Informazioni sui Principi di Antiriciclaggio (AML) e Contrasto al Finanziamento del Terrorismo (CTF)

1. Informazioni Generali

La Politica di Antiriciclaggio e Contrasto al Finanziamento del Terrorismo (di seguito la "Politica") ha lo scopo di prevenire e mitigare i potenziali rischi che Pilot Innovation (di seguito la "Società") possa essere coinvolta in attività illegali.

Per garantire la conformità sia alle normative internazionali sia a quelle nazionali, la Società implementa procedure interne e meccanismi efficaci per prevenire il riciclaggio di denaro, il finanziamento del terrorismo, il traffico di droga e di esseri umani, la proliferazione di armi di distruzione di massa, la corruzione e la concussione, nonché per rispondere a qualsiasi forma di attività sospetta da parte dei propri Utenti.

Per "Riciclaggio di denaro (legalizzazione dei proventi di reato)" si intende quanto previsto dall'articolo 299 del Codice Penale polacco del 6 giugno 1997.
Per "Finanziamento del terrorismo" si intende quanto previsto dall'articolo 165a del Codice Penale polacco del 6 giugno 1997.

La presente Politica non deve essere interpretata come un insieme esaustivo di tutte le politiche, procedure e misure di controllo applicate dalla Società per prevenire il riciclaggio di denaro, il finanziamento del terrorismo e altre attività illecite.

2. Obblighi della Società

2.1 Soggetto obbligato in Polonia

PILOT INNOVATION SP. Z O.O. è un soggetto obbligato ai sensi della legge polacca del 1° marzo 2018 sulla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo (Gazzetta Ufficiale 2018, voce 723, e successive modifiche), nonché di altri atti normativi applicabili.

Autorità di Vigilanza

La Società è soggetta alla supervisione dell'Ispettore Generale delle Informazioni Finanziarie (GIIF), che è l'autorità competente in Polonia responsabile del monitoraggio e della prevenzione dei reati finanziari.

Obblighi della Società

Identificazione del cliente e misure di sicurezza finanziaria (KYC/CDD):

- implementazione delle procedure “Know Your Customer” (KYC);
- valutazione del rischio del cliente in conformità al Risk-Based Approach (RBA);
- applicazione della Enhanced Due Diligence (EDD) per i clienti a rischio più elevato.

Obblighi di segnalazione verso il GIIF:

- segnalazione delle transazioni di valore pari o superiore a 15.000 EUR;
- segnalazione obbligatoria delle operazioni sospette potenzialmente correlate al riciclaggio di denaro o al finanziamento del terrorismo;
- conservazione di registri e documentazione adeguati per un periodo non inferiore a 5 anni.

Conformità agli standard internazionali AML/CTF

La Società garantisce la conformità agli standard internazionali in materia di antiriciclaggio e contrasto al finanziamento del terrorismo, tra cui:

- Direttiva (UE) 2015/849 (IV Direttiva AML);
- Regolamento (UE) 2023/1113 del Parlamento europeo e del Consiglio relativo alle informazioni che accompagnano i trasferimenti di fondi e di determinati cripto-attivi e che modifica la Direttiva (UE) 2015/849 (“Transfer Regulation”);
- Raccomandazioni del FATF (Financial Action Task Force) per il contrasto alla criminalità finanziaria.

3. Obblighi di Adeguata Verifica della Clientela (CDD)

La verifica completa dell’identità del cliente (Customer Due Diligence – CDD) costituisce una misura obbligatoria ai sensi della legge polacca del 1° marzo 2018 sulla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo (Gazzetta Ufficiale 2023, voce 1124). La Società è tenuta a raccogliere, verificare e aggiornare le informazioni sui clienti in tutte le fasi della cooperazione.

A seconda del livello di rischio assegnato al cliente, si applicano diversi livelli di CDD:

- Standard Due Diligence (SDD) – applicata ai clienti a basso rischio;
- Enhanced Due Diligence (EDD) – applicata quando viene identificato un rischio più elevato e richiede dati aggiuntivi.

3.1 Standard Due Diligence (SDD)

Per i clienti persone fisiche sono richiesti i seguenti documenti e controlli:

- passaporto o carta d’identità nazionale;
- prova dell’indirizzo di residenza (es. estratto conto bancario, bolletta utenze);
- verifica biometrica (liveness check) in caso di verifica remota.

Per i clienti societari sono richiesti:

- documenti di costituzione della società;
- documenti identificativi del Titolare Effettivo (UBO) e dei membri del consiglio di amministrazione;
- prova dell'indirizzo della società;
- estratto dal Registro Nazionale delle Imprese (KRS);
- prova della provenienza dei fondi;
- elenco dei 5 principali partner commerciali e relativi contratti;
- informazioni sul sito web della società e prova della proprietà del dominio.

3.2 Enhanced Due Diligence (EDD)

La Società applica misure EDD nei seguenti casi:

- quando i dati del cliente sollevano dubbi sulla loro affidabilità;
- quando il cliente è un'istituzione finanziaria di un paese terzo;
- quando il cliente è una Persona Politicamente Esposta (PEP) o un familiare/stretto collaboratore;
- quando il cliente risiede o opera in una giurisdizione ad alto rischio.

In tali casi, la Società può:

- richiedere documenti aggiuntivi di verifica dell'identità;
- verificare la provenienza dei fondi e del patrimonio del cliente;
- aumentare la frequenza del monitoraggio delle transazioni;
- condurre un'analisi più approfondita dell'attività commerciale del cliente.

3.3 Verifica della Provenienza dei Fondi

La Società è tenuta a garantire che i fondi utilizzati dal cliente provengano da una fonte legittima. A tal fine possono essere richiesti:

- estratti conto bancari;
- documenti che confermano redditi e investimenti;
- prove di vendita di beni o altre transazioni lecite.

4. Persone Politicamente Esposte (PEP)

La Società determina se un cliente o il suo titolare effettivo è una Persona Politicamente Esposta (PEP), un membro della famiglia o un soggetto strettamente associato. Qualora un cliente sia identificato come PEP, vengono automaticamente applicate misure di adeguata verifica rafforzata (Enhanced Due Diligence – EDD).

5. Monitoraggio continuo e aggiornamento dei dati

La Società implementa sistemi di monitoraggio delle transazioni in conformità con la legge polacca del 1° marzo 2018 sulla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo (Gazzetta Ufficiale 2018, voce 723). Lo scopo del monitoraggio è individuare e prevenire operazioni finanziarie sospette che possano essere collegate al riciclaggio di denaro (AML) o al finanziamento del terrorismo (CTF).

5.1 Procedure di monitoraggio

Il monitoraggio delle transazioni è continuo e comprende:

- analisi dei modelli di attività transazionale dei clienti;
- screening automatizzato delle transazioni mediante sistemi di analisi dei dati;
- revisione manuale delle transazioni che soddisfano criteri sospetti;
- screening delle transazioni rispetto alle liste di sanzioni e alle liste delle giurisdizioni ad alto rischio;
- valutazione continua del rischio del cliente e della sua attività transazionale.

La Società applica un approccio basato sul rischio (Risk-Based Approach – RBA), in base al quale i clienti sono classificati in diversi livelli di rischio (basso, medio, alto e inaccettabile) e le loro transazioni sono esaminate con un livello di dettaglio appropriato in funzione della classificazione di rischio.

5.2 Identificazione delle transazioni sospette

La Società è tenuta a mantenere un registro delle transazioni sospette e a segnalarle all'Ispettore Generale delle Informazioni Finanziarie (GIIF).

5.3 Valutazione del rischio

La Società conduce una valutazione interna del rischio con cadenza annuale, tenendo conto di:

- fattori geografici (paesi con elevati livelli di corruzione o debole supervisione finanziaria);
- tipologia di cliente (PEP, istituzioni finanziarie);
- strumenti di pagamento utilizzati (contanti, pagamenti anonimi);
- natura dell'attività del cliente (società operanti in settori con rischio AML/CTF elevato).

Sulla base di tale valutazione, vengono sviluppate azioni correttive per ridurre i rischi e migliorare i processi di monitoraggio.

5.4 Utilizzo della tecnologia nel monitoraggio

La Società utilizza tecnologie avanzate per l'analisi dei dati transazionali, tra cui:

- sistemi di monitoraggio automatizzati con algoritmi di machine learning;
- strumenti di analisi blockchain per tracciare operazioni in criptovalute;
- database di liste di sanzioni, Persone Politicamente Esposte (PEP) e notizie negative;
- strumenti di analisi comportamentale dei clienti.

Queste tecnologie migliorano l'accuratezza nell'individuazione delle transazioni sospette e riducono il numero di falsi positivi.

6. Responsabile designato (RO)

Il Responsabile designato della Società (Responsible Officer – RO) supervisiona la conformità alla Politica AML/CTF e garantisce il rispetto dei requisiti legali della Repubblica di Polonia e degli standard internazionali.

Le principali responsabilità includono:

- supervisione dell'applicazione delle procedure AML/CTF e del monitoraggio delle transazioni;
- cooperazione con il GIIF e presentazione delle segnalazioni di operazioni sospette;
- sviluppo e aggiornamento delle procedure interne AML/CTF;
- formazione dei dipendenti e conduzione di audit interni;
- valutazione dei rischi e implementazione di misure correttive.

Il Responsabile designato funge da principale punto di contatto con le autorità di regolamentazione e garantisce l'efficacia del sistema di controllo interno della Società.

7. Rifiuto del servizio

Clienti non accettabili

La Società non instaura rapporti commerciali con clienti che:

- rifiutano di fornire le informazioni e i documenti richiesti per la verifica;
- sono "Shell Banks" (banche prive di presenza fisica in una giurisdizione regolamentata);
- risiedono o operano in paesi soggetti a sanzioni internazionali o vietati dalla politica interna della Società;
- sollevano sospetti giustificati di potenziale coinvolgimento in riciclaggio di denaro, finanziamento del terrorismo o altre attività illegali.

Paesi e territori vietati

La Società non effettua l'onboarding di clienti provenienti dai seguenti paesi e territori: Afghanistan; Samoa Americane; Bielorussia; Burundi; Cambogia; Camerun; Repubblica Centrafricana; Ciad; Cuba; Repubblica Popolare Democratica di Corea (Corea del Nord); Repubblica Democratica del Congo; Eritrea; Etiopia; Haiti; Iran; Iraq; Kazakistan; Kirghizistan; Libano; Libia; Mali; Mozambico; Myanmar (Birmania); Nicaragua; Pakistan; Palestina; Russia; Senegal; Sierra Leone; Somalia; Sudan del Sud; Sudan; Siria; Tagikistan; Transnistria; Turkmenistan; Uganda; Ucraina – territori non controllati dal governo (oblast di Crimea, Donetsk, Kherson, Luhansk, Zaporizhzhia); Uzbekistan; Venezuela; Yemen; Zimbabwe.

I clienti o i titolari effettivi collegati a tali paesi sono automaticamente classificati come "Respinti / Vietati".

Paesi terzi ad alto rischio

Le seguenti giurisdizioni sono classificate ad alto rischio in conformità al Regolamento delegato (UE) 2024/594, alle dichiarazioni pubbliche del FATF e alla legge AML polacca (art. 2 (2)(13)). I clienti o le controparti collegati a tali paesi possono essere accettati solo previa applicazione di misure di adeguata verifica rafforzata (EDD), approvazione dell'MLRO e verifica documentata dell'origine dei fondi e del patrimonio (SoF/SoW).

Albania; Barbados; Burkina Faso; Camerun; Isole Cayman; Gibilterra; Giamaica; Giordania; Nigeria; Panama; Filippine; Sudafrica; Tanzania; Trinidad e Tobago; Uganda; Emirati Arabi Uniti (EAU); Vietnam; e qualsiasi altra giurisdizione designata ad alto rischio dal FATF o dalla Commissione Europea al momento dell'onboarding o della revisione periodica.

Paesi a rischio medio

Giurisdizioni con supervisione AML/CFT parzialmente efficace, elevati livelli di corruzione o problematiche di trasparenza fiscale, ma generalmente cooperative. Si raccomanda l'applicazione dell'EDD per transazioni di grande volume o esposizione a cripto-attività.

Lista dei paesi a rischio medio:
Andorra; Angola; Argentina; Armenia; Azerbaigian; Bahamas; Bahrein; Bangladesh; Bosnia ed Erzegovina; Botswana; Brasile; Brunei; Cile; Cina (RPC); Colombia; Costa Rica; Croazia; Repubblica Ceca; Repubblica Dominicana; Ecuador; Egitto; El Salvador; Georgia; Ghana; Grecia; Guatemala; Honduras; Hong Kong SAR; Ungheria; India; Indonesia; Israele; Kenya; Kuwait; Laos; Lettonia; Lituania; Malesia; Maldive; Malta; Mauritius; Messico; Moldova; Mongolia; Montenegro; Marocco; Namibia; Nepal; Macedonia del Nord; Oman; Papua Nuova Guinea; Paraguay; Perù; Polonia; Qatar; Romania; Arabia Saudita; Serbia; Singapore; Slovacchia; Slovenia; Sri Lanka; Suriname; Taiwan; Thailandia; Tunisia; Turchia; Ucraina (territorio controllato dal governo); Uruguay.

Paesi a basso rischio

Paesi con regimi AML/CFT solidi, forte governance, bassa percezione della corruzione e piena conformità a UE/OCSE/FATF. L'SDD può essere applicata ove legalmente consentito.

Lista dei paesi a basso rischio:
Austria; Australia; Belgio; Bulgaria; Canada; Croazia; Cipro; Danimarca; Estonia; Finlandia; Francia; Germania; Islanda; Irlanda; Italia; Giappone; Liechtenstein; Lussemburgo; Monaco; Paesi Bassi; Nuova Zelanda; Norvegia; Portogallo; San Marino; Corea del Sud; Spagna; Svezia; Svizzera; Regno Unito.

Attività vietate

La Società non entrerà consapevolmente né manterrà rapporti commerciali con persone o entità coinvolte o collegate a:

- gioco d'azzardo illegale o attività di scommesse non autorizzate;
- commercio di armi o attività legate alla difesa (inclusi intermediari, beni a duplice uso, munizioni, armi chimiche o biologiche, munizioni a grappolo);
- narcotici, precursori o prodotti farmaceutici illegali;
- tratta di esseri umani, schiavitù moderna o sfruttamento minorile;
- shell banks o istituzioni senza presenza fisica o supervisione efficace;
- contenuti per adulti (pornografia, servizi webcam, streaming per adulti, contenuti con minori o bestialità, materiale legato a violenza o stupro);
- violazione della proprietà intellettuale o del diritto d'autore, merci contraffatte;
- istituzioni finanziarie non autorizzate, money transmitter o fornitori di servizi di asset virtuali non autorizzati;
- criptovalute orientate alla privacy o con anonimato avanzato (ad es. Monero, Zcash, Dash);
- schemi Ponzi, piramidali o investimenti ad alto rendimento;
- opzioni binarie, piattaforme di trading non regolamentate o collocamenti di token ICO/ITO;
- clienti che emettono o detengono azioni al portatore o strumenti equivalenti non tracciabili.

Le azioni al portatore si riferiscono a strumenti negoziabili che rappresentano la proprietà di un'entità giuridica, in cui il controllo è detenuto esclusivamente dal possessore fisico e non può essere verificato dalla Società. Sono accettate azioni nominative o dematerializzate.

La Società si riserva il diritto di rifiutare, sospendere o terminare qualsiasi relazione commerciale o transazione che esuli dal proprio appetito di rischio o presenti un rischio AML/CFT non gestibile.

Linee guida EBA e reporting AMLRO

In base alle Linee guida EBA/GL/2022/05 del 14 giugno 2022 e alla posizione KNF sull'AMLRO del 1° dicembre 2022, la Società indica che, nell'ambito delle informazioni periodiche (o ad hoc) di gestione e del rapporto annuale preparato dal dipendente designato (AMLRO), sono richiesti in particolare i seguenti dati e informazioni:

- rischi ML/TF e conformità della Società alle disposizioni AML/CFT;
- cooperazione con le autorità competenti e relativa corrispondenza;
- risultati e azioni delle autorità di intelligence finanziaria e di vigilanza;
- problemi o violazioni rilevanti in ambito AML/CFT e azioni correttive;
- sintesi della valutazione del rischio ML/TF a livello dell'istituzione;
- modifiche alla metodologia di valutazione del rischio cliente;
- classificazione dei clienti per categorie di rischio;
- numero di dossier clienti per categoria di rischio;
- applicazione delle misure di adeguata verifica;
- statistiche sulle transazioni sospette o insolite;
- rapporti rifiutati o terminati;
- richieste da parte di FIU, tribunali o autorità;
- struttura organizzativa AML/CFT;
- risorse umane e tecniche AML/CFT;
- meccanismi di mitigazione del rischio;
- attività di monitoraggio della conformità;
- formazione del personale;
- attività pianificate dell'AMLRO;
- risultati dei controlli interni;
- modifiche normative e impatto sul processo AML/CFT.

Persone Politicamente Esposte (PEP)

PEP nazionali (Polonia / giurisdizione locale)

Persone che ricoprono o hanno ricoperto funzioni pubbliche di rilievo a livello nazionale, tra cui:

- Capo di Stato o Capo del Governo
- Ministri, Vice Ministri, Segretari di Stato
- Membri del Parlamento (Sejm e Senato)
- Membri degli organi direttivi dei partiti politici
- Membri della Corte Suprema o del Tribunale Costituzionale
- Membri della Corte dei Conti o del Consiglio della Banca Nazionale di Polonia
- Ambasciatori, incaricati d'affari
- Alti ufficiali delle forze armate
- Membri degli organi di gestione o controllo di imprese statali
- Direttori e membri degli organi di organizzazioni internazionali

Nota:
Le funzioni locali o regionali non sono considerate PEP, salvo influenza a livello nazionale.

PEP stranieri

Persone con funzioni pubbliche rilevanti in un paese estero:

- Capi di Stato o di Governo
- Ministri o Vice Ministri
- Membri del Parlamento
- Membri di corti supreme o costituzionali
- Membri di banche centrali
- Ambasciatori o alti ufficiali militari
- Dirigenti di imprese statali
- Dirigenti di organizzazioni internazionali

PEP organizzazioni internazionali

Persone con ruoli dirigenziali in:
ONU, FMI, Banca Mondiale, istituzioni UE, NATO, OSCE, ecc.

Familiari dei PEP

Sono considerati correlati:

- Coniuge o partner equivalente
- Figli e loro partner
- Genitori

Stretti collaboratori

Persone che:

- condividono la titolarità con un PEP
- mantengono relazioni commerciali strette
- sono beneficiari di strutture create per un PEP

Clausola di esclusione

Non sono classificati come PEP:

- rappresentanti locali
- funzionari senza poteri decisionali nazionali
- personale tecnico o consulenziale

Documenti di identificazione accettati

1. Scopo e ambito

Il presente Allegato stabilisce l'elenco dei documenti accettati da Pilot Innovation Sp. z o.o. ("la Società") ai fini delle procedure CDD e KYC in conformità con:

- Legge AML polacca del 1 marzo 2018
- Direttiva UE 2015/849
- Raccomandazioni FATF
- Linee guida EBA/GL/2022/05

L'elenco si applica all'onboarding e alla verifica continua di persone fisiche, persone giuridiche e titolari effettivi.

2. Regole generali

1. Tutti i documenti devono essere validi, leggibili e rilasciati da un'autorità competente.
2. Devono contenere almeno:

- nome completo
- data di nascita o costituzione
- nazionalità o giurisdizione
- numero identificativo
- fotografia (persone fisiche)
- date di emissione e scadenza

3. Copie a colori e di qualità sufficiente.
4. Documenti non in italiano o inglese devono essere accompagnati da traduzione certificata.
5. Documenti emessi da giurisdizioni vietate o ad alto rischio non sono accettati.
6. La Società può richiedere documenti aggiuntivi nell'ambito dell'EDD.

8. Cooperazione e scambio di informazioni

La Società coopera attivamente con le autorità di regolamentazione e le forze dell'ordine per prevenire il riciclaggio di denaro e il finanziamento del terrorismo. PayPilot fornisce le informazioni necessarie su richiesta ufficiale in conformità alle leggi applicabili e agli obblighi internazionali.

Per questioni relative alla cooperazione e allo scambio di informazioni, la Società può essere contattata all'indirizzo:
aml@paypilot.org