**ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING COMPLIANCE GUIDELINES**

*Last updated on 25.09.2023*

**1. INTRODUCTION**

The purpose of these Guidelines for Anti-Money Laundering (AML), Combating Terrorist Financing (CFT) and Sanctions measures is to ensure that MikePay 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. These Guidelines have been adopted to ensure that the Company complies with all applicable international rules and regulations for the prevention of Money Laundering and Terrorist Financing.

These Guidelines are subject to a review by the Management Board at least annually. Proposals for a review and the review of these Guidelines may be scheduled more frequently by the decision of the Company's Money Laundering Reporting Officer (MLRO) or the Internal Control Officer.

**2. CONTACT US**

Company name: MikePay LTD, Registration country: Republic of Seychelles, Registration number: 238574, Email: mikepay@mikepay.net

**3. 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 simplified and enhanced due diligence measures, as specified below.

**3.1. 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 during the ongoing monitoring of the Business Relationship;
* within 24 hours - upon executing or mediating of Occasional Transaction(s) outside the Business Relationship, where the value of the transaction(s) amounts to 700 euros or more (or an equal amount in another assets);
* 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 does not perform the 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 applicable for the Company. The use of translations should be avoided in situations where the original documents are prepared in a language applicable for the Company.

Achieving CDD is a process that starts with the implementation of CDD measures. When that process is complete, the Customer is assigned a 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 assertion 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 assertion 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.

**3.2. Application of Simplified Due Diligence Measures (level 1)**

Simplified due diligence (SDD) measures are applied where the Customer’s risk profile indicates low risk level of ML/TF.

When applying SDD measures, the Company must only obtain[[1]](#footnote-0) the following data of the Customer who is a natural person:

* name(s) and surname(s);
* personal number;[[2]](#footnote-1) or

in case of the Customer, which is a legal entity, the following data:

* business name or name;
* legal form;
* registration number, if such number has been issued;
* head office (address) and address of actual operation;
* the Customer´s representative name(s), surname(s) and personal number or date of birth; and ensure that the first payment be carried out through an account with a credit institution, where the credit institution is registered in EEA or in a Third Country which imposes requirements equivalent to those laid down in the relevant law and is supervised by competent authorities for compliance with those requirements.

SDD measures may be carried out only where the ongoing monitoring of the Customer’s Business Relationship is performed in accordance with the Guidelines and there is a possibility to identify suspicious Monetary Operations and transactions.

SDD measures must not be carried out in the circumstances where enhanced due diligence measures (as described below) must be carried out.

Where, in the course of performing ongoing monitoring of the Customer’s Business Relationships, it is established that the risk of ML and/or TF is no longer low, the Company must apply the relevant level of CDD measures.

**3.3. Application of Standard Due Diligence Measures (level 2)**

Standard due diligence measures are applied to all Customers where 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;
* 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 Relationship, 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 or performing transaction. The exact instruction for application standard due diligence measures is provided in the Guidelines.

**3.4. Application of Enhanced Due Diligence Measures (level 3)**

In addition to standard due diligence measures, the Company applies enhanced due diligence (EDD) measures in order to manage and mitigate an established risk of Money Laundering and Terrorist Financing in the case where the risk is established to be higher than usual.

The Company always applies EDD measures, when:

* the Customer's risk profile indicates high risk level of ML / TF;
* 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;
* where cross-border correspondent relationships are commenced with the Customer, which is financial institution of Third Country;
* in the case of performance of transaction or Business Relationship with the PEP, the family member of the PEP or a person known to be the close associate of the PEP;
* where transaction or Business Relationship are carried out with natural persons residing or legal persons established in high-risk Third Countries as identified by the European Commission;
* 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 FATF.

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).

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 reassesses the Customer’s risk profile no later than every six months.

**4. CUSTOMER DUE DILIGENCE MEASURES**

**4.1. 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:

* name(s) and surname(s);
* personal number;[[3]](#footnote-2)
* citizenship;[[4]](#footnote-3)
* photograph;
* signature.[[5]](#footnote-4)

The following valid identity documents which contain data specified above may be used as the basis for the identification of a natural person:

* an identity document;
* a residence permit;
* a driving license issued in a state of the European Economic Area in accordance with the requirements laid down in Annex I to Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licenses (recast).

The Customer, who is natural person, cannot use a representative in the course of business relationship or Occasional Transaction with the Company.

**4.2. 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;
* legal form;
* registration number, if such number has been issued;
* name(s) and surname(s), personal number (in the case of an foreigner – date of birth or where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification) and citizenship of the director(s) or member(s) of the Management Board or member(s) of another equivalent body, and their authorities in representing the Customer;
* an extract of registration and its date of issuance;
* head office (address) and address of actual operation.

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 relevant register of legal entities, the submission of the documents specified above do 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.

**4.3. 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 collects the following data regarding the Customer's Beneficial Owner(s):

* name(s) and surname(s);
* personal number;[[6]](#footnote-5)
* citizenship.[[7]](#footnote-6)

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 when collecting data about the Customer).

The Company does not 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[[8]](#footnote-7) or indirect[[9]](#footnote-8) shareholding. Family connections and contractual connections must also be taken into account here;
* who is the natural person in senior management[[10]](#footnote-9), 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.

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.

**4.4. 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[[11]](#footnote-10) or close associate[[12]](#footnote-11) 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 when collecting data about the Customer).

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 international search engine (e. g. 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.

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.

**4.5. 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 may request from the Customer the following information for understanding the purpose and nature of the Business Relationship or transaction:

* whether the Customer will use the services of the Company for their own needs or will represent the interests of another person;
* contact information;
* information on the registered address and actual living address of the Customer;
* 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 and which activities they are;
* information on the source of funds related to the Business Relationship or transaction, if amount of transactions (incl. expected amount) exceeds established limit.

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.

The area of activity 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.

**4.6. 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 and update the Customer´s risk profile. The regularity of the checks and update 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 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 request 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, who shall assess, before the approval, the 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 the case, where the 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 transactions 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[[13]](#footnote-12) and origin[[14]](#footnote-13) 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;
* the transactions do not correspond to the information previously known about the Customer;
* the Company wants to or should reasonably consider it necessary to assess whether the transactions correspond to the information previously known about the Customer;
* 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.

**5. REFUSAL TO THE TRANSACTION OR BUSINESS RELATIONSHIP AND THEIR TERMINATION**

The Company is prohibited to establish a Business Relationship and the established Business Relationship or transaction shall be terminated (unless it is objectively impossible to do) 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”).

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 10 (ten) business days 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. 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.

**5.1. Not-Acceptable Customers**

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

* Customers who fail or refuse to submit, the requested data and information for the verification of his identity, without adequate justification;
* Shell Banks;
* Customers from the jurisdictions which are being banned by internal policies from the company or international sanctions;
* Customers who were identified as the persons subject to International Sanction Act;
* Customers who were identified as the persons subject to the UN Sanctions; EU Sanctions; Sanctions administered by the Office of Financial Sanctions Implementation, Sanctions administered by the Office of Foreign Assets Control;
* the Company suspects money laundering or terrorist financing;
* any other that the Company considers risky to its business or suspicious in regards to Money Laundering and Terrorist Financing.

 The Company will not accept as Сustomers, persons or entitled from Afghanistan, Algeria, Antigua and Barbuda, Argentina, Armenia, Aruba, Bahamas, Barbados, Belize, Belarus, Benin, Bolivia, Burkina Faso, Burma, (Myanmar), Cabo Verde, Cambodia, Cayman Islands, Central African Republic, Cuba, Crimea (region of Ukraine), Côte d'Ivoire, Congo, Democratic People's Republic of Korea, Dem. Rep. of Ethiopia, Dominican Republic, Donetsk (region of Ukraine), Ecuador, El Salvador, Eritrea, Ghana, Guatemala, Guyana, Guinea, Guinea-Bissau, Haití, Honduras, Iran, Iraq, Jamaica, Jordan, Kenya, Laos, Liberia, Lebanon, Libya, Luhansk (region of Ukraine), Macau, Mali, Malta, Morocco, Mozambique, Myanmar, Nicaragua, Nigeria, Pakistan, Panama, Paraguay, Philippines, People's Republic of China, Russia, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Senegal, Seychelles, South Sudan, Syria, Somalia, Sri Lanka, Trinidad and Tobago, Uganda, Vanuatu, Venezuela, Yemen, Zimbabwe.

Persons or entities from jurisdictions where a particular license or permit is required will not be accepted as Customers if the Company has not received such a permit or license.

**6. IMPLEMENTATION OF SANCTIONS**

Upon the entry into force, amendment or termination of Sanctions, the Company shall verify whether the Customer, their Beneficial Owner 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 inform the FCIS thereof within 3 hours.

**6.1. Procedure for identifying the subject of Sanctions and a transaction violating Sanctions**

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

* [A consolidated list of EU sanctions](https://eeas.europa.eu/topics/sanctions-policy/8442/consolidated-list-of-sanctions_en);
* [A consolidated list of United Nations sanctions](https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list).

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 above mentioned 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 or the Management Board member shall decide whether to ask or acquire additional data from the person or notify the relevant authorities 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.

**6.2. 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 relevant authority 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 that is implemented against the person to ensure legal and proper application of measures.

**In case of any doubts or concerns, please contact us at: mikepay@mikepay.net**

1. When the Customer is state or municipal institution or agency the Company may in the course of applying SDD measures collect only personal number of such entity´s and their representative [↑](#footnote-ref-0)
2. in the case of a foreigner – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification), the number and period of validity of the residence permit and the place and date of its issuance [↑](#footnote-ref-1)
3. in the case of a foreigner – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification), the number and period of validity of the residence permit and the place and date of its issuance (applicable to foreigners); [↑](#footnote-ref-2)
4. where an identity document does not contain data on the customer’s citizenship, financial institutions and other obliged entities must, when identifying the customer that is a natural person in the physical presence of the customer, require the customer to provide the data on citizenship. [↑](#footnote-ref-3)
5. except for the cases where it is optional in the identity document [↑](#footnote-ref-4)
6. in the case of a foreigner – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification), the number and period of validity of the residence permit and the place and date of its issuance (applicable to foreigners); [↑](#footnote-ref-5)
7. where an identity document does not contain data on the customer’s citizenship, financial institutions and other obliged entities must, when identifying the customer that is a natural person in the physical presence of the customer, require the customer to provide the data on citizenship. [↑](#footnote-ref-6)
8. **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 [↑](#footnote-ref-7)
9. **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. [↑](#footnote-ref-8)
10. 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.). [↑](#footnote-ref-9)
11. **family member** means the spouse, the person with whom partnership has been registered (i.e.

the cohabitant), parents, brothers, sisters, children and children’s spouses,

children’s cohabitants [↑](#footnote-ref-10)
12. **close associate** means a natural person who, together with PEP, is a member of the same legal entity or of a body without legal personality or maintains other business relationship; or a natural person who is the only the Beneficial Owner of the legal entity or a body without legal personality set up or operating de facto with the aim of acquiring property or another personal benefit for the PEP. [↑](#footnote-ref-11)
13. **the source of the funds** used in the transaction is reason, explanation and basis (legal relationship and its content) why the funds were transferred [↑](#footnote-ref-12)
14. **the origin of the funds** used in the transaction is the activity by which the funds were earned or received [↑](#footnote-ref-13)