# Varni Labs Sp Zoo Anti-Money Laundering (AML) Policy

## Last updated: 25 July 2024

### 1. Introduction

1.1 Overview - Varni Labs Sp. z o.o. is committed to maintaining the highest standards of compliance and integrity in our operations. Our Anti-Money Laundering (AML) and Know Your Customer (KYC) Policy outlines the procedures and measures we take to prevent the misuse of our services for money laundering and terrorist financing. This document provides comprehensive guidelines for employees, customers, and partners to ensure adherence to regulatory requirements.

1.2 Key Objectives

- Preventing Money Laundering and Terrorist Financing
- Regulatory Compliance with all applicable regulations, rules and laws
- Customer Identification and Verification

### 2. User's Obligations

2.1 Platform Usage - Compliance By accessing, or using the Platform, users acknowledge and agree that they shall not use the Platform in any manner that contravenes the Platform's Terms of Service, Privacy Policy, AML Policy, or any applicable law. By using, or accessing this Platform, users agree and consent to any change made by Us without any notice.

2.2 Accuracy of Information - Users acknowledge and agree that any and all information submitted to Us during the use of the Platform is true, accurate, and complete. All such rendered information/Identification Documents must belong to the user submitting the information/Identification Document.

2.3 Notification of Changes In case of any change of address, users must notify and file a fresh proof of address

2.4 Prohibited Activities Users shall not engage in or conduct any Suspicious Transaction or Money Laundering activity or engage with any person on the Sanctions List. The Sanctions List refers to lists of natural and juridical persons included under any list by any country, government, or international authority, including the US Department of the Treasury's Office of Foreign Assets Control ("OFAC"), the European Union, or the Monetary Authority of Singapore and relevant applicable laws. "Suspicious Transaction" means a transaction, including an attempted transaction, whether or not made in cash, which to a person acting in good faith:

- Gives rise to a reasonable ground of suspicion that it may involve proceeds of an offense specified under the Anti-Money Laundering laws, regardless of the value involved; or

- Appears to be made in circumstances of unusual or unjustified complexity; or
- Appears to have no economic rationale or bona fide purpose; or
- Gives rise to a reasonable ground of suspicion that it may involve financing of activities related to terrorism.

2.5 Account Restrictions - At Our sole discretion, we may block, restrict, or terminate access to any user's account if it is found that the user is engaged in or is suspected of engaging in illegal activities.

**3. Customer Due Diligence (CDD)**

3.1 Identity Verification To establish a business relationship with Varni Labs, customers must undergo a comprehensive identity verification process. This includes (not exclusive):

- Full name, residential address, date of birth, and nationality.
- Series and number of the document confirming the identity;
- Proof of address (e.g., utility bill, bank statement etc.).

3.2 Business Entity Customer Identification To enter into a business relationship with Varni Labs, business entities must provide the following information (not exclusive):

- Name (business name) and organizational form.
- Address of the registered office (country, city with zip code, street with no. of premise).
- Tax Identification Number (TIN).
- Commercial registration number and name of the commercial register.
- Date of registration.
- Identification data of the natural person representing the entity, including full name, date of birth, nationality, and government-issued ID.

3.3 Verification of Legal Status Varni Labs verifies the legal status of the business entity through relevant documents, such as:

- Excerpt from the Commercial Register.
- Founding documents (e.g., Certificate of Incorporation, Memorandum & Articles of Association).
- Shareholder structure and register.
- Directors register and authorized signatory list.

3.4 Identification of Beneficial Owner Varni Labs takes measures to identify and verify the beneficial owners of the business entity. This includes:

- Obtaining the necessary information to identify the natural persons who ultimately own or control the entity.
- Using reliable sources and documents to verify the identity of the beneficial owners.

3.5 Ongoing Monitoring Continuous monitoring of customer transactions is essential to detect and report suspicious activities. Varni Labs employs the following measures:

- Regular transaction reviews.
- Updating customer information periodically.
- Utilizing automated systems for real-time transaction monitoring.

**4. Risk-Based Approach**

4.1 Customer Risk Categorization: Varni Labs categorizes customers into three risk levels: low, medium, and high. This categorization determines the extent and frequency of due diligence measures.

4.2 Enhanced Due Diligence (EDD): For high-risk customers, Varni Labs implements additional measures to mitigate potential risks:

- Detailed background checks.
- Verification of the source of funds.
- Continuous transaction monitoring.

**5. Prohibited Relationships**

5.1 Criteria for Prohibited Relationships: Varni Labs refrains from establishing or maintaining business relationships with individuals or entities that:

- Refuse to provide necessary information.
- Use aliases or false identities.
- Are identified as shell banks or on sanctions lists.
- Are suspected of money laundering or terrorist financing.

**6. Politically Exposed Persons (PEPs)**

6.1 Definition and Identification: Varni Labs exercises heightened scrutiny for customers who are Politically Exposed Persons (PEPs) and their immediate family members or close associates:

- Enhanced due diligence measures.
- Ongoing monitoring of transactions.

**7. Enhanced Security Measures**

7.1 Higher Risk Situations: Varni Labs undertakes enhanced security measures in cases of higher risk of money laundering or terrorist financing. These measures include:

- Additional documentation and information from high-risk customers.
- Verification of the customer's wealth and source of funds.
- Increased monitoring and scrutiny of high-risk transactions.

**8. Monitoring Ongoing Business Relationships**

8.1 Continuous Monitoring: Continuous monitoring of business relationships is crucial to ensure compliance with AML regulations. Varni Labs implements the following measures:

- Regular reviews of customer transactions and activities.
- Periodic updating of customer information and risk assessments.
- Identifying and investigating unusual or suspicious activities.

**9. Screening of Transactions**

9.1 Transaction Screening: Procedures Varni Labs conducts thorough screening of all customer transactions to detect and prevent suspicious activities. This includes:

- Real-time transaction screening using automated systems.
- Retrospective analysis of past transactions.
- Enhanced scrutiny of transactions involving high-risk countries or entities.

**10. Reporting and Record-Keeping**

10.1 Reporting Suspicious Activities: Varni Labs adheres to strict reporting and record-keeping requirements:

- Suspicious Activity Reports (SARs): Any suspicious transactions are reported to the relevant authorities promptly.

10.2 Maintaining Records: Varni Labs maintains detailed records of all customer information and transactions for a minimum of five years. This includes:

- Copies of identification documents and verification records.
- Transaction records and related documentation.
- Reports of suspicious activities and actions taken.
- The personal data collected for AML/CFT purposes is recorded in accordance with the Varni Labs Privacy Policy.

**11. Training and Awareness**

11.1 Employee Training Programs: All employees receive regular training on AML and KYC policies and procedures to ensure they can identify and prevent potential risks. Training programs cover:

- Understanding AML/KYC regulations.
- Identifying and reporting suspicious activities.
- Customer due diligence and risk assessment procedures.

**12. Internal Controls and Audit**

12.1 Ensuring Compliance: Varni Labs implements robust internal controls to ensure compliance with AML regulations:

- Regular audits of AML procedures.
- Continuous improvement of internal controls based on audit findings.

**13. Non-Retaliation Policy**

13.1 Encouraging Reporting: Employees are encouraged to report any concerns or violations without fear of retaliation. Reports can be made anonymously if preferred. Varni Labs is committed to protecting whistleblowers and ensuring their concerns are addressed appropriately.

**14. Exclusion of Business Relations**

14.1 High-Risk Countries: Varni Labs does not enter into business relationships with customers from high-risk third countries identified by the Financial Action Task Force (FATF) or the European Commission as having strategic deficiencies in their AML/CFT regimes.

**15. Conclusion**

15.1 Commitment to Compliance Upholding these standards is fundamental to maintaining the trust and reputation of Varni Labs. All employees, contractors, and associated parties are expected to adhere to these principles at all times. For more detailed information, please refer to the full AML Policy document or contact the AML Officer.