LAW ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

DISCLAIMER

The consolidation provided below is only a provisional document and therefore does NOT represent an official document and/or version. It is provided only for information purposes. It confers no rights and imposes no obligations separate from those conferred or imposed by the legislation formally adopted and published in the Montenegrin language.

Date of last check: 15 April 2024

Pursuant to Article 82 paragraph 1 point 2 and Article 91 paragraph 1 of the Constitution of Montenegro, the Parliament of Montenegro of the 28th convocation, at the Fifth Session of the First Regular (Autumn) Session in 2023, on December 11, 2023, has passed the

THE LAW

ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING[1] *

I. BASIC PROVISIONS

Subject matter

Article 1

This Law shall regulate measures and actions undertaken for the purpose of preventing and detecting money laundering and terrorist financing, as well as affairs, powers and manner of work of the organizational unit of the state administration authority competent for internal affairs performing police affairs (hereinafter referred to as: “the Police”) which performs the activities related to the prevention of money laundering and terrorist financing (hereinafter referred to as: “the financial intelligence unit”) and other issues significant for the prevention and detection of money laundering and terrorist financing.

Money laundering

Article 2

[1] (Official Gazette of Montenegro, no. 110/23 of 12.12.2023)
* With the entry into force of this Law, the Law on the Prevention of Money Laundering and Terrorist Financing shall cease to be valid - "Official Gazette of Montenegro", no. 033/14 of 04.08.2014, 044/18 of 06.07.2018, 073/19 of 27.12.2019, 070/21 of 25.06.2021

Funded by the European Union and implemented by aed in cooperation with the European Commission.

For the purposes of this Law, money laundering shall, in particular, have the following meaning:

Conversion or transfer of money or other property, knowing that such money or other property are derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or assisting any person involved in the commission of such an activity to evade the legal consequences of that person's action;

Concealment or disguise of the true nature, source, location, movement, disposition or ownership of money or other property, rights related to money or other property, knowing that such money or other property are derived from criminal activity or from an act of participation in such activity;

Acquisition, possession or use of money or other property, knowing, at the time of receipt, that such money or other property were derived from criminal activity or from an act of participation in such activity;

Participation in, association to commit, attempt to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in items 1, 2, and 3 of this paragraph.

Activities referred to in paragraph 1 of this Article shall also be considered as money laundering when the person who performed such activities was obliged or could have known that the money or other property derived from criminal activities.

Activities referred to in paragraph 1 of this Article shall also be considered as money laundering when the money or other property that are the subject of money laundering were generated on the territory of another country, if the activities by which they were generated would constitute a criminal activity in Montenegro as well.

Terrorist Financing

Article 3

For the purposes of this Law, terrorist financing shall, in particular, have the following meaning:

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 organizations whose aim is to commit the acts referred to in indent 1 of this item or members of those organizations or individuals whose aim is to commit such acts, or
   - By terrorists or by terrorist organizations for any purpose;

2. Encouraging or assisting in providing or collecting the funds or property referred to in item 1 of this Article.

Reporting Entities

Article 4

Measures for preventing and detecting money laundering and terrorist financing shall be taken before, during and after the completion of any affairs of receiving, investing, converting, keeping, or other form of disposing of money or other property, or transactions.

Measures referred to in paragraph 1 of this Article shall be undertaken by legal persons, business organizations, entrepreneurs and natural persons carrying out business activities (hereinafter referred to as: reporting entities), as follows:

1) credit institutions and branches of foreign credit institutions;

2) subjects that perform the following activities of:

- purchase of claims;
- financial leasing;
- renting safe deposit boxes;
- factoring;
- issuance of guarantees and other assurances;
- granting loans and loan mediation;
- exchange services;

3) payment service providers and institutions dealing with electronic money seated in Montenegro;

4) the Post of Montenegro;

5) companies for the management of investment funds;

6) companies for the management of pension funds;

7) investment companies whose business activities are prescribed by the law regulating the capital market and that provide:

- Investment services on the capital market in Montenegro which include: the reception and transmission of orders in relation to one or more financial instruments; the execution of orders on behalf of customers; dealing on own account; portfolio management; investment advice; services related to underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis; services related to underwriting of financial instruments and/or placing of financial instruments without a firm commitment basis; operation of multilateral trading facility (hereinafter referred to as: "the MTF"); operation of organized trading facility (hereinafter referred to as: "the OTF");
- Ancillary services on the capital market in Montenegro which shall include: keeping and administrating financial instruments for the account of customers, including custody and related services such as funds/collateral management; granting credits and loans to an investor to enable him to carry out a transaction in one or more financial instruments, in case the transaction involves the company which grants loan or credit; providing general recommendations on capital structure, business strategy and related matters and services relating to merger and acquisition of share in undertakings; foreign exchange services where these are connected to the provision of investment services; research and financial analysis or general recommendations related to transactions in financial instruments; services related to underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis; investment services and activities, as well as ancillary activities related to the underlying assets contained in the financial derivatives, if related to investment and ancillary services;

8) Life insurance companies that have a license to perform life insurance business issued in accordance with the law;

9) Mediation companies, representation companies, and entrepreneurs – insurance representatives in the part related to life insurance;

10) Organisers of special games of chance;

11) Pawnshops;

12) Legal persons, business organizations, entrepreneurs and natural persons engaged in activity or affairs of issuance and management of virtual and fiduciary currencies, as well as wallet custody service providers;

13) Legal persons, business organizations, entrepreneurs, and natural persons engaged in the business activity or business of:

- Forfeiting;
- Auditing, independent auditor, accounting and providing tax counselling services;
- Providing services of founding legal persons and other business organizations, as well as business or fiduciary services;
- Management of property for third parties;
- Mediation in renting real estate in transactions where the monthly rent is EUR 10,000.00 or more;
- Construction of residential and business facilities;
- Issuance and management of payment instruments (e.g. checks, traveller's checks, credit cards, bank promissory notes, payment orders, debit cards), which are not considered payment services in accordance with the law governing payment operations;
- Granting loans and mediation in contracting granting loans activities;
- Investment, trade and mediation in real estate trade;
- Trade of motor vehicles if the payments are made or received in the amount of EUR 10,000.00 or more, regardless of whether it is one or several linked transactions;
- Trade of vessels and aircrafts, as well as related service activities, if the payments are made or received in the amount of EUR 10,000.00 or more regardless of whether it is single or several linked transactions;
- Organizing and conducting biddings, trading in works of art, precious metals and precious stones and precious metals and precious stones products, as well as other goods, when the payment is made or received in the amount of at least EUR 10,000.00 in single or several linked transactions.
- Storing or keeping works of art or trading or mediation in trade of works of art, when those affairs are preformed in ports, free zones or a warehouse, when the payment is made or received in the amount of at least EUR 10,000.00 in single or several linked transactions.

In the context of this Law, a lawyer shall also be considered a reporting entity in cases when:

1) providing legal assistance in planning and executing transactions for a customer related to:

- purchasing or selling of real estate or a business organization,
- managing money, securities or other property of a customer,
- opening or managing a bank account, savings deposit or the account for dealing with securities,

- collecting funds for founding, dealing with or managing a business organization,
- founding, dealing with or managing an institution, fund, business organization or other similar form of organization;

2) Executing a financial transaction or transaction concerning real estate on behalf and for a customer.

In the context of this Law, a notary shall also be considered a reporting entity when they prepare notarial acts and certify documents related to the activities referred to in paragraph 3 of this Article, as well as those related to loan agreements.

The Government of Montenegro (hereinafter referred to as: “the Government”) may define other reporting entities that shall undertake the measures referred to in paragraph 1 of this Article if, considering the nature and manner of carrying out activities or business, there is a higher risk of money laundering or terrorist financing.

The Government may exempt the organizers of certain games of chance, except for casinos, from the obligation to apply all or certain measures and activities defined by this Law in a certain part of the performance of work or activity, when, upon a conducted risk assessment, a lower risk of money laundering and terrorist financing is established.

The risk assessment referred to in paragraph 6 of this Article shall be based on the nature, method of carrying out, payment methods and volume of business of the subjects referred in paragraph 6 of this Article.

Use of Gender-Sensitive Language

Article 5

The expressions used in this Law for natural persons in the masculine gender shall imply the same expressions in the feminine gender.

Definitions

Article 6

For the purposes of this Law, the following definitions shall apply:

1) terrorist act means an act defined in the Protocols from the Annex to the International Convention for the Suppression of Financing of Terrorism, as well as the criminal act of terrorism and criminal acts related to terrorism prescribed in the Criminal Code of Montenegro, and any other act intended to cause death or serious body injury to a civilian or any other person that does not actively participate in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government of a state or an international organization to do or to abstain from doing any act;

2) terrorist means a person who:
- alone or with other persons attempts to commit or commits a terrorist act by any means, directly or indirectly,
- alone or with other persons, with intention, encourages or assists in the commission of a terrorist act,
- contributes to the commission of a terrorist act by a group of two or more persons acting with a common purpose and with the aim of continuing the commission of a terrorist act or having knowledge of the intention of a group of two or more persons to commit a terrorist act;

3) terrorist organization means a group of two or more persons, or terrorists, which has been established for a long period of time and acts organized for the purpose of committing criminal acts of terrorist, that are associated:
  - with the intention to attempt to commit or to commit a terrorist act by any means, directly or indirectly,
  - for the purpose of encouraging or assisting in the commission of a terrorist act,
  - for the purpose of organizing and directing other persons to commit a terrorist act,
  - for the purpose of contributing to the commission of a terrorist act by a group of two or more persons acting with the common purpose and the aim of further terrorist activity or having knowledge of the intention of a group of two or more persons to commit a terrorist act;

4) predicate offence means any criminal offence whose commission resulted in the acquisition of material benefit that may be the subject of criminal offence of money laundering;

5) criminal activity means any type of commission, or participation in the commission of any act that is prescribed as a criminal act;

6) customer means a domestic or foreign legal person, business organization, entrepreneur, natural person, trust, other person, or an entity equal to it, carrying out a transaction or establishing business relationship with a reporting entity;

7) other person, or an entity equal to it, means a person that joins or will join money or any other property for a certain purpose;

8) compliance officer for the prevention of money laundering and terrorist financing, or his deputy is a person designated by a reporting entity, authorized and responsible for implementing measures and activities undertaken for the purpose of preventing and detecting money laundering and terrorist financing;

9) credit institution means a business organization performing activities of receiving deposits and other repayable funds from the public and granting credits for its own account;

10) financial institution means the reporting entity referred to in Article 4, paragraph 2, items 1–9 of this Law;

11) financial group means a group consisting of:
  - the parent company with headquarters in Montenegro, subsidiaries and companies in which these companies have a direct or indirect participation in the capital or voting rights of at least 20% and are included in the annual consolidated financial statement in accordance with the law,
  - companies that are interconnected by joint management,
  - legal entities, i.e. natural persons who have a direct or indirect participation in the capital or voting rights of at least 20% in legal entities from the financial sector;

12) reasons for suspicion means a set of facts and circumstances based on the list of indicators referred to in Article 82 and 83 of this Law or on information from publicly available sources or observations, on the basis of which a natural person of average intellectual abilities can suspect, assume or reasonably conclude that a certain transaction, funds or other property do not derive from legal sources, i.e. that such funds or other property do not represent legally acquired property or are intended for purposes punishable by law;

13) financial information means any information or data on financial assets, movement of funds or financial business relationships, available to the financial intelligence unit for the purpose of preventing and detecting money laundering and terrorist financing;

14) financial analysis means operational and strategic analysis performed by the financial intelligence unit within the scope of performing its tasks defined by this Law;

15) operational analysis means all methods and techniques by means of which information are collected, stored, processed and estimated, with the view of providing support to criminal investigations and prosecutions, and is directed to individual cases and specific objectives or to appropriately selected information, depending on the type and volume of the received report and expected use of information after dissemination;

16) strategic analysis means trends and typologies of money laundering and terrorist financing and all methods and techniques by which information is collected, stored, processed and estimated, with the view of providing support for efficient and effective prevention and suppression of money laundering and terrorist financing;

17) collective custody account means an account that a participant member (user of the clearing and balancing system) opens in the system of the central clearing depository company as part of the performance of auxiliary services in accordance with the law governing the capital market, and where the ownership positions of individual owners, customers of the participant member, are kept as one aggregate position;

18) transaction means receiving, investing, converting, keeping or other form of disposing of money or other assets;

19) cash transaction means any transaction where a reporting entity receives cash from a customer or hands over cash to the customer for his possession and disposal;

20) occasional transaction means a transaction executed by a customer who is not in a business relationship with the reporting entity;

21) suspicious transaction means any transaction or attempt to execute a transaction of funds or property for which it is estimated that, based on indicators for recognising suspicious transactions and customers in accordance with this Law, bylaws adopted pursuant to this Law and internal procedures of reporting entities, or based on other objective circumstances and facts, there are reasons for suspicion that they represent material benefit obtained through a criminal activity, or that they are subjects of money laundering or are intended for terrorist financing;

22) risk of money laundering and terrorist financing means the risk that a customer will use the financial system for the purpose of money laundering or terrorist financing, or that a business relationship, a transaction, a product or service will indirectly or directly be used for money laundering or terrorist financing;

23) correspondent relationship means a relationship between:

- credit institutions where one credit institution as a correspondent provides banking services to the other credit institution as to a respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services, and
- between and among credit institutions and financial institutions including similar services that are provided through a correspondent institution to a respondent

institution, including relationships established for securities transactions or funds transfers;

24) shell (fictitious) bank means a credit institution, or other similar institution, registered in a country where it has no physical presence, it does not carry out activity, has no business premises, employees, managing bodies and management and which is not related to a financial group subject to supervision for the purpose of preventing and detecting money laundering and terrorist financing;

25) property means property rights of any kind, regardless of whether they refer to goods of corporeal or incorporeal nature, movable or immovable, securities and other documents (in any form, including electronic or digital), evidencing property rights;

26) funds mean a form of property and represent financial means and benefits of any kind, including:

- money, checks, virtual currencies, monetary liabilities, promissory notes, monetary remittances and other means of payment;
- funds deposited with a reporting entity;
- financial instruments, specified in the law governing capital market, which are traded through appropriate offering, including shares and stakes, certificates, debt instruments, bonds, guarantees and derived financial instruments;
- other documents which prove the right to the financial means or other financial sources;
- interests, dividends and other income from the funds;
- receivables, credits and credentials.

27) money means cash (domestic and foreign), funds in accounts and electronic money;

28) payer means a natural or legal person who has an account with a payment service provider and initiates the transfer of funds from that account and/or a natural or legal person who does not have an account but orders the transfer of funds;

29) payee means a natural or legal person who is the final recipient of the transferred funds;

30) provider of payment services means a credit institution, electronic money institution and payment institution;

31) transfer of funds means any transaction that is at least partially executed electronically by the payment service provider on behalf of the payer, with the aim of making these funds available to the payee at the payment service provider, regardless of whether they are the payer or the payee the same person and whether the payer's payment service provider and the payee's payment service provider are the same person, including the payment transaction being executed:

- by credit transfer, direct debit or money transfer, in the sense of the law regulating payment transactions,
- using a payment card, a payment instrument used to dispose of electronic money, a mobile phone or any other electronic or IT device with similar features;

32) intermediary in the transfer of funds means a provider of payment services that is not in a contractual relationship with the payer or the payee, but participates in the execution of the transfer of funds;

33) business relationship means a business, professional or commercial relationship related to the professional activities of reporting entities which is expected, at the time of its establishing, to be of a permanent nature, as well as the following:

- registration of customer for participation in the organizing games of chance system with organizers that organize games of chance via internet or another telecommunication means;
- conclusion of a contract on the purchase of investment units/shares in an investment fund, in accordance with the law governing the operation of investment funds,
- conclusion of contracts on the provision of investment and/or auxiliary services, in accordance with the law governing the capital market;

34) anonymous legal person means a foreign legal person with unknown owners and/or managers;

35) senior manager means a employed by a reporting entity and has sufficient knowledge of the reporting entity 's exposure to the risk of money laundering and terrorist financing and has the authority to make decisions that affect the reporting entity's exposure to risk and does not always have to be a member of the reporting entity 's management body or other managing body of the reporting entity;

36) group means a group of companies comprised of parent company, daughter companies and companies in which the parent company or the daughter company participate, as well as companies that are interconnected in accordance with the law regulating accounting;

37) person means a Montenegrin citizen, a foreigner and a domestic or foreign legal entity or another legal subject;

38) another subject of civil law means an organized group of individuals who pool or have committed to pool funds or other property for specific purposes;

39) organiser of games of chance means the organiser of games of chance in the context of the law regulating games of chance, as well as the organizer who has the consent of the competent authority for organizing those games via the Internet, or other telecommunication means;

40) insurance agent means a legal or a natural person that possesses a license for performing insurance representation activities issued by the regulatory authority competent for insurance activities;

41) trust means a person engaged in providing services to third parties, in particular:

- establishment of business organizations or other legal persons,
- performance of functions or the appointment of other person to act as a trustee of an express trust or similar foreign legal entity,
- provision of services related to a registered office, business address and other related services,
- performance of functions or enabling another person to carry out the tasks of the trustee of a fund or similar foreign legal entity that receives, manages or allocates property instruments for certain purposes, excluding investment and pension funds,
- performance of functions or the appointment of other person to perform the function of a nominee shareholder on behalf of another person other than a business organization listed on a regulated market that is subject to disclosure requirements pursuant to the EU law or the equivalent international standards;

42) distribution channel means the channel used for the supply of goods and services to end users;

43) electronic money means electronically, or magnetically, stored monetary value issued after the receipt of funds for the purpose of making payment transactions, which represents a claim on the issuer of such electronic money and which is accepted by a natural or legal person other than the electronic money issuer, except:

- money values stored on the instruments that can be used for purchasing goods or services only in the premises used by the issuer of such instrument or upon a commercial contract with an issuer, within the limited network of payment services providers or for a limited scope of goods and services;
- money values used for payment transactions conducted via telecommunication, digital or information technology device, where the purchased goods or service can be delivered and used through telecommunication, digital or information technology device, provided that the telecommunication, digital or information technology operator does not act only as an intermediary between the payment service user and the supplier of the goods and services;

44) anonymous electronic money means a payment instrument that allows (enables) anonymity to the payer and makes it impossible to monitor the transaction between the issuer of the electronic money and the payee;

45) cash means banknotes and coins that are in circulation as the legal tender.

46) virtual currency means a digitally expressed value that is not issued by the Central Bank of Montenegro or a state authority, is not necessarily attached to legally established currency and does not possess a legal status of money or currency, but is accepted by natural or legal persons as a means of exchange and can be bought, sold, exchanged, transferred and stored electronically;

47) fiduciary currency means a legal lender issued by a central bank;

48) legal person means a person that may establish permanent customer relationship with a financial institution or in some other way possess property (e.g. firm, corporation, foundation, partnership or business association and other equivalent structure and similar);

49) customer identification means the process of establishing and verifying customer’s identity;

50) establishing customer’s identity means a part of customer’s identification procedure that refers to the collection of data from personal documents of natural persons and their comparison with data from independent and objective sources or any other secure, remote or electronic procedures that are regulated, recognized, approved or accepted by the state, and for legal persons and business organizations, collecting data from appropriate documents and comparing them to the data in the register where the legal person is registered or with the data from other registers that keep records of legal persons;

51) verifying customer’s identity means a part of the customer identification procedure, which refers to the verification of the identity of natural persons by checking the photo from the natural person's identity document or the verification of data by electronic identification or video-electronic identification in accordance with this Law, and for legal persons and business organizations on the basis of a check of the register in which the legal person or business organization is registered or in another appropriate public register or by inspection of the original or certified photocopy of a document from the register in which the person or business organization is

registered or of the original or certified photocopy of another document from the appropriate public register;

52) custodian wallet provider means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, for the purpose of holding, storing and transferring virtual currencies;

53) crypto wallet means a wallet that serves to store a private cryptographic key and allows users to securely store, send and receive cryptocurrencies;

54) 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 in the context of this Law, or, according to the data from relevant international organizations it does not meet the international standards in the field of the prevention money laundering and terrorist financing;

55) identity document means an identity card and passport;

56) electronic identity document means an identity card and passport that contains a photograph of a person and a contactless chip containing the photograph, personal and other data of that person and that is issued by the competent authority;

57) records of issued personal documents means the records of issued identity cards and the record of travel documents kept by the state administration body responsible for internal affairs in accordance with the law;

58) electronic form of the document means any industry standard file format (pdf, docx, etc.);

59) residents mean:

- business organizations and other legal persons registered in Montenegro, except for their representative offices outside Montenegro,
- parts of foreign companies registered in the register of the competent authority in Montenegro,
- entrepreneurs and natural persons with their headquarters, or residence in Montenegro, who perform economic activity for their own account in order to gain profit and who are registered with the competent authority in Montenegro,
- Montenegrin citizens who reside in Montenegro continually for one year or longer,
- foreigners who, on the basis of a residence permit, stay in Montenegro continually for one year or longer,
- diplomatic, consular and other representations of Montenegro abroad, employees of those representations and members of their families, who are not foreigners;

60) non-residents mean persons who do not fall within the category of residents;

61) qualified provider of electronic trust service means a natural or legal person that provides qualified electronic trust services and meets the conditions for performing those services in accordance with the law regulating electronic identification and electronic signature;

62) electronic identification means a set of data, computer equipment (hardware) or computer program (software) that contain identification data in electronic form or connect a natural person, legal person or authority with such data, and which are used for authentication for a service in electronic form;

63) authentication means an electronic procedure that enables confirmation of the electronic identification of a natural or legal person or the origin and integrity of data in electronic form;

64) qualified certificate for electronic signature means a certificate issued by a qualified electronic trust service provider in accordance with the law governing electronic identification and electronic signature;

65) Internet Protocol address (IP address) means a unique number or string of characters that identifies a device on a computer network that uses the Internet Protocol for communication between users;

66) supervisory officer means an inspector, or a civil servant who performs supervision activities in accordance with the law regulating supervision;

67) ICAO Doc 9303 recommendations mean international recommendations, recognized in the European Union standards related to the issuance of identification documents.

II. NATIONAL RISK ASSESSMENT

Determining the National Risk Assessment

Article 7

National risk assessment of money laundering and terrorist financing (hereinafter referred to as: “the National Risk Assessment”) shall include:

- identification and assessment of the risk of money laundering and terrorist financing at the state level;
- typologies of money laundering and terrorist financing, in accordance with the recommendations of the Financial Action Task Force (FATF);
- identification of sectors and activities in which reporting entities should carry out in-depth measures of knowledge and monitoring of clients' operations and, as necessary, determination of measures to be taken in order to prevent money laundering and terrorist financing;
- identification of sectors and activities in relation to which the risk of money laundering and terrorist financing has been determined;
- determination of appropriate measures to prevent money laundering and terrorist financing based on identified risks and increasing efficiency in the distribution of available resources for control, mitigation and management of identified risks of money laundering and terrorist financing;
- proposal for the improvement of existing regulations in the area of prevention and detection of money laundering and terrorist financing for certain sectors and business activities, i.e. the adoption of new regulations, in accordance with the identified risks of money laundering and terrorist financing, as well as guidelines for instructing the reporting entities in such sectors and business activities for creating an assessment of the risk of money laundering and terrorist financing;
- data on the institutional structure and general procedures of the AML/CFT system, including data on the financial intelligence unit, the state administration body responsible for revenue affairs and the competent state prosecutor's office, as well as data on the available financial resources and human resources capacities of these authorities, to the extent to which these data are available.
- data on activities undertaken at the state level and data on financial resources and personnel capacities allocated to the fight against money laundering and terrorist

financing to the financial intelligence unit, competent authorities referred to in Article 96 paragraph 1 of this Law and competent supervisory authorities referred to in Article 131 paragraph 1 of this Law.

The National risk assessment shall be determined by the Government, at least once every four years.

The National risk assessment shall be updated as necessary.

Coordinating body for creating the National Risk Assessment

Article 8

For creating the National Risk Assessment and the management of identified risks, the Government shall establish a coordinating body that shall:

1) prepare the National Risk Assessment;
2) prepare the report on the identified national risks of money laundering and terrorist financing;
3) prepare proposals of the measures and action plan for mitigating and managing identified risks of money laundering and terrorist financing;
4) carry out the analyses in the area of money laundering and terrorist financing, prepare reports on the conducted analysis and harmonize the cooperation between competent authorities and organizations.

The coordination body referred to in paragraph 1 of this Article has a president, members, and a secretary.

The coordination body referred to in paragraph 1 of this Article shall be established for a period of four years, and the same persons cannot be the president, members and secretary of that body more than twice.

Coordination and harmonization of the work of the coordinating body referred to in paragraph 1 of this Article shall be carried out by the financial intelligence unit.

The manner of carrying out the tasks, as well as other matters of importance for the work of the coordinating body referred to in paragraph 1 of this Article shall be prescribed by the Government.

Publication of data from the National Risk Assessment

Article 9

Certain parts, or data from the National risk assessment can be marked with an appropriate classification level in accordance with the law regulating classified information.

The summary of the National risk assessment is published on the website of the financial intelligence unit and shall not contain data marked with classification level.

In order to facilitate its own assessment of the risk of money laundering and terrorist financing at reporting entities, the financial intelligence unit, in addition to the summary referred to in paragraph 2 of this Article, may also publish other data from the National Risk Assessment on its website.

Report on implementation of the National Risk Assessment

Article 10

The financial intelligence unit shall submit a report to the Government on the implementation of the National risk assessment at least once a year.

The report referred to in paragraph 1 of this Article shall in particular contain data on:

- institutional structure and general procedures of the AML/CFT system, including data on the financial intelligence unit, the state administration body responsible for revenue affairs and the competent state prosecutor's office, as well as data on the available financial resources and human resources capacities of these authorities, to the extent to which these data are available,
- activities undertaken at the state level, human resources capacities and financial resources that are needed by the financial intelligence unit, competent authorities referred to in Article 96 paragraph 1 of this Law and competent supervisory authorities referred to in Article 131 paragraph 1 of this Law, for the prevention of money laundering and terrorist financing.

III. OBLIGATIONS OF REPORTING ENTITIES

1. Measures and actions undertaken by reporting entities

Types of measures and actions

Article 11

A Reporting entity shall, when conducting their activities, undertake measures and actions in accordance with this Law, in particular the following:

1)to identify the risks and conduct risk assessment of money laundering and terrorist financing and establish policies, control and procedures and undertake activities for decreasing the risk of money laundering and terrorist financing;

2)to perform the identification of the customer, to monitor the business relation and control of the customer (hereinafter referred to as: "the client due diligence measures and monitoring the business of the customer");

3) to establish and verify customer’s identity on the basis of reliable, independent and objective sources and monitor customer’s business activities (hereinafter: establishing and verifying the identity of the customer and the monitoring of business relations and the control of the transactions of the customer);

4) to submit information, data and documentations on timely manner to the financial-intelligence unit;

5) to designate authorized officer for implementing measures of detection and prevention of money laundering and terrorist financing and their deputy, as well as provide conditions for their work;

6) to organise regular professional training and development of employees in the area of prevention of money laundering and terrorist financing;

7) to develop and regularly update the list of indicators for the identification of suspicious customers and transactions;

8) to keep records and ensure the protection and keeping of the data and documents obtained in accordance with this Law;

9) to establish and monitor a system that enables complete and timely response to the requests of the financial intelligence unit and competent state authorities in accordance with the Law;

10) to apply measures of detection and prevention of money laundering and terrorist financing in business units and companies that are majority-owned by reporting entities in foreign countries;

11) to take other measures and activities pursuant to this Law.

Risk Analysis

Article 12

A Reporting entity shall be obliged to identify the risks and to perform risk analysis of money laundering and terrorist financing:

- within 60 days since the date of its establishment, i.e. starting to preforming activities, to develop the risk analysis for determining the risk assessment of an individual customer, a group of customers, a country or geographic areas, business relation, transaction or product, services and distribution channels related to the possibility of misuse for the purpose of money laundering or terrorist financing (hereinafter referred to as: "the risk analysis) and update it regularly at least once a year and keep it in accordance with this Law,
- to perform risk analysis for new services, products or distributive channels and according to that assessment, to update the risk analysis,
- to determine categories of money laundering risk and terrorist financing, and
- based on the risk analysis, to make a new risk analysis of each customer, group of customer, state, geographic area, business relation, transaction, product, services or distributive channels which may be used for purposes of money laundering and terrorist financing.

The risk analysis may include the assessment of measures, actions, and procedures which reporting entity shall take for suppressing and revealing of money laundering and terrorist financing.

The risk analysis at least shall include the risk analysis from money laundering and terrorist financing with reference to complete business of reporting entity and risk analysis of money laundering and terrorist financing for any group or type of customer, business relation, services that reporting entity provides to a customer within their activity, i.e. transaction.

The risk analysis has to be made in written and in electronic form and has to be proportional to size of the reporting entity, as well as to a nature and a scope of their business.

A reporting entity shall prepare the risk analysis on the basis of guidelines on risk analysis determined by the competent authorities referred to in Article 131 paragraph 1 of this Law, in accordance with the regulation referred to in Article 15 of this Law and with the National Risk Assessment.

A reporting entity shall be obliged to submit the risk analysis to the competent supervising authority referred to in Article 131, paragraph 1 of this Law upon the request, within three days of the day of the reception of the request.

Lower and higher risk of money laundering and terrorist financing

Article 13

If a reporting entity assesses that a customer, business relation, transaction, product, service, distribution channel, state or geographic area present lower risk of money laundering or terrorist financing, they can apply simplified measures for establishing and verifying the identity of the customer, monitoring of business relations and the control of the transactions in accordance with the provisions of this Law.

If a reporting entity assesses that a customer, business relation, transaction, product, service, distribution channel, state or geographic area present higher risk of money laundering or terrorist financing, they shall apply enhanced measures for establishing and verifying the identity of the customer, monitoring of business relations and the control of the transactions in accordance with this Law.

Money laundering and terrorist financing risk management

Article 14

A reporting entity shall be obliged to establish the system of risk management with reference to money laundering and terrorist financing, by which implementation risks, established through risk analysis will be diminished, which particularly includes:

1) Risk analysis;

2) Adoption and implementation of internal acts on policies, controls and procedures with a view of effective risk management of money laundering and terrorist financing;

3) Continuous monitoring and supervision over established risks of money laundering and terrorist financing; and

4) Establishing an appropriate internal organization, i.e. organizational structure of a reporting entity, proportional to the scope and nature of activities of a reporting entity.

Policies, controls, and procedures referred to in paragraph 1, item 2 of this Article shall be proportional to the scope and nature of activities of a reporting entity, size, and type of customers, as well as to types of products, i.e. services which the reporting entity provides.

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:

- aims, scope and ways of work of system for managing the risk of money laundering and terrorist financing,
- measures of customer due diligence and monitoring the client's business,
- submitting data to the financial intelligence unit pursuant to the law,
- protection and storage of data and keeping records,
- internal controls in the area of prevention and revealing money laundering and terrorist financing,
- security checks of employees pursuant to the law governing data confidentiality,
- designation of compliance officer for prevention of money laundering and terrorist financing and their deputy;

2) Establishing an independent auditor function or designating a person for continuous monitoring and supervision over the established risks of money laundering and terrorist financing, as well as checks of internal policies and procedures referred to in item 1 of this paragraph, proportional to the scope and nature of activity of a reporting entity.

Policies, controls, and procedures referred to in paragraph 1, item 2 of this Article shall be defined by competent managing authority to reporting entity.

Internal policies, controls and procedures referred to in paragraph 3 item 1 of this Article within the reporting entities regarded as a big legal entity in terms of this Law governing accounting shall be established by a high level manager.

A reporting entity shall be obliged to, proportional to the scope and nature of activities, designate a compliance officer for prevention of money laundering and terrorist financing in a managerial position.

A reporting entity shall prepare policies, controls and procedures referred to in paragraph 1, item 2 of this Article according to guidelines for establishing the system for risk management of money laundering and terrorist financing, defined by supervising body referred to in Article 131, paragraph 1 of this Law pursuant to Regulation referred to in Article 15 of this Law and the National Risk Assessment.

Regulation on guidelines for risk analysis and establishing the system for risk management

Article 15

Closer criteria for drafting the guidelines for risk analysis, depending the size and way of organization of reporting entity, scope and nature of affairs, types of customers, products, distributive channels, i.e. services that reporting entity provides, criteria for establishing risk factors, mandatory elements which risk analysis shall include and other elements of importance for drafting the guidelines for establishing the system for risk management of money laundering and terrorist financing shall be prescribed by the state body responsible for interior affairs (hereinafter referred to as: "the Ministry").

Professional basis for drafting the regulation referred to in paragraph 1 of this Article shall be prepared by the financial intelligence unit, along with opinion obtained from supervision bodies referred to in Article 131, paragraph 1 of this Law.

New services, products or distributive channels

Article 16

A reporting entity shall be obliged to assess the risk of money laundering and terrorist financing with reference to a new service, product, or distributive channel, which it provides within its activity, new business practice, as well as ways of providing a new service, products, or distributive channel, before their introduction.

A reporting entity shall be obliged to assess the risk of money laundering and terrorist financing with reference to use of modern technologies in providing the existing or new services, products, or distributive channels.

A reporting entity shall be obliged, based on updated risk analysis, to take additional measures for mitigating the risk and risk management of money laundering and terrorist financing referred to in paragraph 1 and 2 of this Article.

2. Identification of the customer and monitoring of business relation and the control of the transactions of the customer

Customer due diligence measures and monitoring the business of the customer

Article 17

A reporting authority shall be obliged to conduct customer due diligence measures (hereinafter referred to as: “the CDD measures”) the customer and monitoring the business of the customer, especially to:

1) Identify the customer;
2) Establish beneficial owner of customer and verify his identity including the measures necessary to determine ownership and control structure of the customer in cases defined by this Law;
3) Obtain data on the purpose and nature of a business relation or purpose of transaction and other data in accordance with this Law;

4) Monitor regularly the business relation, including control of the transactions undertaken with the reporting entity by the customer during the business relation in order to allow that transactions undertaken in accordance with knowledge of the reporting entity on customer, his/her business profile and risk profile of that customer and, if applicable on the source of these assets, as well as data, information and documentation on that customer are updated.

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

Reporting entity shall be obliged to implement all measures referred to in paragraphs 1 and 2 of this Article, proportionate to the risk of money laundering and terrorist financing.

When determining the scope of application of measures referred to in paragraphs 1 and 2 of this Article, the reporting entity shall be obliged to, at least, take into consideration the following:

1) the purpose of the conclusion and the nature of the business relation;

2) the amount of funds, the value of the property or the scope of the transaction;

3) the duration of the business relation;

4) the compliance of the business with the purpose of the conclusion of the business relation.

A reporting entity shall, in its internal acts, establish procedures for conducting measures referred to in paragraphs 1 and 2 of this Article.

A reporting entity shall be obliged to submit to the supervision authorities referred to in Article 131 paragraph 1 of this Law, at their request, appropriate analysis, documents, and other information proving that the measures were implemented in accordance with the identified risk of money laundering and terrorist financing.

If the reporting entity cannot implement one or more measures referred to in paragraph 1 of this Article, they shall be obliged to inform the financial intelligence unit about it, in the manner prescribed by the act referred to in Article 66, paragraph 15 of this Law.

Cases in which customer due diligence measures are conducted

Article 18

A reporting entity shall conduct the customer due diligence measures and monitoring of customer’s operations:

1) when establishing a business relation with a customer;

2) when executing one or several linked occasional transactions in the amount of EUR 15,000.00 or more, regardless if it is about a single or more mutually connected transactions;

3) during each occasional transaction which, within the meaning referred to in Articles 35 to 38 of this Law, represents the transfer of funds in the value of EUR 1,000.00 or more;

4) when there is a suspicion about the accuracy or veracity of the obtained customer and beneficial owner identification data;

5)when there are reasons for suspicion that property originates from a criminal activity or money laundering or terrorist financing in relation to the transaction, client, funds or assets, regardless of the amount of the transaction;

6) for natural or legal persons trading in goods, when executing occasional cash transactions in the amount of EUR 10.000.00 or more, regardless of whether the transaction is executed as a single transaction or a number of mutually linked transactions.

7) when paying out winnings, i.e. paying stakes, when executing one or more related transactions in the amount of EUR 2,000.00 or more, when the reporting entity is the organizer of games of chance.

The reporting entity shall be obliged to periodically carry out the CDD measures of the client's business in relation to clients with whom he has already has established business relations, based on the money laundering and terrorist financing risk assessment, or when certain circumstances change in relation to the client, or when the reporting entity, on the basis of any kind of legal obligations is obliged to make contact with the client during the relevant calendar year in order to verify all relevant information related to the real owner of the client or if the reporting entity was obliged to do so in accordance with the regulation governing the tax administration.

If the reporting entity, in addition to the existing business relationship, concludes an additional business relationship with the client or based on the existing business relationship, performs the transaction referred to in paragraph 1 items 2 and 7 of this Article, the reporting entity shall be obliged to obtain the missing data about that client, if they exist, regardless of the fact that he has previously implemented measures to know and monitor the customer's business.

A reporting entity shall be obliged, when implementing CDD measures and monitoring the business of the customer, in any case referred to in paragraph 1 of this Article, to obtain data on the customer, business relation and transaction referred to in Article 117 of this Law, depending the type of the reporting entity.

A reporting entity shall be obliged to provide information to the customer on the purpose of processing of data which they obtain when implementing CDD measures and monitoring of customer’s business, pursuant to the Law governing the personal data protection.

Implementation of CDD measures and monitoring customer’s business before establishing a business relation

Article 19

A reporting entity shall apply the measures referred to in Article 17, paragraph 1, items 1, 2 and 3 of this Law prior to establishing a business relation with a customer, including establishing and verifying the identity of person referred to in Articles 27 and 28 of this Law.

By way of exception referred to in paragraph 1 of this Article, a reporting entity can apply customer identity verification measures referred to in Article 17, paragraph 1, items 1 and 2 of this Law during the establishment of a business relation with a customer when a reporting entity estimates it is necessary for not interrupting the usual business and when there is insignificant risk of money laundering or terrorist financing.

If a reporting entity cannot conduct measures referred to in paragraph 1 of this Article, the business relation shall not be established, and if the business relation has already been established it shall be terminated.

A reporting entity shall not establish a business relation with the customer and if the business relation has already been established, the reporting entity shall be obliged to terminate that business relation if they assess that it cannot be managed efficiently by risk analysis of money laundering and terrorist financing with reference to this customer.

A reporting entity is obliged, with internal acts, to define the procedures for refusal of establishing the business relation or termination of already established business relation referred to in paragraph 3 and 4 of this Article.

Implementing CDD measures and monitoring of customer's business before performing a transaction

Article 20

When executing transactions referred to in Article 17, paragraph 1, items 1, 2 and 3 of this Law a reporting entity shall apply the measures referred to in Article 18 paragraph 1 items 2, 3, 6 and 7 of this Law before the execution of a transaction.

If the reporting entity cannot undertake the measures referred to in paragraph 1 of this Article, the transaction shall not be executed.

Identification of the beneficiary, i.e. beneficial owner of a life insurance policy

Article 21

A reporting entity referred to in Article 4, paragraph 2, item 8 and 9 of this Law can verify the identity of the beneficiary of a life insurance policy from the life insurance contract or after concluding of that agreement, but no later than the period of time when beneficiary according to life insurance policy can exercise their rights.

A reporting entity referred to in Article 4, paragraph 2, item 8 and 9 of this Law shall be obliged to verify the identity of the beneficiary under the policy referred to in paragraph 1 of this Article, in case when:

1) natural, i.e. legal person is nominated as a beneficiary, by taking data on their first and last name, i.e. name of the beneficiary;
2) the beneficiary has been appointed by characteristics, class or in any other way, by obtaining the information on that beneficiary to an extent sufficient for identification of the beneficiary at the time of payment.

Verification of identity of the beneficiary referred to in paragraph 2 of this Article shall be undertaken at the time of the payment.

When transferring the rights under the life insurance policy to the third party, partially or completely, the reporting entity shall be obliged to identify a new customer at the time of transferring the rights.

A reporting entity referred to in Article 4, paragraph 2, items 8 and 9 of this Law shall be obliged to define procedures by internal acts for implementation of measures referred to in paragraph 1 of this Article.

Identification of a natural person

Article 22

A reporting entity shall establish the identity of the customer who is a natural person, entrepreneur or a natural person who performs the activity pursuant to Article 18, paragraph 1 item 1 and Article 19 and 20 of this Law, by access to identity document, with their presence.

A reporting entity shall be obliged, in the procedure of establishing the identity referred to in paragraph 1 of this Article, to make an access to the data from an identity document and to check if those data complies with customer.

A reporting entity shall be obliged in the procedure of establishing the identity referred to in paragraph 1 of this Article, to obtain a photocopy of an identification document and to register date, time, first and last name of a person who made an access to photocopy of an identity document and to keep collected data pursuant to this Law.

When establishing the identity of the customer referred to in paragraph 1 of this Article, data on the customer shall be collected, on the way on which the identification of the customer has been performed and on business relation and transaction referred to in Article 117, paragraph 1, item 2, 3, 6 and 7 of this Law.

If all data referred to in paragraph 4 of this Article could not be provided, those data shall be provided by access to genuine document or into certified photocopy of other valid public document that customer presents or by access to a public registry.

If a legal attorney or compliance officer of the customer referred to in paragraph 1 of this Article establish employment relation or perform transaction on behalf of the customer referred to in paragraph 1 of this Article, the reporting entity shall be obliged to:

- establish the identity of that legal attorney or compliance officer pursuant to paragraphs 1 to 5 of this Article and to provide data on that person referred to in Article 117, paragraph 1, item 3 of this Law,
- provide data on the customer referred to in Article 117, paragraph 1 item 3 of this Law from the written Power of Attorney in original or certified photocopy of that Power of Attorney,
- check the data on customer which he/she obtained pursuant to indent 2 of this paragraph.

If the reporting entity, during identification of the customer referred to in paragraph 1 of this Article, i.e. of legal attorney or compliance officer referred to in paragraph 6 of this Article, doubts in veracity of collected detail or in credibility of the documents or other documentations from which the data have been collected, they shall be obliged to ask the written statement of the customer, attorney, i.e. compliance officer on veracity of those data.

The reporting entity may check data from identity documents through financial intelligence unit, through access to Central Registry of Population (hereinafter referred to as: “the CRP"), record of issued identity documents and into international base of stolen, lost and not valid documents, electronically.

If during the checks referred to in paragraph 8 of this Article it is established that data from an identity document are different than those in CRP, the reporting entity shall not establish a business relation, i.e. perform transaction.

After the identification of the client referred to in paragraph 1 of this Article, the reporting entity shall be obliged to enter information on the manner in which the identification was carried out in the records referred to in Article 117, paragraph 1 of this Law.

The manner of check referred to in paragraph 8 of this Article shall be prescribed by the Ministry.

The act referred to in paragraph 10 of this Article shall be marked with appropriate level of data confidentiality, pursuant to the law governing the data confidentiality.

Electronic identification

Article 23

Identification of the customer who is a natural person, entrepreneur or a natural person who performs activity, their legal attorney and compliance officer can be performed without obligatory physical presence, based on means of electronic identification with high level of security of the system for electronic identification or based on qualified certificate for electronic signature, issued by qualified provider of trust service, pursuant to the law governing electronic identification and electronic signature (hereinafter referred to as: “the electronic identification”).

Prior to electronic identification the customer shall obliged to provide to the reporting entity a photocopy of an identity document, and in the case of identification of the legal attorney, i.e. compliance officer, also a photocopy of Power of Attorney by which they prove the capacity of legal attorney, i.e. compliance officer, in electronic form.

Prior to electronic identification, the reporting entity shall be obliged to obtain data on customer, way on which the identification of the customer was carried out, business relation and transaction referred to in Article 177, paragraph 1, item 2, 3, 6 and 7 of this Law.

A reporting entity is obliged to check the data referred to in Article 117, paragraph 1, items 2, 3, 6 and 7 of this Law through financial investigative unit by access to CRP, into record of issued identity documents and into international base of stolen, lost and not valid documents, electronically, in way which is prescribed by the Act referred to in Article 22, paragraph 11 of this Law.

A reporting entity can perform identification electronically only for a service or for a product which they provide within their activity and for the customer for whom a high risk of money laundering and terrorist financing hasn’t been established.

Electronic identification cannot be performed if:

- during the check referred to in paragraph 4 of this Article it is established that data from the identity document of the person referred to in paragraph 1 of this Article are different from those in CRP;
- the means of electronic identification, i.e. qualified certificate for electronic signature referred to in paragraph 1 of this Article is issued under pseudonym;
- there is a reasonable doubt that means of electronic identification, i.e. qualified certificate for electronic signature of the person referred to in paragraph 1 of this Article is abused, i.e. if the reporting entity establishes that circumstances which substantially affect validity of that means of electronic communication, i.e. qualified certificate for electronic signature are changed and the service provider of electronic identification, i.e. qualified provider of electronic trust service has not revoked that means, i.e. certificate;

The electronic identity document referred to in paragraph 1 of this Article is issued in high-risk third country.

If, during the electronic identification, the reporting entity doubts in veracity of collected data or authenticity of documents from which the data have been collected, they shall be obliged to terminate the electronic identification.

In order to preform electronic identification, the reporting entity shall be obliged to provide:

- technical and other conditions which allow the check at any time whether the means of electronic identification, i.e. qualified certificate for electronic signature is valid;
- technical conditions which enable obtaining the data on the customer referred to in paragraph 1 of this Article, business relation and transaction referred to in Article 177, paragraph 1, item 2, 3, 6 and 7 of this Law and their checks pursuant to paragraph 4 of this Article,
- technical conditions for keeping records on performing electronic identification.

After the identification has been carried out electronically, the reporting entity shall be obliged to enter the information on the manner in which the identification of the person referred to in paragraph 1 of this article was carried out in the records referred to in Article 117, paragraph 1 of this Law.

Video-electronic identification

Article 24

Identification of the customer who is a natural person, entrepreneur or natural person who performs activity, their legal attorney and compliance officer can be performed remotely, through the procedure of video identification by use of means of electronic communication (hereinafter referred to as: “the Video-electronic identification").

Video-electronic identification can be performed only by reporting entity who completed special training for conducting video-electronic identification.

A reporting entity is obliged prior the start of video-electronic identification to provide compliance of the person referred to in paragraph 1 of this Article for the complete procedure of video-electronic identification, particularly for recording image and the sound and keeping of recorded material (hereinafter referred to as: “the video-audio record"), pursuant to the law, as well as for collecting data by electronic reading of electronic identification documents and transfer of data read via Internet.

The consent referred to in paragraph 3 of this Article shall be video and audio recorded.

A reporting entity shall be obliged to inform the person referred to in paragraph 1 of this Article on the obligation of obtaining the consent referred to in paragraph 3 of this Law and on the fact that giving the consent will be video and audio recorded.

The person referred to in paragraph 1 of this Law shall be obliged to provide a photocopy of electronic identity document which they will use during video-electronic identification, in electronic form.

When performing video-electronic identification, the reporting identity shall be obliged to perform electronic reading of data from the identity document, issued by competent authority and which is not issued in high-risk third country and to obtain the data on the person referred to in paragraph 1 of this Article, business relation and transaction referred to in Article 117, paragraph 1, items 2, 3, 6 and 7 of this Law.

By electronic reading of the data from electronic identity document, the reporting entity shall be obliged to obtain data on the entrepreneur, i.e. natural person referred to in Article 117, paragraph 1 items 2 and 3 of this Law, as well the digital image and digital reproduction of original signature of the customer according to recommendations of ICAO Doc 9303.

Data referred to in Article 117, paragraph 1, items 2 and 3 of this Article, which cannot be provided by electronic reading of electronic identity document pursuant to paragraph 8 of this Article, shall be obtained immediately from the customer in video-audio communication.

A reporting entity can check the data referred to in paragraph 8 and 9 of this Article, through financial intelligence unit, by access to CRP, register of issued identity documents and international database of stolen, lost and not valid documents, electronically, in way which is prescribed by act referred to in Article 22, paragraph 11 of this Law.

A reporting identity shall be obliged to keep the video-audio record which was created during video-electronic identification pursuant to this Law.

In case of video-electronic identification of the legal attorney, i.e. compliance officer of the customer prior to establishing of business relation, i.e. performing transaction, that legal attorney, i.e. compliance officer shall be obliged to show and to submit a photocopy of Power of attorney by which they proves the capacity of the legal attorney, i.e. compliance officer.

A reporting entity can perform the video-electronic identification only for the service or for the product which they provides within their activity and for the customer for whom a higher risk of money laundering and terrorist financing has not been established.

A reporting entity cannot perform a video-electronic identification an electronic identity document of the person referred to in paragraph 1 of this Article is issued in high-risk third country.

A reporting entity shall be obliged to terminate the video-electronic identification if:

- during the check referred to in paragraph 1 of this Article it is established that data from the identity document of the person referred to in paragraph 1 of this Article are different than those in CRP;
- doubts in veracity of collected data or authenticity of the documents from which the data have been collected;
- it is not possible to provide an uninterrupted transmission of image and sound or transmission of high quality;
- the premise where the person referred to in paragraph 1 of this Article stays is poorly lighted or there is a noise, due to which it is not possible to identify that person or it it is not possibly to hear clearly that person or employee;
- due to other disturbances in communication, transmission of the image and/or the sound or due to other circumstances, the employee cannot perform identification of the person referred to in paragraph 1 of this Article.

The identification of the person referred to in paragraph 1 of this Article can be performed in repeated procedure of video-electronic identification, only if the previous procedure is terminated due to circumstances referred to in paragraph 15 of this Article and only after removal of these circumstances.

After the video-electronic identification has been performed, the reporting entity shall be obliged to enter in the records referred to in Article 117, paragraph 1 of this Law information on the manner in which the identification of the person referred to in paragraph 1 of this Article was carried out.

A reporting entity shall be obliged to regulate the way of performing the video-electronic identification by their internal acts, no later than eight days from the day of submission the ruling referred to in Article 25, paragraph 6 of this Law, which approves performing of video-electronic identification.

Closer conditions and way of video-electronic identification, as well as manner of organizing and the content of a training referred to in paragraph 2 of this Article shall be prescribed by the Ministry.

Authorization for establishing the identity electronically and for video – electronic identification

Article 25

The reporting can carry out electronic identification, i.e. video-electronic identification of a client who is a natural person, an entrepreneur or a natural person performing an activity, their legal representative and an authorized person, only if they have permission to carry out electronic identification, i.e. video-electronic identification.

Request for issuing the authorization referred to in Article 1 of this Article, the reporting entity shall submit to the competent supervising authority referred to in Article 131, paragraph 1 of this Law.

Along with request referred to in paragraph 2 of this Article, the reporting entity shall be obliged to submit the evidence on fulfilment of conditions referred to in Article 23, paragraph 8 of this Law, i.e. conditions prescribed by the act referred to in Article 24 paragraph 19 of this Law.

A supervising authority referred to in Article 131 paragraph 1 of this Law shall submit the request referred to in paragraph 2 of this Article and evidence referred to in paragraph 3 of this Article to the financial intelligence unit.

The head of financial intelligence unit shall create an interagency commission, which establishes the fulfilment of conditions referred to in paragraph 3 of this Article.

Upon proposal of Commission referred to in paragraph 5 of this Article, the head of financial intelligence unit, upon request referred to in paragraph 2 of this Article, shall adopt the decision by which authorizes, i.e. refuse to the reporting entity, the performing of electronic identification, i.e. video- electronic identification.

Commission referred to in paragraph 5 of this Article shall propose adoption of decision by which overrules the request referred to in paragraph 2 of this Article if it establishes that that a specific service or product represents higher risk of money laundering and terrorist financing for the purpose of this Law.

Administrative dispute can be initiated against decision resolution referred to in paragraph 7 of this Article.

Commission referred to in paragraph 5 of this Article shall be consist of representatives of the financial intelligence unit, other organizational units within the Ministry and supervising authorities referred to in Article 131, paragraph 1, items 1, 3, 4 and 8 of this Law.

Commission referred to in paragraph 5 of this Article shall have the President, members and Secretary.

To the President, members and to the Secretary referred to in paragraph 5 of this Article shall have the right to a monthly fee in the amount of 25% of an average gross salary in Montenegro in the previous year, according to data of the administrative authority competent for statistical affairs, which is paid in net amount.

The form and content of the request referred to in paragraph 2 of this Article and way of work of the Commission referred to in paragraph 5 of this Article shall be prescribed by the Ministry.

Identification of a legal entity and business organization

Article 26

A reporting entity shall be obliged to establish the identity of a customer that is a legal person or a business organization, pursuant to Article 19 and 20 of this Law, and obtain the data referred to in Article 117, paragraph 1, items 1, 6 and 7 of this Law of the legal person or business organization that establishes a business relationship or executes a transaction, that is, a legal entity or a business entity for which a business relationship is established or a transaction is executed.

Data referred to in paragraph 1 of this Article can be obtained by the reporting entity from the Central Business Registry (hereinafter referred to as: “the CBR”) or checking other appropriate public register, as well as checking court, business or other public register of a foreign legal person or business organization.

A reporting entity can obtain data referred to in paragraph 1 of this Article by checking the CBR or other appropriate public register, as well as by access to original or into certified photocopy of the document from court, business or other public register where the foreign legal person or business organization is registered, which, on behalf of the legal entity or business organization shall be presented its attorney or compliance officer and which shall not be older than three months of its issue date.

A reporting entity shall keep the original or certified photocopy of the costumer's document in its files.

When accessing the registers referred to in Article 2 of this Law, the reporting entity shall be obliged to print the excerpts from those registers and to mark the date and time and first and last name of the person who has accessed the register.

The data which is not included in the registries referred to in paragraph 2 of this Article, i.e. in documents referred to in paragraph 3 of this Article, the reporting entity shall obtain by accessing the original or certified photocopy of the document or other documentation submitted to him/her by the attorney or compliance officer of the customer referred to in paragraph 1 of this Article.

If reporting entity, during establishing the identity of the legal entity or business organization doubts in veracity of obtained data or in authenticity of documents or public or other documentations from which the data have been obtained, they shall be obliged to, before establishment of business relation or performing transaction, obtain also a written statement on veracity of these data.

If the customer is a foreign legal person who performs activity in Montenegro through their business unit, the reporting entity will establish the identity of the foreign legal person and their business unit.

Establishing the identity of the attorney of a legal person and business organization

Article 27

The reporting entity shall be obliged to establish the identity of the attorney of the customer who is a legal person or business organization pursuant to Article 22 of this Law.

The reporting entity shall be obliged to obtain the data on all directors of the legal person or business organization referred to in Article 117, paragraph 1 item 3 of this Law.

The reporting entity shall be obliged, in the procedure of establishing and checking the power of attorneys of the attorney and all directors referred to in paragraph 2 of this Article to obtain those power of attorneys and to keep them in their documentation.

If the reporting entity has updated data on directors referred to in paragraph 2 of this Article, they are not obliged to obtain again the data on them.

Establishing the identity of the compliance officer of a legal person and business organization

Article 28

If in the name of the attorney of the customer who is a legal entity or a business organization and in the name of all directors of that legal entity, i.e. business organization, a compliance officer establishes business relation or performs transaction, the reporting entity shall establish the identity of that compliance officer pursuant to Article 22 of this Law.

A reporting entity shall be obliged to obtain the data on the attorney and directors referred to in paragraph 1 of this Article, by accessing the original or certified photocopy of power of attorney which they shall keep in their documentation.

Establishing the identity of a trust, other person, i.e. other foreign entity equal to them

Article 29

If the customer is a trust, other person, i.e. other foreign entity equal to them, the reporting entity shall be obliged to:

1) establish the identity of their attorney and compliance officer pursuant to Articles 27 and 28 of this Law;
2) to obtain the data referred to in Article 117, paragraph 1, items 1,2 and 3 of this Law for founders, all trustees, other attorneys, users or group of users of the property they manages with, if future users have already been designated or determinable and other natural person who immediately or indirectly performs the final control of the trust;
3) to obtain the data on the legal form of trust, other person, i.e. other foreign entity equal to them and the act on founding the trust, other person or other foreign entity equal to them.

The data referred to in paragraph 1, item 2 of this Article, the reporting entity shall obtain by accessing the original or certified photocopy of a document from CBR or from other relevant public registry, as well as by accessing to original or certified photocopy of a document from court, business or other public registry which shall not be older than three months and shall check those data.

If a reporting entity, when establish the identity of the attorney and compliance officer of the customer, referred to in paragraph 1 of this Article, doubts in veracity of obtained data or in authenticity of the documents or other documentations from which the data have been obtained, they shall be obliged to obtain a written statement of veracity of those data.

Special cases of establishing customer's identity

Article 30

A reporting entity shall establish and verify customer's identity, in accordance with this Law, in particular:

1) when a customer enters the premises where special games of chance are organized in casinos;
2) on any approach of a lessee or their attorney, or a person they has authorized, to the safe deposit box.

When establishing identity of the customer referred to in paragraph 1 item 1 of this Article a reporting entity shall obtain photocopy of personal identification document of that person in accordance with Article 22 paragraph 3 of this Law, as well a written statement by which the customer, under material and criminal liability, states that they participates in the games of chance on their own behalf and in their name.

The identity of the customer referred to in paragraph 1 item 2 of this Article may be established when the customer accesses the safe deposit box through an electronic identification card, personal access password or through the electronic video identification, or means which allow the identification of the customer on the basis of the customer's biometric characteristics.

When establishing customer's identity in accordance with paragraph 1 of this Article an organizer of games of chance in a casino or a reporting entity engaged in the activity of safekeeping shall obtain the data referred to in Article 117, paragraph 1, item 3 and paragraph 2 of this Law.

Implementation of CDD measures and monitoring of customer's business through a third party

Article 31

Under the conditions provided for by this Law, when establishing business relation with a customer, a reporting entity may entrust the implementation of the measures referred to in Article 17 paragraph 1 Items 1, 2 and 3 of this Law to a third party that meets the requirements defined by this Law.

A third party may be:

1) credit institutions and branches of foreign credit institutions;
2) a company for the management of investment funds;
3) companies for the management of pension funds;
4) investment company which operates pursuant to the law which governs a capital market,
5) life insurance company and branch of foreign life insurance companies;
6) Mediation companies, representation companies and entrepreneurs – insurance representatives in the part related to life insurance;
7) persons referred to in items 1 to 6 of this paragraph with seat in a country of European Union or in other country which implements measures in the area of prevention of money laundering and terrorist financing, stipulated by this Law or more severe measures,

External associates and attorneys of the reporting entity who on behalf of the reporting entity, based on the agreement (externalization or attorney relation) conduct certain CDD measures shall not be considered as a third party for the purpose of this Article.

A reporting entity is responsible for the proper implementation of CDD measures and monitoring of customer's business operations through a third party.

Prohibition of implementing CDD measures and monitoring customer's business operation through a third party

Article 32

A reporting entity shall not entrust the application of CDD and monitoring customer's business operation to a third party when a third party is a shell bank or anonymous company or it is from the high-risk third country.

Obtaining data and documents from a third party

Article 33

The third party that carries out CDD measures and monitoring of customer's business operation in accordance with Article 31 of this Law shall be obliged to deliver to the reporting entity the obtained data and documents on the customer.

The third party referred to in paragraph 1 of this Article shall be obliged at the request of the obligor, without delay, to submit photocopies of documents and other documentation on the basis of which it carried out CDD measures, as well as data collected in accordance with Articles 23 and 24 of this Law if electronic identification and video-electronic identification were performed.

The third party referred to in paragraph 1 of this Article shall be obliged to keep the obtained photocopies of documents and documentation in accordance with this Law.

Obligations of the reporting entity in case of obtaining data and documentation from a third party

Article 34

If the reporting entity assesses that there is a doubt about the credibility of the implemented CDD measures of the client's business by a third party, that is, about the veracity of the obtained data and documentation about the client, they shall be obliged to immediately implement those measures.

The reporting entity shall be obliged to develop an internal act which determines the procedures on acceptance of the identification of the customer and the beneficial owner of the customer through a third person.

3. Obligations during transfer of funds

Payment service provider's obligation of the payer

Article 35

A payment service provider of the payer shall be obliged to collect data on the payer and payee and to record them into a form of the payment order or electronic message which follows the transfer of funds from the payer to the payee.

The data on the payer referred to in paragraph 1 of this Article shall be:

1) first and last name, i.e. title;
2) number of payment account, i.e. a unique designation of the transaction if transfer is performed without opening of the payment account;
3) address; i.e. headquarters.

If the payer is not able to obtain data on the address, i.e. the headquarters, they must provide one of the following data:

1) personal identity number, i.e. identity number of the payer, or
2) number of an ID document, date and place of birth of the payer.

Data on the payee referred to in paragraph 1 of this Article shall be:

1) first and last name, i.e. title;
2) number of payment account, i.e. a unique designation of the transaction if transfer is performed without opening of the payment account;

By exception of paragraph 2 and 3 of this Article, in case of collective transfer of funds from one payer, payment service provider is not obliged, in individual transfer of funds which are part of the collective transfer to record data referred to in paragraph 2 and 3 of this Article into a form of the payment order or electronic message which follow the transfer of funds, if data referred to in paragraph 2,3 and 4 of this Article are included in the form of the payment order or electronic message which follow the transfer of funds for collective transfer and if the form or electronic message for every individual transfer of funds includes at least a number of the payer's account, i.e. a unique designation of the transaction, it transfer of funds is performed without opening of payment account.

Exceptionally of paragraph 5 of this Article is not applicable in case of collective transfer of funds from one of the payers, if payment service provider of the payer and payment service provider of the payee has seat in Montenegro.

It the amount of the transaction of funds, including the amount of payment transactions, linked with that transfer, is less than EUR 1.000, payment service provider shall be obliged to ensure that transfer of funds has at least the following details:

1) first and last name, i.e. the title of the payer and the payee,

2) number of payment account of the payer and of the payee, i.e. a unique designation of the transaction if transfer is performed without opening of the payment account;

Payment service provider shall be obliged to verify the accuracy of collected data on the payer pursuant to Articles 22, 23, 24, 26, 27 and 28 of this Law, prior to transaction of funds.

It is considered that payment service provider checked the accuracy of collected data on the payer before the transfer of funds if they previously established business relation with the payer and established the identity of the payer in way which is prescribed in Articles 22, 23, 24, 26, 27 and 28 of this Law and if they act in accordance to Article 49 of this Law.

By way of exception of paragraph 8 of this Article, in case where transfer of funds, including also the amount of money transaction, linked to that transaction is less than EUR 1.000, payment service provider is not obliged to verify the accuracy of data collected on the payer, unless the payment service provider of the payer:

1) receives funds which needs to be transferred in cash or in anonymous electronic money, or

2) there are reasons for doubt in money laundering and terrorist financing.

The payment service provider may, in accordance with the risk assessment, check the accuracy of the collected data, regardless of the amount of funds being transferred.

The payment service provider of the payer shall be obliged to regulate, by internal act, the procedures for verification of completeness of data collected pursuant to paragraphs 2 to 9 of this Article.

Payment service provider's obligation of the payee

Article 36

Payment service provider of the payee shall be obliged to checks whether the data on the payer and on the payee are recorded into a form of payment order or electronic message which follow the transfer of funds pursuant to Article 35 of this Law.

If the amount of transaction is EUR 1.000 or more, regardless of whether those transactions are performed within the one or more linked transactions, payment service provider of the payee shall be obliged, prior of that transaction to the account of the payee or putting at disposal of funds to the payee, to verify the accuracy of collected data on that payee.

If the amount of funds, including also the amount of payment transactions, connected with that transaction, is less than EUR 1.000, payment service provider of the payee is not obliged to verify the accuracy of data collected on the payee, unless:

1) funds are put at disposal to the payee in cash or in anonymous electronic money,

2) there are reasons for doubt in money laundering and terrorist financing.

The verification of the accuracy of collected data referred to in paragraph 2 and 3 of this Article shall be carried out pursuant to Articles 22, 23, 24, 26, 27 and 28 of this Law.

Payment service provider of the payee can, according to risk assessment, verify the accuracy of data of the payee, regardless of the amount of funds which are subject of transfer.

Procedure in case of non-delivery of accurate and complete data

Article 37

Payment service provider of the payee shall be obliged, according to risk assessment, to make an internal act on procedure, including where applicable, ex-post monitoring or real time monitoring, in case that a form of payment order or electronic message for transaction of funds do not have accurate and complete data referred to in Article 35 of this Law.

If transaction of money funds don't have accurate and complete data referred to in Article 35 of this Law, the payment service provider of the payee shall be obliged, according to risk assessment, in internal act referred to in paragraph 1 of this Article, to regulate when to:

1) refuse the transfer of funds;
2) terminate the performing of transfer of funds till receiving the missing data, which they shall be obliged to request from an intermediary in that transfer, i.e. from the payment service provider of the payer,
3) perform the transfer of funds and simultaneously or afterwards to request from an intermediary in that transfer, or from the payment service provider of the payer the missing data, i.e. data which are not recorded in a form or electronic message which follow the transfer of funds.

If payment service provider of the payer repeatedly does not submit the accurate and complete data pursuant to Article 35 of this Law, payment service provider of the payee shall be obliged to warn them and to determine the date within which the provider needs to harmonize their proceeding with this Law.

If payment service provider of the payer does not comply pursuant to paragraph 3 of this Law, provider service provider of the payee shall be obliged to refuse future transfers of funds which they receives from that payment service provider or to limits or to terminate business cooperation with that payment service provider.

Payment service provider shall be obliged to inform the Central Bank of Montenegro on that payment service provider of the payment who repeatedly does not submit the accurate and full data pursuant to Article 35 of this Law, and on measures which they has taken pursuant to paragraph 3 and 4 of this Law toward that payment service provider.

Payment service provider of the payer shall be obliged to establish whether the lack of accurate and complete data referred to in Article 35 of this Law presents the reasons for doubt in money laundering or terrorist financing and if establishes that this lack presents the reasons for doubt, and to inform financial intelligence unit on that pursuant to Article 66, paragraphs 6, 8 and 10 of the present Law.

If the payment service provider of the payee establishes that lack referred to in paragraph 6 of this Article does not present reasons for doubt in money laundering and terrorist financing, they shall be obliged to make a note which shall be kept pursuant to this Law.

Obligations of the intermediary in transfer of funds

Article 38

An intermediary in the transfer of funds shall be obliged to ensure that all data on the payer and the payee are kept in a form of payment order or electronic message which follow the transfer of funds.

An intermediary in the transfer of funds shall be obliged, using the approach based on the risk assessment, to make an internal act on procedure, including, where applicable, ex-post monitoring or real time monitoring, in case if electronic message by which the funds are transferred, does not have the accurate and complete data referred to in Article 35 of this Law.

If the transfer of funds does not have the accurate and complete data referred to in Article 35 of this Law, the intermediary in transfer of funds shall be obliged to comply pursuant to Article 37, paragraphs 2 to 7 of this Law.

Exemption from obligation of collecting data on the payer and the payee

Article 39

Provisions referred to in Articles from 35 to 38 of this Law shall not be applicable in the following cases:

1) when the transfer of funds is carried out solely for purchase of goods or service, by use of payment card, payment instrument who serves for disposal of electronic money, mobile phone or any other digital or information-technological device, provided that the payer and the payee and number of that card, instrument or device, i.e. the unique identification designation follow that transfer of funds in way which enables accessing the data on the payer, except in case when the payment card, payment instrument which serves for disposal with electronic money, mobile phone or any other digital or information-technological device with similar features are used for performing of transfer of funds between natural persons:
2) during the transfer of funds if the payer withdraws the cash from their account;
3) when paying of taxes, fines and any other public duties is carried out via transfer of funds, and payment service provider of the payer and payment service provider of the payee are seated in Montenegro;
4) when the payer and the payee are payment service providers who act on their own behalf and for their own account,
5) when payment is carried out by the transfer of funds to the payee, exclusively upon delivery of goods or provided services, services of electric supply, water supply, services of collecting, treatment and disposal of waste, maintenance of residential buildings or any other similar permanent services which are subject of concluded service contract, if:
   - the payment service provider of the payee is a reporting entity for the purpose of this Law,
   - the payment service provider of the payer can, through the payee, with unique identification designation of transaction or with other data which follows transfer of funds, access to data on person who had concluded service contract with the payer or contract on payment of goods,
   - the amount of funds does not exceeds the amount of EUR 500,
   - the payments for these services is performed by approval of the account of the payee which refers exclusively for those charges, and
   - all conditions referred to in Article 40, paragraph 1 of this Law are met.

Exceptions to the application of CDD measures and monitoring of the customer in case when electronic money is used

Article 40

A reporting entity shall not obliged, in case when electronic money is used, to conduct measures referred to in Article 17, paragraph 1, items 1,2 and 3 of this Law, if, based on the risk assessment, it has been established a low risk of money laundering and terrorist financing even if:

1) a payment instrument cannot be completed again or does not exceed the amount of EUR 150 and can be used only in Montenegro;
2) the highest amount of a deposit of deposited electronic money does not exceed the amount of EUR 150;
3) the payment instrument is used solely for purchase of goods or services;
4) anonymous electronic money cannot be deposited to the payment instrument,
5) the issuing body of the electronic money performs appropriate measures of monitoring of business relation and control of transactions with a view of revealing complex and unusual transactions referred to in Article 58 of this Law and suspicious transactions.

paragraph 1 of this Article shall not be applicable to the purchase of electronic money in cash or to withdrawal of cash in the value of electronic money in the amount more than EUR 50, nor for initiation of a transaction via the Internet or using means of remote communication, if the amount of the transaction exceeds EUR 50.

A reporting entity can accept paying with anonymous payment instrument, if that payment instrument meets conditions referred to in paragraph 1 of this Article and if does not refer to purchase of electronic money in cash or to withdrawal of cash in value of electronic money in the amount of more than EUR 50.

paragraph 1 of this Article shall not apply to the cases where in connection to transaction or the customer, there are reasons for doubt or grounds of suspicion that property originates from the criminal activity or there is a money laundering or terrorist financing.

4. Establishing Beneficial owner

Beneficial owner

Article 41

Beneficial owner is a natural person who owns or exercises real control over a legal entity, business company, trust, other person, i.e. a subject of foreign law equated with it, i.e. a natural person in whose name, i.e. on whose account a transaction is carried out or a business is established relationship.

A beneficial owner of a business organization, or legal person, for the purpose of this Law, shall be deemed a natural person who:

1) indirectly or directly owns at least 25% of the shares, voting rights and other rights, on the basis of which they participates in the management, or owns more than 25% share of the capital or has a dominating influence in the management of the assets of the business organization or legal person;
2) directly or indirectly has a decisive influence on business operations and decision-making influence in a legal entity, i.e. a business organization.

If it is not possible to identify the beneficial owner or if there is a suspicion that the natural person referred to in paragraph 2 of this Article is the beneficial owner, one or more persons in managerial positions shall be deemed to be the beneficial owner of the business organization or legal person.

Beneficial owner of an association, institution, political party, religious community, artistic organization, chamber, trade Union, employers’ association, foundation or other business organization is any natural person authorized for representation or a natural person who has a controlling position in the management of assets of that entity.

If it is not possible to identify the beneficial owner in accordance with paragraph 4 of this Article, the beneficial owner of an association, institution, political party, religious community, artistic organization, chamber, trade union, employers' association, foundation or other business entity shall be any natural person authorized to represent that entity .

As a beneficial owner of a legal person that receives, manages or allocates assets for certain purposes shall be considered a natural person that:

1) indirectly or directly controls at least 25% of a legal person’s asset or of a similar foreign legal entity;
2) is determined or determinable as a beneficiary of at least 25% of the income from property that is being managed.

The beneficial owner of a foreign trust, foreign institution or a similar foreign entity, who receives, manages or allocates the funds for certain purposes, shall be considered to be a natural person who is:

1) the founder of a foreign trust, foreign institution or a similar foreign entity;
2) the trustee of a foreign trust, foreign institution or a similar foreign entity;
3) the beneficiary of the assets obtained from the property which is managed, where the future beneficiaries had already been determined or are determinable;
4) representative of interests of the recipients of the acquired assets;
5) in the category of persons with interest in the establishment of a foreign trust, foreign institution or a similar foreign entity when the individuals who receive the benefits from the foreign trust, foreign institution of a similar foreign entity have yet to be determined;
6) natural person who, in any other way, indirectly or directly controls the property of a foreign trust, foreign institution or a similar foreign entity.

Manner of identifying a beneficial owner

Article 42

A reporting entity shall be obliged to establish the beneficiary owner of the legal entity, business organization, foreign legal entity, trust, other entity, i.e. foreign entity equal to them through obtaining data on business organization, i.e. legal entity, beneficial owner and category of persons interested in establishing of trust, other entity, i.e. foreign entity equal to them referred to in Article 44 of this Law.

Data referred to in paragraph 1 of this Article the reporting entity may obtain by accessing the registry referred to in Article 43, paragraph 1 of this Law, CBR or any other relevant public registry, and by accessing to the court, business and other public registry where the foreign legal entity or business organization is registered, whereby they shall be obliged to print the excerpt from that registry and time, first and last name of the person who accessed the registry.

Data referred to in paragraph 1 of this Article, the reporting entity can provide also by accessing the original or certified photocopy of the document from CBR or any other relevant public registry, as well by accessing to original or certified copy of the document from the court, business and any other public registry where the foreign entity or business organization is registered, which shall not be older than three months of its issue date.

If during the verification of the data pursuant to paragraph 2 and 3 of this Article, the reporting entity establishes that there is a difference in the data, the reporting entity shall be obliged, without delay, to submit the data which differ to financial intelligence unit and to the public authority competent for tax collection.

A reporting entity shall obtain the data which are not included in registries, i.e. in the documents referred to in paragraph 2 and 3 of this Article, by accessing to original or to certified photocopy of the document or any other documentation, submitted to them by the attorney or by authorised person of a client who is a legal entity or business organization.

A legal entity shall be obliged to, beside the data referred to in paragraph 1 of this Article, also provide the documentation on which basis it is possible to establish the ownership structure and a control member of the customer, as well as a data on beneficial owner.

Data on the beneficial owner of the legal entity, business organization, foreign legal entity or trust, other entity, i.e. foreign entity equal to them which they obtained, the reporting entity shall verify in manner to provide complete and clear insight into beneficial ownership and into managing authority of the customer pursuant to risk analysis and during that verification, the reporting entity shall not rely only on the data from the registry referred to in Article 43, paragraph 1 of this Law.

The reporting entity shall be obliged in the procedure of establishing the identity of the beneficial owner referred to in paragraph 1 of this Article, to provide a photocopy of an identity document of the owner referred to in Article 22, paragraph 3 of this Law.

If the reporting entity during collection of data referred to in paragraph 2, 3, 5, 6 and 7 of this Law, doubts in veracity of obtained data or in authenticity of identity documents or other documentation from which the data were obtained, they shall be obliged to obtain a written statement from the attorney or compliance officer about that.

A reporting entity shall keep the original, certified photocopy and excerpt referred to in paragraph 2, 3, 5 and 6 of this Law in their documentation.

A reporting entity shall be obliged to keep records on measures which they has taken for establishing the beneficial owner referred to in paragraph 1 of this Article.

Registry of beneficial owners

Article 43

Beneficial owners register is the electronic database where the data on beneficial owners are kept with a view to ensuring the transparency of ownership structures and conducting measures for prevention of money laundering and terrorist financing.

The Registry of beneficial owners shall be kept and maintained by the administrative authority competent for collection of taxes.

Legal persons, business organizations, associations, institutions, political parties, religious communities, artistic organizations, chambers, trade Unions, employers' associations, foundations or other business organizations, a legal person that receives, manages or allocates the funds for certain purposes, foreign trust, foreign institution or similar foreign legal entity that receives, manages or allocates the funds for certain purposes, shall enter in the Register the data on beneficial owners and changes of owners 8 days since the changes of the beneficial owner have been made.

Obligation referred to in paragraph 3 of this Article shall not apply to:

- entrepreneur;

- public sector within the meaning of the Law which governs the deadlines for settlement of financial obligations, and
- legal entities and commercial entities to multiple joint stock companies who trades shares on the organized securities market, where they obliged to harmonize themselves with obligation of publishing data and information on beneficial ownership pursuant to the law which governs rights and obligations of the subjects on the securities market and other law.

Entities referred to in paragraph 3 of this Article shall be obliged to verify and to confirm the accuracy of their data in the Register of beneficial owners once a year, no later than 31st March of the current year.

The beneficial owner of the entity referred to paragraph 3 of this Article shall be obliged to submit to that entity the data referred to in Article 44 paragraph 1 point 2 items 1, 2 and 4 of this Law in order to enter these data in the Register of Beneficial Owners.

The entities referred to in paragraph 3 of this article and the actual owners of those entities are responsible for the accuracy of the data entered in the Register of Beneficial Owners.

The manner of verification and updating the data from the Register of Beneficial Owners shall be defined by the Ministry.

Content of the Registry of beneficial owners

Article 44

The Registry of beneficial owners shall include the following data:

1) data on the entity referred to in 43, paragraph 3 of this Law:
    - name, address, seat, identification number or any other identification number, tax identification number (hereinafter referred to as: “the TIN"), date of registration and date of deletion from the CBR, i.e. from the Registry of tax payers,
    - data on their status,
    - form of organization,
    - codes of activity,
    - data on representative, trustee or compliance officer (first and last name, unique personal identification number, date of birth, address of permanent or temporary residence, TIN, citizenship),
    - data on natural person who is registered as a member of managing authority (first and last name, unique personal identification number, date of birth, address of permanent or temporary residence, TIN, citizenship),
    - the amount of the basic (registered) capital,
    - data on members, i.e. founders and percentage of their share, i.e. the number and percentage of their shares (first and last name, unique personal identification number, date of birth, address of permanent or temporary residence, TIN, citizenship, ownership share-percentage of shares and percentage of capital share or data on percentage of direct or indirect of disposal of property or data on percentage on the incomes of the user from the property they manages or the share in the property of the legal entity or other foreign subjects),
    - graphic view of the ownership structure if the reporting entity has a complex ownership structure,

- address for receipt of mail,
- address for receipt of e-mail,
- number of accounts in credit institutions,
- scanned documentation which proves the entered data,

2) data on the beneficial owner, as follows:
   - first and last name, unique personal identification number, date of birth, address of permanent or temporary residence, TIN, citizenship,
   - data on ownership share (percentage of shares or percentage of capital share or data on percentage of direct or indirect disposal of property or data on percentage of income of the user from the property he manages to or property share of the legal entity or other foreign subject) or other type of control (data on that whether the owner has deciding influence in property management, whether they directly provide or have provided assets or they have decisive influence to decision making or has a control status in management),
   - date of registration, date of change, i.e. date of updating and deleting of the beneficial owner from the Registry of beneficial owners,
   - scanned documentation which proves the entered data,

3) the rights have yet to be determined to the category of persons interested in establishing the trust, other entity, i.e. foreign entity equal to them when persons who gain benefit from the trust, other entity, i.e. foreign entity equal to them (first and last name of the founder or fiduciary of the trust, user of assets acquired from the property, managed when the future users have already been determined or may be determined to the trust or representative of interests of the recipients of the acquired assets of the trust, unique personal identification number, date of birth, state of residence, citizenship, number of passport and state of issuance, number of residence permit or work and residence permit pursuant to regulations which govern requirements for entry, movement and residence of foreigners to the territory of Montenegro).

Entering data in the Registry of beneficial owners

Article 45

Entities referred to in Article 43 paragraph 3 of this Law shall be obliged to enter and update in the Registry of beneficial owners the data:

1) referred to in Article 44, paragraph 1, item 1 of this Law,
2) about the beneficial owner referred to in Article 44 paragraph 1 item 2 of this Law;
3) on category of persons with an interest for establishing foreign trust, foreign institution or similar foreign legal entity when individuals who benefit from foreign trust, foreign institution or similar foreign legal entity are to be determined referred to in Article 44 paragraph 1 item 3 of this Law.

In addition to data referred to in paragraph 1 of this Article, entities referred to in Article 43, paragraph 3 of this Law who have a complex ownership structure shall be obliged to deliver to the Registry of beneficial owners also:

- a note on existence of a complex ownership structure of that entity,
- document in electronic form which includes graphics of the ownership structure,
- original or certified photocopy of the document from CBR or any other relevant public registry, and the original or certified photocopy of the document from the court, business or any other public registry where foreign legal entity or business

organization has been registered, which shall not be older than three months of its issue date, in electronic form, for any legal entity, trust or legal arrangement which is included in ownership structure.

A complex ownership structure for the purpose of paragraph 2 of this Article is the ownership structure where the founder, i.e. the owner of the entity referred to in Article 43, paragraph 3 of this Law is at least one legal entity or a legal arrangement or any other foreign entity.

The manner of entering and updating the data from the Register of Beneficial Owners shall be defined by the Ministry.

Maintaining and managing the Registry of beneficial owners

Article 46

The governing authority competent for tax collection shall be obliged to maintain and manage the Registry of beneficial owners in way in which:

- in addition to last entry of the data on the beneficial owner, to keep the previous entry of data from the moment of its registration, and all amendments and deletions of data, according to time and type of change,
- the last entry of data are available to reporting entities referred to in Article 4 of this Law whenever they need those data,
- to enable unlimited access to all data kept in the Registry of beneficial owners to the financial intelligence unit, supervising authorities referred to in Article 131, paragraph 1 of this Law, other authorities competent for prevention and revealing of money laundering and related predicate criminal offences or terrorist financing,
- the data shall be available in the period of five years after deletion of subject referred to in Article 43, paragraph 3 of this Law or from CBR or from the Registry of reporting entities, to financial intelligence unit, supervising bodies referred to in Article 131, paragraph 1 of this Law and to other authorities competent for prevention and revealing of money laundering and related predicate criminal offences or terrorist financing.

Access to the Beneficial Owners Register

Article 47

The access to data from the Registry of beneficial owners shall have:

1) the financial intelligence unit, supervising bodies referred to in Article 131, paragraph 1 of this Law and competent authorities referred to in Article 96, paragraph 1 of this Law;
2) reporting entities; and
3) other legal and natural entities.

Subjects referred to in paragraph 1, item 1 of this Article shall have direct electronic access to all data from the Registry of beneficial owners.

Reporting entities referred to in Article 4 of this Law shall have direct electronic access to data on beneficial owners entered into the Registry of beneficial owners, for conducting the procedure for establishing the customer’s identity.

Other legal entities and natural persons shall have direct electronic access to data on beneficial owners of subjects referred to in Article 43, paragraph 3 of this Law as follows: first and last name, date of birth, citizenship, state of residence, type and scope of ownership share.

Entities referred to in Article 43, paragraph 3 of this Law can submit to the authority competent for tax collecting the request for restriction, i.e. denial of access to all or to a part of the data referred to in paragraph 1, item 3 of this Article to legal entities or natural persons, if the access to those data would led the beneficial owner to risk of fraud, abduction, blackmail, violence or intimidation or if the beneficial owners is a child or a person from whom a business capacity has been taken away.

The financial intelligence unit shall establish the existence of circumstances referred to in paragraph 5 of this Article shall be established by decision.

When the financial intelligence unit establishes the existence of circumstances referred to in paragraph 5 of this Article, the governing body, competent for tax collection will restrict, i.e. deny the access to legal entities or natural persons referred to in paragraph 1, item 3 of this Article, to all or to a part of data to which the request referred to in paragraph 5 of this Article refers.

Administrative dispute can be initiated against decision resolution referred to in paragraph 6 of this Article.

The manner of the access to data from the Registry of beneficial owners shall be closer prescribed by the Ministry.

Supervision regarding delivery of data to the Registry of beneficial owners

Article 48

When performing supervision of entities referred to in Article 43, paragraph 3 of this Law, the governing body competent for tax collection shall control if:

- those subjects have data on beneficial owner referred to in Article 44, paragraph 1, item 2 of this Law and whether those data are complete and identical to data from reliable sources,
- those subjects entered the data referred to in indent 1 of this paragraph and within the deadlines prescribed by this Law.

Within the supervision referred to in paragraph 1 of this Article, governing body competent for tax collecting shall perform indirect and direct supervision in accordance with Article 132 of this Law.

Entities referred to in Article 43, paragraph 3 of this Law shall be obliged, upon request of governing body competent for tax collecting, to submit documentation according to which it is possible to establish the ownership structure and control member of the customer and to collect data on beneficial owner.

5. Monitoring business relation, transaction control and repeated annual control

Monitoring business relation and transaction control

Article 49

A reporting entity shall be obliged to conduct CDD measures, including transaction control and monitoring of the source of assets with which the customer operates, whereby they shall be obliged to collect the data referred to in Article 117, paragraph 1, items 6 and 7 and paragraph from 3 to 6 of this Law, depending on the type of reporting entities.

Measures referred to in paragraph 1 of this Article, shall particularly include:

1) verification of compliance of customer’s business with nature and purpose of the business relation,
2) verification of transactions according to customer’s risk profile of money laundering and terrorist financing,

3) monitoring and verification of compliance of customer’s business with their usual business scope,

4) verification of sources of assets that customer operates with, i.e. performs transaction according to customer’s risk profile of money laundering and terrorist financing,

5) monitoring and updating the data on the customer, beneficial owner of the customer and customer’s risk profile, and verification of data whether the customer or beneficial owner has become or has ceased to be politically exposed person referred to in Article 54 paragraphs 2, 3 and 4 of the present Law.

A reporting entity shall be obliged to provide and to adjust a scope and dynamics of taking measures referred to in paragraph 1 of this Article to the risk of money laundering and terrorist financing to which the beneficial owner is exposed in performing an individual job, i.e. doing business with customer.

Updating the data on customer, beneficial owner and verification of data whether the customer or a beneficial owner of the customer has become or has ceased to be politically exposed person referred to in Article 54 paragraphs 2, 3 and 4 of this Law, by accessing to CRP, record of issued identity documents, Registry of beneficial owners, CBR, registry referred to in Article 55, paragraph 1 of this Law and any other relevant public registry, i.e. verification of original or certified copy of document from CBR or other appropriate public registry.

The data which are not included in registries, records and documents referred to in paragraph 4 of this Article, the reporting entity shall obtain by accessing the original or certified photocopy of the document or other documentation which, upon request, shall be submitted by the customer.

If, during verification of the data referred to in paragraphs 4 and 5 of this Article, the reporting entity established the difference in data, they can call the customer for verification of all relevant information.

Annual control

Article 50

In addition to monitoring business relation and transaction control in accordance with Article 49 of this Law, the reporting entity shall be obliged, at least once a year, no later than expiration of one year from the last control, shall perform the control of the customer who is:

- a foreign legal entity who performs transactions to the reporting entity referred to in Article 18, paragraph 1, items 2, 3, 5 and/or 6 of this Law, and
- a legal entity seated in Montenegro, with foreign capital share of at least 25%, who performs transactions to the reporting entity referred to in Article 18, paragraph 1, items 2, 3, 5 and/or 6 of this Law.

Control of the customer referred to in paragraph 1 of this Article shall perform:

1) obtaining, i.e. verification of data referred to in Article 117 of this Law;

2) obtaining, i.e. verification of data referred to in Article 44 of this Law;

3) obtaining of authorization referred to in Article 28, paragraph 2 of this Law.

If business unit of the foreign legal person performs transactions referred to in Article 18, paragraph 1, items 2,3, 5 and/or 6 of this Law on behalf and for the account of the foreign legal entity, the reporting entity during control of foreign legal entity referred to in paragraph 1, indent 1 of this Article, in addition to data referred to in paragraph 2 of this Article, shall provide also the following data:

1) on the address and on the seat of the business unit of the foreign legal entity,

2) data referred to in Article 117, paragraph 1, item 3 of this Law relating to attorney of business unit of the foreign legal entity.

Data referred to in paragraphs 2 and 3 of this Article, the reporting entity shall obtain by accessing to CRB, records of issued identity documents, Registry of beneficial owners, CBR, court, business or other relevant public registry where the foreign legal entity has been registered or business organization, as well as by accessing to original or certified photocopy of a document from CBR, court, business or other relevant public registry where the foreign legal entity has been registered.

The data which are not included in registries, records and documents referred to in paragraph 4 of this Article, the reporting entity shall obtain by accessing the original or certified photocopy of the document or other documentation which, upon request, shall be submitted by the customer.

If, during the control of the customer referred to in paragraph 2 of this Article, the reporting entity shall be obliged to invite the customer in order to verify all relevant information.

By way of exception to paragraph from 1 to 6 of this Article, in case referred to in Article 61, paragraph 1 of this Law, the reporting entity shall not be obliged to perform the annual control of foreign legal entity.

6. Special forms of verification of the customer and monitoring customer's business

Types of special forms of CDD measures and monitoring of customer's business

Article 51

In addition to CDD measures and monitoring of customer's business, the reporting entity shall conduct also the special CDD measures and monitoring of customer's business, depending on established level of risk of money laundering and terrorist financing:

1) enhanced CDD measures and monitoring of customer's business,

2) simplified CDD measures and monitoring of customer's business.

Cases in which enhanced CDD measures and monitoring customer's business are taken

Article 52

The reporting entity shall be obliged to carry out enhanced CDD measures in the sectors and activities referred to in Article 7 paragraph 1 indent 3 of this Law, as well as in cases where a higher risk of money laundering and terrorist financing has been determined, namely:

1) in correspondent relation with credit or any other financial institution which is seated outside European Union or in the high-risk third country;

2) when the customer or beneficial owner of the client is a politically exposed person referred to in Article 54, paragraph 2, 3 and 4 of this Law;

3) when providing custody services in accordance with the law which governs the capital market;

4) In complex and unusual transaction referred to in Article 58 of this Law;

5) in suspicious transactions;

6) during establishment of business relation or performing transactions with persons from high-risk third countries or when the high-risk third country is included in transaction;
7) when the higher risk of money laundering and terrorist financing has been established in guidelines on risk analysis referred to in Article 12, paragraph 5 of this Law,
8) when higher risk of money laundering and terrorist financing has been established according to National risk assessment.

A reporting entity shall be obliged to implement enhanced CDD measures and monitoring of customer's business even in other cases when it is estimated that in relation to the customer, group of customers, state or geographic area, business relation, transaction, product, service or distributive channel there is or there might be a high risk of money laundering and terrorist financing.

Enhanced CDD measures and monitoring of customer's business in correspondent relation with credit or other financial institution with seat outside European Union or in high-risk third country

Article 53

When establishing the correspondent relation, which includes payment with credit or any other similar institution which is seated outside European Union or in high-risk third country, the reporting entity shall be obliged, in addition to measures referred to in Article 17 of this Law, to provide data, information, i.e. documentation on credit or other financial institution which is the respondent:

1) On certification for performing bank services, including issuing date, name and seat of the competent authority that issued the certificate,
2) On internal procedures which are carried out for preventing and revealing money laundering and terrorist financing, specifically on the procedures of verification of the customer, establishing beneficial owner, announcing the data on suspicion transactions, activities and customers, competent authorities, records keeping, internal controls and other procedures which credit or other financial institution has established with reference to preventing and revealing money laundering and terrorist financing,
3) By obtaining data, information and documents on the assessment of internal control on conducting measures for prevention of money laundering and terrorist financing to the credit institution or other financial organization which is the correspondent,
4) By obtaining data, information and documents on legal, i.e. institutional regulations in the field of preventing money laundering and terrorist financing which are implemented in other state where credit institution or other financial institution is based, i.e. is registered,
5) Check whether the credit institution or other financial institution complies with the laws of the country in which it has seat, i.e. in which it is registered, the relevant regulations in the areas of prevention and detection of money laundering and terrorist financing, including information on whether it is under investigation in connection with money laundering and terrorist financing or measures have been taken against that institution by the competent authorities;
6) Determine that the credit institution or other financial institution does not operate as a shell (fictitious) bank;

7) Determines that the credit institution or other financial institution has no established, i.e. does not establish business relations or conduct transactions with shell (fictitious) banks;

8) Obtain written statement that credit or other similar institution with reference to a brokerage account has established the identity and has performed continuing procedure of implementing measures of establishing and monitoring the business relation with client who has direct access to the account of correspondent and that it is able to provide relevant data in relation to the procedure.

Before establishing a correspondence relationship with the respondent, the reporting entity shall be obliged to obtain the written consent of the senior manager for the establishment of that business relationship.

The reporting entity shall be obliged to regulate their responsibility and the responsibility of the respondent in the contract when concluding a correspondence relationship.

In addition to the measures referred to in paragraph 1 of this Article, the reporting entity shall also be obliged to obtain sufficient information about the credit institution or other financial institution that is the respondent, which is necessary for a complete understanding of the nature of its business and to determine the reputation of that institution from publicly available sources.

The data referred to in paragraph 1 of this Article shall be obtained by the reporting entity by inspecting the documents and documentation submitted by the credit institution or other financial institution, that is, from public or other available data records.

A reporting entity shall be obliged to revise and to amend and if needed, to terminate correspondent relation with credit or other financial institution that is the respondent in high-risk third country.

A reporting entity shall not establish or continue correspondent relation with credit or other similar institution which is based outside European Union or in high-risk third country if:

1) They previously did not take measures referred to in paragraphs 1, 2, 3 and 4 of this Article,

2) Credit or other similar institution does not have established controls of system for preventing money laundering and terrorist financing or if it is not obliged to implement laws and other regulations in the field of preventing and revealing money laundering and terrorist financing, or

3) Credit or other similar institution operates as a shell bank, i.e. if establishes correspondent or other business relations and performs transactions with shell banks.

Politically exposed persons

Article 54

A reporting entity shall be obliged, prior to establishing business relation with the customer, to check in the registry referred to in Article 55 of this Law whether the client, his attorney, compliance officer, or beneficial owner is politically exposed person.

Politically exposed person, within the meaning of this Law, shall be a Montenegrin citizen who performs public office:

1) President of Montenegro, president of the Montenegrin Parliament, president and member of the Government,

2) Member of Parliament,

3) President of political party, member of presidency of political party, their deputies, member of the Steering Committee and other official in political party,
4) State Secretary, Director General and Secretary in the Ministry, director, assistant Police director, head of financial intelligence unit,
5) President and judge of the Supreme court of Montenegro and president and judge of Constitutional court of Montenegro,
6) Supreme State Prosecutor, Special state prosecutor and prosecutor in the Supreme State Prosecution Office and in Special State Prosecution Office,
7) Member of Senate of State Audit Institution and Council of Central Bank of Montenegro,
8) Director and assistant director of governing authority,
9) Mayor, president of municipality, president of Assembly of the Capital, president of Assembly of Royal Capital and president of the municipal assembly,
10) Director of National Security Agency and director of Agency for prevention of corruption,
11) Ambassador, consul, chief of General Staff of Army of Montenegro, general and admiral of the Army of Montenegro,
12) Director, deputy, or assistant director and member of the management body and supervisory body of a legal entity that is majority owned by the state.

Politically exposed person shall be also the person who performs public office in other state or international organization:

1) President of State, Prime Minister, Minister and their deputy;
2) Member of Parliament;
3) Member of managing body of political party;
4) Member of the Supreme court, Constitutional court or other judicial court on high level against whose judgment, save in exceptional cases, is not possible to use regular or extraordinary remedy;
5) Member of Audit court, i.e. Supreme Audit Institution and Council of central banks;
6) Ambassador, consul or high-ranked officer of armed forces;
7) Member of governing body and supervising body of the legal entity majority owned by the state;
8) Director, deputy, i.e. assistant director and member of Board or other relevant office in international organization.

Family members of the person referred to in paragraphs 2 and 3 of this Article and their closest associates shall be considered as politically exposed persons.

Married or common-law partner shall be considered as family members referred to in paragraphs 2 and 3 of this Article, partner in common law marriages between persons of same sex, children born in marriage or out a wedlock and foster children and parents.

Close associate of the person referred to in paragraph 2 and 3 of this Article shall be:

1) A natural person who has common beneficial ownership or property right or other ownership rights of legal entity or legal arrangements, established business relation or other types of closer business relations with politically exposed persons;
2) A natural person who is the sole beneficial owner of a legal entity or legal arrangement that is known to have been created for the benefit of a politically exposed person.

International organization who performs mission in Montenegro shall be obliged to publish and to update the list of the most prominent public officials in that international organization.

Person referred to in paragraph 2, 3 and 4 of this Article shall be the politically exposed persons even in the period of two years after termination of performing a public office.

After expiring the deadline referred to in paragraph 8 of this Article, the reporting entity shall be obliged to implement CDD measures according to the risk analysis and to establish if there is still, in relation to that person, a high risk of money laundering and terrorist financing.

Registry of politically exposed persons

Article 55

A Registry of politically exposed persons shall be an electronic database where the data on politically exposed persons are kept.

Direct electronic access to data from the Registry of politically exposed persons has financial intelligence unit, reporting entities and supervising bodies referred to in Article 131, paragraph 1 of this Law.

Reporting entities shall have access only to currently active politically exposed persons.

A registry of politically exposed persons shall be kept and maintained by the Agency for prevention of corruption.

The manner of keeping and the content of the Registry of politically exposed persons shall be established by the Agency for prevention of corruption.

Enhanced CDD measures and monitoring of business of the customer who is a politically exposed person

Article 56

In case when the customer is a politically exposed person, in addition to measures referred to in Article 17 of this Law, the reporting entity shall be obliged to:

1) Implement adequate measures and to establish the origin of the property and assets which are included in business relation or transactions with that customer;
2) To obtain written consent of senior manager for establishing business relation with that customer before establishing business relation, and if business relation has already been established, to obtain written consent of the senior management for continuation of business relation;
3) To establish whether that customer is the beneficial owner of the legal entity, business organization, trust and other entity, i.e. foreign entity, i.e. natural person equal to them based in other country on whose behalf the business relation is established, make transaction or other activities of the customer;
4) After establishing of business relation, monitor with special attention transactions and other business activities which politically exposed person performs to the reporting entity, i.e. the customer whose beneficial owner is politically exposed person.

A reporting entity shall be obliged, in accordance with the guidelines referred to in Article 12, paragraph 5 of this Law, to arrange procedures which are based on risk analysis that they implements with reference to customer’s identification who is a politically exposed person or through establishing beneficial owner of the customer who is a politically exposed person, and during monitoring of business operations of that customer and beneficial owner.

Enhanced CDD measures and monitoring of customer's business operations in providing custody services

Article 57

When providing custody services to the customer, in addition to measures referred to in Article 17 of this Law, the reporting entity shall be obliged to:

1) Implement adequate measures and to establish the origin of the property and assets which are included in business relation or transactions with that customer:
2) To obtain written consent of senior manager for establishing business relation with that customer before establishing business relation, and if business relation has already been established, to obtain written consent of the senior management for continuation of business relation;
3) To establish whether the customer concludes the agreement on performing custody services on their on behalf and on their own account or it is a sub-custody (credit institution or other legal entity who on its own behalf and the account of third persons – its customers to whom provides custody services, concludes the agreement on performing custody services with reporting entity),
4) Establish, during every transaction, in case of sub-custody, on whose account the sub-custody made transaction.

If a reporting entity cannot execute measures referred to in paragraph 1 of this Article, the business relation shall not be established, and if the business relation has already been established it shall be terminated.

Enhanced CDD measures and monitoring of business of the customer in complex and unusual transactions

Article 58

In case of transactions which are complex and unusually large, and in case of those transactions which are realized in unusual manner or which don't have obvious economic justification or legal purpose or deviate from usual or expected customer's business, and in relation to them or to the customer there are no established reasons for suspicion that property originates from criminal activity or that is about money laundering, i.e. terrorist financing, in addition to measures referred to in Article 17 of this Law, the reporting entity shall be obliged to:

1) Collect and to verify additional data on customer's activity and to update also the identification data on the customer and beneficial owner;
2) Collect and to verify additional data on the nature of business relation and motive and purposed of announced or performed transaction;
3) Collect and verify additional data on property status, origin of property and assets of the customer that are included in business relation or transaction with that customer;
4) Collect information on the origin of money assets and origin of customer's property and beneficial owner, i.e. beneficial owners;
5) Collect information on reasons for planned or performed transactions;
6) Analyse data referred to in items 2 and 3 of this paragraph and to draft the results of analysis in written form, with stating clear conclusions that refer that it is about such transaction.

A reporting entity shall be obliged, upon request of financial intelligence unit or competent supervising authority referred to in Article 131, paragraph 1 of this Law, to make available the results of the analysis referred to in paragraph 1, item 6 of this Article.

A reporting entity shall be obliged to establish, by internal act, the criteria for recognition of transactions referred to in paragraph 1 of this Article.

Enhanced CDD measures and monitoring of customer's business operation from high-risk third country

Article 59

In case of establishing business relation or performing transactions with persons from high-risk third countries or when the high-risk third country is included in transaction, in addition to measures referred to in Article 17 of this Law, the reporting entity shall be obliged to:

1) Take measures referred to in Article 58, paragraph 1 of this Law;

2) Before establishing business relation, to obtain written consent of senior manager.

After establishing business relation with customer from high-risk third country, the reporting entity shall be obliged to conduct enhanced monitoring of business relation and transactions which that customer performs in whereby they will:

- Increase the number and frequency of performed controls and choose the manners for performing transactions which need to be further examined;
- Provide more frequent reporting of compliance officer for prevention of money laundering and terrorist financing on transactions;
- Limit business relations or transactions with customers from states from the list referred to in Article 60 of this Law.

A reporting entity shall be obliged to implement measures referred to in paragraph 1 and 2 of this Article according to risk analysis for money laundering and terrorist financing, which is established in the risk analysis.

When implementing the measures referred to in paragraph 2 of this Article, reporting entity may also take into account the relevant assessment or reports of international organizations or experts for determining standards in the field of preventing money laundering and terrorist financing, and regarding the risks that may be posed by certain third countries.

List of high-risk third countries

Article 60

The financial intelligence unit shall publish the list of high-risk countries on its web page.

Simplified CDD measures and monitoring of customer's business operation

Article 61

If in cases referred to in Article 18 paragraph 1 items 1, 2, 3 and 6 of this Law, in relation to a customer, business relationship, transaction, products, services, distribution channels, countries or geographic areas there is lower risk of money laundering or terrorist financing and if there are no reasons for suspicion of money laundering or terrorist financing, as well as if its beneficial owner is not politically exposed person, reporting entity can apply simplified CDD measures and monitoring of customer's business relation, in manner:

1) To check the identity of the customer and to establish the beneficial owner after establishing business relation;
2) To decrease the frequency of updating data on identity of a customer;
3) To decrease the frequency of constant monitoring of transactions if the value of transaction does not exceed the amount for which the reporting entity, during risk analysis of money laundering and terrorist financing, determined that it is appropriate to business operation and lower risk of the customer,
4) Instead of collecting information on that and implementation of specific measures, to draw conclusions on the purpose and envisaged nature of business relation according to types of transaction and established business relation.

If, after establishing business relation with the customer with implementation of simplified CDD measures and monitoring of customer's business operation, reasons for suspicion or grounds of suspicion appear that property originates from criminal activity or it is about money laundering or terrorist financing, the reporting entity shall be obliged to provide data to financial intelligence unit referred to in Article 66, paragraphs 6 and 10 of this Law and to implement measures referred to in Article 17 of this Law.

A reporting entity shall be obliged, with reference to the customer to whom it is established that there is a lower risk of money laundering and terrorist financing, to implement monitoring of business relation and control of transactions in the scope which they determined in accordance with to paragraph 1, item 3 of this Article.

7. Implementation of measures for prevention and revealing of money laundering and terrorist financing in business units and companies whose majority owners are foreign reporting entities

Obligation of implementing measures for prevention and revealing of money laundering and terrorist financing in business units and companies whose majority owners are foreign reporting entities

Article 62

A reporting entity shall be obliged to ensure that measures for prevention and revealing of money laundering and terrorist financing, established by this Law, are implemented in the same scope also in other business units or companies whose majority owners are reporting entities based in another country which is a member of European Union, i.e. country which has the same standards for implementing measures for prevention and revealing of money laundering and terrorist financing such as standards established by this Law, i.e. by European Union law.

If regulations of other country stipulate standards for implementing measures for prevention and revealing of money laundering and terrorist financing, the same or higher than standards established by this Law, the reporting entity shall be obliged to ensure that their business units or companies whose majority owners are reporting entities in other country, adopt and implement appropriate measures in accordance with to regulations of that country, including measures of data protection.

If regulations of other country stipulate standards for implementing measures for prevention and revealing of money laundering and terrorist financing are lower than standards established by this Law, or if measures for prevention and revealing of money laundering and terrorist financing are implemented in the scope lower than the scope established by this Law, the reporting entity shall be obliged to ensure that their business units or companies whose majority owners are reporting entities in other country, adopt and implement appropriate measures in accordance with to regulations of that country, including measures of data protection, to the extent that regulations of that country allow.

If regulations of other country prohibit the implementation of measures referred to in paragraph 3 of this Article, the reporting entity shall be obliged to immediately inform on that financial intelligence unit and competent supervising body referred to in Article 131, paragraph 1 of this Law and to take other appropriate measures for mitigation and effective risk management of money laundering and terrorist financing, to the extent that regulations of that country allow.

If competent supervising body referred to in Article 131, paragraph 1 of this Law evaluates that measures referred to in paragraph 4 of this Article are not enough, it will order the reporting entity to conduct the following measures in another country:

1) To prohibit the establishing of business relations;
2) To terminate business relations;
3) To prohibit the performing of transactions; or
4) If needed and possible, to terminate business operations in business units or companies whose majority owners are in other country.

A reporting entity referred to in paragraph 1 of this Article who is a member of financial group can, for the purpose of prevention of money laundering and terrorist financing, exchange data on the customer and/or transaction, obtained in accordance with to this Law, with other members of financial group in Montenegro, EU Members States and states that have same or higher standards for implementing measures for prevention and revealing of money laundering and terrorist financing than standards established by this Law, i.e. law of European Union, whereby they shall be obliged to establish the appropriate data protection and/or information protection in accordance with to laws which govern data confidentiality and personal data protection.

A reporting entity referred to in paragraph 1 of this Article who is a member of financial group can make exchange of data referred to in paragraph 6 of this Article with other members of financial group in Montenegro, EU Member States and states which have same or higher standards for implementing measures for prevention and revealing of money laundering and terrorist financing, than standards established by this Law, i.e. European Union law and when existence of reasons for suspicion or ground of suspicion is reported to financial intelligence unit that money assets or other property present illegal gain acquired through criminal activity or they are subject of money laundering and terrorist financing, unless financial intelligence unit restricts or prohibits exchange of information.

8. Prohibitions and restrictions in business operations

Prohibition of providing services that enable the concealment of customer’s identity

Article 63

A reporting entity shall not, for a customer, open, or keep an anonymous account, coded or bearer passbook or provide other service or product that can indirectly or directly enable the concealment of a customer’s identity.

Prohibition of carrying on business with shell banks

Article 64

A reporting identity shall not operate as a shell bank.

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

Restriction in operating with cash

Article 65

Legal entities, commercial entities, entrepreneurs and natural persons who performs activities shall not receive payment or perform payment in cash in the amount of EUR 10.000 or more.

Restriction referred to in paragraph 1 of this Article shall be applied also in case if the payment or paying is carried out in two or more linked transactions in total amount of EUR 10.000 or more.

Payment and paying in the amount referred to in paragraph 1 and 2 of this Article must be performed by payment or transfer to transaction account for paying, open to the credit institution.

Obligations referred to in paragraph 1, 2 and 3 of this Article shall not apply to credit institutions and other payment service providers.

9. Duty to report

Reporting to the Financial intelligence unit

Article 66

A reporting entity shall be obliged to submit accurate and complete data to the financial intelligence unit on CDD measures and on measures of monitoring customer's business operations referred to in Article 117, paragraphs 1 to 6 of this Law for each transaction in cash in the amount of EUR 15,000 or more, or non-cash transaction in the amount of EUR 100,000 or more, without delay, at the latest within three days from the day of transaction.

By exception of paragraph 1 of this Article, the reporting entity referred to in Article 4, paragraph 2, item 13, indents 5,10,11 and 12 of this Law shall be obliged to submit accurate and complete data to the financial intelligence unit on CDD measures and on measures of monitoring customer's business operations referred to in Article 117, paragraphs 1 to 6 of this Law for each transaction in cash in the amount of EUR 10,000 or more, without delay, at the latest within three working days from the day of transaction.

A reporting entity shall be obliged to submit accurate and complete data to the financial intelligence unit on CDD measures and on measures of monitoring customer's business operations referred to in Article 117, paragraphs 1 to 6 of this Law for each transaction in cash in the amount of EUR 10,000 or more, which is carried out to the accounts of legal and natural persons in high-risk third countries and if such transaction includes high-risk third country, without delay, at the latest within three days from the day of transaction.

A reporting entity referred to in Article 4, paragraph 4 of this Law shall be obliged to submit accurate and complete data to the financial intelligence unit on CDD measures and on measures of monitoring customer's business operations referred to in Article 117, paragraphs 1 to 6 of this Law for each transaction according to preliminary contract or the contract in relation to real estate, value of EUR 15,000 or more, as well as according to loan agreement whose value is EUR 10,000 or more, without delay, at the latest within three days from the day of transaction.

In addition to data referred to in paragraph 4 of this Article, the reporting entity referred to in Article 4, paragraph 4 of this Law shall be obliged to submit to the financial intelligence unit also a photocopy of the agreement in electronic form, and for contracts for which implementation is used cash a statement from a physical entity which is a buyer about the origin of that money.

A reporting entity shall be obliged to refrain from execution of suspicious transaction, regardless of the amount, utill passing the order referring to in Article 93 of Law and to inform, without delay the the financial intelligence unit and to provide it CDD measures and on measures of monitoring customer's business operations referred to in Article 117, paragraphs 1 to 6 and paragraph 8 of this Law.

A reporting entity shall be obliged to submit the data referred to in paragraph 6 of this Article to the financial intelligence unit before execution of transactions and to specify the deadline within which the transaction should be carried out.

If reporting entity, for the nature of transactions and other justified reasons cannot act according to paragraph 6 of this Law, they shall be obliged to submit the accurate and complete data on CDD measures and monitoring customer's business operations referred to in Article 117, paragraphs 1 to 6 and paragraph 8 of this Article, without delay, and at the latest on the next working day from the date of execution of the transaction.

When submitting data in the manner referred to in paragraph 8 of this Article, the reporting entity shall be obliged to submit an explanation containing the reasons why they did not act in accordance with paragraph 6 of this Article.

A reporting entity shall be obliged to, without delay, provide the financial intelligence unit with accurate and complete data on CDD measures and the measures of monitoring of the client's business referred to in from Article 117 paragraphs 1 to 6 and paragraph 8 of this Law in relation to funds or other assets that he knows or has reason to suspect represent financial gains obtained through criminal activity or are related to money laundering or terrorist financing.

If customer asks for advice for money laundering and terrorist financing, the reporting entity shall be obliged to inform the financial intelligence unit on that, without delay.

The reporting entity shall be obliged to inform the financial intelligence unit on any access to data, information and documentation which the supervising authority referred to in Article 131, paragraph 1 of this Law performs to the reporting entity, at the latest within three days from the day of access.

A reporting entity shall be obliged to submit the data referred to in paragraphs 1 to 6 and paragraph 10 of this Article, explanation referred to in paragraph 9 of this Article and notifications referred to in paragraph 11 and 12 of this Article to the financial intelligence unit electronically and to sign with electronic signature those data, explanation and notification in accordance with to the law which governs electronic identification and electronic signature.

The reporting entity can announce the data referred to in paragraph 6 and 10 of this Law to the financial intelligence unit also verbally, through the phone or in other available manner, but they shall be obliged to submit those data also in accordance with to paragraph 13 of this Law, at the latest on the next day of the day of announcement.

Closer manner of submitting data referred to in paragraphs 1 to 6 and paragraph 10 of this Article, explanation referred to in paragraph 9 of this Article and notifications referred to in paragraph 11 and 12 of this Article shall by prescribed by the Ministry.

Exemptions from reporting obligation

Article 67

By way of exception of Article 66 paragraph 6 of this Law, the reporting entity referred to in Article 4, paragraph 3 of this Law shall not obliged to submit the financial intelligence unit the data on the customer and case files in procedures of providing legal assistance and representing of the customer before competent authority.

Feedback to the reporting entity

Article 68

According to data, i.e. notifications submitted in accordance with Article 66, paragraphs 6, 10 and 11 of this Law, the financial intelligence unit shall perform financial analysis in relation to persons, transactions or assets and it shall be obliged to inform the reporting entity on the results of that analysis and on that whether there are reasons for suspicion or grounds for suspicion for existence of money laundering and terrorist financing with reference to this entity or whether that transaction, i.e. assets present property acquired through criminal activity.

By way of exception of paragraph 1 of this Article, the financial intelligence unit shall not inform the reporting entity on the results of analysis and on existence of reasons for suspicion, i.e. grounds of suspicion referred to in paragraph 1 of this Article, if it evaluates that such notification may provoke harmful consequences on the course and outcome of the procedure.

If the financial intelligence unit establishes that there are grounds of suspicious that transaction or asset present property gain acquired through criminal activity or it is about money laundering and terrorist financing, in explanation referred to in paragraph 1 of this Article, it can give a recommendation to the reporting entity to terminate a business relation with the customer, i.e. to decline the execution of transactions.

10. Compliance officer for prevention of money laundering and terrorist financing and their deputy and internal control and audit

Designation of compliance officer for prevention of money laundering and terrorist financing i.e. their deputy

Article 69

A reporting entity shall be obliged, within 60 days from the date of their establishment, to designate a compliance officer and at least one of their deputy for the affairs of detecting and preventing money laundering and terrorist financing and submit to the Financial intelligence unit, within three days of the day of their designation, an explanation with following data on those persons (first and last name, unique personal identification number, number, expiry date and issuing state of identity document, number and expiration date of residence permit for an alien, title of working position and contact phone) and name, i.e. first and last name, TIN and address of the seat of the reporting entity.

A reporting entity shall be obliged to inform the financial intelligence unit on the change of compliance officer for prevention of money laundering and terrorist financing, i.e. their deputy within the three days of the day of change.

The notification referred to in paragraph 2 of this Article must contain an explanation of the reasons for the change and data referred to in paragraph 1 of this Article.

Exceptionally, the reporting entity who has four or less employees, affairs of compliance officer for prevention of money laundering and terrorist financing may be performed also by director, if they fulfils requirements referred to in Article 70 of this Law.

In a case of a reporting entity who have four or fewer employees, affairs of compliance officer for prevention of money laundering and terrorist financing can also be performed by a director, if they meet the requirements referred to in Article 70 of this Law.

When a director performs the affairs of compliance officer for prevention of money laundering and terrorist financing, the reporting entity shall be obliged to notify the financial intelligence unit on that and to provide in that notification the data on director in accordance with paragraph 1 of this Article.

Notifications referred to in paragraphs 1, 2 and 6 of this Article shall be submitted to the financial intelligence unit electronically and must be signed with qualified electronic signature in accordance with to the Law which regulates electronic identification and electronic signature.

Requirements for compliance officer for prevention of money laundering and terrorist financing and their deputy

Article 70

As a compliance officer for prevention of money laundering and terrorist financing and their deputy can be designated a person who:

1) Has completed the training for performing jobs of compliance officer for prevention of money laundering and terrorist financing (hereinafter referred to as: “the training") and who has completed professional exam for performing jobs of compliance officer for prevention of money laundering and terrorist financing (hereinafter referred to as: “the professional exam"),
2) Has a license for performing jobs of compliance officer for prevention of money laundering and terrorist financing, and
3) Has not been finally convicted for a criminal act for which an imprisonment longer than six months is prescribed.

One person can be designates as compliance officer for prevention of money laundering and terrorist financing, i.e. their deputy only to one reporting entity.

By way of exception of paragraph 2 of this Article, when a director performs affairs of compliance officer for prevention of money laundering and terrorist financing in accordance with to Article 69, paragraph 5 of this Law, they can be designated as compliance officer for prevention of money laundering and terrorist financing to more reporting entities where therey are a director and the only employee.

Training and professional exam

Article 71

The training shall be delivered by the organizer of adult education who has a license, issued in accordance with regulations which govern education of adults.

The training shall be delivered according curriculum, in accordance with regulations which govern adult education.

After completing the training, the candidate shall take a professional exam before the commission for taking the professional exam, which is formed by the head of the financial intelligence unit.

The financial intelligence unit shall issue a certificate on the passed professional exam, on the prescribed form.

President and members of the Commission referred to in paragraph 3 of this Article shall be entitled to monthly fee for work in the amount of 25% of average gross salary in

Montenegro in previous year, according to data of governing authority competent for statistical affairs, which is paid in net amount.

If a person who has been already employed to the reporting entity takes professional exam, costs of taking the professional exam shall be borne by reporting entity.

Program and manner of passing the professional exam, amount of costs of taking the professional exam, composition of the Commission for taking the professional exam, and the form of certificate referred to in paragraph 4 of this Article shall be prescribed by the Ministry.

License for performing affairs of compliance officer for prevention of money laundering and terrorist financing

Article 72

The license for performing jobs of compliance officer for prevention of money laundering and terrorist financing (hereinafter referred to as: “the license") shall be issued by financial intelligence unit.

The license shall be issued to a person who:

1) has residence, i.e. approved stay in Montenegro;
2) has not been finally convicted for a criminal act for which an imprisonment longer than six months is prescribed; and
3) has completed the training and who has passed the professional exam.

The license shall be issued for a period of five years and it can be renewed.

The request for issuing the license shall be submitted to the financial intelligence unit.

The request for renewal of the license shall be submitted to financial intelligence unit, at least 30 days before expiration of the period for which it was issued.

The license shall be issued in the form prescribed by the Ministry.

Expiry of a license

Article 73

The license shall cease to be valid:

1) upon request of the holder of the license;
2) upon expiration of period of issuance;
3) if the person to whom the license has been issued has been convicted for a criminal act for which an imprisonment longer than six months is prescribed;
4) if the person to whom the license has been issued become permanently incompetent for performing affairs of compliance officer for prevention of money laundering and terrorist financing, i.e. their deputy or if the person lost their business ability;
5) by exercising of pension rights of the person to whom the license has been issued; or
6) in case of negligent business performance.

Negligent business performance

Article 74

It shall be considered that compliance officer for preventing money laundering and terrorist financing, i.e. their deputy negligently performs duties for the purpose of Article 73, paragraph 1, item 6 of this Law, if without justified reason:

1) Does not provide data and information in accordance with Article 66 of this Law, more than four times within of two years;
2) Fails to submit the data and information in a timely manner, in accordance with this Law, more than six times within of two years; and
3) Does not act, i.e. fails to act in a timely manner in line with Articles 93 and 95 of this Law, more than two times within two years.

The existence of circumstances referred to in paragraph 1 of this Article shall be established by the financial intelligence unit according to the report of the competent supervising authority referred to in Article 131, paragraph 1 of this Law, based on the request referred to in Article 131, paragraph 8 of this Law.

Decision on expiry of a license

Article 75

Decision on expiry of license shall be passed by the financial intelligence unit.

Administrative dispute can be initiated against the decision referred to in paragraph 1 of this Article.

The financial intelligence unit shall inform the reporting entity on termination of license, without delay, to whom is the person from whom the license has been revoked, has been designated as compliance officer for preventing money laundering and terrorist financing, i.e. their deputy.

In case of termination of the license, the reporting entity shall be obliged to designate another compliance officer for preventing money laundering and terrorist financing, i.e. their deputy, within 15 days from the day of adopting the decision.

Affairs of the compliance officer for preventing money laundering and terrorist financing, i.e. their deputy

Article 76

Compliance officer for preventing money laundering and terrorist financing, i.e. their deputy shall perform the following affairs:

1) Take care on establishing, activity and developing of the system for preventing money laundering and terrorist financing;
2) Take care on proper and timely data submission to the financial intelligence unit and to cooperate in the procedure of inspection supervision;
3) Draft and regularly update the risk analysis of money laundering and terrorist financing, in accordance with guidelines referred to in Article 12, paragraph 5 of this Law;
4) Monitor implementation of policies, controls and procedures for preventing money laundering and terrorist financing;
5) Initiate and participate in drafting and amending of operative procedures and preparation of internal acts of the reporting entity that refer to prevention of money laundering and terrorist financing;
6) Participate in drafting of internal acts with reference to prevention of money laundering and terrorist financing in reporting entities;
7) Monitor and coordinate harmonization of business operation of the reporting entity with this Law;
8) Cooperate in establishing and drafting of information technology which will be used for prevention and detection of money laundering and terrorist financing;

9) Give initiatives and proposals for improving the system for prevention of money laundering and terrorist financing to governing authority or other similar authority;

10) When introducing new technologies, products and services to the reporting authority, take care on implementation of Article 16 of this Law;

11) Prepare programs of professional training and developments of employees to the reporting entity in the field of prevention and detection of money laundering and terrorist financing;

12) Prepare report in the field of prevention and detection of money laundering and terrorist financing to the reporting entity once a year, and more often if needed, when supervising authority referred to in Article 131, paragraph 1 of this Law requires it.

A reporting entity shall be obliged to submit the report referred to in paragraph 1, item 12 of this Article to competent supervising authority referred to in Article 131, paragraph 1 of this Law, upon their request, within three days of the day of receiving the request.

A compliance officer for prevention of money laundering and terrorist financing, i.e. their deputy shall be directly responsible to supervising authority or to executive or other similar entity of the reporting authority.

If reporting entity is a large or a medium legal entity for the purpose of the law which governs the accounting, compliance officer for prevention of money laundering and terrorist financing, i.e. their deputy shall be functionally and organizationally separated from other organizational parts of the reporting entity.

Working conditions for a compliance officer for prevention of money laundering and terrorist financing

Article 77

A reporting entity shall be obliged to provide to compliance officer for prevention of money laundering and terrorist financing, particularly:

1) Conditions for efficient performing of affairs referred to in Article 76, paragraph 1 of this Law,

2) Functional connection with other organizational parts of the reporting entity in way in which it enables their prompt, quality and timely performing of affairs referred to in Article 76, paragraph 1 of this Law;

3) Appropriate material working conditions;

4) Adequate spatial and technical conditions, which provide appropriate level of protection of data and available information, in accordance with this Law;

5) Appropriate information-technical support which enables continuing and reliable monitoring of activities in the field of preventing money laundering and terrorist financing;

6) Regular professional training with reference to prevention and detection of money laundering and terrorist financing;

7) Replacement during the absence from work.

Managing authority of the reporting entity shall be obliged to provide assistance and support in performing affairs referred to in Article 76, paragraph 1 of this Law to compliance officer for preventing money laundering and terrorist financing and to inform them on the facts of importance for preventing and detection of money laundering and terrorist financing.

A compliance officer for prevention of money laundering and terrorist financing, in case of their absence or inability, shall be replaced by their deputy.

The method of work of a compliance officer for prevention of money laundering and terrorist financing and their deputy shall be regulated by internal act of the reporting entity.

Professional training and development

Article 78

A reporting entity shall be obliged to provide regular professional training and development in the field of preventing and detection of money laundering and terrorist financing for all employees who participate in prevention and detection of money laundering and terrorist financing to that reporting entity.

Professional training and development referred to in paragraph 1 of this Article shall mean introducing employees to this Law and regulations adopted based on this Law, internal acts of the reporting entity in the field of prevention and detection of money laundering and terrorist financing, reliable publications on prevention and detection of money laundering and terrorist financing, list of indicators referred to in Articles 82 and 83 of this Law, and based on regulations which govern international restrictive measures and regulations which govern personal data protection.

A reporting entity shall be obliged, until the end of first quarter of the year, to prepare a program of professional training and development referred to in paragraph 1 of this Article, for that year.

The manner of professional training and development of employees shall be regulated by internal act of the reporting entity.

Rules in performing affairs of preventing money laundering and terrorist financing

Article 79

A reporting entity shall be obliged to determine and to implement relevant rules in conducting with client and to provide reporting, data keeping, internal control, risk assessment, risk management and communication for prevention of money laundering and terrorist financing.

A reporting entity shall be obliged to determine and to implement relevant rules that guarantee adequate exchange of information between employees for efficient performing of obligations prescribed by this Law.

A reporting entity shall be obliged to order and control application of rules referred to in paragraph 1 and 2 of this Article in business units and companies whose majority owner is the reporting entity with seat in other countries.

Internal control and revision

Article 80

A reporting entity shall be obliged to ensure regular internal control and revision of implementing policies, controls and procedures for prevention of money laundering and terrorist financing, i.e. performing affairs of prevention and detection of money laundering and terrorist financing, in accordance to established risk of money laundering and terrorist financing in the risk analysis.

When the law which governs the business activity of the reporting entity prescribes the existence of independent internal revision, the reporting entity shall be obliged to organize also the independent internal revision in which scope is a regular assessment of adequacy, reliability and effectiveness of risk management system of money laundering and terrorist financing.

A reporting entity shall be obliged to organize an independent internal revision within which scope is assessment of adequacy, reliability and effectiveness of risk management system of money laundering and terrorist financing and when they deems it is necessary considering the nature and scope of the business activity.

Internal control and revision referred to in paragraphs 1, 2 and 3 of this Article shall be implemented in way to prevent, detect and improve mistakes made during implementation of regulations in the field of prevention of money laundering and terrorist financing and to regulate policies, controls and procedures to the reporting entity for revealing transactions and persons in relation to money laundering and terrorist financing.

The manner of conducting internal control and revision referred to in paragraphs 1, 2 and 3 of this Article, the reporting entity shall be obliged to prescribe by internal act.

IV. LIST OF INDICATORS FOR IDENTIFYING SUSPICIOUS CUSTOMERS AND TRANSACTIONS

Obligation of applying the list of indicators

Article 81

When establishing reasons for suspicion that assets originates from criminal activity or money laundering or terrorist financing and other circumstances related to the suspicion, reporting entity shall use the list of indicators referred to in Articles 82 and 83 of this Law and takes into account other circumstances for existence of reasons for suspicion of money laundering and terrorist financing.

List of indicators for recognition of suspicious customers and transactions

Article 82

The list of indicators for identifying suspicious customers and transactions shall be defined by the Ministry.

Professional basis for development of the list of indicators referred to in paragraph 1 of this Article shall be prepared by the financial intelligence unit in cooperation with other competent bodies referred to in Article 131, paragraph 1 of this Law.

Own list of indicators of suspicious customers and transactions

Article 83

The reporting entity shall use their own list of indicators for recognizing suspicious customers and transactions, taking into account the complexity and the size of the transactions executed by that reporting entity, the unusual manner of execution, the value or connection of transactions that have no economic or legal purpose, that is, they are not harmonized or are disproportionate with the regular or expected business activities of customers, as well as other circumstances related to the status and other characteristics of the customer of that reporting entity.

List of indicators referred to in paragraph 1 of this Article must be placed in documentation of reporting entity.

V. AFFAIRS, AUTHORIZATIONS, THE MANNER OF WORK AND INFORMATION SYSTEM OF THE FINANCIAL INTELLIGENCE UNIT

Independence and autonomy in performing affairs and exercising of authorizations

Article 84

The financial intelligence unit shall be central national unit in charge of prevention and detection of money laundering and terrorist financing, in accordance with the Law.

The financial intelligence unit shall be operationally independent and self-contained when performing activities prescribed by law, and independent in decision-making related to the decision making related to the reception, collection, keeping, analysing and providing data, notifications, information and documentation and providing of the strategic and operational analyses of the suspicious transactions to the competent authorities and foreign financial intelligence units and international organizations.

The affairs, i.e. authorizations referred to in paragraph 2 of this Article shall be conducted or exercised by employees of the financial intelligence unit.

The financial intelligence unit shall at least once a year submit a report to the Government on its work and the situation in the area of preventing money laundering and terrorist financing.

Head of the financial intelligence unit

Article 85

A person with the rank of deputy director of the Police Directorate and a person that meets the requirements for deputy director of the Police Directorate may be appointed as the head of the financial intelligence unit, in accordance with the law regulating the internal affairs.

The head of the financial intelligence unit cannot be the head of another organizational unit in the Police.

The head of financial intelligence unit, upon public competition, shall be appointed by the Government, on the proposal of the Minister of Internal Affairs.

The Government shall submit the proposal for appointing the head referred to in paragraph 1 of this Article to the Parliament of Montenegro, for providing its opinion.

The Parliament of Montenegro shall provide the opinion referred to in paragraph 4 of this Article upon the proposal of the competent committee.

Entering employment and terms for employment

Article 86

The head of the financial intelligence unit shall participate in the procedure of selecting candidates that are entering employment at the financial intelligence unit that is conducted in accordance with the regulations on civil servants and state employees and the law that regulates internal affairs.

Employees of the financial intelligence unit shall fulfil terms prescribed by the law defining internal affairs and act on internal organization and systematization of the Ministry.

The decision on employee's entering employment in the financial intelligence unit shall be issued by the Minister, upon the proposal of the head of the financial intelligence unit.

Employee from the financial intelligence unit cannot be reassigned to other working position or tasked to perform other duties in the Ministry, without the authorisation of the head of the financial intelligence unit.

Disposal of the budget of the Financial Intelligence Unit

Article 87

The funds that are allocated to Ministry by the budget for the work of the financial intelligence unit shall be independently disposed of by the head of the financial intelligence unit, in accordance with the law regulating planning and execution of the budget and fiscal responsibility.

The funds that are allocated to financial intelligence unit for its work, by the donations or are in other way, shall be independently disposed of by the head of the financial intelligence unit.

The head of the financial intelligence unit within the fuds referred to in paragraph 1 of this Article, shall independently make decisions of conducting the procedure of public procurements and simple procurements as an authorized person according to the Law regulating public procurement.

Material and technical funds of the financial intelligence unit

Article 88

Information system, means of communication, vehicles and other equipment for the work of the financial intelligence unit may only be used by the employees of the financial intelligence unit.

Information system, means of communication, vehicles and other equipment referred to in paragraph 1 of this Article, cannot be given to use to another organizational unit of the Ministry, or Police, without written consent of the head of the financial intelligence unit.

The manner of disposal and of using material and informational system, means of communication, vehicles and other equipment referred to in paragraph 1 of this Article, as well as the space used by financial intelligence unit shall be regulated by the head of financial intelligence unit by an internal act.

The act referred to in paragraph 3 of this Article shall be marked with appropriate level of data confidentiality, pursuant to the law governing the data confidentiality.

Tasks or authorizations of the financial intelligence unit

Article 89

The financial intelligence unit shall be authorized to:

1) Collect, process and analyse the data about natural and legal entities, their assets, suspicious, cash and other transactions, suspicious and other business activities, bank accounts and deposit boxes, prepare and forward financial analyses and other information in accordance with this Law;
2) Receive information from reporting entities, competent authorities referred to in Article 96 paragraph 1 of this Law, supervisory authorities referred to in Article 131 paragraph 1 of this Law, other legal and natural entities, foreign financial intelligence units and authorities responsible for preventing, suppressing and prosecuting money laundering and terrorist financing in other countries, as well as international organizations; the data about persons and assets for which there are reasons or grounds of suspicion that the assets originates from criminal activity or that it is the matter of money laundering or related predicate offences, terrorist financing, which may process and use for the purpose specified by this Law;
3) Order the reporting entity to temporarily suspend the transaction and continuously monitor the clients financial operations;
4) Initiate changes and amendments to regulations related to prevention of money laundering and terrorist financing;

5) Conclude cooperation agreements or establish an independent co-operation aimed at exchanging information with other domestic competent bodies referred to in Article 96 paragraph 1 of this Law and supervisory authorities referred to in Article 131 paragraph 1 of this Law and foreign financial intelligence units, competent authorities in other countries and international organizations;

6) Manage the information system of the financial intelligence unit;

7) Participate in professional training and development of authorized persons for prevention of money laundering and terrorist financing in the case of reporting entities and their deputies;

8) Provide recommendations or guidelines for the uniform implementation of this Law and regulations adopted on the basis of this Law;

9) Propose to the National Security Council natural and legal persons to be included in the National list of designated persons in accordance with the law that regulates international restrictive measures;

10) At least once a year, publish a report that includes statistical data, trends and typologies in money laundering and terrorist financing area, and especially data related to the number of suspicious transaction reports sent to the financial intelligence unit, the number of investigated cases, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences and data on the property that has been frozen or confiscated, and to notify the public, in other appropriate manner, on the phenomenon of money laundering and terrorist financing;

11) Perform other tasks in accordance with the law.

The detailed manner of performing tasks and applying the authorizations referred to in paragraph 1 of this Article shall be regulated by an internal act of the head of the financial intelligence unit.

The act referred to in paragraph 2 of this Article shall be marked with an appropriate level of confidentiality in accordance with the law regulating data confidentiality.

Request to the reporting entity to submit data, information, and documentation

Article 90

If the financial intelligence unit assesses that there are reasons or grounds of suspicion that funds or other assets originate from criminal activity or that is the matter of money laundering, related predicate offences or that they are related to terrorist financing, it can request from a reporting entity to provide data, information and documentation:

1) Referred to in Article 117 paragraphs 1 to 11 of this Law;

2) On state of funds and other assets of a certain customer at a reporting entity;

3) On funds and asset turnover of a certain customer at a reporting entity;

4) On business relationships established with a reporting entity;

5) Other data obtained by a reporting entity in accordance with this Law, documentation and information related to performing activities in accordance with this Law as well as other data in order to monitor fulfilment of the obligations set out by this Law.

In the request referred to in paragraph 1 of this Article the financial intelligence unit shall state legal basis, the data that are to be provided, the purpose of data gathering and the deadline for their provision.

The financial intelligence unit can also require delivery of data, information and documentation referred to in paragraph 1 of this Article and for persons for whom it is possible to conclude that they have cooperated or participated in transactions or on the business of persons for whom there are reasons or grounds of suspicion that assets or property that they own, dispose of or manage with, originate from criminal activity or money laundering, related predicate offences or related to terrorist financing.

A reporting entity shall provide data, information and documentation referred to in paragraphs 1 to 4 of this Article to the financial intelligence unit without delay, in the manner and form as referred in the request, and not later than eight days since the day of receiving the request.

If the request referred to in paragraphs 1 and 3 of this Article is marked with designation "URGENT", the reporting entity shall be obliged to submit data, information and documents to the financial intelligence unit, without delay, and at latest within 24 hours after receiving the request.

The financial intelligence unit can, due to extensive documentation or other justified reasons, upon the reasoned request of a reporting entity, prolong the deadline referred to in paragraph 5 of this Article or carry out data, information and documentation verification at a reporting entity.

The data, information and documentation referred to in paragraph 1 of this Article, a reporting entity shall provide to the financial intelligence unit in the manner prescribed in the act referred to in Article 66, paragraph 15 of this Law.

Delivery of data, information and documentation referred to in paragraph 1 of this Article to the financial intelligence unit shall be made compensation.

Request to deliver data, information and documents to persons that are not reporting entities

Article 91

By way of exception, it the financial intelligence unit estimates that there are reasons or grounds of suspicion that funds or other assets originate from criminal activities or money laundering, and related predicate offences or that are related to terrorist financing, it can request from the entities referred to in Article 43 paragraph 3 of this Law, as well as natural persons that are not reporting entities for the purpose of this Law, to submit or provide with the data, information and documentation in their disposal or to notify, in order to prevent and detect money laundering, related predicate offences or terrorist financing, and especially the following data:

1) On assets or legitimate income, as well as on the relation between income and property;
2) On assets that were transferred to third parties or passed to a legal successor, as well as on the method of acquiring and transferring assets;
3) About the user of the internet protocol address (IP address);
4) Other data that are important for finding and determining property benefits acquired through criminal activity or for determining the existence of grounds of suspicion that the criminal offence money laundering or terrorist financing was committed.

Entities referred to in paragraph 1 of this Article shall submit data, information and documentation to the financial intelligence unit in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law.

Delivery of data, information and documentation referred to in paragraph 1 of this Article to the financial intelligence unit shall be made compensation.

Request to a state authority, relevant authority, supervising authority or public power holder for submitting data

Article 92

Relevant authorities referred to in Article 96 paragraph 1 of this Law, other state authorities, supervising authorities referred to in Article 131 paragraph 1 of this Law and public power holders shall be obliged to provide to the financial intelligence unit direct electronic access to data, information and documentation kept in electronic form.

If data, information and documents referred to in paragraph 1 of this Article is not possible to obtain in manner referred to in paragraph 1 of this Article, the authorities referred to in paragraph 1 of this Article and public power holders shall be obliged to, upon request by the financial intelligence unit, deliver those data, information and documents, without delay, in manner prescribed by act referred to in Article 66 paragraph 15 of this Law.

The financial intelligence unit shall state in the request referred to in paragraph 1 of this Article, the legal basis, the data that are to be provided, the purpose of data gathering and the deadline for their provision.

Order for temporary suspension of transaction and temporary prohibition of access to deposit box

Article 93

The financial intelligence unit may require by an order from the reporting entity to temporarily suspend a transaction, as well as to put a ban on access to deposit box, not longer than for 72 hours, if it evaluates that there are reasons or grounds of suspicion that assets or property originate from criminal activity or money laundering and related predicate offences or terrorist financing.

After submitting the order referred to in paragraph 1 of this Article, the financial intelligence unit shall, without delay, and not later than 24 hours, notify authorities to take measures from their jurisdiction.

If acting upon notification referred to in Article 66, paragraph 6 of this Law, the financial intelligence unit shall submit the order referred to in paragraph 1 of this Article withing 24 hours from receipt of the notification.

If the last day of a deadline referred to in paragraph 1 of this Article occurs during non-working days of the competent authorities, such deadline can be extended with an order for additional 48 hours, taking into account that the total period of suspension of transaction or prohibition of access to deposit box can’t be longer than seven days.

The reporting entity shall, without delay, take measures and actions in accordance with paragraphs 1 and 4 of this Article.

The financial intelligence unit shall provide the order referred to in paragraphs 1 and 4 of this Article to the reporting entity in electronic or in written form.

By way of exception referred to in paragraphs 1 and 4 of this Article, in case of urgency or other circumstances of the transactions execution, the order can be given verbally, but it has to be provided in electronic or written form not later than 24 hours from issuing the verbal order.

The responsible compliance officer for prevention of money laundering and terrorism financing shall make a note on receiving a verbal order referred to in paragraphs 1 and 4 of this Article.

Upon receiving notification referred to in paragraph 2 from this Article, competent authorities shall act, without delay, in accordance with their authorizations and not later than 72 hours from the beginning of the temporary suspension of transactions and shall, without delay, notify the financial intelligence unit in electronic or written form on the decision on further procedure regarding the suspended transactions.

Termination of the measures for temporary suspension of transactions and prohibition of access to deposit box

Article 94

If the financial intelligence unit does not notify the reporting entity about further action after 72 hours from the suspension of transactions or the prohibition of access to deposit box, the reporting entity may execute the transaction or allow access to the deposit box after expiration of that period.

Request for ongoing monitoring of customer's financial business

Article 95

The financial intelligence unit may, in electronic or written form request from the reporting entity an ongoing monitoring of customer's financial business or the business of another person for whom it may be concluded that they has cooperated or participated in transactions or businesses activities for which there are reasons or grounds of suspicion that those are the assets or property originate from money laundering and related predicate offences or terrorist financing, and determines deadline within which the reporting entity shall be obliged to inform the financial intelligence unit and provide the required data.

Reporting entity shall be obliged to proceed according to the request referred to in paragraph 1 of this Article.

The data referred to in paragraph 1 of this Article, the reporting entity shall inform or provide financial intelligence unit before carrying out the transaction or concluding the business and state in the report the deadline estimation within which the transaction or business should be done.

If due to the nature of transaction or business or due to other justified reasons reporting entity is not able to act as it is prescribed in line with paragraph 3 of this Article, they shall forward the data to the financial intelligence unit as soon as they are able to do so, but not later than the next working day from the day of carrying out the transaction or concluding the business activity.

While forwarding the data is prescribed in the paragraph 4 of this Article, reporting entity shall state the reasons for not acting in accordance with the provisions of paragraph 3 of this Article.

Ongoing monitoring of transactions referred to in paragraph 1 of this Article shall not be longer than 3 months from the day of submitting the request referred to in paragraph 1 of this Article.

Deadline referred to in paragraph 6 of this Article may be prolonged up to 6 months starting from the day of submitting the request referred to in paragraph 1 of this Article.

Collecting data, information and documentation upon request or initiative

Article 96

The financial intelligence unit may, upon the justified request or information obtained from the other competent organizational units of the administrative authority competent for police affairs, competent tax authority, administrative authority competent for customs affairs, National Security Agency, Agency for prevention of corruption, state prosecution or court, initiate the procedure for collecting and analysing data, information and documentation, when there are reasons or grounds of suspicion of money laundering and related predicate offences or terrorist financing, or that assets originate from criminal activity, in relation to a certain transaction, property or person.

The head of the financial intelligence unit shall make decision on action upon request or information referred to in paragraph 1 of this Article.

The financial intelligence unit shall provide the response upon the request or information referred to in paragraph 1 of this Article which contains information on bank accounts, deposit boxes, financial information, financial analysis and/or results of operational analysis collected in accordance with the paragraph 1 of this Article.

If there are objective reasons for assumption that providing the response referred to in paragraph 3 of this Article would negatively influence to the course or result of investigation or analysis conducted by financial intelligence unit or disclosing information obviously are not proportionate to the interests of natural or legal person or would not be important considering the cause of its request, the financial intelligence unit shall be refuse delivery of the response upon the request referred to in paragraph 1 of this Article.

The financial intelligence unit shall be obliged to explain refusal to provide response to the request referred to in paragraph 1 of this Article.

The relevant authorities referred to in paragraph 1 of this Article in the case of obtaining the response referred to in paragraph 3 of this Article shall be obliged to provide to the financial intelligence unit the feedback of use of the information, as well as with results of the investigations or monitoring based on those information.

Delivery of notification to relevant authorities upon the establishing the existence of reasons for suspicion of money laundering or terrorist financing or that the assets originate from criminal activity

Article 97

If the financial intelligence unit evaluates on the basis of data, information and documentation obtained in accordance with law, that in relation to certain person, transaction, funds or other assets there are reasons for suspicion of money laundering or terrorist financing, or that the assets originate from the crime offence or criminal activity, it shall inform the competent authority in written form accompanied with necessary data, information and documentation about the reasons for suspicion.

If the financial intelligence unit was acting upon the notification referred to in Article 66 paragraphs 6, 10 and 11 of this Law, in the notification referred to in paragraph 1 of this Article it shall not state that that notification was submitted by a reporting entity nor state data about an employee of the reporting entity who has delivered the data, nor deliver that notification, unless there are grounds for suspicion that an employee of the reporting entity has committed the criminal offence of money laundering or terrorist financing, or if those data, required in written form by a competent court, are necessary for establishing facts in criminal proceedings.

The relevant authority referred to in paragraph 1 of this Article shall provide the financial intelligence unit with the feedback of use of the data, information and documentation referred to in paragraph 1 of this Article, as well as to provide the results of investigations and monitoring based on those data, information, and documentation.

Delivering notification to relevant authorities upon the establishing the existence of the reasons for suspicion that other criminal offence was committed

Article 98

If the financial intelligence unit evaluates on the basis of data, information and documentation obtained in accordance with this Law, that in relation to certain person, transaction, funds or other assets that there are grounds for suspicion that another other criminal offence has been committed that is prosecuted ex officio, it shall inform the competent authority in written form accompanied with necessary, data, information and documentation which confirm these reasons for suspicion, in order for it to undertake measures in their jurisdiction.

If the financial intelligence unit was acting upon the notification referred to in Article 66 paragraphs 6, 10 and 11 of this Law, in the notification referred to in paragraph 1 of this Article it shall not state that that notification was submitted by a reporting entity nor state data about an employee of the reporting entity who has delivered the data, nor deliver that notification, unless there are grounds for suspicion that an employee of the reporting entity has committed the criminal offence which is prosecuted ex officio or if those data are necessary for establishing facts in criminal proceedings.

The relevant authority referred to in paragraph 1 of this Article shall provide the financial intelligence unit with the feedback of use of the data, information and documentation referred to in paragraph 1 of this Article, as well as to provide the results of investigations and monitoring based on those data, information, and documentation.

Analysis on efficiency and effectiveness i of the system for preventing money laundering and terrorist financing

Article 99

The financial intelligence unit shall, at least once a year, analyse the efficiency and effectiveness of the system for preventing money laundering and terrorist financing.

The analysis of efficiency and effectiveness of the system for preventing money laundering and terrorist financing shall be preformed based on comprehensive report that financial intelligence unit prepares makes based on:

- Data referred to in Articles 115 and 120 of this Law;
- Data on the size of reporting entity referred to in Article 4, paragraph 2 of this Law, including the number of natural and legal persons, as well as their economic significance;
- Data on financial resources and personnel capacities allocated to the fight against money laundering and terrorist financing to the financial intelligence unit, competent authorities referred to in Article 96 paragraph 1 of this Law and competent supervisory authorities referred to in Article 131 paragraph 1 of this Law.

The Analysis referred to in paragraph 1 of this Article, shall particularly include analysis of:

- Risk of money laundering and terrorist financing on national level;
- Efficiency and effectiveness of coordinated activities of the financial intelligence unit, surveillance authorities referred to in Article 131 paragraph 1 of this Law, other relevant authorities and reporting entities in preventing money laundering and terrorist financing;
- Quality of financial intelligence data, information and documentation obtained through data, information and documentation through international cooperation and

their adequacy for efficient action in regards to perpetrators of criminal offences and their assets;

- Efficiency and effectiveness of the surveillance bodies referred to in Article 131 paragraph 1 of this Law in adequate surveillance, monitoring and arranging of the work of reporting entity, with the purpose of achieving compliance with the request for preventing of money laundering and terrorist financing proportionally identified risks;
- Adequacy of application of measures referred to in Articles 17 and 52 of this Law and reporting of the transactions of reporting entities proportionally to identified risks;
- Achieved results in prevention of the abuse of legal entities for the purpose of money laundering or terrorist financing and the availability of information and about their beneficial owner to the competent authorities;
- Efficiency and effectiveness in the use of financial intelligence data and other data for conducting an investigation about money laundering and terrorist financing by competent authorities;
- Effectiveness of investigations for criminal offences of money laundering and terrorist financing, prosecuting perpetrators of those criminal offences and sanctions imposed for those criminal offences;
- assets, income and funds temporarily and permanently seized;
- Terrorists, terrorist organizations and persons who finance terrorism which are prevented in collection, transmission and use of funds, as well as misuse of non - governmental sector in this purpose;
- Natural and legal persons included in proliferation of weapons for massive destruction and results reached in preventing of the collection, transmission and use of funds, according to relevant resolutions of the United Nations Security Council.

Financial intelligence unit shall send the report about the results of the analysis referred to in paragraph 1 of this Article, to coordinating body referred to in Article 8 of this Law.

Information system of the financial intelligence unit

Article 100

In performing tasks from its jurisdiction, and during receipt, exchange, processing, providing and making data public, submissions, acts and other documents and other ways of communication with reporting entities, authorities, supervisory authorities, monitoring and competent authorities of other countries, as well as in communication between officials referred to in paragraph 3 of this Article, the financial intelligence unit shall use the information system of financial intelligence unit, that represents integrated collection of information communication technologies necessary for collecting, recording, processing and transmission of data, information and documentation in electronic form (herein after referred to as: “the FIU IS”).

FIU IS shall be established and managed by the financial intelligence unit.

Access to data, information and documents referred to in paragraph 1 of this Article shall have officials of the financial intelligence unit unless prescribed otherwise by this Law.

Parts of information system of financial intelligence unit

Article 101

The FIU IS shall consist of:

- Facility, i.e. space that meets all conditions for accommodation and functioning of computer and communication equipment, according to international standards (data centre);
- Facility, i.e. space in which back up computer system and accompanying equipment shall be placed, and in purpose of securing the continuity of work and elimination of the possibility of loss of the data in cases of incidents, conditions for accommodation and functioning of computer and communication equipment, according to international standards (disaster recovery centre);
- Information and communication infrastructure consisting of a set of information and communication technologies for the work of FIU IS;
- Infrastructure systems consisting of systematically implemented computer programs;
- Application systems consisting of specially developed computer programs for business functions;
- Internet systems consisting of specially developed computer programs for providing services on the Internet.

The parts of FIU IS referred to in paragraph 1 of this Article shall be functionally connected and form a single entity.

Managing and access to the FIU IS

Article 102

The financial intelligence unit shall manage FIU IS in line with international standards from area of project management, processes, information safety, operational risks, continuity of operations and other types of management.

The financial intelligence unit shall develop and improve FIU IS according to international standards from area of the development and improvement of information systems.

Only compliance officers of the financial intelligence unit shall have access and manage FIU IS.

By way of exception referred to in paragraph 3 of this Article, access to the FIU IS shall have access to professional persons engaged in maintenance and improvement of the FIU IS, while they do not have access to data, information and documents in the FIU IS.

Professional persons referred to in paragraph 4 of this Article shall not stay in premises, i.e. access to the FIU IS without presence of officer referred to in paragraph 3 of this Article.

The manner of management and engagement of professional persons referred to in paragraph 4 of this Article in the tasks of maintenance and improvement of the FIU IS and other issues of importance for the functioning of the FIU IS shall be regulated by an internal act of the head of the financial intelligence unit.

The act referred to in paragraph 6 of this Article shall be marked with appropriate level of data confidentiality, pursuant to the law governing the data confidentiality.

Revision of the FIU IS

Article 103

The financial intelligence shall revise the FIU IS at least once every two years.

Revision referred to in paragraph 1 of this Article shall imply check of:

- Functionality of all parts of the FIU IS;
- Reliability of the FIU IS;

- Safety of the FIU IS;
- Efficiency and effectiveness of use of the FIU IS;
- Compliance of use of the FIU IS with valid regulations and international standards.

The result of the revision referred to in paragraph 1 of this Article shall be submitted to the head of the financial intelligence unit, who shall adopt a plan of action for improvement and elimination of deficiencies in the FIU IS.

The act referred to in paragraph 3 of this Article shall be marked with appropriate level of data confidentiality, pursuant to the law governing the data confidentiality.

Electronic communication of the financial intelligence unit and other entities

Article 104

The financial intelligence unit shall use unique official address for electronic communication between reporting entities, relevant authorities referred to in Article 96 paragraph 1 of this Law, supervisory authorities referred to in Article 131 paragraph 1 of this Law and relevant authorities of other countries, which it shall be obliged to publish on the internet site of the financial intelligence unit.

An officer in the financial intelligence unit shall use a unique official address for electronic communication for electronic communication for that officer.

The financial intelligence unit shall assign a unique official address for electronic communication for its needs and the needs of its officers.

For the needs of the financial intelligence unit a sub-domain under the domain of state administration body shall be created (foj.gov.me).

The manner of opening, changing and cancelling the unique official address for electronic communication of the financial intelligence unit and its officers shall be regulated by an internal act of the head of financial intelligence unit.

VI. INTERNATIONAL COOPERATION

Establishing international cooperation

Article 105

With a view of establishing and improving international cooperation, the financial intelligence unit may conclude agreements with the competent authorities of foreign countries and international organizations on exchanging financial intelligence data, information and bank accounts and safe deposit boxes, financial information, financial analysis, other information and documentation that can only be used for the purposes provided for by the Law, as well as on other matters of importance in the field of preventing money laundering and terrorist financing.

Request to the competent authority of a foreign state for providing data and information

Article 106

The financial intelligence unit may request from the authority of a foreign state which in that state performs tasks related to prevention of money laundering and terrorist financing and other matters of importance in the field of preventing money laundering and terrorist financing (hereinafter referred to as: “the foreign Financial Intelligence Unit”) to provide information on bank accounts and safe deposit boxes, financial information, financial analysis and other information, information and documentation on persons and assets of importance for preventing money laundering and terrorist financing, related predicate criminal offences, criminal activities and terrorist financing.

The financial intelligence unit may request from authorities of a foreign state or international organization in charge of preventing and detecting money laundering and terrorist financing or authority of a foreign state in charge of confiscation of assets, to provide data, information and documentation referred to in paragraph 1 of this Article.

The financial intelligence unit, at the request of the supervisory authority referred to in Article 131 paragraph 1 of the Law, may request from the supervisory authority of a foreign state the data, information and documentation referred to in paragraph 1 of this Article.

The request referred to in paragraphs 2 and 3 of this Article shall be submitted through the foreign financial intelligence unit.

By way of exception from paragraph 4 of this Article, if there are reasons for urgency, the financial intelligence unit may submit the request referred to in paragraph 2 of this Article to another authority of a foreign state or to an international organization competent for the prevention and detection of money laundering and terrorist financing, or to an authority of a foreign state competent for confiscation of assets.

In the case referred to in paragraphs 1, 2 and 3 of this Article, data, information and documentation may be exchanged electronically, through the means of secure communication systems of the World Association of the financial intelligence units or through another international communication system that provides the same or a higher level of data protection or in another appropriate way in accordance with an international agreement.

Data, information and documentation obtained in accordance with paragraphs 1, 2 and 3 of this Article, may be used by the financial intelligence unit exclusively for the purpose for which they were obtained and shall not, without the prior consent of the foreign financial intelligence unit, other body of a foreign state or international organization competent for the prevention and detection of money laundering and financing terrorist, i.e. the body of a foreign state competent for confiscation of assets, from which they were obtained, use them or distribute them or make them available to another authority, physical of legal person or use them for administrative purposes, for the purpose of investigation or criminal prosecution, or for other purposes that are not in accordance with the conditions and restrictions set by that competent authority of a foreign state, an international organization.

Delivery of data and information upon the request of the foreign financial intelligence unit or other authority of a foreign state

Article 107

The financial intelligence unit may, upon a request containing reasons for suspicion or grounds of suspicion of money laundering and related predicate offenses or terrorist financing or that the assets are proceeds of crime and by stating a purpose for which data are required, provide information on bank accounts and safe deposits boxes, financial information, financial analysis and other data, information and documentation on persons, transactions and assets of importance for prevention and detection of money laundering, related predicate offences, criminal activities or terrorist financing to a foreign financial intelligence unit.

The financial intelligence unit may provide the data, information and documentation referred to in paragraph 1 of this Article to other authorities of a foreign state, supervisory authorities of a foreign state, or r international organizations in charge of prevention and detection of money laundering, and related predicate offences and terrorist financing, upon their request.

In the case referred to in paragraphs 1 and 2 of this Article, data, information and documentation may be exchanged electronically, through the means of secure communication systems of the World Association of financial intelligence units or through another international communication system that provides the same or a higher level of data protection or in another appropriate way in accordance with international agreement.

By way of exception from paragraph 3 of this Article, the financial intelligence unit may, upon the justified request of the European Union Agency for cooperation in the field of law enforcement of the European Union (hereinafter referred to as: “the Europol”), submit information on bank accounts and safe deposit boxes, financial information and financial analyses referred to in paragraph 1 of this Article, through a network application for the safe exchange of Europol information in cases of prevention, detection and suppression of serious criminal offenses that fall within the competence of Europol.

The financial intelligence unit may respond to A request of a foreign financial intelligence unit even in cases where the predicate criminal offense or criminal activity is not known at the time of receiving the request.

The financial intelligence unit shall inform the requesting authority in writing and state the reasons for the rejection of the request referred to in paragraphs 1, 2 and 4 of this Article.

A foreign financial intelligence unit may provide the obtained data, information and documentation referred to in paragraph 1 of this Article to another competent authority or a third party, only with the prior consent of the financial intelligence unit.

The financial intelligence unit shall not give consent referred to in paragraph 7 of this Article if:

1) Provision of data, information and documentation would be disproportionate to the legitimate interests of an individual or legal entity or Montenegro;
2) Provision of data, information and documentation would endanger or could endanger the course of investigations or the conduct of criminal proceedings in Montenegro, or otherwise harm the interests of those proceedings;
3) Provision of data, information and documentation is not in accordance with the basic principles of the legal system of Montenegro.

The financial intelligence unit shall prepare a written reasoning for the rejection of granting consent referred to in paragraph 7 of this Article and deliver it to the requesting authority.

Data, information and documentation submitted in accordance with paragraphs 1, 2 and 4 of this Article may be used exclusively for the purpose for which they were requested and submitted, in accordance with the Law.

The financial intelligence unit may determine conditions and limitations for the use of data referred to in paragraphs 1, 2 and 4 of this Article.

Competent authorities referred to in Article 96 paragraph 1 of the Law may exchange data on bank accounts and safe deposit boxes, financial information, financial analysis obtained from the financial intelligence unit, upon request and on an individual basis, with other authorities of a foreign state, only with the prior consent of the financial intelligence unit and if such data and financial information and financial analysis are necessary for the prevention, detection and suppression of money laundering, related predicate crimes and terrorist financing.

The provisions of the law governing the protection of personal data shall be applied on the protection of data and information exchanged in accordance with paragraphs 1, 2, 4 and 12 of this Article.

Delivery of data to the competent authority of a foreign state on financial intelligence unit's own initiative

Article 108

The financial intelligence unit may provide, without a request, on its own initiative, to a foreign financial intelligence unit , other authorities of a foreign state, supervisory authorities of a foreign state, authorities of a foreign state responsible for confiscation of pecuniary gain or international organizations responsible for preventing and detecting money laundering and related predicate criminal offenses and terrorist financing, information about bank accounts and safe deposit boxes, financial information, financial analyses and other data, information and documentation about persons or assets for which there are reasons for suspicion or grounds of suspicion of money laundering and related predicate offences or terrorist financing or that the assets are proceeds of crime, and which it has obtained in accordance with this Law, for the purpose of preventing and detecting money laundering, related predicate criminal offenses and terrorist financing.

When delivering data, information and documentation in accordance with paragraph 1 of this Article, the financial intelligence unit may prescribe the terms and limitations under which a foreign authority competent for detection and prevention of money laundering or terrorist financing may use such data.

Temporary suspension of transaction upon the initiative of the competent authority of a foreign state

Article 109

In accordance with this Law, the financial intelligence unit may, by reasoned written initiative of a foreign financial intelligence unit or another body of a foreign state, suspend a transaction or ban access to safe deposit box, with written order, for the period not exceeding 72 hours.

The financial intelligence unit shall act in accordance with Article 93 of this Law in the case referred to in paragraph 1 of this Article.

The financial intelligence unit may reject the initiative referred to in paragraph 1 of this Article if based on the facts and circumstances stated in the initiative, if it evaluates that given reasons are not sufficient for a suspicion or grounds of suspicion that money assets or other assets are proceeds of crime or of money laundering and related predicate offences or terrorist financing, and it shall inform in written form the foreign financial intelligence unit or another authority of foreign state, by stating the reasons for its rejection.

The initiative to a foreign competent authority for temporary suspension of transaction

Article 110

The financial intelligence unit may, within its competencies and authorities, submit written initiative for temporary suspension of transaction or ban to accessing a safe deposit box to a foreign financial intelligence unit or another authority of a foreign state competent for the prevention of money laundering and related predicate criminal offences and terrorist financing, if it evaluates that there are reasons for a suspicion or grounds of suspicion that assets or property are proceeds of crime or of money laundering and related predicate offences or terrorist financing have been committed.

VII. OBLIGATIONS OF THE STATE AND OTHER AUTHORITIES AND INSTITUTIONS

Authority responsible for customs affairs

Article 111

The authority responsible for customs affairs shall be obliged to provide the financial intelligence unit with immediate electronic access to data on:

- Cross border declaration on transport of money, checks, bearer securities, precious metals and precious stones, in the value or amount of EUR 10,000 or more, not later than within 3 days from the day of transporting;
- Cross border transport of money, checks, bearer securities, precious metals and precious stones, in the value or amount of EUR 10,000 or more, that were not declared or were falsely reported, immediately or not later than within 3 days from the day of transporting;
- Transport or attempt of transport of money, checks, securities, precious metals and precious stones in the value or amount lower than EUR 10,000, if in relation to that transport or attempt of transport there are reasons for suspicion of money laundering or terrorist financing, immediately or not later than within 3 days from the day of transporting or attempt of transporting.

Registers of accounts and safe deposit boxes

Article 112

Registers of accounts and safe deposit boxes shall represent an electronic database of open accounts of individuals and legal entities and leased safe deposit boxes, as well as demand deposits and time deposits with credit institutions and branches of foreign credit institutions, managed by the Central Bank of Montenegro.

Credit institutions and branches of foreign credit institutions shall submit data on open accounts of individuals and legal persons and leased safe deposit boxes to the Central Bank of Montenegro, immediately after opening an account or concluding a contract.

Credit institutions and branches of foreign credit institutions shall submit data on demand deposits and time deposits to the Central Bank of Montenegro, no later than the end of the following day since the day of conclusion of the contract.

Registers of accounts and safe deposit boxes shall be maintained through the Central Register of Transaction Accounts in accordance with the law governing payment transactions and in accordance with this Article, whereby data on leased safe deposit boxes may be kept in a separate register or as part of the Central Register of Transaction Accounts.

The Central Bank of Montenegro shall be liable for the authenticity of the data in the registers of accounts and safe deposit boxes with the data provided by credit institutions and branches of foreign credit institutions.

Data from registers of accounts and safe deposit boxes shall not be publicly available and their processing, protection and storage are subject to the regulations governing bank secrecy and the regulations governing the protection of personal data.

The content of registers of accounts and safe deposit boxes, the data submitted for the purposes of these registers, the method of submitting data and the method of obtaining access to the data from these registers shall be prescribed by the Central Bank of Montenegro.

Data from the register of accounts and safe deposit boxes available to the financial intelligence unit

Article 113

The financial intelligence unit shall have direct electronic access to at least the following data from register of accounts and safe deposit boxes:

1) for individuals: first and last name, unique identity number for a resident, type, number and country of issuance of a personal document for a non-resident, address and city of residence;
2) for legal entities: name, registration number, headquarters (address, city, country);
3) type and number of the account, name of the credit institution that opened the account, data on the status of the account (active, closed or blocked), date of opening and closing of the account;
4) Date of conclusion and termination of validity of the agreement on leasing a safe deposit box, as well as the period for which the agreement was concluded.

Data referred to in paragraph 1 of this Article should be available to the financial intelligence unit based on personal data or account number.

Stock exchanges and clearing and depository companies

Article 114

Stock exchanges and clearing and depository companies shall, without delay, inform the financial intelligence unit, if during carrying out activities within the scope of its business, detect facts indicating possible connection with money laundering and related predicate offences or terrorist financing.

Upon the request of the financial intelligence unit , stock exchanges and clearing and depository companies shall provide data, information or documentation indicating possible connection with money laundering and related predicate offences or terrorist financing, in accordance with law.

The clearing and depository company shall electronically submit on quarterly basis data to the financial intelligence unit on each collective custody account, credit institution or other institution with which that custody account is opened, as well as on the number of transactions and total turnover on that collective custody account.

Regarding the deadlines for providing the data referred to in paragraph 2 of this Article, the provisions referred to in Article 90 paragraphs 4, 5 and 6 of this Law shall apply.

Stock exchanges and clearing and depository companies shall submit data referred to in paragraphs 1, 2 and 3 of this Article in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law.

State prosecutors' offices, courts and other state authorities competent for judicial affairs

Article 115

For the purpose of making analysis referred to in Article 99 of this Law, competent state prosecutor's offices, courts and state authorities competent for the judicial affairs shall provide regularly to the financial intelligence unit data and information on proceedings related to on misdemeanours, economic crimes and criminal offences related to money laundering and terrorist financing, their perpetrators, as well as confiscation of assets acquired by committing a criminal offence of criminal activity.

The competent state prosecutors' offices shall submit the following data to the financial intelligence unit:

1) Name of the state prosecutors' office, number and date of raising indictment;
2) Name and surname, date of birth, address and unique identity number of the accused individual, and for foreigners, the number, country of issue and date of expiry of the travel document, that is, the name, identity number, registered office (address) of the accused legal entity;
3) Legal qualification, place, time and manner of committing criminal offence;
4) Legal qualification, place, time and manner of committing predicate criminal offence.

The competent courts shall submit the following data to the financial intelligence unit:

1) Name of the court, case number and date;
2) Name and surname, date of birth, address and unique identity number of the individual against whom proceedings have been initiated or who has submitted a request for judicial protection within the misdemeanour proceedings under this Law, and for foreigners, the number, country of issue and date of expiry of the travel document, that is, the name, registration number, registered office (address) of the legal entity against which proceedings have been initiated or which has submitted a request for judicial protection within the misdemeanour proceedings under this Law;
3) Stage of the proceeding and the final decision;
4) Legal qualification of the criminal offence or misdemeanour;
5) Name and surname, date of birth, address and unique identity number of an individual for whom a temporary security measure (freezing of assets) or temporary seizure of movable property (seizure) has been determined, and for a foreigner, the number, country of issue and date of expiry of the travel document, that is, the name, registration number, headquarters (address) of the legal entity for which a temporary security measure (freezing of assets) or temporary seizure of movable assets (seizure) has been determined;
6) Date of issuance and duration of the order on temporary security measures (freezing of assets) or temporary seizure of movable assets (seizure);
7) Amount of assets or the value of the property for which the order on a temporary security measure (freezing of property) or temporary seizure of movable assets (seizure) has been issued;
8) Amount of confiscated funds or the value of confiscated property;
9) Received and sent rogatory letters regarding criminal offenses referred to in paragraph 1 of this Article or predicate criminal offenses.

The state administration authority competent for judicial affairs shall provide the financial intelligence unit with data on received and sent requests for international legal assistance in connection with the criminal offenses referred to in paragraph 1 of this Article, as well as data on temporarily and permanently seized property.

Data referred to in paragraphs 2, 3 and 4 of this Article shall be submitted to the financial intelligence unit once a year, and no later than the end of February of the current year for the previous year, as well as at the request of the financial intelligence unit, in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law.

VIII. RECORDS, PROTECTING AND KEEPING DATA

1. Records keeping and contents

Records kept by a reporting entity

Article 116

Reporting entity shall keep:

1) records on CDD measures and monitoring of the customer's business;
2) records of complex and unusual transactions;
3) records of data submitted to the financial intelligence unit in accordance with Article 66 of this Law;
4) records of orders on temporary suspension of execution of the transaction or prohibition of access to the safe;
5) records of requests for the ongoing monitoring of client's financial operations;
6) records of access by supervisory authorities referred to in Article 131 paragraph 1 of this Law, to data, information and documentation in connection with which the reporting entity shall act in accordance with Article 123 paragraph 1 of this Law;
7) Records on the professional training and development of employees of the reporting entity in the field of the prevention of money laundering and financing of terrorist.

The reporting entity shall keep records referred to in paragraph 1 of this Article in a manner that will ensure the reconstruction of individual transactions, including the amounts and currency, that could be used as evidence in the process of detecting customer's criminal activities.

Content of the reporting entities' records

Article 117

The records on the CDD measures and monitoring of the customer's business shall contain the following data:

1) For a legal entity: name, registered office (address, city, or municipality for a legal entity with its registered office in Montenegro, and for a legal entity with its registered office in another country, state and the city), tax identification number, information on whether it is a resident or non-resident, reason for the business relationship (establishing a business relationship, making a transaction, trying to make a transaction, renting a safe, accessing the safe, insurance policyholder, insurance beneficiary, seller, buyer), phone number and e-mail address;
2) For an entrepreneur: name, registered office (address, city or municipality for an entrepreneur with headquarters in Montenegro, and for entrepreneurs with headquarters in another country, state and the city), unique identification number, first and last name, information on whether they are a resident or non-resident, reason for the business relationship (establishing a business relationship, making a transaction, trying to make a transaction, renting a safe, accessing the safe, insurance policyholder, insurance beneficiary, seller, buyer), phone number and e-mail address;
3) For a natural person: name and surname, unique identification number, address and municipality of residence, i.e. residence in Montenegro, date of birth, country of birth, citizenship, information on whether the person is a politically exposed, information on whether they are a resident or non-resident, telephone number and e-mail address, type, number, country of issue and date of expiry of the personal document, reason for the business relationship (establishing a business

relationship, making a transaction, attempting to make a transaction, renting a safe, access to a safe, insurance policyholder, insurance beneficiary, seller, buyer), information on whether a natural person is a client, representative, authorized person, real owner, founder, trustee, user of property managed, insured, policy holder, insurance beneficiary, seller or buyer;

4) Data on the manner the customer's identification (identification based on the physical presence, electronic identification or video-electronic identification);

5) Video-audio recording created during the video-electronic identification of the customer;

6) The purpose, allocation, goal, nature of the business relationship and transaction, the basic code of the customers' activity and the scanned documentation accompanying the business relationship or transaction, data on the source of assets and funds that are or will be the subject of the business relationship or transaction, the date of establishment of the business relationship, that is, the date and time of entering the casino or accessing the safe;

7) Transaction data: date and time of transaction execution, transaction amount in euros, transaction amounts by currency, transaction order number, policy or contract, depending on the type of the reporting entity, information on whether the transaction was executed in full or in part, information on the type of transaction (cash or non-cash), data on the type of transaction (regular, suspicious, unusual or complex), data on the credit institution of the payer and payee (account type and number, identification number, name and country of registered office), data on the type of transaction (payment or disbursement), information on the method of execution of the transaction depending on the type of the reporting entity (cash, non-cash, already realized, in instalments, market or non-market), information on the purpose and purpose of the transaction and the name of the branch of the reporting entity preforming the transaction.

If the reporting entity is an organizer of games on chance or provides safe deposit box rental services, the record on CDD measures and monitoring the customer's business, in addition to the data referred to in paragraph 1 point 3 of this Article, for natural persons shall also contain data on the behaviour of the natural person depending on the type of the reporting entity (entry into space for organizing games on chance, access to games on chance via the Internet or other telecommunication means, access to the cash register, access to other places, i.e. locations where transactions are carried out in accordance with the type of game on chance or access to the safe).

If the transaction is related to the reporting entities referred to in Article 4, paragraph 2, point 1 of this Law, the record of measures to know and monitor the customer's business, in addition to the data referred to in paragraph 1, point 7 of this Article, shall also contain the following data about the transaction: type and number of the account, registration number, name and country of the registered office of the credit institution of the account, first and last name, address and the city of residence, i.e. residence of the natural person to whom the transaction is intended, i.e. name, registered office (address, city and country) of the legal person to whom the transaction is intended, telephone and e-mail address of those persons, SWIFT code of the credit institution, country of destination, name and the country of the registered office of the credit institution that is the correspondent.

If the transaction is related to the reporting entities referred to in Article 4, paragraph 2, point 7 of this Law, the record of measures to know and monitor the customer's business, in addition to the data referred to in paragraph 1, point 7 of this Article, shall also contain the following data about the transaction: stock exchange code, security code, number of shares, share price, seller's broker code, buyer's broker code, seller's account number on the stock exchange, as well as buyer's account number on the stock exchange.

If the transaction is related to the reporting entities referred to in Article 4, paragraph 2, items 8 and 9 of this Law, the record of measures to know and monitor the customer's business, in addition to the data referred to in paragraph 1 point 7 of this article, shall also contain the following data about the transaction: insurance start date, insurance duration in years, information on the type of the premium (one-time, monthly, quarterly , semi-annual or annual), first and last name of the beneficiary of the premium insurance and information on the reason for the payment (insured event, termination of the contract or expiration of the contract).

If the transaction is related to the reporting entities referred to in Article 4, paragraph 2, point 13 and paragraph 4 of this Law, the records on the CDD measures of monitoring of the customer's business, in addition to the data referred to in paragraph 1, point 7 of this Article, shall also contain the following data on the subject of the transaction, namely:

1) for valuable items: information about the type of valuable item (art, precious metal, precious stones, securities, crypto wallet or other valuable items), information about the art (name, value, description, category, subcategory, style, theme, technique and material), data on precious metals (name, value, description, weight, number of carats, colour of the metal, type, clarity, size and type of the metal), data on precious stones (width, clarity of diamond, dimensions of diamond, shape, colour and data on clarity, i.e. purity), data on the bearer of securities (symbol, type and status of the security, unique identification mark of the financial instrument in accordance with the ISO 6166 standard ISIN), data on the crypto wallet (code of the crypto wallet and service provider crypto wallet), data on other valuable items (name, value and description);
2) for immovable property: information on the type and the value of the immovable property, address, house number, city, postal code, country, immovable property registration number, information on right in rem to that immovable property, the basis for acquiring the right in rem, area, number of floors, date of registration of the right in rem to the real estate cadastre , cadastral municipality, plot number, area, notes, scope of rights and age of the immovable property;
3) for means of transport: information on the type (road vehicle, vessel, aircraft or other means of transport), value, type and registration number, country in which the means of transport is registered, registration validity date, make and model, chassis number, name of the manufacturer, identification number, information on the category, manufacturer, type/model and serial number of the engine of the means of transport, as well as the type i.e. name of the vessel.

Records of complex and unusual transactions shall contain data referred to in paragraphs 1 to 6 of this Article.

The record of data submitted to the financial intelligence unit in accordance with Articles 66 and 90 of this Law shall contain data referred to in paragraphs 1 to 6 of this Article, data on indicators from the list of indicators for identifying suspicious customers and transactions, data on reasons for suspecting that the property originates from criminal activity or that it is about money laundering, related predicate crimes or terrorist financing, the date of data submission to the financial intelligence unit and the reasons for executing the transaction (reasoning).

The record of orders on temporary suspension of transaction execution or prohibition of access to the safe shall contain the order number of the transaction that is temporarily suspended, the amount of the transaction, the date and time of the start of the temporary suspension of the transaction, the date and time of the extension of the temporary suspension of the transaction, the balance on the account before the blocking and the data referred to in paragraph 1 points 1, 2 and/or 3 of this Article for the person to whom the temporary suspension of the transaction applies.

Records of requests for monitoring the customer's financial operations shall continuously contain the number of requests, information on the type and number of the customer's account, the starting date of monitoring, the extension date of the monitoring, data referred to in paragraph 1 points 6 and 7 and paragraph 3 of this Article that occurred during the monitoring period and the data referred to in paragraph 1 points 1, 2 and/or 3 of this Article for the person to whom that monitoring refers.

The record of the access of supervisory authorities referred to in Article 131 paragraph 1 of this Law to data, information and documentation in connection with which the reporting entity shall be obliged to act in accordance with Article 123 paragraph 1 of this Law shall contain the name of the supervisory authority, the name and surname of the supervisory officer, the date and time of data inspection, information and documentation referred to in paragraph 1 points 1, 2 and/or 3 of this Article for the person whose the data, information and documentation were inspected.

The record of professional training and professional development of employees in the field of prevention of money laundering and financing of terrorist shall contain the name and surname and workplace of the employee who completed the professional training and professional development, the name and date of the professional training and professional development, the name of the professional training and professional development organizer (employer, professional association, financial intelligence unit or other professional body or organization in Montenegro or another country).

Records kept by the customs authority

Article 118

Customs authority shall keep the following:

1) Records of any in-take or out-take or attempt to in-take or out-take across the state border of reported, unreported or falsely reported money, checks, bearer securities, precious metals and precious stones, in the amount or value of EUR 10,000 or more;
2) Records of the in-take or out-take across the state border of money, checks, bearer securities, precious metals and precious stones, in the amount or value less than EUR 10,000, when there are reasons for the suspicion or grounds for suspicion that the property originates from criminal activity or money laundering or terrorist financing.

Content of the records of the customs authority

Article 119

Records of any in-take or out-take or attempt to in-take or out-take across the state border of reported, unreported or falsely reported money, checks, bearer securities, precious metals and precious stones, in the amount or value of EUR 10,000 or more, shall contain following records of data:

1) For the natural person who transports or attempts to transport across the state border cash, checks, bearer securities, precious metals and precious stones: name and surname, unique identification number, address and the city of residence, citizenship , type, number, country of issue and date of validity of the personal document;

2) For the legal person, or the natural person for whom cross border transport of cash, checks, bearer securities, precious metals and precious stones is performed: name, registered office (address, city, or municipality for legal person with headquarters in Montenegro, or the state for legal entities with headquarters in another country), registration number and TIN of the legal person, i.e. first and last name, unique identification number, address and city of residence, i.e. residence and citizenship of the natural person;

3) For the legal person, or the natural person which is the intended recipient of cash: name, registered office (address, city, or municipality for legal person with headquarters in Montenegro, or the state for legal entities with headquarters in another country), registration number and TIN of the legal person, i.e. first and last name, unique identification number, address and city of residence, i.e. residence and citizenship of a natural person;

4) Amount, currency and information on the type, source and purpose of cash that is brought in or taken out or attempted to be brought in or taken out across the state border;

5) Information on valuable items that are imported or exported or attempted to be imported or exported across the state border: information on the type of valuable item (cheques, bearer securities, precious metals or precious stones), the source and purpose of using the valuable item, data on bearer securities (symbol, type and status of the security, unique identification mark of the financial instrument in accordance with the ISO 6166 standard - ISIN), data on precious metals (name, value, description, weight, number of cards, metal colour , type, clarity, size and type of metal), information about precious stones (width, clarity of the diamond, dimensions of the diamond, shape, colour, information about clarity, i.e. clarity), depending on the availability of data;

6) Name of the border crossing point where the entry or amount or attempted entry or amount of cash, checks, bearer securities, precious metals and precious stones across the state border was carried out, date and time of entry or amount or attempted entry or amount of such property across the state borders, information on whether it is entry or exit from Montenegro and the name of the country the property is being exported from or the country it is being imported to;

7) information on whether the import or export of money, checks, bearer securities, precious metals and precious stones was reported, unreported or falsely reported to the administrative authority responsible for customs affairs.

Records on the import or export across the state border of money, checks, bearer securities, precious metals and precious stones, in the amount or value of less than EUR 10,000, where there are reasons for suspicion or grounds for suspicion that the property originates from criminal activity or that it is about money laundering or terrorist financing, shall contain information referred to in paragraph 1 points 1 to 6 of this Article and data on indicators for identifying suspicious customers in relation to a specific case and data on whether the transaction has been withheld from execution.

Records kept by the financial intelligence unit

Article 120

The financial intelligence unit shall keep following:

l) Records of the analyses it performs and the cases on which it acts in accordance with the law;

2) Records of the reporting entities, authorized persons for the prevention of money laundering and terrorist financing, or their deputies;

3) Records of criminal offences and misdemeanours and perpetrators of criminal offences and misdemeanours referred to in Article 115 of this Law;

4) Records on the actions of the supervisory authorities referred to in Article 131 paragraph 1 of this Law towards the reporting entities;

5) Records of the officers of the financial-intelligence unit who had insight, that is, access or to whom data from other authorities was provided in accordance with Article 126 of this Law.

Access to the data from the records referred to in paragraph 1 of this Article shall be done by electronic identification.

Content of the records kept by the financial intelligence unit

Article 121

The record of the performed analyses and the cases acts upon in accordance with the Law shall contain the following data:

- data referred to in Article 117 paragraphs 1 to 6 and paragraphs 8 and 9 of this Law;
- case number, name of the case, number of the received document, name and surname, i.e. the name of the sender and recipient of the document, date of sending the document, date of delivery of the document, information on whether the document is marked with a degree of secrecy, data representing the reasons for temporary suspension of the transaction, data that represent the reasons for continuous monitoring of the customer's financial operations, the legal qualification of the criminal offense, the result of the operational or strategic analysis, the reasons for not providing a response to the request or information in accordance with Article 96 paragraphs 4 and 5 of this Law, scanned received and sent documents, scanned documentation attached to documents; and
- data on persons subject to the financial analysis: mobile phone number, International Unique Mobile Device Identifier (IMEI), photograph, scanned page with personal document data, scanned card of deposited signatures, previous personal data (unique personal identification number, first and last name and date of birth), false personal data (unique identity number, first and last name, date of birth, residential address, citizenship), previous names of the legal entity and information about the founder of the legal entity (identity number, TIN, name, address, city and country of the registered office, the country legal entity is registered in).
- Data on orders for temporary suspension of execution of transactions referred to in Articles 93, 109 and 110 of this Law;
- Data on requests for continuous monitoring of the client's financial operations referred to in Article 95 of this Law;
- Data from responses on requests referred to in Articles 91 and 92 of this Law;
- Data from requests, information and notification referred to in Articles 96, 97 and 98 of this Law;
- Data on international requests and information referred to in Articles 106, 107 and 108 of this Law;
- Data taken over from the authority responsible for customs affairs referred to in Article 111 of this Law;
- Data on bank accounts and safe boxes referred to in Article 113 of this Law;

- Data on delivery of stock exchanges and clearing and depository companies referred to in Article 114 of this Law; and
- Data from documents sent and received;

The record on the reporting entities, authorized persons for the prevention of money laundering and financing of terrorist, i.e. their deputies shall contain the following data:

1) For the reporting entity: identification number, TIN, name and registered office (address, city, or municipality for reporting entities based in Montenegro, or country for reporting entities based in another country) and the work permit information (issued, revoked or not required);
2) For the authorized person for the prevention of money laundering or their deputy: unique identity number, first and last name, information on whether the person is an authorized person for the prevention of money laundering or their deputy, e-mail, phone number, mobile phone number, start and end date of performing the duties of an authorized person for the prevention of money laundering and financing of terrorist, i.e. their deputy, license number, date of issuance and expiration of the license.

Records on criminal offences and misdemeanour and perpetrators of the criminal offences and misdemeanours referred to in Article 115 of this Law shall contain data referred to in Article 115 paragraphs 2, 3 and 4 of this Law.

Records on the actions of supervision bodies referred to in Article 131 paragraph 1 of this Law towards the reporting entities shall contain data referred to in Article 135 paragraphs 1, 2, 4 and 5 of this Law.

The record of the officers of the financial-intelligence unit who had insight into, or access to, or to whom data from other authorities was provided in accordance with Article 126 of this Law, shall contain the unique identification number of the employee of the financial-intelligence unit who had insight, i.e. to whom the data was provided, legal basis, date and time of inspection, access, or delivery of data, as well as the data they had access to, or that was delivered to them.

Data records on non-residents

Article 122

In case a non-resident who is a natural person does not have a unique identification number, the date of birth, country of birth, number, country of issue and the type of personal document, as well as the date of expiry of the personal document shall be entered in the records and registers prescribed by this Law, and for a non-resident who is a legal person, instead of the registration number, the TIN shall be entered, unless otherwise provided by this Law.

2. Data Protection

Prohibition of data disclosure

Article 123

Reporting entities and their employees, including the members of the management and supervisory boards or other business-managing authorities of reporting entities, and other persons to whom data referred to in Article 117 paragraphs 1 to 11 of this Law are available or have been available, shall not reveal to a customer or third person the following:

1) Information disclosed to the financial intelligence unit, i.e. information made available for inspection or submitted documentation about the customer or transaction in accordance with Articles 66 and 90 of this Law;
2) The financial intelligence unit, on the basis of Article 93 of this Law, has issued an order to temporarily suspend the transaction or prohibit access to the safe, i.e. gave instructions to the reporting entity in this regard;
3) That the financial intelligence unit on the basis of Article 95 of this Law has demanded regular monitoring of customer's business;
4) That against the customer or a third party, an investigation is or has been initiated or could be initiated due to the grounds for suspicion or well-founded suspicion that the criminal offense of money laundering, a related criminal offense or the financing of terrorist has been committed.

Disclosure, for the purpose of paragraph 1 of this Article, shall not be considered an attempt to retort the customer from engaging, performing, or participating in an illegal activity.

The prohibition of disclosure referred to in paragraph 1 of this Article shall not apply to data that, in accordance with this Law, is obtained and maintained by the reporting entity and that is necessary for the establishment of facts in criminal proceedings and if the submission of such data in written form is requested or ordered by a competent court or supervision body referred to in Article 131 paragraph 1 of this Law for the purpose of implementing this Law.

Data referred to in paragraph 1 of this Article, notifications on suspicious transactions, financial information, financial analyses, as well as all other data, information and documentation that the financial-intelligence unit in accordance with this Law collected or prepared in order to prevent and detect money laundering, with it connected predicate criminal acts and financing of terrorist may not be submitted to other persons for inspection, nor can their existence be confirmed in the records of the financial-intelligence unit, unless otherwise provided by this Law.

When there are grounds for suspicion that it is money laundering, with related predicate criminal acts and financing of terrorist, data referred to in paragraph 4 of this Article shall be marked with an appropriate level of secrecy in accordance with the law that regulates data confidentiality.

The data, information and documents referred to in paragraph 5 of this Article may be declassified if there is no other way to achieve a timely exchange of data at the national and international level in order to effectively prevent, detect and prosecute money laundering crimes, related predicate crimes and terrorist financing, with the obligation to store data in accordance with Article 130 of this Law.

In order to ensure efficient and timely international cooperation, information, notices and requests referred to in paragraph 4 of this Article marked with the level of secrecy "RESTRICTED" may be submitted to foreign financial intelligence units, other competent authorities of other countries and international organizations and through the communication systems of the World Association of Financial intelligence units.

Exception to the principle of keeping confidentiality

Article 124

The obligation to preserve data confidentiality (business, banking, professional and other secrets) shall not apply to the reporting entities, holders of public authority, state authorities and their employees when submitting data, information and documentation to the financial intelligence unit, in accordance with this Law, as well as to the reporting entity who is a member of the financial group when exchanging data and information with other members of the financial group under the conditions from Article 62 of this Law.

Reporting entity and their employees shall not be liable for damage caused to their customers or third parties if in accordance with this Law they:

1) Provide data, information and documentation on their customers to the financial intelligence unit;
2) Obtain and process data, information and documentation on their customers;
3) Execute the financial intelligence unit's order on temporary suspension of transaction or prohibition of access to the safe deposit box;
4) Carry out the financial intelligence unit's request on continuous monitoring of customer's financial business.

Reporting entity's employees shall not be disciplinary or criminally liable for breach of obligation of keeping data secrecy if they:

1) Provide data, information and documentation to the financial intelligence unit, in accordance with this Law;
2) Process data, information and documentation, obtained in accordance with this Law, with a view to verifying customers and transactions or grounds for suspicion that the property originates from criminal activity or that it is money laundering or terrorist financing.

Protection of the integrity of the authorized person and employees

Article 125

The reporting entity shall be obliged to take the necessary measures to protect the authorized person for the prevention of money laundering and financing of terrorist and other employees who implement the provisions of this Law from threats and other unfavourable or discriminatory actions aimed at their physical or psychological integrity.

Use of received personal data

Article 126

The financial intelligence unit, state authorities, state administration authorities, and holders of public authority, reporting entities and their employees shall be obliged to use the personal data they receive in accordance with this Law only for those purposes they are obtained for.

On inspection, access and submission to the financial intelligence unit of data referred to in Article 47 paragraph 1 point 1, Article 55 paragraph 2, Article 92 paragraph 4 and Articles 111 and 113 of this Law, the authorities that provide electronic access to the above-mentioned data shall keep records that contain information that the financial intelligence unit carried out an inspection, i.e., access, or that the data was delivered to it electronically, as well as the date and time of the beginning, that is, the end of the inspection and access to data.

For the exchange of personal data between the financial intelligence unit and state authorities, state administration bodies and holders of public authority, a security communication link shall be used, which represents a protected system of data exchange between precisely defined entities.

The regulations governing the protection of personal data shall be applied to the processing, protection and storage of personal data referred to in paragraphs 1, 2 and 3 of this Article.

Keeping data

Article 127

Reporting entity shall keep records obtained in accordance with this Law, related documentation, data on identification number of each customer's account, data and documentation on wire transfers, documentation on business correspondence and reports at least ten years after the termination of business relationship, executed transaction, entrance of the customer into casino and facilities where other special games on chance are organized or access to the safe deposit box, unless a specific law prescribes longer period for data keeping.

The reporting entity shall keep a photocopy of a personal identification document, other documents and documentation, as well as written powers of attorney in accordance with the paragraph 1 of this Article.

Reporting entity shall keep data and related documents on compliance officer for prevention of money laundering and terrorist financing, and their deputy, professional trainings of employees in the area of prevention of money laundering and financing of terrorist and the application of measures of internal control audit for the period of four years after the termination of validity of the license, i.e. completed professional training and improvement and completed internal control and audit.

After the expiration of the deadlines referred to in paragraphs 1, 2 and 3 of this Article, the reporting entity shall be obliged to delete or destroy the customer's personal data.

Keeping data with the administrative authority responsible for customs affairs

Article 128

The customs authority shall keep data from records referred to in Article 119 of this Law for the period of ten years after the date of obtaining those data.

After the expiration of the period referred to in paragraph 1 of this Article the personal data referred to in Article 119 of this Law shall be destroyed.

Keeping data in the Register of beneficial owners and registers of accounts and safe deposit boxes

Article 129

The administrative body responsible for tax collection shall be obliged to keep the data in the Register of beneficial owners for ten years from the day that is considered the day of cessation of the existence of the subject referred to in Article 43 paragraph 3 of this Law in accordance with the Law.

The Central Bank of Montenegro shall be obliged to keep the data in the registers of accounts and safes for ten years after the account is closed, that is, after the contract for renting the safe deposit box has expired.

After the expiration of the period referred to in paragraphs 1 and 2 of this Article, personal data from the Register of beneficial owners, i.e. registers of accounts and safe deposit boxes shall be deleted.

Record keeping at the financial intelligence unit

Article 130

The financial intelligence unit shall keep data and information from records kept in accordance with this Law for the period of 11 years after the date of obtaining those data.

Data referred to in paragraph 1 of this Article shall be depersonalized after the deadline referred to in paragraph 1 of this Article has expired, and data that is in paper form shall be destroyed in such a way that it is handed over to the competent recycling centre.

The financial intelligence unit shall not inform a person on information and data it possesses in relation to them, nor another person, nor allow access before the expiration of 10 years from the date of their recording, unless otherwise provided by this Law.

The person referred to in paragraph 3 of this Article shall have the right to check their personal data after the expiration of 10 years from the date of their recording.

The detailed method of depersonalization of data referred to in paragraph 1 of this Article shall be prescribed by the Ministry by an internal act.

The act referred to in paragraph 5 of this Article shall be marked with appropriate level of data confidentiality, pursuant to the law governing the data confidentiality.

IX. SUPERVISION

Inspection and other supervision

Article 131

Inspection and other supervision, within the competencies defined by law, shall be done by:

1) The Central bank of Montenegro in relation to reporting entities referred to in Article 4 paragraph 2 Items 1, 2, 3 of this Law, to which it issues license or approval for operation;
2) The Agency for Electronic Communications and Postal Services in relation to reporting entities referred to in Article 4 paragraph 2 item 4 of this Law;
3) The Commission for the Capital Market of Montenegro in relation to reporting entities referred to in Article 4 paragraph 2 points 5, 6 and 7 of this Law and legal entities referred to in Article 114 of this Law;
4) The Insurance Supervision Agency in relation to reporting entities referred to in Article 4 paragraph 2 items 8 and 9 of this Law;
5) State administrative authority responsible for the affairs of games on chance in relation to reporting entities referred to in Article 4 paragraph 2 point 10 of this Law;
6) Competent tax authority responsible for the affairs for tax collection in relation to reporting entities referred to in Article 4 paragraph 2 item 11 of this Law and entities referred to in Article 43 paragraph 3 of this Law;
7) State administrative authority responsible for digital assets in relation to reporting entities referred to in Article 4 paragraph 2 item 12 of this Law.
8) Ministry, through an authorized person, in relation to the reporting entities referred to in Article 4 paragraph 2 point 13 of this Law;
9) The Bar Association of Montenegro in relation to reporting entities referred to in Article 4 paragraph 3 of this Law;
10) State administration body responsible for judicial affairs in relation to reporting entities referred to in Article 4 paragraph 4 of this Law;

The supervisory authorities referred to in paragraph 1 of this Article shall be obliged to use an approach based on the risks of money laundering and terrorist financing when planning the supervision of reporting entities.

When planning the frequency and scope of the supervision, the supervisory authorities referred to in paragraph 1 of this Article shall be obliged to take into consideration in particular the following:

- Data related to risks of money laundering or terrorist financing determined in the National Risk Assessment;
- Data related to specific national or international risks of money laundering or terrorist financing related to customers, products, services or distribution channels;
- Data related to risk from a certain reporting entities and other available data;
- Significant events or changes related to authority management of the reporting entity, as well as any change of operations.

The supervisory authorities referred to in paragraph 1 of this Article shall be obliged to inform the financial intelligence unit about the activities they plan to undertake, no later than seven working days before the implementation of the supervision, as well as to submit data on the reporting entities for whom the supervision is planned (identification number, TIN and name), the date when the supervision is planned, information on whether it is indirect or direct supervision, and if necessary, coordinate and harmonize their activities in the supervision of the implementation of this Law with the financial intelligence unit.

If the supervisory authority referred to in paragraph 1 of this Article, in the procedure of the supervision over the implementation of this Law, established irregularities in the business of the reporting entity, it shall be authorised to:

- Point out the established irregularities and set a deadline for their removal;
- Issue a misdemeanour order or initiate misdemeanour proceedings against the reporting entity in accordance with the law that regulates misdemeanour proceedings;
- Suspend or revoke the work permit, i.e. take other measures to limit or prohibit the work of the reporting entity, in accordance with the law;
- Order other measures to the reporting entity in accordance with the law.

The supervisory authorities referred to in paragraph 1 of this Article may issue an order to the reporting entity to terminate the performance of business in its branches in another country, i.e. reject the request to open a branch in another country if the reporting entity in that country is unable to implement measures to prevent and detect money laundering and terrorist financing determined by this Law.

The supervisory authority referred to in paragraph 1 of this Article shall be obliged to exchange information with another supervisory authority and, at the request of another supervisory authority, submit the required data and documentation, which such authorities need for supervision in accordance with this Law.

The financial-intelligence unit may submit a request to the supervisory authorities referred to in paragraph 1 of this Article to carry out supervision over a certain reporting entity or type of the reporting entity, based on information and data available to the financial intelligence unit and on the basis of strategic and operational analyses carried out.

The supervisory authorities referred to in paragraph 1 of this Article shall be obliged to act according to the request referred to in paragraph 8 of this Article.

If it is necessary due to the complexity of the control or the importance of eliminating irregularities, the supervisory authorities referred to in paragraph 1 of this article may, together with the financial intelligence unit, conduct a joint inspection of a certain reporting entity or type of reporting entity.

Direct and indirect supervision

Article 132

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall perform direct and indirect supervision over the application of this Law.

When performing the supervision, the supervision officer shall be legitimized with the official identification and a badge, i.e. authorization.

Direct supervision shall be carried out on the basis of the supervisory authority's supervision plan referred to in Article 131 paragraph 1 of this Law which is drawn up on an annual basis and constitutes a business secret.

Direct supervision shall be initiated and conducted in the official premises of the reporting entity, and shall be carried out by the inspection of the business books, other documentation and information system of the reporting entity.

The provisions of the law regulating inspection supervision, i.e. the law regulating the competences of supervisory authorities referred to in Article 131 paragraph 1 of this Law, shall be applied accordingly to the direct supervision procedure.

Indirect supervision shall be carried out by controlling the documentation of the reporting entity submitted to the competent authorities referred to in Article 131 paragraph 1 at their request or made available electronically, that is, by analysing the reports and data submitted by the reporting entity in accordance with the Law.

Upon request referred to in paragraph 6 of this Article, the reporting entity shall be obliged to submit to the supervisory authority referred to in Article 131 paragraph 1 accurate and complete data, information and documentation that are necessary for immediate supervision, and no later than within eight days from the date of submission of the request.

The supervisory authority shall draw up a record i.e. a report on the supervision referred to in paragraph 1 of this Article.

Special powers of supervisory authorities

Article 133

When the supervisory authority referred to in Article 131 paragraph 1 of this Law issues work permits to the reporting entity, or approval for the acquisition of participation in the reporting entity, or for the appointment of members of the managing body of the reporting entity, on the basis of the law, it may at any time obtain information on the conviction of persons subject to the verification of fulfilment of conditions for granting the permit, or the approval and their associates, or related persons, in accordance with the Law.

An associate, or a related person referred to in paragraph 1 of this Article is considered an associate, or a related person, in accordance with the regulation governing the business of the reporting entity.

Data referred to in paragraph 1 of this Article may be used by the competent authority exclusively for the purposes they were obtained for, and shall not be communicated or made available to third parties.

International cooperation of supervisory authorities

Article 134

The supervisory authority referred to in Article 131 paragraph 1 of this Law may, on its own initiative or on the basis of a written and reasoned request of the authority of another state competent for supervision, exchange data, information and documentation in connection with:

1) Regulations governing the business of the reporting entity subject to the supervision, as well as other relevant regulations regarding supervision;

2) Sector in which the reporting entity operates, subject to the supervision by the authority;

3) Supervision of the reporting entity;

4) Transactions or persons for whom there are reasons to suspect, or grounds for suspicion that money laundering or terrorist financing or other predicate criminal offenses are involved in.

The supervisory authorities referred to in paragraph 1 of this Article, in accordance with the principles of reciprocity and keeping confidential information, may request mutual assistance in carrying out supervision over the reporting authority that is part of the group and that operates in the country from which assistance is requested.

The manner of delivering data, information and documentation, as well as performing joint supervision referred to in paragraph 2 of this Article, shall be regulated by the authorities referred to in paragraph 1 of this Article by a special agreement in accordance with the Law.

The authorities referred to in paragraph 1 of this Article may use the data, information and documentation referred to in paragraph 1 of this Article solely:

1) For performing their duties in accordance with this Law;

2) When filing an appeal or other legal remedies against the decision of the authority responsible for supervision, including court proceedings.

The supervisory authority referred to in paragraph 1 of this Article that has established irregularities referred to in Article 137 of this Law, shall also inform other competent supervisory authorities referred to in Article 131 paragraph 1 of this Law, if these irregularities are of importance for their work.

The supervisory authority referred to in paragraph 1 of this Article shall not disclose and exchange data, information and documentation collected in accordance with paragraphs 1 to 4 of this Article with third parties, without the express consent of the supervisory authority that has submitted the data, information and documentation.

The supervisory authority referred to in paragraph 1 of this Article shall not use collected data, information and documentation in accordance with paragraphs 1 to 4 of this Article for a purpose other than the one for which the supervisory authority that provided the data, information and documentation gave its consent, except in justified circumstances in accordance with the Law, in which case it shall be obliged to immediately notify that authority.

Submission of data on actions undertaken in the supervision procedure

Article 135

The supervisory authorities referred to in Article 131 paragraph 1 of this Law shall be obliged to submit to the financial intelligence unit, in accordance with this Law:

- Information about the reporting entity: identification number, TIN, name and the registered office (address, city, or municipality for the reporting entity with headquarters in Montenegro, or country for reporting entity with headquarters in another country), first and last name, unique identification number of the responsible person in the legal entity i.e. name and surname, date of birth and number, date of expiry and country of issuance of the travel document if the responsible person in the legal entity is a foreigner;

- Data on the date of control and a description of the established condition;
- Names and surnames of persons who are engaged in the work of preventing money laundering and terrorist financing in the competent supervisory authority referred to in Article 131 paragraph 1 of this Law;
- Report or records on the control in electronic form.

When irregularities in the operations of the reporting entity are determined the supervisory authorities referred to in Article 131 paragraph 1 of this Law shall be obliged to submit the following data to the financial intelligence unit:

- Date of submission of the misdemeanour order, i.e. the request for initiation of misdemeanour proceedings or other imposed measures;
- Misdemeanour order number;
- Description of the offense referred to in Article 137 of this Law;
- Data on the imposed measures;
- Amount of the imposed penalty.

The supervisory authorities referred to in Article 131 paragraphs 1 and 2 of this Law shall be obliged to submit the data referred to paragraphs 1 and 2 of this Article to the financial intelligence unit within eight days from the day of the performed supervision, i.e. the imposition of the measure.

If the supervisory authority referred to in Article 131 paragraph 1 of this Law suspends or revokes the work permit, i.e. takes other measures to limit or prohibit the work of the reporting entity, in accordance with the law, it shall be obliged to notify the financial intelligence unit within eight days.

If the supervisory authorities referred to in Article 131 paragraph 1 of this Law assess during the supervision that in relation to a transaction or a person there are reasons for suspicion or grounds for suspicion that the property originates from criminal activity or that it is money laundering, related predicate crimes or financing of terrorist they shall be obliged to inform the financial intelligence unit about it without delay.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall deliver data referred to in paragraphs 1 and 2 and notifications referred to in paragraph 4 and 5 of this Article to the financial intelligence unit in the manner prescribed by the act referred to in Article 66, paragraph 15 of this Law.

Access to data

Article 136

The supervisory authorities referred to in Article 131 paragraph 1 of this Law may have immediate access to the data submitted by the reporting entity to the financial intelligence unit in accordance with Article 66 of this Law in the content submitted to them by the reporting entity.

The supervisory authorities referred to in Article 131 paragraph 1 of this Law shall not have direct access to the data referred to in paragraph 1 of this Article in the content in which they were processed by the financial intelligence unit, however, such data may be delivered to them upon request and if the financial-intelligence unit assesses that the request is justified.

The supervisory authorities referred to in Article 131 paragraph 1 of this Law shall have immediate access to the CPR and criminal records.

The financial intelligence unit may, at the reasoned request of the supervisory authorities referred to in Article 131 paragraph 1 of this Law, for the purposes of carrying out checks for the purpose of issuing licenses or approvals issued by that authority in accordance with the law, submit all relevant data that it can obtain by applying its powers.

X. PENAL PROVISIONS

Article 137

A fine in the amount of EUR 3,000 to EUR 20,000 shall be imposed on a legal person for a misdemeanour, if:

1) It fails to establish an appropriate information system, if the reporting entity is a credit institution or financial institution (Article 11 paragraph 1 item 3);

- within the period of 60 days since the day of its establishment, i.e. the beginning of the performance of activities, it does not draft internal act on risk analysis in which it determines and assesses risks, taking into account risk factors of an individual customer, a group of customers, a country or geographic area, business relationship, transaction or product, services and distribution channels related to the possibility of misuse for the purpose of money laundering or terrorist financing and does not update it regularly and keep it in accordance with this Law (Article 12 paragraph 1 indent 1);

3) It fails to establish a risk management system and for money laundering and terrorist financing risk management in accordance with Article 14 paragraph 1;

4) Policies, controls, and procedures referred to in paragraph 14, paragraph 1 item 2 of this Article law are no longer proportional to the scope and nature of activities of a reporting entity, size, and type of customers, as well as to types of products, i.e. services which the reporting entity provides (Article 14 paragraph 2);

5) It fails to establish internal policies, controls and procedures in accordance with Article 14 paragraph 4 and 5 of this Law;

6) It fails to assess the risk of money laundering and terrorist financing in relation to a new service, product or distribution channel that it provides within its activity, new business practice, as well as ways of providing a new service, product or distribution channel, before their introduction (Article 16 paragraph 1);

7) It fails to undertake additional measures to mitigate risks and manage risks from money laundering and terrorist financing referred to in Article 16 paragraphs 1 and 2 of this Law, based on an updated risk analysis (Article 16 paragraph 3);

8) It fails to check whether the person acting on behalf of the customer has the right to representation or is authorized by the customer and does not identify the person acting on behalf of the customer in accordance with this Law (Article 17 paragraph 2);

9) It fails to regulate in its internal acts the procedures for the application of measures referred to in Article 17 paragraphs 1 and 2 of this Law (Article 17 paragraph 5);

10) At the request of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, it fails to submit or submits inaccurate appropriate analyses, documents and other information proving that measures have been applied in accordance with the established risk of money laundering and terrorist financing (Article 17 paragraph 6);

11) It fails to inform the financial intelligence unit that it cannot implement one or more measures referred to in Article 17 paragraph 1 of this Law (Article 17 paragraph 7);

12) It fails to implement CDD measures when there is doubt about the accuracy or credibility of the obtained data about the identity of the client or the beneficial owner of the client (Article 18 paragraph 1 item 4);

13) It fails to implement CDD measures when, in connection with the transaction, client, funds or property, there are reasons for suspicion or grounds for suspicion that the property originates from criminal activity or is a matter of money laundering or terrorist financing, regardless of the amount of the transaction (Article 18 paragraph 1 item 5);

14) For natural or legal persons trading in goods, when executing occasional cash transactions in the amount of EUR 10,000.00 or more, regardless of whether the transaction is executed as a single transaction or a number of mutually linked transactions (Article 18, paragraph 1 item 6).

15) It fails to implement CDD measures during the payment of winnings, or payment of stake, while executing one or several linked transactions in the amount of at least EUR 2,000 when the reporting entity is organizer of games of chance (Article 18 paragraph 1 item 7);

16) It acts contrary to the provisions referred to in Article 19 of this Law;

17) It performs the transaction referred to in Article 18, paragraph 1, item 2, 3, 6 and 7 of this Law, without having previously implemented the prescribed measures referred to in article 17, paragraph 1, point. 1, 2 and 3 of this Law (Article 20);

18) It fails to preform identify check of the user of the beneficial owner of life insurance policy (Article 21 paragraph 2);

19) When transferring rights from a life insurance policy to a third party, partially or in full, it fails to identify the new beneficiary, i.e. the beneficial owner at the time of the transfer of rights (Article 21 paragraph 4);

20) When establishing the customer's identity referred to in Article 22 paragraph 1 of this Law, it fails to obtain a photocopy of identity document on which they enters the date, time and personal name of the person who performed the check of a photocopy of a identity document, and which it keeps in accordance with this Law (Article 22 paragraph 3);

21) It fails to identify the legal representative or authorized person in accordance with Article 22 paragraphs 1 to 5 or fails to obtain data on that person referred to in Article 117 paragraph 1 Items 3 and 4 of this Law (Article 22 paragraph 6 indent 1);

22) It fails to obtain and verify from the written authorization in the original or a certified photocopy of that authorization the data on the client referred to in Article 117 paragraph 1 point 3 of this Law (Article 22 paragraph 6 paragraphs 2 and 3);

23) It fails to obtain written statement on the veracity of data when identifying the customer, representative or an authorized person if it doubts the veracity of the data obtained (Article 22 paragraph 7);

24) It established a business relationship, i.e. carried out a transaction, but it determined that the data from the identity document differed from the data in Central Population Register (Article 22 paragraph 9);

25) After preformed identification in records referred to in Article 117 paragraph 1 of this Law does not enter the data on manner of identification of the client (Article 22 paragraph 10, Article 23 paragraph 9 and Article 24 paragraph 17);

26) It identified the customer based on the certificate contrary to the provisions of Article 23 of this Law;

27) It performs video-electronic identification contrary to the provisions of Article 24 of this Law;
28) If within eight days from the date of submission of the decision referred to in Article 25, paragraph 6 of this Law fails to regulate with internal acts a closer manner of implementing video-electronic identification (Article 24, paragraph 18);
29) It carries out electronic identification, i.e. video-electronic identification of a client who is a natural person, an entrepreneur or a natural person performing an activity, their legal representative and an authorized person, and fails to have a permit for conducting electronic identification, i.e. video-electronic identification (Article 25 paragraph 1);
30) It fails to identify the customer that is a legal person or business organization in accordance with Articles 19 and 20 of this Law (Article 26 paragraph 1);
31) It obtains identity documents referred to in Article 26 paragraph 1 of this Law that are older than three months from the issuance date (Article 26 paragraph 3);
32) It acts contrary to Article 26 paragraph 7 of this Law;
33) It fails to obtain data on all directors of legal person or business organization referred to in Article 117 paragraph 1 item 3 of this Law (Article 27 paragraph 2);
34) In the process of establishing and verifying the authorization for representation of representatives and all directors referred to in Article 27, paragraph 2, it fails to obtain authorization for representation and does not keep it in its documentation (Article 27 paragraph 3);
35) In the process of identification of authorized person of legal person and business organization, it fails to obtain data on representative and all directors on whose behalf the authorized person acts in accordance with Article 28 paragraph 2 of this Law;
36) It fails to identify representative or authorized person of a customer in accordance with the Articles 27 and 28 of this Law where the customer is a trust, other person i.e. foreign entity equal to it (Article 29 paragraph 1 item 1);
37) It fails to identify a trust, another person, or a subject of foreign law equated with it in accordance with Article 29 of this Law;
38) It fails to identify the customer in accordance with this Law when the customer enters the premises where special games of chance are organized in a casino (Article 30 paragraph 1 item 1);
39) It fails to identify the customer in accordance with this Law on any approach of a lessee or their representative, or a person they has authorized, to the safe deposit box (Article 30 paragraph 1 item 2);
40) In the process of identifying the client referred to in Article 30 paragraph 1 point 1 of this Law, fails to obtain a photocopy of that person's identity document in accordance with Article 22 paragraph 3 of this Law, as well as a written statement by which the client declares under material and criminal liability that in games of chance in he participates in the casino for their own account and in their own name (Article 30 paragraph 2);
41) It entrusts the execution of customer due diligence to a third party, if the third party is a shell bank or anonymous company or it’s from a high-risk third country (Article 32);
42) It fails to keep obtained copies of identity documents and documentation in accordance with this Law (Article 33 paragraph 3);

43) It assesses that there is doubt about the validity of the implemented CDD measures by a third party, or the veracity of obtained data on the customer, and does not immediately implement those measures (Article 31 paragraph 1);

44) It fails to regulate in an internal act the procedures on acceptance of the identification of the customer and the beneficial owner of the customer through a third person (Article 34 paragraph 2);

45) It fails to collect data on the payer and the payee prescribed by Article 35 of this Law and does not enter them into the payment order form or the electronic message that follows the transfer of funds from the payer to the payee (Article 35 paragraph 1);

46) It fails to check the accuracy of the collected data about the payer in accordance with Articles 22, 23, 24, 26, 27 and 28 of this Law, before the transfer of funds (Article 35 paragraph 8);

47) It fails to regulate in the internal act the procedures for verifying the completeness of data in accordance with Article 35 paragraphs 2 to 9 of this Law (Article 35 paragraph 12);

48) It fails to not check whether the data on the payer and payee have been entered in the payment order form or the electronic message accompanying the transfer of funds in accordance with Article 35 of this Law (Article 36 paragraph 1);

49) It fails to not check the accuracy of the collected data referred to in Article 36 paragraphs 2 and 3 of this Law in accordance with Articles 22, 23, 24, 26, 27 and 28 of this Law (Article 36);

50) It fails to draw up an internal act of handling, including, as necessary, ex-post monitoring or real-time monitoring, in the event that the payment order form or electronic message that transfer funds does not contain accurate and complete data referred to in Article 35 of this Law (Article 37 paragraph 1);

51) It fails to warn or inform about the period within which it is necessary the payer's payment service provider to submit accurate and complete data in accordance with Article 35 of this Law, if the latter does so frequently (Article 37 paragraph 3);

52) It fails to refuse future transfers of funds or does not limit or terminate business cooperation with the payer's payment service provider, if the latter often does not submit accurate and complete data in accordance with Article 35 of this Law (Article 37 paragraph 4);

53) It fails to notify the Central Bank of Montenegro about the payment service provider of the payer who often fails to submit accurate and complete data in accordance with Article 35 of this Law and about the measures taken against that person in accordance with Article 37 paragraph 3 and 4 of this Law (Article 37 paragraph 5);

54) It fails to determine whether the lack of accurate and complete data referred to in Article 35 of this Law constitutes grounds for suspicion of money laundering or terrorist financing, and if it establishes that this deficiency constitutes grounds for suspicion, fails to notify the financial intelligence unit in accordance with Article 66 paragraphs 6, 8 and 10 of this Law (Article 37 paragraph 6);

55) It fails to ensure that all information about the payer and payee are saved in the payment order form or the electronic message accompanying the transfer of funds (Article 38 paragraph 1);

56) It fails to draw up an internal act of handling, including, as necessary, ex-post monitoring or real-time monitoring, in the event that electronic message that transfer

funds fails to contain accurate and complete data referred to in Article 35 of this Law (Article 38 paragraph 2);

57) It fails to act in accordance with Article 37 paragraphs 2 to 7 of this Law, when the payment order form or electronic message accompanying the transfer of funds fails to contain accurate and complete data referred to in Article 35 of this Law (Article 38 paragraph 3);

58) It fails to establish the beneficial owner of the legal person, business organization or foreign legal person, trust, other person i.e. foreign entity equal to it by gathering data referred to in Article 44 of this Law (Article 42 paragraph 1);

59) It fails to print the extract from the Register referred to in Article 42 paragraph 2 of this Law and fails to mark the date and time and the name and surname of the person who performed the checks;

60) If during data verification of beneficial owner in accordance with Article 42 paragraphs 2 and 3 of this Law determines that there is a difference in the data, and fails to submit such data that differs to the financial intelligence unit or the administrative body responsible for tax collection (Article 42 paragraph 4);

61) If, in the process of determining the beneficial owner, it fails to obtain documentation on the basis of which it is possible to determine the ownership structure and controlling member of the customer and information about the beneficial owner (Article 42 paragraph 6);

62) If verification of data on the beneficial owner is not carried out in accordance with Article 42 paragraph 7 of this Law;

63) It fails to obtain a photocopy of the identity document of the beneficial owner in accordance with Article 22 paragraph 3 of this Law (Article 42 paragraph 8);

64) If when collecting data referred to in Article 42 paragraphs 2, 3, 5, 6 and 7 of this Law, it doubts the veracity of the obtained data or the authenticity of the identity documents and other documentation from which the data were obtained and fails to obtain a written statement from the customer’s representative or authorized person (Article 42 paragraph 9);

65) It fails to keep records of the measures taken to determine the beneficial owner referred to in Article 42, paragraph 1(Article 42 paragraph 11);

66) It fails to enter the prescribed data on beneficial owners and changes in beneficial owners into the Register of Beneficial Owners within eight days from the date of registration in the CBR or the Tax Register, i.e. within eight days from the change of data on the beneficial owner (Article 43 paragraph 3);

67) It fails to verify and confirm the accuracy of its data in the Register of Beneficial Owners once a year, no later than March 31 of the current year (Article 43 paragraph 5);

68) It fails to submit the data referred to in Article 44, paragraph 1, point 2, paragraphs 1, 2 and 4 of this Law to the subject of which it is the beneficial owner, in order to enter such data in the Register of Beneficial Owners (Article 43, paragraph 6);

69) If at the request of the administrative body responsible for tax collection, fails to submit documentation on the basis of which it is possible to determine the ownership structure and controlling member of the client and fails to collect information about the beneficial owner (Article 48 paragraph 3);

70) It fails to implement measures to monitor the client's business relationship, including control of transactions and monitoring of sources of funds with which the client operates (Article 49 paragraph 1);

71) If it fails to implement measures referred to in Article 49 paragraph 2 of this Law;
72) If it fails to provide and adjust the scope and dynamics of the implementation of the measures referred to in Article 49 paragraph 1 of this Law to the risk of money laundering and terrorist financing to which the reporting entity is exposed when performing a particular job, i.e. in dealing with a customer (Article 49 paragraph 3);
73) If it fails to perform control of a customer at least once a year who is a foreign legal person or a legal person based in Montenegro in which the participation of foreign capital is at least 25%, and which carries out transactions with the reporting entity referred to in Article 18 paragraph 1 Items 2, 3, 5 and/or 6 of this Law (Article 50 paragraph 1);
74) During the control of a foreign legal person, it fails to obtain additional data referred to in Article 50 paragraph 3 items 1 and 2 of this Law;
75) It determines the difference in the data and fails to call the customer to verify all relevant information (Article 50 paragraph 6);
76) It fails to undertake enhanced customer due diligence when a higher risk of money laundering and terrorist financing is determined in the guidelines on risk analysis referred to in Article 12 paragraph 5 of this Law (Article 52 paragraph 1 item 7);
77) It fails to implement enhanced customer due diligence in cases where, in accordance with the National Risk Assessment, a higher degree of risk of money laundering and terrorist financing has been determined (Article 52 paragraph 1 item 8);
78) It fails to implement enhanced customer due diligence and in all other cases when it estimates that in relation to the customer, group of customers, country or geographical area, business relationship, transaction, product, service and distribution channel, there is or could be a higher risk of money laundering and terrorist financing (Article 52 paragraph 2);
79) When establishing a correspondent relationship that includes making payments with a credit institution or other financial institution that is based outside the European Union or in a high-risk third country, and which is a respondent, in addition to the measures referred to in Article 17 of this Law, fails to undertake additional measures referred to in Article 53 paragraph 1 points 1 to 8 of this Law;
80) Before establishing a correspondence relationship with the respondent fails to obtain the written consent of the senior manager for the establishment of that business relationship (Article 53 paragraph 2);
81) It fails to regulate its responsibility and the responsibility of the respondent in the contract when concluding a correspondence relationship (Article 53 paragraph 3);
82) It fails to review and amend and, if necessary, terminate the correspondent relationship with a credit or other financial institution that is a respondent in a high-risk third country (Article 53 paragraph 6);
83) It establishes or continues a correspondent relationship with a credit or other similar institution that has its registered office outside the European Union or in a high-risk third country, without having previously taken any of the measures referred to in Article 53 paragraphs 1, 2, 3 and 4 of this Law (Article 53 paragraph 7 item 1);
84) It establishes or continues a correspondent relationship with a credit or other similar institution that is based outside the European Union or in a high-risk third country, if the credit or other similar institution does not have an established control system for the prevention of money laundering and terrorist financing or is not

obliged to apply laws and other regulations in the field of prevention and detection of money laundering and terrorist financing (Article 53 paragraph 7 item 2);

85) It establishes or continues a correspondent relationship with a credit or other similar institution that is based outside the European Union or in a high-risk third country, if a credit or other similar institution operates as a shell bank, i.e. if it establishes correspondent or other business relationships and carries out transactions with shell banks (Article 53 paragraph 7 item 3);

86) Before establishing a business relationship with the customer, fails to check in the Register referred to in Article 55 of this Law whether the customer, their legal representative, an authorized person, or the beneficial owner of the customer is a politically exposed person (Article 54 paragraph 1);

87) During the implementation of enhanced customer due diligence who is a politically exposed person, in addition to the measures referred to in Article 17 of this Law, fails to take adequate measures and determine the origin of property and funds that are included in a business relationship or transaction with that customer (Article 56 paragraph 1 item 1);

88) When conducting enhanced customer due diligence who is a politically exposed person, in addition to the measures referred to in Article 17 of this Law, fails to obtain a written consent of the senior management before establishing a business relationship with a customer, or a written consent of the senior management for the continuation of the business relationship if the business relationship with the customer is already established (Article 56 paragraph 1 item 2);

89) When conducting enhanced customer due diligence, i.e. its beneficial owner who is a politically exposed person, in addition to the measures referred to in Article 17 of this Law, does not determine whether the client who is a politically exposed person is the beneficial owner of a legal entity, business company, trust , another person, i.e. a subject of foreign law equated with them, i.e. a natural person with headquarters in another country on whose behalf a business relationship is established, a transaction or other activity of the client is carried out (Article 56 paragraph 1 point 3);

90) When conducting enhanced customer due diligence who is a politically exposed person, in addition to the measures referred to in Article 17 of this Law, after establishing a business relationship, it fails to monitor with special attention the transactions and other business activities which a politically exposed person performs at the reporting entity, or the customer whose beneficial owner is a politically exposed person (Article 56 paragraph 1 item 4);

91) It fails to develop an internal act with procedures that are based on risk analysis, in accordance with the guidelines referred to in Article 12 paragraph 5 of this Law, which it applies when identifying the customer who is politically exposed person or establishing the beneficial owner of a customer who is politically exposed person (Article 56 paragraph 2);

92) When providing custody services to the customer, in addition to the measures referred to in Article 17 of this Law, fails to take adequate measures and fails to determine the origin of property and funds that are included in the business relationship or transaction with that customer (Article 57 paragraph 1 item 1);

93) When providing custody services to a client, in addition to the measures referred to in Article 17 of this Law, fails to obtain the written consent of a senior manager before establishing a business relationship with that client, and if the business relationship has already been established, fails tp obtain the written consent of a

senior manager to continue the business relationship (Article 57 paragraph 1 point 2);

94) When providing custody services to the customer, in addition to the measures referred to in Article 17 of this Law, it fails to determine whether a customer concludes a contract on the performance of custody services in their own name and on their own account or if it is a sub-custody (Article 57 paragraph 1 item 3);

95) When providing custody services to the customer, in addition to the measures referred to in Article 17 of this Law, during each transaction it fails to determine for whose account the sub-custody performed the transaction (Article 57 paragraph 1 item 4);

96) It fails to execute the measures referred to in Article 57 paragraph 1 of this Law, and establishes a business relationship, that is, fails to terminate an already established relationship (Article 57 paragraph 2);

97) In a case of complex and unusually large transactions, as well as transactions that are realized in an unusual manner or that have no obvious economic justification or legal purpose or deviate from the usual or expected business of the client, for which it was not possible to assess whether they are suspicious transactions, in addition to the measures referred to in Article 17 of this Law does not undertake measures referred to in Article 58 paragraph 1 of this Law;

98) It fails to make available the results of the analysis referred to in Article 58 paragraph 1 point 6 of this Law (Article 58 paragraph 2) at the request of the financial intelligence unit or the competent supervisory authority referred to in Article 131 paragraph 1 of this Law;

99) It fails to establish the criteria for recognition of transactions referred to in Article 58 paragraph 1 of this Law (Article 58 paragraph 3);

100) In case of establishing business relation or performing transactions with persons from high-risk third countries or when the high-risk third country is included in transaction, in addition to measures referred to in Article 17 of this Law, it fails to undertake additional measures referred to in Article 58 paragraph 1 of this Law (Article 59 paragraph 1 item 1);

101) In case of establishing business relation or performing transactions with persons from high-risk third countries or when the high-risk third country is included in transaction, in addition to measures referred to in Article 17 of this Law, fails to obtain written consent by a senior manager before establishing that relation (Article 59 paragraph 1 item 2);

102) After establishing business relation with customer from high-risk third country it fails to enhanced monitoring of business relation and transactions which that customer performs (Article 59 paragraph 2);

103) It fails to implement measures referred to in Article 59 paragraphs 1 and 2 of this Law in accordance with the assessment of the risk of money laundering and terrorist financing, which was determined in the risk analysis (Article 59 paragraph 3);

104) In relation to a customer where a lower risk of money laundering and terrorist financing is identified, it does not implement measures for monitoring of business relationships and the control of the transactions to the extent determined in accordance with Article 60 paragraph 1 item 3 of this Law (Article 61 paragraph 3);

105) It fails to provide that the measures of detection and prevention of money laundering and terrorist financing, as defined by this Law, are implemented, to the same extent, in business units or organizations majority-owned by reporting entities, which have registered office in another country that is a member state of the

European Union, i.e. a country that has the same standards for the implementation of measures of detection and prevention of money laundering and terrorist financing as the standards established by this Law, i.e. the Law of the European Union (Article 62 paragraph 1);

106) It opens or keeps anonymous accounts, anonymous safe deposit box, coded or bearer passbook for its customer, or provide other service or product that directly or indirectly enable concealment of a customer's identity (Article 63);

107) It operates as a shell (fictious) bank (Article 64 paragraph 1);

108) It establishes or continues correspondent relationships with a credit institution that carries out or could carry out business activities as a shell (fictious) bank or with other credit institution that is known for allowing shell (fictious) banks to use its accounts (Article 64 paragraph 2);

109) Legal persons, business organizations, entrepreneurs and natural persons that carrying out business activities receive or make a payment in cash in the amount of 20,000 EUR or more (Article 65 paragraphs 1 and 2);

110) It fails to submit to the financial intelligence unit, without delay, and at the latest within three days from the date of conclusion of executed transactions transaction, accurate and complete data on the measures of knowledge and monitoring of the client's business referred to in Article 117 paragraphs 1 to 6 of this Law for each transaction in cash in the amount of EUR 15,000 or more, or non-cash transaction in the amount of EUR 100,000 or more (Article 66 paragraph 1);

111) It fails to submit to the financial intelligence unit, without delay, and at the latest within three days from the date of conclusion of executed transactions transaction, accurate and complete data on the measures of knowledge and monitoring of the client's business referred to in Article 117 paragraphs 1 to 6 of this Law for each transaction in cash in the amount of EUR 10,000 or more (Article 66 paragraph 2);

112) It fails to submit to the financial intelligence unit, without delay, and at the latest within three days from the date of conclusion of executed transactions transaction, accurate and complete data on the measures of knowledge and monitoring of the client's business referred to in Article 117 paragraphs 1 to 6 of this Law for each transaction in cash in the amount of EUR 10,000 or more, which is carried out to the accounts of legal and natural persons in high-risk third countries and if such transaction includes high-risk third country (Article 66 paragraph 3);

113) It fails to refrain from execution of suspicious transaction, regardless of the amount, until passing the order referring to in Article 93 of this Law and to inform, without delay the financial intelligence unit and fails to provide it with data on measures of monitoring customer's business operations referred to in Article 117, paragraphs 1 to 6 and paragraph 8 of this Law (Article 66 paragraph 6).

114) It fails to provide the financial intelligence unit with the data referred to in Article 66 paragraph 6 before the execution of transactions and fails to specify the deadline by which the transactions should be executed (Article 66 paragraph 7);

115) It fails to submit to the financial intelligence unit, without delay, and at the latest within following of conclusion of executed transactions transaction, data on the measures of knowledge and monitoring of the client's business referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law when, due to the nature of the transactions or other justified reasons, it cannot act in accordance with Article 66 paragraph 6 of this Law (Article 66 paragraph 8);

116) When submitting data in the manner referred to in Article 66 paragraph 8, it fails to explain in detail the reasons why it did not act in accordance with Article 66 paragraph 6 of this Law (Article 66 paragraph 9);

117) It fails to provide to the financial intelligence unit, without delay, with accurate and complete data on the customer due diligence referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law in relation to money or other assets that they know or have reason to suspect it represent proceeds gained through criminal activity or are related to money laundering or terrorist financing (Article 66 paragraph 10);

118) It fails to notify the financial intelligence unit, without delay, that the customer has sought advice on money laundering or terrorist financing (Article 66 paragraph 11);

119) It fails to notify the financial intelligence unit, within the three days of the preformed review of data, on any review of data, information and documentation preformed by the supervisory authority referred to in Article 131 paragraph 1 of this Law (Article 66 paragraph 12);

120) It fails to submit data, explanations and notifications to the financial intelligence unit in the manner prescribed by Article 66 paragraph 13 of this Law;

121) If within 60 days from the day of establishment, i.e. the start of activities, it fails to appoint an authorized person for the prevention of money laundering and terrorist financing and at least one deputy of that person (Article 69 paragraph 1);

122) It fails to submit the notification referred to in Article 69 paragraphs 1, 2 and 6 to the financial intelligence unit (Article 69 paragraph 7);

123) It fails to submit the report referred to in Article 76 paragraph 1 item 12 of this Law to the competent supervisory authority referred to in Article 131 paragraph 1 of this Law at the request of that supervisory authority within three days upon receipt of that request (Article 76 paragraph 2);

124) It fails to provide the prescribed conditions to the compliance officer for the prevention of money laundering and terrorist financing (Article 77 paragraph 1);

125) It fails to provide regular professional training and development of all employees who participate in area of prevention and detection of money laundering and terrorist financing at reporting entity (Article 78 paragraph 1);

126) It fails to prepare program for professional training and development referred to in Article 78 paragraph 1 of this Law, within the prescribed deadline (Article 78 paragraph 3);

127) It fails to order and control the application of the rules referred to in Article 79 paragraphs 1 and 2 of this Law in business units and companies majority-owned by taxpayers with headquarters in other countries (Article 79 paragraph 3);

128) It fails to ensure regular internal control and revision of the implementation of the policies, controls and procedures for preventing money laundering and terrorist financing, or does not ensure performing the affairs of detection and prevention of money laundering and terrorist financing in accordance with the established risk of money laundering and terrorist financing in the risk analysis (Article 80 paragraph 1);

129) It fails to organize an independent internal audit, the scope of which is a regular assessment of the adequacy, reliability and efficiency of the money laundering and terrorist financing risk management system, when the law governing the activity of the reporting entity prescribes the obligation to have an independent internal audit (Article 80 paragraph 2);

130) It fails to use the list of indicators referred to in Articles 82 and 83 of this Law when establishing reasons for suspicion that the property originates from criminal activity or that money laundering or terrorist financing has been committed and other circumstances related to that suspicion (Article 81);

131) It fails to develop its own list of indicators for identifying suspicious customers and transactions (Article 83 paragraph 1);

132) It fails to provide to the financial intelligence unit, without delay, and at the latest within eight days upon receiving the request, accurate and complete data, information and documentation at its disposal (Article 90 paragraph 4);

133) It fails to provide to the financial intelligence unit, upon request marked with designation "URGENT", without delay, and no later than within 24 hours of receiving that request (Article 90 paragraph 5);

134) It fails to provide the requested data, information and documentation to the financial-intelligence unit, in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law (Article 91 paragraph 2);

135) It fails to undertake measures without delay in accordance with Article 93 paragraphs 1 and 4 of this Law (Article 93 paragraph 5);

136) It fails to comply with the request referred to in Article 95 paragraph 1 of this Law (Article 95 paragraph 2);

137) It fails to submit data to the financial-intelligence unit before the execution of the transaction or the conclusion of a business (Article 95 paragraph 3);

138) It fails to submit data to the financial intelligence unit without delay, and at the latest on the next working day from the date of execution of the transaction or conclusion of the deal, when due to the nature of the transaction, i.e. the deal or other justified reasons, it cannot act in accordance with Article 95 paragraph 3 of this Law and fails to explain in detail the reasons why he did not act in accordance with Article 95 paragraph 3 of this Law (Article 95 paragraphs 4 and 5);

139) It fails to notify the financial intelligence unit, without delay if, during the performance of its activities, it discovers facts that point to a possible connection with money laundering and related predicate offences or terrorist financing (Article 114 paragraph 1);

140) Upon request of the financial-intelligence unit, it fails to provide data, information or documentation that points to a possible connection with money laundering and related predicate offences or terrorist financing, in accordance with the Law (Article 114 paragraph 2);

141) It fails to submit quarterly, electronically, to the financial intelligence unit data on each collective custody account, credit institution or other institution with which that custody account was opened, as well as on the number of transactions and total turnover on that collective custody account (Article 114 paragraph 3);

142) It fails to keep records referred to in Article 116 paragraph 1 (Article 116 paragraph 1);

143) It fails to keep the records referred to in Article 116 paragraph 1 in a way that will ensure the reconstruction of individual transactions (including amounts and currency) that could be used as evidence in the process of detecting the criminal activities of customers (Article 116 paragraph 2);

144) Records it keeps in accordance with the Law fail to contain prescribed data (Article 117);

145) Discloses data referred to in Article 123 paragraph 1 points 1 to 4 of this Law to a client or a third party (Article 123 paragraph 1);

146) It fails to undertake the necessary measures to protect the compliance officer for the prevention of money laundering and terrorist financing and other employees who implement the provisions of this Law from threats and other unfavourable or discriminatory actions aimed at their physical or psychological integrity (Article 125);

147) Its employees use the personal data they receive in accordance with this Law for purposes for which they were not obtained (Article 126 paragraph 1);

148) It fails to keep data, information and documentation obtained in accordance with this Law, data on the identification number of each customer's account, data and documentation on electronic money transfer, documentation on business correspondence and reports for ten years after the termination of the customer's business relationship, performed occasional transactions, entry of the customer to the casino and premises where other games of chance are organized or access to the safe, unless a longer record period is prescribed by a special Law (Article 127 paragraphs 1 and 2);

149) It fails to keep data and accompanying documentation on the compliance officer for the prevention of money laundering and terrorist financing and their deputy, the professional training and development of employees in the field of preventing money laundering and terrorist financing and the implementation of internal control and audit measures, for four years from the expiry of the license of the compliance officer for the prevention of money laundering and terrorist financing and their deputy, i.e. completed professional training and development and completed internal control and audit (Article 127 paragraph 3);

150) It fails to submit, within the prescribed period, accurate and complete data, information and documentation that are necessary for carrying out supervision at the request of the competent authority referred to in Article 131 of this Law (Article 132 paragraph 7).

The responsible person in a legal person and the natural person shall be fined in the amount from EUR 500 to EUR 2,000 for misdemeanour referred to in paragraph 1 of this Article.

An entrepreneur shall be fined in an amount from EUR 500 to EUR 6,000 for the misdemeanour referred to in paragraph 1 of this Article.

For the misdemeanour referred to in paragraph 1 of this Article, a legal person, an entrepreneur, a responsible person in a legal person and a natural person may be prohibited from performing their calling, activity or duty for a period of up to six months.

For the misdemeanour referred to in paragraph 1, point 144 of this Article, the request for initiation of misdemeanour proceedings is also submitted by an authorized police officer of the financial intelligence unit.

For misdemeanours referred to in paragraph 1 of this Article committed by credit institutions and other financial institutions, misdemeanour proceedings may not be initiated if three years have passed since the offense was committed.

Article 138

A natural person performing an activity shall be fined for an offense in the amount of EUR 500 to EUR 2,000, if:

1) It fails to submit to the financial intelligence unit, without delay, and at the latest within three days from the date of conclusion of the legal transaction, accurate and complete data on the measures of knowledge and monitoring of the client's business

referred to in Article 117 paragraphs 1 to 6 of this Law for each transaction based on a pre-contract, a contract regarding real estate with a value of EUR 15,000 or more, as well as a loan contract with a value of EUR 10,000 or more (Article 66 paragraph 4);

2) it fails to submit a photocopy of the contract in electronic form, i.e. a photocopy of the statement of the natural person who is the buyer about the origin of the money for the contracts in which it is used for implementation, to the financial intelligence unit, without delay, and no later than within three days of the conclusion of the legal transaction cash (Article 66 paragraph 5).

For the offense referred to in paragraph 1 of this Article, a natural person who performs an activity may be banned from performing a calling, activity, or duty for a period of up to six months.

XI. TRANSITIONAL AND FINAL PROVISIONS

Deadline for Adoption of By-Laws

Article 139

Secondary legislation for implementation of this Law shall be adopted within three months from the date of entry into force of this Law.

Pending the date of entry into force of the bylaws referred to in paragraph 1 of this Article, the bylaws adopted based on the Law on Prevention of Money Laundering and Financing of Terrorist ("Official Gazette of Montenegro", no. 33/14, 44/18 and 73/19 and 70/21) shall be applied if they are not contrary to this Law.

Implementation of measures for already established business relationships

Article 140

Reporting entity shall be obliged to implement measures referred to in Article 17 of this Law in relation to the customers referred to in Article 18 paragraph 2 of this Law with whom it has already established business relationships when executing the first transaction after the entry into force of this Law.

Entering and updating data in the Register of beneficial owners

Article 141

Legal entity, business company, association, institution, political party, religious community, artistic organization, chamber, trade union, employers' association, foundation or other business entity, legal entity that receives, manages or distributes funds for specific purposes, trust, other person, that is, a subject of foreign law equated with it that receives, manages or distributes assets for certain purposes that were registered in the CRPS or the register of taxpayers before the entry into force of this Law, but did not enter or update the data in the Register of beneficial owners, shall be obliged to enter, that is, they update that data within 30 days from the date of entry into force of the act referred to in Article 45, paragraph 4 of this Law.

Establishing records

Article 142

Reporting entities, state and other authorities and institutions shall be obliged to establish records that they shall be obliged to keep in accordance with this Law within three months from the date of entry into force of this Law.

Harmonizing business activities

Article 143

Reporting entities shall be obliged to, in order to prevent money laundering and the terrorist financing, harmonize their operations with this Law within six months from the date of entry into force of the by-laws referred to in Article 139 paragraph 1 of this Law.

Obtaining licences

Article 144

Compliance officers for prevention of money laundering and terrorist financing and their deputies who were appointed before the entry into force of this Law shall be obliged to, within six months from the date of entry into force of the acts referred to in Articles 71 and 72 of this Law obtain a license in accordance with this Law.

Until obtaining a license in accordance with paragraph 1 of this Article, compliance officers for prevention of money laundering and terrorist financing and their deputies shall continue to work in accordance with this Law.

If, within the period referred to in paragraph 1 of this Article, compliance officers for prevention of money laundering and terrorist financing and their deputies do not obtain a license in accordance with this Law, their status as compliance officers for prevention of money laundering and terrorist financing, i.e., deputy authorized persons, shall cease.

The deadline for establishing a register of accounts and safe deposit boxes

Article 145

The Central Bank of Montenegro shall be obliged to establish the registers referred to in Article 112 of this Law within 12 months from the date of entry into force of this Law.

Establishing reporting entities' internal acts and organization

Article 146

Reporting entities shall harmonize internal acts and organization with this Law within six months since the day of entry into force of this Law.

Until the adoption of internal acts referred to in Article 77, 78 and 80 of this Law, the Rulebook on the manner of work of an authorized person, the manner of conducting internal control, the storage and protection of data, the manner of keeping records and the training of employees ("Official Gazette of Montenegro", no. 71/20) shall be applied.

Initiated Proceedings

Article 147

Initiated proceedings that have not been legally concluded by the date of entry into force of this Law shall be concluded under the Law on Prevention of Money Laundering and Terrorist Financing ("Official Gazette of Montenegro", no. 33/14, 44/18, 73/19 and 70/21).

Repealing

Article 148

On the date of entry into force of this Law, the Law on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of the Republic of Montenegro", No. 33/14, 44/18 and 73/19 and 70/21) is hereby repealed.

Entry into Force

Article 149

The present Law shall enter into force on the eighth day of its publication in the Official Gazette of Montenegro.

∗ The provisions of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU and Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 have been transferred into this Law. 1781/2006.

Number: 04-3/23-1/4

EPA 100 XXVIII

Podgorica, December 11, 2023

The Parliament of Montenegro of 28th Convocation

The President

Andrija Mandić