ROX PAY S.R.L.
POLITYKA ZAPOBIEGANIA I PRZECIWDZIAŁANIA PRANIEM PIENIĘDZY I FINANSOWANIU TERRORYZMU

1 - PRZEGLĄD

1.1 – KLUCZOWE PRZEPISY I WYTYCZNE

Niniejszy dokument określa Politykę Rox Pay S.r.l. dotyczącą przeciwdziałania praniu pieniędzy, finansowaniu terroryzmu oraz naruszaniu środków ograniczających[1]i dotyczy Rox Pay S.r.l. i jego operacje.

Normy należy uważać za uzupełniające i mające zastosowanie, ponieważ nie są one sprzeczne z przepisami wydanymi przez władze lokalne.

1.2 – ODBIORCY I SPOSOBY REALIZACJI

Polityka dotyczy firmy Rox Pay S.r.l.

2 – ZASADY OGÓLNE

2.1 RAMY REGULACYJNE AML-CFT

Pranie dochodów pochodzących z nielegalnej i przestępczej działalności jest jedną z najpoważniejszych form przestępczości na rynkach finansowych i stanowi obszar szczególnego zainteresowania zorganizowanej działalności przestępczej.

Pranie pieniędzy ma znaczący negatywny wpływ na całą gospodarkę: ponowne inwestowanie nielegalnych dochodów w legalną działalność oraz zmowy między osobami fizycznymi lub instytucjami finansowymi a organizacjami przestępczymi głęboko wpływają na mechanizmy rynkowe, podważają efektywność i uczciwość działalności finansowej oraz osłabiają gospodarkę. Finansowanie działalności terrorystycznej może wiązać się z wykorzystywaniem dochodów uzyskanych legalnie i/lub pochodzących z przestępstwa.

Zmieniający się charakter prania pieniędzy i finansowania terroryzmu, któremu sprzyja także ciągły rozwój technologii, wymaga stałego dostosowywania środków zapobiegawczych i kontrastowych.

Ramy regulacyjne dotyczące przeciwdziałania praniu pieniędzy (AML) i przeciwdziałaniu finansowaniu terroryzmu (CFT) opierają się na kompleksowym zestawie krajowych, unijnych i międzynarodowych źródeł regulacyjnych.

Na poziomie międzynarodowym kluczowy wkład w harmonizację przepisów wniosła Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy (FATF), najważniejszy organ międzynarodowy zajmujący się walką z praniem pieniędzy, finansowaniem terroryzmu i rozprzestrzenianiem broni masowego rażenia.

1 Zgodnie z definicją zawartą w Wytycznych EUNB (EBA/GL/2024/14): „Unijne środki ograniczające, o których mowa w art. 2 pkt 1 dyrektywy (UE) 2024/1226 oraz krajowe środki ograniczające przyjęte przez państwa członkowskie zgodnie z ich krajowym porządkiem prawnym (w zakresie, w jakim mają one zastosowanie do instytucji finansowych).

Wypełniając swoje obowiązki, FATF ustanowiła zestaw międzynarodowych standardów, „40 zaleceń", do których w 2001 r. dodano kolejnych 9 specjalnych zaleceń w celu zwalczania międzynarodowego finansowania terroryzmu. Temat ten został w pełni zmieniony w lutym 2012 r. wraz z przyjęciem Międzynarodowych standardów w zakresie zwalczania prania pieniędzy oraz finansowania terroryzmu i proliferacji, a następnie podsumowany w wyżej wymienionych „40 zaleceniach".

W ramach walki z rozprzestrzenianiem broni masowego rażenia Organizacja Narodów Zjednoczonych przygotowała zestaw środków mających na celu zwalczanie finansowania programów proliferacyjnych, w tym zakaz udzielania pomocy lub finansowania jakimkolwiek osobom zaangażowanym w taką działalność.

Wdrażając uchwały przyjęte w ramach Organizacji Narodów Zjednoczonych, Unia Europejska wydała zbiór przepisów w celu wdrożenia środków ograniczających, takich jak zamrożenie funduszy i zasobów gospodarczych osób lub podmiotów zaangażowanych w rozwijanie działań wrażliwych na rozprzestrzenianie broni masowego rażenia.

FATF opracował wytyczne dotyczące wdrażania sankcji finansowych przyjętych przez Organizację Narodów Zjednoczonych.

Konkretne środki dotyczące rozprzestrzeniania broni masowego rażenia zostały niedawno uwzględnione w Zaleceniach, zgodnie z rezolucjami Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych.

Wytyczne UE dotyczące zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy i finansowania terroryzmu zawarte są w Dyrektywie UE 2015/849[2]Parlamentu Europejskiego i Rady z dnia 20 maja 2015 roku (czwarta dyrektywa w sprawie przeciwdziałania praniu pieniędzy), zmienionej Dyrektywą UE 2018/843 (piąta dyrektywa w sprawie przeciwdziałania praniu pieniędzy) oraz w Rozporządzeniach i Wytycznych wydawanych każdorazowo odpowiednio przez UE – Unię Europejską oraz przez EBA – Europejski Urząd Nadzoru Bankowego.

Na poziomie krajowym zapobieganie i zwalczanie prania pieniędzy oraz finansowania terroryzmu regulują następujące przepisy pierwotne:

- **Włoski dekret legislacyjny nr. nr 109 z dnia 22 czerwca 2007 r. z późniejszymi zmianami i uzupełnieniami, który zawiera „Przepisy o zapobieganiu, przeciwdziałaniu i zwalczaniu finansowania terroryzmu oraz działalności państw zagrażających pokojowi i bezpieczeństwu międzynarodowemu", wdrażającego Dyrektywę 2015/849 ze zmianami wprowadzonymi Dyrektywą UE 2018/843;**
- **Włoski dekret legislacyjny nr. 231 z dnia 21 listopada 2007 r. wraz z późniejszymi zmianami i uzupełnieniami wdrażającymi dyrektywę 2015/849/UE zmieniającą dyrektywę 2009/138/WE i 2013/36/UE, zmienioną dyrektywą 2018/843/UE w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu (dalej także „Rozporządzenie").**

2 Dyrektywa UE 2024/1640 Parlamentu Europejskiego i Rady z dnia 31.05.2024 r. w sprawie postępowania, jakie powinny być wszczęte przez państwa członkowskie w celu zapobiegania korzystaniu z systemu finansowego w celu prania pieniędzy lub finansowania terroryzmu, do transpozycji do 10 lipca 2027 r., zmienia dyrektywę UE 2019/1937 i uchyla dyrektywę UE 2015/849.

Wreszcie istnieje również prawodawstwo wtórne na poziomie krajowym wydane przez Bank Włoch
oraz Jednostkę Informacji Finansowej („FIU") i jest zawarta w następujących źródłach regulacyjnych:

- **Przepis z dnia 26 marca 2019 r. określający przepisy wykonawcze dotyczące organizacji, procedur i kontroli wewnętrznej mające na celu zapobieganie wykorzystywaniu pośredników finansowych i innych podmiotów do prania pieniędzy oraz finansowania terroryzmu, zmieniony przez Bank Włoch Przepis z dnia 1 sierpnia 2023 r.;**
- **Przepis z dnia 28 marca 2019 r. określający instrukcje dotyczące obiektywnego komunikowania się;**
- **Przepis z dnia 30 lipca 2019 r. ustanawiający przepisy wykonawcze dotyczące należytej staranności wobec klienta, zmieniony przez Bank Włoch Przepis z dnia 13 czerwca 2023 r.;**
- **Przepis z dnia 24 marca 2020 r. określający przepisy wykonawcze dotyczące przechowywania i udostępniania dokumentów, danych i informacji w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;**
- **Przepis z dnia 25 sierpnia 2020 r. określający zasady składania zbiorczych raportów AML;**
- **Przepis z dnia 12 maja 2023 r. w sprawie wskaźników nieprawidłowości dla pośredników ułatwiających identyfikację transakcji podejrzanych, obowiązujący od 1 stycznia 2024 r.**

Rox Pay S.r.l. (dalej „Spółka") wdraża powyższe regulacje w swoich wewnętrznych dokumentach regulacyjnych.

W ujęciu ogólnym Spółka przyjęła niniejszą „Politykę zwalczania prania pieniędzy i finansowania terroryzmu" (zwaną dalej „Polityką") jako wyraz swojego zaangażowania w zwalczanie ww. zjawisk przestępczych w skali międzynarodowej, ze szczególnym uwzględnieniem kontrastu, w świadomości, że dążenie do rentowności i efektywności musi być połączone z ciągłym i skutecznym monitorowaniem integralności struktur korporacyjnych.

Polityka stosowana w Spółce opisuje politykę przyjętą przez Rox Pay S.r.l. zgodnie z zasadami i zasadami określonymi w przepisach krajowych i unijnych, zgodnie z odpowiednimi standardami międzynarodowymi i jest wdrażany łącznie z wewnętrznymi procedurami dotyczącymi przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, Kodeksem Etyki oraz wewnętrznymi procedurami wdrażającymi obowiązujące lokalne prawo pierwotne i wtórne, określające procesy, role i obowiązki.

Aktualna Polityka została zatwierdzona przez Zarząd Spółki.

Wytyczne AML i CFT stosowane są przez firmę Rox Pay S.r.l. zgodnie z obowiązującym prawem.

Spółka zobowiązuje się do przestrzegania niniejszych ram regulacyjnych, a także wszelkich przepisów wykonawczych wydanych przez Bank Włoch w sprawie należytej staranności wobec klienta, zatrzymywania danych i informacji, organizacji, procedur, kontroli i wzmocnionych kontroli przeciwko finansowaniu programów mających na celu rozprzestrzenianie broni masowego rażenia.

Spółka jest całkowicie zaangażowana w zapewnienie, że organizacja operacyjna i system kontroli są kompletne, odpowiednie, funkcjonalne i niezawodne dla nadzoru strategicznego, w celu ochrony Spółki przed tolerancją lub domieszką form niezgodności z prawem, które mogą zaszkodzić jej reputacji i mieć wpływ na jej stabilność.

Z tych powodów Rox Pay S.r.l. przyjęła zasady organizacyjne i behawioralne oraz systemy monitorowania i kontroli mające na celu zapewnienie przestrzegania obowiązującego prawa przez organy administracyjne i kontrolne, pracowników, współpracowników i konsultantów Spółki. Kontrole te są także spójne z zasadami i procedurami określonymi w kodeksie ochrony danych osobowych.

Spółka opiera się również na wskaźnikach anomalii i wzorcach nieprawidłowych zachowań w środowisku gospodarczym i finansowym, które są publikowane na przestrzeni czasu przez Jednostkę analityki finansowej (FIU) w związku z potencjalnymi działaniami związanymi z praniem pieniędzy i finansowaniem terroryzmu.

2.2 - RAMY PRAWNE DOTYCZĄCE ŚRODKÓW OGRANICZAJĄCYCH I EMBARGA

Wszystkie środki ograniczające ustanowione w celu zwalczania finansowania terroryzmu i wszelkich nielegalnych lub podejrzanych działań, które zagrażają międzynarodowemu pokojowi i bezpieczeństwu, mogą mieć charakter handlowy, np. ograniczenia importu/eksportu z/do kraju, lub finansowy, np. częściowe lub całkowite zablokowanie transferu środków, ale także ograniczenia operacyjne i zamrożenie funduszy.

Środki ograniczające obejmują międzynarodowe sankcje finansowe, zwane także embargo, nakładane przez państwo włoskie, agencje zagraniczne (np. OFAC, UKSL) i organizacje ponadnarodowe (ONZ, UE) poprzez szereg obowiązków, których Spółka jest zobowiązana przestrzegać. Rada nakłada pewne środki ograniczające (sankcje) na wszystkie państwa członkowskie ONZ w celu wdrożenia rezolucji przyjętych przez Radę Bezpieczeństwa ONZ na mocy rozdziału VII Karty Narodów Zjednoczonych. Ponadto Unia Europejska może przyjąć sankcje lub samodzielnie o nich decydować w drodze rozporządzeń Rady, które są natychmiast wykonalne w każdym państwie członkowskim, aby zapewnić ich terminowe i jednoczesne zastosowanie.

Na poziomie międzynarodowym istnieją przepisy ustanawiające szczególne zakazy lub ograniczenia dotyczące inwestowania w niektórych sektorach przemysłu lub importu/eksportu z/do „krajów wysokiego lub znaczącego ryzyka". W szczególności dotyczy to rezolucji Rady Bezpieczeństwa ONZ (RB ONZ) na podstawie art. 41 rozdziału VII Karty Narodów Zjednoczonych, na mocy których nakładane są środki ograniczające w stosunku do osób i/lub krajów.

Jeśli chodzi o prawodawstwo wspólnotowe, główne przepisy to:

- Rozporządzenie Parlamentu Europejskiego i Rady 2021/821 z dnia 20 maja 2021 r[3i] **późniejsze zmiany, na mocy których ustanawia się system UE w celu kontroli wywozu, transferu, pośrednictwa i tranzytu produktów podwójnego zastosowania;**

3, które zastąpiło rozporządzenie Rady 428/2009/WE z dnia 5 maja 2009 r

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptowalut oraz zmieniające dyrektywę (UE) 2015/849 (wersja przekształcona);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/886 z dnia 13 marca 2024 r. zmieniające rozporządzenia (UE) nr 260/2012 i (UE) 2021/1230 oraz dyrektywy 98/26/WE i (UE) 2015/2366 w zakresie natychmiastowych poleceń przelewu w euro;
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1226 z dnia 24 kwietnia 2024 r. w sprawie definicji przestępstw i kar za naruszenie unijnych środków ograniczających oraz zmieniająca dyrektywę (UE) 2018/1673 transponowaną do prawa włoskiego dekretem legislacyjnym nr 211/2025.
- **Wytyczne Europejskiego Urzędu Nadzoru Bankowego w sprawie wewnętrznych polityk, procedur i kontroli zapewniających wdrożenie unijnych i krajowych środków ograniczających (EBA/GL/2024/14)**[4];
- **Wytyczne Europejskiego Urzędu Nadzoru Bankowego w sprawie wewnętrznych zasad, procedur i kontroli mających na celu zapewnienie wdrożenia unijnych i krajowych środków ograniczających zgodnie z rozporządzeniem (UE) 2023/1113 (EBA/GL/2024/15) w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmieniające dyrektywę (UE) 2015/849**[5].

Wreszcie na szczeblu krajowym embargo uregulowane jest w następujący sposób:

- **Ustawodawstwo podstawowe:**
  - **Dekret legislacyjny nr 221/2017, który zmienił i uprościł procedury wydawania zezwoleń na eksport produktów i technologii podwójnego zastosowania oraz sankcje dotyczące embargo handlowych, a także wszelkich rodzajów operacji eksportowych materiałów proliferujących.**
- **Prawodawstwo wtórne:**
  - **Bank of Italy Postanowienie z dnia 12 maja 2023 r. zawierające wskaźniki nieprawidłowości dla pośredników w celu ułatwienia identyfikacji transakcji podejrzanych.**

Wreszcie wszystkie regulacje wydane przez Władze USA mają znaczenie dla działalności Spółki ze względu na aspekty reputacyjne oraz odwoływanie się do tych regulacji w przedsięwzięciach kontraktowych wiążących się z potencjalnym zastosowaniem sankcji o skutku eksterytorialnym (tzw. amerykańskie „sankcje wtórne"). Takie przepisy regulacyjne zawarte są w amerykańskiej ustawie Patriot Act6 oraz w środkach związanych z sankcjami gospodarczymi i handlowymi wydanymi przez rząd USA za pośrednictwem Biura Kontroli Aktywów Zagranicznych (OFAC) Departamentu Skarbu.[6]

4, do którego stosowania Bank Włoch zadeklarował zamiar stosowania w nocie nr. 48 z dnia 8 kwietnia 2025 r. i obowiązujące od dnia 30 grudnia 2025 r.

5, do którego stosowania Bank Włoch zadeklarował zamiar stosowania w nocie nr. 52 z dnia 19 maja 2025 r. i obowiązujące od dnia 30 grudnia 2025 r.

6 Ustawa federalna Stanów Zjednoczonych z dnia 26 października 2001 r., oficjalnie zatytułowana „Ustawa o jednoczeniu i wzmacnianiu Ameryki poprzez zapewnienie odpowiednich narzędzi wymaganych do przechwytywania i utrudniania terroryzmu z 2001 r.".

3 – MODELE I METODOLOGIE GRUPOWE

3.1 – ASPEKTY OGÓLNE

Ustanowione krajowe ramy regulacyjne dotyczące działań zapobiegawczych przeciwko praniu pieniędzy, finansowaniu terroryzmu i naruszeniom środków ograniczających opierają się na szeregu obowiązków

które odbiorcy mają obowiązek przestrzegać:

- obowiązek przyjęcia odpowiednich struktur organizacyjnych, procedur i środków kontroli wewnętrznej;
- obowiązek przyjęcia spójnych i spójnych procedur analizy i oceny ryzyk związanych z praniem pieniędzy, finansowaniem terroryzmu oraz naruszaniem środków ograniczających, a także ustanowienia nadzoru, kontroli i procedur niezbędnych do minimalizacji i zarządzania tymi ryzykami;
- obowiązek należytej staranności wobec klienta, poprzez którą Spółka pozyskuje i weryfikuje informacje dotyczące tożsamości klienta i beneficjenta rzeczywistego, a także celu i zamierzonego charakteru relacji lub transakcji, przy jednoczesnym zapewnieniu stałego monitorowania wszystkich transakcji zawieranych przez klienta;
- podejście oparte na ryzyku, w ramach którego obowiązki w zakresie należytej staranności wobec klienta są podzielone na różne stopnie należytej staranności proporcjonalne do profilu ryzyka klienta;
- obowiązek przechowywania dokumentów, danych i informacji w celu umożliwienia ich terminowego pozyskania, przejrzystości, kompletności, niezmienności i integralności oraz ogólnej i szybkiej dostępności;
- obowiązek zgłaszania podejrzanych transakcji;
- obowiązek powstrzymywania się od nawiązywania nowych relacji z klientami, przeprowadzania okazjonalnych transakcji lub utrzymywania istniejących relacji z klientami, w przypadku gdy nie przeprowadzono należytej staranności lub zachodzi podejrzenie, że może istnieć powiązanie z praniem pieniędzy lub finansowaniem terroryzmu;
- obowiązek powiadamiania Ministra Gospodarki i Finansów o naruszeniach, o których mowa w art. 49 i 50 dekretu z mocą ustawy 231/07 oraz przestrzegania ograniczeń w stosowaniu środków pieniężnych i papierów wartościowych na okaziciela;
- monitorowanie wszelkich transakcji z osobami fizycznymi, prawnymi i/lub z Krajami znajdującymi się na listach Rady Unii Europejskiej (UE), na liście Urzędu ds. Kontroli Aktywów Zagranicznych (OFAC), na brytyjskiej liście sankcyjnej (UKSL)[7], w skonsolidowanym wykazie sankcji Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych (ONZ) zawartym w postanowieniach wydanych przez władze krajowe zawierających szczególne środki ograniczające w celu zwalczania terroryzmu;
- monitorowanie transakcji zawieranych z krajami uznawanymi za niechętne do współpracy w kwestiach podatkowych, nadzoru finansowego i przeciwdziałania praniu pieniędzy, zwanych ogólnie „rajami podatkowymi" lub „offshore centrami finansowymi";
- przyjęcie odpowiednich programów szkolenia personelu w celu zapewnienia wdrożenia i właściwego stosowania przepisów ustawowych i wykonawczych;
- obowiązek zapewnienia FIU „obiektywnej komunikacji" zgodnie ze szczegółowymi przepisami
  instrukcje dotyczące metod i częstotliwości komunikacji;

7 Lista OFSI (Office of Financial Sanctions Implementation HMT) została zamknięta 28 stycznia 2026 r.; od tej daty brytyjska lista sankcji jest jedynym oficjalnym źródłem wszystkich oznaczeń sankcji Wielkiej Brytanii.

- obowiązek ujawniania wszelkich naruszeń lub naruszeń, o których mogą dowiedzieć się Jednostki Kontrolne w trakcie wykonywania swoich zadań;
- obowiązek przyjęcia procedur zarządzania wewnętrznym zgłaszaniem naruszeń zgłaszanych przez pracowników (Whistleblowing).

W odniesieniu do działań związanych z finansowaniem terroryzmu włoskie ustawodawstwo nakłada na strony zobowiązane obowiązek wykonania następujących czynności:

- zamrożenie funduszy i zasobów gospodarczych niektórych osób znajdujących się na listach UE;
- informowanie Jednostki Wywiadu Finansowego (FIU) o środkach zastosowanych w celu zamrożenia funduszy lub Specjalnej Jednostki Policji Walutowej Guardia di Finanza (Policja Finansowa) w przypadku zasobów gospodarczych;
- informowanie FIU o podejrzanych transakcjach, relacjach biznesowych i wszelkich innych dostępnych informacjach dotyczących stron znajdujących się na czarnych listach publikowanych przez samą FIU;
- zgłaszanie podejrzanych transakcji, które na podstawie dostępnych informacji są bezpośrednio lub pośrednio związane z działalnością w zakresie finansowania terroryzmu.

W odniesieniu do sankcji międzynarodowych (tzw. embarga) i narażenia na środki ograniczające ustawodawstwo wymaga podjęcia pewnych środków, w tym między innymi:

- kontroli danych osobowych i transakcyjnych operacji związanych z importem i/lub eksportem realizowanych przez klientów, mających na celu zablokowanie importu/eksportu z lub do kraju oraz odpowiednich przepisów. Zakaz może mieć charakter ogólny i obejmować wszystkie rodzaje towarów, o ile nie zostało to wyraźnie dozwolone, lub ograniczać się do niektórych rodzajów towarów, np.: uzbrojenie (patrz kodeks celny);
- całkowite lub częściowe ograniczenia transferów finansowych z/do Kraju;
- wymóg uprzedniej zgody w celu realizacji przelewów;
- obowiązek awizowania przelewów (wychodzących lub przychodzących);
- zakaz finansowania, udzielania pomocy finansowej lub udostępniania rządowi preferencyjnych pożyczek (bezpośrednio lub w niektórych przypadkach pośrednio za pośrednictwem spółek stowarzyszonych lub udziału w międzynarodowych instytucjach finansowych);
- zakaz finansowania klientów współpracujących z krajami objętymi sankcjami;
- wprowadzenie środków ograniczających wobec podmiotów rosyjskich i białoruskich;
- identyfikowalność kontroli przeprowadzanych w odniesieniu do operacji pochodzących z krajów, osób i podmiotów objętych ograniczeniami lub do nich skierowanych.

3.2 - NALEŻYTA STARANNOŚĆ KLIENTA

3.2.1 – Aspekty ogólne

Spółka podejmuje wszelkie środki należytej staranności wobec klienta, gdy:

- nawiązywanie relacji biznesowych;

- wykonywanie transakcji okazjonalnych, aranżowanych przez klientów, takich jak przelewy bankowe lub inne transakcje równe lub wyższe od obowiązującego wyznaczonego progu, niezależnie od tego, czy transakcja jest przeprowadzana w ramach pojedynczej operacji, czy w kilku powiązanych ze sobą operacjach, czy też polega na przekazie środków pieniężnych przekraczającym dopuszczalne prawem limity;

- istnieje podejrzenie prania pieniędzy lub finansowania terroryzmu, niezależnie od ewentualnych odstępstw, wyłączeń lub wyznaczonych progów, które mogą mieć zastosowanie;
- istnieją wątpliwości co do kompletności, rzetelności i prawdziwości informacji lub dokumentacji pozyskanych wcześniej na potrzeby identyfikacji Klienta.

Obowiązki należytej staranności:

- są spełnione:
  - wobec nowych klientów przed nawiązaniem stałej współpracy lub realizacją okazjonalnej transakcji;
  - wobec dotychczasowych klientów, ilekroć wskazane jest zachowanie należytej staranności w świetle zmiany poziomu ryzyka prania pieniędzy lub finansowania terroryzmu związanego z klientem lub gdy istnieją podejrzenia lub wątpliwości co do dokładności lub adekwatności informacji uzyskanych wcześniej od klienta;

- i składają się z następujących działań:
  - identyfikacji Klienta, beneficjenta rzeczywistego i wykonawcy oraz weryfikacji ich tożsamości na podstawie dokumentów, danych lub informacji uzyskanych z wiarygodnego i niezależnego źródła;
  - pozyskiwanie i ocena informacji na temat celu i zamierzonego charakteru relacji biznesowej;
  - prowadzenie ciągłego monitoringu przez cały czas trwania relacji z klientem.

W tym celu Spółka – za pośrednictwem swoich pracowników i/lub agentów/doradców finansowych uprawnionych do składania ofert poza lokalem przedsiębiorstwa i mających bezpośredni kontakt z Klientem – uzyskuje informacje wymagane przepisami oraz gromadzi wszelką inną odpowiednią dokumentację określoną w niniejszej Polityce oraz dokumentach proceduralnych Spółki.

Spółka stosuje zwykłe, uproszczone lub wzmocnione środki należytej staranności wobec klienta, zgodnie z podejściem opartym na ryzyku stosowanym wobec klientów.

3.2.2 - Zdalne wdrażanie klientów

W przypadkach, gdy Spółka korzysta z metod zdalnej identyfikacji dozwolonych na mocy Dekretu Legislacyjnego nr. 231/07, art. 19 ust. 1 lit. a) pkt 2 i 5, przyjmuje specjalne procedury wykonywania obowiązków należytej staranności, także ze względu na ryzyko oszustwa związanego z kradzieżą tożsamości. Identyfikacja polega w tym przypadku na uzyskaniu certyfikatu kwalifikowanego podpisu elektronicznego, który powstaje po procesie identyfikacji przeprowadzanym poprzez:

- korzystanie z Publicznego Systemu Identyfikacji Cyfrowej (SPID) lub Elektronicznego Dowódu Identyfikacji;
- za pomocą bezpiecznych i regulowanych technik i procedur identyfikacji elektronicznej, które są autoryzowane lub uznawane przez Włoską Agencję ds. Cyfryzacji.

We wszystkich przypadkach proces zdalnej identyfikacji polega na zebraniu danych identyfikacyjnych klienta i wykonawcy w formacie elektronicznym, a także dokonaniu

weryfikacji i kontroli autentyczności danych, oprócz tych przewidzianych do identyfikacji osobistej, zgodnie z podejściem opartym na ryzyku, w tym poprzez kontakt telefoniczny pod certyfikowanym numerem (połączenie powitalne) lub przelew pieniężny realizowany przez klienta za pośrednictwem pośrednika bankowego i finansowego z siedzibą we Włoszech.

Mając na celu ograniczenie narażenia na potencjalne ryzyko prania pieniędzy i/lub oszustw, niedozwolone jest nawiązywanie relacji bankowych na odległość z osobami prawnymi lub osobami fizycznymi działającymi w imieniu osoby prawnej, chyba że zostały one zidentyfikowane osobiście (twarzą w twarz).

Nawiązywanie zdalnych relacji bankowych z klientami niebędącymi rezydentami Włoch jest niedozwolone.

3.2.3 – Ocena przedwdrożeniowa i bieżący monitoring procesów otwierania relacji zdalnych.

Procesy zdalnej identyfikacji i onboardingu klientów zostały sformalizowane i uszczegółowione w wewnętrznych regulacjach. Model nadzorowania tych procesów obejmuje:

I. wstępna ocena rozwiązania do zdalnego onboardingu (tzw. Ocena Przedwdrożeniowa).[8]) mające na celu:
   (i) ocenę adekwatności rozwiązania pod kątem kompletności i prawidłowości gromadzonych danych i dokumentów, a także rzetelności i niezależności wykorzystywanych źródeł informacji;
   (ii) ocenić wpływ wykorzystania rozwiązania na ryzyka biznesowe, w tym ryzyka operacyjne, reputacyjne i prawne, poprzez zaangażowanie odpowiednich funkcji technicznych i specjalistycznych;
   (iii) zidentyfikować środki łagodzące i działania naprawcze dla każdego zidentyfikowanego ryzyka;
   (iv) zdefiniuj testy ex ante w celu oceny ryzyka ICT i nadużyć finansowych oraz kompleksowe testy działania rozwiązania.

II. bieżący monitoring przyjętego rozwiązania onboardingowego poprzez kontrole okresowe i sterowane zdarzeniami, mające na celu zapewnienie jego prawidłowego funkcjonowania w czasie (tzw. Bieżący Monitoring).

III. przegląd oceny wstępnej w rozwiązaniu zdalnego onboardingu (tzw. Ocena Przedwdrożeniowa) w przypadku wystąpienia zmian strukturalnych w przyjętym rozwiązaniu lub wystąpienia określonych zdarzeń takich jak:
   (i) zmiany w narażeniu na ryzyka w obszarach przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu oraz embargo;
   ii) wykryte niedociągnięcia umożliwiające działanie naszego rozwiązania;
   iii) wzrost liczby prób oszustwa;
   (iv) zmiany w ustawodawstwie.

3.2.4 – Uproszczone obowiązki w zakresie należytej staranności

Generalnie Spółka stosuje podejście oparte na ryzyku w celu identyfikacji typów klientów, wobec których można zastosować uproszczone środki należytej staranności. Obejmuje to przypadki, w których występują „wskaźniki niskiego ryzyka", jak wskazano w załączniku 1 do Postanowienia Banku Włoch dotyczącego należytej staranności wobec klienta z dnia 30 lipca 2019 r. (zwanego dalej „Przepisem").

8 Nota nr 32 z dnia 13 czerwca 2023 r., w której Bank Włoch zadeklarował zamiar stosowania się do Wytycznych EBA (EBA/GL/2022/15) w sprawie stosowania rozwiązań w zakresie zdalnego onboardingu klientów.

Odpowiednie „wskaźniki niskiego ryzyka" w celu zastosowania uproszczonej procedury należytej staranności opierają się na rodzaju klienta, wykonawcy lub beneficjenta rzeczywistego, obszarze geograficznym zamieszkania lub siedziby głównej, konkretnym produkcie, usłudze lub kanale dystrybucji.

Szczegółowo, rodzaje klientów uznawanych za obarczonych niskim ryzykiem prania pieniędzy, do których może mieć zastosowanie uproszczone badanie due diligence, obejmują:

- Administracje publiczne, instytucje lub organy pełniące funkcje publiczne, zgodnie z prawem Unii Europejskiej;
- Spółki notowane na rynku regulowanym i podlegające wymogom informacyjnym, w tym zapewniającym odpowiednią przejrzystość ostatecznego beneficjenta rzeczywistego;
- instytucje kredytowe i finansowe Wspólnoty Europejskiej wymienione w art. 3 ust. 2 Rozporządzenia o przeciwdziałaniu praniu pieniędzy – z wyjątkiem tych oznaczonych literami i), o), s), v)[9]— oraz instytucje kredytowe i finansowe mające siedzibę w państwach członkowskich lub państwach trzecich posiadających skuteczne systemy prania pieniędzy i finansowania terroryzmu;
- Klienci, wykonawcy lub faktyczni właściciele zamieszkujący lub mający siedzibę na obszarach geograficznych o niskim ryzyku prania pieniędzy.

Spółka nie stosuje uproszczonych środków należytej staranności wobec klienta, gdy:

- powstają wątpliwości, niepewność lub niespójności dotyczące danych identyfikacyjnych oraz informacji zebranych podczas identyfikacji klienta, wykonawcy lub beneficjenta rzeczywistego;
- nie są już spełniane warunki uproszczonego badania należytej staranności wobec klienta w oparciu o wskaźniki ryzyka przewidziane w rozporządzeniu w sprawie przeciwdziałania praniu pieniędzy i odpowiednim rozporządzeniu wtórnemu;
- monitorowanie całości operacji prowadzonych przez Klienta oraz informacje zebrane w trakcie relacji wykluczają typ niskiego ryzyka;
- nadal pojawia się podejrzenie prania pieniędzy lub finansowania terroryzmu.

Funkcja Przeciwdziałania Praniu Pieniędzy ponosi wyłączną odpowiedzialność za ocenę i autoryzację uproszczonych środków należytej staranności wobec klienta, przeprowadzaną poprzez wykonanie wszystkich kroków wymaganych w zwykłym procesie należytej staranności wobec klienta – w tym obowiązek identyfikacji i weryfikacji tożsamości klienta, wykonawcy i Beneficjenta Rzeczywistego oraz pozyskania wszelkich danych i dokumentów niezbędnych do ich pełnej rejestracji (np. imię i nazwisko, status prawny, siedziba oraz, w stosownych przypadkach, kod podatkowy) – aczkolwiek zmniejszając poziom ich głębokości, zakresu i częstotliwości.

3.2.5 – Zaostrzone obowiązki w zakresie należytej staranności

Spółka stosuje wzmożone środki należytej staranności wobec klientów w obecności klientów lub w sytuacjach o podwyższonym ryzyku prania pieniędzy lub finansowania terroryzmu oraz we wszystkich przypadkach, o których mowa w art. 24 Rozporządzenia. Te ulepszone środki obejmują między innymi zaangażowanie osób odpowiedzialnych proporcjonalnie do poziomu ryzyka zidentyfikowanego w odniesieniu do klienta.

9 i) maklerzy giełdowi, o których mowa w art. 201 TUF; o) pośrednicy ubezpieczeniowi, o których mowa w art. 109 ust. 2 lit. a), b), i d), WPR, działający w gałęziach działalności, o których mowa w art. 2 ust. 1 WPR; s) spółki powiernicze zarejestrowane w rejestrze utworzonym na podstawie art. 106 TUB; v) doradcy finansowi, o których mowa w art. 18-bis TUF oraz firmy doradztwa finansowego, o których mowa w art. 18-ter TUF.

W przypadku klientów bankowości prywatnej Spółka dokonuje oceny specyficznych czynników ryzyka wynikających z charakteru prowadzonej przez nich działalności i stosuje wzmożone środki należytej staranności w oparciu o całość dostępnych informacji i przeprowadzonych ocen.

Zaangażowanie Jednostki ds. Przeciwdziałania Praniu Pieniędzy wymagane jest w następujących przypadkach:

- osoby fizyczne i prawne umieszczone na listach osób lub podmiotów objętych środkami zamrożenia funduszy na mocy rozporządzeń lub dekretów europejskich na mocy dekretu z mocą ustawy 109/07, a także osoby blisko z nimi powiązane;
- transgraniczna relacja w zakresie bankowości korespondencyjnej nawiązana z bankiem lub instytucją zlokalizowaną w państwie trzecim w oparciu o geograficzne czynniki wysokiego ryzyka (zgodnie z załącznikiem 2 do przepisów Banku Włoch dotyczących należytej staranności wobec klienta);
- powiązania lub transakcje, w których klientem lub ostatecznym beneficjentem rzeczywistym jest osoba zajmująca eksponowane stanowisko polityczne[10];
- sytuacje zawierające elementy ryzyka wymagające zastosowania określonych środków poufności;
- sytuacja o podwyższonym ryzyku prania pieniędzy lub finansowania terroryzmu ze względu na obiektywne, środowiskowe lub subiektywne zdarzenia losowe;
- klienci sklasyfikowani jako „Trust", usługi przekazów pieniężnych i wymiany walut wirtualnych;
- Spółki powiernicze, z wyjątkiem przypadków przewidzianych w paragrafie 3.4;

Ponadto przed nawiązaniem, kontynuacją lub utrzymaniem bieżących relacji z Osobami na Eksponowanym Politycznie Ekspozycjach lub Podmiotami Korespondencyjnymi z państw trzecich konieczne jest uzyskanie odpowiedniego upoważnienia od Dyrektora Generalnego lub jego delegata, po uzyskaniu opinii Jednostki ds. Przeciwdziałania Praniu Pieniędzy. W przypadku delegatów zgodnie z art. 25 dekretu legislacyjnego 231/07 należących do Jednostki ds. przeciwdziałania praniu pieniędzy, upoważnienie to jest objęte wzmocnionym procesem due diligence.

We wszystkich pozostałych przypadkach zastosowanie wzmocnionych środków jest współmierne do poziomu ryzyka przypisanego klientowi. Jeżeli ryzyko zostanie uznane za średnie/wysokie lub jeśli wystąpią pewne czynniki ryzyka niezależnie od przyznanej oceny, wymagane jest zaangażowanie kierownika jednostki biznesowej odpowiedzialnej za zarządzanie handlowe klientem.

Przykładami takich przypadków są:

- klienci będący osobami prawnymi posiadającymi Wykonawcę zidentyfikowanego jako PEP lub pośredni PEP, niezależnie od profilu ryzyka;
- usługi oferowane za pośrednictwem sieci agentów finansowych, doradców finansowych, wykonawców i agentów;
- klienci sklasyfikowani jako fundacje/organizacje non-profit;
- klienci będący osobami prawnymi na etapie wdrażania;
- klientom negatywne wiadomości na etapie onboardingu („Niekorzystne wiadomości");

10 Osoby na eksponowanym stanowisku politycznym (PEP): wymienione w art. 1 ust. 2 lit. dd) Dekret z mocą ustawy 231/07.

- klienci mający miejsce zamieszkania lub siedzibę w państwach trzecich wysokiego ryzyka lub w przypadku stałych relacji, usług profesjonalnych i operacji z udziałem krajów wysokiego ryzyka;
- spółki, które wyemitowały akcje na okaziciela lub które w swojej strukturze kontroli posiadają spółkę emitującą akcje na okaziciela;
- powiązania lub transakcje, w ramach których klient i ostateczny właściciel rzeczywisty zajmują stanowiska publiczne inne niż te wymienione dla osób zajmujących eksponowane stanowiska polityczne[11];
- spółki będące własnością Trustów, spółek powierniczych, fundacji, spółek akcyjnych poprzez wielopoziomowe uczestnictwo lub holdingi krzyżowe;
- klienci prowadzący działalność gospodarczą szczególnie narażoną na ryzyko prania pieniędzy lub w „kontrowersyjnych" sektorach działalności[12] lub działalność komercyjna wymagająca dużej ilości gotówki, taka jak wymiana pieniędzy na złoto, wymiana pieniędzy, gry hazardowe/zakłady, w tym internetowe, przemysł zbrojeniowy, górnictwo, zbiórka i utylizacja odpadów, produkcja energii odnawialnej, spółki działające w sektorze kryptowalut, budownictwo, zakup instrumentów farmaceutycznych;
- klienci uczestniczący w zamówieniach publicznych lub otrzymujący finansowanie publiczne (służba zdrowia, budownictwo, zbiórka i utylizacja odpadów, produkcja energii odnawialnej, górnictwo, dostawa instrumentów farmaceutycznych);
- w przypadku klientów, którzy nabyli obywatelstwo państwa członkowskiego lub uzyskali prawo pobytu w państwie członkowskim (UE) w ramach programu „Obywatelstwo w ramach programu inwestycyjnego" lub „Program pobytu w ramach programu inwestycyjnego";
- w przypadku klientów będących osobami prawnymi mającymi siedzibę w kraju UE, w których prawa własności spółki posiadają – bezpośrednio lub pośrednio – w ponad 40% osoba prawna, organizacja lub organ z siedzibą w Rosji lub osoba fizyczna posiadająca miejsce zamieszkania lub obywatelstwo rosyjskie.

Zaangażowanie Kierownika jednostki biznesowej odpowiedzialnej za zarządzanie handlowe klientem jest wymagane także w przypadku wystąpienia błędów informatycznych, które mogłyby uniemożliwić wyliczenie w czasie rzeczywistym ryzyka prania pieniędzy klienta.

Wzmocnione środki należytej staranności obejmują pozyskanie dodatkowych informacji o kliencie, wykonawcy i beneficjentu rzeczywistym, zbadanie celu i charakteru relacji oraz zwiększenie częstotliwości procedur mających na celu zapewnienie stałego monitorowania w trakcie trwającej relacji.

W pełnej zgodności z obowiązującymi przepisami prawa oraz postanowieniami wewnętrznych procedur dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu oraz zgodnie z Kodeksem Etyki Spółki, Spółka nie obsługuje transakcji z klientami działającymi w kontrowersyjnych sektorach, które
(i) nie są zgodne z obowiązującym prawodawstwem krajowym oraz (ii) nie zostały, w stosownych przypadkach, uprzednio zatwierdzone przez właściwe włoskie władze krajowe, w szczególności:

- produkcja, tranzyt i/lub obrót materiałami zbrojeniowymi;
- produkcja i sprzedaż lekkiej marihuany, miejsca rozrywki dla dorosłych;

11 Stanowisko publiczne inne niż te sprawowane przez osoby na eksponowanym stanowisku politycznym (PEP), o których mowa w przypisie 1), mające zastosowanie do wszystkich osób sprawujących funkcje w, między innymi, organach publicznych, konsorcjach i stowarzyszeniach o charakterze publicznym wymienionych w sekcji A 8) załącznika 2 do tego przepisu.
12 sektor gospodarczy jest „kontrowersyjny", jeśli towary/usługi wytwarzane/oferowane i/lub sposoby ich wytwarzania/oferowania stoją w sprzeczności z powszechnie podzielanymi wartościami, takimi jak etyka i zrównoważony rozwój, nawet jeśli usługi lub działania są zgodne z prawem, a zatem nie stoją w sprzeczności z zobowiązaniami prawnymi.

- działalność handlowa wymagająca dużej ilości gotówki, inna niż wymieniona powyżej, taka jak nieregulowane organizacje charytatywne i organizacje pozarządowe, produkcja metali i kamieni szlachetnych, przekazy pieniężne.

Ponadto Spółka przywiązuje szczególną wagę do przestrzegania środków ograniczających wprowadzonych przez państwo włoskie, podmioty zagraniczne (np. OFAC, UKSL) i/lub organy ponadnarodowe (ONZ, UE). Środki te mogą mieć charakter komercyjny (np. blokowanie importu/eksportu) lub charakter finansowy, taki jak częściowe/całkowite blokowanie przekazów pieniężnych z lub do określonego kraju lub ograniczenia operacji i/lub zamrożenie funduszy przechowywanych u pośredników finansowych.

W celu wywiązania się z obowiązków określonych we włoskim dekrecie legislacyjnym 109/07 – mających na celu zapobieganie i zwalczanie finansowania terroryzmu oraz działań krajów zagrażających międzynarodowemu pokojowi i bezpieczeństwu, poprzez zastosowanie środków ograniczających w celu „zamrożenia" funduszy i zasobów gospodarczych posiadanych przez osoby fizyczne i prawne, grupy i podmioty specjalnie określone przez Organizację Narodów Zjednoczonych i Unię Europejską („wyznaczone podmioty") – oraz wzmocnione obowiązki w zakresie należytej staranności określone we włoskim dekrecie legislacyjnym 231/07, Spółka przyjęła automatyczne procedury kontrolne. Procedury te umożliwiają weryfikację zgodności danych identyfikacyjnych klienta uzyskanych w procesie należytej staranności z danymi zawartymi w wykazach sporządzanych przez UE oraz inne instytucje i organy międzynarodowe, takie jak:

- osoby, którym powierzono eksponowane stanowisko publiczne lub które przestały sprawować tę funkcję krócej niż rok (PEP), członkowie ich rodzin oraz osoby pozostające z nimi w bliskich stosunkach zgodnie z definicją art. 1 w. 2 litera dd dekretu legislacyjnego 231/07 (PEP będący rezydentem i nierezydentem);
- osoby fizyczne zamieszkujące we Włoszech, sprawujące funkcje publiczne, które nie mieszczą się w definicji PEP, a mimo to są narażone na znaczne ryzyko korupcji i prania pieniędzy;
- osoby fizyczne i prawne działające, choćby częściowo, w państwach, które nie nakładają równoważnych środków i przepisów, zgodnie z wytycznymi Banku Włoch lub innych instytucji krajowych lub ponadnarodowych zaangażowanych w zapobieganie przestępczości;
- osoby fizyczne i prawne objęte embargiem lub zamrożeniem funduszy/zasobów gospodarczych i aktywów finansowych (Listy Sankcyjne ONZ, UE, UKSL, OFAC).

3.3 - PROFILOWANIE KLIENTÓW

Spółka przyjmuje odpowiednie procedury mające na celu określenie profilu ryzyka prania pieniędzy i finansowania terroryzmu (RP) przypisanego każdemu klientowi, na podstawie uzyskanych informacji i przeprowadzonych analiz, zarówno w odniesieniu do elementów oceny wskazanych w Przepisie, jak i dalszych elementów, które z biegiem czasu może przyjąć sama Spółka (tzw. profilowanie).

W oparciu o profilowanie klientów, które również przeprowadza się okresowo, Spółka stosuje standardowe lub ulepszone działania, które obejmują zaangażowanie osób odpowiedzialnych proporcjonalnie do zidentyfikowanego poziomu ryzyka klienta. Wymagana jest uprzednia opinia Jednostki ds. Przeciwdziałania Praniu Pieniędzy zgodnie z obowiązkami określonymi w

dokumencie wewnętrznym „Wewnętrzne procedury dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu”.

Klasyfikacja klientów do uproszczonego badania due diligence jest zatwierdzana przez Jednostkę ds. Przeciwdziałania Praniu Pieniędzy na wniosek Kierownika Jednostki Biznesowej Operacyjnej.

W takim przypadku zakres i częstotliwość wymogów ulega zmniejszeniu, a weryfikacja wygasa po 8 latach, niezależnie od oceny ryzyka, chyba że przestaną być spełnione warunki stosowania uproszczonego due diligence.

Ponadto Spółka posiada wdrożoną procedurę informatyczną pozwalającą na ocenę profilu ryzyka klienta oraz spójne określenie ram czasowych ponownej oceny, odpowiednich do obliczonego poziomu ryzyka; częstotliwość ponownej oceny zależy od procesu zidentyfikowanego w ostatniej przeprowadzonej ocenie lub, w przypadku braku kwestionariusza KYC, od profilu ryzyka klienta, jak określono poniżej:

<table>
<tr><th>Klasa ryzyka (RP)</th><th>Wynik</th><th>Proces due diligence</th><th>Rola walidacyjna</th><th>Częstotliwość ponownej oceny</th></tr>
<tr><td>Klienci zaklasyfikowani do kategorii objętych uproszczonym badaniem due diligence</td><td>NA</td><td>Uproszczone</td><td>Akceptacja automatyczna/Kierownik jednostki biznesowej (*)</td><td>8 lat</td></tr>
<tr><td>Nieistotne</td><td><=5</td><td rowspan="2">Standardowe</td><td rowspan="2">Automatyczna akceptacja</td><td>8 lat</td></tr>
<tr><td>Niski</td><td>>=6 i <=12</td><td>6 lat</td></tr>
<tr><td>Średni</td><td>>=13 i <=24</td><td rowspan="2">Ulepszone</td><td rowspan="2">Kierownik jednostki biznesowej (**)</td><td>2 lata</td></tr>
<tr><td>Wysoka</td><td>>=25</td><td>1 rok</td></tr>
<tr><td colspan="2">W przypadku szczególnych elementów ryzyka (***)</td><td>Ulepszone</td><td>Funkcja walidacji AML</td><td>1 rok</td></tr>
</table>

(*) podawane, jeżeli ocena ryzyka obliczona lub wynikająca z przeprowadzonego KYC jest co najmniej Średnia. (**) zapewnione nawet w przypadku występowania określonych elementów ryzyka, które utrzymują profil ryzyka poniżej Średniego.
(***) Świadczone nawet w obecności Podmiotów Prawnych z RP >39, jeśli prowadzą one działalność handlową związaną z zakupem złota, grami i zakładami wzajemnymi oraz zbieraniem i utylizacją odpadów (kody ATECO wysokiego ryzyka) i/lub jeśli podlegają audytom/dochodzeniom.

3.4 - NARZĘDZIA WSPIERAJĄCE NALEŻYTĄ STARANNOŚĆ

Oprócz już wykorzystywanych tradycyjnych aplikacji, Spółka wdrożyła zaawansowane technologicznie narzędzia wspierające procesy przeciwdziałania praniu pieniędzy:

- Robotic Process Automation (RPA) zastosowany do działań związanych z gromadzeniem danych w obszarach należytej staranności wobec klienta i raportowania podejrzanych transakcji;
- Silnik sztucznej inteligencji, oparty na komponentach statystycznych i wskaźnikach predykcyjnych (Predict Index AML, Reputational Index i Criminal Infiltration Index) zbudowany przy użyciu technik Data Analytics, stosowany w regularnym procesie oceny klientów;
- Platforma wywiadowcza Cogito, aplikacja służąca do gromadzenia aktualności, dokumentów i informacji tekstowych w celu wyszukiwania niekorzystnych wiadomości dotyczących klientów objętych należytą starannością;

- Rozes, narzędzie do analityki danych, które analizując sprawozdania finansowe w czasie rzeczywistym, umożliwia identyfikację spółek, których bilans i wskaźniki finansowe są podobne do tych występujących w spółkach objętych infiltracją przestępczą.

Ponadto w ramach wyżej wymienionych zaawansowanych narzędzi zidentyfikowano pewne „zdarzenia wyzwalające", mające na celu przechwycenie zdarzeń dotyczących klienta i/lub relacji z nim powiązanych, określające zmianę daty ważności „Oceny Klienta – KYC", np.:

- w przypadku zmiany danych rejestrowych beneficjenta rzeczywistego i przedstawiciela prawnego;
- w przypadku zmiany Profilu Ryzyka w związku z wystąpieniem określonych czynników wysokiego ryzyka spośród przewidzianych w Przepisie;
- w przypadku objęcia przez beneficjenta rzeczywistego roli PEP lub rejestracji nowego beneficjenta rzeczywistego PEP;
- w przypadku delegowania na osobę fizyczną relacji z klientem przekazanej osobie sklasyfikowanej jako PEP;
- w przypadku rozbieżności pomiędzy beneficjentem rzeczywistym zarejestrowanym w rejestrze a dowodami zebranymi na podstawie wypisów z Izby Handlowej;
- w przypadku kontroli drugiego stopnia przeprowadzanych przez funkcję AML.

Odpowiedzialność za proces należytej staranności wobec klienta spoczywa na jednostce ds. zarządzania relacjami z klientem, która zazwyczaj zajmuje się nawiązywaniem nowych stałych relacji, przeprowadzaniem okazjonalnych transakcji, okresową ponowną oceną istniejących klientów i zapewnia ciągłe monitorowanie relacji z klientami.

3.5 - OBOWIĄZKI WSTRZYMANIA SIĘ

Spółka powstrzymuje się od nawiązania, realizacji lub kontynuowania relacji, działalności i usług profesjonalnych (tzw. obowiązek wstrzymania się) w przypadku obiektywnej niemożności przeprowadzenia badania due diligence klienta, oceny czy zgłosić podejrzaną transakcję do FIU.

W przypadkach, w których wstrzymanie się od głosu nie jest możliwe, gdyż istnieje prawny obowiązek wykonania operacji, której nie można odłożyć na później lub gdy odmowa mogłaby utrudnić śledztwo, Spółka ma jednak obowiązek niezwłocznego zgłoszenia podejrzanej transakcji.

Ponadto, jeżeli po dalszej ocenie lub w następstwie wzmocnionego procesu due diligence pojawią się elementy obarczone wysokim ryzykiem, które mogą mieć wpływ na profil prawny i/lub reputację Spółki, Spółka zastrzega sobie prawo do ograniczenia lub zakończenia relacji biznesowej z klientem. Ograniczenia te mogą dotyczyć m.in. dostępu Klienta do niektórych rodzajów produktów lub skutkować przerwaniem świadczenia usług oferowanych przez Spółkę w związku z kontem/relacją.

Przyjęte przez Spółkę środki należytej staranności wobec klienta nie wykluczają jednak/nie odmawiają dostępu do usług finansowych klientom lub całym kategoriom klientów wysokiego ryzyka, którzy byliby do nich uprawnieni na mocy obowiązujących przepisów, z wyjątkiem przypadków wyraźnie przewidzianych w Dekrecie Legislacyjnym 231/07 dotyczącym zakazu utrzymywania relacji z określonymi rodzajami podmiotów.

Spółka nie nawiązuje relacji korespondencyjnej z bankiem fasadowym oraz wstrzymuje się od nawiązywania relacji z podmiotami umożliwiającymi dostęp do relacji korespondencyjnych z Bankiem fasadowym. Nie może nawiązywać stosunków gospodarczych z podmiotami, których struktura właścicielska (korporacyjna, skarbowa i finansowa) charakteryzuje się dużą nieprzejrzystością, uniemożliwiającą jednoznaczne zidentyfikowanie beneficjenta rzeczywistego oraz charakteru i przeznaczenia tej struktury.

W tym celu Spółka podejmuje wszelkie środki, aby nie podejmować celowej i świadomej współpracy z instytucjami finansowymi, które z kolei współpracują z bankami fasadowymi.

Ponadto Spółka powstrzymuje się od nawiązywania i kontynuowania relacji biznesowych z osobami szczególnie narażonymi na ryzyko prania pieniędzy/finansowania terroryzmu, takimi jak:

- Spółki powiernicze mające siedzibę w kraju wskazanym przez FATF jako kraj o podwyższonym ryzyku prania pieniędzy lub które nie przyjmują środków zgodnych z obowiązkami nałożonymi Dekretem Legislacyjnym 231/07 lub Dyrektywami Europejskimi;
- Trusty, w przypadku których nie są dostępne odpowiednie, dokładne i aktualne informacje na temat beneficjentów rzeczywistych trustu oraz jego charakteru i celu;
- Firmy bukmacherskie, w tym gry hazardowe online, kasyna i operatorzy Bingo, dla których nie zostały wydane i/lub zweryfikowane zezwolenia i/lub licencje wymagane na mocy ustawodawstwa włoskiego i międzynarodowego;
- Podmioty powiązane i agenci dostawców usług płatniczych (o których mowa w definicji art. 1 c. 2 lit. nn) oraz instytucje pieniądza elektronicznego, które nie spełniają przepisów rozdziału V dekretu z mocą ustawy 231/07 w art. 43 i nast.;
- Spółki z ograniczoną odpowiedzialnością lub spółki kontrolowane poprzez akcje na okaziciela, z siedzibą w krajach wysokiego ryzyka;
- Klienci zajmujący się produkcją i sprzedażą lekkiej marihuany lub lokalami rozrywkowymi dla dorosłych, jeśli nie są w stanie zweryfikować wymaganych prawem zezwoleń.

Spółka wykorzystuje wszystkie informacje uzyskane w procesie due diligence w odniesieniu do swoich klientów i ich transakcji w celu ustalenia, czy dana transakcja lub relacja biznesowa jest bezpośrednio lub pośrednio powiązana z osobami lub podmiotami zaangażowanymi w pranie pieniędzy, finansowanie terroryzmu lub opracowywanie broni masowego rażenia i w żaden sposób nie wspiera transakcji związanych z bronią kontrowersyjną i/lub zakazaną na mocy traktatów międzynarodowych,
np. broń nuklearna, biologiczna i chemiczna, bomby kasetowe, broń zawierająca zubożony uran, miny przeciwpiechotne.

W zakresie produkcji, tranzytu i/lub obrotu materiałami zbrojeniowymi innymi niż wymienione powyżej, Spółka może wspierać transakcje, które zostały należycie autoryzowane przez właściwe organy i są zgodne z obowiązującymi i obowiązującymi przepisami prawa.

3.6 – ZGŁASZANIE TRANSAKCJI PODEJRZANYCH

Ilekroć Spółka podejrzewa lub ma uzasadnione podstawy, aby podejrzewać, że miała miejsce lub jest przeprowadzana lub podejmowana była próba prania pieniędzy lub finansowania

terroryzmu:

- składa raport o podejrzanej transakcji do jednostki analityki finansowej (FIU), jeśli transakcja ma miejsce we Włoszech;

- jeżeli transakcja ma miejsce w innym Kraju, jest zgodna z przepisami prawa lokalnego, a w przypadku gdy przewiduje ono zastosowanie środków równoważnych do przewidzianych przez prawo UE, niezwłocznie informuje o tym Szefa Działu Przeciwdziałania Praniu Pieniędzy, zachowując wszelkie niezbędne środki ostrożności w celu ochrony tożsamości osób zgłaszających podejrzaną transakcję.

Spółka wdrożyła procedury i procesy monitorowania, identyfikowania i zgłaszania podejrzanych działań zgodnie z harmonogramem i metodami wymaganymi przez obowiązujące prawo.

Pracownicy niezwłocznie zgłaszają wszelkie informacje lub podejrzenia dotyczące prania pieniędzy, finansowania terroryzmu lub innej działalności przestępczej bądź dochodów z działalności przestępczej, niezależnie od jej rozmiaru, zgodnie ze zaktualizowanym modelem organizacyjnym i trybami działania określonymi w odpowiednich przepisach wewnętrznych. Do czasu zakończenia procesu raportowania Spółka wstrzymuje się z realizacją transakcji, chyba że jest to niemożliwe ze względu na prawny obowiązek przyjęcia aktu lub nie można odroczyć wykonania operacji ze względu na normalny tryb prowadzenia działalności lub mogłoby to utrudnić prowadzenie śledztwa. W takich przypadkach zgłoszenie następuje niezwłocznie po zawarciu transakcji.

Podstawą podejrzeń jest charakterystyka, skala i charakter transakcji, próba podziału transakcji oraz wszelkie inne okoliczności, o których pracownicy dowiedzą się w związku z pełnionymi obowiązkami, biorąc także pod uwagę zakres finansowy i charakter działalności prowadzonej przez podmiot podejrzanej transakcji, w oparciu o elementy uzyskane na podstawie przepisów dotyczących przeciwdziałania praniu pieniędzy (np. podczas badania due diligence).

Aby ograniczyć ryzyko zaangażowania Spółki – nawet niezamierzonego – w nielegalne działania, o których mowa powyżej, w ramach umów dotyczących transferu środków uruchamiany jest wzmocniony proces due diligence, w przypadku którego uczestnicy zaangażowani w tego typu transakcje (inicjator, beneficjent, banki zaangażowane w transfer środków) mogą wzbudzić podejrzenia prania pieniędzy, finansowania terroryzmu lub naruszenia obowiązujących międzynarodowych ograniczeń dotyczących niektórych towarów, osób lub podmiotów.

Na dalszym etapie procesu raportowania Firma może ograniczyć i/lub przerwać relacje biznesowe z klientami, w szczególności w przypadku, gdy taka relacja może stanowić znaczące ryzyko prawne lub ryzyko dla reputacji dla Rox Pay S.r.l.

3.7 – PRZECHOWYWANIE DANYCH

Spółka przechowuje wszystkie dokumenty i rejestruje wszystkie dane uzyskane w ramach procesu należytej staranności wobec klienta, zapewniając identyfikowalność transakcji klientów w celu ułatwienia funkcji kontrolnych Banku Włoch i FIU, w tym inspekcji.

W tym celu Rox Pay S.r.l., jako pośrednik finansowy z siedzibą we Włoszech, utworzyła Jednolite Archiwum Elektroniczne (Archivio Unico Informatico lub AUI), które umożliwia mu dostarczanie informacji Bankowi Włoch i FIU zgodnie ze standardami technicznymi określonymi w Załączniku 2 do Postanowień o zatrzymywaniu danych. To archiwum przechowuje w formie elektronicznej wszystkie dane identyfikacyjne i inne informacje związane z bieżącymi relacjami biznesowymi i transakcjami z klientami, zgodnie z wymogami obowiązującego prawa.

W związku z tym, w odpowiedzi na niedawne aktualizacje wprowadzone „Przepisami o przechowywaniu danych i dostępie do dokumentów, danych i informacji” oraz „Przepisami o przesyłaniu zbiorczych danych”, Spółka zdecydowała się przyjąć określone zasady zwolnienia z obowiązków rejestracyjnych, które zostały wyraźnie określone. W szczególności dane i informacje dotyczące transakcji zawieranych przez pośredników bankowych i finansowych, objętych przypadkami określonymi w art

8 przepisów o zatrzymywaniu danych oraz art. 3 przepisów o danych zbiorczych nie są rejestrowane w Jednolitym Archiwum Elektronicznym.

Jeśli chodzi o wymogi należytej staranności wobec klienta, Spółka przechowuje kopie lub rejestry wszystkich wymaganych dokumentów przez okres dziesięciu lat po zakończeniu relacji biznesowej.

W przypadku transakcji i trwających relacji biznesowych wszelkie dowody i zapisy potwierdzające, np. oryginały dokumentów lub kopie dopuszczalne w postępowaniu sądowym, są przechowywane przez okres dziesięciu lat od zawarcia transakcji lub zakończenia relacji biznesowej.

3.8 – ZAPOBIEGANIE ŚRODKOM OGRANICZAJĄCYM DOTYCZĄCYM REGULACJI

Spółka, ze względu na charakter, wielkość i złożoność prowadzonej działalności, a także zakres i rodzaj świadczonych usług, narażona jest na ryzyko naruszenia środków ograniczających.

W celu utrzymania systemu organizacyjno-proceduralnego mającego na celu zapewnienie zgodności z unijnymi i krajowymi międzynarodowymi środkami ograniczającymi, ryzyko naruszeń środków ograniczających oceniane jest przez Jednostkę ds. Przeciwdziałania Praniu Pieniędzy na podstawie czynników geograficznych, klientów, produktów/usług i kanałów dystrybucji, zapewniając stałe monitorowanie efektywności systemu, gwarantowane również poprzez okresowe przeprowadzanie samooceny, co pozwala na identyfikację ewentualnych działań naprawczych w odpowiedzi na wykrycie istniejących krytycznych problemów i/lub przyjęcie odpowiedniego zapobiegania i ograniczania ryzyka środki.

Spółka ustanowiła procedury i procesy monitorowania, identyfikowania i raportowania działań naruszających środki ograniczające, z harmonogramem i metodami zgodnymi z wymogami prawnymi.

Istniejące kontrole osób/podmiotów i transakcji przeprowadzane są poprzez zautomatyzowany proces screeningu, który przeprowadzany jest zarówno codziennie, jak i w fazie onboardingu, przy użyciu specjalnych list – aktualizowanych dwa razy dziennie – dotyczących klientów, kontrahentów, krajów i transakcji.

Istnieją procesy monitorowania przepływów przychodzących i wychodzących z krajami i/lub podmiotami objętymi międzynarodowymi sankcjami finansowymi, przy czym obowiązki są określone pomiędzy właściwymi departamentami.

Zapewnia się odpowiednie przeszkolenie personelu oraz zapoznanie go z zasadami, procedurami i mechanizmami kontrolnymi w celu zapewnienia zgodności ze środkami ograniczającymi.

4 – LISTA KLUCZOWYCH PROCESÓW

4.1 – ZARZĄDZANIE RYZYKIEM PRANIA PIENIĘDZY I FINANSOWANIA TERRORYZMU

Proces „Zarządzanie ryzykiem prania pieniędzy i finansowania terroryzmu” to proces, w ramach którego w Spółce realizowane są następujące działania mające na celu ograniczenie ryzyka nieprzestrzegania wymogów w zakresie przeciwdziałania praniu pieniędzy i

finansowaniu terroryzmu:

- Identyfikacja ryzyka braku zgodności z wymogami AML-CFT poprzez stały nadzór nad zmianami w przepisach prawa oraz ocenę wpływu na procesy i procedury biznesowe, a także identyfikację i ocenę ryzyka AML-CFT z wykorzystaniem podejścia opartego na ryzyku;

- Zarządzanie i ograniczanie ryzyka prania pieniędzy i finansowania terroryzmu poprzez wdrażanie i monitorowanie działań łagodzących ryzyko braku zgodności określone w Planie Rocznym (Plan AML) lub zidentyfikowane przez Zarząd Spółki jako stosowane przez wszystkie istotne funkcje biznesowe w ramach wdrażania procedur (przepisy wewnętrzne, aplikacje informatyczne, procesy operacyjne, kontrole);
- Kontrole zgodności (ex ante i ex post) w obszarach regulacyjnych przypisanych przez właściciela poprzez określenie i monitorowanie wskaźników ryzyka oraz ich ewolucji w czasie. Celem jest znalezienie ewentualnych sytuacji niezgodności oraz przeprowadzenie działań kontrolnych ex ante i ex post;
- Zapewniamy doradztwo i wsparcie w kwestiach AML/CFT, uczestnicząc w interdyscyplinarnych zespołach roboczych oraz zapewniając wsparcie strukturom biznesowym lub najwyższemu organowi kierowniczemu w kwestiach i procesach biznesowych, w których istotne jest ryzyko prania pieniędzy i finansowania terroryzmu, realizując działania przewidziane przepisami nadzorczymi i dokonując wstępnej oceny zgodności w tym obszarze przy oferowaniu nowych produktów/usług;
- Monitorowanie i kontrola ryzyka AML/CFT poprzez analizę przepływów informacji otrzymywanych od poziomu I i innych funkcji kontrolnych związanych z operacyjnymi wymogami dotyczącymi przeciwdziałania praniu pieniędzy oraz poprzez wdrażanie mechanizmów kontrolnych monitorujących ryzyko i stałą weryfikację ich adekwatności;
- Przeprowadzenie samooceny AML poprzez przeprowadzenie czynności wstępnych niezbędnych do wypełnienia tzw. Kwestionariuszy „Systemowych" i „Operacyjnych" oraz określenia ryzyka resztkowego;
- Raportowanie do Najwyższych Organów Korporacyjnych i Organów Nadzorczych, w szczególności przygotowanie rocznego raportowania do Organów Korporacyjnych i Rady Nadzorczej, a także przygotowanie okresowych sprawozdań z wykonanej działalności i wszelkich konkretnych żądań Organów Nadzorczych;
- Zapewnienie konkretnych kursów szkoleniowych w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu poprzez organizację odpowiedniego planu szkoleniowego wraz z innymi funkcjami korporacyjnymi odpowiedzialnymi za szkolenia. Celem jest ciągłe szkolenie pracowników i współpracowników.

Szczegółowe zasady i obowiązki Spółki dotyczące tego procesu są szczegółowo opisane w dokumencie wewnętrznym
dokument „Wewnętrzne procedury przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu".

4.2 – ZARZĄDZANIE RELACJAMI Z ORGANAMI NADZORCZYMI W CELU ZWALCZANIA PRANIA PIENIĘDZY I FINANSOWANIA TERRORYZMU

Proces zarządzania relacjami regulacyjnymi w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu to proces, w ramach którego w Spółce prowadzone są działania mające na celu zarządzanie, analizowanie, kierowanie i monitorowanie wszelkiej komunikacji z organami regulacyjnymi w kwestiach związanych z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu. Celem jest nadzorowanie tych działań, w tym archiwizacja dokumentów w jednym repozytorium.

W ramach tego procesu realizowane są następujące działania:

- Zarządzanie relacjami z Organami Nadzorczymi (Przeciwdziałanie Praniu Pieniędzy),

zarządzanie, analizowanie i odpowiadanie na komunikację i wnioski Organów Nadzorczych dotyczące zgodności w tym zakresie;

- Zarządzanie raportami nadzorczymi dotyczącymi przeciwdziałania praniu pieniędzy, poprzez przygotowanie przepływu i wysyłanie raportów nadzorczych dotyczących przeciwdziałania praniu pieniędzy;

- Prowadzenie postępowań administracyjnych związanych z przeciwdziałaniem praniu pieniędzy poprzez badanie roszczeń wzajemnych związanych z postępowaniami administracyjnymi zgłaszanymi Spółce przez właściwe organy (GdF i FIU), a także reprezentowanie Spółki przed MEF, będąc odpowiedzialnym za spis postępowań w związku z tym wnioskiem oraz za alokację do Rezerwy na Ryzyka i Opłaty oraz zapłatę ewentualnych sankcji, w koordynacji z Pionem Budżetu.

Szczegółowe zasady i obowiązki Spółki dotyczące tego procesu są szczegółowo opisane w dokumencie wewnętrznym „Wewnętrzne procedury dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu".

4.3 – ZARZĄDZANIE WYMOGAMI OPERACYJNYMI W CELU ZWALCZANIA PRANIA PIENIĘDZY I FINANSOWANIA TERRORYZMU

Proces zarządzania wymaganiami operacyjnymi AML/CFT to proces, w ramach którego w Spółce realizowane są następujące działania w celu spełnienia wymogów regulacyjnych:

- ograniczenie stosowania środków pieniężnych i papierów wartościowych na okaziciela, poprzez realizację wymogów regulacyjnych dotyczących ograniczeń stosowania środków pieniężnych i obligacji/papierów wartościowych na okaziciela;
- zarządzanie odpowiednimi obowiązkami należytej staranności wobec klienta, poprzez realizację czynności należytej staranności wobec klienta (lub zwiększonego due diligence) w przypadkach przewidzianych przez prawo włoskie (Dekret Legislacyjny 231/07 z późniejszymi zmianami) w zależności od profilu ryzyka klientów, wspieranie Sieci Spółki w wypełnianiu obowiązków wymaganych przez obowiązujące przepisy prawa i regulacje oraz zapewnianie wsparcia strukturom Spółki zarządzającym relacjami z klientami oraz kontrahentami bankowymi i finansowymi w celu umożliwienia nawiązania i utrzymania relacji;
- zarządzanie obowiązkami zgłaszania podejrzanych transakcji, poprzez wykonywanie czynności związanych ze zgłaszaniem podejrzanych transakcji poprzez wykonywanie delegacji Zarządu (dawny art. 36 dekretu legislacyjnego 231/07) oraz monitorowanie wniosków otrzymanych od FIU;
- zarządzanie obowiązkami dotyczącymi zwalczania finansowania terroryzmu poprzez określenie metodologii kontroli mającej na celu zapewnienie wdrożenia unijnych i krajowych środków ograniczających, weryfikację transpozycji aktualizacji list sankcji, a także składanie sprawozdań właściwym organom (krajowym i nadzorczym) w sprawie środków ograniczających (FIU, MAECI i MEF) w zakresie środków zamrożenia kapitału (dawny dekret ustawodawczy 109/07) oraz spełnianie niezbędnych wymogów operacyjnych;
- zarządzanie obowiązkami w zakresie przechowywania danych poprzez weryfikację wiarygodności Systemu Informatycznego poprzez aktualizację Archivio Unico Informatico (AUI), dokonywanie wszelkich zmian, okresowe przesyłanie danych zbiorczych do FIU oraz przekazywanie FIU i Bankowi Włoch powiadomień wymaganych przepisami;
- monitorowanie prawidłowego wdrażania międzynarodowych sankcji finansowych (embargo finansowych);
- ciągłe monitorowanie klientów o najwyższym ryzyku prania pieniędzy i finansowania terroryzmu, monitorowanie wniosków o dalsze dochodzenie w przypadku klientów, którzy potencjalnie narażają Spółkę na wysokie ryzyko prania pieniędzy, uruchamianie, w razie potrzeby, procesu oceny podejrzanych transakcji oraz procesu

sprawdzania klientów, którzy potencjalnie narażają Spółkę na wysokie ryzyko prania pieniędzy.

Szczegółowe zasady i obowiązki Spółki dotyczące tego procesu są szczegółowo opisane w dokumencie wewnętrznym

dokument „Wewnętrzne procedury przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu”.

5 - RAMY ORGANIZACYJNE I ORGANY KONTROLNE

Aby skutecznie zarządzać ryzykiem prania pieniędzy i finansowania terroryzmu oraz naruszenia Środków ograniczających, Spółka określiła funkcje organizacyjne, zasoby i procedury, które są spójne i proporcjonalne do rodzaju i wielkości prowadzonej działalności, złożoności organizacyjnej oraz charakterystyki operacyjnej.

Zapewnia się monitorowanie ryzyk związanych z praniem pieniędzy i finansowaniem terroryzmu:

- przez Dział ds. Przeciwdziałania Praniu Pieniędzy w Rox Pay S.r.l., którego odpowiedzialność jest przypisana Kierownikowi Działu AML, który podlega bezpośrednio Dyrektorowi Generalnemu.
- Przez Członka organu zarządzającego odpowiedzialnego za Przeciwdziałanie Praniu Pieniędzy, z odpowiedzialnością powierzoną Dyrektorowi Generalnemu, który jest głównym punktem kontaktowym pomiędzy Kierownikiem Jednostki ds. Przeciwdziałania Praniu Pieniędzy a Zarządem i zapewnia Zarządowi niezbędne informacje, aby w pełni zrozumieć znaczenie ryzyka prania pieniędzy, z którym boryka się Rox Pay S.r.l. jest odsłonięty.

Monitoring ryzyk związanych z naruszeniem Środków Ograniczających:

- zapewnia starszy pracownik odpowiedzialny za środki ograniczające, którego odpowiedzialność przypisana jest kierownikowi Departamentu AML, który nadzoruje adekwatność i skuteczność polityk, procedur wewnętrznych i kontroli związanych z zarządzaniem środkami ograniczającymi, sankcjami i embargiami. Starszy pracownik proponuje, we współpracy z odpowiednimi komórkami firmy, zmiany organizacyjne i proceduralne niezbędne i/lub właściwe w celu zapewnienia odpowiedniego monitorowania ryzyka naruszenia środków ograniczających, sankcji i embarga.

Zgodnie z obowiązującymi przepisami Spółka ustaliła swoją strukturę organizacyjną i ład korporacyjny tak, aby chronić interesy Spółki, zapewniając jednocześnie należyte i ostrożne zarządzanie oraz unikanie ryzyka – nawet niezamierzonego
- o jakimkolwiek bezpośrednim zaangażowaniu w pranie pieniędzy i/lub finansowanie terroryzmu.

W tym celu, zgodnie z przyjętym w Spółce Systemem Kontroli Wewnętrznej, Zarząd oraz Biegli Rewidenci angażują się w ograniczanie powyższych ryzyk poprzez jasno określone zadania i odpowiedzialności.

Ponadto w Spółce utworzono centralną komórkę do zarządzania wewnętrznym systemem zgłaszania naruszeń, której zadaniem jest nadzorowanie działań związanych z przyjmowaniem, analizowaniem i oceną zgłoszeń przekazywanych przez pracowników w ramach procedury Whistleblowing.

6 – REWIZJA I AKTUALIZACJA POLITYKI

Jednostka ds. przeciwdziałania praniu pieniędzy dokonuje przeglądu polityki co najmniej raz w roku, aktualizuje ją w razie potrzeby i przygotowuje tekst do zatwierdzenia przez Radę Dyrektorów na wniosek Dyrektora Generalnego.

Wszelkie zmiany w Polityce zatwierdzone przez Zarząd Rox Pay S.r.l. są następnie wdrażane w całej Spółce w drodze uchwały kadry kierowniczej wyższego szczebla, ujednolicając obowiązki, procesy i zasady wewnętrzne.