TrustyFi Compliance Program Overview

INTRODUCTION

PULSTECH d.o.o. (**"TrustyFi"**) maintains a strict stance against money laundering, financing of terrorism, and any other illicit activities. TrustyFi is dedicated to implementing policies, procedures, and controls that adhere to the highest industry standards and the most effective anti-money laundering and counter-terrorist financing (**"AML/CTF"**) measures. Established standards are applicable to all TrustyFi's Users and all persons associated with TrustyFi, including directors, staff members, contractors, and consultants, without any exceptions.

The objective of this TrustyFi Compliance Program Overview is to offer the Company's partners, clients, vendors, contractors, employees, regulators, law enforcement authorities, and other relevant stakeholders a high-level overview of the Company's AML/CTF compliance framework and its associated procedures (jointly referred to as the **"Compliance Program"**). It's important to note that this TrustyFi Compliance Program Overview does not encompass the comprehensive set of policies, procedures, and controls established by the Company to prevent money laundering, the financing of terrorism, and other forms of illicit activities and is provided for information purposes only.

TrustyFi is operated by PULSTECH d.o.o., a Slovenian-based legal entity headquartered at Stegne 3, Ljubljana, 1000 Slovenia and authorised to provide virtual currency services according to the decision on entry into the Slovenian register of virtual currency service providers number: 46018-30/2023-16 (41-02) dated 7/25/2023. The Slovenian register of authorised virtual currency service providers can be reached via the web page of the Office of the Republic of Slovenia for the Prevention of Money Laundering.

Being a regulated entity TrustyFi (i) is required to comply with the applicable anti-money laundering and terrorist financing legislation, including but not limited to the Slovenian Act on Prevention of Money Laundering and Financing of Terrorism (ZPPDFT-2), Restrictive Measures Introduced or Implemented by the Republic of Slovenia in accordance with Legal Acts and Decisions Adopted within International Organisations Act (ZOUPAMO), FATF recommendations, handbooks and guidelines, and (ii) is obligated to establish effective internal procedures and mechanisms to counteract money laundering and terrorist financing (**"ML/FT"**).

Capitalised terms not defined in this TrustyFi Compliance Program Overview shall have the meaning as defined in TrustyFi's General Terms.

This TrustyFi Compliance Program Overview outlines:

- Tasks and obligations toward preventing money laundering and terrorist financing;
- Internal controls and procedures;
- User identity verification procedures;

- The role of the Anti-Money Laundering Compliance Officer (the **"AMLCO"**);
- Transactions monitoring and risk assessment;
- Reporting and record-keeping;
- Sanctions;
- Politically Exposed Persons**;**
- Restricted countries and territories.

TASKS AND OBLIGATIONS TOWARDS PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING

For the purposes of detecting and preventing money laundering and terrorist financing, TrustyFi performs the following tasks when performing its activities:

- Creates an assessment of the risk of money laundering and terrorist financing;
- Establishes policies, controls and procedures to effectively mitigate and manage the risks of money laundering and terrorist financing;
- Implements of measures to get to know the customer (customer review);
- Communicates prescribed and required information and submits documentation to the Office of the Republic of Slovenia for the Prevention of Money Laundering;
- Appoints the AMLCO as well as his deputy, and ensures the conditions for their work;
- Takes care of regular professional training of employees and ensures regular internal control over the performance of tasks;
- Prepares a list of indicators for identifying customers and transactions in relation to which there are reasons to suspect money laundering or terrorist financing;
- Ensures the protection and storage of data and manages the records prescribed by the law;
- Performs other tasks and obligations based on the Act on Prevention of Money Laundering and Financing of Terrorism (ZPPDFT-2) and the regulations adopted on its basis.

TRUSTYFI'S INTERNAL CONTROLS AND PROCEDURES

TrustyFi has established and put into practice internal controls and procedures designed to efficiently address and handle risks associated with money laundering and terrorist financing. These risks are identified through a risk assessment aligned with TrustyFi's risk-based approach.

USER IDENTITY VERIFICATION

According to the Act on Prevention of Money Laundering and Financing of Terrorism (ZPPDFT-2), TrustyFi is obliged to verify the identity of its Users prior to performing any transactions. User identification is performed in the following cases:

- Before entering into a business relationship with a User;
- In the case of any transaction with a value exceeding EUR 15,000, whether carried out individually or by means of several transactions which are clearly linked to each other;
- In case of any occasional (without previous business relations) transaction that involves the transfer of funds and exceeds EUR 1,000;
- Where there are doubts as to the authenticity and relevance of information previously obtained about the User or the beneficial owner of the User;
- Whenever there are grounds for suspecting money laundering or terrorist financing in relation to the transaction, the User, the funds or the assets, irrespective of the value of the transaction;
- In other cases subject to TrustyFi's absolute discretion.

During the identification and verification process, TrustyFi may require the Users to provide supporting documents proving the information provided.

TrustyFi needs to unequivocally establish the User's true identity as a legitimate natural or legal entity. While TrustyFi may occasionally utilise third-party sources for fact-checking during User onboarding, TrustyFi holds full legal responsibility for ensuring the checks meet the required standards.

All User identification information will be collected, stored, shared, and safeguarded confidentiality and in strict compliance with TrustyFi's Privacy Notice and the associated regulations in alignment with GDPR requirements.

ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

The AMLCO is an appointed person responsible for implementing and performing the anti-money laundering and 'Know Your Client' (**"AML/KYC"**) procedures, transaction monitoring, mitigating ML/FT risks and performing AML/CFT duties and obligations of TrustyFi. AMLCO is also responsible for staff training, reporting suspicious transactions to the authorities and ensuring TrustyFi's overall compliance with applicable AML/CFT law.

Please do not hesitate to contact the AMLCO in case of any ML/TF concerns connected with TrustyFi via: info@trustyfi.com.

TRANSACTION MONITORING

TrustyFi constantly monitors the Users' accounts and transactions for suspicious activity, illegal transactions or other issues. TrustyFi may employ higher or lower levels of scrutiny when monitoring the Users' transactions based on its risk assessment and risk appetite arrangements.

Based on the transaction monitoring TrustyFi may perform additional checks, require additional information from the Users and in some cases suspend any transactions and the provision of Services.

RISK ASSESSMENT

TrustyFi applies a risk-based approach when performing the AML/KYC procedures in order to assess particular risks and attribute them to each of TrustyFi's Users. The risk-based approach uses several criteria such as:

- Customer risk;
- Geographical risk;
- Product risk; and
- Delivery channel risk.

Risks are assessed and revised periodically. Based on the results of the risk assessment, TrustyFi may request further information or documents from the User, deny the provision of the Services, suspend access to the Platform and take further actions according to the applicable law.

REPORTING AND RECORD-KEEPING

Under applicable law, TrustyFi may be required to and will report all suspicious transactions and other reportable issues to the Slovenian Office for Money Laundering Prevention or other authorities.

Under applicable law, TrustyFi is required to retain and provide to the responsible authorities certain documents and information about its Users and their transactions for extended periods of up to 10 years after the termination of the business relationship with the User. Such information will not be deleted at the Users' request.

SANCTIONS

TrustyFi is prohibited from transacting with persons, entities and bodies under international sanctions. TrustyFi screens all its Users against the lists of applicable sanctions as well as analyses the subject matter of transactions to ensure compliance with international sanctions. Any sanction screening match is escalated to the AMLCO for further action. TrustyFi will not perform any transaction in case it assumes or suspects that a risk of breaching applicable sanctions is associated with it.

POLITICALLY EXPOSED PERSONS (PEP)

TrustyFi realises that due to the possibility of abusing their public office for private gain, PEPs are required to be subject to enhanced scrutiny. Therefore, TrustyFi screens all its Users against the PEPs lists and considers the possibility of establishing business relationships with such persons by assessing the associated risks and determining appropriate due diligence measures. In some cases, TrustyFi may be prohibited from providing the Services to PEPs.

RESTRICTED COUNTRIES AND TERRITORIES

TrustyFi does not offer or provide its Services to individuals residing and entities registered in countries and territories that:

- Have been identified by international organisations as having a high risk of money laundering;
- Have been sanctioned by the UN, the EU, the government of Slovenia or other body;
- Consider TrustyFi's services unlawful and have officially prohibited them;
- Other countries or territories TrustyFi deems high-risk or is not ready to provide services in for other reasons.

TrustyFi reserves its right to, at its absolute discretion, amend the list of restricted countries and territories list at any time.