Pursuant to Article 44 paragraph 2 item 3 of the Central Bank of Montenegro Law (OGM 40/10, 6/13, 70/17,125/23), and in conjunction with Article 12 paragraph 5 of the Law on Prevention of Money Laundering and Terrorist Financing (OGM 110/23) and Articles 4 and 9 of the Rulebook on Detailed Criteria for Developing Guidelines for Risk Analysis and Guidelines for Establishing the System for Managing Risk of Money Laundering and Terrorist Financing (OGM 22/24), the Council of the Central Bank of Montenegro, at its meeting held on 10 June 2024, passed the following

DECISION
on establishing guidelines for risk analysis and guidelines for establishing the system for managing risk of money laundering and terrorist financing with reporting entities supervised by the Central Bank of Montenegro

Article 1
This Decision shall determine the guidelines for risk analysis and the guidelines for establishing the system for managing risk of money laundering and terrorist financing with the reporting entities supervised by the Central Bank of Montenegro.

Article 2
The guidelines for risk analysis and the guidelines for establishing the system for managing risk of money laundering and terrorist financing with the reporting entities supervised by the Central Bank of Montenegro shall be enclosed in Annex which shall make an integral part of this Decision.

Article 3
As from the commencement date of the application of this Decision, the 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Terrorist Financing by Reporting Entities under the Supervision of the Central Bank of Montenegro (OGM 22/19) shall be repealed.

Article 4
This Decision shall enter into force on the eighth day following that of its publication in the Official Gazette of Montenegro.

THE COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

Decision no. 0101-4785-3/2024
Podgorica, 10 June 2024

CHAIRPERSON
VICE-GOVERNOR

Nikola Fabris, m.p.

ANNEX

GUIDELINES FOR RISK ANALYSIS AND GUIDELINES FOR ESTABLISHING THE SYSTEM FOR MANAGING RISK OF MONEY LAUNDERING AND TERRORIST FINANCING WITH REPORTING ENTITIES SUPERVISED BY THE CENTRAL BANK OF MONTENEGRO

I SUBJECT MATTER

These Guidelines shall regulate in more detail, in accordance with the Law on the Prevention of Money Laundering and Terrorist Financing (OGM 110/2023) - (hereinafter: the Law) and enabling regulations adopted on the basis of this Law, the development of risk analysis by applying risk-based approach for risks of money laundering and terrorist financing, which is used by the reporting entities licensed or authorised and supervised by the Central Bank of Montenegro (hereinafter: the Central Bank) 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 the money laundering and terrorist financing and the result of the National Risk Assessment, and to establish at the same time the risk management system associated with the money laundering and terrorist financing and the elements of risk analysis, and to establish the risk management system.

II REPORTING ENTITIES

Pursuant to the Law, these Guidelines shall be applied by the following reporting entities:

1) credit institutions and branches of foreign credit institutions;
2) entities performing the following activities:
   - purchase of receivables;
   - financial leasing;
   - renting safe deposit boxes;
   - factoring;
   - issuing guarantees and other sureties;
   - granting loans and loan mediation;
   - exchange services;
3) payment institutions and electronic money institutions in accordance with the law governing the provision of payment services and the issuance of electronic money.

These Guidelines consist of four parts: the first part applies to all reporting entities, 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, the third part governs the actions with regard to not-for-profit organisations (NPOs), while the fourth part defines de-risking.

III MEANING OF TERMS

Terms used in these Guidelines shall have the following meaning:

1) **high-risk third country** means a country that does not apply or insufficiently applies measures, or does not meet the standards for the prevention money laundering or terrorist financing within the meaning of this Law, or, according to the data from relevant international organisations it does not meet the international standards in the field of the prevention money laundering and terrorist financing;
2) **non-face to face relationships or transactions** means any transaction or relationship where the customer is not physically present or in the same physical location as the reporting entity or a person acting on the reporting entity's behalf. This includes situations where the customer's identity is being verified via video-link or similar technological means;
3) **CDD measures** means the measures of identifying the customer and monitoring the business relationship and the control of the customer's transactions - customer due diligence measures;
4) **EDD measures** means enhanced customer due diligence measures;
5) **not-for-profit organisation** (hereinafter: the NPO) means a legal person or an arrangement or an organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, and social purposes.
6) **occasional transaction** means a transaction that is carried by a customer that is not in a business relationship with the reporting entity;
7) **risk of money laundering and terrorist financing** (hereinafter: the risk) means the risk that a customer will use the financial system for money laundering or terrorist financing, or that a business relationship, a transaction, a product or a service will indirectly or directly be used for money laundering or terrorist financing;
8) **inherent risk** means the level of risk established before risk mitigation procedures;
9) **residual risk** means the level of risk established after the risk mitigation procedures;
10) **risk appetite** means the level of risk a reporting entity is prepared to accept;
11) **risk factors** mean variables that, either on their own or in combination, may increase or decrease the ML/TF risk posed by an individual business relationship or occasional transaction;
12) **risk-based approach** means an approach whereby the Central Bank and the reporting entities identify, assess and understand the ML/TF risks to which the reporting entities are exposed and take AML/CFT measures that are proportionate to those risks;
13) **source of funds** means the origin of the funds involved in a business relationship or occasional transaction. It includes both the activity that generated the funds used in the business relationship (e.g. the customer's salary) as well as the means through which the customer's funds were transferred;
14) **source of wealth** means the origin of the customer's total wealth (e.g. inheritance or savings);
15) **de-risking** means a refusal to enter into or a decision to terminate business relationship with individual customers or categories of customers associated with higher ML/TF risk, or to refuse to carry out higher ML/TF risk transactions.

IV GUIDELINES APPLIED TO ALL REPORTING ENTITIES

A reporting entity shall analyse the 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, a business relationship, a transaction or a 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) enhanced CDD (correspondent relationship, politically exposed persons, high-risk countries, high-risk sectors and activities, custody services, complex and unusual transactions, suspicious transactions);
6) simplified CDD;
7) managing of risks that expose the reporting entities to money laundering and terrorist financing;
8) professional education and training of employees in the reporting entities;
9) mandatory internal acts and procedures governing in more detail the operations of the reporting entities with regard to the area 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 customer due diligence measures as prescribed by the Law 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, they shall refuse to establish business relationship and execute the transaction, and where business relationship has been already established, they 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 level of mandatory and relevant data and information (the KYC procedure), which would be the elements for carrying out the risk assessment. Risk assessment established in such a way would be the 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 the data obtained and the assignment of risk score for individual elements should result in the final risk assessment and overall acceptability of the customer with regard to the establishment of the business relationship with the customer.

Establishing the nature and the purpose of a business relationship pose one of the preconditions for knowing the customer, understanding their business and determining the level of risk and its management, and in particular, for the process of monitoring of business, recognising deviations and taking adequate measures.

The measures the reporting entities take to establish the nature and the purpose of the business relationship as well as other information on the customer and transactions should be proportionate to the risk associated with the relationship and sufficient to enable the reporting entity to understand who the customer is, and who the customer's beneficial owners are, and what the expected and acceptable level of risk is.

The reporting entities should take steps to establish and understand:

a) the nature of customer's activities or business;
b) customer's reasons for choosing the products and services of the reporting entities;
c) the value and sources of funds that will be flowing through the account;
d) how customer will be using the reporting entity's products and services;
e) whether the customer has established business relationships with other parts of the reporting entity or wider group; and
f) what constitutes 'normal' behaviour for this customer or category of customers.

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. Therefore, risk-based approach is a compulsory requirement.

In 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.

To comply with their obligations set out in the Law, the reporting entities should assess:

a) the money laundering/terrorist financing risk to which they are exposed as a result of the nature and complexity of their business (the business-wide risk assessment); and
b) the money laundering/terrorist financing risk to which they are exposed as a result of entering into a business relationship or carrying out an occasional transaction (individual risk assessments).

Each risk assessment should consist of two steps:

i. the identification of money laundering/terrorist financing risk factors - risk identification; and
ii. the assessment of money laundering/terrorist financing risk.

When assessing the overall level of residual money laundering/terrorist financing risk associated with their business and with individual business relationships or occasional transactions, the reporting entities should consider both, the level of inherent risk, and the quality of controls and other risk mitigating factors.

The reporting entities should record and document their business-wide risk assessment, as well as any changes made to this risk assessment in a way that makes it possible for the reporting entity, and for competent authorities, to understand how it was conducted, and why it was conducted in a particular way.

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 money laundering/terrorist financing 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 customers based on risk-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 Article 17 paragraphs 1 and 2 of the 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 they estimate 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 measures in particular in cases prescribed by Article 18 of the Law.

Where the reporting entity has not implemented all measures prescribed for establishing and verifying the customer's identity 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 money laundering and terrorist financing risk analysis 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 best knows the customer and in cooperation with the compliance officer for implementing measures of detection and prevention of money laundering and terrorist financing (hereinafter: the compliance officer).

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 the 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).

In the process of risk analysis, the reporting entity shall take into account the basic risk parameters: the probability of risk and the consequences of risk, based on which they evaluate the possibility of the occurrence of a risky event and its impact on their business. The probability analysis of a risk occurring implies an assessment of the possibility of a risky event occurring, while the analysis of the consequences of a risk assesses all possible impacts from a risky event (e.g. damage, costs, losses, threatened reputation, etc.).

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

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 and 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 and transactions (the existence of the required document), parties involved in the business relationship, the method for the 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 a product/service and a 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 the risks related to new products, especially those that imply the use of new technological achievements or payment methods, and to determine the appropriate risk management measures with additional care in relation to the determined level of risk.

With regard to the value of products/services or transactions, the reporting entity shall 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 direct access to the use of product/service or execution of the transaction.

2.1 Keeping risk assessments up-to-date

The reporting entities shall put in place systems and controls to keep their assessments of the ML/TF risk associated with their business, and with their individual business relationships under review to ensure that their assessment of ML/TF risk remains up to date and relevant.

The systems and controls that the reporting entities should put in place to ensure their individual and business-wide risk assessments remain up to date should include:

- setting a date for each calendar year on which the next business-wide risk assessment update will take place, and setting a date on a risk sensitive basis for the individual risk assessment to ensure new or emerging risks are included;
- where the reporting entity becomes aware before that date that a new ML/TF risk has emerged, or an existing one has increased, this should be reflected in their individual and business-wide risk assessments as soon as possible; and
- carefully recording issues throughout the relevant period that could have a bearing on risk assessments, such as internal suspicious transaction reports, compliance failures and intelligence from front office staff.

As part of this, the reporting entities should ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess these risks and, where appropriate, incorporate them into their business-wide and individual risk assessments in a timely manner.

The systems and controls that the reporting entities should put in place to identify emerging risks should include:

A. Processes to ensure that internal information, such as information obtained as part of a reporting entity's ongoing monitoring of business relationships, is reviewed regularly to identify trends and emerging issues in relation to both, individual business relationships and the reporting entity's business.

B. Processes to ensure that the reporting entity regularly reviews relevant information sources, in particular:

   1) In respect of individual risk assessments,
      i. terror alerts and financial sanctions regimes, or changes thereto, as soon as they are issued or communicated and ensure that these are acted upon as necessary; and
      ii. media reports that are relevant to the sectors or jurisdictions in which the reporting entity is active.

   2) in respect of business-wide risk assessments:
      i. alerts and reports from the law enforcement institutions (Police Administration, Prosecutor's Office);
      ii. thematic reviews and similar publications issued by competent authorities; and
      iii. processes to capture and review information on risks, in particular risks relating to new categories of customers, countries or geographical areas, new products, new services, new distribution channels and new compliance systems and controls.

C. Engagement with other industry representatives and competent authorities (e.g. round tables, conferences and training), and processes to feed back any findings to relevant staff.

The reporting entities should determine the frequency of wholesale reviews of their business-wide and individual risk assessments methodology on a risk-sensitive basis.

2.2. Identification of risk of money laundering and terrorist financing

The reporting entity shall apply a holistic approach when identifying money laundering and terrorist financing risks to which they are exposed or might be exposed due to the establishment of the particular business relationship or the execution of occasional transaction. When identifying money laundering and terrorist financing risk associated with particular 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 their services or products for the purpose of money laundering or terrorist financing.

The reporting entities should gather sufficient information so that they are satisfied that they have identified all relevant risk factors at the beginning of the business relationship and throughout the business relationship or before carrying out the occasional transaction. Where necessary, the reporting entities should apply additional CDD measures, and assess those risk factors to obtain a holistic view of the risk associated with a particular business relationship or occasional transaction.

During the identification of money laundering and terrorist financing risk, the reporting entity shall analyse various information and risk factors.

The reporting entities should use information obtained during the course of the business relationship for individual risk assessment purposes.

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

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

- national money laundering and terrorist financing risk assessment;
- reports, typologies and other information from the Financial Intelligence Unit and other supervisory authorities;
- list of high-risk third countries published by the Financial Intelligence Unit;
- knowledge and experience of the employees in the reporting entities in the area of the prevention of money laundering and terrorist financing;
- information from the Government of Montenegro, relevant alerts, and memoranda containing explanatory notes of the relevant laws;
- information from law enforcement institutions, such as reports on threats, alerts and typologies; and
- information obtained as a part of the initial CDD process and ongoing monitoring.

The information and data for identifying risk of money laundering and terrorist financing, which the reporting entity should consider, shall cover in particular the following:

- money laundering and terrorist financing risk assessment at the EU level;
- list of high-risk third countries published by the European Commission;
- information from civil society organisations on corruption indices at the national level as well as in other countries;
- reports of international bodies and organisations concerning the prevention of money laundering and terrorist financing;

- information from credible and reliable public sources, media and other mass-media channels;
- information from industry bodies, such as typologies and emerging risks;
- information from credible and reliable commercial organisations, such as risk reports; and
- information from statistical organisations and academia.

In order to identity and assess ML/FT risk in their operations, the reporting entities must take steps that are proportionate to their nature and size.

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

I. **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, not-for-profit organisations in accordance with the FATF definition, and the like).

II. **Risk factors associated with business relationship, transactions, services, distribution channels or products -** risk of business relationship (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).

III. **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, as well as 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

1. Customer <u>high-risk</u> factors
When identifying risk associated with a customer, the reporting entities should take into consideration the increased risk related to: a) negative reputation of a customer and beneficial owner of a customer, as well as the management; b) nature and behaviour of a customer and beneficial owner of a customer, including whether this could point to increased TF risk; c) when establishing and identifying the identity of the customer in their absence is implemented; d) if the business relationship is carried out under the unusual circumstances; e) customers live or are registered in countries or geographic areas listed in third part of this Matrix; f) a customer is a politically exposed person;

g) a customer is non-resident customer;
h) legal persons or legal arrangement (trusts) or subjects of international law equal to them performing custody activities and asset management activities;
i) undertakings the ownership structure of which registers nominally the authorised representatives or bearer shares instead of beneficial owners;
j) legal persons and undertakings whose activity is related with the cash transactions;
k) if the ownership structure of a legal person or an undertaking is unusual or complex due to the nature of its business;
l) a customer for which the reporting entity submitted reports on suspicious transactions to the competent authority;
m) 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;
n) a customer is a person that is on the internal black list of the reporting entity or a group.

With regard to the assessment of level of risk, the reporting entity shall gather the following information that may indicate higher level of risk:

- Does the customer or beneficial owner have links to sectors that are commonly associated with higher risk, such as construction, the arms trade, public procurement?
- Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example, certain legal persons engaged in game of chance, casino management or dealers in precious metals?
- Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?
- Where the customer is a legal person, trust, or other type of legal arrangement, what is the purpose of their establishment? For example, what is the nature of their business?
- Is a customer a Politically Exposed Person (PEP), or is their beneficial owner a PEP? Does the customer or beneficial owner have any other relevant links to a PEP, for example are any of the customer's directors PEPs and, if so, do these PEPs exercise significant control over the customer or beneficial owner?
- Is the customer's or the beneficial owner's background consistent with what the reporting entity knows about their former, current or planned business activity, their business's turnover, the source of funds and the customer's or beneficial owner's source of wealth?

The following risk factors may be relevant when identifying the risk associated with a customer's or beneficial owners' reputation:

- Are there adverse media reports or other relevant sources of information about the customer, for example are there any allegations of criminality or terrorism against the customer or the beneficial owner? If so, are these reliable and credible? The reporting entities should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations.
- Has the customer, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing? Does the reporting entity have reasonable

grounds to suspect that the customer or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?

- Does the reporting entity have any in-house information about the customer's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?

The following risk factors may be relevant when identifying the risk associated with a customer's or beneficial owner's nature and behaviour. The reporting entities should note that not all of these risk factors will be apparent at the outset; they may emerge only once a business relationship has been established:

- Is the customer's ownership and control structure transparent and does it make sense? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?
- Does the customer issue bearer shares or does it have nominee shareholders?
- Is the customer a legal person or arrangement that could be used as an asset-holding vehicle?
- Is there a sound reason for changes in the customer's ownership and control structure?
- Does the customer request transactions that are complex, unusually or unexpectedly large, have an unusual or unexpected pattern, no apparent economic or lawful purpose, or lack a sound commercial rationale?
- Are there grounds to suspect that the customer is trying to evade specific thresholds such as those set out in the Law?
- Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share CDD information, or do they appear to want to disguise the true nature of their business?
- Can the customer's or beneficial owner's source of wealth or source of funds be easily explained, for example through their occupation, inheritance or investments? Is the explanation plausible?
- Does the customer use the products and services they have taken out as expected when the business relationship was first established?
- Where the customer is a non-resident, could their needs be better serviced elsewhere? Is there a sound economic and lawful rationale for the customer requesting the type of financial service sought? The reporting entities should take into consideration the right of customers who are legally resident in Montenegro to obtain a basic payment account, and this right applies only to the extent that credit institutions can comply with their AML/CFT obligations as referred to in Article 26 of the Law on Comparability of Fees Related to Consumer Payment Accounts, Payment Accounts Switching and Payment Account with Basic Features (OGM 145/21), which prescribes that a consumer legally resident in Montenegro, including a consumer with no fixed address and an asylum seeker, and a consumer who is not granted a residence permit but whose expulsion is impossible for legal or factual reasons, shall have the right to open and use a payment account with basic features with a credit institution, irrespective of the consumer's place of residence in Montenegro.

When identifying the risk associated with a customer's or beneficial owner's nature and behaviour, the reporting entities should pay particular attention to risk factors that, although not specific to terrorist financing, could point to increased TF risk, in particular in situations where other TF risk factors are also present. To this end, firms should consider at least the following risk factors:

- Is the customer or the beneficial owner a person included in the lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures or are they known to have close personal or professional links to persons registered on such lists?
- Is the customer or the beneficial owner a person who is publicly known to be under investigation for terrorist activity or has been convicted for terrorist activity, or are they known to have close personal or professional links to such a person?
- Does the customer carry out transactions that are characterised by incoming and outgoing fund transfers from and/or to countries where groups committing terrorist offences are known to be operating, that are known to be sources of terrorist financing or that are subject to international sanctions? If so, can these transfers be explained easily through, for example, family ties or commercial relationships?
- Does the customer transfer or intend to transfer funds to persons listed in high-risk countries?
- Does the customer carry out transactions characterised by large flows of money in a short period of time, involving non-profit organisations with unclear links (e.g. they are domiciled at the same physical location; they share the same representatives or employees or they hold multiple accounts under the same names)?

Where the customer is a not-for-profit organisation (NPO), the reporting entities should apply the criteria set out in part IV of the Guidelines that refers to the NPO.

2. <u>High-risk</u> factors in business relationship, transactions, products, services and distribution channels

When identifying risk associated with business relationships, transactions, products, services, distribution channels, the reporting entities should consider the risk related to:

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;
e) transactions associated with virtual assets;
f) transactions associated with oil, arms, precious metals, tobacco products, cultural artefacts and other items that have archaeological, historical, cultural and religious significance or exceptional scientific value, as well as transactions associated with ivory and protected species;
g) transactions that do not have economic grounds in Montenegro.

When identifying risk associated with their products, services or transactions, the reporting entities should consider the risk related to:

a) the level of transparency the product, service or transaction affords;
b) the complexity of the product, service or transaction; and
c) the value or size of the product, service or transaction.

Risk factors that the reporting entities should consider when identifying the risk associated with a product, service or transaction's transparency include:

- To what extent do products or services allow the customer or beneficial owner or beneficiary structures to remain anonymous, or facilitate hiding their identity? Examples of such products and services include bearer shares, fiduciary deposits, offshore vehicles and certain trusts, and legal entities such as foundations that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with nominee shareholders.
- To what extent is it possible for a third party that is not part of the business relationship to give instructions, for example in the case of certain correspondent banking relationships?

Risk factors that the reporting entities should consider when identifying the risk associated with a product, service or transaction's complexity include:

- How complex is the transaction and does it involve multiple parties or multiple jurisdictions?
- To what extent do products or services allow payments from third parties or accept overpayments where this would not normally be expected? Where third party payments are expected, does the reporting entity know the third party's identity, as well as clear legal and economic basis for such transactions? Or are products and services funded exclusively by fund transfers from the customer's own account at another financial institution that is subject to AML/CFT standards and oversight that are comparable to those required under the Law?
- Does the reporting entity understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

Risk factors that the reporting entities should consider when identifying the risk associated with a product, service or transaction's value or size include:

- To what extent do products or services require the use of cash?
- To what extent do products or services facilitate or encourage high-value transactions? Are there any caps on transaction values or levels of premium that could limit the use of the product or service for ML/TF purposes?

Risk factors that the reporting entities should consider when identifying the risk associated with distribution channels:

- When identifying the risk associated with the way in which the customer obtains the products or services they require, the reporting entities should consider the risk related to:

i. the extent to which the business relationship is conducted on a non-face-to-face basis; and
ii. any intermediaries that emerge.

- When assessing the risk associated with the way in which the customer obtains the products or services, the reporting entities should consider a number of factors including:

i. whether the customer is physically present for identification purposes and if not, whether the reporting entity:
   a) used a reliable form of non-face-to-face CDD; and
   b) took steps to prevent impersonation or identity fraud, i.e. whether it has an established system that complies with the requirements set forth in the enabling regulation;

ii. whether the customer has been introduced by another part of the same financial group and, if so, to what extent the reporting entity can rely on this introduction as reassurance that the customer will not expose the reporting entity to excessive ML/TF risk, and what the reporting entity has done to satisfy itself that the group entity applies CDD measures at the level that is not lower than that prescribed by the Law;

iii. whether the customer has been introduced by a third party, for example a bank that is not part of the same group or an intermediary, and if so:
   a) whether the third party is a regulated person subject to AML obligations that are consistent with those of the Law, and whether the third party is a financial institution or its main business activity is unrelated to financial service provision;
   b) whether the third party applies CDD measures, keeps records to standards, is subject to adequate supervision, and whether there are any indications that the third party's level of compliance with applicable AML/CFT legislation or regulation is inadequate (for example whether the third party has been sanctioned for breaches of AML/CFT obligations);
   c) whether they are based in a jurisdiction associated with higher ML/TF risk. Where a third party is based in a high-risk third country that has strategic deficiencies, the reporting entities must not rely on that third party.
   d) what the reporting entity has done to satisfy itself that:
   - the third party always provides the necessary identity documentation;
   - the third party will provide, immediately upon request, relevant copies of identification and verification data or electronic data;
   - the quality of the third party's CDD measures is such that it can be relied upon; and
   - the level of CDD applied by the third party is commensurate to the ML/TF risk associated with the business relationship, considering that the third party will have applied CDD measures for its own purposes;

iv. whether the customer has been introduced through a tied agent, that is, without direct contact with the reporting entity, and to what extent the reporting entity can be satisfied that the agent has obtained enough information to ensure that the reporting entity knows its customer and the level of risk associated with the business relationship;
v. whether independent or tied agents are used, to what extent they are involved on an ongoing basis in the conduct of business, and how this affects the reporting entity's knowledge of the customer and ongoing risk management.

3. Country-specific or geographic area high-risk factors

When identifying risk associated with a customer, the reporting entities should take into consideration the risk related to:

a) the jurisdictions in which the customer has its head office or is resident, and beneficial owner is resident;
b) the jurisdictions that are the customer's and beneficial owner's main places of business; and
c) the jurisdictions to which the customer and beneficial owner have relevant personal or business links, or financial or legal interests.

The reporting entities should note that the nature and purpose of the business relationship, or the type of business, will often determine the relative importance of individual country and geographical risk factors. For example:

- Where the funds used in the business relationship have been generated abroad, the level of predicate offences to money laundering and the effectiveness of a country's legal system will be particularly relevant.
- Where funds are received from, or sent to, jurisdictions where groups committing terrorist offences are known to be operating, reporting entities should consider to what extent this could be expected to or might give rise to suspicion, based on what the reporting entity knows about the purpose and nature of the business relationship.
- Where the customer is a credit or financial institution, the reporting entities should pay particular attention to the adequacy of the country's AML/CFT regime and the effectiveness of AML/CFT supervision.
- Where the customer is a trust or any other type of legal arrangement, or has a structure or functions similar to trusts such as fiduciary ownership or a service of establishing a company, the reporting entity should take into account the extent to which the country in which the customer and, where applicable, the beneficial owner are registered effectively complies with international tax transparency and information sharing standards.

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 on mutual evaluation of relevant international institutions (e.g. Financial Action Task Force (hereinafter: the FATF[1] and Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, hereinafter: MONEYVAL[2]) 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;

With regard to information on risk countries or non-cooperative 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:

FATF: www.fatf-gafi.org

MONEYVAL: www.coe.int/t/dghl/monitoring/moneyval

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.

Risk factors that the reporting entities should consider when identifying the level of terrorist financing risk associated with a jurisdiction include:

a) Is there information, for example from law enforcement bodies or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities, either from official sources, or from organised groups or organisations within that jurisdiction?

b) Is there information, for example from law enforcement bodies or credible and reliable open media sources, suggesting that groups committing terrorist offences are known to be operating in the country or territory?

c) Is the jurisdiction subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union?

Risk factors that the reporting entities should consider when identifying a jurisdiction's level of transparency and tax compliance include:

a) Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards? Is there evidence that relevant rules are effectively implemented in practice? Examples of possible sources include reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the Organisation for Economic Co-operation and Development (OECD), which rate jurisdictions for tax transparency and information sharing purposes; assessments of the jurisdiction's commitment to automatic exchange of information based on the Common Reporting Standard; assessments of compliance EU list of non-cooperative jurisdictions for tax purposes; and IMF assessments (e.g. IMF staff assessments of offshore financial centres).

b) Has the jurisdiction committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?

c) Has the jurisdiction put in place reliable and accessible beneficial ownership registers?

Risk factors that the reporting entities should consider when identifying the risk associated with the level of predicate offences to money laundering include:

a) Is there information from credible and reliable public sources about the level of predicate offences to money laundering - for example corruption, organised crime, tax crime and serious fraud? Examples include corruption perception indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the United Nations Office on Drugs and Crime World Drug Report (UNODC).

b) Is there information from more than one credible and reliable source about the capacity of the jurisdiction's investigative and judicial system effectively to investigate and prosecute these offences?

4. Customer low-risk factors

When identifying risk associated with a customer, the reporting entities should take into consideration the presence of lower risk with a customer which is:

a) a government body or a body of government administration, a local self-government body or a local government body and other legal person performing public authorities;
b) a legal person and a business undertaking in multi-member joint stock companies whose shares are traded on the organised securities market;
c) from the country or geographic area that is less risky in accordance with the risk factors set out in item 6 of this Matrix.

5. <u>High-risk</u> factors in business relationship, transactions, products, services and distribution channels

When identifying risk associated with business relationships, transactions, products and distribution channels, the reporting entities should take into consideration the presence of lower risk in the following cases:

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.
c) distribution channels that enable integrated quality mechanisms of control and monitoring, in particular for the lower risk products.

6. Country-specific or geographic area <u>low-risk</u> factors

When identifying risk associated with a particular country or a geographic area, the reporting entities should take into consideration the following cases:

a) EU Member States that have an effective system for preventing money laundering and terrorist financing - (the Member State is not on the FATF list);
b) countries have an efficient system for the prevention of money laundering and terrorist financing recognised by the FATF;
c) countries in which low level of corruption and other criminal activities has been identified based on the reports of relevant credible institutions.

The reporting entity shall cover risk factors prescribed in these Guidelines in their internal act, whereat the reporting entity may define also other risk factors associated with specific nature of its business. In addition, the reporting entities should note that the mentioned risk factors are not exhaustive, nor is there an expectation that reporting entities will consider all risk factors in all cases.

2.2.2. 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 (if not grounded);
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 52 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), they should give instructions and requirements to external suppliers to tailor the solution to their internal needs and risk assessment and 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.

- **Risk matrix - risk calculation**

Based on the weights of importance of individual risk factors that are an integral part of the risk measuring model (matrix), the reporting entity shall calculate the final money laundering and terrorist financing risk scores (inherent risk) relative to customer, group of customers, business relationship or product or service. The reporting entity should categorise level of risks in relation to the obtained risk score, i.e. the reporting entity should define the risks they deem unacceptable and acceptable (which may be low, medium or high risk) in accordance with its own risk appetite in this area.

2.3. Risk appetite policy - General rule

The reporting entities should establish a clear policy of the risk appetite and its permissible level. A higher level of risk appetite represents the undertaking of business activities with an increased risk of money laundering and terrorist financing. This policy contains the basic principles of taking and managing risks in the area of prevention of money laundering and terrorist financing, as well as the information on exposure and key risk indicators in this area, including information on the risk profile of the reporting entities, risk profiles of customers and transactions, as well as the reasons for their changes.

When determining the risk appetite associated with money laundering and terrorist financing, reporting entities shall take into account quantitative data in order to assess the institution's exposure to risk, as well as certain qualitative information (expert assessment by a compliance officer, evaluations in internal and external audit reports, compliance assessment by the Central Bank, and the like).

In their work, the reporting entities are required to develop a system of risk assessment and management, which will contain quantitative data regarding risk factors, defined through certain risk weightings, which essentially mirror/signify the numerical presentation of the conclusions of qualitative data and information.

In accordance with a certain risk appetite, the reporting entities should clearly document the method and reason for the selected treatment of customers and transactions, i.e. the method of managing the risk of money laundering and terrorist financing, as well as any possible excesses and exceptions to the established risk appetite.

In this regard, it should be emphasised that Article 19 paragraph 3 of the Law prescribes that if a reporting entity cannot conduct CDD measures, the business relationship must not be established, and if the business relationship has already been established, the reporting entity shall terminate such a business relationship. Also, if the reporting entity cannot effectively manage the risk of money laundering and terrorist financing in relation to that customer, they shall refuse or terminate the business relationship.

In addition to the above, the reporting entities should keep in mind that the application of a risk-based approach does not in itself require them to refuse or terminate business relationships with entire categories of customers that are associated with a higher risk of money laundering and terrorist financing, but to continuously apply adequate measures in order to be able to effectively control the risk, and if necessary take further measures and actions (stopping the transaction, reporting to the financial intelligence unit, closing the account, etc.).

The reporting entity’s business in such a way as to terminate or limit the business activities of a particular entire category of customers where the presence of an increased risk of money laundering and terrorist financing has been determined may lead to risk avoidance, rather than risk management in this area in the manner provided for by international standards and domestic regulation.

2.4. Categories of risk of money laundering and terrorist financing

The reporting entity should decide on the most appropriate way to categorise risk. This will depend on the nature and size of the reporting entity’s business and the types of ML/TF risk it is exposed to.

Risk classification has three main categories: high, medium and low, although it is not prohibited to include additional subcategories within these type of risk categories.

Classification of a customer and a group of customers based on the prescribed risk factors		
Risk category	***Code of category***	***Risk factors***
Low risk	A	The reporting entity shall classify a customer into the category A: -to whom it applies simplified customer due diligence in accordance with the Law; -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; - 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 a 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 (entering into business relationship without personal presence).

3. THE MANNER OF CUSTOMER'S IDENTIFICATION

3.1. Measures of establishing and verifying customer's identity, monitoring of business relationship and control of transactions of customer

The reporting entity shall carry out the prescribed measures of establishing and verifying the customer's identity on the basis of documents, data and information from reliable, independent and objective sources and collect data on the customer, or verify the collected data on the customer based on the 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 by the customer with

the reporting entity 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 natural person or an entrepreneur

The reporting entity shall establish and verify the identity of a natural person or their legal representative, an entrepreneur or a natural person carrying out business activity by reviewing personal identification of a customer in their presence and obtain data prescribed by the Law.

The identity of a customer may also be established without the personal presence (which represents high risk) only via video-electronic identification accompanied by the electronic identification, in accordance with and in the manner envisaged by a regulation governing video-electronic identification of a customer.

The reporting entities should clearly define in their policies and procedures the following:

a) who the customer and beneficial owner are for each type of customer and category of products and services, and whose identity has to be verified for CDD purposes;
b) what constitutes an occasional transaction in the context of their business and at what point a series of one-off transactions amounts to a business relationship, rather than an occasional transaction, taking into consideration factors such as the frequency or regularity with which the customer returns for occasional transactions, and the extent to which the relationship is expected to have, or appears to have, an element of duration;
c) what the appropriate level and type of CDD that they will apply to individual business relationships and occasional transactions;
d) how they expect the identity of the customer and the beneficial owner to be verified and how they expect the nature and purpose of the business relationship to be established;
e) which level of monitoring is to be applied in what circumstances;
f) how, and in which situations, weaker forms of identification and verification of identity can be compensated for by enhanced monitoring; and
g) the reporting entity's risk appetite.

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

Data on a customer that is a natural person, an entrepreneur or a natural person carrying out business activity, legal representative and customer's authorised persons	
Data on customer – natural person	- name and last name, unique personal identification number; - address and municipality of permanent or temporary residence in Montenegro; - date of birth, country of birth, citizenship; - data whether a customer - natural person is a politically exposed person; - data whether a customer - natural person is a resident or non-resident;

	- telephone number and e-mail address; - type, number, country of issuance and date of validity of personal identification document; - reason for entering into the business relationship (establishing the business relationship, executing transactions, attempting to execute transaction, renting of safe deposit box, accessing the safe deposit box, vendor, customer); - data whether the natural person is a customer, authorised person, beneficial owner, founder, trustee, user of property they manage; - data on the manner in which the customer identification has been carried out (identification in personal presence, electronic identification or video-electronic identification).
Data on customer – entrepreneur or natural person carrying out business activity	- name of the head office (address and city or municipality of an entrepreneur with head office in Montenegro, and for entrepreneur with head office in another country - country and city); - name and last name, unique personal identification number; - data whether they are a resident or non-resident; - reason for entering into the business relationship (establishing the business relationship, executing transactions, attempting to execute transaction, renting of safe deposit box, accessing the safe deposit box, vendor, customer); - telephone number and e-mail address; - data on the manner in which the customer identification has been carried out (identification in personal presence, electronic identification or video-electronic identification).
Data on customer's business relationship	- data on the purpose, objective, nature of business relationship and transaction; - basic activity code of a customer and scanned documentation supporting the business relationship or transaction; - data on sources of wealth and funds that are or will be subject to the business relationship or transaction; - date of establishing the business relationship or date and time of accessing the safe deposit box.
Data on transaction	- date and time of the execution of the transaction; - amount of transaction in EUR and amounts of transactions per currencies; - number of transaction order or contract; - scanned documentation supporting the execution of the transaction; - data on sources of wealth and funds supporting the execution of the transaction; - data whether the transaction has been executed fully or partially; - data on the type of transaction (cash or cashless); - data on the type of transaction (regular, suspicious, unusual or complex); - data on the credit institution of a payer and payee (type and number of account, identification number, name and country of the head office);

	- data on the type of transaction (payment or disbursement); - data on the manner of executing the transaction (cash, cashless, already executed, in instalments, market or non-market); - data on the purpose of the transaction and the name of the branch of the reporting entity executing the transaction.
Data on legal representative and authorised person	- name and last name, unique personal identification number; - address and municipality of permanent or temporary residence in Montenegro; - date of birth, country of birth, citizenship; - data whether they are politically exposed person; - data whether they are a resident or non-resident; - telephone number and e-mail address; - type, number, country of issuance and date of validity of personal identification document; - reason for entering into the business relationship (establishing the business relationship, executing transactions, attempting to execute transaction, renting of safe deposit box, accessing the safe deposit box, vendor, customer); - data whether a natural person is a customer, representative, authorised person, vendor or a customer; - obtain all of the above listed data also on customer from the written authorisation in original or verified copies of such authorisation.

3.3. Establishing the identity of a customer via video-electronic identification

When identifying a customer, the reporting entities should ensure that the evidence on the identify are based on data or information from reliable and independent sources.

The reporting entities that use or intend to use innovative technological means for identification and verification purposes should assess the extent to which the use of innovative technological solutions can address, or might exacerbate, the ML/TF risks, in particular in non-face to face situations. As a part of their assessment, the reporting entities should have clear view on:

a) Information and Communication Technology (ICT) and security risks, in particular risks that the innovative solution may be unsuitable or unreliable or could be tampered with;
b) qualitative risks, in particular the risk that the sources of information used for verification purposes are not sufficiently independent and reliable; and the risk that the extent of identity verification provided by the innovative solution is not commensurate with the level of ML/TF risk associated with the business relationship;
c) legal risks, in particular the risk that the technological solution provider does not comply with applicable data protection legislation; and
d) impersonation fraud risks, that is, the risk that a customer is not who they claim to be. The reporting entities should also consider the risk that the person is not a real person (new technological solutions).

The aforementioned methods of establishing the identity are envisaged in more detail in the Rulebook on detailed manner of implementation and training for implementation video-electronic identification of a customer (OGM 022/24 of 15 March 2024).

3.4. Establishing and verifying the identity of the customer that is a legal person or a business undertaking

The reporting entity shall identify the customer that is a legal entity or a business undertaking before establishing a business relationship with the customer and before executing the transaction, in such a way so as to obtain the data referred to in Article 117 paragraph 1 items 1, 6 and 7 of the Law, for a legal entity or a business undertaking that establishes a business relationship or executes a transaction, or a legal entity or a business undertaking for which business relationship is established or a transaction is executed.

The reporting entity may obtain data based on which it identifies a legal person by accessing the Central Registry of Business Undertakings (hereinafter: the CRPS) or another adequate public registry, as well as by accessing the court, commercial or other public registry in which the foreign legal person or business undertaking has been registered.

The reporting entity may obtain the above-mentioned data by accessing the original or certified photocopy of the document from the CRPS or other appropriate public registry, as well as by accessing the original or certified photocopy of the document from the court, business or other public registry in which a foreign legal person or a business undertaking is registered, which is submitted on behalf of a legal person or a business undertaking by their representative or an authorised person and which must not be older than three months following the date of their issue. The reporting entity shall keep the documents on the basis of which the identification is made in their documentation. When accessing the registries, the reporting entity shall print an excerpt from those registries and denote the date and time and the name and last name of the person who made an access.

The reporting entity shall obtain data not contained in the registries or documents based on which the identification is carried out by accessing the original or certified photocopy of a document or other documentation submitted to them by representative or authorised person of a customer.

Where the reporting entity, in the process of identifying the customer who is a legal person or a business undertaking has doubts in the accuracy of the obtained data or veracity of identification documents or public or other documents from which the data have been obtained, they shall obtain also written statement from the representative or authorised person of that customer before establishing a business relationship or executing a transaction.

If a customer is a foreign legal person performing their business activity in Montenegro through their business unit, the reporting entity shall identify the foreign person and their business unit.

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

Data on customer – legal person	
Data on customer	- name of a legal person; - name of the head office (address and city or municipality for a legal person with head office in Montenegro, and for a legal person with head office in another country - country and city); - identification number of a legal person and data whether a legal person is a resident or non-resident; - telephone number and e-mail address.
Data on established business relationship	- Date of establishing business relationship or accessing the safe deposit box; - data on the purpose, objective, nature of business relationship and transaction; - basic activity code of a customer and scanned documentation supporting the business relationship or transaction; - data on sources of wealth and funds that are or will be subject to the business relationship or transaction;
Data on executed transaction	- date and time of the execution of the transaction; - amount of transaction in EUR and amounts of transactions per currencies; - number of transaction order or contract; - scanned documentation supporting the execution of the transaction; - data on sources of wealth and funds supporting the execution of the transaction. - data whether the transaction has been executed fully or partially; - data on the type of transaction (cash or cashless); - data on the type of transaction (regular, suspicious, unusual or complex); - data on the credit institution of a payer and payee (type and number of account, identification number, name and country of the head office); - data on the type of transaction (payment or disbursement); - data on the manner of executing the transaction (cash, cashless, already executed, in instalments); - data on the purpose of the transaction and the name of the branch of the reporting entity executing the transaction; - type and the number of account, identification number, name and country of the head office of a credit institution of an account; - name and last name, address and city of permanent or temporary residence of a natural person to whom the transaction is intended; - telephone number and e-mail address of a natural person; - name, head office (address, city and country) of a legal person to whom the transaction is intended; - telephone number and e-mail address of a legal person;

	- SWIFT with credit institution, country of destination, name and country of head office of a credit institution which is a correspondent.
Data on a person representing the customer (legal representative or authorised person)	- name and last name, unique personal identification number; - address and municipality of permanent or temporary residence in Montenegro; - date of birth, country of birth, citizenship; - data whether they are politically exposed person; - data whether they are a resident or non-resident; - telephone number and e-mail address; - type, number, country of issuance and date of validity of personal identification document; - reason for entering into the business relationship (establishing the business relationship, executing transactions, attempting to execute transaction, renting of safe deposit box, accessing the safe deposit box, and the like); - data whether the natural person is a customer, authorised person, beneficial owner, founder, trustee, user of property they manage; - power of attorney of a legal representative and all directors (power of attorney should be kept in a documentation).
Data on beneficial owner of a customer or persons with the interest to establish a trust	Establishing of a beneficial owner of a legal person, a business undertaking, a trust, another person or a subject of international law equal to them shall be made by obtaining data on these entities by accessing the Beneficial Owners' Registry or it may be obtained by accessing the original or certified photocopy of a document from the CRPS or other appropriate public registry, as well as by accessing court, business or other public registry in which a foreign legal person or a business undertaking is registered. The reporting entity shall obtain the following: - a photocopy of a personal identification document of the beneficial owner; - name and last name, unique personal identification number; - address and municipality of permanent or temporary residence in Montenegro; - date of birth, country of birth, citizenship; - data whether they are politically exposed person; - data whether they are a resident or non-resident; - telephone number and e-mail address; - type, number, country of issuance and date of validity of personal identification document; - documentation on the basis of which it is possible to determine the ownership structure and controlling member of the customer and data on the beneficial owner; - data on ownership share (percentage of shares or percentage of share in capital or data on percentage of direct or indirect disposal of property or data on percentage of income of the user from the property they manage or share in the property of the legal person or other subject of international law) or other type of control (data on whether the owner has deciding influence in property management, whether they directly provide or have

	provided funds or they have decisive influence to decision-making process or have a controlling position in management); - date of registration, date of change or modification and deletion of the beneficial owner from the Beneficial Owner Registry; - scanned documentation evidencing the aforementioned data.

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

- **Establishing and verifying the identity of a <u>representative</u>**

The reporting entity shall identify a representative of a customer who is a legal person or a business undertaking.

The reporting entity shall obtain data on all directors of a legal person or a business undertaking – for natural person: name and last name, unique personal identification number, address and municipality of temporary residence or permanent residence in Montenegro, date of birth, country of birth, citizenship, data whether they are politically exposed person, data whether they are resident or non-resident, telephone number and e-mail address, type, number, country of issuance and date of validity of personal identification document, the reason for entering into the business relationship (establishing the business relationship, executing transactions, attempting to execute transaction, renting of safe deposit box, accessing the safe deposit box, vendor, customer), data whether a natural person is a customer, representative, authorised person, beneficial owner, trustee, user of property managed by the customer.

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 their documents.

- **Establishing and verifying the identity of an <u>authorised person</u>**

The reporting entity shall establish and verify the identity of an authorised person of a legal person or a business undertaking if the authorised person, on behalf of representative and all directors, establishes the business relationship of a domestic or legal person or a business undertaking or exercises the transaction in the manner prescribed by Article 28 of the Law.

The reporting entity shall obtain data on the representative and all directors on behalf of which the authorised person is acting in accordance with Article 22 of the Law by accessing the original or certified photocopy of written power of attorney issued by the representative that is kept in their documentation.

With respect to establishing and verifying the identity of the representative as well as the identity of the authorised legal person and business 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 by access to original document or certified photocopy of other valid public document that customer presents or by access to public registry.

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 a business undertaking, they 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 a business undertaking, obtain photocopies of personal identification documents of those persons in accordance with Article 22 paragraph 3 of the Law.

3.6. Establishing and verifying the identity of a foreign trust, other person or a subject of international law equal to them

The reporting entity shall establish and verify the identity of a foreign trust, other person or a subject of international law equal to them in accordance with Article 29 of the Law.

Data on customer that is a foreign trust, other person or a subject of international law 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: - founders; all trustees; other representatives; beneficiary or a group or beneficiaries who manage a property 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 customer that is a foreign trust – legal person	- a legal form of a trust, other person or a subject of international law equal to them; - articles of incorporation of a trust, other person or a subject of international law equal to them - name; - name of the head office (address and city or municipality of an entrepreneur with head office in Montenegro, and for entrepreneur with head office in another country - country and city); - identification number; - data whether they are a resident or non-resident; - telephone number; - e-mail address.
Data on a customer that is a foreign trust – entrepreneur	- name; - name of the head office (address and city or municipality of an entrepreneur with head office in Montenegro, and for entrepreneur with head office in another country - country and city); - unique personal identification number; - name and last name: - data whether they are a resident or non-resident; - telephone number; - e-mail address.

Data on customer that is a foreign trust – natural person	- name and last name; - unique personal identification number; - address and municipality of permanent or temporary residence in Montenegro; - date of birth; - country of birth; - citizenship; - data whether they are politically exposed person; - data whether they are a resident or non-resident; - telephone number; - e-mail address; - type, number, country of issuance and date of validity of personal identification document; - data whether the natural person is a customer, authorised person, beneficial owner, founder, trustee, beneficiary of property they manage, insurer, insurance underwriter, insurance policyholder, vendor or customer;
Data on established business relationship	- reason for entering into the business relationship (establishing the business relationship, executing transactions, attempting to execute transaction, renting of safe deposit box, accessing the safe deposit box, insurance underwriter, insurance policyholder, vendor, customer); - data on the purpose, scope, objective nature of business relationship and transaction, basic activity code of a customer and scanned documentation supporting the business relationship or a transaction; - data on sources of wealth and funds that are or will be subject to the business relationship or transaction; - date of establishing the business relationship or date and time of accessing the safe deposit box. - powers of attorney for representatives and all directors.
Data on executed transaction	- date and time of the execution of the transaction; - amount of transaction in EUR; - amounts of transactions per currencies; - number of transaction order, policy or contract, depending on the type of the reporting entity; - data whether the transaction has been executed fully or partially; - data on the type of transaction (cash or cashless); - data on the type of transaction (regular, suspicious, unusual or complex); - data on the credit institution of a payer and payee (type and number of account, identification number, name and country of the head office); - data on the type of transaction (payment or disbursement); - data on the manner of executing the transaction (cash, cashless, already executed, in instalments, market or non-market); - data on the purpose of transaction; - name of the reporting entity’s branch executing the transaction.
Data on a person representing the	- name and last name: - unique personal identification number;

customer - legal representative or authorised person	- address and municipality of permanent or temporary residence in Montenegro; - date of birth; - country of birth; - citizenship; - data whether they are politically exposed person; - data whether they are a resident or non-resident; - telephone number; - e-mail address; - type, number, country of issuance and date of validity of personal identification document; - data whether the natural person is a customer, authorised person, beneficial owner, founder, trustee, beneficiary of property they manage, insurer, insurance underwriter, insurance policyholder, vendor or customer;
Data on beneficial owner of the customer	- name and last name: - unique personal identification number; - address and municipality of permanent or temporary residence in Montenegro; - date of birth; - country of birth; - citizenship; - data whether they are politically exposed person; - data whether they are a resident or non-resident; - telephone number; - e-mail address; - type, number, country of issuance and date of validity of personal identification document; - data whether a beneficial owner is a founder, trustee, beneficiary of the funds acquired from the property they manage (where future beneficiaries have been already determined or may be determined), representative of interest of recipients of acquired funds, belongs to a category of a person who has an interest to establish the control over or otherwise, directly or indirectly, controls the property of a trust, other person or a subject of international law equal to them.

3.7. 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 41 of the Law.

The reporting entity shall, before establishing business relationship with a legal person, within establishing and verifying the identity of the customer, also determine beneficial owner of the customer and verify their identity and undertake other necessary measures (establishing if the beneficial owner is politically exposed person, eligibility checks, information from available databases, 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. they shall determine the ownership structure of the customer broken down to natural persons that are considered beneficial owners by a definition set forth in the Law.

A beneficial owner is a natural person that has ownership or ultimately exercises control over a legal person, a business undertaking, a trust, other person or a subject of international law equal to them, or a natural person on whose behalf or for whose account transaction is being exercised or a business relationship is being established.

The reporting entity shall obtain data on beneficial owner set out as mandatory by the Law by accessing the original documents or certified copy of documents from the CRPS or other appropriate public registry as well as by accessing 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 they shall obtain them by accessing the CRPS or other public registry.

Where the reporting entity cannot obtain all data on beneficial owner of a legal person, a business undertaking or a foreign legal person in the prescribed manner, they shall obtain those data by accessing 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, a business 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 they shall write the date, time and the name of a person that accessed the document, and they 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 41 paragraphs 6 and 7 of the Law, the data on the category of persons the interest of which is establishing and acting of a legal person or similar subject of international law.

In meeting their obligations aimed at understanding customer's ownership and control structure, the reporting entities should take at least the following steps:

a) forward an inquiry to a customer who their beneficial owners are;
b) document the information obtained (from the sources prescribed by the law);
c) take all necessary and reasonable measures to verify the information: to achieve this, reporting entities should consider using beneficial ownership registers where available;
d) steps b) and c) should be applied on a risk-sensitive basis – which means, for higher level or risk, higher level of checks.

3.7.1 Beneficial ownership registries

Using information contained in beneficial ownership registries does not, in itself, fulfil the duty of a reporting entity to take adequate and risk-sensitive measures to identity the beneficial owner and verify their identity. Reporting entities shall take additional steps to identify and verify the beneficial owner, in particular where the risk associated with the business relationship is increased or where the reporting entity has doubts that the person listed in the registry is the ultimate beneficial owner.

3.7.2 Control through other means

The requirement to identify, and take all necessary and reasonable measures to verify the identity of the beneficial owner relates only to the natural person who ultimately owns or controls the customer. However, to comply with their obligations, the reporting entities should also take reasonable measures to understand the customer's ownership and control structure.

The measures the reporting entities shall take to understand the customer's ownership and control structure should be sufficient so that the reporting entity can be reasonably satisfied that it understands the risk associated with different layers of ownership and control. In particular, the reporting entity should be satisfied that:

a) the customer's ownership and control structure is not unduly complex or opaque; or
b) complex or opaque ownership and control structures have a legitimate legal or economic reason.

The reporting entities should report to the financial-intelligence unit if the customer's ownership and control structure give rise to suspicion and they have reasonable grounds to suspect that the funds may be the proceeds of criminal activity or are related to terrorist financing.

Examples of "control through other means" the reporting entities should consider include, but are not limited to:

a) control without direct ownership, for example through close family relationships, or historical or contractual associations;
b) using, enjoying or benefiting from the assets owned by the customer;
c) responsibility for strategic decisions that fundamentally affect the business practices or general direction of a legal person.

3.7.3 Identifying the customer's senior managing officials

The reporting entities should resort to identifying the customer's senior managing officials as beneficial owners only if:

i. They have exhausted all possible means of identifying the natural person who ultimately owns or controls the customer;
ii. Their inability to identify the natural person who ultimately owns or controls the customer does not give rise to suspicions of money laundering and terrorist financing; and
iii. They are satisfied that the reason given by the customer as to why the natural person who ultimately owns or controls the customer cannot be identified is plausible.

When deciding which senior managing official, or which senior managing officials, to identify as beneficial owner, the reporting entities should consider who has ultimate and overall responsibility for the customer and takes binding decisions on the customer's behalf.

In those cases, the reporting entities should clearly document their reasons for identifying the senior manager, rather than the customer's beneficial owner, and must keep records of actions taken in the process of identifying the beneficial owner.

3.7.4 Identifying the beneficial owner of a public administration or a state undertaking

Where the customer is a public administration or a government institution (state undertaking), the reporting entities should follow the rules set forth in the previous sub-title to identify the senior managing official.

In those cases, and in particular where the risk associated with the relationship is increased, for example because the state undertaking is from a country associated with high levels of corruption, the reporting entities should take risk-sensitive steps to establish that the person they have identified as the beneficial owner is properly authorised by the customer to act on the customer's behalf.

The reporting entities should also have due regard to the possibility that the senior managing official of the customer may be a PEP. Should this be the case, the reporting entities must apply EDD measures to that senior managing official and assess whether the extent to which the PEP can influence the customer gives rise to increased ML/TF risk and whether it may be necessary to apply EDD measures to the customer.

The establishment of a beneficial owner is prescribed in more detail in the Central Bank of Montenegro's Guidelines on establishing the beneficial owner.

3.8. 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 the 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 the 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.

A third party may be:

1) a credit institution and a branch of a foreign credit institution with a head office in the EU Member State or another country applying measures from the area of the prevention of money laundering and terrorist financing set forth by the Law or stricter measures.

Since the reporting entity is responsible for proper establishment and verification of the identity of a customer through a third party, it shall 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 has 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 they have established and verified customer’s identity and obtained data and documents and they 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. MONITORING OF BUSINESS RELATIONSHIP AND CONTROL OF TRANSACTIONS, INCLUDING 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 they are 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 50 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 head 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 they 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 to suspect in money laundering and terrorist financing as well as based on other information and data for which they deem are sufficient to reach a conclusion on the existence of the reasonable doubt in money laundering or terrorist financing. All customers must be included in this 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 reporting entity shall ensure that the actions regarding periodical monitoring of business relationship in accordance with a certain level of risk is recorded, and activities taken during checks are clearly reported.

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 customer's risk profile			
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 their 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 as envisaged by 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 associated with the customer, group of customers, country or geographic area, business relationship, transaction, product, service and distribution channel, as well as in the cases when high risk of money laundering and terrorist financing is established in accordance with the National Risk Assessment.

The application of the enhanced customer due diligence measures shall be mandatory in the following cases:

- when entering into a correspondent relationship with a bank or another credit institution from third-country;
- when a customer or a beneficial owner of a customer is a politically exposed person;
- when providing custody services in accordance with the law governing capital market;
- in cases of complex and unusual transactions;
- in cases of suspicious transactions;
- in cases of electronic money transfer.
- when establishing or the duration of a business relationship or executing transactions with a person from high-risk third country or when high-risk third country is included in a transaction;
- when high risk of money laundering and terrorist financing has been established in guidelines on risk analysis;
- when high risk of money laundering and terrorist financing has been established in accordance with the National Risk Assessment.

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 customer due diligence measures in accordance with the risk assessment, undertake enhanced customer due diligence measures and obtain also additional data, information and documents prescribed by the provisions of the Law, for the institutions with head offices in third countries.

The correspondent relationships are regulated in more detail in the Section III, item 1.7 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 54 of the Law.

The reporting entity shall, before entering into a business relationship with a customer, check in the Registry of politically exposed persons whether a customer, their legal representative, authorised person or beneficial owner of a customer is a politically exposed person. The reporting entities shall carry out checks of the aforesaid using the Registry of the politically exposed persons that is kept and maintained by the Agency for the Prevention of Corruption.

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 should undertake also additional checks in either of the following manners, or their combination:

- by obtaining information on the basis of the access to the politically exposed persons' databases (World Check PEP List, via internet search, etc.).
- by checking open databases;
- 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;

The reporting entities shall make additional checks in all cases.

The procedure of establishing close associates of politically exposed is applied on the basis of documented facts.

The reporting entity shall establish a list of politically exposed persons, which should be made appropriately available to the bank employees that have a 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 customer's source of property (wealth) and the source of funds. The reporting entities should check sources of wealth and sources of funds based on reliable and independent data, documents and information, where the risk associated with PEP is particularly high.

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 undertaking, trust and other person, or subject of international law equal to them with the head office in a foreign country, on whose behalf a business relationship is being established or a transaction is being executed or other customer's activity is being performed, and obtain required information.

For all legal persons in which a politically exposed person appears in any form of connected person, the reporting entities should take enhanced due diligence measures, and the same applies also for natural persons in which the PEP is authorised person per account.

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 due care the 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 ↓	Establishing sources of wealth and sources of funds of customer	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 with the reporting entity ↓ ↓	Obtaining data on whether the PEP is the beneficiary owner of the legal person	Obtaining additional documentation and data ↓	Additional due diligence of a customer ↓	Additional measures ↓
Politically exposed person	Yes	Yes	Yes	A set of data as defined in Article 56 of the Law.	Yes	In accordance with the internal procedures of the reporting entity

The reporting entity shall pass an internal act defining the procedure to terminate the obligation to treat a person as politically exposed person. 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 particular 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 54 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 of the termination of the public function, they should 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 or which are not in alignment with or are disproportionate to the usual or 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 large transactions (in large amounts), even in cases when, in terms of transactions or the customer, there are no reasons to suspect in money laundering or terrorist financing.

Transactions may be unusual because:

a) they are larger than the amount set by the reporting entity in their internal acts as the amount above which checks are mandatory;
b) they are larger than what the reporting entity would normally expect based on their knowledge of the customer, the business relationship or the category to which the customer belongs;
c) they have an unusual, unexpected or complex pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers, products or services, and the firm is not aware of an economic rationale or lawful purpose or doubts the veracity of the information they have been given.

These EDD measures should enable the reporting entity to determine whether these transactions give rise to suspicion and must at least include:

a) taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and
b) monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A reporting entity may decide to monitor individual transactions where this is commensurate to the risk they have identified.

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 results of the analysis, which contains a clear conclusion on the absence of grounds for suspicion for reporting a suspicious transaction (i.e. that it is an unusual transaction), the reporting entity shall record in writing, so that they are available at the request of the competent authority of the administration or supervisory authority, and they could be used in the procedures of customer due diligence.

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 verify additional information on the property status, the origin of the property and the source/origin and final destination, as well as the purpose of the funds involved in the business relationship or transaction with that customer;
4) collect information on the origin of funds and the origin of the property of the customer and the beneficial owner(s); and
5) collect information on the reasons for planned or executed transactions.

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.

Determining deviations from business in terms of recognising and analysing unusual transactions is the basis for enhanced monitoring of the business relationship and subsequent transactions with greater frequency and with greater attention to detail.

As the Law also stipulates that the reporting entity shall establish the criteria for recognising complex and unusual transactions in an internal act, it is particularly important that the reporting entity, within the internal act, sets the minimum amounts of transactions, above which the transaction is considered unusual and must be analysed as such. That minimum limit must be the result of clear factors and analysis.

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

The provisions of the Law stipulate the due diligence measures for a customer from a high-risk third country 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.

A business relationship or transaction always involves a high-risk third country if:

a) the funds were generated in a high-risk third country;
b) the funds are received from a high-risk third country;
c) the destination of funds is a high-risk third country;
d) the reporting entity is dealing with a natural person or a legal person resident or established in a high-risk third country; or
e) the reporting entity is dealing with a trustee established in a high-risk third country or with a trust governed under the law of a high-risk third country.

In addition, when performing CDD measures or during the course of a business relationship, the reporting entities should ensure that they also apply the EDD measures to determine that:

a) the transaction passes through a high-risk third country, for example because of where the intermediary payment services provider is based; or
b) a customer's beneficial owner is resident in a high-risk third country.

In the cases of high-risk third countries, the reporting entity shall apply EDD measures as defined in the second chapter of these guidelines.

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.

After establishing a business relationship, the reporting entity shall monitor transactions and other business activities performed by a customer from a high-risk third country, and take measures in accordance with the level of risk of money laundering and terrorist financing, i.e. increase the number and frequency of performed controls and to select ways of executing transactions that need to be additionally examined, and provide more frequent reporting to the Compliance officer for the Prevention of Money Laundering and Terrorist Financing on transactions, and potentially limit business relationship or transactions with customers from countries on the list.

The financial-intelligence unit 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 way of an internal act, in accordance with Article 12 of the Law, determine the criteria for recognising the customers from high-risk third countries.

4.1.1.5 Enhanced customer due diligence (for all cases of increased risk)

When the reporting entity identifies the increased risk in relation to the transaction, customer or any other element or risk factor, they shall take at least following EDD measures:

1) collect and verify additional information on the customer's activities and update regularly 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.

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:

I. 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.

II. 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.

III. Increase in the quality of information obtained for the EDD purposes to confirm the customer's or beneficial owner's identity including by establishing that the customer's wealth and the funds that are used in the business relationship are not the proceeds of criminal activity and that the source of wealth and source of funds are consistent with the reporting entity's knowledge of the 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 wealth and funds may be the only adequate risk mitigation tool.

IV. 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.

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.

In the cases specified by the Law on the Prevention of Money Laundering and Terrorist Financing, as well as on the basis of the conclusions of the National Risk Assessment, 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.

It is important to note that the simplified due diligence measures do not represent an exemption from any of the prescribed customer due diligence measures; however, this means that the reporting entities may adjust the volume, timing and type of each or all due diligence measures in the manner that is proportionate to the low risk they have identified.

Simplified due diligence measures that the reporting entities may apply include, but they are not limited to:

a) the timing of CDD, i.e. where the product of transaction sought has features that limit its use for ML/FT purposes, for example by, verifying the customer's or beneficial owner's identity during the establishment of the business relationship;
b) adjusting the quantity of information obtained for identification, verification or monitoring purposes, for example by:
    i. verifying identity on the basis of information obtained from one reliable, credible and independent document or data source only; or
    ii. assuming the nature and purpose of the business relationship because the product is designed for one particular use only, such as a company pension scheme or a shopping centre gift card (whereas the product or service, or area or business activity must be low risk).
c) adjusting the quality or source of information obtained for identification, verification or monitoring purposes. For example, where the risk associated with all aspects of the relationship is very low, by relying on the source of funds to meet some of the CDD requirements (e.g. where funds for payouts are from the state budget);
d) adjusting the frequency of CDD updates and reviews of the business relationship, i.e. carrying these out only when trigger events occur such as the when the customer looks to take out a new product or service or when a certain transaction threshold is reached. The reporting entities must make sure that this does not result in a de facto exemption from keeping CDD information up-to-date;
e) adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where the reporting entities choose to do this, they must ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, together, would exceed that threshold.

Where there are indications that the risk may not be low, for example where there are grounds to suspect that ML/TF is being attempted or where the reporting entity has doubts about the veracity of the information obtained, SDD must not be applied. Equally, where specific high-risk scenarios apply and there is an obligation to conduct EDD, SDD must not be applied.

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 financial-intelligence unit, 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, but only in the cases that are specified by the Law, as well as based on the conclusions of the National Risk Assessment.

The 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.

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.

4.2 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, making available or collecting funds or property, in any way, directly or indirectly, with the intention of using them or if it is known that they will be used in full or in part for the execution of a terrorist act, or an attempt of providing, making available or collecting funds or property, in any way, directly or indirectly, with the intention or with the knowledge that they may be used, in full or in part:
   - for preparing or committing terrorist act in the context of this Law,
   - for financing organisations whose aim is to commit the acts referred to in indent 1 of this item or members of those organisations or individuals whose aim is to commit such acts, or
   - by terrorists or by terrorist organisations for any purpose;
2) encouraging or assisting in providing or collecting the funds or property referred to in item 1.

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 the terrorist financing are most frequently executed in smaller amounts, which greatly complicates the 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 detecting and recognising suspicious customers and transactions associated with terrorist financing.

The issue of identifying terrorist financing is a complex one, thus its resolution falls under the competence of different state institutions and authorities, whereas the reporting entity's obligation relates, in particular, to reporting suspicious transactions that may be associated with terrorist financing to the competent administration 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, and to apply relevant indicators.

With regard to the checks/controls of transactions and customers in order to detect and prevent terrorist financing, the reporting entities must pay particular attention to the application of the UN, EU, and domestic lists of designated persons under sanctions, especially the list related to terrorism.

In order to be able to fully protect the system from possible misuses and the transfer of funds that could be used, and which have the ultimate objective of terrorist financing, the reporting entities should develop information and technical solutions that will enable the recognition of data on persons from the lists or purposes of the transactions, which in real time will lead to sending a warning and stopping the transaction or further activities to establish a business relationship, as well as the immediate notification of the relevant institutions, the financial-intelligence unit, and other institutions in accordance with the Law on International Restrictive Measures.

5. MANAGING RISKS OF MONEY LAUNDERING AND TERRORIST FINANCING THE REPORTING ENTITIES ARE EXPOSED TO – MEASURES, ACTIONS AND PROCEDURE FOR RISK MANAGEMENT

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

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, in accordance with the scope of their activities or the business activity, size and type of the customer they deal with, as well as the type of product and services they offer, ensure the adoption adequate policies and procedures and keep them up-to-date, so that these policies and procedures reflect their risk assessment and contain adequate measures aimed at mitigating risks to an acceptable level. Also, the reporting entities shall ensure that these policies and

procedures are implemented efficiently, that they are effective and understood by all relevant employees. When establishing the system for the prevention of money laundering and terrorist financing, the reporting entities shall, by implementing the abovementioned internal acts, determine the organisational structuring, procedures (functional connection) of all parts of the system for the prevention of money laundering and terrorist financing, as well as the implementation of necessary actions and measures and the execution of 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 implementation of risk management through the use of policies, procedures and controls is specified by the Law (Article 14).

The establishment of a risk management system is aimed at protecting the reporting entity's system from possible misuses of the system for the purposes of money laundering and terrorist financing by customers or persons who perform occasional transactions. The scope of the system should be adequate to the assessed risk of exposure.

The reporting entities should ensure that they obtain the approval for their AML/CFT policies, controls and procedures from their senior management, and ensure that senior management has access to data, including insight into the risk assessment of the reporting entity's entire business, and that take an informed position on the adequacy and effectiveness of these policies and procedures, especially their policies and procedures regarding the CDD.

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.), or the reporting entity shall define in their policies and procedures, 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 requirements 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 Risk management measures

The reporting entities shall use automated systems to identify money laundering and terrorist financing risks associated with individual business relationships or occasional transactions and to identify complex and unusual transactions, and ultimately, to detect and report suspicious transactions. The system for the prevention of money laundering and terrorist financing must be adequate, depending on the size of the institution and their risk

profile or nature and scope of their business. The use of automated IT solutions should not be considered a substitute for employee vigilance and their obligations.

Where the risk associated with a business relationship or occasional transaction is increased, the reporting entities must apply EDD measures. These measures may include:

a) verifying the customer's and the beneficial owner's identity on the basis of more than one reliable and independent source.
b) identifying and verifying the identity of other persons that appear in the structure of the customer and who are not the customer's beneficial owner and/or any natural persons who have authority to operate an account or give instructions concerning the transfer of funds or the transfer of securities.
c) obtaining more information about the customer and the nature and purpose of the business relationship to build a more complete customer profile, for example, by carrying out open source or adverse media searches or commissioning a third party intelligence report. Examples of the type of information the reporting entities may seek include:
    i. the nature of the customer's business or employment;
    ii. the source of the customer's wealth and the source of the customer's funds that are involved in the business relationship, to be reasonably satisfied that these are legitimate;
    iii. the purpose of the transaction, including the destination of the customer's funds;
    iv. information on any associations the customer might have with other jurisdictions and the individuals who may influence its operations; or
    v. information on head office of the customer in another country, and explanation of the need to open an account outside their home jurisdiction.
d) increasing the frequency of transaction monitoring.
e) reviewing and, where necessary, updating information and documentation held more frequently.

5.2 Monitoring of business activities of the customer

The reporting entities should apply ongoing monitoring on business relationships with their customers and align them with the proper risk assessment that has been previously conducted.

Monitoring should include:

a) monitoring of transactions to ensure that these are in line with the customer's risk profile, their financial situation, and the reporting entity's wider knowledge of the customer to detect unusual or suspicious transactions; and
b) keeping the documents, data or information they hold up to date, with a view to understanding whether the risk associated with the business relationship has changed and to ascertain that the information that forms the basis for ongoing monitoring is accurate.

The reporting entities should determine the frequency and intensity of monitoring on a risk-sensitive basis, taking into account the nature, size and complexity of their business and the level of risk to which they are exposed.

5.2.1 Transaction monitoring

An effective transaction monitoring system relies on up-to-date and accurate customer information and should enable the reporting entity reliably to identify unusual and suspicious transactions and transaction patterns. The reporting entities should ensure that they have clear processes and automated systems in place (in accordance with the volume of turnover exceeding the possibility of human control factor) to review flagged transactions without undue delay.

The intensity/dynamics of monitoring shall depend on the nature, size and complexity of the reporting entity's business, as well as the risk to which the reporting entity is exposed. The reporting entities should adjust the intensity and frequency of monitoring in line with the risk-based approach. With a view to establishing the efficient monitoring system, the reporting entities should define clear criteria in a way to determine:

a) which transactions they will monitor in real time, and which transactions they will monitor ex-post. As part of this, it should be determined:
   - which high-risk factors, or combination of high-risk factors, will always trigger real-time monitoring; and
   - which transactions associated with higher ML/TF risk are monitored in real time, in particular those where the risk associated with the business relationship is already increased.
b) frequency of transaction monitoring.

In addition to real time and ex-post monitoring of individual transactions, and irrespective of the level of automation used, the reporting entities should regularly perform ex-post reviews on a sample taken from all processed transactions to identify trends that could impact their further risk assessments. Also, the reporting entities should test systems, and it they identify that it is necessary, subsequently improve the reliability and appropriateness of their transaction monitoring system, and ensure that the monitoring system is commensurate to the size and the nature of their business activity.

5.3 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 deputies for the activities of detecting and preventing money laundering and terrorist financing and submit documentation on their appointment to the administration authority.

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

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

Since the compliance officer for the prevention of money laundering and terrorist financing (hereinafter: 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 regulations shall be conditioned by meeting this obligation. There persons must have professional capacity for performing tasks of detecting and preventing money laundering and terrorist financing, and in particular, they must have professional knowledge for the operations of the reporting entities in the areas in which the risk of money laundering and terrorist financing exists, which is proven by completing the professional exam for performing the affairs of the compliance officer for the prevention of money laundering and terrorist financing (hereinafter: the training) and that such a person has passed professional exam for performing the affairs of the compliance officer for the prevention of money laundering and terrorist financing (hereinafter: the professional exam), and has a license for performing the affairs of the compliance officer for the prevention of money laundering and terrorist financing.

The Compliance Officer and their deputy are directly responsible to the management body or management or other similar body of the reporting entity, and are functionally and organisationally separated from other organisational parts of the reporting entity. The reporting entity provide the Compliance Officer and their deputy with spatial and technical possibilities for work that ensure the appropriate level of protection of confidential data and information handled pursuant to the Law, appropriate information and technical support for the implementation of activities, appropriate material conditions for work, regular professional training, as well as other conditions for effective detection and prevention of money laundering and terrorist financing.

The management body of the reporting entity shall provide the Compliance Officer with assistance and support in the performance of their work and report to the Compliance Officer on facts that are important for the prevention and detection of money laundering and terrorist financing.

A person may be designated as a Compliance Officer or their deputy, only with one reporting entity. Exceptionally, in the case when a director is appointed as a Compliance Officer (with a reporting entity with four or fewer employees), the same person may perform the duties of a Compliance Officer with several reporting entities in which they are both the director and the only employee.

The Law specifies in more detail the obligations and requirements (Articles 69 to 78) that relate to the Compliance Officers.

5.4 Internal controls and audit

Pursuant to the provisions of Article 80 of the Law, a reporting entity shall ensure regular internal controls and audit of the implementation of policies, controls and procedures for the prevention of money laundering and terrorist financing or performing tasks of the prevention and detection of money laundering and terrorism financing in accordance with the risk analysis and the identified risk in this area.

Internal controls and audit are aimed at preventing, detecting and correcting irregularities in the area of the prevention of money laundering and terrorist financing, and at improving policies, controls and procedures of the reporting entities for detecting transactions and persons associated with the money laundering and terrorist financing.

The internal audit and controls with the reporting entities, their reports and measures, control procedures and audits of the reporting entities in this area are the subject of regular examinations of their quality assessment by the CBCG and are of particular importance when determining the comprehensive assessment of individual reporting entities' systems.

In this regard, the reporting entity should ensure that the results or the findings of internal controls and audits, are taken into account in the reporting entity's risk management system, i.e. that they are incorporated into the process of regular risk analysis, as well as that the area of internal controls and audits is continuously improved in order to detect system irregularities in a timely manner and eliminate them.

5.5 Reporting to the administration authority on the transactions

5.5.1 Obligation of and deadlines for reporting to the administration authority of cash transactions and cashless transactions in the amount of EUR 100,000 or more

A reporting entity shall submit accurate and complete data to the financial-intelligence unit on CDD measures for each cash transaction in the amount of EUR 15,000 or more or cashless transaction in the amount of EUR 100,000 or more, without delay, no later than within three business days following the day the transaction has been executed.

A reporting entity shall submit to the financial-intelligence unit accurate and complete data obtained through implementation of CDD measures as stipulated by the Law for each transaction in the amount of EUR 10,000 or more, which is executed on the accounts of legal and natural persons in high-risk third countries and if such transaction includes high-risk third country, without delay, no later than within three working days since the day of execution of the transaction.

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

A reporting entity shall refrain from executing the suspicious transaction, regardless of the amount, until the order of the financial-intelligence unit is passed, and they shall notify, without delay, the financial-intelligence unit thereof, and submit data on CDD measures, without delay, in the prescribed manner and state the deadline for their execution. Therefore, the reporting entities shall deliver data and information and report to the financial-intelligence unit on the reasons for suspicion of money laundering and terrorist financing or some other criminal activity or 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. In addition, the reporting entities shall submit accurate and complete data on CDD measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of the Law with regard to funds or other property for which they know or have reasons to suspect that represent property gains acquired by criminal activity or that are connected with money laundering or terrorist financing.

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 financial intelligence unit of a suspicious transaction prior to its execution the reporting entity shall report to the financial intelligence unit subsequently, but not later than the next working day following the day of the transaction execution. If the reporting entity submits 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 administration 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 the report on a suspicious transaction delivered to the administration 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.

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 administration 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.

In addition, if it is determined that there is a suspicion, or reasons to suspect that the origin, purpose, method and the objective of the transactions point to possible money laundering or financing, the Compliance Officer should prepare a description of the transaction, and without referring to a specific indicator from the list of indicators, forward them to the financial-intelligence unit.

Reasons for suspicion are a set of facts and circumstances based on the list of indicators referred to in Articles 82 and 83 of this Law or on information from publicly available sources or observations, on the basis of which a natural person can suspect, assume or reasonably conclude that a certain transaction, funds or other assets do not come from legal sources, that is, that these funds or other assets they do not represent legally acquired property or are intended for purposes that are punishable by law.

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 act 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.

The reporting entities shall continuously take steps to ensure that employees understand:

a) risk assessment and risk exposure in the entire business and how it affects their daily work;
b) policies and procedures for AML/TF, and the manner of their application; and
c) how to recognise suspicious or unusual transactions and activities and how to act in such cases.

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 required 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 the 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 ACTS AND PROCEDURES FOR REGULATING IN MORE DETAIL OPERATIONS OF A REPORTING ENTITY AIMED AT MANAGING RISKS OF MONEY LAUNDERING AND TERRORIST FINANCING AND MITIGATING THEM

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. they shall:

- adopt a policy in relation to this area (if possible link also the risk appetite to the policy)
- draw up an internal act on risk analysis in which they identify and assess risks taking into account the risk factors of an individual customer, group of customers, country or geographical area, business relationship, transaction, product, service or distribution channels that can be used for the purposes of money laundering or terrorist financing and that they are regularly, and at least once a year, updated and kept in accordance with the Law;
- update the risk analysis in accordance with the risk assessment for new products, services or distribution channels;
- determine the procedures related to the objectives, scope and operation of the money laundering and terrorist financing risk management system;
- prescribe the conditions for designating the compliance officer for the prevention of money laundering and terrorist financing and their deputy;
- define the procedures related to CDD measures;
- define the procedures for submitting data to the financial-intelligence unit in line with the Law;
- define the procedures for protection and keeping of data and record keeping;
- define the 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 governing data confidentiality;
- regulate in more detail in their internal acts, the manner of implementing video-electronic identification, and no later than within eight days following that of delivery of the administrative decision approving the implementation of video-electronic identification;
- regulate in their internal acts the procedures for refusing to establish a business relationship or terminating an already established business relationship if it cannot

implement CDD measures, i.e. assess that it cannot effectively manage the risk of money laundering and terrorist financing in relation to that customer;
- develop an internal act which establishes the procedures on acceptance of the identification of the customer and the beneficial owner of the customer through a third person;
- regulate in their internal act the procedures based on the risk analysis they apply in connection with the identification of a customer who is a politically exposed person or the determination of the beneficial owner of a customer who is a politically exposed person, as well as when monitoring the business of that customer and the beneficial owner;
- regulate in their internal act the criteria for recognising transactions that are complex or unusually large, as well as transactions that are executed in an unusual manner or that have no obvious economic justification or legal purpose or deviate from the usual or expected business of the customer, and for which it was not possible to assess whether they are suspicious transactions;
- regulate in their internal act modus operandi of the compliance officer for the prevention of money laundering and financing of terrorism and their deputy;
- prepare a professional training and development programme for employees, by the end of the first quarter of the current year, for that year;
- develop a programme of professional training and education of employees in the area of detection and prevention of money laundering and terrorist financing;
- regulate in their internal act the manner of conducting internal control and audit of the implementation of policies, controls and procedures for preventing money laundering and terrorist financing, and
- develop and regularly update the list of indicators for the identification of suspicious customers and transactions.

Internal policies and procedures for managing the risk of money laundering and terrorist financing must be commensurate with the scope and nature of the reporting entity's activities, the size and type of customers they operate with, as well as the type of products or services it provides.

If the reporting entity is a payment service provider (credit institution, electronic money institution or payment institution), they shall define the following in their internal acts:

- procedures for verifying the completeness of the data collected in accordance with Article 35 of the Law prescribing the obligations of the payer's payment service provider, and
- handling, including, as necessary, ex-post monitoring or real-time monitoring, in the event that the payment order format or the electronic message accompanying the transfer of funds does not contain accurate and complete information referred to in Article 35 of the Law.

If the reporting entity is an intermediary in the transfer of funds, they shall, using risk-based approach, draw up an internal act of handling, including, as necessary, ex-post monitoring or real-time monitoring, in the event that the payment order format or electronic message that following the transfer of funds do not contain accurate and complete data referred to in Article 35 of the Law.

The method of conducting security checks of employees in accordance with the law governing data confidentiality must be determined by internal rules and implemented in relation to all persons who fall into the category of persons to whom a license should be issued, in accordance with the description of the work performed. The aforementioned

checks are performed in accordance with the Law on Data Confidentiality and enabling regulations, in the manner and within the deadlines necessary to ensure the regular performance of business.

An overview of established policies and procedures of the reporting entities is given in the table below:

No.	Internal act	Legal provisions
1.	Money laundering/terrorist financing risk analysis	**Risk analysis** **Article 12** The risk analysis shall be made in writing and in electronic form and be proportionate to size of the reporting entity, as well as to a nature and a scope of its business. A reporting entity shall prepare the risk analysis on the basis of guidelines on risk analysis determined by the competent authorities referred to Article 131 paragraph 1 of the Law, in accordance with the regulation referred to in Article 15 of the Law and the National Risk Assessment. **Enhanced CDD measures in complex and unusual transactions** **Article 58** A reporting entity shall establish, by way of internal act, the criteria for recognising transactions referred to in paragraph 1 of this Article.
2.	Know-Your-Customer (KYC) procedure	**Customer due diligence measures** **Article 17** A reporting entity shall establish, by way of internal act, the procedure for implementing measures referred to in paragraphs 1 and 2 of this Article. **Implementation of CDD measures before establishing a business relationship** **Article 19** A reporting entity shall, by way of internal act, define the procedures for refusal of establishing the business relationship or termination of already established business relationship referred to in paragraphs 3 and 4 of this Article. **Video-electronic identification** **Article 24** A reporting entity shall define the manner of performing the video-electronic identification, by way of its internal act, in accordance with the act referred to in paragraph 19 of this Article, not later than eight days following the day of submission the administrative decision referred to in Article 25 paragraph 6 of this Law, which approves performing of video-electronic identification. **Obligations of reporting entities in case of obtaining data and documentation from a third party** **Article 34**

		A reporting entity shall, by way of internal act, define the procedures on acceptance of the identification of the customer and the beneficial owner of the customer through a third person. **Enhanced CDD measures on a customer or their beneficial owner who is a politically exposed person** **Article 56** A reporting entity shall, pursuant to guidelines referred to in Article 12 paragraph 5 of the Law, by way of internal act, define procedures which are based on risk analysis that he/she implements with reference to identification of a customer who is a politically exposed person or through identifying beneficial owner of a customer who is a politically exposed person, and also during monitoring of business operations of that customer and beneficial owner.
3.	Professional training and development programme	**Professional training and development** **Article 78** A reporting entity shall prepare, by the end of first quarter of the current year, professional training and development programme from paragraph 1 of this Article, for that year. The method of professional training and development of employees shall be defined by internal act of the reporting entity.
4.	Other policies and procedures in the area of money laundering and terrorist financing	**Money laundering and terrorist financing risk management** **Article 14** Policies, controls and procedures referred to in paragraph 1 item 2 of this Article shall include: 1) establishing the internal policies, controls and procedures with reference to: - objectives, scope and modus operandi of the system for managing the risk of money laundering and terrorism financing, - submitting data to the financial-intelligence unit in accordance with the Law, - protection and storage of data and record-keeping, - internal controls in the area of prevention and detection of money laundering and terrorism financing, - security checks of employees pursuant to the law governing data confidentiality, - designation of compliance officer for prevention of money laundering and terrorism financing and his/her deputy; **Working conditions for a compliance officer for the prevention of money laundering and terrorist financing** **Article 77** The modus operandi of the compliance officer for the prevention of money laundering and terrorist financing and their deputy shall be defined by internal act of the reporting entity. **Internal controls and audit** **Article 80** The manner of carrying out the internal controls and audit referred to in paragraphs 1, 2 and 3 of this Article shall be prescribed by the internal act of the reporting entity.

		Reporting entity's list of indicators for recognising suspicious customers and transactions **Article 83** A reporting entity shall develop their own list of indicators for recognising suspicious customers and transactions, taking into account the complexity and the size of the transactions that are executed by that reporting entity, an unusual manner of execution, value or connection of transactions that have no economic or legal purpose or that are not compliant or are disproportionate with the regular or expected business activities of a customer, and other circumstances related to the status and other characteristics of that reporting entity's customer. The list of indicators referred to in paragraph 1 of this Article must be stored in the documentation of a reporting entity.

The reporting entity may prescribe internal acts listed under number 4 in the table above in one or more documents that will together represent their programme for the implementation of measures for the prevention money laundering and terrorist financing.

Policies, controls and procedures in the area of the prevention of money laundering and terrorist financing are determined by the competent management body of the reporting entity. The reporting entity must ensure that the established internal acts in this area are understood and applied by employees in all business units, branches and undertakings majority-owned by the reporting entity, as well as that important data and information are exchanged between these organisational units and undertakings, with adequate protection mechanisms in place in accordance with the degree of confidentiality.

It is the reporting entity's duty to ensure the continuity of risk management by applying the aforementioned internal acts, regardless of possible changes in the composition of the management or employees, or regardless of changes in the structure of the reporting entity, as well as that the established system enables constant review and verification of exposure to risks in the area of money laundering prevention and terrorism financing.

8. THE METHOD OF PROTECTING AND KEEPING DATA AND RECORD-KEEPING

The protection of data collected in the procedures for applying obligations and procedures in accordance with the provisions of the Law is defined in detail in Articles 123 and 124 of the Law, while the record-keeping is defined in Article 117 of the Law.

V. 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 indicating the 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. CREDIT INSTITUTIONS AND FOERIGN CREDIT INSTITUTIONS' BRANCHES

Banks, credit institutions and foreign credit institutions' 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 actions and 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 aimed at recognising those for which there are reasons to suspect of money laundering or terrorist financing.

Risk analysis of the aforesaid institutions aims at recognising and identifying the exposures to money laundering and terrorist financing risk as well as business segments that should be prioritised 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 domestic or foreign legal person, business undertaking, entrepreneur, natural person, trust, other person, or an entity equal to it, carrying out a transaction or establishing business relationship with a reporting entity.

Credit institutions and branches of foreign credit institutions 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 product and service used by the customer;
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 Member States, 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 is stable;
- 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, game of chance, 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, car rental agencies, etc.);
- customer is from a country that does not comply with prevention of money laundering and terrorist financing standards;
- customer structure shows presence of 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 countries that are under sanctions or embargo;
- 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-profit organisations (NPOs that were assessed as high-risk in the National Risk Assessment or another adequate analysis and assessment by the relevant institutions (Financial Intelligence Unit, Central Bank of Montenegro…));
- 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.
- customers that have no economic or other activity in Montenegro, but the accounts are used for transactions concerning activities related to other jurisdictions (as payable-through accounts);
- re-export of goods and/or services (FATF guidelines: "Trade based money laundering common techniques").

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;
- customer is reluctant to provide CDD information or appears deliberately to avoid face-to-face contact;
- customer's evidence of identity is in a non-standard form for no apparent reason;
- customer's behaviour or transaction volume is not in line with that expected from the category of customer to which they belong, or is unexpected based on the information the customer provided upon opening the account;
- 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;
- if a customer provides vague explanations regarding the performance of transactions and support them with inadequate documents accompanying their implementation;
- 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, or on their own behalf but for the account of another person;
- 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.

1.2 Geographic 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 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;

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

- customer's property is 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.

1.3 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;

The product has limited functionality, for example in the case of:

- a fixed term savings product with low savings thresholds;
- a product where the benefits cannot be realised for the benefit of a third party;
- a product where the benefits are only realisable in the long term or for a specific purpose, such as retirement or a property purchase;
- a low-value loan facility, including one that is conditional on the purchase of a specific consumer good or service;
- a low-value product, including a lease, where the legal and beneficial title to the asset is not transferred to the customer until the contractual relationship is terminated or is never passed at all.

The product can only be held by certain categories of customers, for example pensioners, parents on behalf of their children, or minors until they reach the age of majority.

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 having no obvious economic justification;
- transactions relating to founders' borrowings to companies of which they are the beneficial owners;
- transactions relating to borrowings, or frequent borrowings, that are repaid in partial transactions, where it is difficult to track the justification;
- transactions relating to borrowings, or frequent borrowings, that are repaid in partial transactions, where it is difficult to track the justification;
- loans in large amounts in a short period of time, which do not correspond to the business nature of the customer;
- transactions based on the loan agreement, without recording the number and date of the agreement;
- circulation of borrowed funds within connected legal persons and their beneficial owners;
- transaction related to the refund of money based on a loan agreement whose repayment term has expired;
- customer's account is financed exclusively based on loan agreements;
- early repayment of loans, without economic justification;
- transactions based on a loan that are immediately, in the same or similar amount, given as a non-banking loan or a loan to other persons;
- transactions that were given as a loan that was later written off or closed by assignment, compensation etc.;
- transactions based on a loan linked to legal persons established in tax havens;
- transactions based on a loan given or received by a person with a bad reputation or negative statements in the media;
- transactions executed on the basis of a loan, where the borrower is a person who has not repaid a receivable to the lender from previously concluded loan agreements, and the terms agreed for the repayment of previously borrowed funds have expired;
- 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;
- the product allows payments from third parties that are neither associated with the product nor identified upfront, where such payments would not be expected, for example for mortgages or loans;
- the product places no restrictions on turnover, cross-border transactions or similar product features;
- transactions relating to payment of goods and services to customers originating in off-shore destinations and the documentation clearly shows that the goods originate 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.

1.4 Distribution channel risk factors

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

- The product is available only to customers who meet specific eligibility criteria set out by national public authorities, as in the case of state benefit recipients or specific savings products for children.

The following factors may contribute to **increasing** risk:

- non-face-to-face business relationships, where no adequate additional safeguards – for example electronic signatures, electronic identification means and anti-impersonation fraud checks – are in place;

b) reliance on a third party's CDD measures in situations where the bank does not have a long-standing relationship with the referring third party;

c) new delivery channels that have not been tested yet.

1.5 Joint or pooled accounts

A credit institution or a branch of a foreign credit institution which opens a joint or pooled account in order to administer funds that belong to the customer's own clients, shall apply full CDD measures, including treating the customer's clients as the beneficial owners of funds held in the pooled account and verifying their identities.

Where there is a higher risk of money laundering and terrorist financing, these institutions shall apply EDD measures.

1.6 Customers that offer services related to virtual currencies

Credit institutions and branches of foreign credit institutions should take into account the fact that providers engaged in exchange services between virtual currency and fiat currencies and Custodian Wallet Providers, the issuing or holding of virtual currencies/assets, or administering/managing present an area of higher ML/TF risk.

When deciding on entering into a business relationship with such customers, reporting entities should, as part of their ML/TF risk assessment of the customer, consider the general risk associated with virtual currencies/assets.

Credit institutions and branches of foreign credit institutions should consider, *inter alia*, the following as virtual currency businesses:

- Operating as a virtual currency trading platform that effects exchanges between fiat currency and virtual currency;

- Operating as a virtual currency trading platform that effects exchanges between virtual currencies;
- Operating as a virtual currency trading platform that allows peer-to-peer transactions;
- Providing custodian wallet services;
- Arranging, advising or benefiting from 'initial coin offerings' (ICOs).

To manage the ML/TF risk associated with virtual currencies, credit institutions and branches of foreign credit institutions shall always apply enhanced due diligence measures. At a minimum as part of their risk mitigation measures, reporting entities should:

- Obtain data and information from the customer to understand the nature of the business and the ML/TF risks it poses;
- In addition to verifying the identity of the customer's beneficial owners, carry out enhanced due diligence on customer's senior management, including consideration of any adverse information on customer's business activity;
- Understand the extent to which these customers apply their own enhanced customer due diligence measures to their customers either under a legal obligation or on a voluntary basis;
- Establish whether the customer is registered or licensed in a country in which an adequate system for the prevention of money laundering and terrorist financing in a third county is in place, and take a view on the adequacy of that third country's AML/CFT regime.

1.7 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 head 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 shall not establish, or continue a correspondent relationship with a bank or another credit institution 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 it is able to monitor transactions and undertake transaction verification measures and other related measures and actions envisaged in the Law.

The abovementioned imposes an obligation on the bank or another credit institution of another country 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 in the manner prescribed in Article 53 of the Law.

With regard to the abovementioned, the correspondent shall obtain data on the purpose of the services provided to banks and other credit institutions of a foreign country, what are the expected basis for services in accordance with the customers' structure, and the information on whether the provided banking services will be used by third persons.

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.

1.7.1 Product/service and transaction risk factors

The following factors may contribute to **increasing** risk:

- the account can be used by other respondent banks that have a direct relationship with the respondent but not with the correspondent ('nesting', or downstream clearing), which means that the correspondent is indirectly providing services to other banks that are not the respondent;
- the account can be used by other entities within the respondent's group that have not themselves been subject to the correspondent's mandatory due diligence;
- the service includes the opening of a payable-through account, which allows the respondent's customers to carry out transactions directly on the account of the respondent.

The following factors may contribute to **reducing** risk:

- the relationship is limited to a SWIFT Risk Management Application (RMA) capability, which is designed to manage communications between financial institutions;
- the products that include only parties to the correspondent relationship acting in a principal-to-principal capacity, rather than processing transactions on behalf of their underlying customers (for example in the case of foreign exchange services between two banks where the business is transacted on a on a principal-to-principal basis), not including a third party and without processing transactions for their own customers (e.g. in the case between the banks and where the settlement of a transaction does not involve a payment to a third party. In those cases, the transaction is for the own account of the respondent bank.

1.7.2 Respondent risk factors

The following factors may contribute to **increasing** risk:

- the respondent's AML/CFT policies and the systems and controls the respondent has in place to implement them are not in compliance with the internationally accepted standards;
- the respondent is not subject to adequate AML/CFT supervision;
- the respondent, its parent undertaking or an institution belonging to the same group as the respondent has recently been the subject of regulatory enforcement for inadequate AML/CFT policies and procedures and/or breaches of AML/CFT obligations;
- the respondent conducts significant business with sectors that are associated with higher levels of ML/TF risk;
- the respondent's management or ownership includes PEPs, in particular where a PEP can exert meaningful influence over the respondent, where the PEP's reputation, integrity or suitability as a member of the management board or key function holder gives rise to concern or where the PEP is from a jurisdiction associated with higher ML/TF risk. Particular attention should be paid to those jurisdictions where corruption is perceived to be systemic or widespread;
- the history of the business relationship with the respondent gives rise to concern, for example because the amount of transactions is not in line with what the correspondent would expect based on its knowledge of the nature and size of the respondent;
- the respondent´s failure to provide the information requested by the correspondent for CDD and EDD purposes, and information on the payer or the payee that is required under the Law.

The following factors may contribute to **reducing** risk:

- the respondent's AML/CFT controls are not less robust than those required by Law and that are applicable in Montenegro's system, and in the systems of countries that implement the FATF standards;
- the respondent is a part of the same group as the correspondent, is not based in a jurisdiction associated with higher ML/TF risk and complies effectively with group AML standards that are not less strict than those required by the Law, and that are applicable in Montenegro's system, and in the systems of countries that implement the FATF standards.

1.7.3 Geographical risk factors

The following factors may contribute to **increasing** risk:

a) the respondent is based in a jurisdiction associated with higher ML/TF risk:
   - identified as high-risk third country (the list of the Financial Intelligence Unit and internal list of reporting entities);
   - with significant levels of corruption and/or other predicate offences to money laundering and without adequate capacity of the legal and judicial system to effectively prosecute those offences (assessments of relevant international authorities);
   - with significant levels of terrorist financing or terrorist activities; or
   - without effective AML/CFT supervision;

b) the respondent conducts significant business with customers based in a jurisdiction associated with higher ML/TF risk;

c) the respondent's parent undertaking has its head office or is incorporated in a jurisdiction associated with higher ML/TF risk.

The following factors may contribute to **reducing** risk:

a) the respondent has its head office in an EU Member State with a positive report on the system for the prevention of money laundering and terrorist financing (FATF and MONEYVAL);
b) the respondent is based in a third country that has AML/CFT requirements not less robust than those required by the law of Montenegro, and that effectively implements those requirements.

The reporting entity shall obtain data specified in Article 53 and these Guidelines by inspecting identification documents and business documentation, submitted by the bank or credit institution from another country, and/or from public and other available data records (depending on the type of required data).

The reporting entity shall have in place a high-quality system for the prevention of money laundering and terrorist financing that shall contain developed policies and procedures enabling it to recognise and not allow performance of activity that is not in line with the purpose of opening the account and providing services announced by the bank or another financial institution. To this end, in addition to the above-mentioned mandatory factors, the reporting entity may by itself develop specific procedures that will additionally enable it to better assess the risk of establishing a business relationship, e.g. an overview of the structure of customers of those institutions in terms of the type of activity and their jurisdictions, an overview of the customer structure (share of residents and non-residents, as well as a customer overview by their business activity).

On the basis of the abovementioned elements/factors a correspondent bank/reporting entity shall decide on the level of risk, i.e. its exposure and the acceptability of establishing a business relationship with a bank or a credit institution of another country. In accordance with the determined initial risk, based on the abovementioned factors as well as the factors determined by the reporting entity, which influence the risk assessment of correspondent relationships, appropriate due diligence actions and measures shall be undertaken, and they should be documented.

1.7.4 Application of measures

All correspondent institutions shall apply CDD measures, as well as the EDD measures in line with the risk-based approach.

Therefore, correspondents must:

a) identify and verify the identity of the respondent and its beneficial owner. As a part of that, correspondents should obtain sufficient information on the business and reputation of the respondent in order to establish the level of ML risk associated with the respondent. Specifically, the correspondents should:
   - obtain information and data on respondent's management members and consider the relevance, for the purpose of preventing financial crime, of any negative information ad indication, as well as links that the respondent's management or owners may have with PEPs or other high-risk individuals; and
   - obtain information on the major business of the respondent, types of customers and quality of its systems and controls in the area of ML/TF (including information available on recent regulatory or criminal sanctions for AML/CFT failings). Where

the respondent is a branch, subsidiary or affiliate, correspondents should also consider the status, reputation and AML controls of the parent undertaking;

b) determine the standing and reputation of the respondent and the quality of the supervision of which it is a reporting entity (e.g. MONEYVAL and FATF reports);
c) assess the respondent institution's controls in the area of AML/CFT. This implies that the correspondent should perform a qualitative assessment of the respondent AML/CFT control framework, not just obtain a copy of the AML/CFT policy and procedures. This assessment should be appropriately documented. In accordance with the risk-based approach, where the risk is particularly high, and especially where the volume of correspondent banking transactions is substantial, the correspondent should consider on-site inspections and/or sample testing to make sure that the AML/CFT policies and procedures are efficiently implemented;
d) establish and document the nature of all services provided, as well as the responsibilities of each institution. This may include setting out in writing the scope of the relationship, what products and services will be provided and who can use the correspondent banking facility and how (e.g. if it can be used by other banks through their relationship with the respondent);
e) monitor the business relationship, including transactions, in order to identify changes in the respondent's risk profile and detect any unusual or suspicious behaviour, including the activities that are not in line with the purpose of services provided or that are in conflict with the obligations concluded between the correspondent and the respondent;
f) ensure that the CDD information they hold is up to date.

Since Article 53 provides that, prior to establishing a correspondent relationship with the respondent, the reporting entity shall obtain the written consent of the senior manager for establishing such business relationship, the reporting entity should, in the event that the respondent's risk level increases during the business relationship, establish that fact, and notify the management of the bank or another institutions thereof, supporting the notification with the assessment of risks and analysis of possible impact on the correspondent.

Correspondents must also establish that the respondent does not permit its accounts to be used by shell banks. This may include asking the respondent for confirmation that it does not deal with shell banks, having sight of relevant passages in the respondent's policies and procedures, or considering publicly available information, such as legal provisions that prohibit the servicing of shell banks.

The reporting entity shall regulate, by way of a contract, its responsibility and the responsibility of the respondent when concluding a correspondence relationship, which shall include the following:

- the products and services provided to the respondent;
- how and by whom the correspondent banking facility can be used (e.g. if it can be used by other banks through their relationship with the respondent), what the respondent's AML/CFT responsibilities are;
- how the correspondent will monitor the relationship to ascertain the respondent complies with its responsibilities under this agreement (for example through ex-post transaction monitoring);
- the information that should be supplied by the respondent at the correspondent's request (in particular for the purpose of monitoring the correspondent relationship) and a reasonable deadline by which the information should be provided – without

delay (taking into account the complexity of the payment chain or the correspondent chain).

In the case of correspondence relationships, the reporting entity shall apply EDD measures in the following cases:

- where a higher ML/TF risk has been established in the case of a correspondent relationship with a credit institution or another financial institution with head office outside Montenegro or in a high-risk third country, and
- where it assesses that in relation to a customer, group of customers, country or geographic area, business relationship, transaction, product, service and distribution channel there is or could be a higher ML/TF risk.

The reporting entity shall review and modify, and, if necessary terminate, the correspondent relationship with a credit institution which is a respondent in a high-risk third country. The reporting entity shall not establish or continue a correspondent relationship with a credit institution or another financial institution that has a head office outside Montenegro or in a high-risk third country in the following cases:

- the reporting entity failed to take EDD measures prescribed in Article 53 paragraphs 1 to 4 of the Law with regard to these institutions;
- the institution does not have in place the AML/CFT system controls or does not apply laws and other regulations in the area of prevention and detection of money laundering and terrorist financing;
- institution operates as a shell bank, i.e. establishes correspondent or other business relationships and executes transactions with shell banks.

2. FINANCIAL INSTITUTIONS INVOLVED IN FACTORING AND PURCHASE OF RECEIVABLES

In addition to the general part of these Guidelines, financial institutions involved in factoring and purchase of receivables shall apply provisions under this item, in order to be able to recognise risks pointing to suspicious transactions, customers, and business relationships and to manage those risks in the manner so as to prevent any activities that could be characterised as money laundering and terrorist financing.

Observed from the economic perspective, shall be 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 in purchase 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 recognising and identifying the exposures to ML/TF risk as well as business segments that should be prioritised in order to ensure efficient ML/TF risk management. The abovementioned analysis shall classify the customers of these institutions in one of the ML/FT risk categories:

- A (low risk)

- B (medium risk)
- C (high risk)

2.1 Customer risk

Customer shall mean a person to whom a financial institution dealing in factoring or 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 (factor) establishes a business relationship with a creditor and a debtor, whereby it undertakes adequate actions and measures related to the assessment of ML/TF risk for those persons;
- if the creditor or debtor, beneficial owners or authorised persons, resident or non-resident 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 funds of a creditor and debtor is easy to prove 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 creditor and debtor, beneficial owners or their authorised persons are residents and non-residents coming from countries and geographical areas which do not observe internationally accepted AML/CFT standards, which are not EU Member States, and customers that cannot be subject to simplified customer due diligence;
- if the origin of funds 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 prevailed 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 their unusual character or suspicion of money laundering and terrorist financing;
- 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 their unusual character or suspicion of money laundering and terrorist financing;
- 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 customers 'receivables) 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 customer;
- 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 analysis of creditworthiness of both the creditor and the debtor;
- if a financial institution dealing with factoring finance and purchase of receivables or a customer from a tri-party contract (factor, creditor and debtor) makes non-contracted amendments to the contract and requests a drafting of contract annex(es);
- if a debtor makes payments without supporting documentation 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 customer;
- 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 shall apply provisions under this point 3 in order to be able to recognise risks pointing to suspicious transactions and customers and to manage those risks in the manner so as to prevent any activities that could be characterised 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 customer 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 shall 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 categorised under predicate offences.

The following shall, in particular, be considered unusual circumstances referred to in item 1) above:

- 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 specific circumstances referred to in this item 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. the customer accepts a high rate, fee or interest, requires a transaction 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 sent or received does not correspond to customer`s income (if this is known);
- a customer is subject to high costs associated with 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.
- unexpected repayment of the subject of leasing before the deadline or in a short period of time compared to the date of conclusion of the contract.

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 head 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 linked to a higher ML/TF risk.

3.3 Product/service and transaction risk

H**igher-risk** transactions may be:

- economically unjustified transactions, 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 in 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. FINANC IAL INSTITUTIONS PROVIDING CREDITING AND CREDIT INTERMEDIATION SERVICES

Financial institutions involved in crediting and credit intermediation operations shall, in addition to applying the general part of these Guidelines, apply provisions under this item, in order to be able to recognise risks pointing to suspicious transactions, customers, business relationships and to manage those risks in the manner so as to prevent any activities that could be characterised as money laundering and terrorist financing.

These financial institutions offer crediting and credit intermediation services to micro, small and medium-sized business entities, natural persons, and entrepreneurs (hereinafter: the customers) that perform their business activity independently. Therefore, financial institutions offering crediting and credit intermediation services shall assess the risks of individual customers, groups of customers, countries or geographical areas, business relationships, transactions or products, services, and distribution channels, on the basis of ML/TF risk factors 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 recognising and identifying exposures to money laundering and terrorist financing risk as well as business segments that should be prioritised in order to ensure efficient money laundering and terrorist financing risk management. The abovementioned risk analysis shall classify the customers of these institutions shall be classified in one of the ML/FT risk categories:

- A (low risk)
- B (medium risk)
- 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 other person or an entity equal to it;
- if there is a crediting or credit intermediation involving undertakings 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;

- 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 is stable in the part of the discharge of undertaken obligations;
- 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 crteditworthiness has changed due to extraordinary circumstance and/or customer has found themselves in the situation where they 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 customers, beneficial owners or authorised persons who are politically exposed persons and foreign politically exposed persons, non-resident legal or natural persons for whom there are grounds for suspicion of money laundering and terrorist financing, etc.;
- 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;
- 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;
- a customer settles their obligations (e.g. arising from loan granted) 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:

- customer performs business activity or a transaction under unusual circumstances;
- if a customer provides vague explanations regarding the performance of transactions and supports them with inadequate documents accompanying their implementation;
- 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;
- 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 their credit commitments via their accounts held with more than one bank, or partially or entirely prepays their credit commitments;
- if a customer requests extraordinary amendments to the credit agreement;
- if a customer transfers the obligations arising from 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 in which the source of funds cannot be clearly proved;
- 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 EUR 15,000 but their total sum obligate the reporting entity to report them to the competent public authority because they exceed EUR 15,000;
- if customer having no guarantees or steady source of income prevail in the customer structure;

5. REPORTING ENTITIES PROVIDING ACTIVITIES OF CURRENCY EXCHANGE OFFICES

Reporting entities providing currency exchange services should have regard to the inherent risks of the currency exchange services which may expose them to significant ML/TF risks. Reporting entities should be aware that these risks stem from the simplicity of transactions, their speed and their often cash-based character. Reporting entities should also have regard to the fact that their understanding of the ML/TF risk associated with the customer may be limited due to the fact that they usually carry out occasional transactions rather than establish a business relationship.

5.1 Product/service and transaction risk

Reporting entities should take into account the following factors as potentially contributing to increased risk:

- The transaction is unusually large in absolute terms or compared with the economic profile of the customer;
- The transaction has no apparent economic or financial purpose;
Reporting entities should take into account the following factors as potentially contributing to reduced risk:
- The amount changed is low; reporting entities should note that low amounts alone will not be enough to discount TF risk;

5.2 Customer risk factors

Reporting entities should take into account the following factors as potentially contributing to increased risk:

a) The customer behaviour:
- the customer's transactions are just below the applicable threshold for CDD, in particular where these are frequent or within a short period of time;
- the customer cannot or will not provide information about the origin of the funds;
-the customer requests to exchange large amounts of foreign currency which is not convertible or not frequently used;
- the customer exchanges large quantities of low denomination notes in one currency for higher denominations notes in another currency; or vice versa;
- the customer's behaviour makes no apparent economic sense;
- the customer visits many premises of the same reporting entity in the same day (to the extent that it is known by the reporting entity);
- the customer enquiries about identification threshold and/or refuses to answer casual or routine questions;
- the customer converts funds of one foreign currency into another foreign currency;
- exchange of large amounts or frequent exchanges that are not related to the customer's business;

b) The customer's business activity
The customer business is associated with a higher ML/TF risk for example casinos, purchase/sale of precious metal and precious stones, scrap dealer, etc.;

5.3 Distribution channel risk factors

Reporting entities should take into account the following factors as potentially contributing to increased risk:
- The service is provided entirely online without adequate safeguards;
- The provision of services is conducted through an agent network.

5.4 Geographic risk

Reporting entities should take into account the following factors as potentially contributing to increased risk:
- The customer buys currency from an unusual location in comparison to his/her own location without any logical explanation;
- The customer buys currency that does not fit with what is known about the customer's country of citizenship or residence;
- The customer buys or sells a large amount of a currency from a jurisdiction associated with significant levels of predicate offences to ML or terrorist activity;

6. PAYMENT INSTITUTIONS

This part of Guidelines deals with payment institutions as providers of payment services that are required 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 shall apply high-risk factors characteristic for these reporting entities, as well as apply measures for the reduction of identified risks.

The nature of the payment service provision can expose payment institutions to ML/TF risk. This is due to the simplicity and speed of transactions, their worldwide reach and their often cash- based character. Furthermore, the nature of these services means that money remitters often carry out occasional transactions rather than establishing a business relationship with their customers, which means that their understanding of the ML/TF risk associated with the customer may be limited.

6.1 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 an international 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 contribute to **reducing** the ML/TF risk in payment institutions relates to funds transferred from an account that a payer has with a credit or financial institutions within the EU, but only those that implement adequate AML/CFT standards.

6.2 Customer risk factors

A person – user of a payment service provided by the payment institutions shall be considered a customer.

6.2.1 Customer nature

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

- 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;

- the customer's needs may be better serviced elsewhere, for example because the payment institution/ money remitter is not local to the customer or the customer's business.
- the customer´s activity could be associated with TF because the customer is publicly known to have extremism sympathies or is known to be linked to an organised crime group.

6.2.2 Customer behaviour

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

- the customer has used the services of the service provider for many years and customer's 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.

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

- 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 customer`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 increase of volume or number of transactions is not related to a usual pattern like salary remittance or another logical pattern;
- the customer provides inconsistent biographical data or identification documents containing inconsistent information.

6.3 Distribution channel risk factors

The following factors may contribute to **reducing** ML/TF risk:

- agents are themselves regulated financial institutions;
- the service can be funded only by transfers from an account held in the customer's name at an EEA credit or financial institution or an account over which the customer can be shown to have control.

The following factors may contribute to **increasing** ML/TF risk:

- if there are no restrictions to financing instruments, e.g. in case of cash or e-money product payments subject to exceptions under Article 40 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:
  i. represents more than one payment service provider;
  ii. 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;
  iii. carries out a significant number of transactions with payers or payees from jurisdictions associated with higher ML/TF risk;
  iv. appear to be unsure about, or inconsistent in, the application of group-wide ML/TF policies;
  v. 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 provided through an overly complex payment chain, for example with a large number of intermediaries operating in different jurisdictions or geographic areas.

6.4 Country or geographic area risk factors

The following factors may contribute to **increasing** ML/TF risk:

- the payer or the payee is in a country or a geographic area associated with high ML/TF risk;
- reporting entities should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation of weapons of mass destruction.
- the payee is a resident in a jurisdiction that has no, or a less developed, formal banking sector, which means that informal money remittance services, such as hawala, may be used as a means of payment.

6.5 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 terrorist financing by applying enhanced customer due diligence aligned with the size and complexity of the business and its transaction volume.

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

- systems to identify linked transactions, including those that might amount to a business relationship according to their policies and procedures, such as systems to identify series of transactions bellow EUR 1,000.00 which have the same payer and payee and an element of duration;
- systems to identify whether transactions from different customers are destined for the same payee;
- systems to permit as far as possible the establishment of the source of funds and the destination of funds;
- systems that allow the full traceability of both transactions and the number of users included in the payment chain.
- systems that identify whether a transfer is made to, or received from, a high risk third country; and
- systems to ensure that throughout the payment chain only those duly authorised to provide money remittance services can intervene.

In occasional transactions with high ML/TF risk, payment institutions should apply enhanced customer due diligence specified in Section 4.1 of these Guidelines (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 of these Guidelines (mandatory for all reporting entities).

6.6 Payment institution agents

Payment institutions providing payment services through agents shall adopt policies and procedures for the implementation of AML/CFT measures, accordingly they should know their agents.

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 (fit and proper analysis).
- 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 shall assess the risk level and take measures for its reduction.
- conducting professional training and development for agent employees in order to ensure their proper comprehension and management of ML/TF risk.

7. 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) shall apply high-risk factors characteristic for these institutions, as well as apply measures for the reduction of identified risks.

E-money institutions shall 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.

7.1 Product risk factors

E-money institutions shall 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;
- high or unlimited amount of funds to be stored on the e-money product/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 40 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 specifically to be accepted as a means of payment by merchants dealing in goods and services associated with a high risk of financial crime, for example 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);
- high-value cash withdrawals.

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 threshold alone may not be enough to reduce 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 product/account at 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 an account held in the customer's sole or joint name at an EEA credit or financial institution;

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

- it does not allow or strictly limits cash withdrawal;
- 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.

7.2 Customer risk factors

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

- the customer purchases several e-money products from the same issuer, frequently reloads the product or make several cash withdrawals in a short period of time and without an economic rationale;
- where distributors (or agents acting as distributors) are reporting entities themselves, the above-stated also applies to e-money products from different issuers purchased from the same distributor;
- the customer`s transactions are always just below the prescribed transaction limit;
- there are indications that the product is used by several persons 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).

7.3 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 that are not themselves reporting entities under the Law, where the e-money issuer:

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

7.4 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 of weapons of mass destruction.

7.5 Measures aimed at lowering ML/TF risk

Reporting entities should apply CDD measures to:

a) The owner of the electronic money account/ product; and
b) Additional card holders. Where products are linked to multiple cards, reporting entities should establish whether they have entered into one or more business relationships, and whether additional card holders could be beneficial owners.

Reporting entities note that the exemption under Article 40 does not extend to the obligation to conduct ongoing monitoring of transactions and the business relationship, nor does it exempt them from the obligation to identify and report suspicious transactions. This means that reporting entities should obtain sufficient information about their customers, or the types of customers their product will target, to be able to carry out meaningful ongoing monitoring of the business relationship.

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 the 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.
- systems that link e-money products to devices or IP addresses for web-based transactions.

7.6 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 goods;
- the verification of 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.

VI. ACTING IN RELATION TO CUSTOMERS THAT ARE NON-PROFIT ORGANISATIONS – NPOS

When assessing the risk profile of a customer or prospective customer that is a non-profit organisation (hereinafter: NPO) for the first time, reporting entities should ensure that they obtain a good understanding of the NPO's governance, how it is funded, its activities, where it operates and who its beneficiaries are. Not all NPOs are exposed in a similar way to ML/TF risk and that shall be the subject of state authorities' analysis and publication, and the reporting entities should take risk-sensitive measures in relation to the NPOs belonging to a riskier NPO category in order to understand:

a) who controls the customer and who its beneficial owners are. As part of this, reporting entities should identify the NPO's trustees or equivalents, its governing body and any other individual who has control or influence over the NPO. For this purpose, reporting entities should refer to information such as the legal status of the NPO, a description of the NPO's governance set-up and/or a list of the legal representative(s);

b) how the NPO is funded (private donations, government funds, etc.). For this purpose, reporting entities should obtain information about the donor base, funding sources and fundraising methods, such as annual reports and financial statements;

c) what the objectives of the customer's operations are. For this purpose, firms should refer to information such as the customer's mission statement, a list of its programmes and associated budgets, activities, and services delivered;

d) which categories of beneficiaries benefit from the NPO's activities (for example, refugees, legal entities that receive assistance through the services of the NPO or similar). Documentation gathered for this purpose may include mission statements or campaign-related documents;

e) what transactions the NPO is likely to request, based on its objectives and activity profile, including payment of staff or providers posted abroad, and the expected frequency, size, and geographical destination of such transactions. For this purpose, reporting entities should refer to information such as organisational charts, explanations of the organisational structure of the NPO, a list of jurisdictions where the staff is paid and the number of employees to be paid in each of them;

f) where the NPO conducts its programmes and/or operations, in particular whether the NPO conducts its activities only at domestic level, or in other jurisdictions associated with higher ML/TF risks (high-risk third countries). For this purpose, reporting entities should refer to information such as a list of all programmes, activities and services delivered by the NPO, as well as a list of geographical locations served, including its headquarters and operational areas. Reporting entities should also assess whether the NPO's transactions are likely to involve the execution of payments with a third-country institution.

1. RISK FACTORS

When identifying the risk associated with customers that are NPOs, reporting entities should consider at least the following risk factors and assess them on a risk-sensitive basis:

Governance and exertion of control

a) Does the NPO have a legal status under national law or the national law of another country? Is there any documentation that sets out its modalities of governance and identifies the NPO's trustees, members of the governing body or any other individuals who exert control over the NPO?
b) Does the legal structure of the NPO require the annual disclosure of financial statements?

Reputation/adverse media findings

c) To what extent is it difficult for reporting entities to establish the good reputation of the NPO and its managers? Is there a good reason why this may be difficult, for example because the NPO has been established only recently, for instance in the last 12 months?
d) Has the NPO been linked by relevant, reliable and independent sources to extremism, extremist propaganda or terrorist sympathies and activities?
e) Has the NPO been involved in misconduct or criminal activities, including ML/TF-related cases, according to relevant, reliable and independent sources

Funding methods

f) Is the NPO's funding transparent and accountable or difficult to trace? Does it publicly document its funding sources and are these subject to external audits?
g) Do the NPO's funding methods carry ML/TF risks? Does it rely entirely or largely on cash donations, crypto assets or crowdfunding? Or are the NPO's sources of funds channelled through the payments system?
h) Is the NPO funded partly or largely by private donors or donors from jurisdictions associated with higher ML/TF risks or high-risk third countries identified as having strategic deficiencies in their AML/CFT regime?

Operations in jurisdictions associated with higher ML/TF risks and high-risk third countries

i) Does the NPO operate or deliver assistance in jurisdictions associated with higher ML/TF risks or in high-risk third countries or in conflict zones?
j) In such situations, does the NPO rely on third parties or intermediaries to perform its activities? In this context, is the NPO able to monitor and have adequate oversight of the activities by these third parties?
k) Is the business relationship with the NPO likely to involve the execution of transactions with a respondent institution located in jurisdictions associated with higher ML/TF risks or in high-risk third countries?

Reporting entities should also consider at least the following factors that may contribute to reducing risks:

a) The roles and responsibilities of the NPO's governing body and its managers are clearly documented;
b) The NPO is legally required to annually disclose its financial statements or to issue an annual report that identifies the sources of funds, the main purpose of the NPO's activities and the categories of beneficiaries of its programmes;
c) The NPO can demonstrate it is or has been subject to independent reviews or external audits;
d) The NPO has a good public reputation according to relevant, reliable and independent sources;
e) The NPO receives funding from governments, supranational or international organisations that are not associated with high-risk third countries or with jurisdictions with higher ML/TF risks, and the source of its funds can be clearly established;
f) The NPO does not have in its regular activity any links with high-risk third countries, or if it has, the NPO can demonstrate that it has taken appropriate steps to mitigate the ML/TF risks (for instance, with the designation of staff responsible for AML/CFT compliance or the design of procedures to identify the NPO's categories of beneficiaries and assess the ML/TF risks associated therewith);
g) The NPO's activities and beneficiaries do not expose it to higher ML/TF risks;
h) The NPO only delivers assistance and support to individuals through direct material help, such as providing IT equipment or medical devices.

In the event the NPO is conducting activities in jurisdictions subject to EU or UN sanctions, reporting entities should establish whether the NPO benefits from any provisions related to humanitarian aid and derogations in EU/UN financial sanctions regimes, such as humanitarian exemptions or derogations. When deciding how to service these customers and in accordance with their own asset freezing obligations, reporting entities should obtain evidence that provide reasonable assurance that the NPO conducts its activities in these jurisdictions in line with the exemptions provided in the regime, or that it benefits from a derogation granted by a relevant competent authority.

2. GENERAL RULE

For initial screening purposes and for the purposes of screening throughout the business relationship, reporting entities should take the steps necessary to understand how the NPO operates and conducts its business activities. Reporting entities that are likely to have NGO customers, for example because they provide money transfer services or current account

services, should consider establishing a dedicated contact point for this specific category of customers to have a good understanding of the way the sector is set up and operates.

VII. DE-RISKING GUIDELINES

“De-risking” implies risk reduction by refusing to enter into business relationships or by making decisions to terminate business relationships with individual customers or groups of customers that are associated with a high ML/TF risk or refusing to execute transactions showing high ML/TF risk.

1. DE-RISKING

“De-risking” refers to a decision taken by reporting entities to no longer offer services to some categories of customers associated with higher ML/TF risk.

As the risk associated with individual business relationships will vary, even within one category, the application of a risk-based approach does not require reporting entities to refuse, or terminate, business relationships with entire categories of customers that are considered to present higher ML/TF risk.

Reporting entities should carefully balance the need for financial inclusion with the need to mitigate ML/TF risk.

As part of this, reporting entities should put in place appropriate and risk-sensitive policies and procedures to ensure that their approach to applying CDD measures does not result in unduly denying legitimate customers access to financial services.

Where a customer has legitimate and credible reasons for being unable to provide traditional forms of identity documentation, reporting entities should consider mitigating ML/TF risk in other ways, including by:

a) adjusting the level and intensity of monitoring in a way that is commensurate to the ML/TF risk associated with the customer, including the risk that a customer who may have provided a weaker form of identity documentation may not be who they claim to be; and

b) offering only basic financial products and services, which restrict the ability of users to abuse these products and services for financial crime purposes. Such basic products and services may also make it easier for reporting entities to identify unusual transactions or patterns of transactions, including the unintended use of the product; It is important that any limits be proportionate and do not unreasonably or unnecessarily limit customers’ access to financial products and services.

The abovementioned pertains in particular to vulnerable categories of customers, such as refugees, asylum seekers, migrants etc.

1.1 Risk assessment

Reporting entities should have in place internal controls and procedures in a manner that enables them to establish relevant risk factors and assessment of ML/TF risk associated with individual business relationships in accordance with these Guidelines.

In such procedure, reporting entities should make sure that the implementation of established policies, procedures and controls does not lead to an overall refusal to establish or termination of business relationships with entire categories of customers with which higher ML/TF risk has been established.

1.2 Enhanced customer due diligence

Reporting entities shall establish risk-based policies and procedures, in such a way that the necessity of applying customer (or potential customer) due diligence measures does not result in such customer being unjustifiably denied legal access to financial services. In this regard, reporting entities should define the criteria for determining and recording the reasons for which they will make a decision to refuse or terminate a business relationship, an/or refuse to execute a transaction.

In their internal policies, reporting entities should envisage mechanisms for reducing the ML/TF risk, which they will consider before making a decision to reject a customer in accordance with the assessment of the level of ML/TF risk. These mechanisms may include adjusting the level, frequency and intensity of monitoring business activities and applying target restrictions to products or services.

Reporting entities should clearly define in their internal acts in which situations the application of such risk reduction measures could be implemented.

Prior to deciding on refusing or terminating a business relationship, reporting entities should make sure that they have taken into account all possible risk reduction mechanisms that could reasonably be applied in that specific case, considering the ML/TF risk associated with the existing or potential business relationship.

1.3 Reporting and record-keeping

For the purposes of reporting, reporting entities should establish in their internal acts the criteria that will be used to determine justified reasons for suspicion of money laundering and terrorist financing, which could also include consideration of the existence of reasons for suspicion (and reports to the Financial Intelligence Unit) in the event of such situation of refusing to enter into a business relationship or to execute a transaction. Any decision on refusal or termination of a business relationship or refusal to execute a transaction, including the reason for doing so, should be submitted to the Central Bank by the reporting entities upon request.

1.4 Special provisions in connection with Chapter IV of the Law on Comparability of Fees Related to Consumer Payment Accounts, Payment Accounts Switching and Payment Account with Basic Features

In relation to the right to access a payment account with basic features, credit institutions that are required to offer such basic accounts should set out in their internal account opening policies and procedures how they can adapt their EDD requirements to take into account the fact that the limited functions of a payment account with basic features contribute to reducing the risk of a customer abusing those products and services for the purposes of financial crime.

In ensuring a non-discriminatory access to a payment account with basic features in accordance with Chapter IV of the Law on Comparability of Fees Related to Consumer Payment Accounts, Payment Accounts Switching and Payment Account with Basic

Features (OGM 145/21), credit institutions should ensure that, if there are digital solutions for concluding a business relationship, those solutions in accordance with the aforementioned law and these Guidelines, do not lead to the automatic refusal of the customer.

Over time, and as their understanding of the ML/TF risks associated with individual business relationships grows, credit institutions should update their individual customer risk assessments and adjust the scope of monitoring and the type of products and services available to that customer.

1.5 Adjusting the intensity of monitoring

Credit and financial institutions should set out in their policies and procedures how they adjust the level and intensity of monitoring in a way that is commensurate with the ML/TF risk associated with the customer and in line with the customer's risk profile.

In order to effectively manage the ML/TF risk associated with the customer, monitoring should include at least the following steps:

i. setting expectations of the customer's behaviour, such as the nature of the business relationship, as well as the amount, source and destination of transactions, so that the reporting entity is able to spot complex and unusual transactions;

ii. ensuring that the customer's account is reviewed regularly to understand whether changes to the customer's risk profile are justified;

iii. ensuring that any changes to the previously obtained EDD information that might affect the institution's assessment of the ML/TF risk associated with the individual business relationship are taken into account.

Reporting entity's internal policies and procedures should contain guidance on handling applications from individuals that may have credible and legitimate reasons to be unable to provide traditional forms of identity documentation. The internal acts should establish at least the following:

i. measures to be taken if the customer is a person seeking asylum under the Geneva Convention of 28 July 1951 relating to the Status of Refugees, the Protocol thereto of 31 January 1967 and other relevant international treaties, and cannot provide the credit and financial institution with a traditional form of identification, such as a passports or ID card. Reporting entities' policies and procedures should specify which alternative, independent documentation it can rely upon to meet its EDD obligations, where permitted by national law. These documents should be sufficiently reliable, i.e., up to date, issued by an official national or local authority and containing, as a minimum, the applicant's full name and date of birth.
ii. steps to take where the customer is vulnerable and cannot provide traditional forms of identification or an address, for example because the customer is a refugee under the 1951 Geneva Convention or other relevant international treaties, or does not have a fixed address. Reporting entities' policies and procedures should specify which alternative, independent documentation it can rely upon. This documentation may include expired identity documents and documentation provided by an official authority, such as social services or a well-established not-for-profit organisation working on behalf of official authorities (Red Cross or similar), which also provides assistance to this customer.

iii. similar steps may also be applied to individuals who are not granted a residence permit but whose expulsion is impossible for legal or factual reasons. Due to such situations, the internal acts of the reporting entity should define taking into account certificates or documentation produced by an official authority or by an organisation providing support or legal assistance to those individuals on behalf of an official authority. Such authorities may include social work departments, home affairs ministries and migration services. These documents may be used as proof that the individual cannot be expulsed expelled in accordance with national or EU law.

iv. in cases where the financial assistance is provided to persons referred to in items i.-iii. is made available in the form of prepaid cards, and where the conditions related to simplified due diligence specified in Section 2 of these Guidelines are met, reporting entities may, in their internal acts, provide for the postponement of the application of the initial EDD measures to a later date;

v. in cases where the persons referred to in items i. to iii. submit apply for access to a payment account, and are considered as presenting low ML/TF risks, reporting entities should, in their internal acts, enable the acceptance of alternative forms of identification documents, as well as the options for postponing the application of full EDD until after the establishment of the business relationship.

1.6 Targeted and proportionate limitation of access to products or services

Reporting entities' internal policies and procedures should include options and criteria for limiting the availability of specific products or services to customers, in relation to a specific customer or in accordance with risk assessment, and in accordance with other laws governing this matter. These internal acts should include the following options:

i. offer payment accounts with basic features; or

ii. impose targeted restrictions on financial products and services, such as the amount, the type or the number of transfers or the amount of transactions to and from third countries, in particular where these third countries are associated with higher ML/TF risk.

In relation to ML/TF risks associated with customers who are particularly vulnerable, such as the above described persons, reporting entities should ensure that their controls and procedures specify that possible limitations of products and services set out in item (ii) are applied taking into consideration the personal situation of the individuals, their exposure to ML/TF risks and their financial basic needs. In those cases, reporting entities' procedures should include the assessment of the following options to potentially mitigate the associated risks:

i. prohibition of granting loans or overdraft facilities;

ii. monthly turnover limits (unless the rationale for larger or unlimited turnover can be explained and justified);

iii. limits on the amount, the type and/or number of transfers (further or larger transfers are possible on a case-by-case basis);

iv. limits on the amount of transactions to and from third countries (while considering the cumulative effect of frequent smaller transactions within a set period of time), in particular where these third countries are associated with higher ML/TF risk;

v. limits on the size of deposits;

vi. limits on third party payments other than those made by the authority that disburses support for such customers;

vii. limits on payments received from third parties that the institution has not verified; and

viii. prohibiting cash withdrawals from third countries.

2. GENERAL RULE

Removing the risk by prohibiting entire categories of customers, without due consideration of individual customers' risk profiles, may be considered unjustified and a sign of inefficient ML/TF risk management.

POLITICALLY EXPOSED PERSON IDENTIFICATION TEMPLATE **Template PEP**

A politically exposed person, in the context of this Law, shall be a Montenegrin citizen performing public function (table 1 of this Template) and a foreign citizen nominated or assigned a public function by a foreign state or international organisation (table 2 of this Template) including their close family members and close associates.

Members of the immediate family of the politically exposed person shall be married or unmarried spouse, partner in a life community of persons of same sex, their direct blood relative to any degree or a collateral blood relative to the fourth degree or a relative by marriage to the second degree, adopter, adoptee, foster parent or foster child.

Close associate of a politically exposed person shall include:

1) a natural person who has joint beneficial ownership or property right or other ownership rights over a legal person or legal arrangements, established business relationship or other types of closer business relationships with politically exposed persons.
2) a natural person who is the sole beneficial owner of a legal person or legal arrangement in relation to which it is known that it was created for the benefit of a politically exposed person.

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 24 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.	president of a political party and their deputy, a member of presidency of a political party, and their deputies, member of an executive board, member of a general board and other officials of a political party;	YES	NO
4.	State Secretary, Director General of a ministry and Secretary of a ministry, director, deputy police director, head of Financial Intelligence Unit;	YES	NO
5.	President and a judge of the Supreme Court of Montenegro and president and a judge of the Constitutional Court of Montenegro;	YES	NO
6.	Supreme State Prosecutor, Special State Prosecutor and a prosecutor in the Supreme State Prosecutor's Office and Special State Prosecutor's Office;	YES	NO
7.	Member of the State Audit Institution Senate, and a member of Central Bank Council;	YES	NO
8.	director and deputy director of an administrative authority;	YES	NO
9.	mayor, president of a municipality, president of Assembly of the Capital, president of Assembly of Royal Capital and president of the municipal assembly;	YES	NO
10.	Director of the National Security Agency and director of the Agency for Prevention of Corruption;	YES	NO
11.	Ambassador, Consul, Chief of Staff, General and Admiral in the Armed Forces of Montenegro;	YES	NO
12.	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 24 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.	married or unmarried spouse, partner in a life community of persons of same sex;	YES	NO
2.	direct blood relative to any degree or a collateral blood relative to the fourth degree or a relative by marriage to the second degree;	YES	NO
3.	adopter, adoptee, foster parent or foster child.	YES	NO

Table 4

Are you a close associate of persons listed in tables 1 and 2 of this Template?			
1.	Do you have joint beneficial ownership or property right or other ownership rights over a legal person or legal arrangements, established business relationship or other types of closer business relationships, with a politically exposed person referred to in tables 1 and 2 of this Template?	YES	NO
2.	Are you the sole beneficial owner of a legal person or legal arrangement in relation to which it is known that it was created for the benefit of a politically exposed person referred to in tables 1 and 2 of this Template?	YES	NO

Table 5

The data submitted by the customer to the reporting entity upon the expiry of a period of 24 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 24 months as of the day the performance of the public function you were appointed to, ended?	YES	NO
2.	Please specify the function that you have performed, or other grounds based on which you were designated as a politically exposed person (immediate family member or close associate of a person who has performed the public function referred to in tables 1 and 2 of this Template, specify also the function of that politically exposed person). _____ _____		

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.

_____
Senior manager name and surname

_____ _____
Place and date Senior manager signature