AML & KYC Policy

CoiniGo, powered by **MetaWorld Capital sp. z o.o.**
Effective Date: 1st December 2024
Last Updated: 1st December 2024
Version: 1.0
Applies To: All users and customers of CoiniGo ("we", "our", "the Company")

1. PURPOSE

This Anti-Money Laundering (AML) and Know Your Customer (KYC) Policy outlines the procedures and internal controls implemented by the Company, to prevent and mitigate possible risks of money laundering, terrorist financing, and other illicit financial activities.

The Company recognizes the unique challenges of the cryptocurrency industry, such as the pseudonymous nature of blockchain transactions, the use of privacy-enhancing technologies (e.g., mixers, tumblers), and cross-border transaction complexities. This policy addresses these challenges through robust identification, verification, monitoring, and reporting mechanisms.

2. REGULATORY FRAMEWORK

This policy is established in compliance with applicable laws and regulations, including but not limited to:

- The EU Markets in Crypto-Assets Regulation (MiCA)
- The 5th and 6th EU Anti-Money Laundering Directives (AMLD)
- The Financial Action Task Force (FATF) Recommendations
- Local regulations in the jurisdictions in which we operate

3. SCOPE

This policy applies to all users of our platform, including:

- Merchants using our crypto payment gateway
- End customers transacting through our system
- Internal staff and third-party service providers

4. MONEY LAUNDERING AND TERRORIST FINANCING

The Company understands money laundering as:

1. the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
2. the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
3. the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
4. participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

Terrorist financing provides funds for terrorist activity. From a legal standpoint it means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences related to terrorism.

5. RISK-BASED APPROACH AND RISK ASSESSMENT

The Company shall perform a risk-based due diligence and collect information and documentation on each prospective client in order to assess the risk profile associated. The employees shall exercise care, due diligence and good judgement in determining the overall character and nature of all clients. We conduct our business in accordance with the highest ethical standards and will not enter into business relationships with individuals or entities that may adversely affect the Company's reputation and compromise the virtual currency industry.

For the purpose of identification, assessment and analysis of risks of money laundering and terrorist financing related to its activities, the Company prepares a risk assessment, taking account of the following categories:

a) Customer risk;
b) Geographical risk;
c) Product risk; and
d) Delivery channel risk.

After the risk is assessed and attributed to a particular customer, depending on the degree of risk, it should be revised periodically upon knowledge of the customer and its activity.

6. AML & KYC PROCEDURES

6.1. Customer Due Diligence (CDD)

We perform Customer Due Diligence (CDD) to identify and verify the identity of all users before establishing a business relationship. The process includes:

Information Collection

- **For Individual Customers (Shareholders, Directors, UBOs, Authorized Signatories):**
- **Full Legal Name:** As it appears on government-issued identification.
- **Date of Birth:** To confirm age eligibility (e.g., minimum 18 years) and cross-reference with ID.
- **Nationality:** To assess jurisdictional risk and compliance with sanctions.
- **Residential Address:** Verified through a recent utility bill, bank statement, or government-issued document (not older than 3 months).
- **Government-Issued Identification:** A valid passport, driver's license, or national ID card with a clear photograph, name, and document number.
- **Source of Funds (SoF), if required:** Detailed information on the origin of funds, such as employment income, investment returns, inheritance, or cryptocurrency trading profits. Supporting documents (e.g., payslips, tax returns, or bank statements) may be required.
- **Cryptocurrency Wallet Address(es):** All wallet addresses used for pay-in or pay-out transactions, verified to ensure they are controlled by the customer and not linked to illicit activity.
- **Photograph or Video Verification:** A selfie or live video holding the ID document for biometric verification, where applicable.

For Entity Customers (Businesses, Trusts, or Other Organizations):

- **Legal Business Name and Registration Number:** As per the certificate of incorporation or equivalent.
- **Registered Business Address:** Verified through official documents or third-party databases.

- **Certificate of Incorporation:** Or equivalent legal document proving the entity's registration.
- **Ownership Structure:** A detailed chart or description identifying all UBOs with 25% or greater ownership or control.
- **UBO Identification:** Full KYC information for each UBO, including name, date of birth, nationality, address, and ID documents.
- **Authorized Representatives:** Identification and verification of individuals authorized to act on behalf of the entity.
- **Nature of Business:** A detailed description of the entity's activities, including industry, products/services, and primary markets.
- **Source of Funds:** Documentation proving the legitimacy of funds, such as financial statements, contracts, or bank records.
- **Cryptocurrency Wallet Address(es):** All wallet addresses used for transactions, with verification of ownership and screening for illicit activity.
- **Tax Identification Number (TIN):** Or equivalent for the entity and, where applicable, UBOs.

KYC Updates: CoiniGo must update its corporate client's KYC information every 12 months or upon significant changes (e.g., change in address, ownership, or business activities). Failure to provide updated information may result in account suspension.

Enhanced Due Diligence (EDD)

EDD is applied in higher-risk situations, including:

- Any doubts about the authenticity of client identification, documentation and verification
- Politically Exposed Persons (PEPs)
- Clients and transactions involving high-risk jurisdictions
- Unusually large or complex transactions

EDD may involve:

- **Additional Documentation:** Detailed proof of SoF/SoW, such as audited financial statements, contracts, or notarized declarations.
- **Senior Management Approval:** Required for onboarding high-risk customers or approving transactions above a certain threshold.

- **Enhanced Blockchain Analysis:** In-depth tracing of cryptocurrency flows to identify the origin and destination of funds.
- **Third-Party Corroboration:** Verification of customer information through external sources, such as business registries, tax authorities, or legal counsel.
- **Ongoing Monitoring Frequency:** Increased frequency of reviews (e.g., quarterly instead of annually) for high-risk customers.
- **Customer Interviews:** Direct communication with the customer (via video call or in-person) to clarify business activities or transaction purposes.

6. TRANSACTION MONITORING

The Company employs sophisticated transaction monitoring systems to detect and prevent suspicious activities in real-time and post-transaction. Key elements include:

- **Automated Monitoring Systems:**
  - **Blockchain Analytics Tools:** Know-Your-Transactions (KYT) tools are used to trace cryptocurrency transactions, identify wallet ownership, and detect links to illicit activities (e.g., darknet markets, ransomware, or sanctioned entities).
  - **Rule-Based Alerts:** Predefined rules trigger alerts for transactions exceeding monetary thresholds, rapid fund movements, or interactions with high-risk wallet addresses.
  - **Machine Learning Models:** Advanced algorithms analyze transaction patterns to identify anomalies that may not trigger rule-based alerts, such as subtle layering techniques.
- **Red Flags for Suspicious Activity:**
  - Transactions involving wallet addresses linked to known illicit activities (e.g., dark pools, hacking incidents).
  - Use of privacy-enhancing technologies, such as mixers, tumblers, or privacy coins, without clear justification.
  - High-value transactions inconsistent with the customer's KYC profile or stated purpose.
  - Rapid transfers across multiple wallets or exchanges within a short timeframe (indicative of layering).
  - Transactions with jurisdictions subject to sanctions, embargoes, or FATF high-risk designations.
  - Multiple accounts linked to the same individual or entity without a legitimate business purpose.

    - Transactions with no apparent economic or lawful purpose (e.g., round-tripping funds).
    - Inconsistent or incomplete KYC information provided during onboarding or updates.
- **Transaction Thresholds:**
    - Transactions exceeding $100,000 (or equivalent in cryptocurrency) trigger automatic EDD, including source of funds verification and senior management review.
    - Transactions below $100,000 are subject to standard monitoring but may trigger EDD if linked to high-risk indicators.
- **Travel Rule Compliance:** (See detailed clause 8)
    - For transactions exceeding FATF's $1,000 threshold (or local equivalent), the Company collects and shares originator and beneficiary information with other VASPs, as required by Recommendation 16. This includes:
        - Originator's name, account number (or wallet address), and physical address.
        - Beneficiary's name and account number (or wallet address).
        - Transaction amount, date, and purpose (if available).
    - The Company uses secure, interoperable protocols to exchange Travel Rule data with other VASPs.
    - Non-compliant VASPs or unhosted wallets are flagged for additional scrutiny, and transactions may be delayed or rejected until compliance is ensured.
- **Post-Transaction Analysis:**
    - Transactions are reviewed retroactively to identify patterns that may not be evident in real-time, such as gradual layering across multiple transactions.
    - Periodic audits of transaction logs ensure compliance with internal policies and regulatory requirements.
- **Escalation Process:** Alerts are escalated to the AML Compliance Officer within 24 hours of investigation. High-priority alerts (e.g., sanctions hits) are escalated immediately.

7. ONGOING MONITORING

We continuously monitor user accounts and transactions to detect and report suspicious activity. This includes:

- Real-time transaction screening
- Behavior analysis

- Risk scoring models
- Suspicious transactions are flagged and reported to the appropriate financial intelligence units (FIUs) in accordance with legal obligations.

In the event of evidence or signs of suspicious activity in the client's account, from untrusted sources and/or any actions with attributes of fraud, the Company reserves the right to conduct an internal investigation, to block or close the Customer's Account, cancel any payment and to suspend providing services.

The Company has a clear process for identifying, investigating, and reporting suspicious activities:

- **Detection:** Suspicious activities are identified through transaction monitoring, customer behavior analysis, or employee reports.
- **Investigation:** The AML Compliance Officer leads investigations, using blockchain analytics, customer interviews, and external data sources to assess the activity.
- **Reporting:** If suspicion persists, a Suspicious Activity Report (SAR) is filed with the relevant Financial Intelligence Unit (FIU) within the required timeframe. The SAR includes:
  - Customer details (name, ID, address).
  - Transaction details (amount, date, wallet addresses, counterparties).
  - Nature of suspicion and supporting evidence.
  - Any actions taken by the Company (e.g., account suspension).

  Also, please refer to *Section:11 Reportin*g for more detailed information.
- **Account Actions:** Suspicious accounts may be restricted, frozen, or terminated pending investigation. Customers are notified unless prohibited by law.
- **Law Enforcement Cooperation:** The Company responds promptly to law enforcement requests and provides all relevant records, including blockchain transaction data.
- **Confidentiality:** SAR filings and investigations are kept strictly confidential to comply with legal requirements and prevent tipping off.

8. TRAVEL RULE COMPLIANCE (FATF RECOMMENDATION 16)

CoiniGo complies with the Travel Rule as defined in FATF Recommendation 16 and implements technical and procedural safeguards to ensure required transaction information is accurately collected, verified, and transmitted when transferring virtual assets above applicable thresholds.

8.1 Applicability

This section applies to virtual asset transfers where CoiniGo acts as either the originating or beneficiary Virtual Asset Service Provider (VASP) and where the transaction amount:

- Meets or exceeds USD 1,000 (or equivalent in virtual assets), or
- Falls under any lower jurisdictional threshold applicable by local laws.

8.2 Information Requirements

Under the Travel Rule, CoiniGo collects and transmits the following data elements:

Originator Information:

- Full legal name
- Account number or wallet address
- Business registration number and jurisdiction (for legal entities)

Beneficiary Information:

- Full legal name
- Account number or wallet address

This information is collected at onboarding (KYC) and/or pre-transaction stage and is verified using reliable, independent sources.

8.3 Data Roles and Responsibilities

To maintain legal clarity under EU GDPR and applicable data protection laws, CoiniGo explicitly defines its roles in relation to data exchanged under the Travel Rule:

Entity	Role under GDPR	Description
End User	Data Subject	The end-customer initiating or receiving a virtual asset transaction
Partner Business	Data Controller	Collects and determines the purpose of KYC data; responsible for data legality and accuracy
CoiniGo (VASP Gateway)	Data Controller	Independently determines the purpose and means of processing Travel Rule data; ensures compliance and secure transmission

CoiniGo (Counter-party VASP)	Data Controller	Receives and processes Travel Rule data as an independent controller
Travel Rule Protocol (TRP)	Data Processor / Sub-processor	Acts on behalf of VASPs for secure data exchange; bound by contractual terms and confidentiality obligations

Relationship Map

Retail User

↓

Partner Business ⟶ CoiniGo (VASP Gateway) ⟶ CoiniGo (Counter-party VASP)

(Controller) (Controller) (Controller)

↘

Travel Rule Protocol (TRP): Processor or Sub-processor for each Controller

Note: CoiniGo (MetaWorld Capital sp. z o.o.) acts as both VASP Gateway and Counter-party VASP, depending on transaction direction. In both roles, it retains status as an independent Data Controller.

8.4 Secure Transmission & Interoperability

CoiniGo uses encrypted, secure APIs or protocols to transmit required Travel Rule data. All transmissions meet confidentiality and integrity requirements and ensure:

- Mutual authentication between VASPs
- Non-repudiation and traceability
- Data minimization in accordance with GDPR principles

8.5 Handling of Unhosted Wallets

For transactions involving unhosted wallets:

- CoiniGo conducts enhanced risk assessment to validate the legitimacy and intent of the transaction.

- KYC verification of the wallet owner may be required.
- Transfers may be blocked or delayed if insufficient information or risk indicators arise.

8.6 Non-Compliant VASPs or Counterparties

CoiniGo will not engage in transactions with VASPs that:

- Fail to comply with the Travel Rule,
- Do not implement equivalent AML standards, or
- Pose a high jurisdictional or sanctions-related risk.

Mitigation steps may include:

- Delaying or freezing the transaction
- Requesting additional KYC data
- Filing a Suspicious Activity Report (SAR)

8.7 Record Retention and Confidentiality

All Travel Rule-related data is:

- Retained for a minimum of five (5) years
- Stored securely in encrypted environments
- Accessed only by authorized compliance staff
- Shared with competent authorities as required under law

8.8 Sub-Processors and Data Protection

All Travel Rule Processors (e.g., TRP service providers) are contractually bound to:

- Act only on the written instructions of CoiniGo
- Ensure GDPR-compliant technical and organizational measures
- Maintain strict confidentiality and restrict subcontracting without consent.

9. RECORD KEEPING

All KYC records, including identification documents and transaction history, are retained for at least five (5) years after the termination of the customer relationship, or longer where required by law.

Records include:

- **Customer Records:** KYC documents, verification results, and correspondence.
- **Transaction Records:** Full details of pay-in and pay-out transactions, including wallet addresses, amounts, timestamps, and counterparties.

- **Compliance Records:** SARs, investigation reports, screening results, and audit trails.
- **Training Records:** Documentation of employee AML/CTF training sessions.
- **Storage and Security:**
    - Records are stored in encrypted, access-controlled databases compliant with data protection laws (e.g., GDPR, CCPA).
    - Access is restricted to authorized personnel (e.g., compliance team, senior management).
    - Backup systems ensure data integrity and availability for audits.
- **Regulatory Access:** Records are made available to regulators or law enforcement upon request, in accordance with legal procedures.

10. SANCTIONS AND WATCHLISTS

We screen all users against relevant sanctions lists, including:

- UN Sanctions Lists
- EU Sanctions Lists
- OFAC (U.S. Department of the Treasury) Sanctions administered by the Office of Financial Sanctions Implementation ("OFSI-UK")
- Sanctions imposed under the International Sanction Act.
- Local and international PEP and watchlists

11. TRAINING AND AWARENESS

Our employees and agents receive ongoing AML and KYC training, including:

- Legal and regulatory obligations
- Identification of suspicious activity
- Use of internal AML tools and procedures

12. REPORTING

In the event that CoiniGo is legally obligated to report a suspicious transaction or account to the relevant regulatory authorities in accordance with applicable Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) laws and regulations, and such authorities subsequently request additional information or documentation, including Know Your Customer (KYC) details

related to the underlying client or transaction, CoiniGo shall have the right to request such information from its merchants.

Merchants shall be required to provide, upon request and without undue delay, all relevant KYC and due diligence documentation or information they have collected in relation to the customer associated with the transaction or account in question. This may include, but is not limited to, identification documents, proof of address, source of funds declarations, transaction records, and any other information deemed necessary by the regulatory authorities.

CoiniGo will use the information provided solely for the purpose of fulfilling its regulatory obligations and, where applicable, shall transmit the requested data to the competent regulatory or supervisory authority in accordance with data protection and confidentiality requirements.

Failure to provide such information in a timely manner may result in the suspension of services, reporting to regulatory bodies, or termination of the business relationship, as deemed appropriate by CoiniGo and in accordance with its internal compliance policies.

The Company has internal procedures for the timely reporting of suspicious activity to:

- The relevant national FIU (e.g., FIU-NL, FinCEN, etc.)
- Law enforcement, where applicable
- We maintain a zero-tolerance policy towards money laundering and terrorist financing.

13. RISK-BASED APPROACH

We implement a risk-based approach (RBA) to AML compliance, ensuring resources are allocated proportionally to the level of risk presented by a customer, transaction, or geographic region.

14. THIRD-PARTY PROVIDERS

We may rely on third-party KYC/AML service providers who comply with equivalent standards and regulatory obligations. Due diligence is conducted on such providers.

15. POLICY REVIEW

This policy is reviewed at least annually or upon significant regulatory or business changes. All updates will be communicated to relevant stakeholders.