Informacje dotyczące zasad przeciwdziałania praniu pieniędzy (AML) oraz finansowaniu terroryzmu (CTF)

1. Informacje ogólne

Polityka przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (dalej: „Polityka") ma na celu zapobieganie i ograniczanie potencjalnych ryzyk związanych z możliwością zaangażowania Pilot Innovation (dalej: „Spółka") w jakiekolwiek działania o charakterze nielegalnym.

W celu zapewnienia zgodności zarówno z przepisami międzynarodowymi, jak i krajowymi, Spółka wdraża skuteczne procedury wewnętrzne oraz mechanizmy zapobiegające praniu pieniędzy, finansowaniu terroryzmu, handlowi narkotykami i ludźmi, proliferacji broni masowego rażenia, korupcji i przekupstwu, a także reagujące na wszelkie formy podejrzanej aktywności ze strony Użytkowników.

„Pranie pieniędzy (legalizacja środków pochodzących z przestępstwa)" należy rozumieć zgodnie z art. 299 Kodeksu karnego z dnia 6 czerwca 1997 r.
„Finansowanie terroryzmu" należy rozumieć zgodnie z art. 165a Kodeksu karnego z dnia 6 czerwca 1997 r.

Niniejsza Polityka nie powinna być interpretowana jako kompletny zbiór wszystkich polityk, procedur i środków kontrolnych stosowanych przez Spółkę w celu zapobiegania praniu pieniędzy, finansowaniu terroryzmu oraz innym działaniom niezgodnym z prawem.

2. Obowiązki Spółki

2.1 Instytucja obowiązana w Polsce

PILOT INNOVATION SP. Z O.O. jest instytucją obowiązaną w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2018 poz. 723 z późn. zm.), a także innych mających zastosowanie aktów prawnych.

Organ nadzorczy

Spółka podlega nadzorowi Generalnego Inspektora Informacji Finansowej (GIIF), który jest właściwym organem w Polsce odpowiedzialnym za monitorowanie i przeciwdziałanie przestępczości finansowej.

Obowiązki Spółki

Identyfikacja klienta oraz środki bezpieczeństwa finansowego (KYC/CDD):

- wdrożenie procedur „Know Your Customer" (KYC);
- ocena ryzyka klienta zgodnie z podejściem opartym na ryzyku (Risk-Based Approach

– RBA);
- stosowanie wzmożonych środków należytej staranności (Enhanced Due Diligence – EDD) wobec klientów podwyższonego ryzyka.

Obowiązki raportowe wobec GIIF:

- raportowanie transakcji o wartości równej lub wyższej niż 15 000 EUR;
- obowiązkowe raportowanie transakcji podejrzanych, mogących mieć związek z praniem pieniędzy lub finansowaniem terroryzmu;
- prowadzenie odpowiednich rejestrów i dokumentacji przez okres nie krótszy niż 5 lat.

Zgodność z międzynarodowymi standardami AML/CTF

Spółka zapewnia zgodność z międzynarodowymi standardami przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, w tym:

- Dyrektywą (UE) 2015/849 (IV Dyrektywa AML);
- Rozporządzeniem (UE) 2023/1113 Parlamentu Europejskiego i Rady w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmieniającym dyrektywę (UE) 2015/849 („Transfer Regulation”);
- Zaleceniami FATF (Financial Action Task Force) dotyczącymi przeciwdziałania przestępczości finansowej.

3. Obowiązki w zakresie należytej staranności wobec klienta (CDD)

Kompleksowa weryfikacja tożsamości klienta (Customer Due Diligence – CDD) stanowi obowiązkowy środek wynikający z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2023 poz. 1124). Spółka jest zobowiązana do gromadzenia, weryfikacji oraz aktualizacji informacji o klientach na wszystkich etapach współpracy.

W zależności od poziomu ryzyka przypisanego klientowi stosowane są różne poziomy CDD:

- Standard Due Diligence (SDD) – stosowane wobec klientów niskiego ryzyka;
- Enhanced Due Diligence (EDD) – stosowane w przypadku zidentyfikowania podwyższonego ryzyka i wymagające dodatkowych informacji.

3.1 Standard Due Diligence (SDD)

W przypadku klientów indywidualnych wymagane są:

- paszport lub dowód osobisty;
- potwierdzenie adresu zamieszkania (np. wyciąg bankowy, rachunek za media);
- weryfikacja biometryczna (liveness check) w przypadku weryfikacji zdalnej.

W przypadku klientów korporacyjnych wymagane są:

- dokumenty rejestrowe spółki;

- dokumenty identyfikacyjne beneficjenta rzeczywistego (UBO) oraz członków zarządu;
- potwierdzenie adresu spółki;
- odpis z Krajowego Rejestru Sądowego (KRS);
- potwierdzenie źródła środków;
- lista 5 największych partnerów biznesowych wraz z umowami;
- informacje o stronie internetowej spółki oraz potwierdzenie własności domeny.

3.2 Enhanced Due Diligence (EDD)

Spółka stosuje wzmożone środki należytej staranności w następujących przypadkach:

- gdy dane klienta budzą wątpliwości co do ich wiarygodności;
- gdy klient jest instytucją finansową z państwa trzeciego;
- gdy klient jest osobą zajmującą eksponowane stanowisko polityczne (PEP) lub bliskim współpracownikiem/członkiem rodziny;
- gdy klient zamieszkuje lub prowadzi działalność w jurysdykcji wysokiego ryzyka.

W takich przypadkach Spółka może:

- zażądać dodatkowych dokumentów weryfikujących tożsamość;
- zweryfikować źródło środków i majątku klienta;
- zwiększyć częstotliwość monitorowania transakcji;
- przeprowadzić pogłębioną analizę działalności gospodarczej klienta.

3.3 Weryfikacja źródła środków

Spółka jest zobowiązana do zapewnienia, że środki wykorzystywane przez klienta pochodzą z legalnego źródła. W tym celu mogą być wymagane:

- wyciągi bankowe;
- dokumenty potwierdzające dochody i inwestycje;
- dokumenty potwierdzające sprzedaż aktywów lub inne zgodne z prawem transakcje.

4. Osoby zajmujące eksponowane stanowiska polityczne (PEP)

Spółka ustala, czy klient lub jego beneficjent rzeczywisty jest osobą zajmującą eksponowane stanowisko polityczne (PEP), członkiem rodziny takiej osoby lub bliskim współpracownikiem. W przypadku zidentyfikowania klienta jako PEP automatycznie stosowane są wzmożone środki należytej staranności (EDD).

5. Bieżące monitorowanie i aktualizacja danych

Spółka wdraża systemy monitorowania transakcji zgodnie z ustawą z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2018 poz. 723). Celem monitorowania jest wykrywanie i zapobieganie podejrzanym operacjom finansowym, które mogą być powiązane z praniem pieniędzy (AML) lub finansowaniem terroryzmu (CTF).

5.1 Procedury monitorowania

Monitorowanie transakcji ma charakter ciągły i obejmuje:

- analizę wzorców aktywności transakcyjnej klienta;
- automatyczne przesiewanie transakcji z wykorzystaniem systemów analizy danych;
- manualny przegląd transakcji spełniających kryteria podejrzane;
- screening transakcji względem list sankcyjnych oraz list jurysdykcji wysokiego ryzyka;
- bieżącą ocenę ryzyka klienta oraz jego aktywności transakcyjnej.

Spółka stosuje podejście oparte na ryzyku (Risk-Based Approach – RBA), w ramach którego klienci są klasyfikowani do różnych poziomów ryzyka (niski, średni, wysoki oraz niedopuszczalny), a ich transakcje są analizowane z odpowiednim poziomem szczegółowości zależnym od przypisanego poziomu ryzyka.

5.2 Identyfikacja transakcji podejrzanych

Spółka jest zobowiązana do prowadzenia rejestru transakcji podejrzanych oraz ich raportowania do Generalnego Inspektora Informacji Finansowej (GIIF).

5.3 Ocena ryzyka

Spółka przeprowadza wewnętrzną ocenę ryzyka co najmniej raz w roku, uwzględniając:

- czynniki geograficzne (kraje o wysokim poziomie korupcji lub słabym nadzorze finansowym);
- typ klienta (np. PEP, instytucje finansowe);
- stosowane instrumenty płatnicze (gotówka, płatności anonimowe);
- charakter działalności klienta (spółki działające w sektorach podwyższonego ryzyka AML/CTF).

Na podstawie tej oceny opracowywane są działania korygujące mające na celu minimalizację ryzyk oraz usprawnienie procesów monitorowania.

5.4 Wykorzystanie technologii w monitorowaniu

Spółka wykorzystuje zaawansowane technologie do analizy danych transakcyjnych, w tym:

- zautomatyzowane systemy monitorowania wykorzystujące algorytmy uczenia maszynowego;
- narzędzia analityki blockchain do śledzenia operacji kryptowalutowych;
- bazy danych list sankcyjnych, osób zajmujących eksponowane stanowiska polityczne (PEP) oraz negatywnych informacji medialnych;
- narzędzia analizy zachowań klientów.

Technologie te zwiększają skuteczność wykrywania podejrzanych transakcji oraz ograniczają liczbę fałszywych alarmów.

6. Osoba odpowiedzialna (RO)

Osoba odpowiedzialna (Responsible Officer – RO) w Spółce nadzoruje zgodność z Polityką AML/CTF oraz zapewnia przestrzeganie wymogów prawnych Rzeczypospolitej Polskiej i standardów międzynarodowych.

Do kluczowych obowiązków należą:

- nadzorowanie stosowania procedur AML/CTF oraz monitorowania transakcji;
- współpraca z GIIF oraz składanie raportów o transakcjach podejrzanych;
- opracowywanie i aktualizacja wewnętrznych procedur AML/CTF;
- szkolenie pracowników oraz przeprowadzanie audytów wewnętrznych;
- ocena ryzyka oraz wdrażanie działań naprawczych.

Osoba odpowiedzialna pełni funkcję głównego punktu kontaktowego z organami nadzorczymi oraz zapewnia skuteczność wewnętrznego systemu kontroli Spółki.

7. Odmowa świadczenia usług

Klienci niedopuszczalni

Spółka nie nawiązuje relacji biznesowych z klientami, którzy:

- odmawiają przekazania wymaganych informacji i dokumentów w celu weryfikacji;
- są tzw. „Shell Banks” (bankami bez fizycznej obecności w regulowanej jurysdykcji);
- zamieszkują lub prowadzą działalność w krajach objętych sankcjami międzynarodowymi lub zakazanych zgodnie z wewnętrzną polityką Spółki;
- wzbudzają uzasadnione podejrzenia potencjalnego udziału w praniu pieniędzy, finansowaniu terroryzmu lub innych działaniach niezgodnych z prawem.

Kraje i terytoria zabronione

Spółka nie nawiązuje relacji biznesowych z klientami pochodzącymi z następujących krajów i terytoriów:
Afganistan; Samoa Amerykańskie; Białoruś; Burundi; Kambodża; Kamerun; Republika Środkowoafrykańska; Czad; Kuba; Koreańska Republika Ludowo-Demokratyczna (Korea Północna); Demokratyczna Republika Konga; Erytrea; Etiopia; Haiti; Iran; Irak; Kazachstan; Kirgistan; Liban; Libia; Mali; Mozambik; Mjanma (Birma); Nikaragua; Pakistan; Palestyna; Rosja; Senegal; Sierra Leone; Somalia; Sudan Południowy; Sudan; Syria; Tadżykistan; Naddniestrze; Turkmenistan; Uganda; Ukraina – terytoria niekontrolowane przez rząd (obwody: Krym, Donieck, Chersoń, Ługańsk, Zaporoże); Uzbekistan; Wenezuela; Jemen; Zimbabwe.

Klienci lub beneficjenci rzeczywiści powiązani z tymi krajami są automatycznie klasyfikowani jako „Odrzuceni / Zabronieni”.

Państwa trzecie wysokiego ryzyka

Następujące jurysdykcje są klasyfikowane jako wysokiego ryzyka zgodnie z Rozporządzeniem Delegowanym Komisji (UE) 2024/594, publicznymi oświadczeniami FATF oraz ustawą AML (art. 2 ust. 2 pkt 13). Klienci lub kontrahenci powiązani z tymi krajami mogą zostać zaakceptowani wyłącznie po zastosowaniu wzmożonych środków należytej staranności (EDD), uzyskaniu zgody MLRO oraz udokumentowanej weryfikacji źródła środków i majątku (SoF/SoW).

Albania; Barbados; Burkina Faso; Kamerun; Kajmany; Gibraltar; Jamajka; Jordania; Nigeria; Panama; Filipiny; Republika Południowej Afryki; Tanzania; Trynidad i Tobago; Uganda; Zjednoczone Emiraty Arabskie (ZEA); Wietnam; oraz każda inna jurysdykcja wskazana jako wysokiego ryzyka przez FATF lub Komisję Europejską w momencie onboardingu lub przeglądu okresowego.

Kraje średniego ryzyka

Jurysdykcje o częściowo skutecznym nadzorze AML/CFT, podwyższonym poziomie korupcji lub wątpliwościach dotyczących przejrzystości podatkowej, lecz zasadniczo współpracujące. Zaleca się stosowanie EDD dla transakcji o dużym wolumenie lub ekspozycji na kryptoaktywa.

Lista krajów średniego ryzyka:
Andora; Angola; Argentyna; Armenia; Azerbejdżan; Bahamy; Bahrajn; Bangladesz; Bośnia i Hercegowina; Botswana; Brazylia; Brunei; Chile; Chiny (ChRL); Kolumbia; Kostaryka; Chorwacja; Czechy; Dominikana; Ekwador; Egipt; Salwador; Gruzja; Ghana; Grecja; Gwatemala; Honduras; Hongkong SAR; Węgry; Indie; Indonezja; Izrael; Kenia; Kuwejt; Laos; Łotwa; Litwa; Malezja; Malediwy; Malta; Mauritius; Meksyk; Mołdawia; Mongolia; Czarnogóra; Maroko; Namibia; Nepal; Macedonia Północna; Oman; Papua-Nowa Gwinea; Paragwaj; Peru; Polska; Katar; Rumunia; Arabia Saudyjska; Serbia; Singapur; Słowacja; Słowenia; Sri Lanka; Surinam; Tajwan; Tajlandia; Tunezja; Turcja; Ukraina (terytorium kontrolowane przez rząd); Urugwaj.

Kraje niskiego ryzyka

Kraje posiadające silne systemy AML/CFT, wysoki poziom zarządzania, niską percepcję korupcji oraz zgodność z EU/OECD/FATF. W przypadkach dopuszczonych prawnie może być stosowane SDD.

Lista krajów niskiego ryzyka:
Austria; Australia; Belgia; Bułgaria; Kanada; Chorwacja; Cypr; Dania; Estonia; Finlandia; Francja; Niemcy; Islandia; Irlandia; Włochy; Japonia; Liechtenstein; Luksemburg; Monako; Niderlandy; Nowa Zelandia; Norwegia; Portugalia; San Marino; Korea Południowa; Hiszpania; Szwecja; Szwajcaria; Wielka Brytania.

Działalności zabronione

Spółka nie nawiązuje ani nie utrzymuje relacji biznesowych z osobami lub podmiotami zaangażowanymi w:

- nielegalny hazard lub działalność bukmacherską bez licencji;
- handel bronią lub działalność związaną z obronnością (w tym pośrednictwo, towary podwójnego zastosowania, amunicja, broń chemiczna lub biologiczna, amunicja kasetowa);
- narkotyki, prekursory lub nielegalne produkty farmaceutyczne;
- handel ludźmi, współczesne niewolnictwo lub wykorzystywanie dzieci;
- banki typu shell lub instytucje bez fizycznej obecności i skutecznego nadzoru;
- treści dla dorosłych (pornografia, usługi webcam, streaming dla dorosłych, treści z udziałem dzieci lub zwierząt, materiały związane z przemocą lub gwałtem);
- naruszenia własności intelektualnej lub prawa autorskiego, towary podrobione;
- nielicencjonowane instytucje finansowe, przekazy pieniężne lub dostawców usług w zakresie aktywów wirtualnych;
- kryptowaluty prywatności lub anonimowe (np. Monero, Zcash, Dash);
- schematy Ponziego, piramidy finansowe lub wysokodochodowe schematy inwestycyjne;
- opcje binarne, nieregulowane platformy tradingowe lub emisje tokenów ICO/ITO;
- klientów emitujących lub posiadających akcje na okaziciela lub inne instrumenty własności o charakterze anonimowym.

Akcje na okaziciela oznaczają zbywalne instrumenty reprezentujące własność w podmiocie prawnym, gdzie kontrola należy wyłącznie do fizycznego posiadacza i nie może zostać zweryfikowana przez Spółkę. Akcje imienne lub zdematerializowane są dopuszczalne.

Spółka zastrzega sobie prawo do odrzucenia, zawieszenia lub zakończenia relacji biznesowej lub transakcji, które wykraczają poza apetyt na ryzyko Spółki lub stanowią niemożliwe do zarządzania ryzyko AML/CFT.

Wytyczne raportowania AMLRO (EBA/GL/2022/05)

Na podstawie Wytycznych EBA EBA/GL/2022/05 z dnia 14 czerwca 2022 r. oraz Stanowiska KNF dotyczącego AMLRO z dnia 1 grudnia 2022 r., Spółka wskazuje, że w zakresie okresowych informacji zarządczych oraz rocznego raportu działalności sporządzanego przez wyznaczonego pracownika (AMLRO), wymagane są w szczególności następujące dane i informacje:

- ryzyka ML/TF oraz zgodność Spółki z przepisami AML/CFT;
- współpraca Spółki z właściwymi organami państwowymi i powiązana korespondencja;
- ustalenia i działania organów nadzoru i jednostek analityki finansowej skierowane do Spółki;
- poważne problemy i naruszenia AML/CFT oraz działania naprawcze;
- podsumowanie oceny ryzyka ML/TF w skali całej instytucji;
- zmiany metod oceny ryzyka klienta;
- klasyfikacja klientów według kategorii ryzyka;
- liczba akt klientów według kategorii ryzyka;
- stosowanie środków należytej staranności wobec klientów;
- statystyki dotyczące transakcji nietypowych i podejrzanych;

- relacje odrzucone lub zakończone z powodu braku możliwości zastosowania CDD;
- wnioski od FIU, sądów lub organów ścigania;
- opis struktury organizacyjnej AML/CFT;
- opis zasobów ludzkich i technicznych AML/CFT;
- mechanizmy ograniczania ryzyka;
- działania monitorujące compliance;
- realizacja obowiązków szkoleniowych;
- planowane działania AMLRO;
- ustalenia kontroli wewnętrznej;
- zmiany otoczenia prawnego i ich wpływ na proces AML/CFT.

Osoby zajmujące eksponowane stanowiska polityczne (PEP)

Krajowi PEP (Polska)

Osoby pełniące lub które pełniły funkcje publiczne na szczeblu krajowym, w tym:

- Prezydent lub Premier
- Ministrowie, wiceministrowie, sekretarze stanu
- Posłowie i senatorowie
- Członkowie organów partii politycznych
- Członkowie Sądu Najwyższego lub Trybunału Konstytucyjnego
- Członkowie NIK lub Rady NBP
- Ambasadorowie
- Wyżsi oficerowie sił zbrojnych
- Członkowie organów spółek Skarbu Państwa
- Dyrektorzy organizacji międzynarodowych

Uwaga:
Funkcje lokalne (np. burmistrzowie, radni gminni) nie są uznawane za PEP, o ile nie mają wpływu na decyzje krajowe.

Zagraniczni PEP

Osoby pełniące funkcje publiczne w państwie obcym, w tym:

- głowy państw i rządów
- ministrowie
- członkowie parlamentów
- członkowie sądów najwyższych
- członkowie banków centralnych
- ambasadorowie
- kadra zarządzająca spółek państwowych
- kierownictwo organizacji międzynarodowych

PEP organizacji międzynarodowych

Osoby zajmujące wysokie stanowiska kierownicze w organizacjach takich jak:
ONZ, MFW, Bank Światowy, UE, NATO, OBWE.

Członkowie rodzin PEP

Za powiązane z PEP uznaje się:

- małżonka lub partnera
- dzieci i ich partnerów
- rodziców

Bliscy współpracownicy PEP

Osoby:

- posiadające wspólną własność z PEP
- utrzymujące bliskie relacje biznesowe z PEP
- będące beneficjentami podmiotów utworzonych dla PEP

Klauzula wyłączenia

Nie uznaje się za PEP:

- radnych lokalnych
- urzędników bez kompetencji decyzyjnych
- osób pełniących funkcje techniczne lub doradcze

Akceptowane dokumenty identyfikacyjne

1. Cel i zakres

Niniejszy załącznik określa listę dokumentów identyfikacyjnych akceptowanych przez Pilot Innovation Sp. z o.o. („Spółka”) na potrzeby procedur CDD oraz KYC zgodnie z:

- ustawą AML z 1 marca 2018 r.;
- Dyrektywą UE 2015/849;
- zaleceniami FATF;
- Wytycznymi EBA EBA/GL/2022/05.

Lista dotyczy onboardingu i bieżącej weryfikacji osób fizycznych, podmiotów prawnych oraz beneficjentów rzeczywistych, identyfikowanych bezpośrednio przez Spółkę lub poprzez system KYCAid.

2. Zasady ogólne

1. Dokumenty muszą być ważne, czytelne i wydane przez właściwy organ publiczny.
2. Dokumenty muszą zawierać co najmniej:
- imię i nazwisko / nazwę
- datę urodzenia lub rejestracji
- obywatelstwo lub jurysdykcję
- numer identyfikacyjny
- zdjęcie (dla osób fizycznych)
- datę wydania i ważności (jeśli dotyczy)
3. Kopie dokumentów muszą być kolorowe i dobrej jakości.
4. Dokumenty w języku innym niż polski lub angielski muszą posiadać tłumaczenie przysięgłe.
5. Dokumenty wydane przez jurysdykcje zabronione lub wysokiego ryzyka nie są akceptowane.
6. Spółka zastrzega prawo do żądania dodatkowych dokumentów w ramach EDD.

8. Współpraca i wymiana informacji

Spółka aktywnie współpracuje z organami regulacyjnymi i organami ścigania w celu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. PayPilot przekazuje wymagane informacje na podstawie oficjalnych wniosków zgodnie z obowiązującymi przepisami prawa oraz zobowiązaniami międzynarodowymi.

W sprawach dotyczących współpracy i wymiany informacji ze Spółką można kontaktować się pod adresem:
aml@paypilot.org