Crypterium AML/KYC Policy

Introduction

The Anti-Money Laundering and Know Your Customer Policy (the "**AML/KYC Policy**") of Crypterium AS of Harju maakond, Tallinn, Kesklinna linnaosa, A. Lauteri tn 5, 10114, Estonia, registration number 14352837 ("**we**", "**our**", "**us**" or "**Crypterium**") is established to prevent and mitigate possible risks of Crypterium being involved in illegal or illicit activities and to enable Crypterium to meet its legal and regulatory obligations in this area (if any, where applicable). This AML/KYC Policy is subject to changes and updates by Crypterium from time to time to ensure compliance with any applicable legislation and global AML/KYC practices.

Definitions

"**Beneficial Owner**" means any natural person or persons who ultimately own or control the User (as defined below) and, or the natural person or persons on whose behalf a transaction or activity is being conducted, and

(a) in the case of a body corporate or a body of persons, the beneficial owner shall consist of any natural person or persons who ultimately own or control that body corporate or body of persons through direct or indirect ownership of twenty-five per centum (25%) plus one (1) or more of the shares or more than twenty-five per centum (25%) of the voting rights or an ownership interest of more than twenty-five per centum (25%) in that body corporate or body of persons, including through bearer share holdings, or through control via other means, other than a company that is listed on a regulated market which is subject to disclosure requirements consistent with European Union law or equivalent international standards which ensure adequate transparency of ownership information:

Provided that a shareholding of twenty-five per centum (25%) plus one (1) share or more, or the holding of an ownership interest or voting rights of more than twenty-five per centum (25%) in the customer shall be an indication of direct ownership when held directly by a natural person, and of indirect ownership when held by one or more bodies corporate or body of persons or through a trust or a similar legal arrangement, or a combination thereof:

Provided further that if, after having exhausted all possible means and provided there are no grounds of suspicion, no beneficial owner in terms of this paragraph has been identified, subject persons shall consider the natural person or persons who hold the position of senior managing official or officials to be the beneficial owners, and shall keep a record of the actions taken to identify the beneficial owner in terms of this paragraph.

(b) in the case of trusts the beneficial owner shall consist of:

i. the settlor;

ii. the trustee or trustees;

iii. the protector, where applicable;

iv. the beneficiaries or the class of beneficiaries as may be applicable; and

v. any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

(c) in the case of legal entities such as foundations and legal arrangements similar to trusts, the beneficial owner shall consist of the natural person or persons holding equivalent or similar positions to those referred to in paragraph (b).

"**High Risk Jurisdiction**" means the jurisdictions designated by Crypterium as a high risk jurisdiction in respect of any Sale or Service from time to time.

"**Politically Exposed Person**" means a natural person who is or has been entrusted with prominent public functions, other than middle ranking or more junior officials. For the purposes of this definition, the term "natural person who is or has been entrusted with prominent public functions" includes the following:

(a) Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries;

(b) Members of Parliament or similar legislative bodies;

(c) Members of the governing bodies of political parties;

(d) Members of superior, supreme, and constitutional courts or of other highlevel judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

(e) Members of courts of auditors or of the boards of central banks;

(f) Ambassadors, charges d'affaires, consuls and high ranking officers in the armed forces;

(g) Members of the administrative, management or supervisory boards of Stateowned enterprises;

(h) Anyone exercising a function equivalent to those set out in paragraphs (a) to (f) within an institution of the European Union or any other international body;

Furthermore, Politically Exposed Person includes also family members or persons known to be close associates of any individual identified in (a) – (h) above.

The term “family members” includes:

- the spouse, or a person considered to be equivalent to a spouse;
- the children and their spouses, or persons considered to be equivalent to a spouse; and
- the parents.

“Persons known to be close associates” means:

- a natural person known to have joint beneficial ownership of a body corporate or any other form of legal arrangement, or any other close business relations, with that politically exposed person; or
- a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that politically exposed person.

“**Prohibited Jurisdiction**” means the jurisdictions designated by Crypterium as a prohibited jurisdiction in respect of the Sale or Service from time to time.

“**Sanctioned Jurisdiction**” means any country or territory to the extent that such country or territory is the subject of any sanction issued by the United Nations, United States and/or the European Union.

“**Sanctioned Person**” means any individual or entity (a) identified on a sanctions list issued by the United Nations, United States and/or the European Union; (b) organized, domiciled or resident in a Sanctioned Jurisdiction; or (c) otherwise the subject or target of any sanctions, including by reason of ownership or control by one or more individuals or entities described in clauses (a) or (b).

“**Service**” means any other services provided by Crypterium to the Users from time to time, including, without limitation, its payment and cryptocurrency exchange services, wallet services, C-lever.com and Instachange.com services, and any other services or functionalities, past, present, or future.

“**Transaction**” means any transaction with any assets that is conducted by a user through any of the Crypterium’s websites, applications, client accounts, cryptocurrency wallets, Services, or functionalities, and the word “transact” shall be interpreted accordingly.

“**User**” means a person using Crypterium’s Services.

Initial and ongoing screening

a) Crypterium will (and will always reserve a right to) screen a User prior to enabling any Transaction with such User and will continue to screen such User on an ongoing basis, to ensure that such User is not a Sanctioned Person, from a Sanctioned Jurisdiction and/or a person from a Prohibited Jurisdiction.

b) Crypterium will screen a User prior to providing any Service to such User, and will continue to screen such User on an ongoing basis, to ensure that such User is not a Sanctioned Person, from a Sanctioned Jurisdiction and/or a person from a Prohibited Jurisdiction. If a User is a Sanctioned Person, from a Sanctioned Jurisdiction and/or a person from a Prohibited Jurisdiction, Crypterium will refuse to provide Services to such User or discontinue the provision of Services.

In carrying out this screening Crypterium shall ensure to adopt software to enable comprehensive screening to be carried out and which captures all sanctions that Crypterium is bound to follow.

KYC/AML identification procedures

Crypterium adopts a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, Crypterium is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks.

Prior to enabling or entering into a Transaction with or for or on behalf of a User or providing any Service to a User, Crypterium will, if so required by applicable law or if it is otherwise deemed necessary or expedient:

a) identify the User and verify the User's identity on the basis of documents, data or other information based on a reliable and independent source;

b) if there is a Beneficial Owner in relation to the User, identify the beneficial owner and take reasonable measures to verify the beneficial owner's identity;

c) obtain information on the purpose and intended nature of the business relationship with the User, unless the purpose and intended nature are clearly stipulated in the relevant documentation between Crypterium and the User. As part of this

process, Crypterium shall obtain, amongst other matters, information on the source of funds and source of wealth of the User; and

d) if a person purports to act on behalf of the User, (i) identify the person and take reasonable measures to verify the person's identity on the basis of documents, data or information based on a reliable and independent source; and (ii) verify the person's authority to act on behalf of the User.

To identify a User who is an individual, Crypterium will collect information from the User, including but not limited to, his full name, date of birth, place of birth, nationality, place of residence, email address, and the identity document type. Crypterium will verify the identity of the User with documents such as his national ID, passport and/or driver's licence and utility bill.

To identify a User who is a legal entity, Crypterium will collect information from the User, including but not limited to, its full legal name, registration number, date of incorporation / registration, country of incorporation / registration and lists of directors (as applicable to the entity). Crypterium will verify the User with documents such as Memorandum and Articles of Association (or equivalent), additional beneficial ownership information and documents, and a detailed corporate chart (as applicable to the entity).

If the User is not physically present for identification purposes, Crypterium may adopt more stringent standards to verify the identity of the User.

Ongoing monitoring of Users

Crypterium reserves the right to continuously monitor, on a risk sensitive basis, the business relationship with a User (as applicable) by:

a) reviewing from time to time documents, data and information that have been obtained by Crypterium to ensure that such documents, data and information are up to date;

b) conducting appropriate scrutiny of Transactions and activities carried out by Users to ensure that they are consistent with Crypterium's knowledge of the User's business and risk profile, and to ensure that such Transactions and activities are in line with Crypterium's knowledge of the User's or User's source of funds and source of wealth; and

c) identifying transactions that are unusually large in amount or of an

unusual pattern and have no apparent economic or lawful purpose.

For the avoidance of doubt, Crypterium may undertake ongoing monitoring on Users in order to ensure that any Transactions equal to or in excess of € 500 (or its equivalent in any other currency) shall be subject to enhanced due diligence in relation to the source of funds and source of wealth of the User.

To continuously monitor the business relationship with a User (as applicable), Crypterium may carry out a file review to ensure that information held about the User is up-to-date and that identification documents held are still valid. In addition, on a more frequent basis, Crypterium may also monitor transactional activity to identify any red-flags or 'out of the norm' activity.

As part of the second line of defense, the Money Laundering Reporting Officer will carry out checks to ensure that regular and effective on-going monitoring is being effected and ensure that irregular or suspicious activities are effectively escalated.

Sanctioned Jurisdictions, Prohibited Jurisdictions and High Risk Jurisdictions

Crypterium will establish and maintain the following lists of jurisdictions (i) Sanctioned Jurisdictions (ii) Prohibited Jurisdictions and (iii) High Risk Jurisdictions. In determining the list of Sanctioned Jurisdictions, Prohibited Jurisdictions and High Risk Jurisdictions, Crypterium shall take into account the lists issued by the Financial Action Task Force and by other organizations issuing guidelines and lists relating to the adequacy of legislative measures adopted by jurisdictions in relation to money laundering, funding of terrorism and transparency.

Users which are (i) resident or domiciled in, or (ii) have their source of wealth or source of funds linked to a Sanctioned Jurisdiction and/or a Prohibited Jurisdiction shall not be accepted as clients of Crypterium.

Users which are (i) resident or domiciled in, or (ii) have their source of wealth or source of funds linked to High Risk Jurisdictions shall be subject to additional checks and measures by Crypterium.

High risk situations

In certain circumstances, the risk may be higher and Crypterium will need to take additional checks. These include, for example, situations where the User is from a High Risk Jurisdiction, where the User is a Politically Exposed Person, or the User's or User's behavior and activities

raise other red flags.

In a high risk situation, Crypterium will:

a) where a business relationship has not yet been established, obtain approval from senior management to establish the business relationship and take reasonable measures to verify the User's or beneficial owner's source of wealth and source of funds that will be involved in the business relationship; and

b) where a business relationship has been established, obtain approval from senior management to continue the business relationship, take reasonable measures to verify the beneficial owner's identity, and take reasonable measures to verify the User's or beneficial owner's source of wealth and source of funds that will be involved in the business relationship.

Record-keeping

Crypterium will keep (a) transaction records, for a period of ten (10) years beginning on the date on which a transaction is completed, or for such other minimal period as may be required by applicable law; and (b) other information collected by Crypterium for AML/KYC purposes, throughout the continuance of the business relationship with the User and for a period of ten

(10) years beginning on the date on which the business relationship with the User ends, or for such other minimal period as may be required by applicable law.

Money Laundering Reporting Officer

The Money Laundering Reporting Officer shall be the person, duly authorized by Crypterium, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Money Laundering Reporting Officer's responsibility to supervise all aspects of Crypterium's anti-money laundering and counter-terrorist financing. Once such officer is appointed, all our employees will report any suspicious behavior or activities to the Money Laundering Reporting Officer.

Reporting

Where Crypterium suspects that a User is involved in any money laundering, terrorist financing or other illegal activities, it will report any relevant knowledge or suspicion to governmental and regulatory authorities. Crypterium shall not notify any Users of any such suspicious transaction report. Rather, in the event that Crypterium and its employees notify such Users, they may be held liable for tipping off. This is a criminal offence punishable by a fine and/or imprisonment.

Last updated: 13 January 2020