Pursuant to Article 44 paragraph 2 item 3 of the Central Bank of Montenegro Law (OGM 40/10, 46/10, 06/13, 70/17) and Article 17 of the Statute of the Central Bank of Montenegro (OGM 83/17), and in conjunction with Article 7 paragraph 3 of the Law on the Prevention of Money Laundering and Terrorist Financing (OGM 33/14, 44/18) and Article 2 paragraph 1 of the Rulebook on guidelines for developing risk analysis and risk factors for the purpose of preventing money laundering and terrorist financing (OGM 65/18), at its meeting held on 5 April 2019, the Council of the Central Bank of Montenegro adopted the following

GUIDELINES
FOR DEVELOPING RISK ANALYSIS AND RISK FACTORS FOR THE PURPOSES OF PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING BY REPORTING ENTITIES UNDER THE SUPERVISION OF THE CENTRAL BANK OF MONTENEGRO

I. INTRODUCTION

In accordance with the Law governing the prevention of money laundering and terrorist financing (OGM 33/14, 44/18) - (hereinafter: the Law) and enabling regulations under this Law, these Guidelines regulate in more detail the development of risk analysis top be used by the reporting entities licensed and/or authorised and supervised by the Central Bank of Montenegro (hereinafter: the reporting entities) to assess the risk of an individual customer, a group of customers, a country or geographic area, business relationship, a transaction or a product, services and distribution channels based on risk factors associated with money laundering and terrorist financing and the result of the national risk assessment.

Pursuant to the Law, the following reporting entities shall apply these Guidelines:

- banks and other credit institutions and foreign bank branches;
- financial institutions carrying out the operations of purchase of receivables, finance lease, provision of safe deposit boxes, factoring, issuing of guarantees and other sureties, lending and credit mediation and exchange operations;
- payment system service providers, other than banks and other credit institutions and foreign bank branches (hereinafter: the payment institutions) and electronic money institutions having their head offices in Montenegro, and
- legal persons, undertakings and natural persons performing their activities and/or carrying out their business with regard to the issuing and managing virtual currencies, including the conversion of virtual currencies into conventional currencies and vice versa, licensed and/or authorised by the Central Bank of Montenegro.

These Guidelines consist of two parts: the first part applies to all reporting entities, while the second part applies only to individual reporting entities taking into consideration specific circumstances with regard to risks those reporting entities are exposed to in their operations.

II. GUIDELINES APPLIED TO ALL REPORTING ENTITIES

In accordance with the Guidelines, a reporting entity shall analyse risk for the purpose of preventing money laundering and terrorist financing which includes the following:

1) the manner of determining the possibilities of operations with a customer;
2) risk assessment of an individual customer, a group of customers, a country or a geographic area, business relationship, transaction or product, services and distribution channels from the aspect of the prevention of money laundering and terrorist financing;
3) the manner of customer's identification;
4) customer due diligence, including repeated annual control;
5) managing of risks that expose reporting entities to money laundering and terrorist financing;
6) professional education and training of employees in reporting entities;
7) mandatory internal acts and procedures that regulate in more detail the operations of the reporting entities with regard to the function of the prevention of money laundering and terrorist financing.

1. MANNER OF DETERMINING POSSIBILITIES OF OPERATIONS WITH A CUSTOMER

A reporting entity shall, before establishing the business relationship and executing a transaction, apply the prescribed customer due diligence measures in order to provide risk identification and assessment. Where the reporting entity is not able to conduct the aforesaid measures in the manner specified by the Law, it shall refuse to establish business relationship and execute the transaction, and where business relationship has been already established, it shall terminate such a business relationship.

In addition to mandatory establishment of the customer's identity, the reporting entity should establish a system of implementing all measures in the manner specified by the Law in order to determine for each customer, to the maximum extent possible, the sufficient amount of mandatory and relevant data and information, which would be the elements for carrying out the risk assessment. Risk assessment established in such a way would be a basis for making decisions on establishing business relationship with the customer, or its duration, which particularly refers to the application of further measures against such a customer (customer due diligence).

The main preconditions for determining the level of risk and taking necessary measures are: establishing and verifying the identity of a customer, data on the purpose and nature of business relationship or the purpose of transaction, the amount of funds, the value of assets or the volume of the transaction, the duration of the business relationship, the compliance of such a customer with the purpose of entering into the business relationship, and other data and information pertaining the risk profile of the customer. The analysis of these data and assignment of risk score for individual elements should result in final risk assessment and overall acceptability of the customer with regard to the establishing business relationship with the customer.

Exceptionally, a reporting entity may apply the prescribed customer due diligence measures also during the establishment of the business relationship with the customer if this is necessary for the purpose of establishing business relationship and if there is lower risk of money laundering or terrorist financing.

2. RISK ASSESSMENT OF A CUSTOMER, A GROUP OF CUSTOMERS, A COUNTRY OR GEOGRAPHIC AREA, BUSINESS RELATIONSHIP, TRANSACTION OR PRODUCT, SERVICES AND DISTRIBUTION CHANNELS FROM THE ASPECT OF MONEY LAUNDERING AND TERRORIST FINANCING

Risk assessment is a binding condition for establishing business relationship and for its duration. The reporting entity shall act with due care both before establishing business relationship and when making decision on acceptability of the customer, and during the business relationship in order to monitor risk in accordance with the assessment in an efficient manner, to change its score (where necessary) and finally, to control it efficiently.
With that regard, the reporting entity shall, within 60 days following that of its establishment, develop risk analysis for determining the risk assessment of a customer, a group of customers, a country or geographic area, business relationship, transaction or product, services and distribution channels for the purpose of the prevention of money laundering or terrorist financing.

A risk assessment should consist of two related steps:
a. the identification of ML/TF risk; and
b. the assessment of ML/TF risk

The risk analysis used by the reporting entity to determine the risk assessment of money laundering and terrorist financing shall include the identification, measurement, monitoring and control of ML/TF risk. Based on the results of the risk analysis, the reporting entity shall undertake appropriate actions and measures for reducing the risk of money laundering and terrorist financing.

Before establishing a business relationship or executing an occasional transaction, the reporting entity shall apply standardised customer due diligence measures aimed at identifying and assessing risk.

In accordance with the standardised measures for risk assessment of a customer, a group of customers, a country or geographic area, business relationship, transaction or product, services and distribution channels, the reporting entity shall apply the method of analysing determined factors and classify a customer in one of three risk categories, based on which further measures are determined.

Risk category	***Code of risk category***
Low risk	A
Medium risk	B
High risk	C

In addition to standardised customer due diligence measures, the reporting entity may apply also simplified and enhanced customer due diligence.

Special forms of customer due diligence – simplified and enhanced customer due diligence are described in more detail in Section 4.1 of these Guidelines (which refers to all reporting entities).

The reporting entity shall perform the risk assessment of individual customer and a group of customer based on risk analysis-based approach. When developing risk analysis of money laundering and terrorist financing, the reporting entity shall carry out standardised customer due diligence measures in accordance with the Law, which are stipulated by Article 8 of the Law, paragraph 1 and 2:

"(1) A reporting entity shall implement the measures of establishing and verifying the identity of the customer, as well as monitoring of business relationship and the control of the transactions of the customer and, in particular, it shall:

1) establish and verify a customer's identity based on documents, data and information from reliable, independent and objective sources and collect data on the customer, and verify the collected data on the customer based on reliable, independent and objective sources (hereinafter: customer's identification);
2) identify the beneficial owner of customer and verify their identity including the measures necessary to determine ownership and control structure of the customer in cases defined by this Law;
3) obtain data on the purpose and nature of a business relationship or purpose of transaction and other data in accordance with this Law;
4) monitor regularly the business relationship, including control of the transactions undertaken with the reporting entity by the customer during the business relationship and verify their compliance with the nature of a business relationship and the usual scope and type of customer's activities.

(2) During the implementation of the measures referred to in paragraph 1, items 1 and 2 of this Article, the reporting entity shall check that any person acting on behalf of the customer has the right to represent or is authorised by the customer, as well as to establish and verify the identity of any person who acts on behalf of the customer pursuant to the provisions of this Law."

The reporting entity shall, as a rule, implement the measures for establishing and verifying the identity of the customer before establishing the business relationship or before executing the transaction, and in exceptional cases, the reporting entity may carry out the measure for verifying the identity of the customer also during the establishment of the business relationship with the customer if it estimates that this is necessary in order to prevent the disruption of regular operations and if there is a risk of money laundering or terrorist financing. This exception must be specified in the internal acts of the reporting entity.

With a view to ensuring qualitative risk assessment, the reporting entity shall apply customer due diligence in cases prescribed by Article 9 of the Law.

Where the reporting entity has not implemented all measures prescribed for establishing and verifying the identity of the customer based on documents, data and information from reliable, independent and objective sources, the reporting entity shall not:

- establish business relationship with the customer, and where the business relationship has been established, the reporting entity shall terminate such a relationship,
- execute the transaction.

Upon the establishment and verification of the customer's identity, the reporting entity shall, based on the prescribed risk factors, classify customer into the appropriate risk

category of money laundering or terrorist financing. The development of risk analysis for money laundering and terrorist financing requires a good knowledge of the customer and its business and therefore, it is recommended that the classification of customers per risk categories is carried out by the organisational unit that knows customers and in cooperation with the compliance officer for implementing measures of detection and prevention of money laundering and terrorist financing.

Immediately after establishing the business relationship, the reporting entity shall, based on risk analysis, determine initial risk profile of the customer and classify customer into the appropriate risk category, while during the business relationship, based on repeated risk analysis, the reporting entity shall either confirm the initial risk profile of the customer if no deviations occurred or reclassify the customer on the basis of its risk profile; therefore, the reporting entity shall develop the system of records by risk categories and their reclassifications (with listed reasons).

The reporting entity shall review and identify risk of products/services or transactions pertaining the level of their complexity, value and the level of anonymity.

The reporting entity shall, prior to introducing new product/service, analyse and assess the following:

- risk of money laundering and terrorist financing that may arise from such a product/service;
- impact of the new product/service on the exposure of the reporting entity to the risk of money laundering and terrorist financing;
- impact of the new product/service on the possibility of adequate management of risk of money laundering and terrorist financing.

With regard to the level of complexity of a product/service or transaction, the reporting entity shall, when assessing risk, assess in particular the extent to which it can completely create clear review of the basis of those products/services or transactions (the existence of the required document), parties involved in the business relationship, the method for execution, and jurisdictions involved, thus core elements underlying the risk assessment and eligibility for the execution of transactions/services. In such an assessment, the reporting entity shall analyse the elements of complexity and impact on risk and take adequate measures with respect to its findings. With regard to the complexity of product/service or transaction, the reporting entity should pay special attention to whether the multiple parties or multiple jurisdictions are included in the business relationship, to what extent is allowed that the products or services are paid by third parties, whether the transaction is with an economic rationale, i.e. whether it is followed by a reasoned basis and the amount. The reporting entity should understand risks of new products, particularly those that include the use of new technologies or methods of payment.

With regard to the value of products/services or transactions, the reporting entity should assess in particular to what extent the products or services include, facilitate or encourage large value transactions, to what extent the products or services are provided in cash or in large amounts, and it shall take adequate measures to manage this risk.

The reporting entity shall determine the extent to which individual product/service or transaction allows or facilitates the anonymity of the customer or beneficial owner of the

customer (e.g. bearer shares, off-shore legal persons, legal persons structured in such a way as to take advantage of anonymity and virtual currencies, and the like), and to determine risk of possibility that a third party that is not part of the business relationship gives instructions with respect to that business relationship or allows such a party access to the use of product/service or transaction.

The following table shows cases in which the reporting entity is obliged to implement standardised customer due diligence measures, and types of measures the reporting entity shall implement for the purpose of customer due diligence.

Cases in which the reporting entity undertakes to implement standardised customer due diligence measures							
Customer due diligence measures		(1) when establishing a business relationship	(2) when executing one or more connected occasional transactions in the amount of 15,000 euros or more	(3) during each occasional transaction which represents the transfer of funds in the value of 1,000 euros or more;	(4) when there is a suspicion about the accuracy or veracity of the obtained customer and beneficial owner identification data;	(5) when there are reasons for suspicion of money laundering or terrorist financing related to the transaction or customer;	(6) for natural or legal persons trading in goods, when executing occasional cash transactions in the amount of 10,000 euros or more, regardless of whether the transaction is executed as a single transaction or a number of mutually linked transactions.
	(a) customer's identification	✓	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes
	(b) establishing and verifying the identity of beneficial owner	✓	✓ Yes	✓ Yes	✓ Yes (additional data)	✓ Yes (additional data)	✓ Yes
	(c) obtaining data on the purpose and nature of the business relationship and the purpose of the transaction	✓	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes
	(d) customer identification when accessing safe deposit box	✓	-	-	✓ Yes	✓ Yes	-
	(e) obtaining additional data for the customer which is politically exposed person	✓	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes

2.1. Identification of risk of money laundering and terrorist financing

The reporting entity shall identify risks of money laundering and terrorist financing to which it is exposed or could be exposed due to the establishment of the specific business relationship or execution of occasional transaction. When identifying risk of money laundering and terrorist financing associated with a certain business relationship or occasional transaction, the reporting entity shall consider information and data relevant for risk analysis, as well as risk factors of customers, business relationship or a country or geographic area, transaction or product, service or distribution channels in order to prevent the use of its services or products for the purpose of money laundering or terrorist financing.

During the identification of risk of money laundering and terrorist financing, the reporting entity shall analyse the following:

2.1.1. Information and data relevant for analysing risk of money laundering and terrorist financing

The information and data for identifying risk of money laundering and terrorist financing, which the reporting entity is obliged to consider and use from publicly available sources and/or public registries and databases, at least shall cover the following:

- National risk assessment of money laundering and terrorist financing;
- Reports, typologies and other information of the administration competent for the prevention of money laundering and terrorist financing and other supervisory authorities;
- Knowledge and experience of the employees in the reporting entities in the area of the prevention of money laundering and terrorist financing;

The information and data for identifying risk of money laundering and terrorist financing, which the reporting entity may consider, at least shall cover the following:

- Risk assessment of money laundering and terrorist financing at the EU level;
- Information from civil society on corruption indices at the national level as well as in other countries;
- Information from international standard-setting bodies concerning the prevention of money laundering and terrorist financing;
- Information from credible and reliable public sources, media and other mass-media channels.

The development of risk analysis for the purpose of preventing money laundering and terrorist financing shall at least include the following **risk factors**:

- **Risk factors associated with customer:** risk factors relating to its status or activity (e.g. government body, politically exposed person, customer whose activity is connected with cash transactions, non-government organisations, and the like);

- **Risk factors associated with business relationship, transactions, services, distribution channels or products:** risk of business relationship with e.g. customer whose country of origin does not respect money laundering and terrorist financing standards, politically exposed person and other business relationships bearing high risk based on the reporting entity's assessment.

- **Risk factors associated with specific country (or geographic area) which does not have** adequate systems for the prevention of money laundering and terrorist financing, which has high level of corruption or criminal activity, a country and geographic area against which the international organisations have introduced restrictive measures.

Risk factors underlying the level of risk of a customer or a group of customers, country or geographic area, business relationship, transaction or product, service or distribution channels are given in the following risk matrix:

Risk matrix

Customer high-risk factors	
1.	Customer high-risk factors: a) when establishing and identifying the identity of the customer in their absence is implemented; b) if the business relationship is carried out under the unusual circumstances; c) customers live or are registered in countries or geographic areas listed in item 3 of this Matrix; d) a customer is a politically exposed person; e) a customer is non-resident customer; f) legal persons or legal arrangement (trusts) performing custody activities and asset management activities; g) undertakings the ownership structure of which registers nominally the authorised representatives or bearer shares instead of beneficial owners; h) legal persons and undertakings whose activity is related with the cash transactions; i) if the ownership structure of a legal person or an undertaking is unusual or complex due to the nature of its business; j) a customer for which the reporting entity submitted reports on suspicious transactions in the last three years to the competent body of the administration; k) a customer for which the competent body of the administration issued an order for temporary suspension of transaction or request for ongoing monitoring of its financial business; l) a customer is a person that is on the internal list of the reporting entity or a group.

High-risk factors in business relationship, transactions, products, services and distribution channels	
2.	High-risk factors in business relationships, transactions, products, services, distribution channels or products: a) private banking; b) products or transactions that allow concealing the identity of the customer or anonymity of the customer (e.g. internet banking); c) indirect business relationship or a transaction; d) new products and new businesses, including new delivery mechanisms and use of new technologies for both new and existing products.
Country-specific or geographic area high-risk factors	
3.	High-risk countries in which the customer has permanent or temporary residence for natural persons or head office for legal persons are as follows: a) countries that are identified, based on the reports of relevant international institutions[1] (e.g. Financial Action Task Force (hereinafter: FATF[2]) and Committee of Experts on the Evaluation of Anti- Money Laundering Measures and the Financing of Terrorism (hereinafter: MONEYVAL[3]) on joint evaluation, as countries that do not have efficient anti-money laundering and terrorist financing system; b) countries in which high level of corruption and other criminal activities has been identified; c) countries with enforced sanctions, embargo or similar measures; d) countries providing money support or support to terrorist activities or have certain terrorist organisations operating in their countries; e) countries known as off-shore financial centres.
Customer low-risk factors	
4.	Low-risk factors for a customer that is: a) a government body or a local self-government body and other legal person performing public authorities; b) an undertaking or other form of performing business activity that executes public authorities, which is listed on the stock exchange and which is subject to reporting requirements based on the stock exchange rules or in accordance with the regulations that introduce the obligation of transparency of beneficial owner of such an undertaking; c) from a country or geographic area that is less risky in accordance with the risk factors set out in item 6 of this Matrix;

[1] With regard to information on risk countries or non-ccoperative countries or territories that do not meet key international standards on the prevention of money laundering and terrorist financing refer to the websites of the relevant international bodies:
[2] FATF: www.fatf-gafi.org,
[3] MONEYVAL: www.coe.int/t/dghl/monitoring/moneyval

Low-risk factors in business relationships, transactions or for products	
5.	Low-risk factors in business relationships, transactions or for products: a) financial products and institutions providing identified and limited services to a specific type of the customer for the purpose of increasing access to financial inclusion; b) products where risk of money laundering and terrorist financing depends on other factors, such as limits of the amounts for electronic money transfer or transparency of ownership;
Country-specific or geographic area low-risk factors	
6.	Country-specific or geographic area low-risk factors include: a) if those countries are EU Member States; b) if they have an efficient anti-money laundering and terrorist financing system that is recognised by the FATF c) where low level of corruption and other criminal activities has been identified; d) which implement the FATF recommendations for the prevention of money laundering and terrorist financing and for which the compliance with these recommendation is implemented.

The reporting entity shall cover in its internal acts all risk factors that are prescribed in these Guidelines, whereby the reporting entity may define also other risk factors associated with the specific nature of the customer's business.

2.2. Weighting risk factors

The reporting entity shall determine the relevance of different risk factors of money laundering and terrorist financing in the context of a business relationship or occasional transaction. Weight given to different risk factor may vary from product to product, service to service, customer to customer or group of customers. When weighting risk factors, the reporting entity shall ensure that:

a) Weighting is not unduly influenced by just one factor;
b) Economic or profit considerations do not influence the risk rating;
c) Weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
d) Cases referred to in Article 30 paragraphs 1, 3 and 4 of the Law that always classify into high risk category cannot be overruled by weighting;
e) They are able to override any automatically generated risk scores where necessary, whereas the rationale for the decision to override such scores should be documented appropriately;
f) Where a reporting entity uses automated IT systems to allocate overall risk scores to categorise business relationships or occasional transactions (which it obtained from the external provider), it should understand how the system works and how it combines risk factors to achieve an overall risk score. The reporting entity must always be able to

satisfy itself that the overall score reflects the understanding of risk of money laundering and terrorist financing and it should be able to demonstrate this adequately to the competent authority at its request.

2.3. Customer risk categories

Classification of a customer and a group of customers based on the prescribed risk factors		
Risk category	***Code of category***	***Risk factor***
Low risk	A	The reporting entity shall classify into the category A the following: • a customer to whom it applies simplified customer due diligence in accordance with the Law; • a customer upon establishing business relationship provided that the reporting entity has obtained all data and information for that customer as prescribed by the Law, if all determined risk factors are low; • a customer for which the reporting entity did not notice, during the application of customer due diligence, any discrepancy from regular business activities.
Medium risk	B	The reporting entity shall classify into the category B customers that cannot be categorised as A or C and customers where, during the application of customer due diligence, the reporting entity noticed some discrepancies from regular business activities.
High risk	C	The reporting entity shall classify customer into the category C: • Where it identified a significant discrepancy from regular business activities; • to whom high risk factors are related that are associated with the geographic area; • to whom high risk factors are related that are associated with the business relationship; • to whom high risk factors are related that are associated with the product, service, transaction or distribution channels.

3. THE MANNER OF CUSTOMER'S IDENTIFICATION

3.1. Customer due diligence measures

The reporting entity shall carry out the prescribed customer due diligence measures on the basis of documents, data and information from reliable, independent and objective sources and collect data on the customer, and/or verify the collected data on the customer based on reliable, independent and objective sources (hereinafter: customer's identification).

Upon entering into the business relationship, the reporting entity shall regularly monitor the business relationship, including control of the transactions undertaken with the reporting entity by the customer during the business relationship and verify their compliance with the nature of the business relationship and the usual scope and type of customer's business.

3.2. Establishing and verifying the identity of a customer that is a natural person or an entrepreneur

A reporting entity shall establish and verify the identity of a customer that is a natural person or their legal representative, entrepreneur or a natural person carrying out business activity, by checking the customer's personal identification document in their presence and shall obtain the required data in accordance with the Law.

The identity of a customer that is a natural person may be established on the basis of eligible electronic certificate of a customer issued by a certification service provider in accordance with the regulations. During the procedure, the reporting entity shall obtain data on the customer from the eligible electronic certificate and it shall enter the data into the data records pursuant to Articles 78 and 79 of the Law.

The reporting entity shall obtain for a customer that is a natural person and/or their legal representative, entrepreneur or a natural person carrying out business activity the following data:

Data on customer – natural person	
Data on customer – natural person	• name; • address of permanent or temporary residence; • date and place of birth; • tax identification number of a natural person or their representative; • number, type and the title of the body which issued the document; • name, address of temporary or permanent residence, data and place of birth of the natural person who has access to the safe deposit box; • purpose and assumed nature of the business relationship, including the information on the customer's activity or status (employed, unemployed, student, retired, farmer, etc.); • date of establishing the business relationship or date and time of accessing the safe deposit box.
Data on customer – entrepreneur or natural person carrying out business activity	• name; • address of permanent or temporary residence; • date and place of birth of the entrepreneur or a natural person performing business activity, establishing business relationship or executing transaction, and the number, type and name of the authority issued the document; • tax identification number of the entrepreneur or a natural

	person performing the business activity; • name of the company, address and identification number, if assigned, of the entrepreneur or a natural person performing the business activity.
Data on transaction	• data and time of the execution of the transaction; • the amount and the currency in which the transaction was executed; • the purpose of the transaction and the name and temporary or permanent residence or the name and registered office of a person to whom the transaction is intended; • the manner of executing the transaction; • data on sources of wealth and assets which are or will be subject to the business relationship or transaction.
Data on legal representative and authorised person	• name, address of temporary or permanent residence, date and place of birth, tax identification number and number of personal identification document and the name of authority that issued personal document. The reporting entity shall obtain data on the owner of the account from the written authorisation that is stored in accordance with the Law.

3.3. Establishing and verifying the identity of the customer that is a legal person or an undertaking

The reporting entity shall establish and verify the identity of a customer that is a legal person or an undertaking by checking the original or certified copy of the document (which must not be older than three months) from the Central Registry of Commercial Entities (hereinafter: CRPS) or by checking the original or certified copy of another appropriate public registry submitted by the representative on behalf of the legal entity or undertaking, as well as by checking the court, business or other public registry of a foreign legal person or an undertaking.

The reporting entity may establish and verify the identity of a legal person or an undertaking and obtain mandatory data by checking the CRPS or other appropriate public registry as well as by checking the certified copy of the court, business or other public registry in which the foreign legal person or undertaking has been registered before establishing the business relationship. In that respect, the reporting entity shall write, on the excerpt from the registry, the date, time and the name of a person that checked the document, and the document shall be kept by the reporting entity in accordance with the Law.

The reporting entity shall keep the original or the certified copy of the document referred to in paragraphs 1 and 2 of this item in its files in accordance with the Law.

Where the reporting entity, in the process of establishing and verifying the identity of the legal person, has doubts in the accuracy of the obtained data or veracity of identification documents and other business documents from which the data have been obtained, it shall

obtain also written statement from the representative or authorised person before establishing a business relationship or executing a transaction.

If a customer is a foreign legal person performing its business activity in Montenegro through its business unit, the reporting entity shall establish and verify the identity of the foreign person and its business unit.

Data obtained by the reporting entity on the customer that is a legal person or an undertaking are given in the matrix below:

Data on a customer that is a legal person or an undertaking	
Data on customer	• name of a legal person or an undertaking; • address; • head office and identification number of a legal person that has established the business relationship or had executed the transaction, or a legal person for which business relationship is established or a transaction is executed.
Data on established business relationship	• date of establishing business relationship or accessing safe deposit box; • purpose and assumed nature of the business relationship, including information on customer's activity.
Data on executed transaction	• Date and time of the execution of transaction; • Amount of transaction and currency in which the transaction was executed; • The purpose of the transaction, name and temporary or permanent residence, or name and head office of a person to whom the transaction is intended; • The manner of the execution of transaction; • Data on sources of wealth and funds that are or will be subject to the business relationship or transaction.
Data on a person representing the customer (legal representative or authorised person)	• name; • address of the temporary or permanent residence; • date and place of birth and tax identification number of a representative or an authorised person, which enters into a business relationship or executes transaction for a legal person or another person from civil law; • number and type of the personal identification document; • Name of authority issued the personal identification document.
Data on beneficial owner of the customer	• name; • address of the temporary or permanent residence; • date and place of birth of beneficial owner of a legal person or an undertaking, or in case of Article 20 paragraphs 5 and 6, data on category of person the interest of which is establishing and acting of a legal person or similar legal entity of foreign law.

3.4. Establishing and verifying the identity of a representative, and the identity of an authorised person of legal person and undertaking

- Establishing and verifying the identity of a representative

The reporting entity shall establish and verify the identity of the representative and all directors of a domestic or a foreign legal person or an undertaking in the manner specified under Article 16 of the Law. The reporting entity shall obtain the required data by checking personal identification document of the representative in his presence and by checking personal identification documents of all directors submitted by the representative.

The reporting entity shall, during establishing and verifying the power of attorney for the representative and all directors, obtain power of attorney of the representative and keep it in its documents.

- Establishing and verifying the identity of an authorised person

The reporting entity shall establish and verify the identity of an authorised person of a legal person or an undertaking if the authorised person, on behalf of representative and all directors, establishes the business relationship of a domestic or legal person or an undertaking or exercises the transaction in the manner prescribed by Article 17 of the Law.

The reporting entity shall obtain data on the representative and all directors that are represented by the authorised person by checking the personal identification document and written original power of attorney issued by the representative or its copy certified in accordance with the Law and it shall keep them in its documents.

With respect to establishing and verifying the identity of the representative as well as the identity of the authorised legal person and undertaking, the following action is envisaged in the same manner:

Where it is not possible to determine all prescribed data from the personal identification document of the representative or authorised person, those data shall be obtained from another public document submitted by the representative or authorised person.

Where the reporting entity has doubts in the accuracy of the obtained data during establishing and verifying the identity of the representative and authorised person of a legal person or an undertaking, it shall also request their written statements on the accuracy of those data.

The reporting entity shall, during establishing the identity of the representative and all directors as well as authorised person that acts on behalf of the representative for a domestic or a foreign legal person or an undertaking, obtain photocopies of personal identification documents of those persons in accordance with Article 14 paragraph 5 of the Law.

Where both legal representative and authorised person are absent during the execution of the transaction (i.e. the execution of the transaction using e-banking), the procedures where the reporting entity requires the use of eligible digital certificate and password for confirming the identity of the legal representative or authorised person during the execution of transactions shall be deemed applicable.

3.5. Establishing and verifying the identity of a foreign trust, other person or a foreign entity equal to them

The reporting entity shall establish and verify the identity of a foreign trust, other person or a foreign entity equal to them in accordance with Article 18 of the Law.

Data on customer that is a foreign trust, other person or a foreign entity equal to them	
Data on a customer that is a foreign trust	The reporting entity shall establish and verify data on the identity of a customer that is a foreign trust that refer to: • A settlor; all trustees; protector (representative); beneficiary or a group or beneficiaries who manage an asset provided that the future beneficiaries have been already determined or may be determined; • Other natural person who directly or indirectly has ultimate control over the foreign trust.
Data on a customer that is a foreign trust – a legal person or an undertaking	• Name, address, head office and identification number of a legal person that establishes a business relationship or executes a transaction, or a legal person for which the business relationship is established or the transaction is executed; • Name, address of the temporary or permanent residence, place of birth and tax identification number of the representative or authorised person who establishes business relationship or executes the transaction for a legal person, a foreign trust, other person, or a foreign entity equal to them referred to in Article 18 of the Law, the number and type of personal identification document and the name of the authority that issued personal identification document; • Name, address of the permanent or temporary residence, date and place of birth and tax identification number of the authorised person who requests or executes the transaction for the customer, as well as the number and type of personal identification document and the name of the authority that issued personal identification document.
Data on customer that is a foreign trust – natural person	• Name, address of the temporary or permanent residence, place of birth and tax identification number of the natural person or its representative, entrepreneur or natural person performing activity who establishes business relationship or executes transaction, or a natural person for whom business relationship is established or transaction is executed, as well as the number and type of personal identification document and the name of the authority that issued personal identification document.
Data on established business	• Date of establishing business relationship or accessing the safe deposit box; • Purpose and assumed nature of the business relationship, including

relationship	information on customer's activity.
Data on executed transaction	• Date and time of the execution of the transaction; • Amount of transaction and currency in which the transaction was executed; • Purpose of the transaction, name and temporary or permanent residence, or name and head office of a person to whom the transaction is intended; • the manner of executing the transaction; • Data on sources of wealth and funds that are or will be subject to business relationship or transaction.
Data on person representing the customer (legal representative or authorised person)	• Name; address of temporary or permanent residence; • Date and place of birth and tax identification number of representative or authorised person that enters into the business relationship or executes the transaction for the legal person or other civil law entity; • number and type of personal identification document and the name of the authority that issued personal identification document.
Data on beneficial owner of the customer	• Name; address of permanent or temporary residence; • Date and place of birth of beneficial owner of a legal person or an undertaking, or in case referred to in Article 20 paragraphs 5 and 6 of the Law, data on category of persons the interest of which is founding and acting of the legal person or similar foreign legal entity.

3.6. The manner of determining beneficial owner

The definition of beneficial owner underlying the obligation and the manner of determining beneficial owner is prescribed by Article 20 of the Law.

The reporting entity shall, before establishing business relationship with a legal entity, within establishing and verifying the identity of the customer, also determine beneficial owner of the customer and verify its identity and undertake other necessary measures (establishing if the beneficial owner is politically exposed person, eligibility checks, etc.).

Full and complete implementation of these obligations is one of the conditions for establishing the business relationship with the customer. Therefore, the reporting entity shall accurately and clearly identify the beneficial owner and managing body (management structure) of the customer, i.e. it shall determine the ownership structure of the customer broken down to natural persons that are considered by a definition beneficial owners. The reporting entity shall obtain data on beneficial owner set out as mandatory by the Law by checking the original documents or certified copy of documents from the CRPS or other appropriate public registry as well as by checking court, business or other registry of a foreign legal person in which the beneficial owner is registered and these documents cannot

be older than three months following the issuing date, or it shall obtain them by checking the CRPS or other public registry.

Where the reporting entity cannot obtain all data on beneficial owner of a legal person, an undertaking or a foreign legal person in the prescribed manner, it shall obtain those data by checking the original document or certified copy of the document or other business documentation submitted by the representative or authorised person of the customer that is a legal person, an undertaking or a foreign legal person.

The reporting entity shall, during the establishment of the identity of beneficial owner, obtain a photocopy of personal identification document (e.g. personal ID, passport, driver's licence or other document containing a photo of a person whose identity is being established or verified by the reporting entity), on which it shall write the date, time and the name of a person that checked the document, and it shall keep the document in accordance with the Law.

The reporting entity shall obtain the following data: name, address of the temporary or permanent residence and the date and place of birth of the beneficial owner of a legal person or, in case of Article 20 paragraph 5 and 6 of the Law, the data on the category of persons the interest of which is establishing and acting of a legal person or similar foreign legal entity.

3.7. Establishing and verifying customer's identity through a third party

The reporting entity shall define, by way of internal acts, the procedures on accepting the identification of the customer and beneficial owner through a third party.

The reporting entity may, under the conditions provided for by this Law, entrust to a third party the implementation of the measures of establishing, collecting and verifying the identity of the customer, identifying beneficial owner of the customer and verifying its identity, including measures required for determining ownership and controlling structure of the customer, as well as obtaining data on the purpose and the nature of business relationship or the purpose of the transaction and other data in accordance with this Law.

A third party shall identify the identity of the customer on the basis of documents, data and information from reliable, independent and objective sources and gather all necessary data on the customer or verify gathered data on the customer (hereinafter: customer's identification).

The third party may be: bank or other credit institution and foreign bank branch, a company for the management of investment funds, a branch of a foreign company for the management of investment funds and a company from EU Member States authorised to be directly engaged in the management of investment funds on the territory of Montenegro; a company for the management of pension funds; an authorised participant at the securities market and a branch of a foreign legal person in Montenegro dealing with brokering in purchase and sale of securities upon the order of a customer in their name and for account of a third person with a charge of commission (brokerage activities), and managing portfolio of securities owned by another person (investment manager activities) and legal persons possessing the Commission for Capital Markets' license for performing custody business, except banks; life insurance companies and branches of foreign life insurance companies; mediation companies, representation companies and entrepreneurs – agents in insurance in

the part related to life insurance; equivalent persons with registered office in a Member State of the European Union or another state which applies the standards in the area of the prevention of money laundering and terrorist financing at least to the extent defined by the Law.

The reporting entity shall not accept the execution of measures conducted by a third party if the third party has established and verified customer's identity without its presence.

Since the reporting entity is responsible for proper establishment and verification of the identity of a customer through a third party, it may not entrust measures of establishing and verifying the identity of a customer to a third party if a third party is a quasi-bank or anonymous undertaking or if a customer is from the country which is on the list of the countries that do not apply standards from the area of the prevention of money laundering and terrorist financing published by relevant bodies at their websites or submitted to the reporting entity based on the data of the relevant international organisations.

Where the reporting entity doubts in the validity of establishing and verifying customer's identity by a third party, or the veracity and reliability of the obtained data on the customer, it shall directly establish and verify the customer's identity.

Third party shall, upon a request of a reporting entity, without delay, provide copies of identification documents and other documents upon which it has established and verified customer’s identity and obtained data and documents and it shall keep the obtained copies of identification documents and documentation in accordance with the Law.

When a person establishes and verifies customer's identity on behalf of the reporting entity pursuant to the agreement on entrusting the activities, such a person shall not be considered third party within the meaning of the Law.

4. CUSTOMER DUE DILIGENCE (AND REPEATED ANNUAL CONTROL)

The reporting entity shall establish appropriate procedures for regular and careful customer due diligence to ensure that the transactions correspond to the findings of the reporting entity on such a customer, type of activity, sources of funds, purpose and intended nature of business relationship or transactions, where the scope of measures should be in accordance with the risk of money laundering and terrorist financing. The reporting entity shall ensure the volume or frequency of application of measures of monitoring the business relationship be adjusted to the assessed risk of money laundering and terrorist financing to which it is exposed in its business with customer and in accordance with risk analysis.

In addition to monitoring of business relationship and control of transactions, the reporting entity shall, at least once a year, and no later than after the expiry of one-year period since the last control of the customer, also conduct repeated control of a foreign legal person in the manner stipulated by Article 28 of the Law.

By way of derogation from the paragraph above, the reporting entity shall, at least once a year, and no later than after the expiry of one-year period since the last control of the customer, also conduct repeated control if the customer is, pursuant to the cases referred to in the Law, a legal person with registered office in Montenegro if the foreign share capital in that legal person is at least 25%.

The reporting entity shall obtain data on the purpose and the nature (basis) of the business relationship or the purpose of transaction and other data in accordance with the Law, and it shall continuously apply measures for detecting suspicious activities of the customer. These measures shall be applied on the basis of the list of indicators for identifying suspicious customers and transactions, for which there are reasons for suspicion of money laundering and terrorist financing as well as based on other information and data. All customers must be included in the procedure regardless of their risk profile.

The reporting entity shall, during the business relationship with the customer, update all data and classify customer into the appropriate classification category of risk of money laundering and terrorist financing. For instance, this implies the case when the reporting entity establishes that certain activities of the customer deviate significantly from the normal course of operations and in such a case, it shall carry our additional analysis of the customer's business in order to determine reasons for such a deviation. Pursuant to additional analysis, the reporting entity shall assess the risk profile of a customer and if needed, reclassify the customer.

The following table shows the dynamics in monitoring of business relationship in accordance with the risk profile of the customer:

Monitoring of business relationship in accordance with the risk profile of the customer			
Risk category	***Code of risk category***	***Customer due diligence***	***Monitoring of customer***
Low risk	A	Simplified customer due diligence is applied in the volume and in the manner specified by risk analysis	2 years
Medium risk	B	Standardised customer due diligence with additional required measures as per reporting entity assessment	1 year
High risk	C	Enhanced customer due diligence is applied	6 months

The reporting entity shall specify in its internal acts the dynamics of the assessment of the customer in accordance with the Guidelines.

Where a certain customer, based on risk factors, may be classified into different risk categories with respect to money laundering and terrorist financing, the reporting entity shall ultimately classify customer into the higher-risk category.

4.1 Special forms of customer due diligence

Special forms of customer due diligence, in the context of this Law, shall be:

- enhanced customer due diligence;

- simplified customer due diligence

Where the risk analysis indicates that the established risk factors of the customer, business relationship, transactions, products, services, distribution channel, country or geographic area belong to a high-risk category of money laundering or terrorist financing, the reporting entity shall apply enhanced customer due diligence measures in accordance with the Law.

Where the risk analysis indicates that the established risk factors of the customer, business relationship, transactions, products, services, distribution channel, country or geographic area belong to a low-risk category of money laundering or terrorist financing, the reporting entity shall apply simplified customer due diligence measures (risk matrix, item 4 indents a) and b)) in accordance with the Law.

4.1.1 Enhanced customer due diligence

The reporting entity shall apply enhanced customer due diligence measures in cases that are specifically envisaged by the Law (the overview is given within this point), and always when it is established, based on risk analysis of the customer, that there is or there could be a higher risk of money laundering or terrorist financing connected with the customer, group of customers, country or geographic area, business relationship, transaction, product, service and distribution channel, as well as in cases when high risk of money laundering and terrorist financing is determined in accordance with the national risk assessment.

The application of the enhanced customer due diligence measures shall be mandatory when:

- entering into the correspondent relationship with a bank or other credit institution that has their head office outside the European Union or in a country that is not on the list of countries applying international standards in the area of money laundering and terrorist financing that are equivalent to the EU standards or higher;
- entering into the business relationship or executing one or more connected occasional transactions in the amount of 15,000 euros or above with the customer that is a politically exposed person or beneficial owner of the customer that is a politically exposed person;
- in cases of complex and unusual transactions;
- in cases of electronic money transfer.

4.1.1.1 Correspondent relationship with banks or other credit institutions of other countries

When establishing a correspondent relationship with banks and other similar institutions of foreign countries, the reporting entity shall, in addition to the actions and measures of detecting and monitoring customers in accordance with the risk assessment, obtain also additional data, information and documents prescribed by the provisions of the Law.

The correspondent relationships are regulated in more detail in the Section III, item 1.2 of these Guidelines.

4.1.1.2 Politically Exposed Persons

Politically Exposed Persons belong to the high-risk category, against which a reporting entity shall implement enhanced customer due diligence measures.

Definition of politically exposed persons is laid down in Article 32 of the Law.

With a view to establishing politically exposed persons and their close family members and their close associates within the meaning of the Law, the reporting entity may act in either of the following manners, or their combination:

- by having a customer fill in the form (which is provided in the annex to these guidelines and makes an integral part thereof, the PEP Form);
- by obtaining information from the media;
- by obtaining information by checking the politically exposed persons' data bases (*World Check PEP List*, via internet search, etc.).

The procedure of establishing close associates of politically exposed persons is applied where the reporting entity assesses, on the basis of documented facts that such relationship exists.

The reporting entity shall establish and verify the identity of the customer pursuant to the Law, and, during that procedure, establish whether the customer is a politically exposed person.

The reporting entity shall establish a list of politically exposed persons, which should be made appropriately available to the bank employees in direct contact with customers.

The reporting entity shall establish an internal document containing the procedures which shall define in more detail the obligation to carry out the above mentioned actions and measures of enhanced due diligence of customers identified as being politically exposed persons, as well as the obligation to determine the source of property (wealth) and the source of funds of the customer.

In addition to the above mentioned, in order to establish a business relationship with a politically exposed person, the reporting entity shall obtain a written consent from a senior manager prior to establishing business relationship with a customer, and if the business relationship has already been established, obtain a written consent from a senior manager for continuing the business relationship.

The reporting entity shall also determine whether the politically exposed person is a beneficial owner of a legal person, business organization, trust and other person, i.e. a legal or a natural person equal to it with the registered office in a foreign country, on whose behalf a business relationship is being established or a transaction carried out or other customer's activity performed and obtain required information.

Politically exposed persons fall within the high-risk category and are subject to the reporting entities' obligation to apply enhanced customer due diligence measures, as well as to

monitor with special attention transactions and other business activities carried out with a reporting entity by a politically exposed person or the customer whose beneficial owner is a politically exposed person.

Additional measures that the bank carries out in the procedure of enhanced customer due diligence are presented in the table below:

Case prescribed by law ↓	Determining the source of property (wealth) and the source of funds of the customer	Obtaining a written consent from a senior manager for establishing business relationship with a customer or a written consent from a senior manager for continuing the business relationship ↓	Obtaining data on whether the PEP is the beneficiary owner of the legal person	Obtaining additional documentation and data ↓	Additional review and monitoring of customer's operations ↓	Additional measures ↓
Politically exposed person	Yes	**Yes**	**Yes**	Data set defined in Article 33 of the Law	Yes	As per the reporting entity's assessment

The reporting entity shall pass an internal document defining the procedure to terminate the obligation to treat a person as politically exposed. This shall include the reporting entity's obligation to exclude this person and their close family members and close associates from the list of politically exposed persons following the expiry of a period of 12 months as of the day the performance of the public function in the state has ended. However, where the reporting entity, based on the risk analysis of a specific customer whose performance of the public function defined by the Law has ended, determines that the customer presents a higher risk, the reporting entity shall continue to classify that customer into a high-risk category (C category) and take prescribed measures against that person.

After establishing a business relationship with a politically exposed person, their close family members and close associates pursuant to the Law, the reporting entity shall keep separate records on these persons and transactions.

The reporting entity shall update their list of politically exposed persons on a regular basis, in order to carry out the procedure of enhanced customer due diligence in line with the Law also for those customers who were not politically exposed persons at the time the business relationship was established, but were appointed to perform a public function within the meaning of Article 32 of the Law after the business relationship was established.

In addition, the reporting entity shall make the politically exposed person aware that, in the case they stop performing the public function, they shall inform the reporting entity thereof.

4.1.1.3 Complex and unusual transactions

Complex and unusual transactions are the transactions characterised by complexity and unusually high amounts, unusual pattern of execution, value or connection of transactions which have no apparent economic or lawful purpose, i.e. which are not in alignment with or are disproportionate to the usual, i.e. expected operations of the customer, as well as by other circumstances relating to the status or other characteristics of the customer.

The reporting entity shall analyse all complex and unusually high transactions, even in cases when, in terms of transactions or the customer there are no reasons for suspicion in money laundering or terrorist financing.

In relation to complex and unusual transactions, the reporting entity shall analyse the background and purpose of such transactions, including the information on the property, the origin of the property and the source of the funds. The reporting entity shall document such analysis results in written form to make them available upon the request by the administrative authority or the supervisory body.

In relation to complex and unusual transactions, the reporting entity shall, in addition to the customer due diligence, take at least the following enhanced measures:

1) collect and verify additional information on the customer's activities and update the identification data on the customer and the beneficial owner of the customer;
2) collect and examine additional information on the nature of the business relation and the data on the purpose of the announced or executed transaction; and
3) collect and examine additional information on the customer's property, the origin of the property and the source of the funds.

When taking the above mentioned measures, account must also be taken of the following criteria:

- the type, business profile and the structure of the customer,
- geographical origin of the customer,
- nature of the business relationship, product or transaction,
- reporting entity's previous experience with the customer,
- status and ownership structure of the customer,
- purpose of concluding the business relationship or executing the business transaction,
- information on the customer obtained from publicly accessible databases, and other data and information,

- other information that may indicate that the transaction is unusual.

The reporting entity shall, by means of an internal document, define the criteria for identifying complex and unusual transactions.

4.1.1.4 Wire transfer

Measures that the reporting entity shall take when executing wire transfers are provided for by the Law.

A reporting entity that is a payment service provider shall establish and verify the customer's identity on the basis of documents, data and information from authentic, independent and objective sources, including a qualified electronic confirmation if it is available, and obtain accurate and complete data on a payer and enter them into a form or message supporting wire transfer, sent or received in any currency that is the subject of the wire transfer. When collecting these data, the payment service provider shall identify the payer by using a personal identification document issued by a competent authority.
If the reporting entity is unable to obtain all data and information regarding the obligations prescribed by the Law, they shall not execute wire transfer of funds.

Specifically, data referred to in paragraph 2 of this item shall support the wire transfer when passing through the payment chain.

A payment service provider, that is an intermediary service provider or payee, shall refuse to execute funds transfer if the data on payer are not complete and/or shall require payer data supplement in the shortest possible period.

The reporting entity shall take enhanced customer due diligence measures during the execution of a wire transfer.

4.1.2 Simplified customer due diligence

A reporting entity shall establish the customer's risk profile and, on a regular basis, monitor the business relationship and control the transactions in accordance with the established risk profile of a particular customer.

A reporting entity may apply the simplified customer due diligence measures only upon establishing that they belong to a category with lower risk of money laundering or terrorist financing, based on risk factors determined by the risk analysis, especially bearing in mind what are the necessary factors allowed for the application of simplified customer due diligence measures.

Simplified customer due diligence measures shall not be undertaken if the customer is a resident of a country that does not apply or insufficiently applies international standards in the area of prevention of money laundering and terrorist financing, based on data of the relevant international organizations. In addition, if there are grounds for suspicion that the customers in relation to which undertaking simplified due diligence measures has been approved are involved in money laundering or terrorist financing, the reporting entity shall

submit a suspicious transaction report to the administrative authority (data referred to in Article 79 of the Law), as well as the aforesaid data relating to the funds for which the reporting entity suspects to be the proceeds of criminal activity or to be related to terrorist financing. In that case, customer's risk profile must be reclassified and designated as a high-risk category.

Apart from specific customer categories (matrix) in relation to which simplified due diligence can be applied, where the reporting entity assesses that, due to the nature of a business relationship, the form and the manner of executing a transaction, customer's business profile, i.e. other circumstances relating to the customer, there is a lower degree of risk of money laundering or terrorist financing, the reporting entity may apply simplified customer due diligence measures envisaged by the Law.

Information collected by the reporting entity by applying simplified due diligence should be sufficient to provide reasonable assurance that the assessment of low risk relating to a business relationship or an occasional transaction was justified, and be sufficient to provide enough information on the nature of a business relationship or an occasional transaction for the purpose of identifying unusual and suspicious transactions.

The reporting entity may adjust the scope, timing or type of some or all measures of customer due diligence in a manner corresponding to the lower degree of risk that has been established.

The reporting entity shall establish a customer's risk profile and, on a regular basis, monitor the business relationship and control the transactions in accordance with the established risk profile of a particular customer.

4.2 Due diligence measures for customers from high-risk third countries

Provisions of the Law stipulate the due diligence measures for a customer from a high-risk third countriy that do not apply or insufficiently apply measures for the prevention and detection of money laundering or terrorist financing, based on which the reporting entity shall, in addition to the standardised customer due diligence measures, take additional enhanced due diligence measures, which include collecting additional information for the purposes of carrying out that due diligence.

In this regard, the reporting entity shall take at least the following enhanced due diligence measures:

1) collect and verify additional information on the customer's activities and update the identification data on the customer and the beneficial owner of the customer;
2) collect and verify additional information on the nature of the business relation and the data on the purpose of the announced or executed transaction; and
3) collect and verify additional information on the customer's property, the origin of the property and the source of the funds.

In addition to the specified standardised due diligence measures and the (abovementioned) special measures stipulated by the Law, the reporting entity should take enhanced measures in relation to the following:

- information on the identity of the customer or the beneficial owner of the customer, or the customer's ownership structure and control, to make sure that the reporting entity understands the risk related to the business relationship. This may include the collection and assessment of information on the reputation of the customer or the beneficial owner of the customer, as well as the assessment of any negative reference to the customer or the beneficial owner of the customer, such as the following:

    a) information on any past or current business activities of the customer or the beneficial owner of the customer, and

    b) examination of any negative media references to the customer's reputation, information on family members or close business associates.

- information on the assumed nature of a business relationship, to determine whether the nature and the purpose of the business relationship are legitimate and to enable the customer to assess the customer's risk profile in a more adequate manner.

This may include collecting the following data and information on:

    a) the number, significance or dynamics of expected transactions in the account, to enable the reporting entity to detect any suspicious deviation;
    b) the reason why the customer requests a specific product or service, especially when it is unclear why the customer's requirements cannot be better accommodated in a different manner or in a different jurisdiction;
    c) the destination of the funds;
    d) the nature of operations of the customer or the beneficial owner of the customer, to enable the customer to better understand the announced nature of the business relationship.

- improvement of the quality of information collected for the purpose of applying the enhanced due diligence measures, in order to verify the identity of the customer or the beneficial owner of the customer including the following:

    a) verification that the customer's property or funds used in the business relationship are not criminal proceeds, and that the sources of property and funds correspond to reporting entity's knowledge of customer and the nature of the business relationship. In specific cases, when the risk relating to the business relationship is particularly high, the verification of the sources of property and funds may be the only tool adequate for risk mitigation. The sources of funds or property may be verified, inter alia, by comparing it to VAT or corporate income tax declarations, copies of audited statements, payslips, public documents or references in the independent media;

- increase in the frequency of verifications to ensure that the reporting entity is still able to manage risks relating to individual business relationships or conclude that the business relationship no longer suits the reporting entity's risk profile, and to more efficiently identify the transactions that require additional analyses including the following:

    a) increased frequency of verification and monitoring of business relationships to determine if the customer's risk profile has changed and if the risk is still manageable;

b) more frequent control of business relationship to ensure that any changes in the customer's risk profile are identified, assessed and, where required, that adequate measures are taken; or

c) more frequent implementation of enhanced analysis of transactions to identify any unusual or unexpected transactions that may raise doubts about the risk of money laundering and terrorist financing. This may include determining the destination of funds or the reason for executing specific transactions.

In addition, the reporting entity shall, prior to establishing a business relationship with a customer from a high-risk third country, obtain a written consent of a senior manager, to ensure that the senior management is aware of the risk that the reporting entity is exposed to and that they may reach an adequate decision on the measures for managing that risk;

The reporting entity shall, after establishing a business relationship, monitor transactions and other business activities performed with them by a customer from a high-risk third country, and take measures adequate to the degree of risk of money laundering and terrorist financing.

The competent administrative authority shall publish on their web site the list of high-risk third countries, based on the data from international organisations.

The reporting entity shall, by means of an internal document, in accordance with Article 7 of the Law, determine the criteria for recognising the customers from high-risk third countries.

4.3 Measures for preventing terrorist financing based on the risk-based approach

Unlike money laundering, terrorist financing has different characteristics, thus the assessment of risk of terrorist financing requires a more extensive set of factors for risk assessment as well as a more complex methods in order to establish the existence of terrorist financing.

Pursuant to Article 3 of the Law, the following shall, in particular, be considered as terrorist financing:

1) providing or collecting or an attempt of providing or collecting funds or property, in any way, directly or indirectly, with the intention to be used or with the knowledge that they may be used, in their entirety or in part:
   - for preparing or committing terrorist act;
   - by terrorists;
   - by terrorist organizations.

2) encouraging or assisting in providing or collecting the funds or property from item 1 of this paragraph.

The nature of the source of terrorist financing may vary depending on the type of terrorist organisation or terrorist, since the funds used for financing the preparation or the execution of a terrorist act may originate from legal as well as illegal sources. When the sources of financing of a terrorist act arise from criminal activities, the risk-based approach applied to money laundering is also applicable to terrorist financing.

Transactions associated with terrorist financing are usually executed in small amounts, thus when applying the money laundering risk-based approach, they are considered to be low-risk transactions, which greatly hinders identification of terrorist financing.

In cases when the sources of terrorist act financing come from legal sources, it is much more difficult to determine that the legally acquired funds are being used for terrorist purposes. In that regard, some activities for the preparation of the terrorist acts may be overt, for example purchase of necessary materials or paying for specific services.
When implementing measures of prevention of terrorist financing, the reporting entities shall apply indicators for detection and recognition of suspicious customers and transactions associated with terrorist financing.

The issue of identifying terrorism financing is a complex one, thus its resolution falls under the competence of different state institutions, whereas the reporting entity's obligation relate, in particular, to reporting suspicious transactions that may be associated with terrorist financing to the competent administrative authority for the prevention of money laundering and terrorist financing. In this regard, it shall be of extreme importance that the reporting entities monitor cash transactions and transactions with countries for which the relevant international organisations or authorities have determined to be financing or assisting terrorist activities.

5. MANAGEMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISK THE REPORTING ENTITIES ARE EXPOSED TO

Risk of money laundering and terrorist financing means the risk that a customer will use the financial system for money laundering or terrorist financing, or that a business relationship, a transaction or a product will indirectly or directly be used for money laundering or terrorist financing (Article 5 item 13 of the Law)

In relation to the obligation of managing the risk of money laundering and terrorist financing the reporting entities are exposed to, the reporting entities shall develop effective policies, controls and procedures that are proportional to the scope of its activities, and the business activity, size and type of the customer it deals with, as well as the type of product and services they are offering and implement them in an efficient manner. When establishing the system for the prevention of money laundering and terrorist financing, the reporting entities shall, by implementing the abovementioned internal documents, determine the organisational structuring, procedures (functional connection) of organizational parts of the system for the prevention of money laundering and terrorist financing, as well as the implementation of necessary measures and controls with a view to achieving high-quality risk management and risk minimisation. The reporting entity shall take measures, in particular those referring to the application of adequate degree of verification and monitoring of customers, with a view to ensuring the efficiency of the risk management system. The above mentioned system, which refers to the risk management through the use of policies, controls and procedures is set out in the Law (Article 7b).

With a view to achieving adequate management of the risk of money laundering and terrorist financing, the reporting entity shall, inter alia, reduce the exposure to risk stemming from the application of new technologies that might allow anonymity (electronic or internet banking,

electronic money, etc.), i.e. the policies and procedures of the reporting entity shall define, in particular, the following:

- identification of a customer that is a user of electronic banking services;
- authenticity of the signed electronic document;
- reliable measures against forging documents and document signatures;
- systems ensuring and enabling safe electronic banking;
- other conditions in line with positive regulations governing the area of money laundering and terrorist financing.

To ensure accurate identification of a customer that is a user of electronic banking services, the reporting entity may use various methods for establishing and verifying the customer's identity, including PINs, passwords, smart cards, biometrics, and qualified electronic certificates.

5.1 Performing the activities of detecting and preventing money laundering and terrorist financing

The reporting entity shall, within 60 days from the date of their establishment, designate a compliance officer and at least one of their deputy for the activities of detecting and preventing money laundering and terrorist financing and submit documentation on their appointment to the administrative authority.

The reporting entity shall fully implement the provisions of the Law prescribing the following:

- performing the activities of detecting and preventing money laundering and terrorist financing;
- requirements for a compliance officer;
- compliance officer's obligations;
- working conditions for a compliance officer;
- professional training and development; and
- internal control and audit.

Since the compliance officer and their deputy are responsible for establishing and functioning of the system for the prevention of money laundering and terrorist financing, the implementation of all provisions of the Law and enabling regulation shall be conditioned by meeting of this obligation. The abovementioned persons must be professionally trained for performing the activities of preventing and detecting money laundering and terrorist financing and have professional competencies for reporting entity's operations in the areas where the risk of money laundering or terrorist financing exists.

Taking the aforesaid into consideration, the Law provides that the compliance officer shall be directly accountable to the management or other managing or other similar reporting entity's body, and be functionally and organizationally separated from other organizational parts of the reporting entity. The reporting entity shall provide for the compliance officer and their deputy appropriate spatial and technical working conditions ensuring an appropriate degree of protecting confidential data and information they deal with on the basis of this Law;

These activities may be performed solely by a person that is employed with only one reporting entity for carrying out activities and tasks that are in accordance with the systematisation act of the reporting entity or employment contract, organised in the manner ensuring a fast, high-quality and timely performance of tasks defined by this Law and regulations passed on the basis of this Law. Another necessary requirement shall be that this person has not been finally convicted of a criminal act for which an imprisonment longer than six months is provided, and which makes them unfit for performing activities of prevention of money laundering and terrorist financing and against whom there is no criminal proceedings for criminal acts prosecuted ex officio.

5.2 Reporting to the administrative authority on the transactions

5.2.1 Obligation of and deadlines for reporting to the administrative authority on the cash transactions

A reporting entity shall report to the administrative authority on any cash transaction in the amount of at least 15,000 euros, without delay, and not later than three working days following the day of execution of the transaction, in a prescribed form, in the manner stipulated by the Law.

5.2.2 Obligation of and deadlines for reporting to the administrative authority on a suspicious transaction, customer and business relationship

Reporting entities shall, without delay and in a prescribed manner, report to the competent administrative authority on any suspicious transaction prior to its execution, i.e. submit data and information and report to the competent administrative authority on the reasons for suspicion of money laundering and terrorist financing or some other criminal activity, i.e. on the reasons that clearly and unambiguously indicate that the transaction, customer or business relationship in question is suspicious and specify the indicators based on which it was assessed that the transaction, customer or a business relationship in question is a suspicious one.

Where, due to the nature of the transaction or other justified reasons, the reporting entity is unable to report, in a prescribed manner, to the competent administrative authority of a suspicious transaction prior to its execution the reporting entity shall report to the competent administrative authority subsequently, but not later than the next working day. In the report on a suspicious transaction delivered to the administrative authority, the data and information that point to the suspicion of money laundering and terrorist financing or some other criminal activity must be substantiated by documentation and reasons for which they have been described as such. If the reporting entity shall submit the data and information on a suspicious transaction subsequent to its execution, they shall submit an explanation and specify the objective reasons that prevented them from reporting to the competent administrative authority within a prescribed deadline. The reporting entity may communicate such information via a telephone, but shall also deliver those data in written form, not later than the next working day following the day of communication.

In case of a transaction, customer or business relationship for which there are grounds for suspicion of money laundering or terrorist financing, the reporting entity shall refuse to execute the transaction, or shall inform the competent administration authority of the reasons for suspicion prior to its execution, to enable the competent administrative authority to

prevent the execution of such transaction, i.e. stop it in accordance with the provisions of the Law.

When establishing grounds for suspicion of money laundering or terrorist financing or some other criminal activity, reporting entities shall use the list of indicators for identifying suspicious customers and transactions. Identification of a suspicious transaction or a customer or a business relationship shall be based on the criteria specified in the list of indicators for identifying suspicious customers and transactions. Reporting entities shall update and adjust the list of indicators in accordance to the known trends and typologies of money laundering or the circumstances arising from the business activities of the reporting entity itself. The fact that a transaction or a customer meets one of the indicators shall not necessarily mean that the transaction or the customer in question is suspicious, but that fact shall point to the need for additional analyses stipulated by the Law. The reporting entity shall take a broader view, in line with the “know-your-customer” policy, to adequately implement measures of monitoring that customer’s business relationship that include monitoring customer’s transactions in order to establish that those transactions have a clear purpose and intended nature, that the source of the funds has been verified and does not point to suspicion of money laundering and terrorist financing or some other criminal activity, that there is clear knowledge on the customer and their business activities, etc.

An employee of the reporting entity who is in direct contact with the customer, or who, in performing tasks assigned to them, suspects that in relation to the customer there is a risk of money laundering or terrorist financing or if they know or suspect that the funds are the proceeds of criminal activity, shall make an internal report and deliver it to the designated compliance officer in charge of prevention of money laundering and terrorist financing within the timeframe and in the manner prescribed by an internal document of that reporting entity. The report shall contain sufficient data and information on the customer and the transaction to enable the compliance officer to assess whether the customer, i.e. the transaction point to the suspicion of money laundering and terrorist financing.

6. PROFESSIONAL TRAINING AND EDUCATION OF EMPLOYEES AT THE REPORTING ENTITY

An adequate and timely professional training and education of employees performing the activities of detecting and preventing money laundering and terrorist financing represents a significant element of the efficiency of the system for the prevention of money laundering and terrorist financing.

Professional training and education of employees relating to prevention of money laundering and terrorist financing shall include profound knowledge of regulatory requests as well as internal policies and procedures adopted by the reporting entity with a view to ensuring successful risk management in this area.

All employees whose tasks in any way relate to the implementation of measures for prevention of money laundering and terrorist financing must be included in the programme for professional training and education.

Education must be tailored to suit specific requirements of the employees in individual business lines, i.e. the particular features of the activities they perform.

In that regard, techniques for the detection and prevention of money laundering must be presented to the persons employed at the counters as well as other sectors' employees included in the programme for detection and prevention of money laundering and terrorist financing.

Special attention must be paid to new employees, who are obliged to become familiar with the basic measures and actions taken by reporting entity in terms of detection and prevention of money laundering and terrorist financing.

In addition, education of a compliance officer and their deputies is also extremely important in the aim of their training for detection of new forms, techniques, and trends relating to money laundering and terrorist financing. This includes their knowledge and awareness of legal and regulatory changes in order to align the internal documents with the new regulations in a timely manner.

The reporting entity's management must be aware of the risk to which the reporting entity would be exposed as a result of non-compliance with the regulations in the area of prevention of money laundering and terrorist financing, as well as inadequate training of employees tasked with conducting measures of detection and prevention of money laundering and terrorist financing.

The reporting entity shall keep adequate records on completed education relating, in particular, to persons included in the education, dates and venues of the seminars, courses, workshops, etc.

Professional training and education of employees of the reporting entity related to prevention of money laundering and terrorist financing, is aimed at raising the employee's awareness of the significance of timely taken measures for the prevention of money laundering and terrorist financing.

The reporting entity should record and document their risk assessments of business relationships and occasional transactions as well as any changes made to risk assessments within their reviews and controls. This would ensure the possibility to present documented records on the classification of all customers in terms of risk of money laundering and terrorist financing as well as related implemented risk management measures.

7. MANDATORY INTERNAL DOCUMENTS AND PROCEDURES FOR REGULATING IN MORE DETAIL OPERATIONS OF A REPORTING ENTITY RELATING TO THE AREA OF PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

The reporting entity shall establish policies, controls and procedures and take actions aimed at mitigating the risk of money laundering and terrorist financing, i.e.:

- draft an internal document on the risk analysis for the purpose of prevention of money laundering and terrorist financing on the basis of these guidelines;
- perform the assessment of impact on the exposure to the risk of money laundering and terrorist financing when making organisational changes, introducing new products, new practices, including new channels of distribution, introducing new technologies for new or existing products or services;
- define procedures for detection of suspicious customers and transactions;

- define procedures for submitting data to the administrative authority in line with the Law;
- define procedures for protection and keeping of data and record keeping;
- define procedures of internal controls in the area of detection and prevention of money laundering and terrorist financing;
- establish mechanisms of security checks of employees in accordance with the law that regulates data confidentiality;
- develop an internal document which establishes the procedures for conducting customer due diligence measures as well check whether any person acting on behalf of the customer has the right to represent or is authorised by the customer, and establish and verify the identity of any person who acts on behalf of the customer;
- develop an internal document which establishes risk-based procedures that shall be applied when identifying a customer or beneficial owner of a customer who is a politically exposed person, in line with these guidelines;

- develop an internal document which establishes the procedures on acceptance of the identification of the customer and the beneficial owner of the customer through a third person;
- develop an internal document which establishes the criteria for recognising complex and unusual transactions;
- develop an internal document which establishes the criteria for recognising customers and transactions from high-risk third countries;
- develop an internal document which defines procedures for preventing the use of new technologies for money laundering or terrorist financing;
- develop a programme of professional training and education of employees in the area of detection and prevention of money laundering and terrorist financing;
- define the procedure for designating a compliance officer and their deputy, as well as provide working conditions for them in line with the Law;
- determine cases when the enhanced customer due diligence measures shall be applied in line with the Law.

Where the reporting entity is a bank or other credit institution, they shall, in addition to the aforesaid, in their internal documents define the following:

- taking customer due diligence measures in relation to any occasional wire transfer executed by a customer that is not in a business relationship with the bank;
- the measures and activities of monitoring business relationship and the control of transactions in accordance to the risk to which a bank is exposed when performing specific business activity or when dealing with a customer;
- procedure on entering into correspondent relationship with a bank or other credit institution.

An overview of internal documents and procedures to be developed by the reporting entity pursuant to the Law is presented in the table below:

	Internal document / Obligation of the Compliance Officer	Legal basis
1.	Know your customer procedure (KYC)	**Measures for establishing and verifying the identity of the customer and monitoring of business relationships and the control of the transactions of the customer** **Article 8** A reporting entity shall, by **internal documents,** define the procedures for the implementation of measures referred to in paragraphs 1, 2 and 5 of this Article. **Performing the affairs of detecting and preventing money laundering and terrorist financing** **Article 43** (1) A reporting entity shall establish and apply appropriate rules regarding the procedures with a customer and enable reporting, keeping of data, internal control, risk assessment, risk management and communication, with a view to prevent money laundering and terrorist financing.
2.	Risk analysis for the purpose of prevention of money laundering and terrorist financing	**Measures of verifying identity and monitoring of business of politically exposed persons** **Article 33** A reporting entity shall, in accordance with the guidelines of a competent authority from Article 94 of this Law make an internal document containing the procedures that are based on risk analysis and apply them when identifying the customer or beneficial owner of a customer who is a politically exposed person. **Third party obligations** **Article 25** (2) The reporting entity is obliged to develop an **internal document** which determines the procedures on acceptance of the identification of the customer and the beneficial owner of the customer through a third person. **Measures for the establishing and verifying identity of the customer and monitoring of business relationships and the control of the transactions of a customer from high-risk third countries** **Article 35a** A reporting entity shall, by an internal document, in accordance with Article 7 of this Law, determine the criteria for recognising the customers and transactions from high-risk third countries.
3.	Programme for preventing money laundering and terrorist financing (containing procedures aimed at employees for the purpose of detection and prevention of ML and TF)	**Internal control and revision** **Article** 48 (1) A reporting entity shall adopt a program for conducting the measures for preventing money laundering and terrorist financing and ensure its implementation. **Complex and unusual transactions**

		Article 35 A reporting entity shall, by an **internal document**, in accordance with Article 7 of this Law, determine the criteria for recognising complex and unusual transactions. **New and developing technologies** **Article 7c** A reporting entity shall adopt an **internal document** in accordance with Article 7 Paragraph 3 of this Law with a view to preventing the new technologies to be used for money laundering or terrorist financing.
4.	Developing policies and procedures for detection of suspicious customers and transactions	*Usually a part of the AMLFT Programme (3)*
5.	The list of indicators for the identification of suspicious customers and transactions (developed by the Bank)	**1. Measures and actions undertaken by reporting entities** **Types of measures and actions** **Article 6** Reporting entities shall, when conducting their activities, undertake measures and actions in accordance with this Law, in particular the following: - develop and regularly update the list of indicators for the identification of suspicious customers and transactions;
6.	Policy and procedures for keeping data, information and documentation the Bank obtains in the process of the implementation of the Law.	**Keeping data** **Article 91** (1) Reporting entity shall keep records obtained in accordance with this Law, related documentation, data on identification number of each customer's account, data and documentation on wire transfers, documentation on business correspondence and reports at least ten years after the termination of business relationship, executed transaction, entrance of the customer into casino and facilities where other special games of chance are organised or access to the safe deposit box, unless a specific law prescribes longer period for data keeping.
7.	Program of professional training and improvement	**Compliance officer's obligations** **Article 45** 8) prepare programs of professional training and improvement of the employees at reporting entities in the area of detecting and preventing money laundering and terrorist financing
8.	Policy and procedures for keeping data, information and documentation the Bank obtains in the process of the	**VIII. RECORDS, PROTECTING AND KEEPING DATA** **1. Keeping records and its contents** **Records kept by a reporting entity**

	implementation of the Law.	**Article 78** (1) Reporting entity shall keep: 1) data records on customers, business relationships, accounts and transactions (carried out in the country and with foreign countries) from Article 9 of this Law; 2) data records from Article 41 of this Law; 3) data records from Article 35 of this Law; 4) records of orders on temporary suspension of transactions referred to in Article 61 of this Law; 5) records of requests for the ongoing monitoring of customer's financial status referred to in Article 63 of this Law. (2) The reporting entity shall keep records referred to in Paragraph 1 of this Article in a manner that will ensure the reconstruction of individual transactions (including the amounts and currency) that could be used as evidence in the process of detecting customer's criminal activities.
9.	Internal document containing the criteria for recognising complex and unusual transactions	**Complex and unusual transactions** **Article 35** (5) A reporting entity shall, by an internal document, in accordance with Article 7 of this Law, determine the criteria for recognising complex and unusual transactions.
10.	Assessment of impact of introducing a new product, practice, distribution channel, new technology and organisational changes on the risk exposure	**Article 7** (5) A reporting entity is obliged, during all important changes in the business processes, such as: introduction of new products, new practice, including new distribution channels, the introduction of new technologies for new and existing products, services or organizational changes, to perform appropriate assessment of the impact of these changes on the exposure to the risk of money laundering and terrorist financing. (6) A reporting entity is obliged to implement the assessment of the risk from Paragraph 5 of this Article before the introduction of changes in the business processes and, in accordance with the results of the assessment, to adopt measures to reduce the risk of money laundering and terrorist financing.
11.	Reporting to the Administration for Prevention of Money Laundering and Terrorist Financing on any cash transaction in the amount of or exceeding 15,000 euros	**6. Reporting obligation and applying measures in business units and business organizations whose majority owners are foreign countries** **Reporting obligation** **Article 41** (1) A reporting entity shall provide to the administrative authority a report that contains accurate and complete data from Article 79 Items 1 to 4 and 8-11 of this Law on any transaction executed in cash in the amount of at least €15,000, immediately after without delay, and not later than three working days since the day of execution of the

		transaction.
12.	Reports on suspicious transactions	**Article 41** (2) A reporting entity shall refrain from carrying out a transaction which he/she knows or suspect to be related to proceeds of criminal activity or to terrorist financing and provide , without delay, to the administrative authority the data from Article 79 of this Law.

III. GUIDELINES APPLIED TO INDIVIDUAL REPORTING ENTITIES

Individual reporting entities shall, in addition to applying guidelines provided in Part II of these guidelines, apply the provisions of this part, which are relevant to them, in order to be able to more accurately recognise risks pointing to suspicious transactions, customers and business relations, and to manage such risks in a way that will make carrying out of activities that might be described as money laundering or terrorist financing impossible.

1. BANKS, CREDIT INSTITUTIONS AND FOREIGN BANK BRANCHES

Banks, credit institutions and foreign bank branches shall more closely recognise risks pointing to suspicious transactions, customers and business relations, and to manage such risks in a way that will make carrying out of activities that might be described as money laundering or terrorist financing impossible.

Institutions specified in this item shall undertake measures for detection and prevention of money laundering and terrorist financing, before, during and after the conduct of any business of receiving, investing, exchanging, keeping or other form of disposing of money or other property, or any transactions for which there are reasons to suspect of money laundering or terrorist financing.

Risk analysis of the aforesaid institutions aims at recognizing and identifying the exposures to money laundering and terrorist financing risk as well as business segments that should be prioritized in order to ensure efficient money laundering and terrorist financing risk management. Customers of these institutions shall be classified in one of the money laundering and terrorist financing risk categories.

- ✓ A (low risk)
- ✓ B (medium risk) and
- ✓ C (high risk)

1.1 Customer risk

Customer means a legal person, natural person, entrepreneur, and other person, or an entity equal to it, carrying out transactions or establishing business relationship with a bank, credit institution or a branch of a foreign bank.

Banks, credit institutions and branches of foreign banks shall perform money laundering and terrorist financing risk analysis paying special attention to:

1) origin of the customer’s funds;
2) purpose and presumed nature of the customer’s business relationship;
3) profession or the activity of the customer;
4) country or geographic area of the customer;
5) category of the product or service that the customer is using;
6) customer’s political exposure;
7) information from the general public media;
8) information from public data bases and other data and information;

9) established correspondent relationship with the bank or other credit institution depending on their country or geographical area, etc.

1.1.1 Customer nature

The following circumstances can affect a lower ML/TF risk:

- customer is a renowned legal person, natural person, entrepreneur and other person or an entity equal to it;
- customer structure shows presence of customers, beneficial owners or authorised persons, residents and non-residents, from the countries and geographical areas that comply with internationally accepted standards in the area of prevention of money laundering and terrorist financing, the EU Members and customers that implement simplified customer due diligence;
- origin of customer's funds may be easily proved and stems from activities that do not point to the risk of money laundering and terrorist financing;
- customer creditworthiness in the part of the discharge of undertaken obligations;
- customers having a steady source of income prevail in the customer structure.

The following circumstances can affect a higher ML/TF risk:

- customer or a beneficial owner of a customer performs an activity that bears high-risk of money laundering and terrorist financing (such as construction, sale of real estate, manufacture of and trade in arms, provision of consulting services etc.);
- customer or a beneficial owner of a customer performs an activity involving large circulation of cash (such as hotels, restaurants, game of chance organisers, goods ad passenger transporters, etc.);
- customer is from a country that does not comply with prevention of money laundering and terrorist financing standards;
- customer structure shows presence of high-risk customers, beneficial owners or authorised persons that are politically exposed persons and foreign politically exposed persons, non-resident legal and natural persons for which there are grounds for suspicion of money laundering and terrorist financing, etc.
- customer's business activities show deviation from the usual volume and type of business;
- customer creditworthiness changes under extraordinary circumstances;
- customer structure is prevailed by customers that do not have a steady source of income but have ownership over property and dispose of funds;
- presence of customers from the non-EU countries, countries under sanctions or embargo and countries that do not classify as equivalent third countries;
- presence of customers that, according to FATF data classify as customers from non-cooperative countries or territories or that are off-shore companies on the list of high-risk countries, i.e. non-cooperative countries or territories or that do not meet key international standards relating to prevention of money laundering and terrorist financing;
- non-government and non-profit organisations;
- non-resident legal and natural persons with whom specific deviations pointing to unusual business operations have been detected;

- customer structure shows presence of customers from countries for which it was published by the media that they provide funding or support to terrorist activities and which have established terrorist organisations acting within their territory, etc.

1.1.2 Customer behaviour

The following circumstances can affect a lower ML/TF risk:

- when establishing a business relationship and when executing a transaction, a customer provides clear and unambiguous data that are assessed as sufficient grounds for lower risk;
- customer executes economically justified transfers, payments, pay-outs supported by adequate documentation within which there are no elements indicating their unusual character or suspicion of money laundering and terrorist financing;
- customer meets their obligations (e.g. arising from loan granted) in line with the planned dynamics and in line with other information on the customer.

The following circumstances can affect a higher ML/TF risk:

- customer performs business activity or a transaction under unusual circumstances;
- when meeting their obligations (e.g. arising from a loan granted) a customer uses unusual means of payment or means that enable anonymity, payment from different bank accounts without adequate explanation;
- a customer provides unclear explanations in regard to the execution of a transaction supported by inadequate documentation for its execution;
- documentation supporting the execution of transactions shows elements indicating their unusual character or grounds for suspicion of money laundering and terrorist financing;
- customer acts on behalf of another person for customer's own account without obvious economic justification;
- the distance between a customer and the organisational unit where a business relation is being established or a transaction executed is significant and unexpected;
- customer establishes a business relation without economic justification with more than one bank;
- customer meets their obligations (e.g. arising from a loan granted) via their accounts with more than one bank or meets their obligations before they are due in part or in full;
- customer uses unusual means of payment or means that enable anonymity, payment from different bank accounts without adequate explanation.

1.1.3 Geographical risk

The following circumstances can affect a lower ML/TF risk:

- customer's funds or property have been obtained in a country known to be in compliance with international prevention of money laundering and terrorist financing standards;

- customer is from a EU country or a country that has established an effective system for prevention of money laundering and terrorist financing, which is not under sanctions, embargo or any similar measure;
- customer is from a country which possesses information from credible and reliable sources on the quality of surveillance regarding the prevention of money laundering and terrorist financing including information on the quality and efficiency of the implementation of regulation and performance of the surveillance thereof;
- customer doing business with persons that are situated in the areas known for complying with the standards of prevention of money laundering and terrorist financing.

The following circumstances can affect a higher ML/TF risk:

- customer's property acquired in a country known to have terrorist organisations acting on its territory or to have shown shortcomings in combating money laundering and terrorist financing;
- customer is from a country that does not have an adequate and efficient system for combating money laundering and terrorist financing;
- customer is a trust from a country that does not comply with the international tax transparency standards;
- customer is from a country that does not possess information from credible and reliable sources on the quality of the surveillance in the area of prevention of money laundering and terrorist financing including the information on the quality and efficiency of implementation of regulation and performance of the surveillance thereof;
- customer is from a non-EU country or a country which is under sanctions, embargo or a similar measure;
- customer for which there are information, from credible and reliable sources, on the number of predicate offences to money laundering (e.g. by means of corruption, fraud, organised crime, tax evasion, etc.);
- customer maintaining business relationships with customers from off-shore destinations.

1.1.4 Product/service and transaction risk

The following circumstances can affect a lower ML/TF risk:

- transactions relating to (e.g. payment and pay-out of wages, social benefits, participations in commissions, working groups and bodies, etc.);
- transactions that do not deviate from the customer's usual business activities;
- transactions executed supported by adequate documentation and economic justification;
  and which have the source of funds fully supported by adequate evidence;
- the structure of funds employed in the execution of transactions is prevailed by non-cash funds;
- customer structure is prevailed by customers with guarantees and steady source of income.

The following circumstances can affect a higher ML/TF risk:

- use of new or developing technologies that enable anonymity in case suspicious activities relating to the execution of transaction were detected through them;

- provision of services to a customer via private banking;
- mortgage loan secured against the value of assets in other jurisdiction, particularly a country where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the ownership structure is hard to prove;
- transactions without obvious economic justification;
- transactions relating to founders' borrowings to companies of which they are the beneficial owners;
- transactions indicating payment or collection based on consulting services;
- transactions that are not supported by adequate documentation;
- transactions in which the source of funds cannot be clearly proved;
- transactions with which disproportionately large amounts are deposited as security for e.g. being granted a loan;
- transactions relating to payment of goods and services to customers originating in off-shore destinations and the documentation clearly shows that the goods originates in the neighbouring countries;
- transactions based on payment of goods and services in countries that do not usually produce the type of goods being paid for or provide that type of services;
- transactions intended for persons against which the UN or EU measures are in force, as well as transactions performed by the customer on behalf and for the account of such persons;
- payment of funds from a customer's account, i.e. transfer of funds to a customer's account that is different from the account specified by the customer upon identification, i.e. through which they usually conduct or have conducted business (in particular if a cross-border transaction is in question);
- transactions intended for non-profit organisations seated in an off-shore country, i.e. a tax haven country or a non-EU country;
- structure of funds employed in the execution of transactions is prevailed by cash.

For the purposes of risk analysis in relation to suspicious transactions, customers and business relations during the provision of safe deposit boxes, issuance of guarantees and other assurances and exchange services, banks shall apply accordingly the guidelines established for the analysis of risks during the performance of other business activities.

1.2 Correspondent relationships with banks or other credit institutions from other countries

A reporting entity shall conduct enhanced customer due diligence on entering into correspondent relationship with a bank or other credit institution, with registered office outside the EU or in a country that is not on the list of countries applying international standards in the area of money laundering and terrorist financing that are on the level of EU standards or higher, or with those that apply the aforesaid standards when it is assessed that a higher degree of risk of money laundering and terrorist financing is present.

A reporting entity must not establish, or continue a correspondent relationship with a bank that operates or could operate as a shell bank or with other credit institution known for allowing shell banks to use its accounts.

Correspondent relationship is defined by the Law as a relationship with established high-risk factors that, due to its structure, i.e. the type of service it envisages, includes the obligation of performing enhanced customer due diligence.
In that regard, it should be especially pointed out that, when executing transactions for the customers of banks and other credit institutions from other countries, the correspondent bank is unable to perform direct establishing and verification of the identity of a customer, which means that, in line with their internal documents and procedures, the correspondent bank is unable to determine their risk level that is necessary for establishing and undertaking prescribed actions ad measures. In that part it must rely on the executed application of required actions and measures by the bank with which it is in a correspondent relationship, i.e. accept the execution of transactions with insufficient established data and information.
The correspondent bank shall establish a system that will ensure that the message supporting the transaction contains complete and accurate data on the instructing party and the payment beneficiary. This is of particular significance in cases where the customers of banks or other credit institutions are non-residents in those other countries. The reporting entity shall as a correspondent make sure that they are able to monitor transactions and undertake transaction verification measures and other related measures and actions envisaged in the Law.

The abovementioned imposes an obligation to the bank or other credit institution that when concluding a correspondent relationship it shall perform a verification of the bank's system and the system of bank's jurisdiction and undertake other prescribed enhanced customer due diligence actions and measures.

Risk factors that the correspondent bank shall consider when assessing risk shall include general characteristics of a bank or a credit institution from another country, data on the services and products which are the object of the business relationship as well as the data on the system in which the bank or the credit institution from another country operates.

1.2.1 General features of a bank or a credit institution from another country and information about them primarily refer to the following:

- banking licence date, name and head office of the licencing authority;
– information about the owners (especially beneficial owners) as well as members of the management body of the bank or credit institution from another country, with the identification of information that affect risks related to these persons (whether they are politically exposed persons, i.e. whether there are some other available information that could affect risk assessment);
– main business activities of the bank or credit institution from another country, information about the market, including a description of the market where the basic bank or credit institution services are offered;
– policies and procedures adopted with a view to detecting and preventing money laundering and terrorism financing, including a description of procedures and/or actions and customer due diligence that the bank or credit institution from another country apply, as well as the procedure of analysis and application of indicators, the recognition of suspicious transactions, the collection of necessary documentation from customers, reporting to the competent authorities;
- a description of the system of internal controls and other procedures that a bank and/or credit institution has set up with regard to preventing and detecting money laundering and terrorism financing;

- a written statement issued by the bank or credit institution from another country in which it has its head office and/or in which it is registered indicating that, in accordance with the laws of that country, it is obliged to apply adequate regulations in the area of detecting and preventing money laundering and terrorism financing, including the information whether it is subject to any ML/TF investigation or measures imposed by competent authorities;
- a written statement that the bank or another credit institution is not doing business as a shell bank;
- a written statement that the bank or another credit institution has no established business relationship and/or does not establish business relationships nor deals with shell banks;
- a description of the record keeping.

1.2.2 product/service risk, in particular:

– the purpose of services offered to banks or other credit institutions from a foreign country;
- expected services in accordance with the customer structure;
– information whether the offered banking services will be used by third parties;

1.2.3 system in which a bank or credit institution operates, in particular:

– the country in which it operates, as well as the country of its parent undertaking, if different from the country in which the bank or another credit institution from a foreign country operates,
- a description of the AML/CFT system in the country (for the purpose of establishing the level of jurisdiction risk, i.e. whether they originate from a country associated with a higher ML/TF risk), the information whether the country is on any of the relevant lists;
- a description of the AML/CFT supervision in the country (with the information about the supervisory authority) and any records of whether the bank or credit institution has been subject to misdemeanour proceedings, as well as whether any irregularities have been identified or any sanctions imposed during those proceedings, with the information on the identified irregularities, types of sanction(s), and time of sanctioning;

A reporting entity shall obtain the information listed in the previous sections (points 1.2.1, 1.2.2, and 1.2.3) by accessing official documents and business documents that are submitted by the bank or credit institution from another country and/or public or other available records (depending on the type of requested data).

A reporting entity shall establish a quality AML/CFT system that will incorporate developed policies and procedures capable of recognizing and preventing any activity that is not in line with the purpose for which an account has been opened and services announced by a bank or another credit institution. To that end, in addition to the listed mandatory factors, a reporting entity may develop its own procedures that will ensure additional quality in assessing the risk of establishing a business relationship. e.g. an overview of the structure of customers of those institutions regarding the type of activity and their jurisdictions, as well as regarding the share of residents and non-residents, and an overview of customers per activity.

On the basis of the previously listed elements/factors, the correspondent bank/reporting entity shall pass a decision on the level of risk, that is, its exposure and acceptability of establishing a business relationship with the bank or credit institution from another country. Appropriate actions and measures of monitoring and verification of their operations are taken

in accordance with the established initial risk on the basis of the factors indicated above as well as factors established by the reporting entity and which affect the risk assessment of correspondent relationships.

In this regard, certain factors of risk level reduction can be established if a bank or credit institution from another country:

- operates in an EU Member State in line with EU regulations;
- is on the list of countries applying AML/CFT international standards equivalent to the EU standards or higher;
- is not based in a country with a higher ML/TF risk.

A reporting entity is obliged to obtain a written approval from a senior manager before establishing a correspondent business relationship.

2. FINANCIAL INSTITUTIONS PROVIDING FACTORING AND PURCHASE OF RECEIVABLES SERVICES

In addition to the general part of these Guidelines, financial institutions offering factoring and purchase of receivables (claims) services are obliged to apply provisions under this point 2 in order to be able to recognize risks pointing to suspicious transactions, clients, and business relationships and to manage those risks in the manner so as to prevent any activities that could be characterized as money laundering and terrorism financing.

Observed from the economic perspective, factoring is a legal transaction where a person that carries out factoring operations (factor) purchases the object of factoring resulting from a legal transaction of sale of goods or delivery of service concluded between the creditor of the object of factoring and debtor of the object of factoring.
Financial institutions dealing with the buying and collection of receivables, that is, the relieving of a financial institution from bad credit investments, influence the provision of liquidity and/or better competitive advantage in the sale of products and services because they can offer longer repayment periods to the relevant debtors.

Risk analysis of the aforesaid institutions aims at recognizing and identifying the exposures to ML/TF risk as well as business segments that should be prioritized in order to ensure efficient ML/TF risk management. Clients of these institutions shall be classified in one of the ML/FT risk categories:

- ✓ A (low risk)
- ✓ B (medium risk) and
- ✓ C (high risk)

2.1 Customer risk

Customer is a person to whom a factoring institution or an institution dealing with the purchase of receivables offers the service of collection of receivables and/or factoring financing.

2.1.1 Customer nature

The following circumstances can affect a lower ML/TF risk:

- creditor and debtor are renowned legal persons, natural persons, entrepreneurs and other persons and/or entities equal to them;
- if a financial institution establishes a business relationship with a creditor and a debtor undertakes adequate actions and measures related to the assessment of ML/TF risk for those persons;
- if the structure of creditors and debtors includes customers, beneficial owners or authorised persons, residents and non-residents coming from countries and geographical areas which observe internationally accepted AML/CFT standards, EU Members States, and customers subject to simplified customer due diligence;
- if the origin of assets of a creditor and debtor is easily provable and stems from activities that do not point to ML/TF risk;
- if a debtor`s financial position is stable when it comes to settling liabilities;
- if debtors having a steady source of income prevail in the customer structure;
- if a financial institution purchases receivables of their customers from resident debtors (legal and natural persons).

The following circumstances can affect a higher ML/TF risk:

- creditor and debtor are legal persons, natural persons, entrepreneurs and other persons and/or entities equal to them that are not know for good business;
- if the structure of creditors and debtors includes customers, beneficial owners or authorised persons, residents and non-residents coming from countries and geographical areas which do not observe internationally accepted AML/CFT standards, which are non-EU Members States, and customers that cannot be subject to simplified customer due diligence;
- if the origin of assets of a creditor and debtor is difficult to prove and stems from activities that do point to ML/TF risk;
- if a debtor`s financial position is not adequate when it comes to settling liabilities;
- if the customer structure is dominated by debtors having no steady source of income;
- if a financial institution purchases receivables of their customers from non-resident debtors (legal and natural persons).

2.1.2 Customer behaviour

The following circumstances can affect a lower ML/TF risk:

- if a debtor regularly settles its invoiced liabilities towards a financial institution;
- if clear and unambiguous data is obtained during the establishment of a business relationship and the execution of transactions between a factor, a creditor and a debtor;
- there are transfers, payments and disbursement of funds which are economically justifiable and supported with proper documents which contain no elements pointing to unusual and/or suspicious transactions;
- if parties to a factoring contract (factor, creditor and debtor) settle their obligations in line with planned schedule and other customer information;

- if the execution of contracted factoring transactions is carried out via means of remote communication which allow anonymity.

The following circumstances can affect a higher ML/TF risk:

- if a debtor fails to settle its invoiced liabilities towards a financial institution;
- if unclear and ambiguous data is obtained during the establishment of a business relationship and the execution of transactions between a factor, a creditor and a debtor;
- there are transfers, payments and disbursement of funds which are not economically justifiable and which are not supported with proper documents containing elements pointing to unusual and/or suspicious transactions;
- if parties to a factoring contract (factor, creditor and debtor) do not settle their obligations in line with planned schedule;
- if the execution of contracted factoring transactions is carried out via means of remote communication during which unusual or suspicious activities have been detected;
- if a potential ML/TF risk is detected on the debtor`s side in factoring (the purchase of receivables of a creditor`s clients, thus making the creditor`s debtors become debtors of the financial institution);
- if a financial institution pays the value of receivables and fails to adequately analyse business of both the seller and the buyer;
- if a financial institution dealing with factoring and which purchases receivables from a creditor selling goods fails to analyse the type of goods traded by the creditor;
- if a financial institution fails to perform the credit rating of both the creditor and the debtor;
- if a financial institution dealing with factoring finance and purchase of receivables or a client from a tri-party contract (factor, creditor and debtor) makes non-contracted amendments to the contract and request a drafting of contract annex(es);
- if a debtor makes payments without supporting documents and/or documented receivable (e.g. the relevant invoice).

2.2 Product/service and transaction risk

The following circumstances can affect a lower ML/TF risk:

- if there is a financing involving factoring finance of and purchase of receivables from persons (natural or legal) dealing with export of domestic products and services;
- if there is a financing of persons (natural or legal) dealing with trade, agriculture, tourism, hospitality, services, food production, renewable energy sources, and the like;
- if factoring finance leads to mitigating short-term liquidity problems related to the protection of persons (natural or legal) with a view to collecting receivables;
- if there are multiple guarantees provided in factoring finance transactions;
- if non-cash prevails in total deployed assets;
- if cash is immediately and efficiently available in a very short period of time following delivery and invoicing a client;
- if there is factoring finance that positively affects sale increase;
- if there is factoring finance that positively affects easier planning of cash flow;
- if there is a possibility of receiving funds, depending on the creditworthiness.

The following circumstances can affect a higher ML/TF risk:

- if a financial institution dealing with factoring and purchase of receivables offers a newly introduced product;
- if cash prevails in total deployed assets;
- if the structure of creditors and debtors contains persons without a steady source of income;
- if a sale of assets (invoice) is treated as loan;
- if there are no guarantees provided in factoring finance transactions;
- if there is factoring finance that negatively affects sale increase;
- if there is a possibility of receiving funds regardless of the creditworthiness.

3. FINANCIAL INSTITUTIONS PERFORMING FINANCIAL LEASING OPERATIONS

Financial institutions dealing with financial leasing are obliged to apply provisions under this point 3 in order to be able to recognize risks pointing to suspicious transactions and clients and to manage those risks in the manner so as to prevent any activities that could be characterized as money laundering and terrorism financing.

These institutions could be subject to a greater ML/TF risk given the limited availability of information on the origin of client funds during the repayment of the subject of leasing, in which case they shall apply enhanced customer due diligence.

Risk factors that the financial institution dealing with financial leasing is obliged to take into consideration when assessing risks are as follows:

1) the customer`s business activity or transactions are carried out under unusual circumstances;
2) annuities are paid by third parties in the name of the lessee but which have not been identified with the lessor as they are not parties to the lease contract;
3) fraudulent actions categorized under predicate offences.

The unusual circumstance under item 1) above are considered the following in particular, but not limited to:

- frequent and unexpected entering into multiple financial lease contracts with several lessors, without economic justification;
- insisting on the payment of a higher percentage of the initial payment in the procurement of the subject of leasing that the one prescribed and which the lessor requests when concluding a financial lease contract, in accordance with its general operating conditions.

The reporting entity – the lessor should take into consideration that certain circumstances indicated in this item 1 will not be obvious at the very beginning of establishing a business relationship and/or when performing one transaction.

3.1 Customer risk

The following circumstances related to customer behaviour could point to a higher risk:

- a customer acts in someone else`s name, for example when it is visible that other persons watch the customer inside or outside the premises where the transaction is being performed or the customer reads instructions from a note,
- the customer`s behaviour has no economic justification, e.g. he/she accepts a high rate, fee or interest, requires a transactions in a currency which is not an official means of payment or is unusual in the legal system in the country of the lessor or gives significant amounts of currency in big and small denominations;
- the amount that is set or received does not correspond to customer`s income (if this is known);
- a customer is subject to high costs requesting early contract termination;
- a customer is a person whose request for establishing a business relationship has been rejected by another lessor, regardless of the way the lessor has learned about this fact and/or the customer is a person of bad reputation.

3.2 Geographic risk

Geographic risk exists if a transaction connected to the subject of leasing is performed via a high-risk country (a country that has strategic deficiencies in its AML/CFT system, which has been subject to restrictive measures in accordance with the UN Security Council resolutions, which has a high level of corruption or criminal activity or which the reporting entity deems to be of high-risk on the basis of its own judgement) and/or if the customer performing the transaction is a resident of a high-risk country.

The following circumstances could point to a higher risk:
- the customer permanently or temporarily resides and/or has a registered office or permanently performs its activity in a country whose legal and institutional framework is such that there is a high level of ML/TF risk;
- the subject of leasing is repaid from a country connected to a higher ML/TF risk.

3.3 Product/service and transaction risk

A higher-risk transaction could be:
- economically unjustified transaction, e.g. unexpected early repayment of the subject of leasing or repayment shortly after the signing of the financial leasing contract;
- placement of funds in small amounts which equal monthly annuities reach a significant aggregate amount on annual level, due to which they do not exceed the limit for mandatory reporting to the public administration authority;
- customers repay annuities from funds whose origin is difficult to establish.

4. FINANCIAL INSTITUTIONS PROVIDING CREDITING AND CREDIT INTERMEDIATION SERVICES

Financial institutions offering crediting and credit intermediation services are obliged to apply provisions under this point 4 in order to be able to recognize risks pointing to suspicious transactions, clients, business relationships and to manage those risks in the manner so as

to prevent any activities that could be characterized as money laundering and terrorism financing.

Financial institutions offering crediting and credit intermediation services to micro, small and medium-sized business entities, natural persons, and entrepreneurs (clients) that perform their activity independently. Therefore, financial institutions offering crediting and credit intermediation services are obliged to assess risks for individual clients, groups of clients, countries or geographical areas, business relationships, transactions or products, services, and distribution channels, on the basis of ML/TF risk and results of the national ML/TF risk assessment.

In the process of risk analysis, financial institutions offering crediting and credit intermediation services assess the probability that their business will be used for the purpose of ML/TF.

Risk analysis of the aforesaid institutions aims at recognizing and identifying the exposures to ML/TF risk as well as business segments that should be prioritized in order to ensure efficient ML/TF risk management. Clients of these institutions shall be classified in one of the ML/FT risk categories:

- ✓ A (low risk)
- ✓ B (medium risk) and
- ✓ C (high risk)

4.1 Customer risk

Customer is a person/user of credit line service and/or direct credit arrangments or credit arrangements offered by a financial institution in cooperation with commercial banks.

4.1.1 Customer nature

The following circumstances can affect a lower ML/TF risk:

- customer is a renowned legal person, natural person, entrepreneur and another person and/or entity equal to them;
- if there is a crediting or credit intermediation involving companies dealing with trade, agriculture, tourism, hospitality, services, food production, renewable energy sources, and the like;
- if a customer regularly services their obligations on the basis of a loan granted and observes defined repayment deadlines;
- if there are frequent international transactions involving the support from renowned international institutions;
- if there is verified donated capital;
- if the origin of a customer`s funds can be easily proved and they come from activities that do not point to ML/TF risk;
- if a customer`s financial capacity is stable when it comes to settling commitments undertaken;
- if customers having a steady source of income prevail in the customer structure.

The following circumstances can affect a higher ML/TF risk:

- a customer is a legal person, a natural person, an entrepreneur and/or other person equal to it that is not renowned when it comes to their business activity or occupation;
- a customer whose financial capacity has changed due to extraordinary circumstance and/or customer has found himself/herself in the situation where he/she cannot adequately respond to the repayment requirements specified in the credit or credit intermediation agreement;
- if customers having no steady source of income prevail in the customer structure but they own real estate or have funds that are at their disposal;
- if the customer structure has high-risk clients, beneficial owners or authorised persons who are politically exposed persons and foreign politically exposed person, non-resident legal or natural persons suspected of ML/TF and the like;
- if a customer is not employed and/or there is no possibility of accessing automated system of evaluation of credit applications made by that customer;
- if low-income customers prevail in the customer structure.

4.1.2 Customer behaviour:

The following circumstances can affect a lower ML/TF risk:

- a customer provides clear and unambiguous data during the establishment of a business relationship and the execution of transaction;
- the customer performs transfers, payments and disbursement of funds which are economically justifiable and supported with proper documents which contain no elements pointing to unusual and/or suspicious transactions;
- a customer settles his/her obligations regularly in line with planned schedule;
- a customer uses products and services which do not allow anonymity.

The following circumstances can affect a higher ML/TF risk:

- a customer performs a business activity or a transaction under unusual circumstances;
- if a customer provides vague explanations regarding the performance of transactions and support them with inadequate documents accompanying their implementation;
- if the documents accompanying the execution of transactions contain elements that point to unusual and/or suspicious transactions;
- if a customer acts on behalf of another person for his/her own account without obvious economic justification;
- if a customer uses unusual ways of payment or funds which allow anonymity, payments form different bank accounts without adequate explanation;
- if a customer settles his/her credit commitments via his/her accounts held with more than one bank or partially or entirely prepays his/her credit commitments;
- if a customer requests extraordinary amendments to the credit agreement;
- if a customer transfer obligations from the credit agreement to a third party.
-

4.2 Product/service and transaction risk

The following circumstances can affect a lower ML/TF risk:

- the use of new technologies or developing technologies that allow anonymity in case that the use of these technologies would prevent detection of suspicious activities in the execution of transactions;
- transactions whose execution is accompanied by adequate documents and whose origin of funds has been verified;
- if non-cash prevails in the structure of deployed funds.

The following circumstances can affect a higher ML/TF risk:

- the use of new technologies or developing technologies that allow anonymity in case that the use of these technologies would enable detection of suspicious activities in the execution of transactions;
- transactions where the origin of funds cannot be clearly demonstrable;
- if the financial institution offering crediting and credit intermediation offers a newly introduced product;
- if credit commitments have been settled under extraordinary circumstances by a third party whose identity has not been confirmed in a required manner;
- if cash prevails in the structure of deployed funds;
- transactions having no obvious economic justification;
- more interconnected transactions whose individual amounts do not exceed 15,000 euros but their total sum obligate the reporting entity to report them to the competent public authority because they exceed 15,000 euros or more;
- if customer having no guarantees or steady source of income prevail in the customer structure;

5. PAYMENT INSTITUTIONS

This part of Guidelines deals with payment institutions as providers of payment services that are obliged to perform ML/TF risk analysis and assessment related to products, services, transactions, customer, country or geographic area.

In addition to the general provisions in these Guidelines, when drafting their own AML/CFT guidelines, payment institutions are obliged to apply high-risk factors characteristic for these reporting entities, as well as to apply measures for the reduction of identified risks.

Due to the nature of their business, payment institutions could be exposed to ML/TF risk particularly due to the fact that they do not establish any business relationships with their customers but perform occasional transactions.

5.1 Product, service and transaction risk

Payment institutions should prepare ML/TF risk analysis to consider the following **high-risk factors**:

- a product allows high-value transactions;

- a product or a service has a global reach;
- a transaction is based on cash or funded with anonymous e-money;
- one or more payers from different countries transfer money to a payee in Montenegro.

A risk factor that **could lower ML/TF risk** in payment institutions refers to funds transferred from an account that a payer has with a credit or financial institutions within the European Economic Area (EEA).

5.2 Customer risk factors

High-risk customer factors shall include at least the following:

- customer`s activity:
  - the customer owns or operates an undertaking or manages the undertaking and handles large amounts of cash;
  - the customer`s undertaking has a complicated ownership structure;

- customer behaviour characteristics - examples:
  - indications that a customer acts on someone else's behalf, for example the customer is watched by other persons in the vicinity of the place where the transaction is executed or the customer reads instructions from a note;
  - the customer`s behaviour has no economic justification, for example the customer accepts an unfavourable exchange rate or charges, requires a transaction in a currency which is not an official tender or commonly used in the payer`s or payee`s country or requests or provides significant amounts of currency in either high or low denominations;
  - the customer`s transactions are always just below the prescribed thresholds;
  - the manner in which the customer uses a service is unusual, e.g. the customer sends funds to themselves or sends funds on immediately upon their receipt;
  - the customer appears to have but few data on the payee or reluctantly provides information about the payee.
  - several service provider`s customers transfer funds to the same payee or appear to have the same identification information, for example address or phone number.
  - transactions are not accompanied by required information on the payer or the payee;
  - sent or received amount of funds does not correspond to the customer`s income (if known).

The following factors could contribute to reducing risks (**low-risk factors)**:

- the customer has used the services of the service provider for many years and his/her behaviour has not given rise to suspicion and there are no indications that ML/TF risk could increase;
- the transferred funds are of low value, however, one has to bear in mind that low amounts could carry TF risks in certain circumstances.

5.3 Distribution channel risk factors

High-risk factors of distribution channels shall include at least the following:

- if there are no restrictions to financing instruments, e.g. in case of cash or e-money product payments subject to exceptions under Article 13 of the Law, electronic transfers or cheques;
- the used distribution channel allows a certain level of anonymity;
- the service is provided entirely online, without adequate safeguards;
- money remittance service is offered through an agent which:

  - represents more than one payment service provider;
  - has unusual turnover patterns compared with other agents in similar locations, e.g. unusually high or low transactions, unusually large cash transactions or a high number of transactions that fall just under the customer due diligence threshold or an agent that undertakes business outside normal business hours;
  - carries out a significant number of transactions with payers or payees from jurisdictions associated with higher ML/TF risk;
  - appear to be unsure about, or inconsistent in, the application of group-wide ML/TF policies;
  - is not from the financial sector or conducts other business as its main activity;
  - money remittance service is offered through a large network of agents across different countries or geographic areas;
  - money remittance service is offered via the official payment chain, e.g. through a large number of intermediaries operating in different countries or geographic regions or settlement systems (formal and informal) that cannot be traced.

The following factors could contribute to **reducing risks**:

- regulated financial institutions are agents;
- a service can be financed only from transfers from the customer`s account at a credit or financial institution within the EEA or from an account over which the customer can be shown to have control.

5.4 Country or geographic area risk factors

High-risk factors of a country or a geographic area shall include at least the following:

- the payer or the payee is in a country or a geographic area associated with high ML/TF risk;

- the payee is a resident in a jurisdiction which either does not have a banking sector or has a poorly regulated and underdeveloped banking sector, meaning that unofficial money remittance services such as *hawala* can be used.

5.5 Measures aimed at lowering ML/TF risk

Given that the business of a payment institution is based on occasional transactions, it is obliged to provide and establish a system for monitoring and control to ensure the detection

and prevention of money laundering and financing of terrorism by applying enhanced customer due diligence.

Payment institutions should set up systems to include at least the following:

- systems for identification of connected transactions;
- systems for identification of transactions of different customers having the same payee;
- systems that would enable the identification of the sources and destination of funds;
- systems that enable full tracking of transactions and the number of users involved in the payment chain.

In occasional transactions with high ML/TF risk, payment institutions should apply enhanced customer due diligence specified in Section 4.1 hereof (mandatory for all reporting entities). However, when the risk associated with an occasional transaction is low, payment service providers may apply simplified customer due diligence in line with provisions of Section 4.1 hereof (mandatory for all reporting entities).

5.6 Payment institution agents

Payment institution providing payment services through an agent shall adopt policies and procedures for the implementation of AML/CFT measures.

The AML/CFT policies and procedures should include the following:

- carrying out of identification of the person who is the owner or the person controlling the agent when the latter is a legal person, in order for the payment institution to be sure that ML/TF risk it is exposed to in its operations has not increased due to the services being offered via the agent;
- the collection of documents and information (evidence) on executive officers and other persons responsible for the management of the agent, including the assessment of their professional capacity, integrity, and reputation.
- taking of appropriate measures that would make the payment institution sure that the agent`s AML/CFT internal controls are proportionate to the risk level. In case the agent`s AML/CFT internal controls differ from the corresponding controls of the payment institution, the payment institution is obliged to assess the risk level and take measures for its reduction.
- conducting initial and refresh training for agent employees in order to ensure their proper comprehension and management of ML/TF risk.

6. ELECTRONIC MONEY INSTITUTIONS

In addition to the general provisions in these Guidelines, when drafting their own AML/CFT guidelines, electronic money institutions (e-money institutions) are obliged to apply high-risk factors characteristic for these institutions, as well as to apply measures for the reduction of identified risks.

E-money institutions are obliged to perform risk analysis to identify the risk of product, customer, distribution channels, country or geographic area with a view to preventing their misuse for the purpose of ML/TF.

6.1 Product risk factors

E-money institutions are obliged to perform ML/TF risk analysis to consider at least the following **high-risk factors**:

1. limits associated with the issuing and use of e-money, whereby the product enables the following:

- high-value or unlimited-value transactions, as well as cash payments;
- high-value, loading and redemption;
- a high or unlimited amount of funds to be stored on an e-money account;

2. the manner and/or methods of funding shopping or storing e-money whereby the product could be:

- subject to anonymous loading in cash, anonymous e-money or e-money products subject to exceptions under Article 13 of the Law;
- financed with payments from unidentified third parties;
- financed with other e-money products.

3. utility and negotiability, whereby the product enables the following:

- transfers from a one person`s account to another person`s account;
- that is has been accepted by a large number of merchants or points of sale;
- that it has been specially designed to be accepted as means of payment by merchants dealing in goods and services associated with a high risk of financial crime, e.g. online gambling;
- that it can be used in cross-border transactions or in different jurisdictions;
- that it can be used by persons other than the customer, e.g. certain partner card products (excluding low-value gift cards);
- payment of large amounts of cash.

Risk factors that could contribute to the **lowering of ML/TF risk** related to products of an e-money institution are as follows:

1) products have the following restrictions:

- low restrictions in terms of payments, loading or redemption, although the e-money institution should bear in mind that a low limit in and of itself is not necessarily sufficient to lower TF risk);
- limited number of payments, loading or redemption, over a certain period of time;
- limited amount of funds that can be stored on the e-money account on any one time;

2) the manner and/or methods of financing e-money require that funds paid to the account are soon afterwards paid out from the nominative account of the customer or the customer has a joint account with a credit or financial institution within the EEA;

3) utility and negotiability related to the product under the following circumstances:

- does not allow or strictly limits outgoing cash payments;
- can be used only in Montenegro;
- it is accepted by a limited number of merchants or points of sale with whose business the e-money issuer is familiar;

4) its use is restricted by merchants trading in goods and services associated with a high risk of financial crime;

5) it is accepted as a means of payment for limited types of services or products with low ML/TF risk.

6.2 Customer risk factors

High customer risk factors shall include at least the following:

- the customer purchases several e-money products from the same issuer, makes frequent economically unjustifiable payments over a short period of time and requests cash payments; where distributors (or agents acting as distributors) are the reporting entities themselves, this also applies to e-money products from different issuers that have been purchased from the same distributor;
- a customer`s transactions are always just below the prescribed transaction limit;
- there are indications that the product is used by several person whose identity is not known to the issuer, e.g. the product that is used from several IP addresses at the same time;
- frequent changes of a customer`s identification information such as home address or IP address, or linked bank accounts;
- the product is not used for its intended purpose, e.g. it is used across the border but it was designed to be used as a gift card in a shopping centre.

Product risk factors that **could contribute to lowering ML/TF risk** for products intended exclusively for a specified category of customers such as state aid beneficiaries or members of an undertaking which issues these products for the purpose of covering corporate costs.

6.3 Distribution channel risk factors

High-risk factors of distribution channels shall include at least the following:

- distribution over the internet without personal contact (non-face-to-face distribution) and adequate safeguards such as electronic signature, electronic identification documents issued in line with special regulations;
- distribution through intermediaries who are not reporting entities under the Law where the e-money issuer:

- relies on the intermediary to carry out certain AML/CFT requirements of the e-money issuer; and
- is not sure that the intermediary has in place adequate AML/CFT systems and controls.

6.4 Country or geographic area risk factors

High-risk factors of a country or a geographic area shall include at least the following:

- the payee is located in a country or a geographic area or a product is financed from sources in a country or geographic area associated with higher ML/TF risk. An e-money institution should pay particular attention to jurisdictions known for funding or supporting terrorist activities or where terrorist groups operate, and jurisdictions subject to financial sanctions, embargoes or measures that are related to terrorism, terrorism financing or proliferation.

6.5 Measures aimed at lowering ML/TF risk

The system of internal controls in an e-money institution should include the following:

- transaction monitoring systems that detect anomalies or suspicious behavioural patterns, including thee unexpected use of products in a way for which it was not designed;
- systems that identify discrepancies between provided and detected information such as between the information of the country of origin and electronically detected IP addresses;
- systems that enable the delivery of information about other business relationships and which could identify patterns such as the same funding instruments or the same contact details;
- systems that identify whether the product is used with merchants dealing in goods and services associated with a high risk of financial crime.

6.6 Enhanced customer due diligence

Enhanced customer due diligence that an e-money institution should apply in high-risk situations includes:

- obtaining additional information about customers during identification, such as the information about the sources of funds;
- the application of additional verification measures from reliable and independent sources (e.g. checking against publicly available databases) in order to confirm the identity of the customer or beneficial owner;
- the collection of additional information about the intended nature of the business relationship, for example by surveying customers about their business, country or geographic area to which they intend to transfer e-money;
- the collection of information about a merchant and/or payee, especially where the e-money issuer has grounds to suspect that their products are used to purchase illicit or goods intended for certain individuals only;

- the verification of identity in order to confirm the customer`s identity in order to check that the customer is who they claim to be;
- applying enhanced monitoring to the customer relationship and occasional transactions;
- determining the source and/or destination of funds.

6.7 Simplified customer due diligence

Simplified customer due diligence in low-risk situations includes:

- the verification of the customer`s identity based on payments drawn on an account in the sole or joint name of the customer or an account which the customer can be shown to have control with a credit or financial institution within the EEA;
- the verification of identity on the basis of less reliable sources;
- the use of alternative methods to verify identity;
- the assumption of nature and intended purpose of the business relationship where this is obvious, for example in the case of certain gift cards that do not fall under the closed loop/network exemption;
- reducing the intensity of monitoring until a certain monetary threshold has been reached. Since ongoing monitoring is an important means of obtaining more information on customer risk factors during the course of a customer relationship, that threshold for both individual transactions and transactions that appear to be linked over the course of 12 months should be set at a level that the e-money institution has assessed as presenting a low risk for both money laundering and terrorist financing purposes.

IV. TRANSITIONAL AND FINAL PROVISIONS

The reporting entities shall harmonize their internal regulations with these Guidelines and carry out other necessary activities to ensure the implementation of these Guidelines within 60 days following their publication date.

The Guidelines on Bank Risk Analysis Aimed at Preventing Money Laundering and Terrorism Financing no. 0101-258/2-8 as of 25 February 2010 shall be repealed as of the day of entry into force of these Guidelines.

These Guidelines shall enter into force on the eighth day following that of their publication in the Official Gazette of Montenegro.

COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

CHAIRMAN
G O V E R N O R,

Decision no. 0101-
Podgorica,____2019

Radoje Žugić

ANNEX

FORM FOR THE IDENTIFICATION OF A POLITICALLY EXPOSED PERSON **PEP Form**

FORM FOR THE IDENTIFICATION OF A POLITICALLY EXPOSED PERSON

A politically exposed person, in the context of this Law, is a Montenegrin citizen performing public function (table 2 of this Form) and a foreign citizen nominated or assigned a public function by a foreign state or international organization (table 2 of this form) including their close family members and close associates.
Close family members of a politically exposed person shall include the spouse or extra-marital partner and the children born in a marital or extra-marital relationship and adoptees, their spouses or extra-marital partners, parents, brothers and sisters.
Close associate of a politically exposed person shall include:

1) natural person who is known to have joint ownership over legal persons, established business relationship or any other close business relationships, with a politically exposed person;
2) any natural person who has ownership over a legal person or has established business relationships for the benefit of the politically exposed person referred to in tables 1 and 2 of this Form that has shared profits from the property or established business relationship or other type of close business contacts.

In accordance with the Law, please answer the following questions:

Table 1

Are you a Montenegrin citizen performing a public function, this including a period of at least 12 months as of the date the performance of the public function has ended?

1.	President of Montenegro, Speaker of the Parliament of Montenegro, Prime Minister and Government Member,	YES	NO
2.	Member of Parliament;	YES	NO
3.	Member of governing bodies of political parties;	YES	NO
4.	Secretary of State, director general and secretary within a ministry, head of the administrative authority and deputy head;	YES	NO
5.	Mayor and Deputy Mayor, President and Vice-President of the Municipality, President of the Municipal Assembly of the Capital and Old Royal Capital;	YES	NO
6.	President and the judge of the Supreme Court of Montenegro and president and the judge of the Constitutional Court of Montenegro;	YES	NO
7.	Member of the State Audit Institution Senate, and a member of Central Bank Council;	YES	NO
8.	Ambassador, Consul, Chief of Staff, General and Admiral in the Armed Forces of Montenegro;	YES	NO
9.	Director, deputy director, or assistant director and the member of the administrative and supervisory bodies in majority state-owned legal persons.	YES	NO

Table 2

Are you a foreign citizen performing a public function, this including a period of at least 12 months as of the date the performance of the public function has ended?

1.	Head of State, Prime Minister , Minister and Deputy Minister;	YES	NO
2.	Member of Parliament;	YES	NO
3.	Member of governing bodies of political parties;	YES	NO
4.	Member of a Supreme Court, Constitutional Court or other high-level legislative authorities, against the decision of which, except in exceptional circumstances, it is not possible to use ordinary or extraordinary legal remedy;	YES	NO
5.	member of courts of auditors, or supreme audit institutions and central bank councils;	YES	NO
6.	Ambassador, Consul, or Senior officer of the armed forces;	YES	NO
7.	member of the administrative and supervisory bodies in majority state-owned legal persons ;	YES	NO
8.	Director, deputy director, or assistant director, a board member or a holder of any equivalent function in an international organisation.	YES	NO

			Table 3
Are you a member of the close family of persons listed in the table 1?			
1.	marital or extramarital partner ;	YES	NO
2.	a child born within or outside marriage and an adoptee and their marital or extramarital partner;	YES	NO
3.	parent, brother or sister.	YES	NO
			Table 4
Are you a close associate of persons listed in tables 1 and 2 of this Form?			
1.	Do you have joint ownership over legal persons, established business relationship or any other close business relationships, with a politically exposed person referred to in tables 1 and 2 of this Form?	YES	NO
2.	Do you have ownership over a legal person or established business relationships for the benefit of the politically exposed person referred to in tables 1 and 2 of this Form?	YES	NO
			Table 5
The data submitted by the customer to the reporting entity upon the expiry of a period of 12 months as of the day the performance of a public function has ended, based on which the obligation of a reporting entity to treat a person as a politically exposed one shall be terminated:			
1.	Has the period of 12 months as of the day the performance of the public function you were appointed to, ended?	YES	NO
2.	Are you a close family member or a close associate of a person who has performed the public function referred to in tables 1 and 2 of this Form?	YES	NO

If your answer to any of the questions specified in tables 1, 2, 3 and 4 is YES, pursuant to the Law you are a politically exposed person. Therefore, you are required to specify the source of property or funds that have been or will be the object of a business relationship or transaction:

_____

_____

By signing below I certify that the above information is accurate and truthful.

_____

Customer Name and Surname:

_____

Customer Address: Customer Date of Birth:

_____

Place and Date: Customer Signature:

_____

Name and Surname of the reporting entity employee:

_____

Place and Date:

_____

Signature of the reporting entity employee:

_____

I agree to the establishing of a business relationship and/or execution of a transaction with the politically exposed person.

Name and Surname of the responsible person in the reporting entity: Signature of the responsible person in the reporting entity:

_____ _____

Place and Date:

_____