UAB CHRONOS GLOBAL

Konstitucijos pr. 26,
LT-08131 Vilnius, Lithuania
info@columis.com

OUR COMMITMENT TO ANTI-MONEY LAUNDERING (AML) AND COUNTER-TERRORIST FINANCING (CTF)

At **UAB Chronos Global**, we are committed to maintaining a secure and compliant environment for all our customers. As a Crypto Asset Service Provider in Lithuania, we operate under strict regulatory requirements to prevent money laundering, terrorist financing, fraud, and other illicit activities.

We believe transparency and trust are essential in the financial and crypto industries. Our robust AML framework ensures that our platform is safe, secure, and compliant with Lithuanian laws, European Union directives, and international best practices.

We employ a risk-based approach and cutting-edge AML measures to safeguard our platform against financial crime. This includes robust customer verification, transaction monitoring, and compliance with the Travel Rule to prevent illicit activities such as money laundering, terrorist financing, fraud, and sanctions evasion.

How We Protect Our Platform and Customers

1. Customer Due Diligence (CDD) and Know Your Customer (KYC)

Before engaging with our services, every customer undergoes a strict identity verification process to confirm their legitimacy. This includes:

- Identity verification using reliable and independent data sources.
- Collection of personal and business information for individuals and corporate customers.
- Screening against global sanctions lists and Politically Exposed Persons (PEP) databases.
- Ongoing monitoring of customer profiles to ensure continued compliance.

We apply levels of due diligence based on each customer's risk level:

- Standard Due Diligence (CDD) – Applied to all customers engaging in standard transactions.
- Enhanced Due Diligence (EDD) – Applied to high-risk customers, including those from high-risk jurisdictions, or customers engaging in complex transactions.

If a customer's risk profile changes, we may request additional information or take further steps to mitigate potential risks.

2. Compliance with the Travel Rule

We comply with the Travel Rule, as required under Regulation (EU) 2023/1113, ensuring transparency in crypto transactions. This means that:

When a customer sends or receives crypto assets, we collect, verify, and share key transaction details with the receiving or sending entity.

If a counterparty crypto service provider does not comply with the Travel Rule, we may block or reject the transaction to mitigate compliance risks.

These measures ensure that all crypto transactions meet financial transparency standards, preventing illicit fund transfers.

3. Transaction Monitoring & Suspicious Activity Reporting

We utilize advanced real-time monitoring tools to detect unusual or suspicious transactions. We use both automated and manual approaches to detect:

- High-value transactions, including those exceeding €15,000 (or equivalent in crypto):
- Unusual transaction patterns that deviate from a customer's typical behaviour.
- Transfers to or from high-risk jurisdictions.
- Transactions involving known high-risk crypto wallets or darknet-related activities.

If suspicious activity is detected, we take immediate action, including:

- Blocking transactions for further investigation.
- Filing a Suspicious Activity Report (SAR) with the Financial Crime Investigation Service (FCIS) in Lithuania.
- Requesting additional verification or documentation from customers.
- Terminating accounts that fail to meet compliance requirements.

4. Sanctions Compliance & Screening

We strictly comply with international sanctions and take proactive measures to ensure our platform is not used for illicit activities. Our system automatically screens:

- All customers and transactions against sanctions lists from the European Union (EU), United Nations (UN), United States (OFAC), United Kingdom (HMT), and Lithuanian authorities.
- Crypto transactions involving flagged or blacklisted addresses associated with financial crime.
- Business relationships involving entities or individuals from sanctioned jurisdictions.

If a sanctioned individual, entity, or transaction is identified, we:

- Immediately freeze the related account or funds.
- Report the case to the relevant authorities.

- Cooperate fully with law enforcement agencies to prevent violations.

5. Risk-Based Approach & Internal Controls

To ensure effective compliance, we implement a three-line defense model:

1. First Line of Defense – Our front-line employees ensure that AML procedures are followed during customer onboarding, transactions, and ongoing monitoring.
2. Second Line of Defense – Our Risk and Compliance teams, including the Money Laundering Reporting Officer (MLRO), oversee AML controls, investigate suspicious activity, and ensure compliance with regulatory requirements.
3. Third Line of Defense – Our independent internal audit reviews AML procedures, assesses risks and ensures the effectiveness of our compliance framework.

Our AML policy is reviewed at least annually to reflect regulatory changes, new threats, and best practices.

6. Employee Training & Awareness

We believe that knowledge is key to an effective AML program. That's why we invest in regular AML and compliance training for all employees, including:

- Mandatory annual training for all employees on financial crime risks.
- Specialized training for compliance staff and senior management.
- Real-case scenario exercises to improve detection and response to suspicious activities.
- Continuous updates on the latest AML regulations and industry developments.

7. Secure Data Collection & Retention

To comply with regulatory requirements, we securely store customer identification and transaction data for a period of:

- 8 years for customer and transaction records.
- 5 years for communication records related to compliance.

We ensure full compliance with GDPR and data protection laws, meaning your personal and financial information is kept secure and confidential at all times.

Zero-Tolerance Policy on Financial Crime

At UAB Chronos Global, we take a strict stance against money laundering, terrorist financing, fraud, and other illegal activities. We do not engage with:

- Customers from prohibited or sanctioned countries.
- Businesses with non-transparent ownership structures.
- Any activity that poses a high risk of financial crime.
- Any activity that is out of the company's risk appetite.

If a customer fails to meet our compliance standards, we reserve the right to reject or terminate the business relationship.

Building a Safe and Transparent Crypto Ecosystem

We are committed to providing a secure and compliant platform that protects our customers while supporting innovation in the crypto space.

For any inquiries regarding our AML policy or compliance measures, please contact us at info@columis.com.