GUIDELINES FOR ANTI-MONEY LAUNDERING, COMBATING FINANCING TERRORIST AND SANCTION MEASURES

INTRODUCTION

DEFINITIONS………..

PRINCIPLES FOR STRUCTURE AND MANAGEMENT OF THE COMPANY……………………………..

THE MANAGEMENT BOARD ……………………………………………………………………………………

THE FIRST LINE OF DEFENSE – THE EMPLOYEES ……………………………………………………………..

THE SECOND LINE OF DEFENSE – RISK MANAGEMENT AND COMPLIANCE, MLRO …………..

THE THIRD LINE OF DEFENSE – INTERNAL AUDIT ……………………………………………………………..

PRINCIPLES OF CUSTOMER DUE DILIGENCE MEASURES IMPLEMENTATION ……………………..

MAIN PRINCIPLES……

THE LIST OF CUSTOMER DUE DILIGENCE MEASURES…………………………………………………..

THE VERIFICATION OF INFORMATION USED FOR THE CUSTOMER’S IDENTIFICATION…….

APPLICATION OF SIMPLIFIED DUE DILIGENCE MEASURES (LEVEL 1)
APPLICATION OF STANDARD DUE DILIGENCE MEASURES (LEVEL 2)
APPLICATION OF ENHANCED DUE DILIGENCE MEASURES (LEVEL 3)

CUSTOMER DUE DILIGENCE MEASURES………………………………………………………………………

IDENTIFICATION OF THE CUSTOMER – NATURAL PERSON……………………………………………

IDENTIFICATION OF THE CUSTOMER – LEGAL ENTITY…………………………………………………….

THE IDENTIFICATION OF THE CUSTOMER’S BENEFICIAL OWNER…………………………………

POLITICAL EXPOSED PERSON’S IDENTIFICATION……………………………………………………………

IDENTIFICATION OF THE PURPOSE AND NATURE OF THE BUSINESS RELATIONSHIP OR A TRANSACTION………..

MONITORING OF THE BUSINESS RELATIONSHIP…………………………………………………………..

IMPLEMENTATION OF SANCTIONS………………………………………………………………………..

PROCEDURE FOR IDENTIFYING THE SUBJECT OF SANCTIONS AND A TRANSACTION VIOLATING SANCTIONS ………………………………………………………………………………………..

PROCEDURE IN THE EVENT OF IDENTIFICATION OF THE SUBJECT OF SANCTIONS OR A TRANSACTION VIOLATING SANCTIONS …………………………………………………………………..

REFUSAL TO THE TRANSACTION OR BUSINESS RELATIONSHIP AND THEIR TERMINATION

REPORTING OBLIGATION ……………………………………………………………………………………….

TRAINING OBLIGATION …………………………………………………………………………………………

COLLECTION AND PRESERVATION OF DATA ………………………………………………………….

AVOIDING CONFLICT OF INTERESTS ……………………………………………………………………

INTERNAL CONTROL OF EXECUTION OF THE GUIDELINES …………………………………………..

ANNEXES ……

VERSION CONTROL TABLE ………………………………………………………………………………….

INTRODUCTION

The purpose of these Guidelines for Anti-Money Laundering (AML), Combating Terrorist Financing (CFT) and Sanctions measures is to ensure that Maindprofit LTD (Company) has internal guidelines to prevent the use of its business for money laundering and terrorist financing and internal guidelines for implementation of international sanctions.

DEFINITIONS

The Company means legal entity with following data:

company name: Maindprofit LTD
registration number: 2023 - 00283
address: Ground Floor, TheSotheby Building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia.

The Guidelines – this document including all annexes as provided above. The Guidelines include inter alia the Company's Internal control rules regarding the Guidelines and the Company's risk assessment policy regarding risk based approach for ML/TF risks.

The Money Laundering (ML) means the concealment of the origins of illicit funds through their introduction into the legal economic system and transactions that appear to be legitimate. There are three recognized stages in the money laundering process:

placement, which involves placing the proceeds of crime into the financial system;
layering, which involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds; integration, which involves placing the laundered proceeds back into the economy to create the perception of legitimacy
The Terrorist Financing (TF) means the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism in the meaning of applicable legislation.

International sanctions may ban the entry of a subject of an international sanction in the state, restrict international trade and international transactions, and impose other prohibitions or obligations.

The subject of Sanctions is any natural or legal person, entity, or body, designated in the legal act imposing or implementing Sanctions, with regard to which the Sanctions apply.

The Customer means a natural person or a legal entity which has the business relationship with the Company or a natural person or legal entity with which the Company enters into the occasional transaction.

The Beneficial Owner means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or exercises control in another manner over a transaction, act, action, operation or step or over another person and in whose interests or for whose benefit or on whose account a transaction or act, action, operation or step is made. In the case of a legal entity, the beneficial owner is a natural person whose direct or indirect holding, or the sum of all direct and indirect holdings in the legal person, exceeds 25 percent, including holdings in the form of shares or other forms of bearer.

The Employee means the Company´s employee, including persons which are involved in application of these Guidelines in the Company.

The Management Board means management board of the Company.

The Business Relationship means a relationship that is established upon conclusion of a longterm contract by the Company in economic or professional activities for the purpose of provision of a service or distribution thereof in another manner or that is not based on a

long-term contract, but whereby a certain duration could be reasonably expected at the time of establishment of the contact and during which the Company repeatedly makes separate transactions in the course of economic or professional activities while providing a service.

The Occasional Transaction means the transaction performed by the Company in the course of economic or professional activities for the purpose of provision of a service or sale of goods or distribution thereof in another manner to the Customer outside the course of an established business relationship.

PRINCIPLES FOR STRUCTURE AND MANAGEMENT OF THE COMPANY

The organizational structure of the Company must correspond to its size and the nature, scope, and level of complexity of its activities and services provided, including the risk appetite and related risks, and must be structured in accordance with the principle of three lines of defense. The organizational structure of the Company must correspond to the complete understanding of potential risks and their management. The reporting and subordination chains of the Company must be ensured in such a way that all employees know their place in the organizational structure and know their work duties.

The Management Board

The Management Board is the carrier of the culture of compliance with the requirements of money laundering and terrorist financing prevention, guaranteeing that the Management Board members and employees of the Company operate in an environment where they are fully aware of the requirements for the prevention of money laundering and terrorist financing and the obligations associated with these requirements, and the relevant risk considerations are taken into account to a suitable extent in the decision-making processes of the Company.

The Management Board members bear ultimate responsibility for the measures taken to prevent the use of the Company's services for money laundering or terrorist financing. They provide oversight and are accountable for:

establishing and maintaining AML[1] processes, procedures, risk, and control processes;
adopting these Guidelines and other internal guidelines and instructions;
determining the Company's Guidelines for AML measures;
appointing an MLRO and ensuring that the MLRO has the powers, resources and expertise required to perform their assignment;
allocating sufficient resources to ensure the effective implementation of the Guidelines and other related documents and to maintain the organization;
ensuring all relevant employees complete annual AML training.

The first line of defense – the Employees

The first line of defense has the function of applying the due diligence measures upon business relationship and occasional transactions and applying due diligence measures during the business relationship. First line of defense comprises the structural units and employees of the Company with whose activities risks are associated and that must identify and assess these risks, their specific features and scope and that manage these risks by way of their ordinary activities, primarily by way of application of due diligence measures. The risks arising from the activities of and provision of services by the Company belong to the first line of defense. They are the managers (owners) of these risks and responsible for them.

The employees of the Company must act with the foresight and competence expected from them and according to the requirements set for their positions, proceeding from the interests and the goals of the Company, and ensure that the country's financial system and economic space are not used for money laundering and terrorist financing. The Company takes measures to assess the suitability of the employees before they start working with the relevant training.

For the aforementioned reasons, the employees are required to:
adhere to all requirements outlined in the Guidelines and other related documents;
collect required customer information in accordance with their function and accountabilities; report information, situations, activities, transactions or attempted transactions that are unusual for any type of service or customer relationship, regardless of the amount, whether or not the transaction was completed without delay to the MLRO;
not inform or otherwise make customers aware if the customer or any other customers are or may be the subject of a report or if a report has been or may be filed;
complete the appropriate AML training required for the employee's position.

The second line of defense – Risk Management and Compliance, MLRO

The second line of defense consists of the risk management and compliance functions. These functions may also be performed by the same person or structural unit depending on the size of the Company and the nature, scope and level of complexity of their activities and provided services, incl. the risk appetite and risks arising from activities of the Company.

The objective of the compliance function is to guarantee that the Company complies with effective legislation, guidelines and other documents and to assess the possible effect of any changes in the legal or regulative environment on the activities of the Company and on the compliance framework. The task of compliance is to help the first line of defense as the owners of risk to define the places where risks manifest themselves (e.g., analysis of suspicious and unusual transactions, for which compliance employees have the required professional skills, personal qualities, etc.) and to help the first line of defense manage these risks efficiently. The second line of defense does not engage in taking risks.

Risk policy is implemented, and the risk management framework is controlled by the risk management function. The performer of the risk management function ensures that all risks are identified, assessed, measured, monitored, and managed, and informs the appropriate units of the Company about them. The performer of the risk management function for the purposes of AML primarily performs the supervision over adherence to risk appetite, supervision over risk tolerance, supervision over identification of changes in risks, performs the overview of associated risks, and performs other duties related to risk management.

The Management Board have appointed an MLRO for performing the second line of defense functions. This person is not operationally involved in the areas that the MLRO will be monitoring and verifying and is thus independent in relation to these. The MLRO is accountable for the following activities:
produce and when necessary, update the Company's Guidelines; monitoring and verifying on an ongoing basis that the Company is fulfilling the requirements prescribed by these Guidelines and related documents and according to external laws and regulations
provide the Company's staff and Members of the Board with advice and support regarding the rules relating to money laundering and terrorist financing inform and train the members of the Management Board and relevant persons about the rules relating to money laundering and terrorist financing
investigate and register sufficient data on received internal notifications and decide whether the activity can be justified or whether it is suspicious;
file the relevant reports (i.e. UARs, SARs, STRs, etc.) with the appropriate regulatory authorities in accordance with local jurisdictional requirements;
check and regularly assess whether the Company's procedures and guidelines to prevent the use of the business for money laundering or terrorist financing are fit for purpose and effective;
identify the incidents in accordance with the Company's Guidelines and take measures regarding such incidents.
The MLRO reports to the Management Board quarterly. This report must be in writing and include at least the following items:

number of customers under all risk classifications
number of hits of persons in relation to the Sanctions lists and applied measures;
number of customers or customers' representatives identified as PEPs or persons with a connection to a PEP;
number of internal notifications on suspicious activity or transactions;
number of the relevant reports (SARs, UARs, etc.) reported to the Financial Intelligence Unit (FIU);
number and content of a request for information from the FIU within the framework of an investigation; confirmation that the Company's risk assessment for money laundering and terrorist financing is up to date; confirmation that these Guidelines and other related documents are up to date; confirmation that the staffing in respect of AML measures is sufficient; all inadequacies (if any) identified by control function have been addressed;
list of obligatory trainings which have been held for the staff in respect of AML measures.

The third line of defense – Internal audit

The third line of defense is comprised by the independent and effective internal audit function. The internal audit function may be performed by one or several Employees, the Company's structural unit with the relevant functions or by the third party, which provides the relevant service to the Company.

The Employees, the Company's structural unit or third party, which performs the internal audit function must have the required competency, tools, and access to the relevant information in all structural units of the Company. The internal audit methods must comply with the size of the Company, the nature, scope, and level of complexity of the activities and provided services, incl. the risk appetite and risks arising from activities of the Company.

The decision to conduct an internal audit is made by a resolution of the Management Board. The Management Board must assess the need to conduct an internal audit at least annually. The Company's structure chart

[1] For the purpose of simplifying these Guidelines, relation to «AML» includes also prevention of terrorism financing and implementation of Sanctions

PRINCIPLES OF CUSTOMER DUE DILIGENCE MEASURES IMPLEMENTATION
Customer due diligence (CDD) measures are required for verifying the identity of a new or existing Customer as a well-performing risk-based ongoing monitoring of the business relationship with the Customer. The CDD measures consist of 3 levels, including the simplified and enhanced due diligence measures, as specified below.
Main Principles

The CDD measures are taken and performed to the extent necessary considering the customer's risk profile and other circumstances in the following cases:

upon establishment of the business relationship and ongoing monitoring of the business relationship; upon executing or mediating of occasional transaction(s) outside the business relationship where the value of the transaction(s) exceeds 15 000 euros (or an equal amount in another assets) over a period of up to one year;
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; upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided for in these Guidelines and applicable legislation.
The Company does not establish or maintain the business relationship and not perform transaction if:

the Company is not able to take and perform any of required CDD measures;

the Company has any suspicions that the Company's services or transaction will be used for money laundering or terrorist financing;
the risk level of the Customer or of the transaction does not comply with the Company's risk appetite.
In the case of receiving information in foreign languages within the framework of CDD implementation, the Company may request to demand translation of the documents to another language appliable for the Company. The use of translations should be avoided in situations when the original documents are prepared in a language appliable for the Company.

Achieving CDD is a process that starts with the CDD measures implementation. When that process is complete, the Customer assigns documented individual risk level which shall form the basis for follow-up measures, and which is followed up and updated when necessary.

The Company has applied CDD measures adequately if the Company has the inner conviction that they have complied with the obligation to apply due diligence measures. The principle of reasonability is observed in the consideration of inner conviction. This means that the Company must, upon the application of CDD measures, acquire the knowledge, understanding and assertation that they have collected enough information about the Customer, the Customer's activities, the purpose of the business relationship and of the transactions carried out within the scope of the business relationship, the origin of the funds, etc., so that they understand the Customer and the Customer's (business) activities, thereby taking into account the Customer's risk level, the risk associated with the business relationship and the nature of such relationship. Such a level of assertation must make it possible to identify complicated, high-value and unusual transactions and transaction patterns that have no reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

The Verification of Information used for the Customer's Identification

Verification of the information for the Customer's identification means using data from a reliable and independent source to confirm that the data is true and correct, also confirming, if necessary, that the data directly related to the Customer is true and correct. This inter alia means that the purpose of verification of information is to obtain reassurance that the Customer who wants to establish the business relationship is the person they claim to be.

The face-to-face identification (personal meeting with the Customer) or identification using information technology means (using of high-confidence e-identification system) is deemed to be the reliable and independent verification of the information obtained in the course of identification.

In situations not specified in abovementioned identification methods the reliable and independent source (must exist cumulatively) is verification of the information obtained in the course of identification:

Which originates from two different sources; where the Customer sends a photo taken of the facial image of the Customer and the identity document used for identification immediately before the data is sent and the Company makes sure that the photo was taken recently; which has been issued by (identity documents) or received from a third party or a place that has no interest in or connections with the Customer or the Company, i.e. that is neutral (e.g. information obtained from the Internet is not such information, as it often originates from the Customer themselves or its reliability and independence cannot be verified); the reliability and independence of which can be determined without objective obstacles and reliability and independence are also understandable to a third party not involved in the business relationship; and the data included in which or obtained via which are up to date and relevant and the Company can obtain reassurance about this (and reassurance can in certain cases also be obtained on the basis of the two previous clauses).

Application of Simplified Due Diligence Measures (level 1)

Simplified due diligence (SDD) is applied where the Customer's risk profile indicates low risk and where, in accordance with the risk assessment produced by the Company, it has been identified that in such circumstances the risk of money laundering or terrorist financing is lower than usual. Regarding the Company services provided and the Company's risk assessment, the Company will not apply SDD measures to their Customers. Thus, to all Customers at least standard due diligence measures shall be applied as specified below.

Application of Standard Due Diligence Measures (level 2)

Standard due diligence measures are applied to all Customers if CDD measures must be applied in accordance with the Guidelines. The following standard due diligence measures should be applied:

identification of the Customer and verification of the submitted information based on information obtained from a reliable and independent source, including using means of electronic identification and of trust services for electronic transactions; identification and verification of a representative of the Customer and their right of representation;
identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the Company to make certain that it knows who the beneficial owner is, and understands the ownership and control structure of the Customer; understanding of business relationships, transaction or operation and, where relevant, gathering information thereon; gathering information on whether the Customer is PEP, their family member or a person known to be close associate; monitoring of the business relationship.

The CDD measures specified above must be applied before establishing the business relationship. The exact instruction for application standard due diligence measures is provided in the Guidelines.

Application of Enhanced Due Diligence Measures (level 3)

In addition to CDD, the Company applies enhanced due diligence (EDD) measures in order to manage and mitigate an established risk of money laundering and terrorist financing that is higher than usual.

The Company always applies EDD measures, when:

the Customer's risk profile indicates high risk level;
upon identification of the Customer or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
the Customer is a PEP; the Customer is from a high-risk third country or their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk third country; the customer is from such country or territory or their place of residence or seat or the seat of the payment service provider of the payee is in a country or territory that, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CFT systems that are in accordance with the recommendations of the Financial Action Task Force, or that is considered a low tax rate territory; the Customer's economic or professional activity, field or factors indicate the risk of money laundering or terrorist financing, which is higher than usual;
the Customer's total amount of incoming or outgoing payments related to business relationship exceeds the limits, established by the Company.
Prior to applying EDD measures, the Company's employee ensures that the business relationship or transaction has a high risk and that a high-risk rate can be attributed to such business relationship or transaction. Above all, the employee assesses prior to applying the EDD measures whether the features described above are present and applies them as independent grounds (that is, each of the factors identified allows application of EDD measures with respect to the Customer).

When applying EDD measures, the following additional and relevant due diligence measures shall be followed:

verification of information additionally submitted upon identification of the Customer based on additional documents, data or information originating from a credible and independent source; gathering additional information on the purpose and nature of the business relationship or transaction and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;[1]
gathering additional information and documents regarding the actual execution of transactions made in the business relationship in order to rule out the ostensibility of the

transactions; gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction made in the business relationship in order to rule out the ostensibility of the transactions; the making of the first payment related to a transaction via an account that has been opened in the name of the Customer participating in the transaction in a credit institution registered or having its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council are in force; the application of due diligence measures regarding the Customer or their representative while being at the same place as the Customer or their representative; gathering additional information about the customer and its beneficial owner, including identification of all owners of the Customer, incl. those whose shareholding is below 25%; gathering information on the origin of the funds and wealth of the customer and its beneficial owner; improving the monitoring of the business relationship by increasing the number and frequency of the applied control measures and by choosing transaction indicators or transaction patterns that are additionally verified;2,3
an analysis of the Customer's digital impression on the Internet is made (Adverse Media Search);
obtaining the approval of the Management Board for transactions with new and existing
Customers; he amount of EDD measures and this scope shall be determined by the employee, who is applying such measures. The employee shall notify about EDD measures applied within 2 working days after the start of applying of the EDD measures by sending relevant notification to the MLRO.

In the case of application of EDD measures, the Company monitors the business relationship more often than usual and reassesses the Customer's risk profile no later than every six months.

CUSTOMER DUE DILIGENCE MEASURES
Identification of the Customer – natural person

The Company identifies the Customer who is a natural person and, where relevant, their representative and retains the following data on the Customer:

first and last name(s);
personal identification code;
date of birth;
citizenship;
the place of residence or seat;
economic or professional activity.
The following valid identity documents may be used as the basis for the identification of a natural person:

an identity card;
a residence permit card;

an Estonian citizen’s passport;
an alien’s passport;
a driving permit issued in the Republic of Estonia;
a driving permit issued in a foreign country if the document includes user’s name, photograph or facial image, signature or image of a signature and date of birth or personal identification code;
a travel document issued in a foreign country (passport).

During the verification of the data obtained during the identification of the Customer and representative from a credible and independent source, the first credible and independent sources is always:
an identity document specified above or a colored and legible copy/image of this document.
The following information obtained may be the second reliable and independent source:

the Customer´s photo (selfie) with identity document;
the utility bill (e. g. invoice, issued and paid once a month from utilities, including electric, natural gas, water, waste, etc.)
information for checking the data[3] directly associated with the person (e. g. place of work, residence or study).

The Customer who is natural person can´t use representative in the course of business relationship or occasional transaction with the Company.

Identification of the Customer – legal entity

The Company identifies the Customer which is a legal entity and their representative and retains the following data on the Customer:

business name or name (with the legal form);
registry code or registration number and date of registration;
name of the director(s) or names of member(s) of the management board or member(s) of another equivalent body, and their authorities in representing the Customer;
location of the Customer, whereby the theory of the country of establishment must be proceeded from;
place of business;
the details of the telecommunications.
The following documents issued by a competent authority or body not earlier than six months before their use may be implied for identification of the Customer:

registry card of the relevant register; or
registration certificate of the relevant register; or
a document equivalent with an aforementioned documents or relevant documents of establishment of the Customer.

The Company verifies the correctness of the Customer's data specified above, using information originating from a credible and independent source for that purpose. Where the Company has access to the commercial register, register of non-profit associations and foundations or the data of the relevant registers of a foreign country, the submission of the documents specified about does not need to be demanded from the Customer.

The identity of legal entity and the right of legal entity's representation can be verified on the basis of a document specified above, 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, thereby using at least two different sources for verification of data in such an event.

During the verification of the data from a credible and independent source obtained during the identification of the legal entity, the source considered credible and independent when the Company:

sees the original of the document specified above;
sees a copy of the document specified above that has been authenticated by a notary, certified by a notary or officially certified; or
has access to the data in the commercial register, register of non-profit associations and foundations or the relevant registers of foreign countries via a computer network.
Two different sources during the identification of a legal entity means that the data medium, place or measure of obtaining information must be different (i.e. it cannot be the same data medium).

The representative of the legal entity shall be identified as the Customer, who is a natural person in accordance with these Guidelines. The Company must also identify and verify the nature and scope of the right of representation. The name, date of issue and name of issuer of the document that serves as a basis for the right of representation must be ascertained and retained, except in case, when the right of representation was verified using information originating from the relevant register (e. g. the commercial register, register of non-profit associations and foundations or the relevant register of a foreign country).

The Company must observe the conditions of the right of representation granted to the legal entity's representatives and provide services only within the scope of the right of representation.

The identification of the Customer's beneficial owner

The Company must identify the beneficial owner of the Customer and take measures to verify the identity of the beneficial owner to the extent that allows the Company to make sure that they know who the beneficial owner is.

The Company shall request from the Customer information to the Customer's beneficial owner (e.j. providing the Customer with an opportunity to specify their beneficial owner in KYC questionnaire).

The Company doesn´t establish the business relationship, if the Customer, who is a natural person has beneficial owner who is not the same person as the Customer.

The beneficial owner of a legal entity is identified in stages where the obliged entity proceeds to each subsequent stage if the beneficial owner of the legal entity cannot be determined in the case of the previous stage. The stages are as follows:

is it possible to identify, in respect of the Customer that is a legal entity or a person participating in the transaction, the natural person or persons who actually ultimately control the legal entity or exercise influence or control over it in any other manner, irrespective of the size of the shares, voting rights or ownership rights or its direct or indirect nature; whether the Customer that is a legal entity or the person participating in the transaction has a natural person or persons who own or control the legal entity via direct[4] or indirect[5] shareholding. Family connections and contractual connections must also be taken into account here; who is the natural person in senior management[6], who must be defined as the beneficial owner, as a result of execution of the previous two stages have not made it possible for the obliged entity to identify the beneficial owner.
If the documents used for the legal entity´s identification or the other submitted documents do not indicate directly who the beneficial owner of the legal entity is, the relevant data (incl. data about being a member of a group and the ownership and management structure of the group) are registered on the basis of the statement of the representative of the legal entity or the document written by hand by the representative of the legal entity.

The Company shall apply reasonable measures to verify the accuracy of the information established on the basis of statements or a handwritten document (e.g. by making inquiries in the relevant registers), requiring the submission of the legal entity's annual report or other relevant document. If the Company has doubts about the accuracy or completeness of the relevant information, the Company shall verify the information provided from publicly available sources and, if necessary, request additional information from the Customer.

Where the Company establishes the business relationship with the Customer whose information on beneficial owners must, in accordance with the statutes of a Member State of the European Union, be submitted to the state or be registered there, the Company shall obtain a relevant registration certificate or registry extract upon identification of the Customer´s beneficial owner.

The beneficial owner does not have to be identified in the case of the Customer listed on a regulated market that is subject to disclosure requirements consistent with European Union

law or subject to equivalent international standards which ensure adequate transparency of ownership information.

Political Exposed Person's identification

The Company shall take measures to ascertain whether the Customer, the beneficial owner of the Customer or the representative of this Customer is a PEP, their family member[7] or close associate[8], or if the Customer has become such a person.

The Company shall request from the Customer information to identify if the Customer is a PEP, their family member or close associate (e. g. providing the Customer with an opportunity to specify the relevant information in KYC questionnaire).

The Company shall verify the data received from the Customer by making inquiries in relevant databases or public databases or making inquiries or verifying data on the websites of the relevant supervisory authorities or institutions of the country in which the Customer has place of residence or seat. PEP must be additionally verified using Google and the local search engine of the Customer's country of origin, if any, by entering the customer's name in both Latin and local alphabet with the customer's date of birth.

At least the following persons are deemed to be PEPs:

head of State or head of government;
minister, deputy minister or assistant minister;
member of a legislative body;
member of a governing body of a political party;
judge of the highest court of a country;
auditor general or a member of the supervisory board or executive board of a central bank;
the Chancellor of Justice;
ambassador, envoy or chargé d'affaires;
high-ranking officer in the armed forces;
member of an administrative, management or supervisory body of a state-owned enterprise;
director, deputy director and member of a management body of an international organisation;
a person who, as per list published by the European Commission, is considered a performer of prominent public functions by a Member State of the European Union, the European Commission or an international organisation accredited on the territory of the European Union is deemed a politically exposed person.
Middle-ranking or more junior officials are not considered PEPs.

The Company shall identify close associates and family members of PEPs only if their connection with PEP is known to the public or if the Company has reason to believe that such a connection exists.

Where the Customer who is a PEP no longer performs important public functions placed upon them, the Company shall at least within 12 months take into account the risks that remain related to the Customer 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 Customer.

Identification of the purpose and nature of the business relationship or a transaction

The Company shall understand the purpose and nature of the establishing business relationship or performing transaction. Regarding the services provided, the Company shall request from the Customer at least the following information for understanding the purpose and nature of the business relationship or transaction:

the estimated transactions turnover with the Company per calendar year;
the estimated source of funds used in the business relationship or transaction;
if the business relationship or transaction is related to the Customer´s performance of economic or professional activities.
The Company shall apply additional measures and collect additional information to identify the purpose and nature of the business relationship or an occasional transaction in cases where:

there is a situation that refers to high value or is unusual and/or
where the risk and/or risk profile associated with the Customer and the nature of the business relationship gives reason for the performance of additional actions in order to be able to appropriately monitor to business relationship later.
If the Customer is a legal entity, in addition to aforementioned the Company shall identify the Customer´s:

area of activity, where the Company shall understand what the Customer deals with and intends to deal with in the course of the business relationship and how this corresponds to the purpose and nature of the business relationship in general and whether it is reasonable, understandable and plausible; payment practices, including the countries from which payments are received and to which payments are made, the expected duration of the business relationship, the extent and channels of cash, payment channels (branch, Internet bank, card payments), etc.; main business partners, where the Company must identify who are the Customer's main partners with which transactions will be concluded in the declared area of activity and with the declared activity volumes.
The area of activity, payment practices and main business partners must fit into the experience profile of the Customer's representative (or key persons) and/or the beneficial owner. Thus, the Company has to identify where the representative's and/or beneficial owner's capacity, capability, skills and knowledge (experience in general) comes from in order to operate in this area of activity, with these business volumes and with these main business partners.

Monitoring of the business relationship

The Company shall monitor established business relationships where the following ongoing due diligence (ODD) measures are implemented:

ensuring that the documents, data, or information collected in the course of the application of due diligence measures are updated regularly and in the case of trigger events, i.e., primarily the data concerning the Customer, their representative (incl. the right of representation) and beneficial owner as well as the purpose and nature of the business relationship;
ongoing monitoring of the business relationship, which covers transactions carried out in the business relationship to ensure that the transactions correspond to the Company's knowledge of the Customer, their activities and risk profile;
identification of the source and origin of funds used in the transaction(s).
The Company shall regularly check and update the documents, data and information collected within the course of the implementation of CDD measures. The regularity of the checks must be based on the risk profile of the Customer and the checks must take place at least:

once semi-annually for the high-risk profile Customer;
once annually for the medium-risk profile Customer;
once every two years for the low-risk profile Customer.
The collected documents, data and information must also be checked if an event has occurred which indicates the need to update the collected documents, data and information.

In the course of the ongoing monitoring of the business relationship, the Company shall monitor the transactions concluded during the business relationship in such a manner that the latter can determine whether the transactions to be concluded correspond to the information previously known about the Customer (i.e., what the customer declared upon the establishment of the business relationship or what has become known in the course of the business relationship).

The Company shall also monitor the business relationship to ascertain the customer's activities or facts that indicate criminal activities, money laundering or terrorist financing or the relation of which to money laundering or terrorist financing is probable, incl. complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or that are uncharacteristic of the specific features of the business in question. In the course of the business relationship, the Company shall constantly assess the changes in the Customer's activities and assess whether these changes may increase the risk level associated with the Customer and the business relationship, giving rise to the need to apply EDD measures.

In the course of the ongoing monitoring of the business relationship, the Company applies the following measures:

screening i.e., monitoring transactions in real-time;
monitoring i.e., analyzing transactions later.

The objective of screening is to identify:

suspicious and unusual transactions and transaction patterns;
transactions exceeding the provided thresholds;
politically exposed persons and circumstances regarding international sanctions.
The screening of the transactions is performed automatically and includes the following measures:

When monitoring transactions the Employee shall assess transaction with a view to detect activities and transactions that:

deviate from what there is reason to expect based on the CDD measures performed, the services provided, the information provided by the customer and other circumstances,
without deviating according to previous clause, may be assumed to be part of a money laundering or terrorist financing; may affect the Customer´s risk profile score.
In case, when aforementioned fact is detected, the employee shall notify MLRO and postpone any transaction of the Customer until MLRO´s decision regarding this.

In addition to aforementioned, the MLRO shall review the Company´s transaction regularly (at least once per week) to ensure that:

the Company´s employees properly performed the aforementioned obligations;
there are no transactions and transaction patterns that are complicated, high-value and unusual and that have no reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features.
The Company identifies the source[9] and origin[10] of the funds used in transaction(s) if necessary. The need to identify the source and origin of funds depends on the Customer's previous activities as well as other known information. Thereby the identification of the source and origin of the funds used in transaction shall be performed in the following cases:

the transactions exceed the limits established by the Company;
if the transactions do not correspond to the information previously known about the Customer;
if the Company wants to or should reasonably consider it necessary to assess whether the transactions correspond to the information previously known about the Customer;
if the Company suspects that the transactions indicate criminal activities, money laundering or terrorist financing or that the relation of transactions to money laundering or terrorist financing is probable, incl. complicated, high-value and unusual transactions and transaction

patterns that do not have any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

IMPLEMENTATION OF SANCTIONS

Upon the entry into force, amendment or termination of Sanctions, the Company shall verify whether the Customer or a person who is planning to have the business relationship or transaction with them is a subject of Sanctions. If the Company identifies a person who is a subject of Sanctions or that the transaction intended or carried out by them is in breach of Sanctions, the Company shall apply Sanctions and immediately inform the FIU thereof.

Procedure for identifying the subject of Sanctions and a transaction violating Sanctions

The Company shall use at least one of the following sources (databases) to verify the Customer´s relation to Sanctions:

ComplyAdvantage watchlists via Sum&Substance software;
Financial sanctions information and search;

Other internal databases or databases managed by third parties, which contain at least the lists from databases specified above.
In addition to aforementioned sources, the Company may use any other sources by the decision of the Employee who is applying CDD measures.

To verify that the persons' names resulting from the inquiry are the same as the persons listed in a notification containing Sanction(s), their personal data shall be used, the main characteristics of which are, for a legal entity, its name or trademark, registry code or registration date, and for a natural person, their name and personal identification or date of birth.

In order to establish the identity of the persons specified in the relevant legal act or notice being the same as those identified as a result of the inquiry from databases, the Company must analyze the names of the persons found as a result of the inquiry based on the possible effect of factors distorting personal data (e. g. transcribing foreign names, different order of words, substitution of diacritics or double letters etc.).

The Company shall perform abovementioned verification on an ongoing basis in the course of an established business relationship. The frequency of the ongoing verifications depends on the Customer's risk profile:

once per week for the high-risk profile Customer;
once per month for the medium-risk profile Customer;
once per quarter for the low-risk profile Customer.

If the Employee has doubts that a person is a subject of Sanctions, the Employee shall immediately notify the MLRO or the Management Board member. In this case the MLRO of the Management Board member shall decide on whether to ask or acquire additional data from the person or notify the FIU immediately of their suspicion.

The Company shall primarily acquire additional information on their own about the person who is in business relationship or is performing a transaction with them, as well as the person intending to establish the business relationship, perform a transaction or an act with them, preferring information from a credible and independent source. If, for some reason, such information is not available, the Company shall ask the person who is in the business relationship or is performing a transaction or an act with them, as well as the person intending to establish a business relationship, perform a transaction or an act with them, whether the information is from a credible and independent source and assess the answer.

Actions when identifying the Sanctions subject or a transaction violating Sanctions

If the employee of the Company becomes aware that the Customer which is in business relationship or is performing a transaction with the Company, as well as a person intending to establish the business relationship or to perform a transaction with the Company, is the subject of Sanctions, the employee shall immediately notify the MLRO or the Management Board member, about the identification of the subject of Sanctions, of the doubt thereof and of the measures taken.

The MLRO or the Management Board member shall refuse to conclude a transaction or proceeding, shall take measures provided for in the act on the imposition or implementation of the Sanctions and shall notify immediately the FIU of their doubts and of the measures taken.

When identifying the subject of the Sanctions, it is necessary to identify the measures that are taken to sanction this person. These measures are described in the legal act implementing the Sanctions, therefore it is necessary to identify the exact sanction what is implemented against the person to ensure legal and proper application of measures.

REFUSAL TO THE TRANSACTION OR BUSINESS RELATIONSHIP AND THEIR TERMINATION
The Company is prohibited to establish business relationship and the established business relationship or transaction shall be terminated in case when:

the Company suspects money laundering or terrorist financing;
it is impossible for the Company to apply the CDD measures, because the Customer does not submit the relevant data or refuses to submit them or the submitted data gives no grounds for reassurance that the collected data are adequate;
the Customer which capital consists of bearer shares or other bearer securities wants to establish the business relationship;

the Customer who is a natural person behind whom is another, actually benefiting person, wants to establish the business relationship (suspicion that a person acting as a front is used);
the Customer´s risk profile has become inappropriate with the Company´s risk appetite (i. e. the Customer´s risk profile level is “prohibited”).
The aforementioned is not applied when the Company has notified the FIU of the establishment of the business relationship, transaction or an attempted transaction in accordance with the procedure provided below and received from the FIU a specific instruction to continue the business relationship, the establishment of the business relationship or the transaction.

In the event of a termination of the business relationship in accordance with this chapter, the Company shall transfer the Customer’s assets (the LPA´s unit redemption price) within reasonable time, but preferably not later than within one month after the termination and as a whole to an account opened in a credit institution which is registered or whose place of business is in a contracting state of the European Economic Area or in a country where requirements equal to those established in the relevant directives of the European Parliament and of the Council are applied. In exceptional cases, assets may be transferred to an account other than the Customer’s account or issued in cash by informing the Financial Intelligence Unit about this with all the relevant and sufficient information at least 7 working days in advance and on the condition that the Financial Intelligence Unit does not give a different order. Irrespective of the recipient of the funds, the minimum information given in English in the payment details of the transfer of the Customer’s assets is that the transfer is related to the extraordinary termination of the Customer relationship.

REPORTING OBLIGATION
The Company through its MLRO must report to the FIU on the activity or the circumstances that they identify in the course of economic activities and whereby:

the characteristics indicate the use of criminal proceeds or the commission of crimes related to this (this is primarily a report on a suspicious and unusual transaction or activity, i.e. UTR or UAR);
in the case of which they suspect or know or the characteristics of which indicate the commission of money laundering or related crimes (this is primarily a report on a transaction or activity whereby money laundering is suspected, i.e., STR or SAR);
in the case of which they suspect or know or the characteristics of which indicate the commission of terrorist financing or related crimes (this is primarily a report on a transaction or activity whereby terrorist financing is suspected, i.e., TFR);
in the case of which an attempt of the activity or circumstances specified in previous clauses is present.
The minimal characteristics of suspicious and unusual transactions are provided in the guidelines made by the FIU (one of annexes of these Guidelines).

The Company through its MLRO must report the FIU:

about the circumstances of refusal of establishment of the business relationship and about the termination of the business relationship on the basis of circumstances provided in the previous chapter (primarily a suspicious and unusual transaction or activity report, i.e. UAR); about each transaction that has become known whereby a pecuniary obligation of over 10. 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 (an amount-based report, CTR);
about identifying the subject of the Sanctions and the implementation of Sanctions or suspicion thereof (international sanction report, ISR).
The reports specified above must be made before the completion of the transaction if the Company suspects or knows that money laundering or terrorist financing or related crimes are being committed and if said circumstances are identified before the completion of the transaction. If the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction or it may impede capture of the person who committed possible money laundering or terrorist financing, the transaction will be concluded and a report will be submitted the FIU thereafter. The Company is in contact with the Financial Intelligence Unit in order to identify such circumstances.

If the necessity of abovementioned report arises, the Employee to whom became known such necessity must immediately notify the MLRO about this.

In any case (i.e. also in the situation where an activity or circumstance is identified after the completion of the transaction), the reporting obligation must be performed immediately, but not later than two working days after the identification of the activity or circumstance or the emergence of the actual suspicion (i.e. the situation where the suspicion cannot be dispelled).

The report shall be sent in accordance with the guidelines, issued by the FIU (one of annexes of these Guidelines).

The Company, a structural unit of the Company, a Management Board member, MLRO and the Employee is prohibited to inform a 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.

TRAINING OBLIGATION

The Company ensures that its employees, its contractors and others participating in the business on a similar basis and who perform work tasks that are of importance for preventing the use of the business for money laundering or terrorist financing ('Relevant Persons') have the relevant qualifications for these work tasks. When a Relevant Person is

recruited or engaged, the Relevant Person's qualifications are checked as part of the recruitment/appointment process by carrying out background checks comprising extracts from criminal records in addition to the customary taking of references, which is documented using a special standard form assessing employee suitability.

In accordance with the requirements applicable to the Company on ensuring the suitability of Relevant Persons, the Company makes sure that such persons receive appropriate training and information on an ongoing basis to be able to fulfil the Company's obligations in compliance with the applicable legislation. It is ensured through training that such persons are knowledgeable within the area of AML/CFT to an appropriate extent considering the person's tasks and function. The training must provide, first and foremost, information on all the most contemporary money laundering and terrorist financing methods and risks arising therefrom.

This training refers to relevant parts of the content of the applicable rules and regulations, the Company's risk assessment, the Company's Guidelines and procedures and information that should facilitate such Relevant Persons detecting suspected money laundering and terrorist financing. The training is structured on the basis of the risks identified through the risk assessment policy.

The content and frequency of the training is adapted to the person's tasks and function on issues relating to AML/CFT measures. If the Guidelines is updated or amended in some way, the content and frequency of the training is adjusted appropriately.

For new employees, the training comprises a review of the content of the applicable rules and regulations, the Company's risk assessment policy, these Guidelines and other relevant procedures.

The employees and the Management Board members receive training on an ongoing basis under the auspices of the MLRO in accordance with the following training plan:

periodicity: at least once a year for the Management Board members. At least once a year for the Company's employees and Relevant Person engaged.
scope: review of applicable rules and regulations, the Company's Guidelines and other relevant procedures. Specific information relating to new/updated features in the applicable rules and regulations. Report and exchange of experience relating to transactions reviewed since the previous training.
In addition to the above, Relevant Persons are kept informed on an ongoing basis about new trends, patterns and methods and are provided with other information relevant to the prevention of money laundering and terrorist financing.

The training held is to be documented electronically and confirmed with the Relevant Person signature. This documentation should include the content of the training, names of participants and date of the training.

COLLECTION AND PRESERVATION OF DATA

The Company through the person (incl. Employees, Management Board members and MLRO) who firstly receives the relevant information or documents shall register and retain:

all data collected within CDD measures implementation;
information about the circumstances of refusal of the establishment of the business relationship by the Company;
the circumstances of the refusal to establish business relationship on the initiative of the Customer if the refusal is related to the application of CDD measures by the Company;
information on all of the operations made to identify the person participating in the transaction or the Customer´s beneficial owner;
information if it is impossible to take the CDD measures using information technology means;
information on the circumstances of termination of the business relationship in connection with the impossibility of application of the CDD measures
the each transaction date or period and a description of the contents of the transaction;
information serving as the basis for the reporting obligations specified above;
data of suspicious or unusual transactions or circumstances of which the Financial Intelligence Unit was not notified.
In addition to the abovementioned information the Company shall register the following data regarding a transaction:

upon opening an account, the account type, number, currency and significant characteristics of the securities or other property;
upon making a payment relating to shares, bonds or other securities, the type of the securities, the monetary value of the transaction, the currency and the account number;
in the case of another transaction, the transaction amount, the currency and the account number.
The data specified above shall be retained for 5 years after the expiry of the business relationship or the completion transaction. The data related to the performance of the reporting obligation must be retained for 5 years after the performance of the reporting obligation.

Documents and data must be retained in a manner that allows for exhaustive and immediate response to the queries made by the FIU or, pursuant to legislation, other supervisory authorities, investigation authorities or the court.

The Company implements all rules of protection of personal data upon application of the requirements arising from the applicable legislation. The Company is allowed to process personal data gathered upon CDD implementation 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 deletes the retained data after the expiry of the time period, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a precept of the competent supervisory authority, data of importance for prevention, detection or investigation of money laundering or terrorist financing may be retained for a longer period, but not for more than five years after the expiry of the first time period.

AVOIDING CONFLICT OF INTERESTS

The Employees (incl. MLRO) must avoid the conflict of interests and when this happens, immediately notify the Management Board member or the MLRO.

The conflict of interests is understood as all the circumstances known to the Company or its employees that may affect the decisions of making a transaction or establishing business relationship and which do not correspond to the interests of the Company or its customer.

To achieve the goal of avoiding the conflict of interests, the Company shall collect and regularly update its employee's data in order to identify their interests in the context of preventing money laundering and terrorist financing. The Company collects the following data about each employee:

the birthplace and place of residence of the employee;
other job positions and contracts of the employee that they have in the context of the economic field;
the data regarding the close relatives of the employee (spouse, parents, children, siblings and their children): for each person, their place of residence and place of work.
other data known to the employee which may indicate to the interests in the context of preventing money laundering and terrorist financing.
The failure of the employee to provide the data specified above is considered to be a significant violation of the employment contract and may result in the extraordinary cancellation of the employment contract for reason arising from the employee.

The Company identifies and analyses, inter alia, whether the persons directing customers to the Company (e.g. agents, resellers, etc.) have any interests regarding the Customer (e.g., provide them with legal services, accounting services, services providing the establishment of companies and other legal structures, etc.) which cause the conflict of interests between the person directing customers to the Company and the Customer.

In case of identifying a conflict of interests or circumstances indicating a conflict of interests, the Company shall apply all necessary measures to prevent it. If it is impossible to prevent the conflict of interests, the Company must not conclude any transactions or establish the business relationship.

The Management Board is responsible for avoiding conflict of interests in the Company.

INTERNAL CONTROL OF EXECUTION OF THE GUIDELINES

The performance of the Guidelines shall be internally controlled by the Internal Control Officer appointed by the Management Board. The Internal Control Officer must have the required competency, tools, and access to the relevant information in all structural units of the Company.

The Internal Control Officer shall provide the internal control report to the Management Board at least quarterly. The Management Board is responsible for exercising control over the due performance of the requirements set out in these Guidelines, including the performance of internal control function. For this reason, the Management Board is obliged to:

analyze the results of performed internal control;
implement actions to eliminate deficiencies occurred.
A detailed overview of internal control activities will be given in document "Internal Control Guidelines"