AML Policy

Anti-Money Laundering Policy (AML Policy)

Money laundering is defined as the process where the identity of the proceeds of crime is so disguised that it gives an impression of legitimate income. Criminals specifically target financial services firms through which they attempt to launder criminal proceeds without the firms' knowledge or suspicion.

In response to the scale and effect of money laundering, the European Union has passed Directives designed to combat money laundering and terrorism. These Directives, together with regulations, rules and industry guidance, form the cornerstone of our AML/CTF obligations and outline the offenses and penalties for failing to comply.

General provisions
This Anti-money Laundering Policy (hereinafter referred to as "AML Policy") outlines the procedures and mechanisms used by STEX for the purpose of preventing money laundering. STEX adheres to the following policies:

- not entering into business relationships with criminals and/or terrorists;
- not processing transactions that are result from criminal and/or terrorist activities;
- not facilitating any transactions related to criminal and/or terrorist activities.

Definitions:

Money Laundering – is a set of activities with the property aimed to:
conceal the nature, source, location, disposition, movement, right of ownership or other rights related to such property; convert, transfer, acquire, possess or use such property for the purpose of concealing the illicit origin of property; assisting a person involved in criminal activity to evade the legal consequences of his or her action; participation in, association to commit, attempts to commit and facilitating the commission of illegal actions.

Terrorist Financing – acts of financing of terrorism as defined in § 2373 of the Penal Code of Estonia.

International Sanctions – list of non-military measures decided by the EU, the UN or Estonian government, which is aimed to maintain or restore peace, prevent conflicts and follow the rule of law, human rights and international law.

Compliance Officer or CO – representative appointed by the Management Board responsible for the compliance with the Rules & serving as contact person of the FIU.

FIU - Financial Intelligence Unit of the Police and Border Guard Board of Estonia.

Business Relationship – a relationship of the Service Provider with the Client.

Transaction – cash flow or payment order or cryptocurrency wiring form a Client to the Provider of service.

Client – a natural or legal person using services of Service Provider.

Beneficial Owner – is a natural person, who:

Exercises control over a transaction, Owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest, Holds the position of a senior managing official, if, the person specified in clause above cannot be identified, In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership.

Politically Exposed Person or PEP - is a natural person who is or who has been entrusted with prominent public functions.

Equivalent Third Country – a country, which is not a Member State of European Economic Area but applying an equivalent regime to the EU corresponding (AML) framework.

Virtual currency - a value represented in the digital form, which is digitally transferable / tradable, and which persons accept as a payment instrument, but that is not the legal tender of any country or funds.

Customer Due Diligence (CDD)- identification and verification of the identity of the client and any beneficial owner of the client, as well as obtaining information about the objectives of the intended nature of the business relationship.

Advanced Customer Check (EDD - Enhanced Due Diligence) - an additional measure customer due diligence to be applied if:

- the client was not physically present during identification;
- the client is a Politically Exposed Person;
- or in any other situation that, by its nature, may pose a higher risk of money laundering or terrorist financing;
- **Know Your Customer** (KYC);
- **Money Laundering Regulations** (MLR).

Transaction - customer asset management. The transaction is performed through the customer account.

Risk Client Profile - an illustration of the risks and threats that may be encountered by an organization when working with the Client. This may include the probability of negative consequences and a plan of potential costs and the level of violation for each risk. It is in the company's best interest to be proactive when it comes to its risk management systems. Some risks can be minimized if properly taken into account. Compliance with risk accounting

requirements ensures that the company and its employees comply with regulatory and ethical processes.

Accounting system - the company's internal electronic system for storing information on customers.

Proof address – utility bill, property tax receipt and etc.

The Service Provider' activities description:
The Service Provider offers services of exchanging of virtual currencies against virtual currencies, a virtual currency against a fiat currency, and vice versa.
The Service Provider is a subject to authorisation by the FIU.

Compliance Office
The MB shall appoint a CO to monitor the compliance with the Rules & relevant laws, compile & keep updated the data regarding countries with low tax risk, high and low risk of Money Laundering and Terrorist Financing and economic activities, instruct the Representatives, report to the MB on compliance with the Rules, process the data on suspicious activities, report to the FIU on events of suspected ML or TF, respond to FIU enquiries; make proposals on remedying deficiencies.
Tasks of the CO can be performed by a department.

Application of due diligence measures
The Service Provider shall determine and take due diligence (DD) measures using results of conducted risk assessment / provisions of national risk assessment, published on the web-page of the Ministry of Finance of Estonia.

DD measures shall include the following procedures:

Identifying the Client and verifying its identity, including e-identifying, Identifying and verifying the Client's representative and the right of representation, Identifying the Client's Beneficial Owner, Assessing and obtaining information on the purpose of the Business Relationship and the Transaction, Conducting ongoing DD on the Client's business to ensure the Transactions being carried out are consistent with the Provider of service's knowledge of the Client and its source of funds, Obtaining information whether the Client is a PEP or PEP's family member / close associate.

To comply with the DD obligation, the Representatives shall have the right and obligation to:

request appropriate identity documents to identify the Client and its representatives, reguest Proof address, request documents and information regarding the Client's activities / legal origin of funds, request information about Beneficial Owners of a legal person, screen the risk profile of the Client/Transaction, assess the risk whether the Client or another person linked with the Transaction may become involved in ML or TF, re-identify the Client / its representative, in case of any doubts regarding the correctness of the information, refuse to participate in or carry out the Transaction if there is any suspicion that the Transaction is linked with ML or TF, or that the Client / another person linked with the Transaction could be involved in ML or TF.

The objective of the continuously applied DD measures is to ensure on-going monitoring of Clients and Transactions.
Updated data shall be recorded in the Provider of service's Client database.

Identification of a person:

Upon implementing DD measures the following person shall be identified:

Client – a natural or legal person, Representative of the Client – an individual who is authorized to act on behalf of the Client; · Beneficial Owner of the Client, PEP – if the PEP is the Client or a person connected with the Client.

Upon establishing the relationship with the Client and when carrying out a Transaction, the Service Provider shall identify and verify the Client while being present at the same place as the Client or by using information technology means.

For identification of a Client and verification of the identity of a Client by using information technology means, the Provider of service shall use:
a document issued by the Republic of Estonia for the purpose of digital identification; · another electronic identification system within the meaning of the Regulation (EU). If the Client is a foreign national, the identity document issued by the competent authority of the foreign country is also used simultaneously. The documents to be used for identification: https://www2.politsei.ee/en/teenused/inquiries/
Documents that can be used for identification:
Personal ID card (whether ID card, e-resident card or residence permit card), passport or diplomatic passport.

Legal person and its passive legal capacity shall be identified and verified on the basis of an extract of a registry card of commercial register, foreign legal persons shall be identified on the basis of an extract of the relevant register / a transcript of the registration certificate / an equal document issued not earlier than six months before submission.

The following data shall be recorded:

For a natural person:

1. Name of the Client; 2. Personal identification code (in case of absence the date and place of birth and place of residence) 3. Information regarding identification and verification of the right of representation.

For a legal person:

1. Name of the Client 2. Registry code (or registration number and registration date) of the Client 3. Names and authorisations of members of the Management Board or the head of branch or the other relevant body.

Verification Procedures

STEX shall establish its own procedures for determining compliance with the anti-money laundering standards and Know Your Customer (KYC) policy.

STEX Customers complete a verification procedure (they must provide an identification document issued by the state: passport or an ID card). STEX reserves the right to collect Customers' identification information for AML Policy purposes. This information is processed and stored strictly in accordance with the STEX Privacy Policy.

STEX may also request a second Customer identification document: a bank statement or utility bill no older than 3 months, which includes the Customer's full name and current address.

STEX shall verify the authenticity of documents and information provided by Customers and reserves the right to request additional information on Customers who have been identified as dangerous or suspicious.

If the Customer's identification information has been changed or their activity appears suspicious, STEX is entitled to request updated documents from the Customer, even if they have been authenticated in the past.

Anti-Money Laundering Officer

The Anti-Money Laundering Officer is a STEX employee who is responsible for ensuring compliance with the AML Policy, such as:

- collection of Customers' identity information;
- establish and update internal policies and procedures for creating, reviewing, submitting and storing all reports required in accordance with existing laws and regulations;
- transactions monitoring and analysis of any significant deviations from the Customers' usual activities;
- the introduction of a records management system for storing and retrieving documents, files, forms and logs;
- regularly update risk assessments.

An Anti-Money Laundering Officer has the right to engage with law enforcement agencies that lead with the prevention of money laundering, financing of terrorism and other illegal activities.

Transactions Monitoring:

In order to screen out suspicious or unusual Transactions and the purpose and actual substance of a Transaction, the Representative can take the following actions:
ask the Client to provide (additional) information about the professional or economic activities, ask the Client explanations about the reasons for the Transaction and documents evidencing the origin of the assets and/or source of wealth, being particularly attentive to Transactions, which are linked with natural or legal persons, whose country of origin is a state, wherefrom it is particularly difficult to receive information about the Client and/or

transactions with persons, who originate from such states, which do not contribute sufficiently int prevention of ML.

If it is necessary to obtain additional documents or information from the Client on the source of virtual assets, a request is sent to the Client.

The monitoring of the Customer's transactions and the analysis of the obtained data is also a tool for risk assessment and the detection of suspicious transactions. If money laundering is suspected STEX shall monitor all transactions and reserves the right to:

- reporting of suspicious transactions to the relevant law enforcement agencies;
- request the Customer to provide any additional information and documents;
- suspend or terminate the Customer's Account.

The above list is not exhaustive. The AML Policy Compliance Officer monitors the Customers' transactions every day to determine whether to report them and treat them as suspicious.

Risk assessment

In accordance with international requirements, STEX applies a risk-based approach to anti-money laundering and financing of terrorism. Thus, measures aimed at the prevention of money laundering and financing of terrorism are commensurate with the identified risks, allowing resources to be effectively dedicated. Resources are used on a priority basis; the greatest attention is given to the greatest risks.

The Representative will establish a risk profile of a Client based on information gathered under the Rules.

For search regarding financial sanctions imposed against a person please refer to: https://www.sanctionsmap.eu/#/main

Assessment of risk profile of natural persons:

When establishing the risk category of a Client being a natural person, the country of residence of the Client, the beneficiaries of the Transaction, the region where the Client operates, and status of PEP shall be taken into account.

Assessment of risk profile of legal persons:

When establishing the risk category of a legal person, assessment shall be based on the country of location of the legal person, its area of activity, the transparency of ownership structure and the management.

Suspicious and unusual Transactions and Transactions with characteristics of ML and TF.

The Representative shall decide whether a Transaction is unusual, having regard to the entire information known about the Client and the Transaction.

Upon assessing a Transaction, it is necessary to establish whether the unusual circumstance or change is understandable / whether the Transaction has characteristics pointing to ML or TF.

Any Transactions and activities of Clients, which have no clear economic or legal reason, and which cannot be considered normal economic activity of a Client shall be regarded as suspicious.

Among other aspects, particular attention must be paid to the following Transactions/circumstances:

Client makes single and/or consecutive large Transactions outside the schedule,a third person makes payments on behalf of the Client, Exists any of characteristics of suspicious transactions as provided by guidelines of FIU.

In all the cases referred to above, the Client shall be asked for explanation and necessary documents evidencing of the legal origin of the funds.

Prior to beginning a cooperation with a client, an initial verification of clients shall take place, the questionnaire form is to be filled on the site, and the identification document (passport, ID card) is to be provided. Passports and ID cards shall be checked via the sources described in the procedure.

Prohibited Transactions

- The Client does not have sufficient authorisations to carry out the Transaction, or the authorisations are unclear;
- The Client's need to carry out the Transaction has not been reasonably justified;
- The management, ownership and control structure of the Client being a legal person is unclear and/or it is structured in an unreasonably complicated way from the economic point of view, or it has changed frequently without justification;
- Economic activities of a legal person or its accounting or payment practices are not transparent;
- The Client may be a fictitious company or a fictitious person;
- The Beneficial Owner of the Client being legal person cannot be established;
- The Client being a legal person uses an agent or another legal person as its representative without clear authorisations (i.e. during pre-contract negotiations);
- The Client or the representative of the Client refuses to provide information for the purposes of establishing the substance of the Transactions and assessment of the risks;
- The Client has not presented sufficient data or documents to prove legal origin of the assets and funds, after having been asked to do so;
- The Client, the Beneficial Owner of a Client being a legal person, or another person associated with the Client is or has been linked with organised crime, ML or TF;

- The Client, the Beneficial Owner of a Client being a legal person, or another person associated with the Client is or has been linked with traditional sources of income of organised crime;
- International Sanctions are being applied against the Client, the Beneficial Owner of a Client being a legal person, or another person associated with the Client;
- The Client has nominee shareholders or shares in bearer form.