KYC / AML / CTF POLICY

INTRODUCTION

This is a short version of our AMP Policy and procedure, which TimaxPay applies to its services. Timax-Art Consulting OÜ is a company, established under the laws of Estonia and we follow two internal procedures:

- AML procedure for providers of a service of exchanging a virtual currency against a fiat currency;
- AML procedure for Providing a virtual currency wallet service

The procedures are monitored by the compliance Officer and his team. They monitor the compliance of the Rules with the relevant laws and compliance of the activity of the Representatives with the procedures established by the Rules.

TimaxPay is available **only to EU member states based customers**, which means all the deposits coming to our bank account will be **from EU member states only.** As per definition from our AML policy we do not work with offshore banks and shell banks or with any country listed as “High risk”.

Due to the regulations established by the money laundering and terrorism financing prevention legislation we do not provide Services to (by ordering Services you confirm that you do not qualify):

- politically exposed persons;
- persons included in the international sanctions list (https://www.sanctionsmap.eu/#/main);
- residents of high risk third countries (http://www.fatf-gafi.org/countries/#high-risk).

Estonian Cryptocurrency Exchanges are defined in the Estonian law as Providers of Alternative Means of Payment, licensed as an Estonian Financial Institution by holding a Financial Activity License from the Estonian Financial Intelligence Unit (FIU), which is the Anti Money Laundering (AML) authority in Estonia with the ability to grant, revoke and supervise Financial activity licenses. The AML and KYC

requirements of the service providers are subject to are set forth in the Estonian Money Laundering and Terrorist Financing Act and other legal guidelines given by the Estonian Minister of Finance.

A cardinal part of the licensing procedure, and a significant FIU consideration for granting licenses is the quality of the Rules of Procedures which according to the Act, must be meticulously drafted by the license applicant. These Rules of Procedure must comply with the Estonian law's various requirements, which require them, among other things, to include specification of customer due diligence measures the company intends to take, assessment of money laundering risk, the manner of the collection and keeping of records, internal control rules, etc.

Timax-Art Consulting OÜ has been issued operating licenses by the Financial Intelligence Unit for:

- Providing services of exchanging a virtual currency against a fiat currency: License FVR000293
- Providing a virtual currency wallet service : License FRK000250

Given the above, TimaxPay aims to be fully compliant and transparent especially when it comes to AML /CTF (Counter-Terrorist Financing)

TimaxPay has implemented protection measures, which protect TimaxPay from involvement in money laundering or suspicious activity by the following:

- Performing an enterprise-wide risk assessment to determine the risk profile of the Company.
- Establishing AML / CTF policies and procedures.
- Implementing internal controls throughout its operations that are designed to mitigate risks of money laundering and terrorism financing.
- Performing know your customer ("KYC") procedures on all users and clients.
- Designating a Compliance Officer with full responsibility for the AML / CTF Program.
- Conducting an periodic AML audit.

- Providing AML training to its employees.

DUE DILIGENCE MEASURES

1. Identifying the Client and verifying its identity using reliable, independent sources, documents or data, including e-identifying;
2. Obtaining proof of address, such as a copy of a utility bill or bank statement from the account holder;
3. Identifying and verifying of the representative of the Client and the right of representation;
4. Identifying the Client's Beneficial Owner / Shareholders;
5. Assessing and, as appropriate, obtaining information on the purpose of the Business Relationship;
6. Conducting ongoing Due Diligence on the Client's business (legal persons) to ensure the Provider of services knowledge of the Client and its source of funds is correct;
7. Obtaining information whether the Client is a PEP or PEP's family member or PEP's close associate;
8. The Provider of service shall establish the source of wealth of the Client, where appropriate;
9. Risk assessment according to Risk categories and a List of risk countries* and application of additional due diligence measures.

Documents used in opening an account relationship must be verified prior to establishing the account. TimaxPay shall:

1. Request appropriate identity documents to identify the Client or its representatives;
2. Request documents and information regarding the activities of the Client and legal origin of funds;
3. Request information about Beneficial Owners / shareholders of a legal person;
4. Screen the risk profile of the Client, select the appropriate Due Diligence measures, assess the risk whether the Client is or may become involved in Money Laundering or Terrorist Financing;
5. Re-identify the Client or the representative of the Client, if there are any doubts regarding the correctness of the information received in the course of initial identification;

6. Annual review of a Client being a legal entity is carried out regularly once a year;
7. No entering into Business Relationships with anonymous Clients.

RISK CATEGORIES AND RISK ASSESSMENT

The risk is divided to **3 categories**:

RISK	**NORMAL**	**HIGHER** (High 1)	**THE HIGHEST** (High 2)
WHEN	The risk level is normal, there are no high risk characteristics present.	1. The place of residence or employment or business of a Client is in a country, which is included in the list of risk countries. 2. The Client is local PEP or a person. associated with a PEP 3. The legal person registered in the European Economic Area or in Switzerland, whose area of activity is associated with enhanced money-	1. The Client is suspected to be or to have been linked with a Financial offence or other suspicious activities 2. The Client is a non-resident individual, whose place of residence or activities is in a country, which is listed in the list of risk countries 3. The representative or the Beneficial Owner / Shareholders of a legal person is a PEP

		laundering risk. 4. The legal person is situated in a country, which is listed in the list of risk countries. 5. The legal person is a non-profit association, trust, civil law partnership or another contractual legal arrangement, whose activities and liability are insufficiently regulated by law, and the legality offinancing of which is not easy to screen. 6. The representative or the Beneficial Owner / Shareholder of a legal person is a local PEP or his / her family member.	or his or her family member 4. There is information that legal person is suspected to be or to have been linked with a financial offence or other suspicious activities 6. A legal person registered outside the European Economic Area, whose Meld of business is associated with a high risk of Money Laundering, or registered in a low tax rate country**.

⇩ ⇩ ⇩

	SIMPLIFIED	NORMAL	ENHANCED

	due diligence (Section 8)	**due diligence** (Section 6)	**due diligence** (Section 9)
WHEN	– A company listed on a regulated market that is subject to disclosure requirements consistent with European Union law; – a legal person governed by public law founded in Estonia; – a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area; – an authority of the European Union; – a credit institution or a financial institution, acting on behalf of itself, located in a contracting state of the European Economic	– Upon establishing a new Business Relationship; – In the event of insufficiency or suspected incorrectness of the documents or information gathered previously in the course of carrying out DD measures; – Upon suspicion of Money Laundering or Terrorist Financing.	The risk level of the Client is higher: – The Client is a person associated with a PEP – The Client is PEP or local PEP – The actual place of residence or employment or business of a Client is in a country, which is included in the list of risk countries – the Client is suspected to be or to have been linked with a financial offence or other suspicious activities – The Client is a non-resident individual, whose place of residence or activities

	Area or in a third country (see Exhibit 1), which in the country of location is subject to equal requirements and the performance of which is subject to state supervision.		is in a country, which is listed in the list of risk countries – when suspicion arises regarding truthfulness of the provided data and/or of authenticity of the identification documents regarding the Client or its Beneficial Owners – in a situation with higher risk of Money Laundering and terrorists financing – in case of companies that have nominee shareholders or shares in bearer form

(High 1)**THE HIGHEST** (High 2)

MEASURES	**Include:**	**Include:**	**IN ADDITION TO NORMAL DUE DILIGENCE THE MEASURES INCLUDE:**

	– the Client can be identified on the basis of publicly available information; – the ownership and control structure of the Client is transparent and constant; – the operations of the Client and their accounting or payment policies are transparent; – Client reports to and is controlled by an authority of executive power of Estonia or a contracting state of the European Economic Area, another agency performing public duties, or an authority of the European Union.	– Identification of a natural person (Identification details and copy of ID documents), video call in case of deposit of more than 15.000 EUR – Identification of a legal person (Corporate details, Certificate of incorporation, Articles of association, ID of representatives and shareholders)	– the Client can be identified on the basis of publicly available information; – the ownership and control structure of the Client is transparent and constant; – the operations of the Client and their accounting or payment policies are transparent; – Identification and verification of a Client on the basis of additional documents, data or information, which originates from a reliable and independent source – Identification and verification of a Client while being present at the same place – Asking the identification or

			verification documents to be notarised or officially authenticated – Obtaining additional information on the purpose and nature of the Business Relationship and verification from a reliable and independent source – Reassessment of a risk profile of a Client not later than 6 months after establishment of Business Relationship

The above listed DD measures can be combined, as appropriate, in respect to other listed or non-listed risks.

* List Of Risk Countries

We distinguish two different types of **risk countries**:

1. Countries which according to FATF **does not follow requirements of prevention of Money Laundering and Terrorism Financing**. You can find it here: http://www.fatf-gaM.org/countries/#high-risk

1. Countries which according to the FIU are under **big threat of terrorism**:

Afghanistan, Algeria, United Arab Emirates, Bahrein, Bangladesh, Egypt, Indonesia, Iraq, Iran, Yemen, Jordanian, Qatar, Kuwait, Lebanon, Libya, Malaysia, Mali, Morocco, Mauritania, Nigeria, Oman, Pakistan, Palestine, Saudi Arabia, Somalia, Sri Lanka, Sudan, Syria, Tunisia, Turkey, Ethnic groups of

Caucasus belonging to Russian Federation (Chechens, Lesgid, ossetians, Ingushes etc.)

TimaxPay has its sole discretion to enter into business relationship with any legal or natural person from such country up front.

** List Of Non-low Tax Countries

List of countries that are NOT regarded as low tax rate countries (established by estonian Financial Ministry) can be found here:

https://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulu-maksustamine/nimekiri-territooriumidest

DETECTION OF SUSPICIOUS TRANSACTIONS

TimaxPay shall diligently monitor transactions for suspicious activity. Transactions that are unusual will be carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose.

Implemented internal controls will serve as ongoing monitoring system in order to detect the suspicious activity or transaction. When such suspicious activity is detected, TimaxPay shall determine whether a filing with any law enforcement authority is necessary. Suspicious activity can include more than just suspected money laundering attempts. Activity may be suspicious, and TimaxPay may wish to make a filing with a law enforcement authority, even if no money is lost as a result of the transaction.

TimaxPay shall initially make the decision of whether a transaction is potentially suspicious. Once TimaxPay has finished the review of the transaction details, he or she will consult with its management to make the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be filed.

TimaxPay shall maintain a copy of the filing as well as all backup documentation. The fact that a filing has been made is confidential. No one, other than those involved in the investigation and reporting should be told of its existence. In no event should the parties involved in the suspicious activity be told of the filing.

REPORTING REQUIREMENTS

Reasonable procedures for maintaining records of the information used to verify a person's name; address and other identifying information are required under this Policy. The following are required steps in the record keeping process:

- TimaxPay shall maintain a record of identifying information provided by the customer.
- Where TimaxPay relies upon a document to verify identity, TimaxPay shall maintain a copy of the document that the Company relied on that clearly evidences the type of document and any identifying information it may contain.
- TimaxPay shall also record the methods and result of any additional measures undertaken to verify the identity of the customer.
- TimaxPay shall record the resolution of any discrepancy in the identifying information obtained.
- All transaction and identification records will be maintained for a minimum period of five years.

If you have more questions,

please contact : info@timaxpay.com