Why Bitcoinus needs to know my identity?

This procedure establishes the order of realizing the requirements of law regulations, which regulate money laundering and terrorist financing prevention in Bitus LTD. It is applicable to the company, which deals with the release and buyout of electronic money, provides with the services of payment, issues the measures of payment and engages in other activities, requiring the security of the prevention of the money laundering and terrorist financing.
This procedure was prepared according to the requirements of money laundering and terrorist financing prevention law (hereafter – Law) of United Kingdom and the directive 2005/60/EC of 26 October 2005 of the European Parliament and Council on the prevention of the use of financial system for the purpose of money laundering and terrorist financing and the requirements of the regulation (EC) 1781/2006 (hereafter – Regulation (EC) 1781/2006) of 15 November 2006 of the European Parliament and Council on the payer's information, given while transferring the funds (OL 2006 L 345, p. 1).
The definitions used in this procedure are perceived in the way they are defined in Law.

RISK ASSESSMENT OF MONEY LAUNDERING AND/OR TERRORIST FINANCING

1. The risk of money laundering and terrorist financing in the company is assessed by distinguishing such kinds of risks as the risk of the customer, products and/or services, country and/or geographical region, the opening of a virtual account.
2. In order to assess the risk of money laundering and/or terrorist financing in a company, the professional competence and procedure is followed.
3. Deficient or incomplete information about the customer is considered as a criterion by the company when assessing whether the transfer of money or any other related transaction is suspicious and needed to be reported to the corresponding institutions.

IDENTIFICATION OF CUSTOMER AND BENEFICIARY

1. Third party KYC / AML software provider must determine whether the customer and the beneficiary operate on their own, or are being in control, also identify and verify their identities.
2. In order to ensure a comprehensive prevention, while examining and defining the identity of the customer and beneficiary, the company must:

- obtain the information from the customer about the purpose and the intended nature of the business relationship;
- get the identification documents of the customer, containing the information about the beneficiary and the customer himself;
- rely on documents, data or information obtained from a reliable and independent source: the information provided by the bank of the customer, official documents, which contain personal photography and / or the corresponding registration number, are unable to be easily copied or forged (passport, identity card, driving license, a legal entity registration certificate, notarized copies of documents, etc.), which indicate the name of the customer, surname, personal identification number or another unique sequence of numbers for the identification of a person, a personal picture and (or) the signature, etc. (for a natural

person), or the name, address, code, registration certificate number, VAT number, etc. (for a legal person); publicly available information by databases; by the recommendations of the other credit institutions, etc.;obtain such information that it would be possible to understand the management system of the customer (legal person) and the nature of business.
3. Verifying the identity of the customers, the attention is paid whether the customer is not entered in the list of consolidated individuals, their groups and companies with institutions, which carry the financial penalties of European Union (renewed consolidated list is given in the official website of the European Commission: http:// eeas.europa.eu/cfsp/sanctions/consol- list_en.htm).
4. It is prohibited for the employees of the company or the third party KYC / AML software provider to run the monetary operations if the customer does not provide the documents verifying his identity; provides incomplete or false data, which is known for the employees of the company; avoids providing

information, necessary for identification; conceals beneficiary identification; avoids providing or does not provide information, needed for beneficiary identification; or the provided data is insufficient.

5. During customer identification (natural person), there are some documents, required from him, which contain the data of his identity:

- name (names);
- surname (surnames);
- personal number (applicable to the citizens of the Republic of Lithuania);
- date of birth, personal number or another unique sequence of numbers for the identification of a person (applicable for foreigners);
- nationality (nationalities);
- living place data;
- financial data (source of income);
- in addition: Checking if the person is politically exposed person + other sanctions.

6. Regarding the method based on the risk assessment, these means of identification are applied:

- Simplified identification of the customer. When there is only a request for the document verifying the identity.
- Consolidated identification of the customer. When there is a request for other sources or institutions to verify or provide information about the person's identity or the person himself.

7. When the monetary operation is run and the transaction is made with a representative, the requested data about both the principal and the representative must be established; requirements, set for customer identification, are equally applicable for the customers who directly approach the company as much as for those whose diplomatic relations, monetary operations and transactions are run with the representative, or the customer is physically absent during the process of his identification.

8. In case of disapproval from the customer to verify the identity by the indicated means or causing suspicions due to performed actions, the company can report this issue to the corresponding institutions.

Explanation of Proof of Sources of Funds (POSOF)

A **Proof of Sources of Funds (POSOF)** is any (collection of) document(s) that explains where the funds used for a fiat deposit originated and where the crypto assets used for a fiat withdrawal originated.

Bitcoinus may request a proof of source of funds for clients depositing and withdrawing USD/EUR wire transfers.

Bitcoinus reserves the right to ask any client using any funding methods for a POSOF.

Any POSOF document submitted needs to cover all deposits or withdrawals via that particular funding method. If a client has made deposits or withdrawals earlier they should make sure that the POSOF documentation covers any previous deposits or withdrawals as well as the most recent one.