AML COMPLIANCE NOTICE

Last updated on 01.11.2025

INTRODUCTION

Datalink sp. z o.o. (**“Trustyfi”, “Company”**) maintains a strict stance against money laundering, financing of terrorism, and any other illicit activities. Trustyfi is dedicated to implementing an internal control system that includes 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 apply 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 AML Compliance Notice 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 **“AML Compliance Notice”**). It's important to note that this Trustyfi AML Compliance Notice 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 Datalink sp. z o.o., established and existing under the laws of the Republic of Poland, registration number 0001124387, a duly authorized Virtual Assets Service Provider, which maintains its principal place of business at ul. Hoża 86, apt. 210, Warsaw 00-682, Poland, VASP authorization number: RDWW-1491. The Register can be reached here.

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 Republic of Poland Act of 1 March 2018 on counteracting money laundering and financing of terrorism, 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 AML Compliance Notice shall have the meaning defined in Trustyfi’s Terms of Service.

This Trustyfi AML Compliance Notice outlines:

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

- The role of the Company’s Money Laundering Reporting Officer (“MLRO”);
- Transactions monitoring and risk assessment;
- Reporting and record-keeping;
- Sanctions;
- Politically Exposed Persons**;**
- Restricted countries and territories.

TASKS AND OBLIGATIONS TOWARD PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING

To detect and prevent 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 measures to get to know the customer (customer review);
- Communicates prescribed and required information and submits documentation to the Financial Crime Investigation Unit of the Republic of Poland;
- Appoints the MLRO 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 concerning 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 Republic of Poland Act of 1 March 2018 on counteracting money laundering and financing of terrorism and the regulations adopted on its basis.

TRUSTIFY’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 Republic of Poland Act of 1 March 2018 on counteracting money laundering and financing of terrorism, Trustyfi is obliged to verify the identity of its Users prior to performing any transactions. User identification is performed in the following cases:

- Establishing a business relationship with a User;
- In the case of any transaction, irrelevant to its value;
- In case of any occasional (without previous business relations) transaction, regardless of its value;
- 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 during the identification and verification process.

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.

In some cases, for example, when the transaction amount exceeds Trustyfi's internal limits, the User's actions are suspicious or their purpose is unclear, or the User's risk level has increased, Trustyfi may, at its own discretion, ask the User to pass additional verification procedures and provide additional details or documents.

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

ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

The MLRO 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. MLRO 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: support@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 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 risk assessment results, 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 Polish Financial Crime Investigation Unit.

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 MLRO for further action. Trustyfi will not perform any transaction if it assumes or suspects that a risk of breaching applicable sanctions is associated with it.

POLITICALLY EXPOSED PERSONS (PEPs)

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 JURISDICTIONS

Trustyfi does not offer or provide its Services to individuals residing in or 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 Poland, or another 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.

You may find a full list of restricted jurisdictions on our website.