Applebrie Limited OU ("iCrypt")

(Estonia)

PREVENTION OF MONEY LAUNDERING & TERRORIST FINANCING MANUAL

February 2019

Contents

AML manual

Applebrie Limited OU ("iCrypt")

(the "Company")

1. INTRODUCTION

Applebrie Limited OU is a limited liability company registered in Estonia with registration number 14593050 and with registered address at Peterburi Tee 47, Lasnamae Linnaosa, Tallinn, Estonia, 11415. Applebrie Limited OU operates under the trading name iCrypt and has its domain as iCript.io (hereinafter the "**Company**" and/or "**iCrypt**").

The Company is authorized and regulated in Estonia by the Financial Intelligence Unit (hereinafter the "FIU" and/or "competed supervisory authority")) and Tax and Customs Board to provide the following services:

a) Services of exchanging a virtual currency against a fiat currency, and
b) providing a virtual currency wallet service.

iCrypt developed a software platform which enable its Clients to make, via the internet, use of the above authorized services (hereinafter the "Services"). Clients are facilitated with a digital wallet, on a pay-per-transaction basis conduct cryptocurrency exchange transactions and transfer your electronic money or cryptocurrency to third parties online.

2. MANUAL APPLICABILITY: VIRTUAL CURRENCY EXCHANGE

The purpose of the Manual is to lay down the Company's internal practices, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing (hereinafter referred to as the "**AML**").

The Manual is developed and periodically updated by the Copany's Compliance Officer (hereinafter the "Compliance Officer") based on the general principles set up by the Company's Board of Directors (hereinafter the "Board") and Senior management in relation to the prevention of Money Laundering and Terrorist Financing.

The Manual shall be communicated to all the employees of the Company that manage, monitor or control in any way the Clients' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein.

The Manual has been prepared to comply with the provisions of AML Law of the Estonian Financial Intelligence Unit, Tax and Customs Board and EU Directive 2015/849.

The Manual applies to all Company's Clients as well as all the relevant Company's dealings with its Clients, including virtual currency exchange transactions and wallet services, irrespective of the Client account size and frequency of transactions.

In this respect, the Compliance Officer shall be responsible to update the Manual so as to comply with the relevant **Money Laundering and Terrorist Financing** (hereinafter the "**AML Laws**") and future requirements, as applicable, regarding the Client identification and due diligence procedures which the Company must follow.

"Money Laundering and Terrorist Financing" is defined as the process where the identity of the proceeds of crime is so disguised that it gives an impression of legitimate income (hereinafter referred to as the "**AML**").

Criminals particularly target financial services firms through which they attempt to launder their funds form criminal actions in order to clear their criminal funds, and the most challenging is that their intention is to do such clearing without the firms' knowledge or suspicion.

Therefore, the European Union has passed Directives designed to combat money laundering and terrorism financing. These Directives, together with regulations, rules and industry guidance, form the cornerstone of our AML obligations and outline the offenses and penalties for failing to comply with.

Whilst the cryptocurrency industry is currently unregulated and does not fall within the scope of many regulatory obligations, iCrypt have implemented systems and procedures that meet the standards set forth by the European Union for AML. These systems and procedures reflect the senior management's desire to prevent money laundering and not be used by criminals to launder proceeds of crime.

3. CORPORATE GOVERNANCE: RISK BASED APPROACH

3.1. Governing Body

The Governance Body of the company shall be the senior management, which is particularly the Board of Directors (hereinafter the "**Board**") and the Head Managers of the Company's functions.

The Board of Directors has appointed a management board member who is in charge of implementation of Money Laundering and Terrorist Financing Prevention Act and guidelines adopted on the basis thereof.

The management board member responsible for the AML function has appointed a person who acts as a contact person of the Financial Intelligence Unit Anti the Money Laundering Compliance Officer (hereinafter "**Compliance Officer**").

The FIU and the competent supervisory authority are informed of the appointment of a Compliance Officer.

The aim of the Governance Body in relation to the prevention of Money Laundering and Terrorist Financing include the following:

(a) to determine a general policy principle of the Company in relation to the prevention of Money Laundering and Terrorist Financing;
(b) to consult and ensure review and advices from a senior official that possesses the skills, knowledge and expertise relevant to the business and ensure that the policy determined is of the minimum standards requirements of the Law and of the Directive, as applicable.
(c) assure that appropriate, effective and sufficient systems and controls are introduced for achieving and satisfying the risks that the company may face;
(d) establish a process for monitoring all data and information concerning Clients' identity, transactions' documents (as and where applicable) and other relevant files and information maintained so as to be fully facilitated in the effective execution of the AML Policy;
(e) to establish a clear and quick reporting chain based on which information regarding suspicious transactions or solve uncertainties when employees find themselves in difficulty to asses any Client profile;
(f) to ensure sufficient resources, including competent staff and technological equipment, for the effective discharge of this Manual;
(g) to meet and decide the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies identified on ongoing basis;
(h) to develop and establish the Client Acceptance Policy and review such Policy as may be required from time to time;

3.2. Anti-Money Laundering Compliance Officer (the "Compliance Officer")

The Company ensures that only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties of a compliance officer may be appointed as a compliance officer.

The FIU shall verifying the suitability of the compliance officer or compliance officer candidate. Where, as a result of the check carried out by the Financial Intelligence Unit, it becomes evident that the person's reliability is under suspicion due to their past acts or omissions, the person's reputation cannot be considered impeccable and the Company may extraordinarily terminate the Compliance Officer's employment contract due to the loss of confidence.

The Compliance Officer will report directly to the board of the Company and has the competence, means and access to relevant information across all the units of the company for the purpose of performing its duties.

The duties of a Compliance Officer include, inter alia:

1) Review the AML Policy and this Manual of the Company and update it periodically as may be necessary;
2) to monitor and assess the correct and effective implementation of AML Policy and this Manual, the practices, measures, procedures and controls and in general the implementation of the Manual
3) Ensure the implementation of the AML Policy and this Manual throughout the company

4) In the event that the Compliance Officer identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, gives appropriate guidance for corrective measures and where deems necessary informs the Board;
5) to receive information from the Company's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities and take further actions as per the manual;
6) Organization of the collection and analysis of information referring to unusual transactions or transactions or circumstances suspected of money laundering or terrorist financing, which have become evident in the activities of the company;
7) reporting to the FIU in the event of suspicion of money laundering or terrorist financing;
8) periodic submission to the Board of written statements on compliance with the requirements arising from the relevant Laws;
9) to ensure the preparation and maintenance of the lists of Clients categorized, following a risk based approach, which contains, among others, the names of Clients, their account number and the dates of the commencement of the Business Relationship. Moreover, the Compliance Officer shall ensure that the said list is timely updated with all new or existing Clients, in light of any additional information obtained;
10) performance of other duties and obligations related to compliance with the requirements stipulated below;
11) to evaluate the systems and procedures applied by a third person on whom the Company may rely for Client identification and due diligence purposes, according to the Manual, and approves the cooperation with it;
12) to ensure that the branches and subsidiaries of the Company, if any, that operate in countries outside the EEA, have taken all necessary measures for achieving full compliance with the provisions of the Manual, in relation to Client identification, due diligence and record keeping procedures;

The Compliance Officer has the right to:

1) make proposals to the Board for amendment and modification of the rules of procedure containing AML requirements and organisation of employees appropriate training
2) demand that the departments of the Company eliminate within a reasonable time the deficiencies identified in the implementation of the AML requirements;
3) receive data and information required for performance of the duties of a compliance officer;
4) make proposals for organisation of the process of submission of notifications of suspicious and unusual transactions;
5) receive training in the field.

Where no Compliance Officer has been appointed, the duties of a Compliance Officer are performed by the Board of the Company.

3.3. The Risk Based Approach

The Company is taking security measures and has adopted policies, practices and procedures that promote high ethical and professional standards and prevent the Company from being used, intentionally or

unintentionally, by criminal elements. To prevent the abuse of its technologies and systems providing the Services, for the purpose of Money Laundering and Terrorist Financing.

The Company shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of Money Laundering and Terrorist Financing appears to be comparatively higher.

In this aspect the measures are being considered with a risk based approach to ensure that the risk of money laundering and terrorist financing is appropriately considered and managed in the course of daily activities.

The risk-based approach adopted by the Company, and described in the Manual, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the Money Laundering and Terrorist Financing risks faced by the Company.

The Company has put in place Know Your Customer (KYC) mechanisms as an essential element for service, risk management and control procedures. Such mechanisms include:

- Customer acceptance policy
- Customer identification policy - identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, financial instruments, services, and geographical areas of operation of its Clients;
- Ongoing monitoring of high-risk clients - continuous monitoring and improvements in the effective operation of the policies, procedures and controls.
- Risk management mechanism - managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
- Categorization of clients on a risk basis

KYC constitutes a core feature of services' risk management and control procedures. The intensity of KYC programs beyond these essential elements is tailored to the degree of risk.

The adopted risk-based approach that is followed by the Company, and described in the Manual, has the following general characteristics:

a) recognizes that the money laundering or terrorist financing threat varies across Clients and depend on different indicators:
    - countries of origin,
    - transaction origin - the country of origin and destination of Clients' funds
    - investment purposes and nature of business transactions,
    - the nature (e.g. non-face-to-face) and economic profile of Clients as well as of financial instruments and services offered,
    - the volume and size of transactions
b) allows the Board to differentiate between Clients in a way that matches the risk of their particular business;
c) allows the Board to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;
d) helps to produce a more cost-effective system;

e) promotes the prioritisation of effort and actions of the Company in response to the likelihood of Money Laundering and Terrorist Financing occurring through the use of the Services.

4. RISK MANAGEMNT FRAMEWORK

4.1. Identification of Risks

The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed.

The Company shall assess and evaluate the risks it faces, for the use of the Services for the purpose of Money Laundering or Terrorist Financing. The particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk.

The Company shall be, at all times, in a position to demonstrate that the extent of measures and control procedures it applies are proportionate to the risk it faces for the provision of the Services, for the purpose of Money Laundering and Terrorist Financing.

For the purpose of identification, assessment and analysis of risks of money laundering and terrorist financing related to their activities, the Company prepare a risk assessment, taking account of at least the following risk categories:

- risks relating to customers nature;
- risks relating to countries, geographic areas or jurisdictions
- risks relating to products, services or transactions
- risk relating to communication, mediation or products, services, transactions or delivery channels between the obliged entity and customers.

The steps taken to identify, assess and analyze risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of the Company.

As a result of the risk assessment, the Company established:

(a) fields of a lower, normal and higher risk of money laundering and terrorist financing;
(b) the risk appetite and services provided in the course of business activities;
(c) the risk management model, including simplified and enhanced due diligence measures, in order to mitigate identified risks.

The following, inter alia, are sources of risks which the Company faces with respect to Money Laundering and Terrorist Financing:

(a) Risks based on the Client's nature:

- complexity of ownership structure of legal persons;
- companies with bearer shares;
- companies incorporated in offshore centers;
- PEPs;
- Clients engaged in transactions which involves significant amounts of cash;
- Clients from high risk countries or countries known for high level of corruption or organised crime or drug trafficking;
- unwillingness of Client to provide information on the Beneficial Owners of a legal person

(b) Risks based on the Client's behaviour:

- situations where the origin of wealth and/or source of funds cannot be easily verified;
- unwillingness of Clients to provide information on the Beneficial Owners of a legal person.

(c) Risks based on the Client's initial communication with the Company:

- non-face-to-face Clients;
- Clients introduced by a third person.

(d) (d) Risks based on the Company's services:

- services that allow payments or transfers to third persons/parties;
- large cash deposits or withdrawals;

4.2. Measures and Procedures to Manage and Mitigate the Risks

Taking into consideration the assessed risks, the Company shall determine the type and extent of measures it will adopt in order to manage and mitigate the identified risks in a cost-effective manner. These measures and procedures include:

- adaption of rules of procedure that allow for effective mitigation and management of, inter alia, risks relating to money laundering and terrorist financing the Client Due Diligence Procedures in respect of Clients in line with their risk profile;
- assessed Money Laundering and Terrorist Financing risk;
- requiring the quality and extent of required identification data for each type of Client to be of a certain standard (e.g. documents from independent and reliable sources, third person information, further information and documentary evidence, etc.);
- obtaining additional data and information from the Clients, where this is appropriate for the proper and complete understanding of their activities and source of wealth and for the effective management of any increased risk;
- ongoing monitoring of high-risk Clients' transactions and activities, as and when applicable;

To follow the measure and procedures, the Company established, and states herein below, internal control rules that describe the internal control system including the procedure for the implementation of internal audit and, where necessary, compliance control.

The measure and procedures must contain at least the following:

(a) procedure for the application of due diligence measures regarding a customer, including a procedure for the application of simplified and enhanced due diligence, and even highly enhanced due diligence in exceptional cases or highly risk ranked customers (Paragraph 6 below).
(b) a model for identification and management of risks relating to a customer and the determination of the customer's risk profile;
(c) the methodology of handling suspicious customers or circumstances involved;
(d) instructions for performing the reporting obligation;
(e) the procedure for data retention and making data available;
(f) instructions for effectively identifying whether a person is a politically exposed person or a local politically exposed person subject to international sanctions or a person whose place of residence or seat is in a high-risk third country or country that meets the criteria;
(g) the procedure for identification and management of risks relating to new and existing technologies, and services and products, including new or non-traditional sales channels and new or emerging technologies.

The measure and procedures must be proportionate to the nature, size and level of complexity of the economic and professional activities of the Company and these must be established by the senior management.

The Company shall regularly check if the established measure and procedures and the internal control rules are up to date and, where necessary, establish new rules of procedure and internal control rules or make required modifications therein.

The Company shall ensure that the employees whose employment duties include the establishment of business relationships or the making of transactions are provided with training in the performance of the duties and obligations in accordance to Money Laundering and Terrorist Financing Prevention Act[1] and such training must be provided when the employee commences performance of the specified employment duties, and thereafter regularly or when necessary.

4.3. Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities change as well as the services by the Company change.

In this respect, it is the duty of the Compliance Officer to undertake regular reviews of the characteristics of existing Clients, new Clients, services and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented, as applicable.

4.4. Relevant International Organizations

For the development and implementation of appropriate measures and procedures on a risk based approach, and for the implementation of Client Identification and Due Diligence Procedures, the Compliance Officer and the Administration/Back-Office Department shall consult data, information and reports [e.g. Clients from countries which inadequately apply Financial Action Task Force's (hereinafter "FATF"), country assessment reports] that are published in the following relevant international organizations:

(a) FATF - www.fatf-gafi.org
(b) (b) The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (hereinafter "MONEYVAL") - www.coe.int/moneyval
(c) The EU Common Foreign & Security Policy (CFSP) - eeas.europa.eu/cfsp/
(d) The UN Security Council Sanctions Committees- www.un.org/sc/committees
(e) The International Money Laundering Information Network (IMOLIN) - www.imolin.org
(f) The International Monetary Fund (IMF) – www.imf.org

[1] Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

5. CLIENT ACCEPTANCE PROCESS

The Client Acceptance Policy (hereinafter, the "CAP"), following the principles and guidelines described in this Manual, defines the criteria for accepting new Clients and defines the Client categorization criteria which shall be followed by the Company and especially by the employees which shall be involved in the Client Account Opening process.

Having CAP the Company maintains clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk. Before accepting a potential client, Know Your Client (the "KYC") and due diligence procedures are followed, by examining factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators.

The General Principles of the CAP are the following:

(a) The Company shall classify Clients into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Client.
(b) Where the Client is a prospective Client, an account must be approved only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted, according to the principles and procedures set in Manual.
(c) No account shall be opened in anonymous or fictitious names(s).

5.1. Criteria for Accepting New Clients (based on their respective risk)

Upon assessment of factors referring to a higher risk, the following is deemed a situation increasing risks related to the customer as a person:

1) the business relationship foundations based on unusual factors, including in the event of complex and unusually large transactions and unusual transaction patterns that do not have a reasonable, clear economic or lawful purpose or that are not characteristic of the given business specifics;
2) the customer is a resident of a higher-risk geographic area listed in subsection 4 of this section;
3) the customer is a legal person or a legal arrangement, which is engaged in holding personal assets;
4) the customer is a cash-intensive business;
5) the customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;
6) the ownership structure of the customer company appears unusual or excessively complex, given the nature of the company's business.

Upon assessment of factors referring to a higher risk, in particular the following is deemed a situation increasing risks related to the product, service, transaction or delivery channel:

1) private banking;
2) provision of a product or making or mediating of a transaction that might favour anonymity;
3) payments received from unknown or unassociated third parties;
4) a business relationship or transaction that is established or initiated in a manner whereby the customer, the customer's representative or party to the transaction is not met physically in the same place;

5) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

Upon assessment of factors referring to a higher risk, in particular as situation where the customer, a person involved in the transaction or the transaction itself is connected with a following country or jurisdiction is deemed a factor increasing the geographical risk:

1) that, according to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective AML systems;
2) that, according to credible sources, has significant levels of corruption or other criminal activity;
3) that is subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
4) that provides funding or support for terrorist activities, or that has designated terrorist organizations operating within their country, as identified by the European Union or the United Nations.

Upon selection of enhanced due diligence measures the Company takes into account the relevant guidelines of the European supervisory authorities regarding risk factors.

The criteria for accepting new Clients and categorization of Clients based on their risk it is being described below. The Compliance Officer shall be responsible for categorizing Clients in one of the following three (3) categories based on the criteria of each category set below:

5.1.1. Low Risk Clients

The Company shall accept Clients who are categorized as low risk Clients as long as the general principles under this Paragraph 5 and the below Paragraph 6 are followed. The Simplified Client Identification and Due Diligence Procedures for low risk Clients shall be applied, according to Paragraph 6 of this Manual, and provided that there is a low risk or no suspicion for money laundering and terrorist financing:

- Credit or financial institution covered by the EU Directive.
- Credit or financial institution carrying out one or more of the financial business activities as these are defined by the Law and which is situated in a country outside the EEA, which:
    - in accordance with a decision of the Advisory Authority, imposes requirements equivalent to those laid down by the EU Directive (see Appendix 4 for the list of equivalent third countries), and
    - it is under supervision for compliance with those requirements.
- Listed companies whose securities are admitted to trading on a Regulated Market in a country of the EEA or in a third country which is subject to disclosure requirements consistent with community legislation.
- Domestic public authorities of countries of the EEA.
- Clients whose transaction doesn't exceed the value of 3,000Euros.
- And any other client that the company assesses to be of low risk in regard to money laundering.

5.1.2. Normal Risk Clients

These are the Clients who does not fall under the 'low risk Clients' or 'high risk Clients' categories set in this Paragraph.

The Company shall accept Clients who are categorized as normal risk Clients as long as the general principles under this Paragraph 5 and the below Paragraph 6 are followed. The Company shall apply the Enhanced Client Identification and Due Diligence measures for normal risk Clients, according to Paragraph 6 of this Manual.

5.1.3. High-Risk Clients

The Company shall accept Clients who are categorized as High-Risk Clients as long as the general principles under Paragraphs 5 and 6 of this Manual are followed.

Moreover, the Company shall apply the Highly Enhanced Client Identification and Due Diligence measures for high risk Clients, according Paragraphs 6 of the Manual and the due diligence and identification procedures for the specific types of High-Risk Clients shall be monitored by at least one member of the Governance Body, as applicable.

The Company has in place an internal procedure for KYC required documents for different types of High-Risk clients, depending on their profile and information recorded, geographical origin, behavior, funds origin, account value, etc.

The following types of Clients can be classified as High Risk Clients with respect to the Money Laundering and Terrorist Financing risk which the Company faces:

- Clients who are not physically present for identification purposes (non-face-to-face Clients);
- Clients whose own shares or those of their parent companies (if any) have been issued in bearer form;
- Trust accounts;
- 'Client accounts' in the name of a third person;
- PEPs' accounts;
- Clients who are involved in electronic gambling/gaming activities through the internet;
- Clients from countries which inadequately apply FATF's recommendations;
- Clients included in the leaked documents of Mossack Fonseca (Panama Papers);
- Cross-frontier correspondent banking relationships with credit institutions-Clients from third countries;
- Any other Clients that their nature entail a higher risk of money laundering or terrorist financing;
- Any other Client determined by the Company itself to be classified as such.

5.2. Not Acceptable Clients

The following list predetermines the type of Clients who are not acceptable for establishing a Business Relationship or an execution of an Occasional Transaction with the Company:

- Clients who fail or refuse to submit, the requisite data and information for the verification of his identity, without adequate justification

- Shell Banks
- Clients from the jurisdictions which are being banned by internal policies from the company or international legislative sanctions;
- any other that the Company considers risky to its business or suspicious in regards to Money Laundering and Terrorist Financing.

The Company will not accept as customers, persons or entitled from United States, Syria, Sudan, Iran, North Korea and other countries and jurisdictions, where these services can not be provided by legislation countries.

6. CLIENT DUE DILIGENCE AND IDENTIFICATION PROCEDURES

The Company applies due diligence measures:

1) upon establishment of a business relationship;
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;
3) upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided.
4) Where the Company's policy requires an enhanced due diligence depending on the exceeding of a certain sum deposit, the due diligence measures must be applied as soon as the exceeding of the sum becomes known or, where the exceeding of the sum depends on the making of several linked payments, as soon as the sum is exceeded.

For the purposes of this document, a customer/client includes: The person or entity that maintains an account with the Company or those on whose behalf an account is maintained (i.e. beneficial owners), the beneficiaries of transactions conducted by professional intermediaries.

The Company maintains a systematic procedure for identifying new customers and cannot enter into a service relationship until the identity of a new customer is satisfactorily verified. The Company may accept the transaction order however it will not activate the account completely until the client provides all the KYC documents and satisfy the Company.

The Company pays special attention in the case of non-EU resident customers and in no case are short-circuit identity procedures followed just because the new customer is unable to present enough documents and information to satisfy the KYC and due diligence procedures.

As part of its obligation to exercise due diligence in customer identification, the Company must confirm that the identity information which it holds for its customers remains fully updated with all necessary identification and information throughout the business relationship.

The Company maintains clear standards and policies, on what records must be kept for customer identification and individual transactions. Such practice is essential to permit the Company to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to

criminal prosecution. To ensure that records remain up-to-date and relevant, the Company undertakes regular reviews of existing records.

The Company reviews and monitors on a regular basis the validity and adequacy of customer identification information in its possession. Notwithstanding the above and taking into account the degree of risk, if it becomes apparent at any time during the business relationship that the Company lacks sufficient or reliable evidence (data) and information on the identity and financial profile of an existing customer, the Company will immediately takes all necessary actions using the identification procedures and measures to provide due diligence, in order to collect the missing data and information as quickly as possible and in order to determine the identity and create a comprehensive financial profile of the customer.

An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated, a significant transaction that appears to be unusual and/or a significant change in the situation and legal status of the customer such as:

- Volume of transactions,
- Value of transactions,
- Nature and source of funds
- Change of directors/secretary
- Change of registered shareholders and/or actual beneficiaries,
- Change of registered office
- Change of trustees
- Change of corporate name and/or trade name
- Change of main trading partners and/or significant new business
- Change of persons authorized to handle its account,
- Request for opening a new account in order to provide new investment services and/or financial instruments

However, if the Company becomes aware, at any time, that it lacks sufficient information about an existing customer, immediate steps are taken to ensure that all relevant information is obtained as quickly as possible. In no solution, remediation and/or mitigation has can be found then the Company will terminate the client's account, and not continue with his business.

Where the customer refuses or fails to provide the required documents and information for identification and creation of a financial portrait, during the execution of an individual transaction without adequate justification, the Company will not proceed in a contractual relationship or will not execute the transaction and may also report it to the competent authority. This can lead to a suspicion that the customer is engaged in money laundering and terrorist financing.

If during the business relationship the customer refuses or fails to submit all required documents and information, within reasonable time, the Company has the right to terminate the business relationship and close the accounts of the client. The compliance department also examines whether to report the case to the competent authority.

6.1. Identification requirements of a Natural Person

Client identification must be carried out as soon as reasonably practicable after first contact is made.

The company may relie on third parties to provide documents of behalf of the clients however this will be done only when that third party (the representative) will be able to provide the necessary documents of proof for his appointment and the reasoning of this appointment, as per the § 21. (3) of AML Act.

The Company obtains all information necessary to establish to its full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account. Therefore, the Company has categorized the clients as follows:

(a) Category 1 (Low risk Clients)- Simplified Client Identification and Due Diligence

1. The Company shall obtain the following information to ascertain the true identity of the natural persons:
   (a) true name and/or names used as these are stated on the official identity card or passport;
   (b) full permanent address, including postal code;
   (c) telephone (home and mobile) and fax numbers;
   (d) e-mail address, if any;
   (e) date and place of birth;
   (f) nationality; and
   (g) details of the profession and other occupations of the Client.

In order to verify the Client's identity/name the Company shall request the Client to present an original document which is issued by an independent and reliable source that carries the Client's photo (e.g. Passport, National Identity cards, Driving License etc.). After the Company is satisfied for the Client's identity from the original identification document presented, it will keep copies.

The Company shall be able to prove that the said document is issued by an independent and reliable source. In this respect, the Compliance Officer shall be responsible to evaluate the independence and reliability of the source and shall duly document and file the relevant data and information used for the evaluation, as applicable.

The company accepts copies of the documents, if no originals are provided, however in such a case the Company will conduct an additional verification check through a reliable electronic source (i.e. WorldCheck, etc.)

2. The Client's permanent address shall be verified by a recent (up to 6 months) one of the following documents:
   - a utility bill,
   - a local authority tax bill or
   - a bank statement or
   - any other document same with the aforesaid.

Verification of identity and current address should be sought from a reputable credit or financial institution in the applicant's country of residence.

Document acceptable and provided by the Clients must be provided preferably in color, copy must be clearly readable, full document must be visible and document must be valid for at least another 3 months.

3. In addition to the above, the Company shall require and receive information on public positions which the prospective Client holds or held in the last twelve (12) months as well as whether he is a close relative or associate of such individual, in order to verify if the Client is a PEP.

(b) Category 2 (Normal Risk Clients))- Enhanced Client Identification and Due Diligence

For Clients that fall within this Category the Enhanced Due Diligence shall be applied, where the Company may request the following additional information to the KYC Low Risk Clients:

(a) about the customer identification;
(b) about the planned substance of the business relationship;
(c) about the origin of the funds and wealth of the customer and its beneficial owner;
(d) about the underlying reasons of planned or executed transactions;
(e) any other information in order to assist the Company to decide whether to establish or continue a business relationship;

In addition, the Company may demand that a customer make a payment from an account held in the customer's name in a credit institution of a contracting state of the European Economic Area or in a third country that implements requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council.

The Company may also perform the following procedures as part of its independent and internal checks, when comes to a need of an enhanced due diligence:

(a) verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;
(b) 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;
(c) 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 sensibility of the transactions;
(d) the application of due diligence measures regarding the person or their representative while being at the same place as the person or their representative.

(c) Category 3, 4, 5 and 6 (High Risk Clients)- Highly Enhanced Client Identification and Due Diligence

For the High-Risk clients, the Company ensures to gather the documents that are requested from Low and Normal risk Clients, however they shall be in a certified true copy form or provide other additional documents, as the Company may see feet and reasonable.

Thus, in addition to the documents provided as part of the assessment in Category 1 and 2, the company may ask additional documents (as applicable) or the received once to be authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions.

If in doubt for the genuineness of any document (passport, national identity card or documentary evidence of address), the Company shall seek verification of identity with an Embassy or the Consulate of the issuing country or a reputable credit or financial institution situated in the Client's country of residence.

Further to the above, the Company shall request, depending on the circumstances and risk profile of the client, additional documents and a auto-portrait ('Selfie picture'), phone call, video call, proofs of source of funds and supportive documents, notarization KYC documents, and even apostilled documents. All these measures are being used according to the scale of risk being identified internally by the Governance Body.

In addition to the aim of preventing Money Laundering and Terrorist Financing, the abovementioned information is also essential for implementing the financial sanctions imposed against various persons by the United Nations and the European Union. In this respect, passport's number, issuing date and country as well as the Client's date of birth always appear on the documents obtained, so that the Company would be in the position to verify precisely whether a Client is included in the relevant list of persons subject to financial sanctions which are issued by the United Nations or the European Union based on a United Nations Security Council's Resolution and Regulation or a Common Position of the European Union's Council respectively.

6.2. Identification Requirements of a Legal Entity

Company searches, and other commercial enquiries to ensure that the applicant has not been or in the process of being dissolved, struck off, wound up or terminated. If changes to company structure occur or ownership occurs subsequent to opening of an account with the company, further checks should be made.

(a) Category 1 (Low risk Clients))- Simplified Client Identification and Due Diligence

The Company identifies a legal person by verifies and retains the following details on the legal person:

1. the name or business name of the legal person;
2. the registry code or registration number and the date of registration;
3. the names of the director, members of the management board or other body replacing the management board, and their authorisation in representing the legal person;
4. the details of the telecommunications of the legal person.

The information provided by the legal entity is verified by using information originating from a credible and independent source for that purpose and requesting the following documents:

1. the registry card of the relevant register;
2. the registration certificate of the relevant register, or
3. a document equal to the document specified above.

Where the original document is not available, the identity can be verified on the basis of a document which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions.

The Company shall take all necessary measures for the full ascertainment of the legal person's control and ownership structure as well as the verification of the identity of the natural persons who are the Beneficial Owners and exercise control over the legal person.

The verification of the identification of a legal person that requests the establishment of a Business Relationship or the execution of an Occasional Transaction, comprises the ascertainment of the following:

(a) the registered number;
(b) the registered corporate name and trading name used;
(c) the full addresses of the registered office and the head offices;
(d) the telephone numbers, fax numbers and e-mail address;
(e) the members of the board of directors;
(f) the individuals that are duly authorised to operate the account and to act on behalf of the legal person;
(g) (g) the Beneficial Owners of private companies and public companies that are not
(h) listed in a Regulated Market of an EEA country or a third country with equivalent
(i) disclosure and transparency requirements;
(j) (h) the registered shareholders that act as nominees of the Beneficial Owners;
(k) (i) the economic profile of the legal person, according to the provisions of Section

For the verification of the identity of the legal entity, the Company shall request and obtain, among others, original or certified true copies of the following documents:

(a) certificate of incorporation and certificate of good standing (where available);
(b) certificate of registered office;
(c) certificate of directors and secretary;
(d) certificate of registered shareholders in the case of private companies and public companies that are not listed in a Regulated Market of an EEA country or a third country with equivalent disclosure and transparency requirements;
(e) memorandum and articles of association of the legal person;
(f) a resolution of the board of directors for the opening of the account and granting authority to those who will operate it;
(g) in the cases where the registered shareholders act as nominees of the Beneficial Owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the Beneficial

Owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the Beneficial Owner has been agreed;

(h) documents and data for the verification, according to the procedures set in Sections 6.1 above of the identity of the persons that are authorised by the legal person to operate the account, as well as the registered shareholders and Beneficial Owners of the legal person.

Where deemed necessary for a better understanding of the activities, sources and uses of funds/assets of a legal person, the Company shall obtain copies of its latest audited financial statements (if available), and/or copies of its latest management accounts.

(b) Category 2 (Normal Risk Clients)- Enhanced Client Identification and Due Diligence

For Legal Entities that fall within this Category the Enhanced Due Diligence shall be applied, where the Company may request the following additional information:

(a) about the customer and its beneficial owner;
(b) about the planned substance of the business relationship;
(c) about the origin of the funds and wealth of the customer and its beneficial owner;
(d) about the underlying reasons of planned or executed transactions;
(e) any other information in order to assist the Company to decide whether to establish or continue a business relationship;

When an account has been opened, but problems of verification arise in the service relationship which cannot be resolved, the Company can close the account and return the money to the source from which it was received.

(d) Category 3, 4, 5 and 6 (High Risk Clients)- Highly Enhanced Client Identification and Due Diligence

Where the applicant legal entity falls within this category the Company will ask that all of the documents provided, as part of the main identification process as per the assessment in Category 1 and 2, be authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions.

As an additional due diligence measure, on a risk-sensitive basis, the Company shall carry out (when deemed necessary) a search and obtain information from the records of the Registrar of Companies and/or any other relevant competent authority in the legal entity's country of incorporation and/or request information from other sources in order to establish that the applicant company (legal person) is not, nor is in the process of being dissolved or liquidated or struck off from the registry of the Registrar of Companies and Official Receiver and that it continues to be registered as an operating company in the records of the appropriate authority of incorporation.

Further to the above, the Company shall request, depending on the circumstances and risk profile of the client, additional documents and an auto-portrait ('Selfie picture'), phone call, video call with the appointed/authorized person, proofs of source of funds and supportive documents, notarization KYC

documents of individuals, and even apostilled documents. All these measures are being used according to the scale of risk being identified internally by the Governance Body.

It is pointed out that, if at any later stage any changes occur in the structure or the ownership status or to any details of the legal entity, or any suspicions arise emanating from changes in the nature of the transactions performed by the legal entity via its account, then it is imperative that further enquiries should be made for ascertaining the consequences of these changes on the documentation and information held by the Company for the legal entity and all additional documentation and information for updating the economic profile of the legal entity is collected.

In the case that the direct/immediate and principal shareholder is another legal entity the Company shall verify the ownership structure and the identity of the natural persons who are the Beneficial Owners and/or control the other legal entity.

Apart from verifying the identity of the Beneficial Owners, the Company shall identify the persons who have the ultimate control over the legal person's business and assets. In the cases that the ultimate control rests with the persons who have the power to manage the funds, accounts or investments of the legal entity without requiring authorization and who would be in a position to override the internal procedures of the legal entity, the Company, shall verify the identity of the natural persons who exercise ultimate control as described above even if those persons have no direct or indirect interest or an interest of less than 10% in the legal person's ordinary share capital or voting rights.

6.3. Establishing the Source of Funds as part of Enhanced Due Diligence (EDD)

The company should follow a risk-based approach when establishing Source of Funds ("SOF"). The risk-based approach is that the Company is on alert to any possibility that the funds may not be from a legitimate source or are not destined for a legitimate purpose. For example, when funds are sourced from a high-risk third country with inadequate AML legislation and regime, it is appropriate to obtain more information before proceeding with any transaction. A detail / extent depends on the client's money laundering and terrorist finance risks.

For the purpose of ensuring that the source of the funds is legitimate, the Company undertakes the following measures:

1. Considers the reliability of the client based on the information provided;
2. Questions information and/or proof documents of the source of funds that the client intends to invest for the use of Services;
3. Considers the jurisdiction and the bank rating that those money are being transferred;
4. Considers whether the funds are being transferred from an account which is held in name of the client or a third party;

Where the funds come from a third party, the risk is greater and further enquiries shall be made by the Company:

- about the relationship between the client and the ultimate underlying principal of the funds (i.e. the actual provider of the funds)

- assessing whether the purpose of the transaction is in line with the documented profile of the client.

The Company undertakes to ensure that that the source of funds is logical and backed by supporting documentation (e.g. a deed of sale, etc.). See Appendix III for examples of details required when assessing the source of funds, together with suggested documentary evidence.

6.4. Account in names of companies whose shares are in bearer form

The Compliance Officer shall apply the following with respect to accounts in names of companies whose shares are in bearer form:

1. The Company may accept a request for the establishment of a Business Relationship or for an Occasional Transaction from companies whose own shares or those of their parent companies (if any) have been issued in bearer form by applying, in addition to the procedures above, all the following supplementary due diligence measures:
   (a) The Company takes physical custody of the bearer share certificates while the Business Relationship is maintained or obtains a confirmation from a bank operating in a country of the EEA that it has under its own custody the bearer share certificates and, in case of transferring their ownership to another person, shall inform the Company accordingly.
   (b) The account is closely monitored throughout its operation. At least once a year, a review of the accounts' transactions and turnover is carried out and a note is prepared summarizing the results of the review which shall be kept in the Client's file.
   (c) If the opening of the account has been recommended by a third person, at least once every year, the third person who has introduced the Client provides a written confirmation that the capital base and the shareholding structure of the legal entity or that of its holding company (if any) has not been altered by the issue of new bearer shares or the cancellation of existing ones. If the account has been opened directly by the legal entity, then the written confirmation is provided by the legal entity's directors.
   (d) When here is a change to the Beneficial Owners, the Company examines whether or not to permit the continuance of the account's operation.

6.5. Trust accounts

In cases where the Beneficial Owner of a legal person, requesting the establishment of a Business Relationship or the execution of an Occasional Transaction is under a trust the Company shall implement the following procedure:

(a) The Company shall ascertain the legal substance, the name and the date of establishment of the trust and verify the identity of the trustor, trustee and Beneficial Owners, according to the procedures set in this Manual.
(b) Furthermore, the Company shall ascertain the nature of activities and the purpose of establishment of the trust as well as the source and origin of funds requesting the relevant extracts from the trust deed and any other relevant information from the trustees. All relevant data and information should be recorded and kept in the Client's file.

6.6. 'Client accounts' in the name of a third person

The Company shall apply the following with respect to "Client accounts" in the name of a third person:

1) The Company may open "client accounts" (e.g. omnibus accounts) in the name of financial institutions from EEA countries or a third country which, in accordance with a relevant decision of the Advisory Authority it has been determined that the relevant third country applies procedures and measures for preventing Money Laundering and Terrorist Financing equivalent to the requirements of the EU Directive (see Appendix 4 for the list of equivalent third countries). In these cases, the Company shall ascertain the identity of the abovementioned financial institutions according to the Client identification procedures prescribed in throughout the Manual.
2) In case the Company receives a request to open "client accounts" (e.g. omnibus accounts) in the name of financial institutions originating from countries other than the EEA or an equivalent third country, then the Company shall examine such requests on a case by case basis and shall undertake additional due diligence measures on such financial institutions. Such additional measures shall include a country-profile assessment in terms of AML reputation and legislation, analysis of the AML measures applied by such financial institutions, whether he financial institution is supervised in terms of AML, analysis of the line of business and clientele type of the financial institution and any additional measures deemed necessary during the assessment. It is stressed that the Company shall be extra vigilant on such cases.

3) In the case that the opening of a "client account" is requested by a third person acting as an auditor/accountant or an independent legal professional or a trust and company service provider situated in a country of the EEA or a third country which, in accordance with a relevant decision of the Advisory Authority it has been determined that the relevant third country applies procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the EU Directive (see Appendix 4 for the list of equivalent third countries), the Company shall proceed with the opening of the account provided that the following conditions are met:

    (a) the third person is subject to mandatory professional registration in accordance with the relevant laws of the country of operation;
    (b) the third person is subject to regulation and supervision by an appropriate competent authority in the country of operation for Anti-Money Laundering and Terrorist Financing purposes;
    (c) The Compliance Officer has assessed the Client identification and due diligence procedures implemented by the third person and has found them to be in line with the Law and the Directive. A record of the assessment should be prepared and kept in a separate file maintained for each third person;
    (d) the third person makes available to the Company all the data and documents prescribed in the Manual.

6.7. Accounts represented by a third party:

The obliged entity identifies the customer's representative and retains the same personal data as of the customer. However, in addition to the KYC and onboarding process described in this manual, the representative shall provide evidence of 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.

A representative of a legal entity applying for an account with the Company must submit a document certifying his or her powers, which has been authenticated by a notary or in accordance with an equal procedure and legalized or certified by a certificate replacing legalization (apostille), unless otherwise provided for in an international agreement.

The certification and legalization of such document it is being requested by the company only in in cases of High-Risk Clients who necessitate Highly Enhanced Due Diligence. In other cases the signature of the customer shall satisfy the company.

Reliance on data gathered by other person ("third party") and outsourcing of application of due diligence measures

The Company may rely on data and documents gathered by another person ("third party"), where all the following criteria are met:

1) the Company gathers at least from that third-party the due diligence information, their representative and the beneficial owner, as well as what is the purpose and nature of the business relationship or transaction;
2) the Company has ensured that, where necessary, it is able to immediately obtain all the data and documents whereby it relied on data gathered by another person;
3) the Company has established that the third party who is relied on is required to comply and actually complies with requirements equal to those established by Directive (EU) 2015/849 of the European Parliament and of the Council, including requirements for the application of due diligence measures, identification of politically exposed persons and data retention, and is under or is prepared to be under state supervision regarding compliance with the requirements;
4) the obliged entity takes sufficient measures to ensure compliance with the criteria provided herein.

The Company may also outsource an activity related to the clients' identification:

1) another obliged entity;
2) an organisation, association or union whose members are obliged entities, or
3) another person who applies the due diligence measures and data retention requirements provided by AML Laws and who is subject to or is prepared to be subject to AML supervision or financial supervision in a contracting state of the European Economic Area regarding compliance with requirements.

To outsource an activity, the obliged entity concludes a written contract which ensures that:

1) the outsourcing of the activity does not impede the activities of the Company or performance of the duties and obligations provided in applicable AML Laws;
2) the third party performs all the duties of the Company relating to the outsourcing of the activity;
3) the outsourcing of the activity does not impede exercising supervision over the Company;
4) the competent authority can exercise supervision over the person carrying out the outsourced activity via the Company, including by way of an on-site inspection or another supervisory measure;
5) the third party has the required knowledge and skills and the ability to comply with the requirements provided in this manual and the relevant AML Laws;
6) the Company has the right to, without limitations, inspect compliance with the requirements provided for in this Act;
7) documents and data gathered are retained and, at the request of the Company, copies of documents relating to the identification of a customer and its beneficial owner or copies of other relevant documents are handed over or submitted to the competent authority immediately.

In case of any outsourcing arrangements the Company shall be responsible for compliance with requirements arising from AML Laws.

6.8. Transactions with Politically Exposed People ("PEP")

When the client is a PEP, a family member of a PEP or a person known to be a close associate of a PEP, the Company applies the following due diligence measures in addition to the due diligence measures stipulated above in this manual:

(i). have appropriate risk-based procedures to determine whether the Client (or the Beneficial Owner) is a PEP;
(ii). ii. have Senior Management approval for establishing Business Relationships with such Clients or for the continuation of the Business Relationships with existing Clients which have become PEPs;
(iii). take adequate measures to establish the source of wealth and source of funds;
(iv). categorize the client as high-risk and conduct enhanced on-going monitoring of the Business Relationship.

Where a PEP no longer performs important public functions placed upon them, the Company must at least within 12 months take into account the risks that remain related to the person and apply relevant and risk sensitivity-based measures as long as it is certain that the risks characteristic of PEPs no longer exist in the case of the person.

6.9. Correspondent relationship with credit institution of third country

In respect of cross-frontier correspondent banking relationships with credit institutions-Clients from third countries, the Company shall:

(i). gather sufficient information about the credit institution-Client to understand fully the nature of the business and the activities of the Client and to assess, from publicly available information, the reputation of the institution and the quality of its supervision;

(ii). assess the systems and procedures applied by the credit institution-Client for the prevention of Money Laundering and Terrorist Financing;
(iii). obtain approval from the Senior Management before entering into correspondent bank account relationship;

7. ON-GOING MONITORING PROCESS

The Company established principles for monitoring a business relationship which include at least the following:

1) checking of transactions made in a business relationship in order ensure that the transactions are in concert with the Company's knowledge of the customer, its activities and risk profile;
2) regular updating of relevant documents, data or information gathered in the course of application of due diligence measures;
3) identifying the source and origin of the funds used in a transaction;
4) in economic or professional activities, paying more attention to transactions made in the business relationship, the activities of the customer and circumstances that refer to a criminal activity, money laundering or terrorist financing or that a likely to be linked with money laundering or terrorist financing, including to complex, high-value and unusual transactions and transaction patterns that do not have a reasonable or visible economic or lawful purpose or that are not characteristic of the given business specifics;
5) in economic or professional activities, paying more attention to the business relationship or transaction whereby the customer is from a high-risk third country or a country or territory or whereby the customer is a citizen of such country or whereby the customer's place of residence or seat or the seat of the payment service provider of the payee is in such country or territory.
6) the nature, reason and background of the transactions as well as other information that allows for understanding the substance of the transactions must be identified and more attention must be paid to these transactions.

8. SUSPICIOUS TRANSACTIONS

8.1. Suspicious Transactions

Where the Company identifies an activity or facts whose characteristics refer to the use of criminal proceeds or terrorist financing or to the commission of related offences or an attempt thereof or with regard to which the obliged entity suspects or knows that it constitutes money laundering or terrorist financing or the commission of related offences (the "suspicious transaction"), the Company will report such case to the Financial Intelligence Unit ("FIU") immediately, but not later than within two working days.

A suspicious transaction will often be one which is inconsistent with a Client's known, legitimate business or personal activities or with the normal business of the specific account. The Company shall ensure that it maintains adequate information and knows enough about its Clients' activities in order to recognize on time that a transaction or a series of transactions is unusual or suspicious.

In order to identify suspicious transactions, the Company's Compliance officer shall perform the following activities:

- monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc.
- receive and investigate information from the Company's employees, on suspicious transactions which creates the belief or suspicion of money laundering. The information is received in a written report form (hereinafter the "Internal Suspicion Report"), a specimen of such report is attached in Appendix 1 of the Manual;
- evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the Compliance Officer is evaluated and shall be done on a report (hereinafter the "Internal Evaluation Report"), a specimen of such report is attached in Appendix 2 of the Manual;
- if, as a result of the evaluation described above, the Compliance Officer decides to disclose this information to FIU, then he prepares a written report, which he submits to the Unit, according to Section 8.2 below.
- if as a result of the evaluation described above, the Compliance Officer decides not to disclose the relevant information to the Unit, then he fully explain the reasons for his decision on the Internal Evaluation Report.

8.2. Report to FIU

The Company shall notify FIU of each learned transaction whereby a pecuniary obligation of over 32 000 euros or an equal sum in another currency is performed in cash, regardless of whether the transaction is made in a single payment or in several linked payments over a period of up to one year, and shall assist FIU with any additional information requested and available to the Company.

In case of any such suspicion, the Company may suspend and/or postpone the transaction until the report, as per this paragraph, is made. If such suspension and/or postponement may cause considerable harm, it is not possible to omit the transaction or it may impede catching the person who committed possible money laundering or terrorist financing, the transaction or professional act will be carried out or the Service will be provided and a report will be submitted the FIU thereafter.

The report is submitted via the online form of the Financial Intelligence Unit or via the X-road service.

The data used for identifying the person and verifying the submitted information and, if any, copies of the documents are added to the report.

The Company will not inform the person, its beneficial owner, representative or third party about a report submitted on them to the FIU, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the FIU or about the commencement of criminal proceedings. After a precept made by the FIU has been complied with, the Company may inform a person that the FIU has restricted the use of the person's account or that another restriction has been imposed.

The prohibition of informing is not applied upon submission of information to:

1) competent supervisory authorities and law enforcement agencies;
2) credit institutions and financial institutions in between themselves where they are part of the same group;
3) institutions and branches that are part of the same group where the group applies group-wide procedural rules and principles in accordance with AML Laws;
4) a third party who operates in the same legal person or structure as an obliged entity who is a notary, enforcement officer, bankruptcy trustee, auditor, attorney or other legal service provider, provider of accounting services or provider of advisory services in the field of accounting or taxation and whereby the legal person or structure has the same owners and management system where joint compliance is practiced.

The exchange of information regulated in this section must be retained in writing or in a form reproducible in writing for the next five years and information is submitted to the competent supervisory authority at its request.

8.3. Discharge of liability

The Company, its employee, representative and the person who acted on its behalf is not liable for damage caused to a person or customer participating in a transaction in the provision of Services:

1) upon performance of duties and obligations arising from AML Laws in good faith, from failing to make the transaction or from failing to make the transaction within the prescribed time limit;
2) in connection with the performance of the duty to report in good faith;
3) by implementing cooperation and exchange of information and considering the concerns when establishing relationships with shell banks in good faith.

The performance of the duty to report and submission of information by the Company is not deemed breach of the confidentiality requirement arising from law or contract and the statutory or contractual liability for the disclosure of the information is not applied to the person who performed the duty to report. An agreement derogating from this provision is void.

The Company established a system of measures ensuring that its employees and representatives who are involved in the report and submission of information, either within the obliged entity or directly to the FIU, are protected from being exposed to threats or hostile action by other employees, management body members or customers of the obliged entity, in particular from adverse or discriminatory employment actions.

9. RECORD-KEEPING AND DATA PROTECTION PROCEDURES

The Company has in place mechanisms and secured systems in order to ensure a proper record of the business conducted and services provided to its Clients. The Company registers the following:

1) transaction date or period and a description of the substance of the transaction.

2) the account type, number, the monetary value of the transaction, the currency and any significant characteristics, if available;
3) the deposition number and the market price of the product on the date of deposition or a detailed description of the property where the market price of the property cannot be determined;
4) information on the circumstance of refusal to establish a business relationship or make an occasional transaction (if applicable);
5) the circumstances of a waiver to establish a business relationship or make a transaction, including. an occasional transaction, on the initiative of a person participating in the transaction or professional act, a person using the official service or a customer where the waiver is related to the application of due diligence measures by the obliged entity (if applicable);
6) information according to which it is not possible to take the due diligence measures using information technology means;
7) information on the circumstances of termination of a business relationship in connection with the impossibility of application of the due diligence measures;
8) information serving as the basis for the duty to report under § 49 of this Act;
9) upon making transactions with a civil law partnership, community or another legal arrangement, trust fund or trustee, the fact that the person has such status, an extract of the registry card or a certificate of the registrar of the register where the legal arrangement has been registered.

The Company will retain records of the following for no less than ***five years*** after making the transaction, termination of the business relationship and/or performing the duty to report:

1) the originals or copies of the documents which serve as the basis for identification and verification of persons;
2) the document prescribed for the digital identification of a person, any electronic enquiry to the identity documents database, and the audio and video recording of the procedure of identifying the person and verifying the person's identity, as applicable;
3) the documents serving as the basis for the establishment of a business relationship;
4) the entire correspondence relating to the performance of the duties and obligations arising from AML Laws;
5) all the data and documents gathered in the course of monitoring the business relationship
6) all the data on suspicious or unusual transactions or circumstances which the FIU was not notified of.

The Company will retain the above documents and data in a manner that allows for exhaustively and immediately replying to the enquiries of the FIU or, in accordance with legislation, those of other supervisory authorities, investigative bodies or courts, inter alia, regarding whether the obliged entity has or has had in the preceding five years a business relationship with the given person and what is or was the nature of the relationship.

Where the Company makes, for the purpose of identifying a person, an enquiry with a database that is part of the state information system, the record-keeping duties will be deemed performed where information on the making of an electronic enquiry to the register is reproducible over a period of five years after termination of the business relationship or making of the transaction.

9.1. Protection of personal data

The Company implements all rules of protection of personal data upon application of the requirements arising from AML Laws and Data Protection Laws (including and considering the RU General Data Protection Rules).

The Company has in place a Privacy Policy which implements the minimum standards for the safeguarding of data collected and the process of data processing. The Privacy Policy is being properly communicated to the Clients.

In regards to money laundering and terrorist financing, the Company is allowed to process personal data gathered only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

The Company submits information concerning the processing of personal data before establishing a business relationship or making an occasional transaction with eth Clients. General information on the duties and obligations of the obliged entity upon processing personal data for AML purposes is given among this information.

10. EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING

The Company ensures that the employees whose employment duties include the establishment of business relationships or the making of transactions are provided with training in the performance of the duties and obligations arising from AML Laws and this policy, and such training must be provided when the employee commences performance of the specified employment duties, and thereafter regularly or when necessary.

In training, information, inter alia, on the duties and obligations provided for in the rules of procedure, modern methods of money laundering and terrorist financing and the related risks, the personal data protection requirements, on how to recognize acts related to possible money laundering or terrorist financing, and instructions for acting in such situations must be given.

The Compliance Cfficer has the duty to make proposals to the management board on organization of trainings of the employees and representatives of the Company and must keep a record file of all trainings performed and planned once.

APPENDIX I

INTERNAL SUSPICION REPORT
FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER'S DETAILS

Name: ..... Tel: .....

Department: ..... Fax: .....

Position: .....

CLIENT'S DETAILS

Name: ..... Date of Birth: .....

Address: .....

.....

Tel: ..... Occupation: .....

Fax: ..... Details of Employer: .....

Passport No.: ..... Nationality: .....

ID Card No.: ..... Other ID Details: .....

INFORMATION/SUSPICION

Brief description of activities/transaction: .....

.....

Reason(s) for suspicion: .....

.....

.....

Informer's Signature Date

..... ……....

FOR COMPLIANCE OFFICER'S USE

Date Received: ..... Ref. .....

Reported to FIU: Yes/No ..... Date Reported: ..... Ref .....

APPENDIX II

INTERNAL EVALUATION REPORT
FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference: ..... Client's Details: .....

Informer: ..... Department: .....

INQUIRIES UNDERTAKEN (Brief Description)

.....

.....

.....

.....

.....

.....

.....

.....

.....

ATTACHED DOCUMENTS

.....

.....

.....

COMPLIANCE OFFICER'S DECISION

.....

.....

.....

COMPLIANCE OFFICER'S SIGNATURE.....

DATE.....

APPENDIX III

List of examples of appropriate information and/or supporting documents required to establish Source of Funds:

Source of funds/wealth	Information / Documents that may be required
Employment Income	- Nature of employer's business - Name and address of the employer - Annual salary and bonuses for the last couple of years - Last month/recent pay slip - Confirmation from the employer of annual salary - Latest accounts or tax declaration if self employed
Savings / deposits	- Bank statement and enquiry of the source of wealth
Property Sale	- Details of the property sold (i.e. address, date of sale, sale value of property sold, parties involved) - Copy of contract of sale - Title deed from land registry
Sale of shares or other investment	- Copy of contract - Sale value of shares sold and how they were sold (i.e. name of stock exchange) - Statement of account from agent - Transaction receipt/confirmation - Shareholder's certificate - Date of sale
Loan	- Loan agreement - Amount, date and purpose of loan - Name and address of Lender - Details of any security
Company Sale	- Copy of the contract of sale - Internet research of Company Registry - Name and Address of Company - Total sales price - Clients' share participation - Nature of business - Date of sale and receipt of funds - Media coverage
Company Profits / Dividends	- Copy of latest audited financial statements - Copy of latest management accounts - Board of Directors approval - Dividend distribution - Tax declaration form

APPENDIX IV

Third countries outside the EEA which impose procedures and take measures for preventing money laundering and terrorist financing equivalent to those laid down by the EU Directive.

The list of the said countries may be reviewed, in particular in light of public evaluation reports adopted by the FATF, FSRBs, the IMF or the World Bank according to the revised 2003 FATF Recommendations and Methodology. Currently, these countries are:

1. Argentina
2. Australia
3. Brazil
4. Canada
5. China
6. French overseas territories (Mayotte, New Caledonia, French Polynesia, Saint Pierre and Miquelon and Wallis and Futuna) *
7. Dutch overseas territories (Aruba, Curacao, Sint Maarten, Bonaire, Sint Eustatius and Saba) *
8. Hong Kong
9. India
10. Israel
11. Japan
12. South Korea
13. Malaysia
14. Mexico
15. New Zealand
16. Russian Federation
17. Singapore
18. Switzerland
19. South Africa
20. The United States of America
21. Turkey
22. UK Crown Dependencies (Jersey, Guernsey, Isle of Man) may also be considered as equivalent by Member States
23. United States.
24. Those overseas territories which are not members of the EU/EEA but are part of the membership of France and the Kingdom of the Netherlands of the FATF.

Jurisdictions with strategic AML deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies. The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction:

1. North Kores - Democratic People's Republic of Korea (DPRK)
2. Iran
3. Yemen
4. Tunisia
5. Sri Lanka
6. Trinidad and Tobago
7. Syria
8. Ethiopia
9. Serbia

10. The Bahamas
11. Botswana
12. Cambodia
13. Ghana
14. Pakistan