AML/KYC POLICY

1. General

This Anti-Money Laundering and Know Your Client (hereinafter "AML/KYC") Policy governs the application of due diligence measures by the Xshop OÜ (hereinafter the "Company"). Due diligence measures are applied when the clients use the following services of the Company: exchanging the virtual currency into fiat currency and vice versa or a virtual currency against another virtual currency; using the virtual currency wallet.

Please read this AML/KYC policy carefully in order to better understand how we apply the due diligence measures in order to prevent and mitigate possible risks of the Company being involved in money laundering or terrorist financing related activity.

2. Concepts

2.1. Beneficial owner is 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 favor or on whose account a transaction or act, action, operation or step is made.

2.1.1. In the case of legal persons, a beneficial owner is the natural person who ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person.

2.1.2. Direct ownership is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

2.1.3. Indirect ownership is a manner of exercising control whereby a company which is under the control of a natural person holds or multiple companies which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

2.1.4. Where, after all possible means of identification have been exhausted, the beneficial owner cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner, the natural person who holds the position of a senior managing official is deemed as a beneficial owner.

2.2. Politically exposed person is a natural person who is or who has been entrusted with prominent public function and includes the following:

2.2.1. head of state, head of government, minister and deputy or assistant minister;

2.2.2. a member of parliament or of similar legislative body;

2.2.3. a member of the governing body of a political party;

2.2.4. a member of supreme court;

2.2.5. a member of a court of auditors or of the board of a central bank;

2.2.6. an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces;

2.2.7. a member of an administrative, management or supervisory body of a state-owned enterprise;

2.2.8. a director, deputy director and member of the board or equivalent function of an international organization, except middle-ranking or more junior officials.

2.3. family members includes the following:

2.3.1. the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or local politically exposed person;

2.3.2. a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or local politically exposed person;

2.3.3. a parent of a politically exposed person or local politically exposed person;

2.4. persons known to be close associates include the following:

2.4.1. a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person or a local politically exposed person;

2.4.2. a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person or local politically exposed person.

2.5. Compliance Officer (CO) is a representative, appointed by the Management Board and whose appointment has been co-ordinated with the FIU, who responsible for the effectiveness of the Rules, conducting compliance over the adherence to the Rules and serving as contact person of the FIU.

2.6. Responsible MB Member is a representative appointed by the Management Board who is in charge of implementation of the AML Act and legislation and guidelines adopted on the basis thereof.

2.7. FIU is the Financial Intelligence Unit of Estonia.

2.8. AML Act is the Estonian Money Laundering and Terrorist Financing Prevention Act of 26 October 2017 as amended.

3. Identification and Verification

3.1. Upon implementing due diligence measures the following persons shall be identified by the Company:

3.1.1. the client;

3.1.2. the representative of the client;

3.1.3. the beneficial owner of the client;

3.1.4. politically exposed persons.

3.2. The person specified in section 3.1. shall be identified either being present or by using non *face-to-face* identification means.

3.3. Additional video verification requirement (further described in Section 4) applies to a client who is:

3.3.1. an e-resident;

3.3.2. a person from a country outside the European Economic Area or whose place of residence or seat is in such country;

3.3.3. a natural person from an EEA country whose total sum of transactions exceeds 15,000 euros per calendar month; or

3.3.4. a legal person from an EEA country whose total sum of transactions exceeds 25,000 euros per calendar month

3.4. The Company shall establish the business relationship or permit the relevant transaction only where the client has gone through the video verification process.

3.5. The client will be required to fill in the KYC questionnaire where the client shall be asked at least the following information:

3.5.1. For the natural persons:

i. Name;

ii. Personal code/date of birth;

iii. Address/location;

iv. Citizenship;

v. Occupation, area of activity;

vi. Name and date of issuance of document used for identification;

vii. Postal code and city;

viii. The country of tax residency;

ix. E-mail and telephone;

x. Area of activity;

xi. Purpose and nature of the business relationship;

xii. Connection with Estonia (economic or family interests);

xiii. Expected volumes of monthly transactions;

xiv. Existence of a beneficial owner;

xv. Whether the person is a politically exposed person.

3.5.2. For the legal persons:

i. Name;

ii. Registry code or registering number and the date of registration;

iii. Legal form;

iv. Legal capacity;

v. Address/location;

vi. Name and number of the document used for identification and verification of the identity of a foreign legal person;

vii. Postal code and city;

viii. The country of tax residency;

ix. Area of activity (main and secondary);

x. Activity profile;

xi. Location(s) of activity;

xii. E-mail and telephone;

xiii. Have the securities of the company been accepted for trading on a regulated securities market? If yes, then on which securities market?

xiv. Information about the beneficial owners;

xv. Information about the authorized persons (representatives – legal and contractual);

xvi. Information about the members of the management board;

xvii. Purpose and nature of the business relationship;

xviii. Economic connections with Estonia;

xix. Most important business partners;

xx. Information whether the person is a politically exposed person.

3.6. The Company shall request clients (natural and legal persons) to declare and submit information regarding their beneficial owner.

3.7. For the identification and verification purposes the Company shall request to submit:

3.7.1. for natural persons any of the following documents:

i. personal ID card (whether ID card, e-resident card or residence permit card); or

ii. passport or diplomatic passport; or

iii. travel document issued in a foreign country; or

iv. driving license (if it has name, facial image, signature and personal code or date of birth of holder on it).

3.7.2. if the natural person is a representative of a legal or another natural person, then that natural person is also required to submit a document certifying the right of representation and scope thereof and, where the right of representation does not arise from law, the name of the document serving as the basis for the right of representation, the date of issue, and the name of the issuer.

3.7.3. for legal persons any of the following documents:

i. if the legal person or the branches of foreign companies are registered in Estonia then the identification shall be conducted on the basis of an extract of a registry card of commercial register; or

ii. foreign legal persons shall be identified on the basis of an extract of the relevant register or a transcript of the registration certificate or an equal document, which has been issued by competent authority or body not earlier that six months before submission thereof.

3.8. A copy shall be made of the page of the identity document containing at least personal data and a photo of the client.

3.9. The Company may require additional information and documents from the client as the Company deems necessary.

3.10. The clients are required to update the Company immediately if there are any changes to the information submitted to the Company.

4. Video Verification

4.1. Video verification is the procedure of identification of person and verification of data using information technology means as per § 31 of the AML Act and as further specified in the Regulation "Requirements and procedure for identification of persons and verification of person's identity data with information technology means"[1]

4.2. Preconditions for using video verification

4.2.1. The natural person or the legal representative of a legal entity (the Client) must use:

i. a document intended for the digital identification of a person and issued on the basis of the Identity Documents Act or other high-confidence e-identification system, which has been added to the list published in the Official Journal of the European Union[2]; and

ii. an information technology means, which has a working camera, microphone, the hardware and software required for digital identification and an internet connection of adequate quality.

4.2.3. The Client must show to the Company in front of the camera the personal data page of the valid travel document issued by the foreign country.

4.3. Client confirmation

4.3.1. The Client identifies themselves when entering the information system specified by the service provider and confirms that they have read the information about the use of

[1] Full text available here: https://www.riigiteataja.ee/en/eli/509012019003/consolide

[2] Full list (based on Article 9 of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, pp. 73–114)) available here: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

information technology means on the service provider's website or in the specified information system and agree to the conditions of identification of a person and verification of person's identity with information technology means.

4.3.2. The Client further confirms that:

i. he or she carries out the procedures specified in the regulation personally, except for the cases where assistance is permitted by the Company as described in Sections 4.6.3 below;

ii. the data submitted by him or her in the KYC questionnaire (described in Section 3.5 above) and in the course of the interview (specified in Section 4.6 below) are true and complete, and he or she is aware of the consequences associated with the submission of incorrect, misleading or incomplete information upon the establishment of a business relationship;

iii. he or she meets the conditions established by the service provider for the establishment of business relationships and the conclusion of transactions on occasional basis;

iv. they agree with the application of Estonian law.

4.4. Technical characteristics of the information system

4.4.1. Minimum requirements for the quality of information flow transmitting synchronised sound and image:

i. the information system used must allow for digital identification of a person and digital signing;

ii. the service provider must verify the quality of its own and, if possible, the client's information flow and ensure that the transmission of clear, recordable and reproducible synchronised sound and image, which is sufficient to understand the transmitted content unambiguously and reliably, is guaranteed.

4.4.2. Requirements for recording and reproducibility of recording:

i. The information flow containing image and sound is recorded in such a manner that allows for it to be reproduced with a quality equal to the initial transmission of synchronised sound and image;

ii. The information flow that contains image and sound must be recorded with the time stamp, the client's IP address, the personal identification code of the person to be identified, if there is no personal identification code, then the birth date and place and country of residence, whilst the time stamp must be tied to the data concerning it in such a manner that any later changes in data, the person who made the changes, and the time, manner and reason thereof can be identified;

iii. The service provider is obliged to record the data collected with identification questionnaires and the following procedures in the manner specified in point ii. above:
   a. the identification of the person;
   b. the unsuccessful identification of a person and verification of person's identity data as set out in Section 4.7 below;
   c. the carrying out of the mandatory real-time interview.

iv. The recording starts with the identification of the person and ends when the data specified in point iii. above have been collected and the procedures specified in the same subsection have been carried out.

v. The recordings containing the data and procedures must be reproducible within five years of the end of the business relationship;

vi. The service provider has the right to record the KYC questionnaire specified in Section 3.5 above as data stream containing image and sound.

4.4.3. The Company shall take measures in order to prevent the risks of the automated system being manipulated.

4.5. Requirements for framing the face and document of a person

4.5.1. Upon identification of a person and verification of person's identity data with information technology means, the person's head and shoulders must be visible and framed. The face must be clear of shadows and uncovered, and clearly distinguishable from the background and other objects, and recognizable;

4.5.2. The service provider may instruct the person to change his or her body position and place themselves and the document in the frame to make it possible to identify the person and verify person´s identity, including to view the data or images on the document;

4.5.3. The service provider has the right to require the removal of items covering the head or face and glasses or compliance with any other instructions of the service provider given in order to guarantee the identification of a person and verification of person's identity data.

4.6. Interview

4.6.1. In order to collect and verify the information and data required for the determination of the Client's risk profile, the employee of the service provider carries out an interview, during which the employee of the service provider asks partly structured questions, proceeding from the answers in the KYC questionnaire;

4.6.2. The CO must carry on the interview in real time;

4.6.3. With the CO's permission, the natural person or the legal representative of a legal entity may use the assistance of another person to eliminate any technical problems when the interview is carried out;

4.6.4. The COO must assess the client's reaction during the interview, the reliability of the obtained information and data and compliance with the information and data obtained with other procedures, and record his or her opinion and the circumstances that are the basis thereof in the client profile and risk profile.

4.7. Unsuccessful identification of the Client

4.7.1. The video verification is considered unsuccessful if:

i. The Client has intentionally submitted data that do not correspond to the identification data entered in the identity documents database or do not coincide with the information or data obtained with other procedures;
ii. the session expires or is interrupted during the identification of a person, the identification questionnaire or the interview, or the information flow that transmits synchronised sound and image does not comply with the requirements;
iii. the Client has not given the confirmations stipulated in Section 4.3 above;
iv. the Client refuses to comply with the service provider's instructions;
v. the Client uses the assistance of another person without the service provider's permission;
vi. there are circumstances that give rise to suspicions of money laundering or terrorist financing.

4.7.2. The session specified in Section 4.7.1(ii) above expires when the Client has not completed any activities in the service provider's information system during a period of 15 minutes.

4.7.3. In the event of the circumstances set out in Section 4.7.1(i) the Company rejects the application of the Client for opening an account or conclusion of a transaction.

4.7.4. In the event of the circumstances set out in clauses 4.7.1(i) and 4.7.1(vi) the Company sends a notice to the FIU.

4.8. Results of the procedures and the Client's risk profile

4.8.1. The CO must consider the identification questionnaire, interview and other accessible information, and the systematized collection and analysis of data and clarification of facts when assessing the Client's risk profile;

4.8.2. The CO must assess the answers given in the identification questionnaire and record his or her opinion and the circumstances that are the basis thereof in the client profile and risk profile.

4.9. Inspection of the performance of the guidelines

4.9.1. The Responsible MB Member shall regularly, but at least once a year, inspect the performance of the CO under the video verification guidelines.

5. Updating Data and Documents

5.3. The Company may request the client to update the information and/or documents as found necessary after the initial identification and verification of the client.

5.4. The Company may verify the identity of the client in an on-going basis (e.g. if the information submitted by the client has changed).

6. Risk Assessment

The Company will establish a risk profile for each client and will apply due diligence measures in accordance with the clients' risk profile.

7. Registering and Storing of Data

The Company will register and store the data of the clients in accordance with the Company's Privacy policy and in accordance with the legal requirements to AML/KYC and prevention of terrorist financing.

8. Refusing to Open Client Account, Making Transactions or Terminating the Client Relationship

The client account for using the services of the Company will be activated after the completion of the identification and verification. The Company may refuse to open the account for the client, refuse from the transactions with the client or terminate the client relationship in accordance with the laws if the client has not submitted the information or documents requested by the Company to comply with the AML/KYC requirements or there is a suspicion of money laundering or terrorist financing.

9. Changes to this AML/KYC Policy

This AML/KYC policy was last modified in June 2020. Any new versions of this AML/KYC policy will be published by the Company on the Company website.