Informationen zu den Grundsätzen zur Bekämpfung von Geldwäsche (AML) und Terrorismusfinanzierung (CTF)

1. Allgemeine Informationen

Die Richtlinie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (nachfolgend die „Richtlinie“) hat zum Ziel, potenzielle Risiken zu verhindern und zu mindern, dass Pilot Innovation (nachfolgend das „Unternehmen“) in illegale Aktivitäten verwickelt wird.

Um sowohl internationalen als auch nationalen Vorschriften zu entsprechen, implementiert das Unternehmen wirksame interne Verfahren und Mechanismen zur Verhinderung von Geldwäsche, Terrorismusfinanzierung, Drogen- und Menschenhandel, der Verbreitung von Massenvernichtungswaffen, Korruption und Bestechung sowie zur Reaktion auf jede Form verdächtiger Aktivitäten seiner Nutzer.

„Geldwäsche (Legalisierung von Erträgen aus Straftaten)“ ist im Sinne von Artikel 299 des polnischen Strafgesetzbuches vom 6. Juni 1997 zu verstehen.
„Terrorismusfinanzierung“ ist im Sinne von Artikel 165a des polnischen Strafgesetzbuches vom 6. Juni 1997 zu verstehen.

Diese Richtlinie ist nicht als umfassende Sammlung aller Richtlinien, Verfahren und Kontrollmaßnahmen zu verstehen, die das Unternehmen zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und anderen rechtswidrigen Aktivitäten anwendet.

2. Pflichten des Unternehmens

2.1 Verpflichtetes Unternehmen in Polen

PILOT INNOVATION SP. Z O.O. ist ein verpflichtetes Unternehmen gemäß dem polnischen Gesetz vom 1. März 2018 zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (Gesetzblatt 2018, Position 723, in der jeweils gültigen Fassung) sowie gemäß anderen anwendbaren Rechtsvorschriften.

Aufsichtsbehörde

Das Unternehmen unterliegt der Aufsicht des Generalinspektors für Finanzinformationen (GIIF), der in Polen die zuständige Behörde für die Überwachung und Verhinderung von Finanzkriminalität ist.

Pflichten des Unternehmens

Kundenidentifizierung und finanzielle Sicherheitsmaßnahmen (KYC/CDD):

- Umsetzung von „Know Your Customer“-Verfahren (KYC);
- Risikobewertung der Kunden gemäß dem risikobasierten Ansatz (Risk-Based Approach – RBA);
- Anwendung verstärkter Sorgfaltspflichten (Enhanced Due Diligence – EDD) für Kunden mit höherem Risiko.

Meldepflichten gegenüber dem GIIF:

- Meldung von Transaktionen mit einem Wert von 15.000 EUR oder mehr;
- Verpflichtende Meldung verdächtiger Transaktionen, die potenziell mit Geldwäsche oder Terrorismusfinanzierung in Zusammenhang stehen;
- Ordnungsgemäße Aufbewahrung von Aufzeichnungen und Dokumentation für mindestens 5 Jahre.

Einhaltung internationaler AML/CTF-Standards

Das Unternehmen stellt die Einhaltung internationaler Standards zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung sicher, einschließlich:

- Richtlinie (EU) 2015/849 (4. AML-Richtlinie);
- Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates über Angaben, die Geldtransfers und bestimmte Kryptowerte begleiten, sowie zur Änderung der Richtlinie (EU) 2015/849 („Transfer Regulation“);
- Empfehlungen der FATF (Financial Action Task Force) zur Bekämpfung von Finanzkriminalität.

3. Sorgfaltspflichten gegenüber Kunden (CDD)

Die umfassende Überprüfung der Kundenidentität (Customer Due Diligence – CDD) ist eine verpflichtende Maßnahme gemäß dem polnischen Gesetz vom 1. März 2018 zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (Gesetzblatt 2023, Position 1124). Das Unternehmen ist verpflichtet, Kundeninformationen in allen Phasen der Geschäftsbeziehung zu erheben, zu überprüfen und zu aktualisieren.

Abhängig vom bewerteten Risikoniveau des Kunden werden unterschiedliche CDD-Stufen angewendet:

- Standard Due Diligence (SDD) – angewendet bei Kunden mit geringem Risiko;
- Enhanced Due Diligence (EDD) – angewendet, wenn ein höheres Risiko festgestellt wird und zusätzliche Daten erforderlich sind.

3.1 Standard Due Diligence (SDD)

Für natürliche Personen sind folgende Dokumente und Prüfungen erforderlich:

- Reisepass oder nationaler Personalausweis;

- Nachweis der Wohnadresse (z. B. Kontoauszug, Versorgungsrechnung);
- Biometrische Verifizierung (Liveness-Check) bei Fernverifizierung.

Für juristische Personen sind folgende Unterlagen erforderlich:

- Gründungsunterlagen;
- Identifikationsdokumente des wirtschaftlich Berechtigten (UBO) und der Mitglieder der Geschäftsleitung;
- Nachweis der Firmenadresse;
- Auszug aus dem Nationalen Gerichtsregister (KRS);
- Nachweis der Herkunft der Gelder;
- Liste der fünf wichtigsten Geschäftspartner sowie entsprechende Verträge;
- Informationen über die Website des Unternehmens und Nachweis des Domain-Eigentums.

3.2 Enhanced Due Diligence (EDD)

Das Unternehmen wendet EDD-Maßnahmen in folgenden Fällen an:

- wenn die Kundendaten Zweifel an ihrer Glaubwürdigkeit aufwerfen;
- wenn der Kunde ein Finanzinstitut aus einem Drittland ist;
- wenn der Kunde eine politisch exponierte Person (PEP) oder ein enger Familienangehöriger bzw. nahestehende Person ist;
- wenn der Kunde in einer Hochrisiko-Jurisdiktion ansässig ist oder von dort aus tätig wird.

In solchen Fällen kann das Unternehmen:

- zusätzliche Identitätsprüfungsdokumente anfordern;
- die Herkunft der Gelder und des Vermögens des Kunden überprüfen;
- die Häufigkeit der Transaktionsüberwachung erhöhen;
- eine vertiefte Analyse der Geschäftstätigkeit des Kunden durchführen.

3.3 Überprüfung der Herkunft der Gelder

Das Unternehmen ist verpflichtet sicherzustellen, dass die vom Kunden verwendeten Gelder aus einer legitimen Quelle stammen. Zu diesem Zweck können folgende Unterlagen angefordert werden:

- Kontoauszüge;
- Dokumente zur Bestätigung von Einkommen und Investitionen;
- Nachweise über den Verkauf von Vermögenswerten oder andere rechtmäßige Transaktionen.

4. Politisch exponierte Personen (PEP)

Das Unternehmen stellt fest, ob ein Kunde oder dessen wirtschaftlich Berechtigter eine politisch exponierte Person (PEP), ein Familienmitglied oder ein nahestehender

Geschäftspartner ist. Wird ein Kunde als PEP identifiziert, werden automatisch verstärkte Sorgfaltspflichten (Enhanced Due Diligence – EDD) angewendet.

5. Laufende Überwachung und Datenaktualisierung

Das Unternehmen implementiert Systeme zur Transaktionsüberwachung gemäß dem polnischen Gesetz vom 1. März 2018 zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (Gesetzblatt 2018, Position 723). Ziel der Überwachung ist es, verdächtige Finanzoperationen zu erkennen und zu verhindern, die mit Geldwäsche (AML) oder Terrorismusfinanzierung (CTF) in Verbindung stehen können.

5.1 Überwachungsverfahren

Die Transaktionsüberwachung erfolgt kontinuierlich und umfasst:

- Analyse der Muster der Transaktionsaktivität des Kunden;
- automatisiertes Transaktions-Screening unter Verwendung von Datenanalysesystemen;
- manuelle Überprüfung von Transaktionen, die verdächtigen Kriterien entsprechen;
- Screening von Transaktionen gegen Sanktionslisten und Listen von Hochrisiko-Jurisdiktionen;
- laufende Risikobewertung des Kunden und seiner Transaktionsaktivitäten.

Das Unternehmen wendet einen risikobasierten Ansatz (Risk-Based Approach – RBA) an, bei dem Kunden in verschiedene Risikostufen (niedrig, mittel, hoch und unzulässig) eingestuft werden. Ihre Transaktionen werden abhängig von der jeweiligen Risikoklassifizierung mit angemessener Detailtiefe überprüft.

5.2 Identifizierung verdächtiger Transaktionen

Das Unternehmen ist verpflichtet, ein Register verdächtiger Transaktionen zu führen und diese dem Generalinspektor für Finanzinformationen (GIIF) zu melden.

5.3 Risikobewertung

Das Unternehmen führt jährlich eine interne Risikobewertung durch und berücksichtigt dabei:

- geografische Faktoren (Länder mit hohem Korruptionsniveau oder schwacher Finanzaufsicht);
- Kundentyp (PEP, Finanzinstitute);
- verwendete Zahlungsinstrumente (Bargeld, anonyme Zahlungen);
- Art der Geschäftstätigkeit des Kunden (Unternehmen in Sektoren mit erhöhtem AML/CTF-Risiko).

Auf Grundlage dieser Bewertung werden Korrekturmaßnahmen entwickelt, um Risiken zu minimieren und die Überwachungsprozesse zu verbessern.

5.4 Einsatz von Technologie bei der Überwachung

Das Unternehmen verwendet fortschrittliche Technologien zur Analyse von Transaktionsdaten, einschließlich:

- automatisierter Überwachungssysteme mit Machine-Learning-Algorithmen;
- Blockchain-Analysen zur Nachverfolgung von Kryptowährungstransaktionen;
- Datenbanken mit Sanktionslisten, politisch exponierten Personen (PEP) und negativen Medienberichten;
- Tools zur Analyse des Kundenverhaltens.

Diese Technologien erhöhen die Genauigkeit bei der Erkennung verdächtiger Transaktionen und reduzieren die Anzahl von Fehlalarmen.

6. Verantwortlicher Beauftragter (RO)

Der Verantwortliche Beauftragte (Responsible Officer – RO) des Unternehmens überwacht die Einhaltung der AML/CTF-Richtlinie und stellt die Einhaltung der gesetzlichen Anforderungen der Republik Polen sowie internationaler Standards sicher.

Zu den wichtigsten Aufgaben gehören:

- Überwachung der Anwendung von AML/CTF-Verfahren und der Transaktionsüberwachung;
- Zusammenarbeit mit dem GIIF und Einreichung von Meldungen über verdächtige Transaktionen;
- Entwicklung und Aktualisierung interner AML/CTF-Verfahren;
- Schulung der Mitarbeiter und Durchführung interner Audits;
- Bewertung von Risiken und Umsetzung von Korrekturmaßnahmen.

Der Verantwortliche Beauftragte fungiert als Hauptansprechpartner für Aufsichtsbehörden und stellt die Wirksamkeit des internen Kontrollsystems des Unternehmens sicher.

7. Ablehnung von Dienstleistungen

Unzulässige Kunden

Das Unternehmen geht keine Geschäftsbeziehungen mit Kunden ein, die:

- sich weigern, die erforderlichen Informationen und Dokumente zur Verifizierung bereitzustellen;
- „Shell Banks“ sind (Banken ohne physische Präsenz in einer regulierten Jurisdiktion);

- in Ländern ansässig sind oder dort tätig sind, die internationalen Sanktionen unterliegen oder durch die interne Richtlinie des Unternehmens verboten sind;
- begründete Verdachtsmomente hinsichtlich einer möglichen Beteiligung an Geldwäsche, Terrorismusfinanzierung oder anderen illegalen Aktivitäten aufwerfen.

Verbotene Länder und Gebiete

Das Unternehmen nimmt keine Kunden aus den folgenden Ländern und Gebieten auf: Afghanistan; Amerikanisch-Samoa; Belarus; Burundi; Kambodscha; Kamerun; Zentralafrikanische Republik; Tschad; Kuba; Demokratische Volksrepublik Korea (Nordkorea); Demokratische Republik Kongo; Eritrea; Äthiopien; Haiti; Iran; Irak; Kasachstan; Kirgisistan; Libanon; Libyen; Mali; Mosambik; Myanmar (Birma); Nicaragua; Pakistan; Palästina; Russland; Senegal; Sierra Leone; Somalia; Südsudan; Sudan; Syrien; Tadschikistan; Transnistrien; Turkmenistan; Uganda; Ukraine – nicht von der Regierung kontrollierte Gebiete (Krim, Donezk, Cherson, Luhansk, Saporischschja); Usbekistan; Venezuela; Jemen; Simbabwe.

Kunden oder wirtschaftlich Berechtigte, die mit diesen Ländern verbunden sind, werden automatisch als „Abgelehnt / Verboten“ eingestuft.

Hochrisiko-Drittländer

Die folgenden Jurisdiktionen werden gemäß der Delegierten Verordnung (EU) 2024/594, den öffentlichen Erklärungen der FATF sowie dem polnischen AML-Gesetz (Art. 2 (2)(13)) als Hochrisikoländer eingestuft. Kunden oder Gegenparteien mit Bezug zu diesen Ländern können nur nach Anwendung verstärkter Sorgfaltspflichten (EDD), Genehmigung durch den MLRO sowie dokumentierter Prüfung der Herkunft der Gelder und Vermögenswerte (SoF/SoW) akzeptiert werden.

Albanien; Barbados; Burkina Faso; Kamerun; Cayman Islands; Gibraltar; Jamaika; Jordanien; Nigeria; Panama; Philippinen; Südafrika; Tansania; Trinidad und Tobago; Uganda; Vereinigte Arabische Emirate (VAE); Vietnam; sowie jede andere Jurisdiktion, die zum Zeitpunkt des Onboardings oder der regelmäßigen Überprüfung von der FATF oder der Europäischen Kommission als Hochrisiko eingestuft wird.

Länder mit mittlerem Risiko

Jurisdiktionen mit teilweise wirksamer AML/CFT-Aufsicht, erhöhtem Korruptionsniveau oder Bedenken hinsichtlich der steuerlichen Transparenz, jedoch grundsätzlich kooperativen Rahmenbedingungen. EDD wird für Transaktionen mit hohem Volumen oder Krypto-Exposition empfohlen.

Liste der Länder mit mittlerem Risiko:
Andorra; Angola; Argentinien; Armenien; Aserbaidschan; Bahamas; Bahrain; Bangladesch; Bosnien und Herzegowina; Botswana; Brasilien; Brunei; Chile; China (VR China);

Kolumbien; Costa Rica; Kroatien; Tschechische Republik; Dominikanische Republik; Ecuador; Ägypten; El Salvador; Georgien; Ghana; Griechenland; Guatemala; Honduras; Hongkong SAR; Ungarn; Indien; Indonesien; Israel; Kenia; Kuwait; Laos; Lettland; Litauen; Malaysia; Malediven; Malta; Mauritius; Mexiko; Moldau; Mongolei; Montenegro; Marokko; Namibia; Nepal; Nordmazedonien; Oman; Papua-Neuguinea; Paraguay; Peru; Polen; Katar; Rumänien; Saudi-Arabien; Serbien; Singapur; Slowakei; Slowenien; Sri Lanka; Suriname; Taiwan; Thailand; Tunesien; Türkei; Ukraine (regierungskontrolliertes Gebiet); Uruguay.

Länder mit niedrigem Risiko

Länder mit robusten AML/CFT-Regimen, starker Governance, geringer Korruptionswahrnehmung und vollständiger Einhaltung der EU/OECD/FATF-Standards. SDD kann angewendet werden, sofern rechtlich zulässig.

Liste der Länder mit niedrigem Risiko:
Österreich; Australien; Belgien; Bulgarien; Kanada; Kroatien; Zypern; Dänemark; Estland; Finnland; Frankreich; Deutschland; Island; Irland; Italien; Japan; Liechtenstein; Luxemburg; Monaco; Niederlande; Neuseeland; Norwegen; Portugal; San Marino; Südkorea; Spanien; Schweden; Schweiz; Vereinigtes Königreich.

Verbotene Tätigkeiten

Das Unternehmen wird wissentlich keine Geschäftsbeziehungen mit Personen oder Unternehmen eingehen oder aufrechterhalten, die an folgenden Aktivitäten beteiligt sind oder mit diesen in Verbindung stehen:

- illegales Glücksspiel oder nicht lizenzierte Wettaktivitäten;
- Waffenhandel oder verteidigungsbezogene Tätigkeiten (einschließlich Vermittler, Dual-Use-Güter, Munition, chemische oder biologische Waffen, Streumunition);
- Betäubungsmittel, Vorläuferstoffe oder illegale Arzneimittel;
- Menschenhandel, moderne Sklaverei oder Ausbeutung von Kindern;
- Shell-Banken oder Institute ohne physische Präsenz oder wirksame Aufsicht;
- Erwachseneninhalte (Pornografie, Webcam-Dienste, Live-Streaming für Erwachsene, Inhalte mit Minderjährigen oder Bestialität, Gewalt- oder Vergewaltigungsinhalte);
- Verletzung von geistigem Eigentum oder Urheberrechten, gefälschte Waren;
- nicht lizenzierte Finanzinstitute, Geldübermittler oder Anbieter virtueller Vermögenswerte;
- Privacy-Coins oder anonymitätsverstärkte Kryptowährungen (z. B. Monero, Zcash, Dash);
- Ponzi-Systeme, Pyramidensysteme oder Hochrendite-Investitionsprogramme;
- binäre Optionen, nicht regulierte Handelsplattformen oder ICO/ITO-Tokenplatzierungen;
- Kunden, die Inhaberaktien oder vergleichbare nicht nachverfolgbare Eigentumsinstrumente ausgeben oder halten.

Inhaberaktien sind übertragbare Instrumente, die Eigentum an einer juristischen Person repräsentieren, wobei die Kontrolle ausschließlich beim physischen Inhaber liegt und vom Unternehmen nicht überprüft werden kann. Namensaktien oder dematerialisierte Aktien sind zulässig.

Das Unternehmen behält sich das Recht vor, jede Geschäftsbeziehung oder Transaktion abzulehnen, auszusetzen oder zu beenden, die außerhalb seiner Risikobereitschaft liegt oder ein nicht beherrschbares AML/CFT-Risiko darstellt.

EBA-Leitlinien / AMLRO-Berichterstattung

Auf Grundlage der EBA-Leitlinien EBA/GL/2022/05 vom 14. Juni 2022 sowie der KNF-Position zum AMLRO vom 1. Dezember 2022 gibt das Unternehmen an, dass im Rahmen der erforderlichen regelmäßigen (oder ad hoc) Managementinformationen sowie des jährlichen Tätigkeitsberichts des benannten Mitarbeiters (AMLRO) insbesondere folgende Daten und Informationen erforderlich sind:

- ML/TF-Risiken und Einhaltung der AML/CFT-Vorschriften;
- Zusammenarbeit mit zuständigen Behörden und entsprechende Korrespondenz;
- Feststellungen und Maßnahmen der Finanzaufsichts- und FIU-Behörden;
- wesentliche Probleme und Verstöße im AML/CFT-Bereich sowie Abhilfemaßnahmen;
- Zusammenfassung der institutsweiten ML/TF-Risikobewertung;
- Änderungen der Methode zur Bewertung des individuellen Kundenrisikoprofils;
- Klassifizierung der Kunden nach Risikokategorien;
- Anzahl der Kundenakten nach Risikokategorie;
- Anwendung von Sorgfaltspflichten gegenüber Kunden;
- Statistiken zu ungewöhnlichen oder verdächtigen Transaktionen;
- abgelehnte oder beendete Geschäftsbeziehungen;
- Anfragen von FIU, Gerichten oder Strafverfolgungsbehörden;
- Beschreibung der AML/CFT-Organisationsstruktur;
- personelle und technische Ressourcen der AML/CFT-Funktion;
- Risikominderungsmechanismen und Verfahren;
- Compliance-Monitoring-Aktivitäten;
- Schulungsmaßnahmen;
- geplante Aktivitäten des AMLRO;
- Feststellungen der internen Kontrolle;
- Änderungen des regulatorischen Umfelds und deren Auswirkungen auf AML/CFT.

Politisch exponierte Personen (PEP)

Nationale PEP (Polen / lokale Jurisdiktion)

Personen mit bedeutenden öffentlichen Funktionen:

- Staats- oder Regierungschef
- Minister, stellvertretende Minister, Staatssekretäre
- Parlamentsmitglieder
- Mitglieder politischer Parteigremien
- Mitglieder des Obersten Gerichts oder Verfassungsgerichts
- Mitglieder des Rechnungshofs oder der Nationalbank Polens
- Botschafter
- hochrangige Militärangehörige
- Leitungsorgane staatlicher Unternehmen
- Führungskräfte internationaler Organisationen

Hinweis: lokale Funktionen gelten nicht als PEP, außer bei nationalem Einfluss.

Ausländische PEP

- Staats- oder Regierungschefs
- Minister
- Parlamentsmitglieder
- Mitglieder höchster Gerichte
- Zentralbankmitglieder
- Botschafter
- Führungskräfte staatlicher Unternehmen
- Führungskräfte internationaler Organisationen

PEP internationaler Organisationen

UNO, IWF, Weltbank, EU, NATO, OSZE usw.

Familienmitglieder von PEP

- Ehepartner
- Kinder
- Eltern

Nahestehende Personen

- gemeinsame wirtschaftliche Berechtigung
- enge Geschäftsbeziehungen
- Strukturen zugunsten von PEP

Ausschlussklausel

Nicht als PEP gelten:

- lokale Vertreter
- Beamte ohne nationale Entscheidungsbefugnis

- technische oder beratende Funktionen

Akzeptierte Identifikationsdokumente

1. Zweck und Umfang

Dieser Anhang legt die von Pilot Innovation Sp. z o.o. („das Unternehmen“) akzeptierten Identifikationsdokumente für CDD- und KYC-Zwecke fest gemäß:

- polnischem AML-Gesetz
- EU-Richtlinie 2015/849
- FATF-Empfehlungen
- EBA-Leitlinien EBA/GL/2022/05

2. Allgemeine Regeln

1. Dokumente müssen gültig und lesbar sein.
2. Dokumente müssen enthalten:
- vollständiger Name
- Geburtsdatum oder Gründungsdatum
- Staatsangehörigkeit oder Jurisdiktion
- Identifikationsnummer
- Foto
- Ausstellungs- und Ablaufdatum
3. Farbkopien erforderlich.
4. Beglaubigte Übersetzung bei Bedarf.
5. Dokumente aus verbotenen Jurisdiktionen werden nicht akzeptiert.
6. Zusätzliche Dokumente können im Rahmen von EDD angefordert werden.

8. Zusammenarbeit und Informationsaustausch

Das Unternehmen arbeitet aktiv mit Aufsichtsbehörden und Strafverfolgungsbehörden zusammen, um Geldwäsche und Terrorismusfinanzierung zu verhindern. PayPilot stellt die erforderlichen Informationen auf offizielle Anfrage gemäß den geltenden Gesetzen und internationalen Verpflichtungen zur Verfügung.

Für Fragen zur Zusammenarbeit und zum Informationsaustausch kann das Unternehmen unter folgender Adresse kontaktiert werden:
aml@paypilot.org