BLASFORA

ANTI MONEY LAUNDERING AND COUNTER TERRORIST FINANCING POLICY

Effective: May 9, 2025

1. Introduction

1.1. BLASFORA HOLDINGS LTD (the «Company»), a company registered and operating in the Republic of Cyprus, is committed to full compliance with **The Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007 (Law 188(I)/2007)** and subsequent amendments, as well as applicable EU Directives and international AML/CFT standards.
1.2. This Policy outlines the fundamental principles and internal controls to prevent the misuse of the Company's services for money laundering or terrorist financing. BLASFORA HOLDINGS LTD operates in the field of scoring, financial risk assessment, and behavioral analytics using AI/ML-based technologies and digital integrations.
1.3. The purpose of this Policy is:
• To ensure appropriate risk management systems are in place to identify, assess, monitor, and mitigate money laundering and terrorist financing risks.
• To establish consistent standards for customer due diligence (CDD), ongoing monitoring, record-keeping, and suspicious transaction reporting.
• To ensure employees are trained and understand their obligations under AML/CFT law.
1.4. This document will be reviewed and updated periodically based on changes in regulation, risk exposure, or business processes.

2. Company Information

Legal Name: BLASFORA HOLDINGS LTD
Jurisdiction: Republic of Cyprus
Registered Address: Charalampou Mouskou, 20-1A, ABC BUSINESS CENTRE, 8010, Paphos, Cyprus
Senior Management:
Director: Iryna Yanovska
Compliance Officer/MLCO: Iryna Yanovska

BLASFORA HOLDINGS LTD cooperates with MOKAS (Unit for Combating Money Laundering), the official Financial Intelligence Unit (FIU) of Cyprus.

3. Scope and Applicability

3.1. This Policy applies to:
• All company staff, contractors, and agents.
• All customers and partners engaging with the Company's financial data, scoring, or analytics services.
• The processing and analysis of financial and behavioral data used in credit risk evaluation.
3.2. The Policy applies regardless of whether the data relates to natural or legal persons and whether it is collected via direct integration (e.g., via REST API, Webhooks) or via third-party platforms.

4. Definitions

4.1. For the purposes of this Policy, the following definitions apply:
«Applicable Legislation»: refers to the Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007 (Law 188(I)/2007) and its amendments, as well as relevant Directives issued by the Cyprus Securities and Exchange Commission (CySEC) or other competent authority.
«Authority»: refers to MOKAS (Unit for Combating Money Laundering), the Financial Intelligence Unit (FIU) of the Republic of Cyprus.
«Beneficial Owner»: a natural person who ultimately owns or controls a legal entity through direct or indirect ownership of at least 25% of the shares or voting rights or otherwise exercises control over the management.
«Business Relationship»: a professional or commercial relationship which is expected to have an element of duration, established between the Company and a Customer, including but not limited to repeat scoring requests, API access, or long-term integration for client risk evaluation services.
«Customer»: any natural or legal person using the services of the Company, including access to analytics tools, scoring models, and integration services.
«Politically Exposed Person (PEP)»: an individual who is or has been entrusted with prominent public functions, including their immediate family members or close associates, as defined under Cypriot AML law.
«Sanctions Lists»: official lists of individuals or entities subject to restrictions under UN, EU, OFAC, or other recognized sanctions regimes.
«Suspicious Transaction»: any transaction or activity that appears unusual, inconsistent with a customer's known activities, or may involve the proceeds of criminal activity or terrorist financing.
«Risk Scoring»: the Company's automated system of evaluating a client's financial and behavioral risk based on transaction data, profiling models, and machine learning algorithms.
«Source of Funds»: the origin of the funds involved in a transaction, such as income, investment proceeds, or business revenue.

«Source of Wealth»: the origin of a person's overall financial standing or total net worth, including assets accumulated over time.
«Record Keeping»: the Company's obligation to retain documentation of customer identity, transactions, scoring decisions, and monitoring alerts for no less than five (5) years after the end of the relationship.
«Working Days»: Monday to Friday, excluding public holidays observed in the Republic of Cyprus.
«Reliable Source»: any data or verification source considered trustworthy and reputable for confirming a customer's identity or risk status (e.g., government registers, regulated databases, or international watchlists).

5. Governance and Oversight

5.1. As the Company is governed by a sole Director, all AML-related responsibilities and oversight obligations rest with the Director, who acts in a fiduciary capacity. The Director shall ensure that the Company operates in full compliance with applicable laws, maintains an adequate internal control environment, and fosters a strong compliance culture.
5.2. Responsibilities of the Director include:
• Approving and periodically reviewing the AML Manual and associated internal policies;
• Appointing a Money Laundering Compliance Officer (MLCO) in accordance with CySEC Directive DI87-01;
• Ensuring that the MLCO holds sufficient authority, independence, and access to all relevant information and departments;
• Overseeing the implementation of effective AML controls, procedures, and training programmes;
• Reviewing and approving all reports prepared by the MLCO, including the Annual Report and the Monthly Prevention Statement.

6. Role and Duties of the MLCO

6.1. The MLCO occupies a position of sufficient seniority and shall report directly to the Director. The MLCO shall ensure the Company's full and continuous compliance with AML obligations.
6.2. Core duties include:
• Designing, maintaining, and implementing AML policies and internal controls tailored to the Company's risk exposure;
• Monitoring adherence to the AML framework across all departments and functions;
• Receiving and evaluating Internal Suspicion Reports, drafting Internal Evaluation Reports, and submitting Suspicious Transaction Reports (STRs) to MOKAS when deemed appropriate;

• Acting as the designated point of contact with MOKAS and cooperating fully during investigations;
• Preparing and submitting the Annual AML Compliance Report and Monthly Prevention Statements in accordance with CySEC deadlines;
• Updating the Company's risk assessments and client classifications in line with emerging risks and regulatory expectations;
• Facilitating regular AML training for all relevant personnel and maintaining training records;
• Keeping registers of suspicious activity and STRs submitted to the authorities.

7. Risk-Based Approach (RBA)

7.1. The Company employs a proportionate and risk-sensitive approach to AML compliance in accordance with Section 58A of the AML Law. The risk-based framework allows the Company to differentiate between clients and activities based on the perceived level of money laundering or terrorist financing risk.
7.2. Risk considerations include:
• Nature and complexity of client structures (e.g., PEPs, bearer shares, offshore entities);
• Geographical risk exposure (e.g., high-risk third countries, FATF blacklists);
• Client behaviour and transaction patterns lacking economic rationale;
• Use of anonymity-enhancing instruments or non-face-to-face onboarding;
• Services offered and distribution channels used.
7.3. Clients are categorised into Low Risk, Normal Risk, or High Risk based on documented assessments, which inform the extent of due diligence required.

8. Client Due Diligence (CDD) and Know-Your-Customer (KYC) Procedures

8.1. The Company undertakes CDD and KYC procedures:
• Prior to establishing a business relationship;
• When conducting occasional transactions exceeding €10,000;
• Where there is suspicion of money laundering or terrorist financing;
• In cases where existing identification information appears unreliable or incomplete.
8.2. The MLCO shall ensure that all required identification and verification data is obtained and retained for the prescribed statutory period.
8.3. Documentation Requirements
To satisfy CDD obligations, the following documentation shall be collected from clients, depending on their status:
8.3.1. For natural persons:

- Valid government-issued photo identification (e.g., passport, national ID card, residence permit);

- Proof of address dated within the last 3 months (e.g., utility bill, bank statement, official government correspondence);
- Source of funds and/or source of wealth declarations, supported by documentation where applicable (e.g., payslips, tax returns, inheritance documents, property sale agreements).

8.3.2. For legal entities:

- Certificate of Incorporation and recent Certificate of Good Standing (if applicable);
- Memorandum and Articles of Association or equivalent founding documents;
- Company registry extract or equivalent document indicating directors, shareholders, and registered office;
- Identification and proof of authority for directors and authorised representatives;
- Identification of beneficial owners (in line with the 25% threshold or control criterion), including relevant ID and address documents;
- Ownership structure chart, especially where multi-tier or cross-border;
- Documentation confirming source of funds or source of wealth (e.g., audited financials, contracts, tax returns);
- Regulatory license or proof of supervision if the entity operates in a regulated sector;
- Where applicable, enhanced due diligence measures shall be applied for entities established in high-risk jurisdictions or offshore centres.

9. Ongoing Monitoring

9.1. The Company monitors the business relationship throughout its duration to ensure that transactions are consistent with the client's risk profile, expected activity, and declared source of funds.
9.2. The frequency and depth of monitoring shall be proportionate to the client's risk classification, and any unusual activity will be escalated to the MLCO for assessment.

10. Reporting of Suspicious Transactions

10.1. If, after evaluation, the MLCO determines that there is knowledge or reasonable grounds to suspect that a transaction or attempted transaction may involve criminal proceeds or terrorist financing, a formal Suspicious Transaction Report shall be submitted to MOKAS without delay.
10.2. In accordance with Section 48 of the AML Law, under no circumstances shall any employee or officer disclose to the client (a "tipping-off" offence) the fact that a report has been made.

11. Record-Keeping

11.1. All records, including due diligence documents, risk assessments, internal reports, and communication with MOKAS, shall be retained for a minimum period of five (5) years from the termination of the business relationship or the completion of the transaction.
11.2. Records shall be stored in both physical and electronic formats and must be readily available for regulatory inspection or audit.

12. Training

12.1. The Company commits to the ongoing education and training of all relevant staff regarding AML obligations, red flags, reporting obligations, and procedural updates. The MLCO is responsible for overseeing and maintaining training schedules and logs.

13. Conclusion

13.1. This policy is intended to demonstrate the Company's unwavering commitment to combating money laundering and terrorist financing in full compliance with Cyprus legal requirements and international best practices. The AML Manual shall be reviewed and updated on an annual basis or as required by changes in the regulatory environment.