popełnianych prostych przestępstw typu kradzież, wyłudzenia świadczeń społecznych, aż do zorganizowanych procederów takich jak handel narkotykami, handel bronią, pranie pieniędzy, porwania dla okupu, wymuszenia, oszustwa i wyłudzenia finansowe (terrorysty postępują analogicznie jak zorganizowane grupy przestępcze lub z nimi współpracują).
- 4) Środki przekazywane z państw wspierających terroryzm.
- 5) Środki pochodzą od pojedynczej osoby fizycznej dysponującej odpowiednim majątkiem.
- 6) Dochody uzyskiwane z eksploatacji i sprzedaży zasobów naturalnych, np. diamentów, w tzw. upadłych państwach ogarniętych wojną domową, w których nie ma sprawnej władzy państwowej.
- 7) Własne dochody członków, np. z legalnej pracy zarobkowej, zasiłków społecznych – czyli samofinansowanie się, które jest możliwe w przypadku niewielkich grup terrorystycznych lub komórek działających w ramach większej sieci.

W przypadku legalnych źródeł funduszy mówi się o tzw. „odwrotnym praniu” lub „brudzeniu” pieniędzy (ang. *black washing*), jako przeciwieństwie Prania pieniędzy. Środki finansowe pozyski-

wane w uczciwy sposób drogą skomplikowanych transakcji i manipulacji trafiają do terrorystów w celu finansowania ich działalności. Wykorzystywanie nawet legalnych dochodów do finansowania terroryzmu jest czynem zabronionym.

3. Funkcjonowanie grup terrorystycznych wymaga nie tylko pozyskiwania środków, ale również ich dystrybucję w ramach sieci. Wykorzystywane są trzy główne metody transferowania:

- 1) System finansowy – rozliczenia bezgotówkowe, przy wykorzystaniu różnorodnych pośredników finansowych; zapewniają szybki transfer środków pomiędzy odległymi punktami; w tym również korzystanie z kart prepaid (przedpłaconych), wykorzystanie kryptowaluty, zakładanie rachunków na słupa, fikcyjne faktury.
- 2) Fizyczny przewóz gotówki przez kurierów oraz tzw. systemy bankowości podziemnej – co zapewnia względna anonimowość; kurierzy zamiast gotówki mogą również przewozić kamienie szlachetne.
- 3) Międzynarodowy system wymiany handlowej, obrót towarami (np. diamenty), które są sprzedawane, a środki przeznaczone na finansowanie terroryzmu.

§ 5

Fazy Prania pieniędzy i rodzaje Transakcji podejrzanych

1. Fazy Prania pieniędzy.

Przyjmuje się, że typowy proceder Prania pieniędzy przebiega w trzech stadiach, jednakże w praktyce nie wszystkie fazy muszą wystąpić, a czasami fazy te mogą się na siebie nakładać:

- 1) I faza – lokowanie (umieszczanie, umiejscowienie);
- 2) II faza – maskowanie (rozwarstwienie, mnożenie, ukrywanie, odseparowywanie);
- 3) III faza – integracja (legitymacja, włączenie).

2. I faza – stanowi fizyczne rozporządzenie dochodami pochodzącymi bezpośrednio z przestępstwa, poprzedzona jest najczęściej przewiezieniem brudnej gotówki jak najdalej od źródła jej pochodzenia. Polega na wprowadzeniu brudnych pieniędzy do obrotu finansowego, najczęściej poprzez wpłaty gotówkowe na rachunki bankowe, rzadziej poprzez transakcje bezgotówkowe (przelanie środków z wyłudzeń kredytów, odszkodowań z tytułu ubezpieczenia, defraudacji z rachunku).

- 1) Cechy: prostota, jednorodność, powtarzalność, krótkoterminowość dokonywanych transakcji.
- 2) Najczęściej stosowane techniki:
 - a) rozdrabnianie wpłat – tzw. smurfing lub dzielenie wpłat – tzw. structuring, tj. dokonywanie wielu depozytów lub wpłat na rachunki bankowe poniżej limitu obligującego do wykonywania czynności identyfikacji i rejestracji transakcji w rejestrze,
 - b) otwieranie rachunków bankowych na osoby podstawione, tzw. słupów (np. studenci, bezdomni), fałszywe nazwiska, nieistniejące organizacje, stowarzyszenia, fundacje, przedsiębiorstwa „przykrywkę”,
 - c) „mieszanie”, tj. łączenie brudnych pieniędzy z legalnymi dochodami podmiotu gospodarczego. Rodzaje działalności gospodarczej przynoszące zmienne w czasie i trudne do zweryfikowania pod kątem wysokości dochody, a przez to stwarzające sposobność do „wyprania” środków to np.: restauracje, hotele, pizzerie, pralnie chemiczne, bary szybkiej obsługi,
 - d) wymiana walut lub nominałów – z niskich kwot na wysokie.
- 3) I faza odgrywa zasadniczą rolę w procesie prania i jest najdogodniejszym i stosunkowo najłatwiejszym momentem do wykrycia przestępstwa.

2. II faza – następuje seria transakcji mająca na celu oddzielenie brudnych pieniędzy od źródeł ich pochodzenia; celem staje się przeprowadzenie jak największej ilości transakcji w jak najkrótszym czasie, tak by uległ zatarciu ślad wskazujący na nielegalne bądź nieujawnione pochodzenie środków; najczęściej wykorzystywane są przelewy elektroniczne.

- 1) Cechy: duża ilość realizowanych transakcji, transakcje często nie mają ekonomicznego uzasadnienia, prane środki często zmieniają formę, wykorzystywanie elektronicznych form przekazu pieniędzy.
- 2) Najczęściej stosowane techniki:
 - a) „skrzynka rozdzielcza” – czyli zasilanie rachunku niewielkimi wpłatami z różnych źródeł, a następnie po osiągnięciu odpowiednio wysokiego salda przelanie środków na inny rachunek,
 - b) zakup aktywów,
 - c) transfery zagraniczne,
 - d) rachunek docelowy – polega na przelewaniu wysokich kwot na jeden rachunek, z którego są one niezwłocznie wypłacane w gotówce.

3. III faza – polega na stworzeniu rzekomego prawnego wyjaśnienia źródeł pochodzenia wypłyniętych środków i wprowadzenie ich do legalnego obrotu poprzez:

- 1) transakcje kupna-sprzedaży środków trwałych (np. jachtów, nieruchomości, antyków),
- 2) zakup upadających przedsiębiorstw,
- 3) uzyskiwanie kredytu na realizację inwestycji, bez względu na jego koszt, a następnie jego szybka spłata z nielegalnych źródeł,
- 4) transakcje w imporcie i eksporcie – często połączone z przemytem gotówki zagranicę.

§ 6

1. Rodzaje Transakcji podejrzanych:

- 1) **transakcja nadzwyczajna** – transakcja realizowana na zapotrzebowanie Klienta w sposób kosztowny, dotycząca wysokich kwot i nieuzasadniona pod względem gospodarczym,
- 2) **transakcja niejasna** – transakcja, której sens ekonomiczno-finansowy jest niejednoznaczny, tzn. której charakterystyki finansowe są niepełne albo cel realizacji niedookreślony,
- 3) **transakcja nietypowa** – transakcja niepodobna do innych realizowanych przez danego Klienta albo określoną kategorię Klientów, np. nie ma związku z zakresem działalności zleciennodawcy; lub też transakcja, w trakcie realizacji której sposób zachowania Klienta budzi podejrzenia pracownika, np. gdy Klient dokonuje transakcji bankowych z uczestnictwem osób trzecich; transakcja lub jej niektóre elementy są nietypowe w porównaniu z wcześniej przeprowadzanymi przez Klienta.

§ 7

Środki bezpieczeństwa finansowego

1. Instytucja zobowiązana jest do wykonywania środków bezpieczeństwa finansowego.

2. Środki bezpieczeństwa finansowego polegają na:

- a) identyfikacji klienta i weryfikacji jego tożsamości;
- b) identyfikacji beneficjenta rzeczywistego oraz podejmowaniu uzasadnionych czynności w celu:
 - weryfikacji jego tożsamości,
 - ustalenia struktury własności i kontroli – w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej,
- c) ocenie stosunków gospodarczych i, stosownie do sytuacji, uzyskaniu informacji na temat ich celu i zamierzonego charakteru;

- d) bieżącym monitorowaniu stosunków gospodarczych z klientem, w tym:
 - 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,
 - badanie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta – w przypadkach uzasadnionych okolicznościami,
 - zapewnienie, że posiadane dokumenty, dane lub informacje dotyczące stosunków gospodarczych są na bieżąco aktualizowane.
3. Środki bezpieczeństwa finansowego są stosowane w szczególności:
- a) przy nawiązywaniu stosunków gospodarczych;
 - b) gdy istnieje podejrzenie prania pieniędzy lub finansowania terroryzmu bez względu na wartość transakcji, formę organizacyjną oraz rodzaj klienta;
 - c) gdy zachodzi wątpliwość co do prawdziwości lub kompletności dotychczas uzyskanych danych identyfikacyjnych klienta.
4. Środki bezpieczeństwa finansowego powinny być stosowane wobec klientów, z którymi zawierane są umowy na dostarczenie usług prowadzenia ksiąg rachunkowych/usług polegających na sporządzaniu deklaracji, prowadzeniu ksiąg podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego.

§ 8

Identyfikacja tożsamości klienta

1. Pracownik odpowiedzialny za obsługę lub współpracę z klientem identyfikuje:
- 1) tożsamość Klienta w przypadku osób prawnych poprzez ustalenie i zapisanie:
 - a) nazwy (firmy),
 - b) formy organizacyjnej,
 - c) adresu siedziby lub adresu prowadzenia działalności,
 - d) NIP, a w przypadku braku takiego numeru – państwa rejestracji, rejestru handlowego oraz numeru i daty rejestracji,
 - e) imienia i nazwiska oraz numeru PESEL lub daty urodzenia – w przypadku gdy nie nadano numeru PESEL, oraz państwa urodzenia osoby reprezentującej Klienta;
 - 2) tożsamość Klienta w przypadku osób fizycznych poprzez ustalenie i zapisanie:
 - a) imienia i nazwiska,
 - b) obywatelstwa,
 - c) numeru PESEL lub daty urodzenia – w przypadku gdy nie nadano numeru PESEL, oraz państwa urodzenia,
 - d) serii i numeru dokumentu tożsamości,
 - e) adresu zamieszkania – w przypadku posiadania tej informacji przez Spółkę,
 - f) jeżeli klient jest osobą fizyczną prowadzącą działalność gospodarczą – dodatkowo nazwy, NIP oraz adresu głównego wykonywania działalności gospodarczej;
 - 3) tożsamość osoby upoważnionej do działania przez Klienta poprzez ustalenie i zapisanie:
 - a) imienia i nazwiska,
 - b) obywatelstwa,
 - c) numeru PESEL lub daty urodzenia – w przypadku gdy nie nadano numeru PESEL,
 - d) państwa urodzenia,
 - e) serii i numeru dokumentu tożsamości,
 - f) adresu zamieszkania.
 - 4) Weryfikacja ustalonych danych odbywa się na podstawie:

- a) dokumentów rejestrowych Klienta (KRS, CEIDG lub innych odpowiednich);
- b) weryfikacji dowodów tożsamości (w przypadku osób fizycznych);
- c) koncesji, licencji, zezwoleń na prowadzenie działalności lub innych dokumentów wydanych przez właściwe organy, potwierdzających uprawnienie do wykonywania określonej działalności;
- d) odpisów z rejestru działalności regulowanej, np. rejestru funduszy inwestycyjnych;
- e) umowy, statutu Klienta;
- f) dostępnych wewnętrznych baz danych;
- g) dokumentów w formie aktu notarialnego.

§ 9

Identyfikacja beneficjenta rzeczywistego

1. Instytucja obowiązana w ramach stosowania środków bezpieczeństwa finansowego jest zobligowana do ustalenia beneficjenta rzeczywistego klienta.

2. Identyfikacja tożsamości beneficjenta rzeczywistego polega na ustaleniu i zapisaniu:

- 1) imienia i nazwiska;
- 2) obywatelstwa;

oraz w przypadku możliwości uzyskania przez Spółkę:

- 3) numeru PESEL lub daty urodzenia – w przypadku gdy nie nadano numeru PESEL;
- 4) państwa urodzenia;
- 5) serii i numeru dokumentu tożsamości;
- 6) adresu zamieszkania.

3. Ustalenie i weryfikacja tożsamości beneficjenta rzeczywistego następują na podstawie i według kolejności złożonego przez klienta „Oświadczenia o beneficjencie rzeczywistym klienta” lub wyciągu z KRS, lub zaświadczenia o wpisie do ewidencji działalności gospodarczej, w tym udostępnianych na zewnętrznych stronach internetowych (KRS, CEIDG).

§ 10

Identyfikacja PEP

1. W celu ustalenia, czy klient lub beneficjent rzeczywisty jest osobą zajmującą eksponowane stanowisko polityczne (PEP), instytucja obowiązana przyjmuje od klienta w formie pisemnej „Oświadczenie PEP”, że jest on albo nie jest osobą zajmującą takie stanowisko, składane pod rygorem odpowiedzialności karnej za złożenie fałszywego oświadczenia.

2. W przypadku stosunków gospodarczych z osobą zajmującą eksponowane stanowisko polityczne instytucja obowiązana stosuje wobec tej osoby środki bezpieczeństwa finansowego oraz podejmuje następujące działania:

- 1) uzyskuje akceptację kadry kierowniczej wyższego szczebla na nawiązanie lub kontynuację stosunków gospodarczych z osobą zajmującą eksponowane stanowisko polityczne;
- 2) stosuje odpowiednie środki w celu ustalenia źródła majątku klienta i źródła pochodzenia wartości majątkowych pozostających w dyspozycji klienta w ramach stosunków gospodarczych lub transakcji.

§ 11

Ocena ryzyka

1. Instytucja obowiązana identyfikuje i przeprowadza ocenę ryzyka prania pieniędzy i finansowania terroryzmu stosunków gospodarczych oraz transakcji okazjonalnych. Ocena podlega zapisaniu

w formie papierowej lub elektronicznej i jest przechowywana zgodnie z poniżej przyjętymi zasadami.

2. Ocena określenia ryzyka związanego z praniem pieniędzy oraz finansowaniem terroryzmu została przygotowana w oparciu o obowiązujące przepisy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wraz ze strategią przyjętą przez Generalnego Inspektora Informacji Finansowej w ramach Krajowej Oceny Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu.

3. W oparciu o ocenę ryzyka ustala się zakres stosowanych środków bezpieczeństwa finansowego.

§ 12

Szkolenia

Instytucja obowiązana:

- 1) zapewnia udział osób wykonujących obowiązki związane z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu w programach szkoleniowych dotyczących realizacji tych obowiązków,
- 2) stawia do dyspozycji pracowników i współpracowników przepisy prawne w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

§ 13

Rejestr transakcji

1. Obowiązek identyfikacji i rejestracji dotyczy transakcji, których wartość przekracza 15 000 euro, oraz transakcji podejrzanych i powiązanych.

2. Przy ustalaniu równowartości w euro stosuje się średni kurs NBP dla danej waluty obowiązujący w dniu dokonywania transakcji lub w dniu złożenia dyspozycji (zlecenia) przeprowadzenia transakcji.

3. Rejestr transakcji zawiera:

- datę przeprowadzenia transakcji,
- dane identyfikacyjne stron transakcji,
- opis transakcji (kwotę, walutę i rodzaj transakcji, okoliczności),
- 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.

3. Koordynator AML powinien zabezpieczyć prowadzony przez siebie rejestr w sposób umożliwiający dostęp do niego wyłącznie osobom upoważnionym.

4. Dane do rejestru transakcji wprowadza się i zatwierdza bezzwłocznie, nie później jednak niż następnego dnia roboczego po zrealizowaniu transakcji.

§ 14

Raportowanie do GIIF

1. Instytucja obowiązana na podstawie art. 72 Ustawy raportuje do GIIF transakcje, których wartość przekracza równowartości 15 tys. euro, oraz transakcje powiązane.

2. Termin na przekazanie danych do GIIF to 7 dni od realizacji transakcji.

3. W przypadku transakcji podejrzanej instytucja obowiązana przekazuje informację do GIIF niezwłocznie, nie później jednak niż w terminie 2 dni roboczych od dnia potwierdzenia przez instytucję obowiązana podejrzenia.

§ 15

Anonimowe zgłaszanie naruszeń

1. Instytucja obowiązana udostępnia każdemu pracownikowi lub współpracownikowi możliwość anonimowego zgłaszania informacji o rzeczywistych lub potencjalnych naruszeniach przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

2. Zgłoszenie takie może zostać złożone na podany adres e-mail lub za pośrednictwem platformy elektronicznej gwarantującej zachowanie anonimowości osobie zgłaszającej zawiadomienie.

4. Przekazanie zgłoszenia nie może stanowić żadnych sankcji dla osoby zgłaszającej, której dane są chronione z mocy prawa.

5. Dane osobowe osoby zgłaszającej chronione są polityką ochrony danych osobowych funkcjonującej w instytucji obowiązanej oraz chronione są programem szyfrującym, do którego dostęp ma jedynie osoba upoważniona i członkowie kadry kierowniczej wyższego szczebla.

6. Każde zgłoszenie musi być rozpatrzone i zweryfikowane przez Koordynatora AML.

7. W razie stwierdzenia rzeczywistego naruszenia przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu Koordynator AML musi podjąć stosowne działania eliminujące to naruszenie w terminie niezwłocznym.

§ 16

Przechowywanie dokumentów oraz raportowanie do GIIF

Rejestr transakcji, wszelkie informacje o transakcji oraz dokumenty dotyczące transakcji, kontroli GIIF, a także stosowane środki bezpieczeństwa finansowego wobec klientów będą przechowywane przez okres 5 lat.

4.4. Analiza oceny ryzyka AML

Instytucje obowiązane, które mają obowiązek identyfikacji i oceny ryzyk związanych z praniem pieniędzy i finansowaniem terroryzmu odnoszących się do ich działalności, przy sporządzaniu swoich ocen ryzyka mogą uwzględniać obowiązującą Krajową Ocenę Ryzyka Prania Pieniędzy i Finansowania Terroryzmu.

Ważne

Ocenę ryzyka należy co 2 lata aktualizować.

Ocena ryzyka prania pieniędzy oraz finansowania terroryzmu

Rozdział 1: Cel i podstawa prawna

1. Celem analizy jest określenie ryzyka związanego z praniem pieniędzy oraz finansowaniem terroryzmu w
2. Ocena określenia ryzyka związanego z praniem pieniędzy oraz finansowaniem terroryzmu została przygotowana w (należy podać rok).
3. Ocena określenia ryzyka związanego z praniem pieniędzy oraz finansowaniem terroryzmu została przygotowana w oparciu o obowiązującą ustawę z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wraz ze strategią przyjętą przez Generalnego Inspektora Informacji Finansowej w ramach Krajowej Oceny Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu.

Rozdział 2: Opis metodologii oceny ryzyka prania pieniędzy oraz finansowania terroryzmu

Należy wskazać przede wszystkim przyjęte założenia procesu oceny ryzyka według konkretnych kroków na podstawie tego, jakiego okresu dotyczy oraz na podstawie jakiego zakresu danych zostało dokonane oszacowanie ryzyka. Prawidłowe zidentyfikowanie ryzyk pozwala na etapie szacowania wdrożyć stosowne środki i mechanizmy pozwalające zminimalizować je do poziomu akceptowanego. Oczywiście należy nadać wagę ryzyka i umieścić w macierzy ryzyk tak, aby dokonać oszacowania ryzyka końcowego dla instytucji obowiązanej.

Rozdział 3: Opis klientów, państw lub obszarów geograficznych, produktów, usług, transakcji oraz kanałów ich dostaw oraz czynniki ryzyka

Należy wskazać czynniki ryzyka związane ze stosunkami gospodarczymi zawieranymi z klientami lub z transakcjami okazjonalnymi realizowanymi przez nich. Na bazie tego ryzyka i jego oceny należy zastosować środki bezpieczeństwa finansowego, których zadaniem jest przede wszystkim uzyskanie informacji na temat klientów oraz celu, dla którego korzystają oni z usług i produktów oferowanych przez instytucje obowiązane.

Ryzyka muszą zostać zidentyfikowane w obszarach:

- **Klienta** – na ocenę ryzyka klienta ma wpływ jego rodzaj, branża, typ prowadzonej działalności; GIIIF wskazuje branże podwyższonego ryzyka: obrót walutami, pośrednictwo w obrocie nieruchomościami itp.
- **Kraju/obszaru geograficznego** – dotyczy tylko instytucji obowiązanych, które obsługują klientów lub świadczą usługę podmiotom zagranicznym.
- **Produktu/usługi** – dla oceny ryzyka produktu/usługi istotne znaczenie ma jego podatność na pranie pieniędzy. Tą podatność wskazuje Krajowa Ocena Ryzyka Prania Pieniędzy.
- **Kanału dystrybucji** – dla oceny ryzyka kanału dystrybucji należy przeanalizować kanał pozyskania klienta. W tym przypadku przede wszystkim należy uwzględnić, czy klient zawiera umowę na odległość, czy za pośrednictwem, ewentualnie osobiście w biurze.

Najlepiej czynniki te analizować na danych historycznych posiadanych przez instytucję obowiązującą z poprzedniego roku.

Rozdział 4: Wskazanie poziomu ryzyka prania pieniędzy oraz finansowania terroryzmu

Na podstawie przeanalizowanych czynników ryzyk w obszarach: klient, obszar geograficzny, produkt/usługa, kanał dystrybucji należy ocenić ryzyko końcowe, które pozostaje pomimo zastosowania tzw. czynników kontroli oraz środków bezpieczeństwa. Ryzyko standardowe istnieje niezależnie od czynników kontroli. Prawidłowe funkcjonowanie czynników kontroli zmniejsza jednak prawdopo-

bieństwo wystąpienia prania pieniędzy lub finansowania terroryzmu. Dlatego w zależności od ich skuteczności ryzyko końcowe ma mniejszą lub większą wartość.

Przy wykazaniu ryzyka końcowego można korzystać z tzw. matrycy ryzyk.

Wyznaczone ryzyko końcowe, które jest ryzykiem niezarządzanym, jest ryzykiem prania pieniędzy i finansowania terroryzmu w Spółce.

Rozdział 5: Wnioski wynikające z oceny ryzyka prania pieniędzy oraz finansowania terroryzmu

W tym punkcie należy uwzględnić:

- Czynniki mogące mieć wpływ na podwyższenie ryzyka wskazanego w rozdziale 4.
- Czynniki mogące mieć wpływ na obniżenie ryzyka wskazanego w rozdziale 4.
- Jakie środki można podjąć, by mitygować ryzyko z poziomu wysokiego lub średniego do poziomu niskiego.

4.5. Oświadczenie o beneficjencie rzeczywistym

Zgodnie z art. 2 ust. 2 pkt 1 TerroryzmU poprzez beneficjenta rzeczywistego rozumie się:

1. każdą osobę fizyczną sprawującą bezpośrednio lub pośrednio kontrolę nad klientem poprzez posiadane uprawnienia, które wynikają z okoliczności prawnych lub faktycznych, umożliwiające wywieranie decydującego wpływu na czynności lub działania podejmowane przez klienta, lub każdą osobę fizyczną, w imieniu której są nawiązywane stosunki gospodarcze lub jest przeprowadzana transakcja okazjonalna, w tym:
 - a) w przypadku osoby prawnej innej niż spółka, której papiery wartościowe są dopuszczone do obrotu na rynku regulowanym podlegającym wymogom ujawniania informacji wynikającym z przepisów prawa Unii Europejskiej lub odpowiadających im przepisów prawa państwa trzeciego:
 - osobę fizyczną będącą udziałowcem lub akcjonariuszem, której przysługuje prawo własności więcej niż 25% ogólnej liczby udziałów lub akcji tej osoby prawnej,
 - osobę fizyczną dysponującą więcej niż 25% ogólnej liczby głosów w organie stanowiącym tej osoby prawnej, także jako zastawnik albo użytkownik, lub na podstawie porozumień z innymi uprawnionymi do głosu,
 - osobę fizyczną sprawującą kontrolę nad osobą prawną lub osobami prawnymi, którym łącznie przysługuje prawo własności więcej niż 25% ogólnej liczby udziałów lub akcji lub które łącznie dysponują więcej niż 25% ogólnej liczby głosów w organie stanowiącym tej osoby prawnej, także jako zastawnik albo użytkownik, lub na podstawie porozumień z innymi uprawnionymi do głosu,
 - osobę fizyczną sprawującą kontrolę nad osobą prawną poprzez posiadanie uprawnień, o których mowa w art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2021 r. poz. 217), lub
 - osobę fizyczną zajmującą wyższe stanowisko kierownicze w przypadku udokumentowanego braku możliwości ustalenia lub wątpliwości co do

- tożsamości osób fizycznych określonych w tiret pierwsze–czwarte oraz w przypadku niestwierdzenia podejrzeń prania pieniędzy lub finansowania terroryzmu,
- b) w przypadku trustu:
- założyciela,
 - powiernika,
 - nadzorcę, jeżeli został ustanowiony,
 - beneficjenta lub – w przypadku gdy osoby fizyczne czerpiące korzyści z danego trustu nie zostały jeszcze określone – grupę osób, w których głównym interesie powstał lub działa trust,
 - inną osobę sprawującą kontrolę nad trustem,
 - inną osobę fizyczną posiadającą uprawnienia lub wykonującą obowiązki równoważne z określonymi w tiret pierwsze–piąte,
- c) w przypadku osoby fizycznej prowadzącej działalność gospodarczą, wobec której nie stwierdzono przesłanek lub okoliczności mogących wskazywać na fakt sprawowania kontroli nad nią przez inną osobę fizyczną lub osoby fizyczne, przyjmuje się, że taka osoba fizyczna jest jednocześnie beneficjentem rzeczywistym,
- d) w przypadku klienta będącego osobą fizyczną prowadzącą działalność gospodarczą, wobec którego nie stwierdzono przesłanek lub okoliczności mogących wskazywać na fakt sprawowania kontroli nad nim przez inną osobę fizyczną lub osoby fizyczne, przyjmuje się, że taki klient jest jednocześnie beneficjentem rzeczywistym.

OŚWIADCZENIE O BENEFICJENCIE RZECZYWISTYM DLA KLIENTA

Nazwa klienta	
Adres klienta	
NIP klienta	

Oświadczenie przyjmowane jest przez instytucję obowiązaną, tj. podmiot prowadzący działalność w zakresie usługowego prowadzenia ksiąg rachunkowych/usług polegających na sporządzaniu deklaracji, prowadzeniu ksiąg podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego* zgodnie z wymogami ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, która ma obowiązek dokonać identyfikacji beneficjenta rzeczywistego Klienta oraz podejmować uzasadnione czynności w celu weryfikacji jego tożsamości oraz ustalenia struktury własności i kontroli.

Beneficjent rzeczywisty to osoba fizyczna lub osoby fizyczne sprawujące bezpośrednio lub pośrednio kontrolę nad Klientem poprzez posiadane uprawnienia, które wynikają z okoliczności prawnych lub faktycznych, umożliwiające wywieranie decydującego wpływu na czynności lub działania podejmowane przez Klienta, lub osoba fizyczna lub osoby fizyczne, w imieniu których są nawiązywane stosunki gospodarcze lub przeprowadzana jest transakcja okazjonalna. Należy wskazać beneficjentów rzeczywistych Klienta zgodnie z jednym z poniższych wariantów A, B, C.

A. Klient posiada akcjonariuszy lub udziałowców. Prosimy o wskazanie osób fizycznych, które w sposób bezpośredni lub pośredni (np. poprzez posiadanie udziałów w spółce matce Klienta) kontrolują powyżej 25% udziałów/akcji Klienta/głosów w organie stanowiącym Klienta lub posiadają w stosunku do Klienta uprawnienia przysługujące jednostce dominującej w rozumieniu przepisów o rachunkowości:

	Beneficjent rzeczywisty 1	Beneficjent rzeczywisty 2	Beneficjent rzeczywisty 3
Imię i nazwisko			
Obywatelstwo			
Udziały/Uprawnienia			
Poziom udziałów/akcji (w %)			
PESEL/data urodzenia (jeśli nie nadano PESEL)			
Kraj urodzenia			
Rodzaj i numer dokumentu tożsamości			
Dane adresowe (ulica, nr domu, lokalu, kod pocztowy, miasto i kraj)			
Numer telefonu			
Adres e-mail			

B. Brak osób kontrolujących powyżej 25% udziałów/akcji/praw do głosu (np. rozproszona struktura własności i kontroli). Prosimy o wskazanie osób fizycznych zajmujących wyższe stanowiska kierownicze (jeśli powołano zarząd, należy wskazać wszystkich członków zarządu):

	Beneficjent rzeczywisty 1	Beneficjent rzeczywisty 2	Beneficjent rzeczywisty 3
Imię i nazwisko			
Obywatelstwo			
Funkcja/Stanoisko			
Kontrolowane udziały (w %)			

4. Wzory dokumentów

	Beneficjent rzeczywisty 1	Beneficjent rzeczywisty 2	Beneficjent rzeczywisty 3
PESEL/data urodzenia (jeśli nie nadano PESEL)			
Kraj urodzenia			
Rodzaj i numer doku- mentu tożsamości			
Dane adresowe (ulica, nr domu, lokalu, kod pocztowy, miasto i kraj)			
Numer telefonu			
Adres e-mail			

C. Klient jest podmiotem notowanym na giełdzie Unii Europejskiej:

Nazwa giełdy	
Kod ISIN podmiotu	
Udziały w %	

Jestem świadomy/a odpowiedzialności karnej za złożenie fałszywego oświadczenia.

.....
data oraz imię i nazwisko osoby wypeł-
niającej oświadczenie w imieniu Klienta

*niewłaściwe skreślić

4.6. Oświadczenie PEP

data

.....
imię i nazwisko Klienta

OŚWIADCZENIE KLIENTA

Oświadczenie przyjmowane jest przez instytucję obowiązana, tj. podmiot prowadzący działalność w zakresie usługowego prowadzenia ksiąg rachunkowych/usług polegających na sporządzaniu deklaracji, prowadzeniu ksiąg podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego* zgodnie z wymogami ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu.

Niniejszym oświadczam, iż została mi przedstawiona definicja osoby zajmującej eksponowane stanowisko polityczne, która uregulowana jest w art. 2 ust. 2 pkt 11 ustawy z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu.

Zgodnie z tą definicją pod pojęciem osoby zajmującej eksponowane stanowisko polityczne – rozumie się, z wyłączeniem grup stanowisk średniego i niższego szczebla, osoby zajmujące znaczące stanowiska publiczne lub pełniące znaczące funkcje publiczne, w tym:

- szefów państw, szefów rządów, ministrów, wiceministrów oraz sekretarzy stanu,
- członków parlamentu lub podobnych organów ustawodawczych,
- członków organów zarządzających partii politycznych,
- członków sądów najwyższych, trybunałów konstytucyjnych oraz innych organów sądowych wysokiego szczebla, których decyzje nie podlegają zaskarżeniu, z wyjątkiem trybów nadzwyczajnych,
- członków trybunałów obrachunkowych lub zarządów banków centralnych,
- ambasadorów, chargés d'affaires oraz wyższych oficerów sił zbrojnych,
- 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,
- dyrektorów, zastępców dyrektorów oraz członków organów organizacji międzynarodowych lub osoby pełniące równoważne funkcje w tych organizacjach,
- dyrektorów generalnych w urzędach naczelnych i centralnych organów państwowych oraz dyrektorów generalnych urzędów wojewódzkich,
- inne osoby zajmujące stanowiska publiczne lub pełniące funkcje publiczne w organach państwa lub centralnych organach administracji rządowej.

Niniejszym poświadczam własnoręcznym podpisem, iż jestem*/nie jestem* osobą zajmującą eksponowane stanowisko polityczne.

Jestem świadomy/a odpowiedzialności karnej za złożenie fałszywego oświadczenia.

.....
podpis pracownika biura
przyjmującego oświadczenie

.....
czytelny podpis Klienta

*niewłaściwe skreślić

4.7. Rejestr transakcji podejrzanych

Lp.	Data i miejsce transakcji	Podmiot transakcji	Kontra-hent transakcji	Opis transakcji (kwota, waluta, rodzaj transakcji, okoliczności)	Dokumenty transakcji	Data przekazania Koodynatorowi AML	Stanowisko Koodynatora AML	Zawiadomienie GIIF	Data przekazania zawiadomienia
1.								Tak/Nie	
2.									
3.									
4.									
5.									
6.									
7.									
8.									

4.8. Zawiadomienie odnośnie transakcji podejrzanej

..... data i miejscowość

.....

.....

(pełna nazwa i dane instytucji obowiązanej)

.....

.....

(imię, nazwisko, numer telefonu, adres e-mail osoby upoważnionej do kontaktów z GIIF)

ZAWIADOMIENIE DO GIIF

Na podstawie art. 74 ustawy z dnia 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu zawiadamiam o okolicznościach transakcji, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu:

.....

.....

.....

.....
 (Opisać transakcję i jej okoliczności, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu)

Posiadane dane o osobie fizycznej, prawnej lub jednostce organizacyjnej nie posiadającej osobowości prawnej, której transakcja podejrzana dotyczy:

- 1) Nazwisko, imię lub nazwa wraz z formą organizacyjną:
- 2) Adres zamieszkania/siedziby:

- 3) Obywatelstwo:
- 4) Numer PESEL/rejestru sądowego:
- 5) Numer NIP:
- 6) Numer REGON:
- 7) Rodzaj, seria i numer dokumentu tożsamości:

Dodatkowe informacje o transakcji:

.....

Informacja o załącznikach:

.....

(miejscowość, data)

.....

(podpis osoby zgłaszającej)

Ważne

Zawiadomienie jest przekazywane niezwłocznie, nie później jednak niż w terminie 2 dni roboczych od dnia potwierdzenia przez instytucję obowiązana podejrzenia.

Podstawa prawna:

- ustawa z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. z 2020 r. poz. 971 ze zm.)
- art. 3 ust. 1 pkt 37 ustawy z 29.9.1994 r. o rachunkowości (t.j. Dz.U. z 2021 r. poz. 217 ze zm.)
- art. 165a ustawy z 6.6.1997 r. – Kodeks karny (t.j. Dz.U. z 2020 r. poz. 1444 ze zm.)

