Anti-Money Laundering, counter Terrorist Financing and sanctions Procedure

Approved by: The Management Board

Appointed Control Person: Arsen Martyn

Date of approval: 1.10.2018

References to external rules:

Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of Money Laundering or Terrorist Financing

Estonian Money Laundering and Terrorist Financing Prevention Act

Contents

DEFINITIONS

In the course of this Policy the following terms shall have the following meanings

a. **Actual Beneficiary** – a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favour or on whose account a transaction or act, action, operation or step is made.

b. **Board** – Management Board of BITONGROUP.

c. **Client** – person setting up and account at the Website and/or using BITONGROUP's services; only natural persons are allowed to use BITONGROUP's services.

d. **BITONGROUP** – BITONGROUP OÜ, a private limited company, established in the Republic of Estonia with the registration no. 14568649

e. **Employee –** all staff of BITONGROUP, including contractors, temporary staff and administrators.

f. **FIU** – Financial Intelligence Unit of Estonian Police and Board Guard Board.

g. **Money Laundering** – either a) the conversion or transfer of property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions; b) the acquisition, possession or use of property derived from criminal activity or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein; c) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.

h. **MTPA** – Money Laundering and Terrorist Financing Prevention Act of Estonia, available here: https://www.riigiteataja.ee/en/eli/521122017004/consolide

i. **Politically Exposed Person** – natural person who is or who has been entrusted with prominent public functions including a head of State, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors or of the board of a central bank; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a State-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials. The family member or a close associate of the person described in the previous sentence will be also regarded as Politically Exposed person within the meaning of this Policy.

j. **Terrorist Financing** – financing and supporting the activities that fall under the definition of terrorism according to the Penal Code of Estonia.

k. **Website** – https://bitonmarket.io/

1. General Provisions

1.1. This Policy is applicable to:

1.1.1. all functional areas and business processes of BITONGROUP;

1.1.2. all Employees and Board acting on behalf of BITONGROUP.

1.2. The objective of this Policy is to establish rules for:

1.2.1. client identification and verification,

1.2.2. client risk classification;

1.2.3. client due diligence measures;

1.2.4. enhanced due diligence measures and applicability of these measures;

1.2.5. monitoring of Clients activities and transactions;

1.2.6. termination of business relationship;

1.2.7. record keeping, update and storage of the Client's data;

1.2.8. identification and reporting of suspicious and unusual activities and transactions, including rights, responsibilities of Contact Persons tasks within BITONGROUP;

1.2.9. staff training and awareness;

1.2.10. supervision of the fulfilment of the requirements set in this Policy.

1.3. In addition to the Control Person, the Board shall be conducting regular checks to assure that the provisions of this Policy are being implemented by the Employees as stipulated in this Policy and in accordance with applicable laws.

1.4. This Policy and amendments to this Policy shall be established by the Board, and the Board shall be responsible for providing the proper training for the Employees in order to insure that this policy is fully implemented in the course of provision of services to Clients.

2. BITONGROUP's services and becoming a Client

2.1. Company core business is an Internet platform which allows to place goods by trusted legal entities or individuals, with integrated blockchain technology, which solves the problems of transparency, security and automation when carrying out transactions within the platform, blocking technologies and crypto-currency.

2.2. In order to sign up to the Website, the Client is required to:

2.2.1. fill out and submit the respective application available on the Website;

2.2.2. validate his/her e-mail address; and

2.2.3. agree to the terms.

1.1. After signing up, the Client will be able to log in to his/her Account at the Website using his/her e-mail address and personal password. By enabling signing up to the Website, Clients will be able to consume BITONGROUP's services only after the establishment of business relationship.

1.2. For establishing of the business relationship and in order to be able to use BITONGROUP's services, the Client has to:

1.2.1. meet the Customer requirements as stipulated in section 3.4 of this Policy;

1.2.2. submit all the documentation and data listed in section 4.2 of this Policy; and

1.2.3. provide all confirmations as required by BITONGROUP.

1.3. Prior to establishing of the business relationship, the Client is required to confirm that:

1.3.1. the Client is at least 18 years old;

1.3.2. the Client meets all customer requirements as stipulated in section 3.4 of this Policy; and

1.3.3. the documentation and data provided by the Client to BITONGROUP is accurate, appropriate, up-to-date and precise.

1.4. The precise content and wording of these confirmations shall be determined by the Board.

1.5. BITONGROUP will decide whether to establish the business relationship with the Client after it has received all required documentation, data and confirmations, identified the Client and performed all other applicable due diligence measures in respect to the Client.

2. The general principles for applying due diligence measures

2.1. BITONGROUP applies following due diligence measures:

2.1.1. performing of BITONGROUP KYC process as described in section 4 to this Policy and decides whether to grant Client an access to BITONGROUP's services (establish business relationship) on the basis of the results of the KYC process;

2.1.2. monitoring of the business relationship;

2.1.3. refusing to perform transactions as requested by the Client/stopping of providing services to the Client;

2.1.4. termination of the established business relationship.

2.2. BITONGROUP applies due diligent measures at least:

2.2.1. upon establishment of a business relationship;

2.2.2. upon verification of information gathered while applying due diligence measures or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered earlier while updating the relevant data;

2.2.3. upon suspicion of Money Laundering or Terrorist Financing.

2.3. BITONGROUP does not conduct nor take part of cash transactions.

2.4. BITONGROUP will not establish business relationships nor offer services to:

2.4.1. persons under 18 years of age;

2.4.2. persons who wish to use a representative;

2.4.3. persons who does not confirm that he/she is the Actual Beneficiary;

2.4.4. persons under International Sanctions;

2.4.5. persons who submit false information, documentation or data to BITONGROUP.

2.5. BITONGROUP shall rely on the Client's confirmations upon identifying of the Actual Beneficiary. BITONGROUP will only take additional steps in identifying the Actual Beneficiary if, as a result of the data provided by the Client and the explanations given, it becomes doubtful that the Client is the Actual Beneficiary, including, for example, if the Client submits contradictory information or explanations in relation to public databases or otherwise doubts are risen about the fact that the Client is the Actual Beneficiary.

2.6. BITONGROUP does not apply simplified due diligence measures as stipulated in § 32 of the MTPA.

3. Initial Client identification and verification upon establishment of the business relationship (BITONGROUP KYC process)

3.1. BITONGROUP does not provide services to Clients (i.e. establish business relationships) who haven't been approved by BITONGROUP's Employee. For preliminary clients checks company is using KYC service provider such as Veriff (https://veriff.me/)

3.2. The Client who wishes access to BITONGROUP services has to access the KYC application process from the Client's Profile Dashboard.

3.3. For the purposes of performing KYC process, the Client is required to submit the following information and documentation:

3.3.1. a photo of himself/herself ("selfie"), to be realized with a live camera/webcam;

3.3.2. an ID document of himself/herself, to be inputted through a live webcam/camera, or alternatively upload in a PDF, PNG or JPG format. The user is also required to identify the type of ID document he/she is uploading, among the allowed ones (Passport, Driving Permit, National ID Card);

3.3.3. a proof of address document, to be inputted through a live webcam/camera, or alternatively upload in a PDF, PNG or JPG format. The user is also required to identify the type of proof of address document he's uploading, among the allowed ones (utility bill, bank statement, credit card statement);

3.3.4. his/her personal data in literal form, comprising of first and last name, date of birth, personal identification code (if applicable), gender, nationality, full address and country of residence.

3.4. The data and documentation entered by the Client during the KYC process shall be automatically checked by KYC service provider Veriff.

3.4.1. verifies the correspondence between "Selfie" and ID document;

3.4.2. verifies the correspondence between ID document and personal data provided by the Client, rectifying small differences (i.e. typos);

3.4.3. verifies the correspondence between proof of address document and address info provided by the Client, rectifying small differences (i.e. typos);

3.4.4. checks the validity of the ID document by assessing it in accordance with section 4.6 of this Policy;

3.4.5. verifies that the Client fulfils the conditions stipulated in sections 2.6 and 3.4 of this Policy.

3.5. The system available to the Responsible person or entity automatically checks the full name of the Client against the Reuters DB. The Employee shall manually enter the Client's name to the search engine managed by FIU (available at: https://www2.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/) for identifying persons under sanctions.

3.6. The Responsible person or entity shall reject the Client's application if any of the following apply:

3.6.1. there is no correspondence between "Selfie" and ID document;

3.6.2. the ID document is invalid according to section 4.6 of this Policy;

3.6.3. there is no correspondence between ID document and personal data provided by the Client;

3.6.4. there is no correspondence between proof of address document and address info provided by the Client;

3.6.5. Client doesn't fulfil the conditions described in sections 2.6 and 3.4 of this Policy;

3.6.6. person is identified as a person under sanctions or politically exposed person by Reuters DB or FIU search engine;

3.6.7. Employee identifies other high risks that apply in regards the Client, according to the section 5 of this Policy.

3.7. The personal identification document is considered to be valid only if the document meets all of the following requirements:

3.7.1. the document has been issued and the data has been entered in the document by the local institution legal institution;

3.7.2. the period of validity of the document has not expired;

3.7.3. the document is fit for use and allows the establishment of the identity of the user of the document and the determination of the entries made therein and the correctness thereof;

3.8. If verification is reject the by Veriff, then according to section 4.5 of this Policy, Employee may apply enhanced due diligence measures in order to exclude any doubt with regard to the Client's identity or involvement in Money Laundering and/or Terrorist Financing or breach of international sanctions. If doubt remains, BITONGROUP shall not establish the business relationship with such Client.

3.9. BITONGROUP must regularly update the data gathered about a client upon establishing the business relationship. In regards to the clients whose data has already been identified and verified (upon establishing of the business relationship), their data must be updated on annual basis (once per Year) , including the data regarding their status in regards to international sanctions.

4. Evaluation of the risks related to Money Laundering and Terrorist Financing

4.1. In assessing the degree of risks of Money Laundering and Terrorist Financing, three categories of risks must be taken into account:

4.1.1. geographical risk;

4.1.2. customer risk;

4.1.3. transaction risk.

4.2. The geographical risk is considered to be high if the Client or transaction is known to have a link with the following countries or territories:

4.2.1. countries and territories for which a United Nations or EU sanction, embargo or other analogous measure has been imposed;

4.2.2. countries designated by the European Union or the Financial Action Task Force as countries which do not have adequate measures to prevent money laundering and terrorist financing;

4.2.3. countries that are known to support terrorism or where there is a high level of corruption.

4.3. Customer risk is considered to be high when the Client:

4.3.1. is a Politically Exposed Person;

4.3.2. is a person under sanctions according to Reuters and/or FIU corresponding search engine (https://www2.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/);

4.3.3. is a person who, according to the knowledge of BITONGROUP's Employees, has previously been suspected of being involved in Money Laundering and/or Terrorist Financing.

4.4. The risk associated with the transaction is considered to be high if:

4.4.1. the purposes of requested transaction include concealment of the actual party or the object of the transaction;

4.4.2. the transaction has no reasonable commercial, economic, fiscal or legal purpose.

4.5. The risk or Money Laundering and/or Terrorist Financing is considered to be high if there is any reason to suspect that a Customer or Customer transaction may be related to Money Laundering of Terrorist Financing.

4.6. BITONGROUP will not establish business relationship if any of the risks listed in section 5.1 of this Policy should be evaluated "high" according to sections 5.2 – 5.5. In such a case BITONGROUP Employees must notify the Contact Person and in accordance with the instructions of the Contact Person may apply enhanced due diligence measures as described in section 7 of this Policy. If the application of enhanced due diligence measures do not exclude doubt with regard to the Client's identity or involvement in Money Laundering and/or Terrorist Financing or breach of international sanctions, the Employee is required not to establish business relationship with such Client.

4.7. If the high risk is identified in relation to a Client with whom the business relationship has been already established, the Employee is required to notify the Contact Person and in accordance with the instructions of the Contact Person, apply enhanced due diligence measures according to section 7 of this Policy.

5. Monitoring of the established business relationships, refusal to perform transactions, and termination of the business relationships

5.1. BITONGROUP shall monitor the business relationships created with Clients throughout the duration thereof.

5.2. Employees shall monitor Clients, their conduct and transactions, inter alia:

5.2.1. by checking of transactions made in a business relationship in order ensure that the transactions are in concert with the obliged entity's knowledge of the customer, its activities and risk profile;

5.2.2. by conducting regular inquiries to Reuters and FIU search engine in order to establish whether the Client has become subject to sanctions;

5.2.3. by paying attention to complicated and unusually large transactions or unusual trading patterns that do not have a visible economic or legal purpose;

5.2.4. by monitoring whether the first monetary payment related to the Client's Account is carried out via a bank account that has been opened in the name of the Client in a credit institution registered or having its place of business in a contracting state of European Economic Area (EEA) or in a country where the applicable AML/CTF regulations are equal to EEA countries.

5.3. Upon identifying an unusual, suspicious or irregular transaction, an Employee shall analyse the circumstances of the transactions, including whether there are any reasons for performing an irregular transaction and decide on taking further measures, including applying enhanced due diligence measures, refusing to perform the transaction, notifying the Contact Person, etc. The Employee shall assess the unusualness of the transaction in accordance with the principal of reasonability, assessing the possible suspicions that have arisen rather to the Client's disadvantage.

5.4. BITONGROUP shall update the data and documents collected for identification purposes at least once within the period of two years. For the purposes of updating the documentation available to BITONGROUP in regards to the Client, BITONGROUP shall request the Client to confirm the validity of the documentation and ask the Client to submit new data and valid ID document if the data has changed or the ID document expired.

5.5. BITONGROUP has the right to refuse to provide or restrict the Client from using BITONGROUP's services, if:

5.5.1. on the basis of monitoring of the established business relationship, BITONGROUP comes to suspect Money Laundering or Terrorist Financing or the commission of related offences or an attempt at such activity;

5.5.2. on the basis of monitoring of the established business relationship, BITONGROUP comes to suspect that the Client does not meet all customer requirements as stipulated in section 3.4 of this Policy.

5.6. BITONGROUP will stop providing services to Client, and has the right to terminate the business relationship with the Client, if:

5.6.1. the Client refuses to provide information BITONGROUP requires in order to apply due diligence measures and/or enhanced due diligence measures;

5.6.2. BITONGROUP's application of enhanced due diligence measures do not exclude doubt with regard to the Client's identity, the Client meeting all customer requirements as stipulated in section 3.4 of this Policy or involvement in Money Laundering or Terrorist Financing or the commission of related offences or an attempt at such activity or breach of international sanctions.

6. Enhanced due diligence measures

6.1. If so required by this Policy and after consulting with the Contact Person, the Employee shall apply at least one of the following enhanced due diligence measure in respect to the Client:

6.1.1. verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;

6.1.2. gathering additional information on the purpose and nature of the business relationship, transaction or operation and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;

6.1.3. gathering additional information and documents regarding the actual execution of transactions made in the business relationship in order to rule out the ostensibility of the transactions;

6.1.4. gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction made in the business relationship in order to rule out the ostensibility of the transactions;

6.1.5. if the Client or its activities are related to high-risk third country, the Employee shall:

6.1.5.1. gather additional information about the customer;

6.1.5.2. gather additional information on the planned substance of the business relationship

6.1.5.3. gather information on the origin of the funds and wealth of the customer

6.1.5.4. gather information on the underlying reasons of planned or executed transactions;

6.1.5.5. request permission from the Board to establish or continue a business relationship.

6.1.6. if the Client or its activities are related to Politically exposed person, the Employee shall:

6.1.6.1. obtain approval from the Board to establish or continue the business relationship;

6.1.6.2. applies measures to establish the origin of the wealth of the person and the sources of the funds that are used in the business relationship or upon making occasional transactions;

6.1.6.3. monitors the business relationship in an enhanced manner.

6.2. The Employee will only apply the kind of enhanced due diligence measures that are appropriate in regards to the specific situation.

6.3. Upon application of enhanced due diligence measures, BITONGROUP must apply the monitoring of a business relationship more frequently than usually, including reassess the Client's risk profile not later than six months after the establishment of the business relationship.

7. Notification obligation

7.1. The Employee and shall be obligated to immediately notify the Contact Person, if:

7.1.1. in the performance of BITONGROUP's economic activities, they identify an activity or circumstances which might be an indication of Money Laundering or Terrorist Financing, breach of international sanctions or in the event of which they have reason to suspect or they know that it is Money Laundering or Terrorist Financing, or breach of international sanctions particularly if the characteristics of the activity or circumstances point to the indicators of suspicious transactions described in the suspicious transaction guidelines published by the FIU.

7.1.2. BITONGROUP refuses to create a Client relationship or perform a transaction or procedure in accordance to the requirements of this Policy;

7.1.3. BITONGROUP terminates the contract due to the Client's failure to submit to BITONGROUP the data and documents necessary for applying the enhanced due diligence measures set forth in section 7 of this Policy.

7.2. It shall be prohibited for the Employee, the Contact Person and the Board to inform the Client of the notice submitted with regard to the Client in accordance with section 8 of this Policy.

7.3. If the Client's activity cannot, pursuant to this Policy, be fully qualified as an activity of which the FUI has to be notified, the subsequent activities of the Client shall be placed under special attention and the FUI shall be notified as soon as a justified suspicion arises with regard to the Client's activity.

8. Contact Person's duties in ensuring compliance with this procedure

8.1. The Board will designate a Contact Person from the members of the Board, who is charge of implementation of this Policy and applicable legislation.

8.2. The duties of the Contact Person are as follows:

8.2.1. inspecting the fulfilment of the requirements of MTPA by Employees;

8.2.2. inspecting the fulfilment of the requirements of financial and civil sanction implementation;

8.2.3. making proposals to amend or supplement this Policy, if necessary;

8.2.4. introducing the requirements set forth in this procedure, and the amendments thereof to Employees, if their work duties include the creation of Client relationships and the performance of transactions;

8.2.5. conducting or ensuring the organisation of training to introduce the relevant legal acts and the requirements set forth in this Policy for Employees at least once a year;

8.2.6. analysing the notices sent by Employees and Representatives in the fulfilment of the obligations arising from this procedure, and deciding whether the notices are to be forwarded to the Financial Intelligence Unit;

8.2.7. forwarding information to the Board and the FIU in the case of a suspicion of Money Laundering and Terrorist Financing, breach of financial and/or civil sanctions, and responding to the enquiries and precepts presented by the FIU;

8.2.8. gathering information about cases of refusal to create a Client relationship or perform a transaction with a Client as well as about suspicious or unusual procedures, and analysing and storing such information in accordance with the established procedure;

8.2.9. presenting to the Board an inspection report on compliance with this procedure once a year and, if necessary a follow-up inspection report, including the following information:

8.2.9.1. the aim of inspection;

8.2.9.2. the date of inspection;

8.2.9.3. the name and title of the person who carried out the inspection;

8.2.9.4. a description of the inspection carried out;

8.2.9.5. an analysis of the inspection results or general conclusions from the inspection carried out;

8.2.9.6. if the inspection uncovered deficiencies in this procedure and/or in the practical implementation thereof, the report shall include descriptions of such deficiencies together with an analysis of the related possible risks, prescribing a term for eliminating the deficiencies, the recommended measures for eliminating the deficiencies, and the date for carrying out a follow-up inspection;

8.2.9.7. in the case of a follow-up inspection, an analysis of the follow-up inspection results and a list of the measures taken to eliminate the deficiencies shall be annexed to the inspection report, indicating the time actually spent on eliminating the deficiencies.

8.2.10. informing the Board in writing of deficiencies in the compliance with this procedure as well as the legal acts regulating financial and civil sanctions and the prevention of Money Laundering and Terrorist Financing;

8.2.11. organising or ensuring the availability and maintenance of the technical tools necessary for the fulfilment of the obligations set forth in this procedure.

8.3. The Contact Person shall have the right to:

8.3.1. make proposals to the Board to amend this procedure;

8.3.2. make proposals to the Board to train Employees with regard to the requirements arising from this procedure and the relevant legal acts;

8.3.3. demand the fulfilment of the obligations set forth in this procedure, and the elimination of deficiencies;

8.3.4. inspect the performance and formalisation of transactions in accordance with this procedure and the legal acts regulating financial and civil sanctions and the prevention of Money Laundering and Terrorist Financing.

8.4. The Contact Person may only forward the information or data he or she has learnt with regard to a suspicion of Money Laundering to:

8.4.1. the Board;

8.4.2. the internal auditor;

8.4.3. the FUI;

8.4.4. investigative bodies in connection with commenced criminal proceedings on the basis of an enquiry request presented in accordance with the requirements stipulated in applicable legal acts;

8.4.5. the courts on the basis of a court ruling or judgement.

9. Record keeping, update and storage of the Client's data

9.1. BITONGROUP shall store the data and documents gathered upon the establishment of the business relationship with the Client and other data and documents related to the provision of services to the Client:

9.1.1. to properly monitor the Client relationships;

9.1.2. to present, if necessary, the required data and documents concerning the performed transactions to the FIU and other institutions or courts in accordance with the requirements of legal acts.

9.2. BITONGROUP shall store data and documents regarding:

9.2.1. refusal of establishing of the business relationship with the Client by BITONGROUP;

9.2.2. circumstances of a waiver to establish a business relationship on the initiative of the Client where the waiver is related to the application of due diligence measures by the obliged entity

9.2.3. circumstances of application of enhanced due diligence measures in regard to the Client;

9.2.4. circumstances of termination of the business relationship and/or stopping of providing services to the Client;

9.2.5. circumstances of submitting a notification to the FUI.

9.3. BITONGROUP shall retain the data and documentation listed in section 10.2 of this Policy for no less than five years after termination of the business relationship.