AML Policy Atvater s.r.o.

Last updated on: 05.03.2025

Name of the company: Atvater s.r.o.

ID number: 22144820

Legal address: Revolucni 1082/8, Nove Mesto, 11000 Prague 1, Czech Republic

Telephone number: +35796171286

Email address: support@atvater.com

INTRODUCTION

The purpose of these Guidelines for Anti-Money Laundering (AML), Combating Terrorist Financing (CFT) and Sanctions measures is to ensure that **Atvater s.r.o.** (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.

These Guidelines have been adopted to ensure that the Company complies with the rules and regulations set out in:

- Act on Certain Measures against the Legalization of Proceeds from Crime and Terrorist Financing (Act No. 253/2008) (AML Act);
- Act on the Implementation of International Sanctions (Act No. 69/2006) (Sanctions Act);
- the Czech Financial Analytical Office's general guidelines regarding measures against money laundering, terrorist financing and regarding implementation of international sanctions;
- DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (AMLD5).

These Guidelines are the subject of a review by the Director at least annually. The proposal for a review and the review of these Guidelines may be scheduled more often by the decision of the Company's Money Laundering Reporting Officer (MLRO) or the Internal Control Officer.

These Guidelines shall be accepted and approved by the resolution of the Director.

DEFINITIONS

The Company means legal entity with following data:

- company name: Atvater s.r.o.;
- identification number: 22144820;
- address: Revolucni 1082/8, Nove Mesto, 11000 Prague 1, Czech Republic.

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.

Sanctions mean an essential tool of foreign policy aimed at supporting the maintenance or restoration of peace, international security, democracy and the rule of law, following human rights and international law or achieving other objectives of the United Nations Charter or the common foreign and security Policy of the European Union. Sanctions include:

- international sanctions which are imposed with regard to a state, territory, territorial unit, regime, organization, association, group or person by a resolution of the United Nations Security Council, a decision of the Council of the European Union or any other legislation imposing obligations on Czech Republic;
- sanctions of the Government of the Czech Republic which is a tool of foreign policy which may be imposed in addition to the objectives specified in previous clause in order to protect the security or interests of Czech Republic.

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.

MLRO means Money Laundering Reporting Officer, who is appointed to the Company as a contact person in the meaning of section 2 of § 22 of AML Act.

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

Director means executive director of the Company.

The Business Relationship means a relationship that is established upon conclusion of a long-term 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.

Virtual currency means an electronically storable or transferable unit that is:
(a) capable of performing a payment, exchange, or investment function, whether or not it has an issuer, unless it is:
1. a security, investment instrument or cash pursuant to the Payment System Act (Act No. 370/2017),
2. unit according to § 3 (3) c) points 4 to 7 of the Payment System Act (Act No. 370/2017), or
3. the unit by which the payment is made according to § 3 (3) e) the Payment System Act (Act No. 370/2017), or
(b) a unit referred to in point (a) (2) and which can ultimately be paid only for a narrowly defined range of goods or services which includes an electronically storable or transferable unit referred to in point (a).

PEP means a natural person who performs or has performed prominent public functions and with regard to whom related risks remain.

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 Director

The Director is the carrier of the culture of compliance with the requirements of money laundering and terrorist financing prevention, guaranteeing that the Director 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 inthe decision-making processes of the Company.

The Director bears 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.

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

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 Director 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 Director with advice and support regarding the rules relating to money laundering and terrorist financing
- inform and train the members of the Director 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 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 Director 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 reported to the Financial Analytical Office (FAU);
- number and content of a request for information from the FAU 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 Director. The Director must assess the need to conduct an internal audit at least annually.

The Services Provided

The Company's main economic activity are the services related to virtual currency. For this reason, the Company offers to the Customers the transaction types specified in the Program of Operations (annex of the Risk Assessment Policy).

THE CUSTOMER'S IDENTIFICATION

The Company shall identify the Customer in accordance with procedure specified by the Guidelines and collect the Customers data in the following cases:

- when it is clear that the value of the occasional transaction(s) exceeds the amount of € 1;
- upon establishment of the business relationship, when it is clear that the value of the transaction(s) in the course of this business relationship exceeds the amount of € 1;
- upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided for in these Guidelines and applicable legislation.

Implementation of the Customer's identification

The identification of the Customer who is a natural person, shall be performed by the Employee in the physical presence of the Customer. The Customer, who is a natural person, is not allowed to use representative during identification.

The identification of the Customer which is a legal person or a trust fund shall be performed by the Employee in the physical presence of a natural person acting on behalf of the Customer (e.g. the Customer's Director, management board member, etc.).

After the Customer's identification is performed, the Company shall in the course of business relationship with the Customer or in further transactions, check the validity and completeness of the Customer's identification data, information gathered in the course of the due diligence process, or reasons for exempting the Customer from the due diligence process, and shall take record of any changes and modifications.

The identification of the Customer may be performed remotely if in the course of identification process the following requirements are fulfilled:

- the Customer, who is a natural person, sends to the Company copy of identity document and at least one other document from which the Customer's data may be collected (e.g., another identity document or proof of address with the Customer's data specified);
- the Company enters into an agreement with the Customer on this transaction or business relationship, the content of which will be recorded in text form;
- the Customer proves in a credible manner the existence of a payment account held in his name with a credit institution or a foreign credit institution operating in the territory of a Member State of the European Union or a state forming the European Economic Area and the first payment under contract concluded is made through this institution;

The aforementioned requirement to send other document may be avoided in case when the Customer's first payment is accompanied by the Customer's data shall be collected.

Identification of the Customer – natural person

The Company identifies the Customer who is a natural person on the basis of identity document[2] and retains the following data on the Customer:

- first and last name(s);
- personal number and, if not assigned, date of birth and sex
- place of birth;
- citizenship;
- the place of residence;
- occupation or professional activity;
- estimated transactions monthly turnover with the Company
- email; and

the following data regarding identity document used:

- number of the identity document;
- the state or the authority which issued it;
- its period of validity.

The Company shall verify the conformity of the Customer's image with the image in the identity document.

Identification of the Customer – legal entity

The Company identifies the Customer which is a legal entity 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;
- estimated transactions monthly turnover with the Company
- contact details (email and phone number, if applicable).

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

[2] identity document means a document issued by a public administration body stating the name and surname, date of birth and from which the Customer's image and other information enabling the person presenting the document to be identified as its authorized holder.

- 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 relevant register of a foreign country, the submission of the documents specified about does not need to be demanded from the Customer.

The legal entity's representative shall be identified as the Customer who is natural person. Each legal entity's representative who intends to perform transactions with the Company on behalf of legal entity shall be identified accordingly.

Political Exposed Person's identification

In the course of the Customer'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[3] or close associate[4], 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. In case of suspicion 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 (the Prime Minister or similar);
- minister, deputy minister or assistant minister;
- member of a legislative body;
- member of a governing body of a political party;
- a head of a local government
- judge of the highest court of a country;
- auditor general or a member of the supervisory board or executive board of a central bank;

[3] **family member** means the spouse, or a person considered to be equivalent to a spouse, of a PEP; a child and their spouse, or a person considered to be equivalent to a spouse, of a PEP; a parent of a PEP

[4] **close associate** means a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person

- 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.

CUSTOMER DUE DILIGENCE

Main Principles

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 shall be applied by the Company through the responsible Employee in the following cases:

- when it is clear that the value of the occasional transaction(s) exceeds the amount of € 15 000;
- when occasional transaction(s) is performed with a PEP;
- when occasional transaction(s) is performed with the Customer which is established or located in high-risk third country[5];
- in the course of the business relationship;
- when the Customer was identified remotely as specified above;

[5] Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies

- upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided for in these Guidelines and applicable legislation.

In the aforementioned cases the Company shall apply customer due diligence (CDD) measures specified in this chapter.

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 measures 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 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. g. 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[6] or indirect[7] shareholding. Family connections and contractual connections must also be taken into account here;
- who is the natural person in senior management[8], 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.

---

[6] **direct ownership** is a manner of exercising control whereby the natural person owns a 25 percent shareholding plus one share or an ownership right of over 25 percent in the company

[7] **indirect ownership** is a manner of exercising control whereby a 25 percent shareholding plus one share or an ownership right of over 25 percent in the company is owned by a company that is controlled by a natural person or several companies that are controlled by the same natural person.

[8] a **member of senior managemen**t is a person who makes the strategic decisions that fundamentally affect business activities and/or practices and/or the company general (business) trends or in its absence carries out everyday or regular management functions of the company within the scope of executive power (e.g. chief executive officer (CEO), chief financial officer (CFO), director or president, etc.).

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.

Upon the determination of the discrepancy between the information on the beneficial owners of the Customer that is a legal person available in the relevant register and the information on the beneficial owners of the same Customer available to them, the Company shall notify the Customer thereof and propose to provide accurate information on its beneficial owners to the relevant register.

As part of the notification, the Company shall state what it sees in the discrepancy. If it is expedient in the circumstances, the Company shall allow the Customer to comment on this discrepancy.

If the Customer does not eliminate or refute the discrepancy without undue delay from the notification, the liable person shall report the discrepancy to the court which is competent to proceed with the discrepancy pursuant to the law governing the registration of beneficial owners.

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. 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 and cryptocurrency use, 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.

In addition to aforementioned measures, in the course of understanding the purpose and nature of the performing transaction the Company may establish source and origin of funds used in the transaction(s) as described below.

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:

- established thresholds for the Customer´s transactions, depending on the Customer´s risk profile and the estimated transactions turnover declared by the Customer;
- the scoring of virtual currency wallets where the virtual currency shall be sent in accordance with the Customer´s order;
- the scoring of virtual currency wallets from which the virtual currency is received.

If the Customer gives order for transaction which exceeds the threshold established or for transaction to the virtual currency wallet with high-risk score (e.g. wallets related to fraud, crime, etc.), the transaction shall be manually approved by the Employee, which shall access before the approval a necessity to apply any additional CDD measures (e. g. applying EDD measures, asking source and origin of funds or asking additional information regarding the transaction).

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 (e.g. exceeding estimated transactions turnover, virtual currency sending each time to new virtual currency wallet, volume of transactions exceeding limit);
- 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.

ENHANCED DUE DILIGENCE MEASURES

In addition to CDD measures, 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.

[9] **the source of the funds** used in the transaction is reason, explanation and basis (legal relationship and its content) why the funds were transferred

[10] **the origin of the funds** used in the transaction is the activity by which the funds were earned or received

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;[112]
- 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%;[2]
- gathering information on the origin of the funds and wealth of the customer and its beneficial owner;[2,123]
- 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]

[112] this measure shall be always applied, where the Company comes in contact with the high-risk third country via the Customer or transaction

[123] this measure shall be always applied, where the Customer is a PEP

- an analysis of the Customer's digital impression on the Internet is made (Adverse Media Search);
- obtaining the approval of the Director for transactions with new and existing Customers;[2,3]

The 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.

SIMPLIFIED DUE DILIGENCE MEASURES

Simplified due diligence (SDD) measures may be applied where the Customer's risk profile indicates low risk and where, in accordance with the Company's risk assessment, it has been identified that in such circumstances the risk of money laundering or terrorist financing is lower than usual.

In the course of SDD measures, the Company shall perform at least the following:

- verify, that SDD measures may be applied in accordance with applicable legislation;
- perform identification of the Customer as specified above;
- identify beneficial owner as specified above.

IMPLEMENTATION OF SANCTIONS

Upon the entry into force, amendment or termination of Sanctions, the Company shall verify whether persons in the Customer's ownership structure, 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 FAU 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:

- A consolidated list of EU sanctions;
- A consolidated list of United Nations sanctions.

The Company shall verify the Customer's relation to Sanctions in the course of the Customer's identification process as described 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 code 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 each time when aforementioned sanction lists are updated by the relevant authorities.

If the Employee has doubts that a person is a subject of Sanctions, the Employee shall immediately notify the MLRO or the Director. In this case the MLRO of the Director shall decide on whether to ask or acquire additional data from the person or notify the FAU 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 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 Director, about the identification of the subject of Sanctions, of the doubt thereof and of the measures taken.

The MLRO or the Director 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 FAU 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 FAU of the establishment of the business relationship, transaction or an attempted transaction in accordance with the procedure provided below and received from the FAU 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 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 FAU about this with all the relevant and sufficient information at least 7 working days in advance and on the condition that the FAU 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

If the Company finds a suspicious transaction in connection with its activity, it shall notify the FAU without undue delay. If the circumstances of the case so require, in particular if there is a risk of delay, the Company shall notify the suspicious transaction immediately upon detection.

The minimal characteristics of suspicious transactions are provided in the relevant annex of these Guidelines.

If the necessity of abovementioned report arises, the Employee to whom such necessity became known must immediately notify the MLRO about this. The MLRO shall take decision and send the relevant report to the FAU.

The report shall be sent in accordance with the guidelines, issued by the FAU.

In the notification of a suspicious transaction, the Company shall state the identification data of the person to whom the notification relates, the identification data of all other participants in the transaction available at the time of notification, information on significant circumstances of the transaction and any other information that could be relevant to its assessment in terms of anti-money laundering or anti-terrorist financing measures.

The Company shall postpone the Customer's transaction in which regard notification was submitted to the FAU. The Company has right to perform transaction at the earliest 24 hours after sending the suspect's notification to FAU if the latest didn't provide other instructions.

The Company, a structural unit of the Company, a Director, 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 FAU, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the FAU or about the commencement of criminal proceedings. After a precept made by the FAU has been complied with, the Company may inform a person that the FAU 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 Director 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 Director. At least once a year for the 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, Director and MLRO) who firstly receives therelevant information or documents shall register and retain:

- all data collected within the Customer's identification process, as well as any changes and modifications of this data;
- 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 on the circumstances of termination of the business relationship in connection with the impossibility of application of the CDD measures
- 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 FAU was not notified.

In addition to the abovementioned information the Company shall register the each transaction amount, the currency and the account number.

The data specified above shall be retained for 10 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 FAU 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.

INTERNAL CONTROL OF EXECUTION OF THE GUIDELINES

The performance of the Guidelines shall be internally controlled by the Director, or the Employee appointed by the Director for performing relevant functions (hereinafter in this chapter – Internal Control Officer). 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 perform internal control functions at least in the following fields:

- the Company´s compliance with established risk assessment policy and risk appetite;
- CDD measures implementation;
- implementation of Sanctions;
- the Company´s obligation to refusal to the transaction or business relationship and their termination;
- the Company´s reporting obligation to the FAU;
- the Company´s training obligation regarding the AML/CFT requirements;

- the Company´s obligation for collection and preservation of data.

The exact measures for performing internal control shall be determined by the Internal Control Officer and must correspond to the Company's size and their nature, scope and level of complexity of the activities and services provided. The Internal Control Offices must consider at least examination fields specified above. The internal control measures shall be performed at the time determined by the Internal Control Officer with the frequency set by him or her, at least once per month, if the nature of measure does not expressly provide otherwise.

The results of internal control measures implementation (hereinafter in this chapter – the Internal Control Data) shall be saved separately from other data and retained within 10 years. Only Management Board members and Internal Control Officer may have access to the Internal Control Data. Internal Control Officer may provide access to the Internal Control Data to other Employees or third parties (e. g. advisors, auditors, etc.) only with prior consent of Management Board. The persons have access to the Internal Control Data must not disclose it to anyone without prior consent of the Management Board.

The Internal Control Data shall be saved in chronological order with format, which allows to analyze this and understandable connect this to other relevant data.

The Internal Control Officer shall provide the internal control report to the Management Board at least quarterly and to the general meeting of the Company's shareholders at least annually. The provided internal control report shall include at least the following:

- period of exercising the internal control;
- name and position of the person executing the internal control;
- description of the internal control measures that has been performed;
- results of the internal control;
- general conclusions from the exercised internal control;
- determined deficiencies, which were eliminated in the period of exercising the internal control;
- determined deficiencies, which were not eliminated at the end of period of exercising the internal control;
- measures that are required to implement for elimination of determined deficiencies.

The Management Board shall review the internal control report provided and make resolution regarding it. The Internal Control Officer shall be notified about the essence of such resolution in format which can be reproduced in writing. For this reason, the Management Board is obliged to:

- analyze the results of performed internal control;
- implement actions to eliminate deficiencies occurred.

The Company must review and, if necessary, update internal control procedure at least annually and in the following cases:

- following the publication by the European Commission of the results of an EU-wide money laundering and terrorist financing risk assessment (available on the European Commission's website http://ec.europa.eu);
- after the publication of the results of the National Money Laundering and Terrorist Financing Risk Assessment;
- upon receipt of an instruction from the FAU to strengthen the applicable internal control procedures;
- in the event of significant events or changes in the management and operations of the Company.

Risk assessment and risk appetite

The target of the implementation of internal control measures for Company's compliance with established risk assessment policy (incl. established risk appetite) is examination of the following circumstances:

- Company establishes and uses risk-based approach when providing services to the Customers (e.g., CDD measures implemented in accordance with risk level);
- Company determined factors which affecting the arise of ML/TF risks and determined factors are relevant;
- Company determined and assessed ML/TF of all services which Company provides;
- Company composed the risk profile of the Customer prior the performing transactions or creating business relationship;
- Company updates risk profile of the Customer on regular basis;
- Company follows established risk appetite;
- Company keeps records of all incidents in accordance with established risk assessment policy;
- risk assessment policy was reviewed during the last year and there is no information that MLRO had required earlier review.

Customer due diligence measures implementation

The target of the implementation of internal control measures for Company's compliance with CDD measures implementation is an examination of the following circumstances:

- the Company apply CDD measures prescribed by the Guidelines to all relevant Customers;
- the Company collects proper documents and information when applying CDD measures;
- the Company properly verifies data and documents collected when applying CDD measures;
- the Company applies the relevant level of CDD measures (e. g. EDD measures, etc.);

- the Company applies proper EDD measures to specific Customers (e. g. PEP, high-risk country, etc.);
- the Company performs Customers´ identification in accordance with established procedure;
- the Company properly identifies Customers´ representative(s);
- the Company properly identifies Customers´ beneficial owners;
- the Company properly identifies Customers´ PEP status;
- the Company properly identifies purpose and nature of business relationship or transaction;
- the Company properly monitors business relationships with Customers.

Implementation of Sanctions

The target of the implementation of internal control measures for Company's compliance with implementation of Sanctions is an examination of the following circumstances:

- the Company applies procedure for identification of a subject of Sanctions or transaction violating Sanctions;
- the Company performs actions if identifies a subject of Sanctions or transaction violating Sanctions.

Obligation to refusal of transaction or business relationship and their termination

The target of the implementation of internal control measures for Company's compliance with obligation to refuse the transaction or business relationship and their termination is an examination of the following circumstances:

- the Company refuses transaction or business relationship if it´s obligatory in accordance with the Guidelines;
- the Company refuses or terminates transaction or business relationship if it´s obligatory in accordance with the Guidelines.

Reporting obligation

The target of the implementation of internal control measures for Company's compliance with reporting obligation is an examination of the following circumstances:

- the Company sends reports and information to the FAU, if it's required by the Guidelines (incl. relevant FAU's guidelines);
- the reports sent to FAU are filled in accordance with the FAU's guidelines.

Training obligation

The target of the implementation of internal control measures for Company's compliance with training obligation in AML/CTF field is an examination of the following circumstances:

- all Employees (incl. MLRO and Director) have relevant training;
- each Employee (incl. MLRO and Director) has been training for the last 360 days.

Obligation of collection and preservation of data

The target of the implementation of internal control measures for Company's compliance with obligation of collection and preservation of data is an examination of the following circumstances:

- all data which shall be saved in accordance with the Guidelines (hereinafter in this chapter – the Saved Data) have been properly saved in chronological order with format, which allows to analyze this and understandable connect the Saved Data to other relevant data;
- only Employees (incl. MLRO and Director) or authorized third parties have access to the Saved Data;
- all relevant logbooks are kept in accordance with the Guidelines;
- the Saved Data in electronic format has backup;
- the Saved Data in other formats (e. g. on paper) has backup in electronic format;
- the Saved Data is irrevocably deleted in accordance with the Guidelines.

ANNEXES

Annex title	Document description
1. Risk Assessment Policy	Establishes principles for the Company´s risk management (incl. risk assessment and risk factors) regarding to money laundering and terrorist financing risks. Includes its own annexes.
2. Requirements for data collecting and verification	Establishes requirements for data and documents shall be collected and verified in the course of application CDD/EDD measures.
3. Requirements for business relationship's monitoring	Establishes measures shall be applied in the course of the Business Relationship's monitoring (ODD measures).
4. Transactions log	Establishes the set of data shall be saved regarding each transaction with the Customer.
5. The list of Employees and their responsibilities	The list of employees with their liabilities within the Guidelines specified.
6. Training protocol	The draft of the document shall be signed by the Employee(s) when the relevant training has been performed.

7. MLRO report form	The report form, which MLRO shall quarterly provide to the Management Board.
8. FAU & other guidelines	Contains guidelines issued by the FAU and other authorities (FATF).
9. List of sources	Non-exhaustive list of sources may be used for applying CDD/EDD measures.
10. Indicators of suspicious transactions	Contains non-exhaustive list of indicators of suspicious transactions.