Bitpanda Broker MENA FZCO

AML & KYC Overview

AML & KYC Processes Overview

Bitpanda Broker MENA FZCO

bitpanda

Summary of AML & KYC Processes – Bitpanda Broker MENA FZCO

1. Introduction

This document provides an overview of Bitpanda Broker MENA FZCO's approach to Anti-Money Laundering ("AML"), Counter-Terrorist Financing ("CFT"), Counter-Proliferation Financing ("CPF") and Know Your Customer ("KYC") compliance.

Bitpanda Broker MENA maintains a risk-based framework designed to prevent its products and services from being used for money laundering, terrorist financing, proliferation financing, sanctions evasion or other financial crime, and to comply with applicable UAE laws, regulations and Virtual Assets Regulatory Authority ("VARA") requirements.

2. Overview

Money laundering involves the concealment or disguise of the illicit origin of funds or assets so that they appear legitimate. It is commonly described through the stages of placement, layering and integration.

Terrorist financing involves the provision, collection or movement of funds or other assets for terrorist purposes. Unlike money laundering, the funds involved may originate from legitimate as well as illicit sources.

Proliferation financing involves the provision of funds or financial services that support the proliferation of weapons of mass destruction and related activities, including in circumstances covered by applicable targeted financial sanctions.

Bitpanda Broker MENA maintains controls designed to identify, assess and mitigate exposure to these risks, including applicable sanctions and targeted financial sanctions requirements.

3. AML, CTF & CPF Regulatory Framework

Bitpanda Broker MENA is subject to the applicable UAE legal and regulatory framework for anti-money laundering, combating the financing of terrorism and proliferation financing, as well as the requirements applicable to Virtual Asset Service Providers ("VASPs") regulated by VARA.

This framework includes, among others:

- Federal Decree-Law No. 10 of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing, together with its applicable implementing regulations;
- applicable UAE requirements relating to targeted financial sanctions ("TFS"), including the implementation of relevant United Nations Security Council resolutions;
- the Virtual Assets and Related Activities Regulations, as amended from time to time;
- the VARA Compliance and Risk Management Rulebook, including its requirements relating to AML/CFT, proliferation financing, sanctions compliance and targeted financial sanctions; and
- other applicable VARA Rules, Directives and Guidance.

Bitpanda Broker MENA maintains policies, procedures, systems and controls designed to support compliance with these requirements and to mitigate the financial crime risks relevant to its activities.

4. Roles of Relevant Parties

Bitpanda Broker MENA maintains appropriate governance and oversight arrangements for its AML/CFT/CPF compliance framework. Key responsibilities include:

- **Board:** Provides oversight of the AML/CFT/CPF compliance framework and ensures that appropriate systems and controls are maintained to support compliance with applicable regulatory requirements.
- **Money Laundering Reporting Officer ("MLRO"):** Oversees the implementation and ongoing effectiveness of the AML/CFT/CPF framework, including relevant risk assessments, policies and procedures, transaction monitoring and suspicious activity reporting obligations.
- **Employees:** Employees are required to comply with applicable financial crime policies and procedures, complete relevant training, and promptly escalate suspicious activity or other financial crime concerns in accordance with internal procedures.

5. Risk-Based Approach (RBA)

Bitpanda Broker MENA applies a risk-based approach to identify, assess and mitigate money laundering, terrorist financing and proliferation financing risks associated with its business activities, customers and services.

Relevant risk factors include, among others:

- customer profile, business activities and background;
- geographic risk, including exposure to higher-risk jurisdictions;

- products, services and Virtual Assets involved;
- nature, purpose and expected activity of the business relationship;
- transaction activity and associated risk indicators;
- ownership and control structures, where applicable; and
- exposure to sanctions, targeted financial sanctions and other relevant financial crime risks.

The level of customer due diligence and ongoing monitoring applied is proportionate to the risks identified. Enhanced Due Diligence ("EDD") and additional controls are applied where higher risks are identified, including in circumstances involving Politically Exposed Persons ("PEPs") or other higher-risk relationships, in accordance with applicable regulatory requirements.

6. Customer Due Diligence (CDD)

Bitpanda Broker MENA applies Customer Due Diligence ("CDD") measures before establishing a business relationship and, where applicable, throughout the course of the relationship. These measures are applied on a risk-sensitive basis and include, as appropriate:

- identifying customers and verifying their identity using reliable and independent information and documentation;
- identifying and verifying Ultimate Beneficial Owners ("UBOs"), where applicable;
- understanding the purpose and intended nature of the business relationship;
- assessing the customer's risk profile and applying appropriate due diligence measures;
- screening customers and relevant connected parties against applicable sanctions and targeted financial sanctions lists and identifying Politically Exposed Persons ("PEPs"); and
- conducting ongoing due diligence and monitoring to ensure that customer information and activity remain consistent with the customer's risk profile.

Enhanced Due Diligence ("EDD") and additional measures are applied where higher risks are identified. Depending on the circumstances and applicable regulatory requirements, these measures may include obtaining additional information regarding the customer, the purpose of the relationship, and the source of funds and/or source of wealth.

Where Bitpanda Broker MENA is unable to satisfactorily complete required due diligence, or where identified risks cannot be appropriately managed, it may decline to establish or may terminate a business relationship, and take any further action required under applicable laws and regulatory requirements.

7. Transaction Monitoring & Reporting

Bitpanda Broker MENA maintains risk-based systems and controls to monitor customer activity and transactions for unusual or potentially suspicious activity. These controls include automated monitoring and, where appropriate, manual review by relevant compliance personnel.

Monitoring is designed to identify activity that may indicate money laundering, terrorist financing, proliferation financing, sanctions-related concerns or other financial crime risks, taking into account the customer's risk profile and expected activity.

Where potentially suspicious activity is identified, it is reviewed and escalated in accordance with Bitpanda Broker MENA's internal procedures. Where required, the MLRO submits the appropriate report to the UAE Financial Intelligence Unit (“UAEFIU”) through the goAML platform, in accordance with applicable legal and regulatory requirements.

Bitpanda Broker MENA also maintains internal escalation procedures requiring employees to promptly report relevant suspicions or financial crime concerns to the MLRO.

8. Record Keeping & Retention

Bitpanda Broker MENA maintains records of customer identities, transactions, and reports for a minimum of eight years. Records include:

- Customer identification documents.
- Transaction history and account details.
- Suspicious Transaction Reports and internal assessments.

These records support regulatory compliance and facilitate investigations by authorities when required.

9. Off-boarding & Training

Bitpanda Broker MENA may terminate a business relationship where required by applicable laws or regulatory requirements, where required due diligence cannot be satisfactorily completed, or where identified financial crime risks cannot be appropriately managed.

Employees receive regular training on applicable AML/CFT/CPF requirements, including customer due diligence, identification and escalation of suspicious activity, sanctions and targeted financial sanctions, and relevant internal procedures. Refresher training is conducted periodically to maintain awareness of regulatory requirements and evolving financial crime risks.

10. Review and Updates

The AML & KYC policy is reviewed at least annually to align with evolving regulations and emerging risks. Review processes include:

- Regulatory gap analysis to identify changes in compliance requirements.
- Risk assessment updates based on new business operations and threats.
- Internal audits to evaluate policy effectiveness and implementation.

Amendments to the policy are approved by the Board and communicated to employees to ensure full compliance.