Anti-Money Laundering (AML) and Know Your Customer (KYC) Policy Privé Market (Operated by Mephexus Group s.r.o.)

Effective Date: April 02, 2024

Last Updated: April 10, 2025

1. Introduction

Mephexus Group s.r.o., operating under the brand Privé Market (hereinafter "the Company"), is an online marketplace offering high-value assets for sale, including yachts, cars, real estate, jewelry, and watches. The Company facilitates transactions between buyers and sellers and accepts payments in both fiat currencies and cryptocurrencies. Recognizing the risks of money laundering, terrorist financing, fraud, and other financial crimes associated with high-value transactions and cryptocurrency use, the Company has established this AML/KYC Policy to ensure compliance with applicable laws and regulations, safeguard its operations, and protect its customers and stakeholders.

This policy outlines the Company's procedures for customer identification, risk assessment, transaction monitoring, reporting obligations, and staff training. It applies to all employees, contractors, agents, and third-party partners acting on behalf of the Company.

2. Legal and Regulatory Framework

The Company adheres to the following legal and regulatory frameworks:

Czech Republic: Act No. 253/2008 Coll. on Certain Measures Against Money Laundering and Terrorist Financing, as amended, and related regulations enforced by the Financial Analytical Office (FAU).

European Union: Directive (EU) 2015/849 (4th AMLD), Directive (EU) 2018/843 (5th AMLD), and Directive (EU) 2018/1673 (6th AMLD), which set standards for AML/CFT compliance across EU member states.

International Standards: Recommendations of the Financial Action Task Force (FATF), including specific guidance on virtual assets and virtual asset service providers (VASPs).

Cryptocurrency Regulations: Applicable Czech and EU regulations governing the use of virtual assets in financial transactions.

EU Sanctions and High-Risk Third Countries: Compliance with EU sanctions regimes and the European Commission's list of high-risk third countries with strategic deficiencies in their AML/CFT regimes.

The Company is committed to updating this policy in response to changes in legislation or regulatory guidance.

3. Objectives

The objectives of this AML/KYC Policy are to:

Prevent the use of Privé Market for money laundering, terrorist financing, or other illegal activities.
Identify and verify the identity of customers and beneficial owners involved in transactions.
Assess and mitigate risks associated with customers, transactions, and payment methods (including cryptocurrencies).

Monitor transactions for suspicious activity and report such activity to the appropriate authorities. Ensure compliance with all applicable laws and regulations, including EU restrictions on banned countries and citizens.

4. Scope

This policy applies to:

All customers (buyers and sellers) using the Privé Market platform.

All transactions facilitated through the platform, whether in fiat currency or cryptocurrency.

All employees, contractors, and third-party service providers acting on behalf of Mephexus Group s.r.o.

5. Key Definitions

AML: Anti-Money Laundering – Measures to prevent and detect the process of disguising illegally obtained funds as legitimate income.

KYC: Know Your Customer – Procedures to identify and verify the identity of customers and beneficial owners.

CDD: Customer Due Diligence – The process of assessing customer risk and verifying their identity.

EDD: Enhanced Due Diligence – Additional scrutiny applied to high-risk customers or transactions.

Cryptocurrency: Digital or virtual currencies (e.g., Bitcoin, Ethereum) that use cryptography for security and operate on decentralized networks.

Beneficial Owner: The natural person who ultimately owns or controls a customer or transaction.

Suspicious Activity: Any transaction or behavior that may indicate money laundering, terrorist financing, or other illegal activity.

High-Risk Third Country: A jurisdiction identified by the European Commission as having strategic deficiencies in its AML/CFT regime.

6. Customer Due Diligence (CDD) Procedures

The Company implements a risk-based approach to CDD, ensuring that the level of scrutiny corresponds to the assessed risk of each customer or transaction.

6.1. Standard CDD Requirements

For all customers (individuals or legal entities) engaging in transactions on Privé Market, the Company will:

Identify the Customer: Collect and verify the following:

For individuals: Full name, date of birth, nationality, residential address, and a government-issued identification document (e.g., passport, driver’s license, or ID card).

For legal entities: Company name, registration number, registered address, incorporation documents, and identification of authorized representatives.

Identify the Beneficial Owner: Determine the natural person(s) who ultimately own or control the customer (e.g., ownership of 25% or more of a legal entity).

Verify Identity: Use reliable, independent sources to confirm the customer's identity (e.g., document scans, electronic verification tools).

Purpose of Transaction: Obtain information on the intended nature and purpose of the customer's activity on the platform (e.g., buying a yacht for personal use).

6.2. Enhanced Due Diligence (EDD)

EDD is applied to high-risk customers or transactions, including but not limited to:

Transactions exceeding a threshold of **EUR 10,000** (or equivalent in cryptocurrency).

Customers from high-risk jurisdictions (as identified by FATF or the European Commission's list of high-risk third countries—see Section 7).

Politically Exposed Persons (PEPs), their family members, or close associates.

Transactions involving cryptocurrencies with a history of anonymity (e.g., privacy coins like Monero).

Unusual or complex transaction patterns.

EDD measures include:

Additional identity verification (e.g., video calls, notarized documents).

Source of funds/wealth verification (e.g., bank statements, tax returns, proof of cryptocurrency origin).

Ongoing monitoring of the customer's activity.

6.3. Simplified Due Diligence (SDD)

SDD may be applied to low-risk customers (e.g., transactions below EUR 1,000 with no red flags), subject to approval by the AML Compliance Officer. However, SDD does not exempt the Company from basic identity verification.

7. EU Restrictions: Banned Countries and Citizens

The Company complies with European Commission restrictions related to AML/CFT and sanctions, which impact transactions and customer onboarding. These restrictions include:

7.1. European Commission List of High-Risk Third Countries

Under Directive (EU) 2015/849, the European Commission identifies jurisdictions with strategic deficiencies in their AML/CFT regimes that pose significant threats to the EU financial system. As of the latest delegated regulation (up to April 2025, based on available data), the following countries are designated as high-risk third countries requiring EDD:

Afghanistan
Barbados
Burkina Faso
Cameroon
Cayman Islands
Democratic Republic of the Congo
Gibraltar

Haiti
Jamaica
Jordan
Mali
Mozambique
Myanmar
Nigeria
Panama
Philippines
Senegal
South Sudan
Syria
Tanzania
Trinidad and Tobago
Uganda
United Arab Emirates
Vanuatu
Yemen

Note: This list is subject to periodic updates by the European Commission via delegated acts. The Company will monitor and adopt the most current list published on the European Commission's official website (ec.europa.eu). Transactions involving customers or beneficial owners from these jurisdictions will trigger EDD, and the Company may refuse service if risks cannot be mitigated.

7.2. EU Sanctions Regime

The Company adheres to EU sanctions imposed under the Common Foreign and Security Policy (CFSP), which **bans** transactions with specific countries, entities, or individuals. Key sanctioned jurisdictions include:

North Korea
Iran
Russia
Belarus
Syria

The Company screens all customers and transactions against the EU Consolidated Financial Sanctions List (available at eeas.europa.eu) to ensure no dealings with sanctioned parties. Services will be denied to any customer or beneficial owner subject to EU sanctions.

7.3. Implementation

Screening Process: All customers and beneficial owners are screened against the European Commission's high-risk third countries list and EU sanctions list during onboarding and transaction processing.

Prohibited Transactions: The Company will not process transactions involving banned countries or sanctioned individuals/entities unless explicitly permitted by an EU exemption.

Updates: The AML Compliance Officer is responsible for maintaining an up-to-date list of restricted jurisdictions and ensuring system filters reflect these restrictions.

8. Cryptocurrency-Specific Procedures

Given the Company's acceptance of cryptocurrency payments, additional measures are implemented to address associated risks:

Wallet Screening: Screen cryptocurrency wallets for links to illicit activities using blockchain analytics tools (e.g., Chainalysis, Elliptic).

Source of Crypto Funds: Require customers to provide evidence of the origin of cryptocurrency (e.g., exchange transaction records, wallet statements).

Mixing/Tumbling Detection: Flag transactions involving mixers or tumblers, which obscure the origin of funds, for further review.

Compliance with VASP Rules: Ensure that cryptocurrency transactions comply with FATF's Travel Rule and Czech regulations for virtual asset service providers, if applicable.

9. Risk Assessment

The Company conducts a risk assessment for each customer and transaction based on:

Customer Risk: Jurisdiction (including EU high-risk third countries and sanctioned jurisdictions), PEP status, criminal history, or adverse media.

Product Risk: High-value assets (e.g., yachts, real estate) inherently carry higher risks.

Payment Risk: Cryptocurrency payments are considered higher risk than fiat due to potential anonymity.

Geographic Risk: Transactions involving high-risk or sanctioned countries as per EU lists.
A risk score is assigned to each customer, determining the level of due diligence required (CDD, EDD, or SDD).

10. Transaction Monitoring

The Company monitors transactions in real-time and post-transaction to detect suspicious activity. Red flags include:

Large or frequent transactions inconsistent with the customer's profile.

Rapid movement of funds (e.g., immediate resale of purchased assets).

Use of multiple payment methods or wallets to obscure fund origins.

Transactions with sanctioned individuals, entities, or jurisdictions as per EU restrictions.

Suspicious activity is escalated to the AML Compliance Officer for investigation.

11. Record-Keeping

The Company retains all AML/KYC records for a minimum of 5 years (or longer if required by law), including:

Customer identification documents and verification data.

Transaction records (fiat and cryptocurrency).

Risk assessments and monitoring reports.

Suspicious activity reports (SARs) and correspondence with authorities.

Records are stored securely in compliance with the General Data Protection Regulation (GDPR) and Czech data protection laws.

12. Reporting Obligations

The Company complies with reporting requirements under Czech and EU law:

Suspicious Activity Reports (SARs): Any suspicious transaction, including those involving EU high-risk third countries or sanctioned parties, is reported to the Financial Analytical Office (FAU) within 3 days of detection.

Cash Transactions: Transactions exceeding EUR 10,000 in cash (if applicable) are reported to the FAU.

Sanctions Screening: Customers and transactions are screened against EU sanctions lists, with violations reported as required.

Employees are trained to recognize and report suspicious activity internally to the AML Compliance Officer.

13. AML Compliance Officer

The Company appoints an AML Compliance Officer responsible for:

Overseeing the implementation of this policy.

Conducting risk assessments and audits.

Investigating suspicious activity and filing SARs.

Monitoring updates to EU high-risk third countries and sanctions lists.

Serving as the point of contact with regulatory authorities.

Ensuring staff training and policy updates.

Contact: [Insert AML Compliance Officer contact details].

14. Staff Training

All employees receive annual AML/KYC training covering:

Legal and regulatory requirements, including EU restrictions.

Identification of suspicious activity.

Cryptocurrency-specific risks and compliance.

Internal reporting procedures.

New hires complete training within their first month of employment.

15. Third-Party Partners

Third-party service providers (e.g., payment processors, blockchain analytics firms) must:

Comply with AML/KYC standards equivalent to this policy, including EU restrictions.

Be subject to due diligence before onboarding.

Provide regular compliance reports to the Company.

16. Policy Review and Updates

This policy is reviewed annually or upon significant regulatory changes (e.g., updates to EU high-risk third countries or sanctions). Updates are approved by the AML Compliance Officer and senior management.

17. Non-Compliance

Failure to comply with this policy may result in:

Termination of customer accounts or transactions.

Disciplinary action against employees (up to and including termination).

Reporting to law enforcement or regulatory authorities.

18. Contact Information

For questions or to report suspicious activity:

Mephexus Group s.r.o.

Světova 523/1, 180 00 Praha - Libeň, Czech Republic

Email: compliance@mephexus.com