Law on the Prevention of Money Laundering and Terrorist Financing
(Official Gazette of Montenegro, No. 110/23 dd 12th December 2023)

I. GENERAL PROVISIONS

Subject Matter of the Law
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 that performs police affairs (hereinafter: the Police) which performs the activities related to the prevention of money laundering and terrorist financing (hereinafter: financial intelligence unit) and other issues significant for the prevention and detection of money laundering and terrorist financing.

Money Laundering
Article 2

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

1) 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;
2) 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 that activity;
3) the 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 that activity;
4) participation in, association to commit, attempt to commit and aiding, abetting, facilitating and counselling the commission of any of the actions from Items 1, 2 and 3 of this paragraph.

Activities from 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 from paragraph 1 of this Article shall also be considered as money laundering in case 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

In the context of this Law, the following shall, in particular, be considered as terrorist financing:

1) providing, making available or collecting funds or property, in any way, directly or indirectly, with the intention of using them or if it is known that they will be used in full or in part for the execution of a terrorist act, or an attempt of providing, making available or collecting funds or property, in any way, directly or indirectly, with the intention or with the knowledge that they may be used, in full or in part:

- for preparing or committing terrorist act in the context of this Law,
- for financing organizations whose aim is to commit the acts from 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 from 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 from 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 in accordance with the law regulating provision of payment services and electronic money issuance;
4) 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: MTF); operation of organized trading facility (hereinafter referred to as: OTF);
   - ancillary services on the capital market in Montenegro which 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) organizers of games of chance;
11) pawnshops;
12) legal persons, business organizations, entrepreneurs and natural persons that perform business activity or affairs of virtual assets and fiduciary assets exchange as well as custodian wallet 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 persons;
    - mediation in renting real estate in transactions where the monthly rent is 10,000 euros or more;
    - construction of residential and business facilities;
    - issuance and management of payment instruments (e.g. checks, traveler's checks, credit cards, bank promissory notes, payment orders, debit cards), which are not considered payment services in accordance with the law regulating 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 EUR10,000 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 EUR10,000 or more regardless of whether it is single or several linked transactions;
    - trade or mediating in trade, including organizing and conducting auctions 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 EUR10,000 or more, regardless whether it is performed in a single or more linked transactions;
    - storing and keeping works of art or trading or acting as intermediaries in the trade of works of art when this is carried out in by ports, free zone or warehouse, if payments are made or received in the amount of where the value of EUR10,000 or more, regardless whether it is performed in a single or more of linked transactions.

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

1) provides legal assistance in planning and executing transactions for a customer related to:
    - purchase or sale of real estate or a business organization,

- management of 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) executes a financial transaction or transaction concerning real estate on behalf and for a benefit of a customer.

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

The Government of Montenegro (hereinafter: Government) may define other reporting entities that shall undertake the measures from 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 determined.

The risk assessment from paragraph 6 of this Article is based on the nature, method of carrying out, payment methods and volume of business of the subjects from paragraph 6 of this Article.

Use of gender-sensitive language
Article 5

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

Definition of Terms
Article 6

The certain terms used in this Law have the following meaning:

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 terrorism, 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 from Article 4, paragraph 2, items 1 - 9 of this Law;
11) **Financial group** means a group comprised of:

- a parent company whose head office is situated in Montenegro, dependent companies and companies where these companies have direct or indirect participation in capital or voting rights of at least 20% and are involved in the annual consolidated financial statement in accordance with the law;
- companies that are mutually linked by joint management;
- legal or natural persons that have direct or indirect share in capital or voting right of at least 20% in legal persons from financial sector;

12) **reasons for suspicion** mean a set of facts and circumstances based on the list of indicators from Art. 82 and 83 of this Law or on information from publicly available sources or observations, on the basis of which a natural person can suspect, assume or reasonably conclude that a certain transaction, funds or other 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 analysis 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, kept, processed and assessed, 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, kept, processed and assessed, 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 regulating 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 property;
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 recognizing 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 directly or indirectly 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 (fictious) 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 that governs 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 onto 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) **payment service provider** means a credit institution, electronic money institution and payment institution;
31) **money transfer** means any transaction executed at least partially electronically by a payment service provider on behalf of the payer, with the aim to make the funds available to the payee at a payment service provider, regardless of whether or not the payer and the payee are one and the same person, or whether the payer's payment service provider and the payee's payment service provider are one and the same person or not, including the payment transaction which is being carried out:
    - by a credit transfer, direct debit or money remittance within the meaning of the law regulating payment system,
    - by using a payment card, payment instrument that serves for disposing with electronic money, 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 regulating the operation of investment funds,
    – conclusion of contracts on the provision of investment and/or auxiliary services, in accordance with the law regulating the capital market;
34) **anonymous legal person** means a foreign legal person with unknown owners and/or managers;
35) **senior manager** is an employee of a reporting entity that 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 law** means an organized group of individuals who pool or have committed to pool funds or other property for specific purposes;

39) **organizer of games of chance** means the organizer 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 person equal to it,
- 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** is 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 which has not been issued and is not guaranteed by the Central Bank of Montenegro, nor by a state authority, and that is not necessarily attached to legally established currency and does have 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** is a legal mean of payment issued by 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** is 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** is 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 for keeping a private cryptographic key and allows users to securely keep, 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** includes the record 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 head office, 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 regulating 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: National Risk Assessment) includes:

- 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 relation to which the reporting entities shall apply measures of enhanced verification of the customer and monitoring of its business activities and, if necessary, establishing measures that shall be taken for the purpose of prevention of money laundering and terrorist financing has been determined;
-
- 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 for the fight against money laundering and terrorist financing to the financial-intelligence unit, competent authorities from Article 96 paragraph 1 of this Law and competent supervisory authorities from Article 131 paragraph 1 of this Law.

The National risk assessment shall be determined by the Government, at least once every three 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 proposal of the measures and action plan for mitigating and managing identified risks of money laundering and terrorist financing;
4) conduct 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 from 1 of this Article has a president, members and a secretary.

The coordination body from 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 from paragraph 1 of this Article shall be carried out by the financial intelligence unit.

The specific composition of the coordinating body, manner of carrying out the tasks, as well as other matters of importance for the work of the coordinating body from 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 parts or data from the National risk assessment that are not marked with proper level of confidentiality shall be published on the website of the financial intelligence.

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 parts or data from

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 from 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 spent financial resources that were allocated to the financial intelligence unit, competent authorities from Article 96 paragraph 1 of this Law and competent supervisory authorities from Article 131 paragraph 1 of this Law, for the combating money laundering and terrorist financing.

II. 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 terrorism 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 relationship and control of the customer transactions;
3) establish appropriate information system, if it is a credit or other financial institution and, in that way provide automated support for the assessment of the risk of the customer, ongoing monitoring of business relationships of the customer and the control of the transactions and the automatic recognizing suspicious clients or transactions;
4) to submit information, data and documentations on timely manner to FIU
5) to designate authorized officer for implementing measures of detection and prevention of money laundering and terrorist financing and his/her deputy, as well as provide conditions for their work;
6) to organise regular professional training and development of employees;
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 prevention and detection 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 identify the risks and to perform risk analysis of money laundering and terrorism financing to:

- within 60 days since the date of its establishment, develop the risk analysis for determining the risk assessment of an individual customer, a group of customers, a country or geographic areas, 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 update it regularly at least once a year and keep it in accordance with this Law,
- to perform risk analysis for new products, services or distributive channels and according to that assessment, to update the risk analysis,
- to determine categories of money laundering risk and terrorism financing and
- to, based on the risk analysis, make a new risk analysis of each customer, group of customer, state, geographic area, business relationship, transaction, product, services or distributive channels which may be used for purposes of money laundering and terrorism financing.

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

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

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

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

A reporting entity shall submit the risk analysis to the competent supervisory authority from Article 131, paragraph 1 of this Law upon his 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 relationship, transaction, product, service, distribution channel, state or geographic area present lower risk of money laundering or terrorist financing, they may apply simplified Customer Due Diligence measures in accordance with this Law.

If a reporting entity assesses that a customer, business relationship, transaction, product, service, distribution channel, state or geographic area present higher risk of money laundering or terrorist financing, they shall apply enhanced Customer Due Diligence measures in accordance with this Law.

Money laundering and terrorist financing risk management
Article 14

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

1) risk analysis;
2) adoption and implementation of internal regulations on policies, controls and procedures with a view of effective risk management of money laundering and terrorism financing;
3) ongoing monitoring and supervision over established risks of money laundering and terrorism 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 from 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 reporting entity provides.

Policies, controls and procedures from paragraph1, item 2 of this Article shall include:

1) Establishing the internal policies, controls and procedures with reference to:
   - goals, scope and manner of work of system for managing the risk of money laundering and terrorism financing,
   - submitting data to FIU in accordance with the law,
   - protection and storage of data and keeping records,
   - internal controls in the area of prevention and detection of money laundering and terrorism financing,
   - security checks of employees pursuant to the law regulating data confidentiality,
   - designation of compliance officer for prevention of money laundering and terrorism financing and his/her deputy;
2) Establishing an independent auditor function or designating a person for continuous monitoring and supervision over the established risks of money laundering and terrorism financing, as well as checks of internal policies and procedures from item 1 of this paragraph, proportional to the scope and nature of activity of a reporting entity.

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

Internal policies, controls and procedures from paragraph 3, Item 1 of this Article at the reporting entity, who is a big legal person in terms of the law regulating accounting shall be defined by senior manager.

A reporting entity shall to, proportionally to the scope and nature of activities, designate a compliance officer for prevention of money laundering and terrorism financing in a managerial

position.

A reporting entity shall prepare policies, controls and procedures from paragraph 1, item 2 of this Article according to guidelines for establishing the system for risk management of money laundering and terrorism financing, defined by supervising body from Article 131, paragraph 1 of this Law pursuant to Regulation from Article 15 of this Law and 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, services i.e. distributive channels, that reporting entity provides, criteria for establishing risk factors, mandatory elements which risk analysis must include and other elements of importance for drafting the guidelines for establishing the system for risk management of money laundering and terrorism financing shall be prescribed by the state administration authority competent for internal affairs .

Professional basis for drafting the regulation from paragraph 1 of this Article shall be prepared by FIU, along with opinion obtained from supervision bodies from Article 131, paragraph 1 of this Law.

New services, products or distributive channels

Article 16

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

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

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

2. **Identification of the customer and monitoring of business relationship and control of the customer's transactions - Customer Due Diligence**

Customer due diligence measures and monitoring the business of the customer

Article 17

A reporting authority shall Identification of the customer and monitoring of business relationship and the control of the transactions of the customer- Customer Due Diligence (hereinafter CDD measures) the customer and monitoring the business of the customer, especially to:

1) Identify the customer;
2) To 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 relationship or purpose of transaction and other data in accordance with this Law;
4) monitor regularly the business relationship, including control of the transactions

undertaken with the reporting entity by the customer during the business relationship in order to allow that transactions undertaken in accordance with knowledge of the reporting entity on customer, his/her business profile and risk level of money laundering and terrorist financing of that customer and, if applicable on the source of these funds, as well as that data, information and documentation on that customer are updated.

When implementing measures from paragraph 1, Items 1 and 2 of this Article, the reporting entity shall verify 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 implement all measures from paragraph 1 and 2 of this Article, proportionate to the risk of money laundering and terrorist financing.

When determining the scope of implementation of measures from paragraph 1 of this Article, the reporting entity shall to, at least, take into consideration the following:

- the purpose of the conclusion and the nature of the business relationship;
- the amount of funds, the value of the property or the scope of the transaction;
- the duration of the business relationship;
- the compliance of the business with the purpose of the conclusion of the business relationship.

A reporting entity shall, in its internal regulations, establish procedures for conducting measures from paragraph 1, 2 of this Article.

A reporting entity shall submit to the supervision authorities from Article 131 paragraph 1 of this Law, upon 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 a reporting entity cannot implement one or more measures from paragraph 1 of this Article, it shall inform the financial intelligence unit on that, in the manner prescribed by the regulation from Article 66 paragraph 15 of this Law.

Cases in which customer due diligence measures are implemented
Article 18

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

1) when establishing a business relationship with a customer;
2) when executing occasional transactions in the amount of EUR15,000 or more, regardless to that whether the transaction is executed as a single transaction or more linked transactions;
3) during each occasional transaction which, within the meaning from Articles 35 to Article 38 of this Law, represents the transfer of funds in the amount of EUR1,000 or more;
4) when there is a suspicion about the accuracy or authenticity of the customer's and beneficial owner's identification data;
5) when in relation to the transaction, customer, funds or property, there are reasons for suspicion or reasonable grounds to suspect that the property derives from criminal activity or of money laundering or terrorist financing, 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 EUR10.000 or more, regardless of whether the transaction is executed as a single transaction or a number of mutually linked transactions;

7) during the payment of lottery winnings, or payment of stake, while executing one or several linked transactions in the amount of EUR2,000 or more, when customer is organizer of games on chance.

A reporting entity shall periodically implement CDD measures also in relation to customers with which it has already established business relationships based on the risk analysis of money laundering and terrorism financing or upon change of specific circumstances with reference to the customer or when the reporting entity, pursuant to any legal obligation, shall establish contact with the customer during calendar year for check of all relevant information linked with beneficiary owner of the customer, of if a reporting entity was obliged to perform in accordance with regulation regulating tax administration.

If a reporting entity concludes an additional business relationship with a customer or on the basis of the existing business relationship executes the transaction from paragraph 1 items 2 and 7 of this Article, the reporting entity shall obtain only the data that is missing in accordance with this Law, under the condition that he previously taken measures to establish and to verify the identity of the customer and measures of monitoring of customer's business.

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

A reporting entity shall provide information to the customer on the purpose of processing of data which he/she obtains when implementing CDD measures and monitoring of customer's business, pursuant to the Law regulating the personal data protection.

Implementation of CDD measures before establishing a business relationship
Article 19

A reporting entity shall implement the measures from Article 17, paragraph 1, items 1, 2 and 3 of this Law before establishing a business relationship with a customer, including establishing and verifying the identity of person from Article 27 and 28 of this Law.

By way of exception from paragraph 1 of this Article, a reporting entity can implement measures from Article 17, paragraph 1, Items 1 and 2 of this Law also during the establishment of a business relationship with a customer if a reporting entity estimates that it is necessary, and in order not to interrupt the usual business relationship and when there is insignificant risk of money laundering or terrorist financing.

If a reporting entity cannot conduct measures from paragraph 1 of this Article, the business relationship must not be established, and if the business relationship has already been established it must be terminated.
A reporting entity must not establish a business relationship with the customer and if the business relationship has already been established, the reporting entity shall terminate that business relationship, if it assesses that it cannot efficiently manage the risk of money laundering and terrorism financing in relation to this customer.
A reporting entity shall, with internal regulations, define the procedures for refusal of establishing the business relationship or termination of already established business relationship from paragraph 3 and 4 of this Article.

Implementing CDD measures before conducting a transaction
Article 20

Reporting entity shall apply measures from Article 17 paragraph 1 Item 2 of this Law before conducting the transactions from Article 18 paragraph 1 Items 1, 2, 3,6 and 7 of this Law.

If the reporting entity cannot undertake one or more measures from paragraph 1 of this Article, the transaction must not be conducted.

Identification of the beneficiary i.e. beneficiary owner of a life insurance policy
Article 21

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

A reporting entity from Article 4, paragraph 2, item 8 and 9 of this Law shall verify the identity of the beneficiary i.e. beneficiary owner under the policy from paragraph 1 of this Article, in case when:

1) natural, i.e. legal person is nominated as a beneficiary, by taking data on his/her 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 i.e. beneficiary owner from 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 person, partially or completely, the reporting entity shall identify a new customer at the time of transferring the rights.

A reporting entity from Article 4, paragraph 2, items 8 and 9 of this Law shall to, by internal regulations, define procedures for implementation of measures from 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 business activity pursuant to Article 18, paragraph 1 item 1 and Article 19 and 20 of this Law, by access to identity document, with his/her presence.

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

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

When establishing the identity of the customer from paragraph 1 of this Article, there shall be collected data on the customer, business relationship and transaction from Article 117, paragraph 1, item 2,3,4 and 6 of this Law.

If all data from paragraph 4 of this Article can not be obtained, those data shall be obtained by access to original document or certified photocopy of other valid public document that customer presents or by access to public registry.

If legal representative or authorized person the customer from paragraph 1 of this Article establish employment relationship or perform transaction on behalf of the customer from paragraph 1 of this Article, the reporting entity shall to:

- establish the identity of that legal representative or authorized person pursuant to paragraph 1 to paragraph 5 of this Article and to provide data on that person from Article 117, paragraph 1, items 3 and 4 of this Law,
- to provide data on the customer from Article 117, paragraph 1 items 3 and 4 of this Law from the written Power of Attorney in original or certified photocopy of that Power of Attorney,
- to check the data on customer which he/she obtained pursuant to indent 2 of this paragraph.

If the reporting entity, in the process of identification of the customer from paragraph 1 of this Article, its legal representative or authorized person from 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, he/she shall ask the written statement of the customer, its legal representative or authorized person on veracity of those data.

The reporting entity may check data from identity documents of the customer, its legal representative or authorized person from paragraph 1 of this Article through financial – intelligence unit, through access to Central Registry of Population (hereinafter: CRP), record of issued identity documents and international base of stolen, lost and not valid documents, electronically.

If during the checks from 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 relationship or execute a transaction.

After caring out the identification of the customer from paragraph 1 of this Article, the reporting entity shall enter the information on the manner in which the identification was carried out in the records from article 117, paragraph 1 of this Law.

The manner of data verification from paragraph 8 of this Article shall be prescribed by the Ministry.

Act from paragraph 10 of this Article shall be marked with appropriate level of data confidentiality, pursuant to the law regulating the data confidentiality.

Electronic identification
Article 23

Identification of the customer who is a natural person, entrepreneur or a natural person who performs business activity, his/her legal representative and authorized person 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 regulating electronic identification and electronic signature (hereinafter: electronic identification).

Prior to electronic identification the customer from paragraph 1 of this Article shall provide to the reporting entity a photocopy of an identity document, and in the case of identification of its legal representative or authorized person, also a photocopy of Power of Attorney by which he/she proves the capacity of legal representative or authorized person, in electronic form.

Prior to electronic identification, the reporting entity shall obtain data on customer from paragraph 1 of this Article, business relationship and transaction from Article 177, paragraph 1, Items 2,3,4 and 6 of this Law.

A reporting entity shall check the data from Article 117, paragraph 1, Items 2,3,4,6 and 7 of this Law through financial intelligence unit, by access to CRP, into record of issued identity documents and into international base of stolen, lost and not valid documents, electronically, in the manner which is prescribed by Act 114from Article 22, paragraph 11 of this Law.

A reporting entity may perform identification electronically only for a service or for a product which it provides within its business activity and for the customer for whom a high risk of money laundering and terrorism financing hasn't been established.

Electronic identification cannot be performed if:

- during the check from paragraph 4 of this Article it is established that data from the identity document of the person from paragraph 1 of this Article are different from those in CRP;
- the mean of electronic identification or qualified certificate for electronic signature from paragraph 1 of this Article is issued under pseudonym;
- there is a suspicion that a mean of electronic identification or qualified certificate for electronic signature of the person from paragraph 1 of this Article is abused, or if the reporting entity establishes that circumstances which substantially affect validity of that means of electronic communication or qualified certificate for electronic signature are changed and the service provider of electronic identification or qualified provider of

electronic trust service was not revoked that mean or certificate;

- the electronic identity document from 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, he/she shall terminate the electronic identification.

In order to perform electronic identification, the reporting entity shall provide:

- technical and other conditions which enable the verification at any time whether the mean of electronic identification or qualified certificate for electronic signature is valid;

- technical conditions for keeping records on performing electronic identification.

After performed electronic identification , the reporting entity shall enter, into records from Article 177 paragraph 1 of this Law, data on the manner in which the identification of a person from paragraph 1 of this Article was conducted.

Video-electronic identification
Article 24

Identification of the customer who is a natural person, entrepreneur or natural person who performs business activity, his/her legal representative and authorized person can be performed remotely, through the procedure of video identification by use of means of electronic communication (hereinafter: 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 shall prior the start of video-electronic identification to provide consent of the person from 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: 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 provision of consent from paragraph 3 of this Article must be video and audio recorded.

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

The person from paragraph 1 of this Article shall provide to the reporting entity a photocopy of electronic identity document which he/she will use during video-electronic identification, in electronic form.

When performing video-electronic identification, the reporting identity shall perform electronic reading of data from the identity document, issued by competent authority and which is not issued in high-risk third country and obtain the data from paragraph 1 of this Article,

business relationship and transaction from Article 117 paragraph 1, items 2,3,4,6 and 7 of this Law.

By electronic reading of the data from electronic identity document, the reporting entity shall obtain data on the entrepreneur or natural person from 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 from Article 117, paragraph 1, Items 2 and 3 of this Law, which cannot be obtained through 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 from paragraphs 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 the manner prescribed by act from Article 22, paragraph 11 of this Law.

A reporting identity shall 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 representative or authorized person of the customer prior to establishing of business relationship or executing transaction, that legal representative or authorized person shall display and submit a photocopy of the Power of Attorney by which he/she proves the capacity of the legal representative or authorized person.

A reporting entity may perform the video-electronic identification only for the service or for the product which he/she provides within his/her business activity and for the customer for whom a higher risk of money laundering and terrorism financing hasn't been established.

A reporting entity must not perform a video-electronic identification if an electronic identity document of the person from paragraph 1 of this Article is issued in high-risk third country.
A reporting entity shall terminate the video-electronic identification if:

- during the verification from paragraph 1 of this Article it is established that data from the identity document of the person from 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 are collected;
- it is not possible to provide an uninterrupted transmission of image and sound or high-quality transmission;
- the room where the person from 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 is not possible to hear clearly that person or employee;
- due to other disturbances in communication, transmission of the image and/or the sound or other circumstances, the employee cannot perform identification of the person from paragraph 1 of this Article.

The identification of the person from paragraph 1 of this Article may be performed in repeated procedure of video-electronic identification, only if the previous procedure is terminated due

to circumstances from paragraph 15 of this Article and only after removal of these circumstances.

After performed video -electronic identification , the reporting entity shall enter, into records from Article 177 paragraph 1 of this Law, data on the manner in which the identification of a person from paragraph 1 of this Article was conducted.

A reporting entity shall define the manner of performing the video-electronic identification by its internal regulations, in accordance with act from paragraph 19 of this Article, not later than eight days from the day of submission the decision from Article 25, paragraph 6 of this Law, which approves performing of video-electronic identification.

Closer conditions and manner of performing video-electronic identification, as well as the manner of organizing and content of the training from paragraph 2 of this Article, shall be prescribed by the Ministry.

Authorization for performing the electronical identification and video – electronic identification
Article 25

A reporting entity may perform electronic identification or video-electronic identification of the customer who is a natural person, entrepreneur or natural person who performs business activity, its legal representative and authorized person only, if it has authorization for performing the electronic identification or video-electronic identification.

Request for issuing the authorization from paragraph 1 of this Article, the reporting entity shall submit, onto prescribed form, to the competent supervising authority from Article 131, paragraph 1 of this Law.

Along with request from paragraph 2 of this Article, the reporting entity shall submit evidences on fulfilment of conditions from Article 23 paragraph 8 of this Law i.e. conditions prescribed by act from Article 24 paragraph 19 of this Law.

A supervising authority from Article 131, paragraph 1 of this Law shall submit the request from paragraph 2 of this Article and evidences from paragraph 3 of this Article to the financial intelligence unit.

The head of the financial intelligence unit shall form an interagency commission which establishes the fulfilment of conditions from paragraph 3 of this Article.

Upon proposal of the commission from paragraph 5 of this Article, the head of financial intelligence unit, shall, upon request from paragraph 2 of this Article, adopt the decision by which authorizes or refuses to the reporting entity to perform electronic identification or video-electronic identification.

The Commission from paragraph 5 of this Article shall propose adoption of the decision by which the request from paragraph 2 of this Article is refused if it establishes that a specific service or product represents higher risk of money laundering and terrorism financing for the purpose of this Law.

An administrative dispute can be initiated against the decision from paragraph 7 of this Article.

Commission from paragraph 5 of this Article shall be consisted of representatives of the financial intelligence unit, other organizational units and supervising authorities from Article 131, paragraph 1, Items 1, 3, 4 and 8 of this Law.

The Commission from paragraph 5 of this Article has the president, members and secretary.

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

The view and content of the request from paragraph 2 of this Article and manner of work of the Commission from 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 verify the identity of a customer that is a legal person or a business organization, pursuant to Article 19 and 20 of this Law, in the manner to obtain the data from Article 117, paragraph 1, Items 1,6 and 7 of this Law for the legal person or business organization that establishes business relationship or executes a transaction or legal person or business organization on whose behalf a business relationship is being established or transaction executed.

A reporting entity may obtain data from paragraph 1 of this Article by checking the Central Business Registry (hereinafter: CBR) or other appropriate public register, as well as checking court, business or other public register of a foreign legal person or business organization in which is entered foreign legal person or business organization.

A reporting entity may also obtain data from paragraph 1 of this Article by access into original or certified photocopy of the document from the CBR or other appropriate public register, as well as checking original or 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 submits its legal representative or authorized person and which mustn't be older than three months of its issue date.

A reporting entity shall keep the original or certified photocopy of the documents from paragraph 3 of this Article in its files.

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

The data which are not included in the registries from paragraph 2 of this Article or in the documents from paragraph 3 of this Article, the reporting entity shall obtain by accessing the original or certified photocopy of the document or other documentation submitted by the legal representative or authorized person of the customer from paragraph 1 of this Article.

If a reporting entity, during identification of the customer that is a legal person or business

organization doubts in veracity of the obtained data or authenticity of the documents or public or other documentations from which the data were obtained, it shall also, before establishment of business relationship or performing transaction, obtain from the legal representative or authorized person, a written statement on veracity of these data.

If the customer is a foreign legal person that performs activity in Montenegro through its business unit, the reporting entity shall perform identification of the foreign legal person and its business unit.

Establishing the identity of the legal representative of a legal person and business organization
Article 27

A reporting entity shall establish the identity of the legal representative of the customer who is a legal person or business organization pursuant to Article 22 of this Law.

A reporting entity shall obtain the data on all directors of the legal person or business organization from Article 117, paragraph 1 item 3 of this Law.

A reporting entity shall, in the procedure of establishing and checking the power of attorneys of the authorized representative and all directors from paragraph 2 of this Article obtain those power of attorneys and to keep them in his/her documentation.

If the reporting entity has update data on directors from paragraph 2 of this Article, he/she is 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 legal representative 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 relationship 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 obtain the data on the legal representative and directors from paragraph 1 of this Article, by accessing the original or certified photocopy of power of attorney which he/she shall keep in his/her 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 to:

1) establish the identity of his/her legal representative or authorized person pursuant to Article 27 and 28 of this Law;

2) to obtain the data from Article 117, paragraph 1, items 1,2 and 3 of this Law for founders, all trustees, other representatives, users or group of beneficiaries of the property he/she manages with, if future beneficiaries have already been designated or determinable and other natural person who directly 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 regulation on founding the trust, other person or other foreign entity equal to them.

The data from 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 must not be older than three months and shall check those data.
If a reporting entity, when establish the identity of the legal representative and authorized person of the customer, from 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, he/she shall 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 his/her legal representative, or a person he/she has authorized, to the safe deposit box.

When establishing identity of the customer from paragraph 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 he/she participates in the games of chance on his/her own behalf and in his/her name.

The identity of the customer may be established when the customer accesses the safe deposit box through an electronic identification card or personal access password or through the electronic video identification, or means which allow the identification of the customer on the basis of the his/her 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 from Article 117, paragraph 1, Items 3 and 2 of this Law.

Implementation of CDD measures through a third person
Article 31

Under the conditions provided for by this Law, when establishing business relationship with a customer, a reporting entity may entrust the implementation of the measures from 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) a bank and other credit institution and branch of a foreign bank.
2) a company for the management of investment funds;
3) a company for the management of pension funds;
4) investment company whose business activity is defined by the law which governs a capital market,
5) life insurance company and branch of foreign life insurance company;
6) mediation company, representation company and entrepreneurs – agents in insurance in the part related to life insurance;
7) persons from Items 1 to 6 of this paragraphs with seat in a country of European Union or in other country which implements measures in the area of prevention of money laundering and terrorism financing, stipulated by this law or more severe measures,

External associates and representatives of the reporting entity who based on the agreement (externalization- external representation or legal representation) conduct certain CDD measures shall not be considered as a third party within the meaning 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 must not entrust the implementation of CDD measures and monitoring customer's business operation to a third party when a third party is a shell (fictious) 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 person that implements CDD measures and monitoring of customer's business operation in accordance with Article 31 of this Law shall deliver to the reporting entity the obtained data and documents on the customer.
A third party referred to in paragraph 1 of this Article shall upon a request of a reporting entity, without delay, provide photocopies of identification documents and other documents based on which it implemented CDD measures, as well as data obtained pursuant to Article 23 and Article 24 of this Law, if there has been performed electronical identification and video-electronic identification.

A third party referred to in paragraph 1 of this Article shall keep the obtained photocopies of

identification documents and documentation in accordance with this Law.

Obligations of reporting entities in case of obtaining data and documentation from a third party
Article 34

If a reporting entity doubts the validity of the performed CDD measures by a third party, or the veracity of obtained data and documentations on customer, the reporting entity shall directly implement those measures.
Create

The reporting entity shall through an internal regulation define 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 collect data on the payer and payee and enter them into a payment order form or electronic message accompanying the transfer of funds from the payer to the payee.
The data on the payer from paragraph 1 of this Article shall be:

1) first and last name or (business) name;
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 or registered office.

If the payment service provider is not able to obtain data on the address or registered office of the payer, it must provide one of the following data:

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

Data on the payee from paragraph 1 of this Article shall be:

1) first and last name or business name,
2) number of payment account or a unique designation mark 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 from paragraph 2 and 3 of this Article into a form of the payment order or electronic message accompanying transfer of funds , if data from paragraph 2,3 and 4 of this Article are included in the payment order for or electronic message accompanying 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 or a unique designation mark of the transaction, it transfer of funds is performed without opening of payment account.

The exception from 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.

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

1) first and last name or business address of the payer and the payee,
2)number of payment account of the payer and of the payee or a unique designation mark of the transaction if transfer is performed without opening of the payment account.

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

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

By 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:
1) payment service provider of the payer receives funds which needs to be transferred in cash or in anonymous electronic money, or
2) there are reasons for suspicion in money laundering and terrorism financing.

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

The payment service provider of the payer shall define, by internal regulation, the procedures for verification of completeness of data collected pursuant to paragraph 2 and 9 of this Article.

Obligations of the Payment Service Provider of the payee
Article 36

Payment service provider of the payee shall verify whether the data on the payer and on the payee are entered into a payment order form or electronic message accompanying transfer of funds pursuant to Article 35 of this Law.

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

If the amount of money transfers, including also the amount of payment transactions connected with that transfer, 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, or
2) there are reasons for suspicion in money laundering and terrorism financing.

The verification of the accuracy of the collected data from paragraphs 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 may, in accordance with risk assessment, verify the accuracy of data of the payee, regardless to the amount of funds that are subject of transfer.

Procedure in case of delivering of inaccurate and incomplete data
Article 37

Payment service provider of the payee shall, in accordance with risk assessment, make an internal regulation on procedure, including where applicable, ex-post monitoring or real time monitoring, in case that a payment order form or electronic message accompanying money transfer does not contain accurate and complete data from Article 35 of this Law.
If a payment order form or electronic message accompanying money transfer does not contain accurate and complete data from Article 35 of this Law, the payment service provider of the payee shall, in accordance with the risk assessment, through internal regulation from paragraph 1 of this Article, prescribe when to:

1) refuse the transfer of funds;
2) terminate the performing of transfer of funds till receiving the missing data, which he/she shall 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 or data which are not entered in a payment order form or electronic message accompanying 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 warn him/her and determine the date within which the it needs to comply with his/her activities with this Law.

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

Payment service provider of the payee shall inform the Central Bank of Montenegro on that payment service provider of the payer who repeatedly does not submit the accurate and complete data pursuant to Article 35 of this Law, and on measures which he/she has taken pursuant to paragraphs 3 and 4 of this Law toward that payment service provider of the payer .

Payment service provider of the payee shall establish whether the lack of accurate and complete data from Article 35 of this Law presents the reasons for suspicion in money laundering or terrorism financing and if establishes that this lack presents the reasons for suspicion, and inform financial intelligence unit on that pursuant to Article 66, paragraphs 6, 8 and 10 of this Law.

If the payment service provider of the payee establishes that deficiency from paragraph 6 of this Article does not present reasons for suspicion in money laundering and terrorism financing, he/she shall make a note that is kept pursuant to this Law.

Obligations of the intermediary in transfer of funds
Article 38

An intermediary in the transfer of funds shall ensure that all data on the payer and the payee are kept in payment order form or electronic message accompanying transfer of funds .

An intermediary in the transfer of funds shall, using the approach based on the risk assessment, to make an internal regulation on procedure, including, where applicable, ex-post monitoring or real time monitoring, in case if the payment order form or electronic message accompanying the funds transfer, does not contain accurate and complete data from Article 35 of this Law.

If the payment order form or electronic message accompanying transfer of funds does not contain the accurate and complete data from Article 35 of this Law, the intermediary in transfer of funds shall perform pursuant to Article 37, paragraph from 2 to 7 of this Law.

Exemption from obligation of collecting data on the payer and the payee
Article 39

Provisions from 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 services, 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 or the unique identification designation mark follow that transfer of funds in the manner which enables access to 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 his/her 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 on 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 payer can, through the payee, with unique identification designation mark of transaction or with other data accompanying 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 doesn't exceeds the amount of EUR 500;
- If the payments for these services is performed by approval of the account of the payee which refers exclusively for those charges; and

- all conditions from Article 40, paragraph 1 of this Law are met.

Exemptions from implementation of CDD measures in case when electronic money is used
Article 40

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

1) a payment instrument cannot be loaded again or the maximum monthly limit for payment is restricted t amount of EUR 150 and can be used only in Montenegro;
2) the amount of deposited electronic money doesn't exceed the amount of EUR 150;
3) the payment instrument is used solely for purchase of goods or services;
4) if anonymous electronic money cannot be deposited to the payment instrument,
5) if the issuing body of the electronic money performs appropriate measures of monitoring of business relationship and control of transactions with a view of revealing complex and unusual transactions from 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, as well as initiating a transaction via the Internet or using means of remote communication, if the amount of the transaction exceeds 50 euros.

A reporting entity may accept payment with anonymous payment instrument, if that payment instrument meets conditions from 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 be applicable to the cases where in connection to transaction or the customer, there are reasons for suspicion or reasonable grounds to suspect that property derives from the criminal activity or that money laundering or terrorism financing has been committed.

4**. Establishing Beneficial owner**

Beneficial owner
Article 41

Beneficial owner is the natural person that has ownership or ultimately exercises control over a legal person, business organization, foreign trust, foreign institution or similar foreign entity equal to it or natural person on whose behalf or for whose account transaction is being carried out.

A beneficial owner of a business organization, or legal person, in the context of this Law, shall be a natural person who:

1) directly or indirectly owns at least 25% of the shares, voting rights or other rights, on the basis of which he/she participates in the management, or owns at least 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 decisive influence on business activity and decision making process in the legal person or business organization.

If it is not possible to identify the beneficial owner or if there is a suspicion that the natural person from 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 legal person or business organization.

If it is not possible to determine 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 organization is 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) directly or indirectly controls at least 25% of a legal person's assets;
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, other person or a similar foreign entity equal to them , who receives, manages or allocates the funds for certain purposes, shall be considered a natural person who is:

1) the founder of a foreign trust, other person or a similar foreign entity equal to it;
2) the trustee of a foreign trust, other person or a foreign entity equal to it;
3) the beneficiary of the assets obtained from the property which he/she manages, 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, other person or a foreign entity equal to it when the individuals who receive the benefits from the foreign trust, other person of a foreign entity equal to it has yet to be determined;
6) natural person who, in any other way, directly or indirectly 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 establish the beneficiary owner of the legal entity, business organization, trust, other person or similar foreign entity equal to it, through obtaining data on entities, their beneficial owners and category of persons interested in establishing of trust, other person or similar foreign entity equal to it from Article 44 of this Law.

Data from paragraph 1 of this Article, the reporting entity may obtain by accessing the registry from 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 he/she shall print the excerpt from that registry and time, first and last name of the person who accessed the registry.

Data from paragraph 1 of this Article, the reporting entity may obtain 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 photocopy 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 paragraphs 2 and 3 of this Article, the reporting entity establishes that there is a difference in the data, the reporting entity shall, without delay, submit the data which differ to financial intelligence unit and the state administrative authority competent for tax collection.

A reporting entity shall obtain the data which are not included in registries or in the documents from paragraphs 2 and 3 of this Article, by accessing to original or to certified photocopy of the document or any other documentation, submitted by the legal representative or authorized person of the customer who is a legal entity or business organization.

A legal entity shall, in addition to the data from paragraph 1 of this Article, also obtain the documentation on basis of which 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 person, business organization, trust, other person or foreign entity equal to it which he/she 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 must not rely only on the data from the registry from Article 43, paragraph 1 of this Law.

The reporting entity shall, in the procedure of identification of the beneficial owner from paragraph 1 of this Article, provide a photocopy of an identity document of the beneficial owner from Article 22, paragraph 3 of this Law.

If the reporting entity during collection of data from paragraph 2, 3,5,6 and 7 of this Article, doubts in veracity of obtained data or authenticity of identity documents or other documentation from which the data were obtained, he/she shall obtain a written statement from the legal representative or authorized person.

A reporting entity shall keep the original, certified photocopy and excerpt from paragraphs 2,3,5 and 6 of this Law in his/her documentation.

A reporting entity shall keep records on measures which he/she has taken to identify the beneficial owner from paragraph 1 of this Article.

Beneficial Owners Register

Article 43

Beneficial Owners Register(hereinafter: the 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 Register is kept by the administrative authority competent for tax collection.

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

Obligation from 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
- legal persons and business organizations in multiple joint stock companies who trades shares on the organized securities market, where they are obliged to be compliant with obligation of publishing data and information on beneficial ownership pursuant to the law regulating rights and obligations of the subjects on the securities market and other law.

Subjects from paragraph 3 of this Article shall verify and confirm the accuracy of data entered into the Registry once a year, and not later than 31st March of the current year. .

The beneficial owner of the subject from paragraph 3 of this Article shall submit to that subject the data from Article 44 paragraph 1 point 2 idents 1, 2 and 4 of this Law in order to enter these data in the Register.

The subjects from paragraph 3 of this Article and their beneficial owners are responsible for the accuracy of data entered into the Registry.

The manner of verification of the data from the Registry shall defined by the Ministry.

Content of the Beneficial Owners Register

Article 44

The Beneficiary Owners Register shall contain the following data:

1) data on the subject from 43, paragraph 3 of this Law:
   - name, address, seat, identification number or any other identification number, tax identification number (hereinafter: TIN), date of registration and date of deletion from the CBR or from the Registry of tax payers;
   - data on their status;
   - form of organization;
   - codes of business activity;
   - data on legal representative, trustee or authorized person (first and last name, unique personal identification number, date of birth, adress 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 or 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 he/she manages or the share in the property of the legal entity or similar foreign entity equal to it);
   - graphic view of the ownership structure if the reporting entity has a complex ownership structure;
   - address for mail receiving;
   - e-mail address;
   - number of accounts in credit institutions;

- scanned documentation which proves the entered data;

2) data on the beneficial owner:
   - 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 he/she directly provides/provided funds or he/she has 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;
   - scanned documentations which proves entered data;

3) data on the category of persons interested in establishing the trust, other person or similar foreign entity equal to it when persons who gain benefit from the trust, other person or foreign entity equal to it (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 into the Beneficial Owners Register

Article 45

Subjects from Article 43 paragraph 3 of this Law, shall enter and update in to the Registry the data:
1) from Article 44, paragraph 1, Item 1 of this Law;
2) on the beneficial owner from Article 44 paragraph 1 item 2 of this Law;
3) on the category of persons with an interest for establishing foreign trust, other person or similar foreign legal entity equal to it when persons who benefit from foreign trust, other person or similar foreign legal entity equal to it are to be determined from Article 44 paragraph 1 item3 of this Law.

In addition to data from paragraph 1 of this Article, subjects from Article 43, paragraph 3 of this Law who have a complex ownership structure shall also enter into the Registry:
- a note on existence of a complex ownership structure of that person;
- 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 must 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 within the meaning of paragraph 2 of this Article is the ownership structure where the founder, i.e. the owner of the subject from Article 43, paragraph 3 of this Law is at least one legal person or a legal arrangement or any other foreign subject equal to it.

The manner of entering and updating data into the Registry shall be prescribed by the Ministry.

Maintaining and managing the Beneficial Owners Register

Article 46

The administrative authority competent for tax collection shall maintain and to manage the Beneficial Owners Register in the manner that:

- in addition to last entry of the data from Article 44 of this Law, it keeps the previous entries 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 will be available to reporting whenever they need those data;
- to enable unlimited access to all data, kept in the Registry to the financial intelligence unit supervising authorities from Article 131, paragraph 1 of this Law, other authorities competent for prevention and detection of money laundering and related predicate criminal offences or terrorism financing;
- the data shall be available in the period of five years after deletion of subject from Article 43, paragraph 3 of this Law or from CBR or from the Registry of tax payers, to the financial intelligence unit, supervising bodies from Article 131, paragraph 1 of this Law and to other authorities competent for prevention and detection of money laundering and related predicate criminal offences or terrorism financing.

Access to the Beneficial Owners Register
Article 47

The access to data from the Beneficial Owners Register of beneficial owners shall have:

(1) the financial intelligence unit, supervising bodies from Article 131, paragraph 1 of this Law and competent authorities from Article 96, paragraph 1 of this Law;
(2) Reporting entities; and
(3) other legal and natural persons.

Subjects from paragraph 1, Item 1 of this Article shall have direct electronic access to all data from the Registry.

Reporting entities have direct electronic access to data on beneficial owners entered into the Registry, for the purpose of conducting the procedure for establishing the customer's identity.

Other legal and natural persons have direct electronic access to data on beneficial owners of subjects from Article 43, paragraph 3 of this Law, based on electronic identification in accordance with the law regulating electronic identification, as follows: first and last name, year of birth, citizenship, country of residence, type and scope of ownership share.

Subject from Article 43, paragraph 3 of this Law may submit to the administrative authority competent for tax collection, the request for restriction or denial of access to all or to a part of the data from paragraph 4 of this Article, to legal or natural persons from paragraph 1 Item 3 of this Article, if the access to those data would led the beneficial owner to risk of fraud, kidnaping,

blackmail, violence or intimidation or if the beneficial owner is a child or a person deprived of his or her legal capacity.

Financial intelligence unit shall establish the existence of circumstances from paragraph 5 of this Article, by a decision.
When the financial intelligence unit establishes the existence of circumstances from paragraph 5 of this Article, the administrative authority competent for tax collection shall restrict, or deny the access to legal or natural persons from paragraph 1, Item 3 of this Article, to all or to a part of data to which the request from paragraph 5 of this Article refers to.

The administrative dispute may be initiated against decision from paragraph 6 of this Article.

The detailed manner on the access to data from the Registry shall be prescribed by the Ministry.

Supervision regarding data entry into the Beneficial Owners Register
Article 48

When performing supervision of subjects from Article 43, Paragraph 3 of this Law, the administrative authority competent for tax collection shall control if:

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

Within the supervision from paragraph 1 of this Article, administrative authority competent for tax collection shall perform direct and indirect supervision pursuant to Article 132 of this Law.

Subjects from Article 43, paragraph 3 of this Law shall, upon request of administrative authority competent for tax collection, submit documentation based on which it is possible to establish the ownership structure and control member of the customer and to collect data on the beneficial owner.

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

Monitoring of the business relationship and transactions
Article 49

A reporting entity shall conduct measures of monitoring business relationship of the customer, including control of the transaction and monitoring of the source of funds with which the customer operates, whereby he/she shall collect the data from Article 117, paragraph 1, Items 6 and 7 and paragraph 3 to 6 of this Law, depending on the type of reporting entities.

Measures from paragraph 1 of this Article, particularly includes:

1) verification of compliance of customer's business with nature and purpose of the business relationship;
2) control of transactions in accordance with the scope client's risk of money laundering and terrorism financing;
3) monitoring and verification of compliance of customer's business with his/her usual scope of business activity;

4) verification of sources of funds that customer operates with or performs transaction in accordance with its scope of risk of money laundering and terrorism financing;
5) monitoring and updating the data on the customer, beneficial owner of the customer and scope of risk of money laundering and terrorist financing, and verification of data whether the customer or beneficial owner has became or ceased to be politically exposed person referred to Article 54 paragraphs 2,3 and 4 of this Law.

A reporting entity shall provide and adjust a scope and dynamics of taking measures from paragraph 1 of this Article to the risk of money laundering and terrorist financing to which the beneficial owner is exposed in performing an specific business activity or doing business with a customer.

A reporting entity may update the data on customer, beneficial owner of the customer and verify data whether the customer or beneficial owner of the customer has became or ceased to be politically exposed person referred to Article 54 paragraphs 2,3 and 4, by accessing to CRP, record of issued identity documents, Beneficial Owners Register, CBR, registry from Article 55, paragraph 1 of this Law or any other relevant public registry or by accessing the original or certified photocopy of the document from CBR or other public registry.

The data which are not included in registries, records and documents from 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 its request, shall be submitted by the customer.

If, during verification of the data from paragraphs 4 and 5 of this Article, the reporting entity established the difference in data, he/she can call the customer for verification of all relevant information.

Annual control
Article 50

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

- a foreign legal person who carries out transactions at the reporting entity from Article 18, paragraph 1, Items 2,3,5 and/or 6 of this Law, and
- a legal person with head office situated in Montenegro, with foreign capital share of at least 25%, who performs transactions at the reporting entity from Article 18, paragraph 1, items 2,3,5 and/or 6 of this Law.

Control of the customer from paragraph 1 of this Article shall include:

1) Obtaining or verification of data from Article 117 of this Law;
2) Obtaining or verification of data from Article 44 of this Law;
3) Obtaining of authorization from Article 28, paragraph 2 of this Law.

If a business unit of the foreign legal person performs transactions from 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 from paragraph 1, Indent 1 of this Article, in addition to data from paragraph 2 of this Article, shall provide also the following:

1) data on the address and head office of the business unit of the foreign legal person;

2) data from Article 117, paragraph 1, Item 3 of this Law that refer to legal representative of business unit of the foreign legal entity.

Data from paragraphs 2 and 3 of this Article, the reporting entity shall obtain by accessing to CRB, records of issued identity documents, Beneficial Owners Register, CBR, court, business or other relevant public registry where the foreign legal person has been registered, 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.

Data which are not included in registries, records and identifying documents from paragraph 5 of this Article, the reporting entity shall provide by accessing to the original or certified photocopy of the identification document or other documentation which, upon request, shall be provided by the customer.

If, during verification of the data from paragraph 2 of this Article, the reporting entity established the difference in data, he/she may call the customer for verification of all relevant information.

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

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

Types of special forms of CDD measures
Article 51

In addition to CDD measures, the reporting entity shall also apply the special CDD measures depending on established level of risk of money laundering and terrorism financing:

1) Enhanced CDD measures,
2) Simplified CDD measures.

Cases in which enhanced CDD measures are applied
Article 52

A reporting entity shall apply enhanced CDD measures in sectors and business activities from Article 7 paragraph1 ident 3 of this Law, as well as in cases when higher risk of money laundering and terrorism financing is established, as follows:

1) in correspondent relationship with credit or any other financial institution which has head office situated outside European Union or in the high-risk third country;
2) when the customer or beneficial owner of the customer is a politically exposed person from Article 54, paragraph 2, 3 and 4 of this Law;
3) when providing custody services pursuant to the law which governs the capital market,
4) in complex or unusual transaction from Article 58 of this Law;
5) in suspicious transactions;
6) in process of establishing business relationship carrying out transaction with a person 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 terrorism financing has been established in guidelines on risk analysis from Article 12, paragraph 5 of this Law,
8) When in accordance with National Risk Assessment a higher risk of money laundering and terrorism financing has been established.

A reporting entity shall apply enhanced CDD measures even in other cases when it estimates that in relation to the customer, group of customers, country or geographic area, business relationship, transaction, product, service or distributive channel there is or there might be a high risk of money laundering and terrorism financing.

Enhanced CDD measures in correspondent relationship with credit or other financial institution whose head office is situated outside European Union or in high-risk third country

Article 53

When establishing the correspondent relationship which includes payment with credit or other financial institution whose head office is situated outside European Union or in high-risk third country, and which is the respondent, the reporting entity shall, in addition to measures from Article 17 of this Law, take additional measures, as follows:

1) obtain a license for performing bank services, as well as issuance date, name and head office of the competent authority that issued the license;
2) obtain documentation on internal procedures which are carried out for prevention and detection of money laundering and terrorism financing, specifically on the procedures of verification of the customer, identifying beneficial owner, reporting data on suspicion transactions, activities and customers to competent authorities, records keeping, internal controls and other procedures which credit or other financial institution has established with reference to prevention and detection of money laundering and terrorist financing;
3) obtain data, information and documentation on the assessment of internal control on conducting measures for prevention of money laundering and terrorist financing to the credit or other financial organization;
4) obtain data and information on legal or institutional regulations in the field of prevention of money laundering and terrorist financing which are implemented in other country where credit institution has head office or in which the credit institution is registered;
5) verify whether credit or other financial institution, in accordance with the law of a country where its head office is situated or in which it is registered, shall implement relevant regulations in the field of prevention and detection of money laundering and terrorist financing, including the information whether the institution is under investigation related to money laundering and terrorist financing or whether it is the subject of measures taken by competent authorities,
6) establish that credit or other financial institution does not operate as a shell(fictious) bank,
7) verify that credit or other financial institution does not have established or it does not establishes business relationships or caries out transactions with shell(fictious) banks,
8) obtain a written statement that credit or other financial institution with reference to a brokerage account has verified the identity and has performed ongoing procedure of applying CDD of a customer who has direct access to the account and that, upon the reporting entity's request it is able to provide relevant data in relation to the procedure.

In addition to measures from paragraph 1 of this Article, a reporting entity shall also obtain enough information on credit or other financial institution that is the respondent, which are necessary for complete understanding of the nature of its business operations and establishing reputation of that institution from publicly available sources.

A reporting entity shall obtain data from paragraph 1 of this Article by accessing identification documents and documentation which credit or other financial institution provides or from the public or other available data records.

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

A reporting entity must not establish or continue correspondent relationship with credit or other financial institution which has its head office situated outside the European Union or in a high-risk third country if:

1) it previously failed to take measures from paragraphs 1 to 4 of this Article,
2) a credit or other financial institution does not have established controls of system for the prevention of money laundering and terrorist financing or does not implement laws and other regulations from the area of prevention and detection of money laundering and terrorist financing, or
3) a credit or other financial institution operates as a shell (fictious) bank or if it establishes correspondent or other business relationships and carries out transactions with shell (fictious) banks.

Politically exposed persons
Article 54

A reporting entity shall, prior to establishing business relationship with the customer, verify, in the registry from Article 55 of this Law, whether the client, his legal representative , authorized person or beneficial owner of a customer is politically exposed person.

Politically exposed person, for the purpose of this Law, shall be a Montenegrin citizen who performs public office, and that is:

1) President of Montenegro, President of Montenegrin Parliament, Prime minister and member of the Government,
2) member of the Parliament,
3) president of a political party and his/her deputy, a member of presidency of political party, and his/her deputies, member of an executing board, member of a main board and other officials in a political party;
4) State Secretary, Director General of a ministry and Secretary of a ministry, director, deputy of 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 Prosecutor's Office and Special State Prosecutor's Office,
7) member of the Senate of the State Audit Institution and Council of the Central Bank of Montenegro,
8) director and deputy director of an administrative authority;
9) mayor, president of a 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 to a director and member of governing body and supervising authority of the legal person that is in majority owned by the state.

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

1) President of a State, Prime minister, minister and his/her deputy,
2) Member of Parliament,
3) Member of managing body of a political party,

4) Member of the Supreme court, Constitutional court or other judicial court on high level against whose judgment, save in exceptional cases, it is not possible to use regular or extraordinary remedy,
5) Member od Audit court or a 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 person majority owned by a state,
8) director, deputy or assistant to a director and member of a board or other relevant position in international organization.

Politically exposed persons shall be also members of an immediate family of the person from paragraphs 2 and 3 of this Article and their close associates.

Members of the immediate family of the person from paragraphs 2 and 3 of this Article shall be married or unmarried spouse, partner in a life community of persons of same sex, their direct blood relative to any degree or a collateral blood relative to the fourth degree or a relative by marriage to the second degree, adopter, adoptee, foster parent or foster child.

Close associate of the person from paragraphs 2 and 3 of this Article shall be:

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

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

A person from paragraphs 2,3 and 4 of this Article shall be the politically exposed person even in the period of two years after termination of performing a public office.

After expiring the deadline from paragraph 8 of this Article, the reporting entity shall implement measures of establishing and monitoring business operation of the customer according to the risk analysis and to establish if there is still, in relation to that person, a high risk of money laundering and terrorism 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 shall have financial intelligence unit, reporting entities and supervisory authorities from Article 131, paragraph 1 of this Law.

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

The 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 defined by the Agency for Prevention of Corruption.

Application of Enhanced CDD measures on a customer or its beneficial owner who is a politically exposed person

Article 56

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

1) take adequate measures and establish the origin of the property and funds which are included in business relationship or transactions with that customer;
2) obtain written consent of a senior manager for establishing business relationship with that customer before establishing business relationship, and if business relationship has already been established, to obtain written consent of the senior management for continuation of business relationship,
3) establish whether that customer is the beneficial owner of the legal person, business organization, trust and other person or foreign entity equal to it i.e. natural person with head office situated in other country on whose behalf the business relationship is established, transaction carried out or other customer's activity conducted.
4) after establishing business relationship, monitor, with special attention, transactions and other business activities which politically exposed person performs at the reporting entity, or the customer whose beneficial owner is politically exposed person.

A reporting entity shall, pursuant to guidelines from Article 12, paragraph 5 of this Law, through internal regulation define procedures which are based on risk analysis that he/she implements with reference to identification of a customer who is a politically exposed person or through identifying beneficial owner of a customer who is a politically exposed person, as and also 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 a customer, in addition to measures from Article 17 of this Law, the reporting entity shall:

1) take adequate measures and establish the origin of property and funds which are included in business relationship or transaction with that customer;
2) obtain written consent of a senior manager for establishing business relationship with that customer before establishing business relationship and if business relationship has already been established, to obtain written consent of a senior manager for continuation of business relationship,
3) establish whether the customer concludes the agreement on performing custody services on his/her behalf and on his/her own account or it is a sub-custody (credit institution or other legal person 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 a reporting entity);
4) when carrying out every transaction, in case of sub-custody, establish on whose account the sub-custody made transaction.

Enhanced CDD measures in complex and unusual transactions

Article 58

In case of transactions that are complex and unusually large, as well as transactions carried out in unusual manner or which have no apparent economic or lawful purpose or deviate from usual or expected customer's business, and for which it was not possible to assess whether they are suspicious transactions, in addition to measures from Article 17 of this Law, the reporting entity shall:

1) collect and verify additional data on customer's business activity, as well as identification data on the customer and beneficial owner,
2) collect and to verify additional data on the nature of business relationship and motive and purposed of announced or executed transaction,
3) collect and verify additional data on the status of client's property, origin of the property and funds which are included in business relationship or transaction with that customer;
4) collect information on the origin of money and origin of customer's property and beneficial owner or beneficial owners,
5) collect information on reasons for planned or executed transactions,
6) analyze data from items 2 and 3 of this paragraph and to put the results of analysis in written form, stating clear conclusions that imply such transaction.

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

A reporting entity shall establish, by internal regulation, the criteria for recognizing transactions from paragraph 1 of this Article.

Enhanced CDD measures for the customers from high-risk third country
Article 59

In case of establishing business relationship 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 from Article 17 of this Law, the reporting entity shall t:

1) take measures from Article 58, paragraph 1 of this Law,
2) before establishing business relationship, obtain written consent of a senior management.

After establishing business relationship with customer from high-risk third country, the reporting entity shall apply enhanced CDD measures -enhanced monitoring of business relationship and transactions which that customer performs whereby he/she shall:

- increase the number and frequency of performed controls and choose the manners for carrying out transactions which need to be further examined;
- provide more frequent reporting of compliance officer for prevention of money laundering and terrorism financing on transactions;
- limit business relationships or transactions with customers from countries from the list from Article 60 of this Law.

A reporting entity shall implement measures from paragraphs 1 and 2 of this Article in accordance with risk assessment of money laundering and terrorism financing, which is established in the risk analysis.

List of high-risk third countries

Article 60

Financial intelligence unit shall publish the list of high-risk countries on its website.

Simplified CDD measures and monitoring of customer's business activities

Article 61

If in the cases from in Article 18 paragraph 1 items 1, 2, 3 and 6 of this Law, in relation to a customer, a group of customers, a country or geographical area, business relationship, transaction, product, service and channel of distribution, the lower risk of money laundering and terrorist financing is identified and if there are no reasons to suspect or no reasonable grounds to suspect that the money or other property derives from criminal activity or that money laundering or terrorist financing has been committed, and if the customer or its beneficial owner is not politically exposed person, a reporting entity may apply the simplified CDD measures, as follows:

1) verify the customer's identity and determine a beneficial owner after the establishment of the business relationship;
2) reduce the frequency of updating data on customer's identity;
3) reduce the volume of ongoing monitoring of transactions if the value of transaction does not exceed the amount for which the reporting entity, in the process of drafting of the risk analysis, has estimated that is appropriate to business activities and lower risk of money laundering and terrorist financing of the customer;
4) instead of gathering information thereof and conducting specific measures, draws conclusions on the purpose and intended nature of the business relationship according to the type of transaction or established business relationship.

If, after the establishment of the business relationship with a customer by applying the simplified CDD measures, there appear reasons to suspect or reasonable grounds to suspect that the property derives from the criminal activity or it is money laundering or terrorist financing, a reporting entity shall submit to the Financial Intelligence Unit data from Article 66 paragraphs 6 and 10 of this Article and implement measures from Article 17 of this Law.

A reporting entity shall also implement CDD measures, in the volume set in accordance with paragraph 1 item 3 of this Article, onto a customer in relation to which it identifies the existence of the lower risk of money laundering and terrorist financing.

7. Implementation of measures for the prevention and detection of money laundering and terrorist financing in business units and business organisations majority owned by reporting entities in another country

Obligation to implement measures for the prevention and detection of money laundering and terrorist financing in business units and business organisations majority owned by reporting entities in another country

Article 62

A reporting entity shall ensure that the measures for the prevention and detection of money laundering and terrorist financing, defined by this Law, are implemented in the same volume in business units or business organisations majority owned by a reporting entity with head office in another country which is a Member State or in the country that has the same standards for the

implementation of measures for the prevention and detection of money laundering and terrorist financing as the standards defined by this Law or the European Union legislation.

If the regulations of another country stipulates standards for the implementation of measures for the prevention and detection of money laundering and terrorist financing that are the same as or higher than the standards defined by this Law, a reporting entity shall ensure that their business units or business organisations majority owned by the reporting entity adopt and implement the appropriate measures in accordance with the regulations of that country including data protection measures.

If the regulations of another country stipulates standards for the implementation of measures for the prevention and detection of money laundering and terrorist financing lower than the standards defined by the Law or where the measures for the prevention and detection of money laundering and terrorist financing are conducted in lower volume that the volume defined by this Law, a reporting entity shall ensure that their business units or business organisations majority owned by the reporting entity implement measures for the prevention and detection of money laundering and terrorist financing in accordance with this Law, including data protection measures, to the extent that the respective country's regulations so allows.

If the regulations of another country prohibit the implementation of measures from paragraph 3 of this Article, a reporting entity shall immediately notify the Financial Intelligence Unit and the competent supervisory authority from Article 131 paragraph 1 of this Law thereof and take other appropriate measures to mitigate and effectively manage risk of money laundering and terrorist financing, to the extent that the respective country's regulations so allows.

If the competent supervisory authority from Article 131 paragraph 1 of this Law assesses that the measures from paragraph 4 of this Article are not sufficient, it shall order the reporting entity to implement also the following measures in another country:

1) prohibit the establishment of a business relationships;

2) terminate business relationships;

3) prohibit the execution of the transactions; or

4) terminate, where necessary and possible, the activities in business units or business organisations majority owned by the reporting entity in another country.

The reporting entity from paragraph 1 of this Article, that is member of a financial group, may, for the purpose of prevention of money laundering and terrorist financing, exchange data and information on the customer and/or transaction obtained in accordance with this Law with other members of the financial group in Montenegro, EU Member States and countries that have the same or higher standards for the implementation of measures for the prevention and detection of money laundering and terrorist financing than the standards defined by this Law or the European Union legislation, whereat it shall ensure appropriate protection of data confidentiality in accordance with the laws governing the data confidentiality and personal data protection.

A reporting entity from paragraph 1 of this Article which is a member of the financial group may exchange data and information on the customer and/or transaction obtained in accordance with this Law with other members of the financial group in Montenegro, European Union Member States and countries that have the same or higher standards for the implementation of measures for the prevention and detection of money laundering and terrorist financing than the standards defined by this Law or the European Union legislation also in the case that the Financial Intelligence Unit has been reported that there are reasons to suspect or reasonable grounds to suspect that funds or other property represent property gains acquired by criminal activity or are subject to money laundering or intended for terrorist financing, unless the Financial Intelligence Unit Limits or prohibits the exchange of data and information.

8. Prohibitions and restrictions in operations

Prohibition to provide services enabling concealment of customer's identity

Article 63

A reporting entity shall not open or keep an anonymous account for the customer, anonymous safe deposit box, passbook or securities accounts under a code or bearer shares or provide other service or product which, directly or indirectly, enables the concealment of the customer's identity.

Prohibition of shell bank activities

Article 64

A reporting entity shall not operate as a shell bank.

A reporting entity shall not establish or maintain a correspondent relationship with a credit institution that operates or might operate as a shell bank or with other credit institution that is known to allow its accounts to be used by a shell bank.

Restriction in cash transactions

Article 65

Legal persons, business organisations, entrepreneurs and natural persons performing the business activity shall not receive payment or make payments in cash in the amount of EUR 10,000 or more.

The restriction from paragraph 1 of this Article shall also be applied in the event if the payment or transaction is carried out in two or more linked transactions, in total amount of EUR 10,000 or more.

The payment in the amount defined in paragraphs 1 and 2 of this Article shall be executed through payment or transfer of funds to the transaction account opened with a credit institution.

The requirements from paragraphs 1, 2 and 3 of this Article shall not apply on credit institutions and other payment service providers.

9. Reporting obligations

Reporting to the Financial-intelligence unit

Article 66

A reporting entity shall submit accurate and complete data to the Financial Intelligence unit on CDD measures from Article 117 paragraphs 1 to 6 of this Law for each cash transaction in the amount of EUR 15,000 or more or cashless transaction in the amount of EUR 100,000 or more, without delay, no later than within three business days following the day the transaction has been executed.

Notwithstanding paragraph 1 of this Article, a reporting entity from Article 4 paragraph 2 item 13 indents 5, 10, 11, 12 and 13 of this Law shall submit to the Financial Intelligence Unit accurate and complete data obtained through implementation of CDD measures from Article 117

paragraphs 1 to 6 of this Law for each cash transaction in the amount of EUR 10,000 or more, without delay, no later than within three working days since the day of execution of the transaction.

A reporting entity shall submit shall submit to the Financial Intelligence Unit accurate and complete data obtained through implementation of CDD measures from Article 117 paragraphs 1 to 6 of this Law for each transaction in the amount of EUR 10,000 or more, which is executed on the accounts of legal and natural persons in high-risk third countries and if such transaction includes high-risk third country, without delay, no later than within three working days since the day of execution of the transaction.

A reporting entity from Article 4 paragraph 4 of this Law shall submit to the Financial Intelligence Unit accurate and complete data obtained through implementation of CDD measures from Article 117 paragraphs 1 to 6 of this Law for each transaction based on preliminary contract, the real estate agreement in the amount of EUR 15,000 or more, and based on the loan agreement in the amount of EUR 10,000 or more, without delay, no later than within three working days since the day of conclusion of that legal affair.

In addition to data from paragraph 4 of this Article, the reporting entity from Article 4 paragraph 4 of this Law shall also submit to the Financial Intelligence Unit a photocopy of the agreement in electronic form, and in the case of contracts where cash is used, a photocopy of the statement of the natural person ,who is a buyer, on the origin of that money.

A reporting entity shall refrain from executing the suspicious transaction, regardless to the amount, until the order from Article 93 of Law is passed, and it shall inform, without delay, the Financial Intelligence Unit thereof and submit data obtained through implementation of CDD measures from Article 117 paragraphs 1 to 6 and paragraph 8 of this Law.

A reporting entity shall submit the data from paragraph 6 of this Article to the Financial-intelligence unit prior to the execution of transactions and specify the time limit for the execution of transactions.

If the reporting entity, due to the nature of transactions and other justified reasons, is not able to act in accordance with paragraph 6 of this Law, it shall submit to the Financial Intelligence Unit the accurate and complete data obtained through implementation of CDD measures from Article 117 paragraphs 1 to 6 and paragraph 8 of this Article, without delay, no later than the next business day since the day of execution of the transaction.

The reporting entity shall, when submitting data in the manner from paragraph 8 of this Article, submit an explanation that contains reasons why it did not act in accordance with paragraph 6 of this Article.

The reporting entity shall submit to the Financial Intelligence Unit, without delay, accurate and complete data obtained through implementation of CDD measures from Article 117 paragraphs 1 to 6 and paragraph 8 of this Law in relation to funds or other property for which it knows or has reasons to suspect that represent property gains acquired by criminal activity or that are connected with money laundering or terrorist financing.

If a customer requests and advice in relation to money laundering or terrorist financing, the reporting entity shall notify, without delay, the Financial Intelligence Unit thereof.

The reporting entity shall notify the Financial Intelligence Unit, on any acess to data, information and documents that the supervisory authority from Article 131 paragraph 1 of this Article examined with the reporting entity, no later than three working days since the day when the access is provided.

The reporting entity shall submit to the Financial Intelligence Unit data from paragraphs 1 to 6 and paragraph 10 of this Article, the explanation from paragraph 9 of this Article and the

notifications from paragraphs 11 and 12 of this Article in electronic form, and it shall sign those data, reasoned explanation and notifications by eligible electronic signature in accordance with the law regulating electronic identification and electronic signature.

The reporting entity may also provide data from paragraphs 6 and 10 of this Article to the Financial-intelligence unit verbally, via telephone or in any other available manner, but it shall submit those data in accordance with paragraph 13 of this Article, no later than next working day since the day the data are provided verbally.

The manner and conditions of providing the data from paragraphs 1 to 6 and paragraph 10 of this Article, the explanations from paragraph 9 of this Article and notifications from paragraphs 11 and 12 of this Article shall be defined by the Ministry**.**

Exemptions from reporting obligation

Article 67

By way of exception from Article 66 paragraph 6 of this Law, a reporting entity from Article 4 paragraph 3 of this Law shall not be required to submit to the Financial Intelligence Unit data on customer and case files in the proceedings of providing legal assistance and representing the customer before the competent authority.

Feedback to the reporting entity

Article 68

The Financial Intelligence Unit shall, based on data or notifications submitted pursuant to Article 6, paragraphs 6, 10 and 11 of this Law, conduct the financial analysis in relation to persons, transactions or property, and it shall notify the reporting entity of the results of that analysis and on whether there are still reasons to suspect or reasonable grounds to suspect of money laundering and terrorist financing in relation to that person, transaction or property or whether that transaction or property present gains acquired by criminal activity.

Notwithstanding paragraph 1 of this Article, the Financial Intelligence Unit shall not notify the reporting entity on the results of analysis and on the existence of reasons for suspicion or reasonable grounds for suspicion from paragraph 1 of this Article, if it assesses that such notification may result in harmful consequences on the course and outcome of the procedure.

If the Financial Intelligence Unit establishes that there are reasonable grounds to suspect that the transaction or property represent property gains acquired by criminal activity or that money laundering or terrorist financing has been commited, it may provide, in the explanation from paragraph 1 of this Article, the reporting entity with a recommendation to terminate a business relationship with the customer or to decline the execution of transactions.

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

Designation of compliance officer for prevention of money laundering and terrorist financing and his deputy

Article 69

A reporting entity shall, within 60 days since the day of its establishment or day when it started to conduct business operations, designate a compliance officer for the prevention of money laundering and terrorist financing and at least one of his deputies and submit to the Financial-Intelligence Unit, within three days since the day of their designation, a notification containing the information on those persons (name and surname, unique personal identification number, number and date of expiry of personal identification document and issuing country; number and date of expiry of residence permit for an alien; title of working position and contact phone number) as well as the name and surname, Tax Identification Number (TIN) and address of the head office of the reporting entity.

A reporting entity shall notify the Financial Intelligence Unit on the change of compliance officer for the prevention of money laundering and terrorist financing or his deputy within three days since the day when the change is performed.

The notification from paragraph 2 of this Article shall contain explanation with reasons for execution of the change and information from paragraph 1 of this Article.

By way of exception , the reporting entity that has four or less employees is not obliged to designate the deputy of the compliance officer for prevention of money laundering and terrorist financing.

At the reporting entity that has less than four or less employees the affairs of compliance officer for the prevention of money laundering and terrorist financing may be performed by the director if he meets the conditions from Article 70 of this Law.

When the director performs the tasks of the compliance officer for prevention of money laundering and terrorist financing, the reporting entity shall notify the Financial Intelligence Unit thereof and in that notification provide the information on director pursuant to paragraph 1 of this Article.

The notifications from paragraphs 1, 2 and 6 of this Article shall be submitted to the Financial Intelligence Unit in electronic form and shall be signed by eligible electronic signature in accordance with the law regulating electronic identification and electronic signature.

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

Article 70

As a compliance officer for the prevention of money laundering and terrorist financing and his deputy, may be designated a person that :

1) completed the training for performing tasks of compliance officer for the prevention of money laundering and terrorist financing (hereinafter: the training) and who has passed the professional exam for performing tasks of compliance officer for the prevention of money laundering and terrorist financing (hereinafter: the professional exam),
2) has a license for performing tasks of compliance officer for the prevention of money laundering and terrorist financing, and
3) has not been convicted by a final court decision for a criminal offence for which an imprisonment longer than six months is prescribed.

One person may be designated as compliance officer for the prevention of money laundering and terrorist financing or his deputy only at one reporting entity.

Notwithstanding from paragraph 2 of this Article, when a director performs tasks of the compliance officer for the prevention of money laundering and terrorist financing in accordance with Article 69 paragraph 5 of this Law, he may be designated as compliance officer for the prevention of money laundering and terrorist financing to more reporting entities where he is both the director and 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 the regulations governing education of adults.

The training shall be delivered due to the curriculum in accordance with the regulations governing education of adults.

After completed training, a candidate shall be taken the professional exam before the professional exam commission which shall be formed by the Head of the Financial Intelligence Unit.

The Financial Intelligence Unit shall issue a certificate on passed professional exam.

The chairperson and members of the committee from paragraph 3 of this Article shall be entitled to a monthly compensation in the amount of 25% of average gross salary in Montenegro from the previous year based on data of the administration authority competent for the statistical affairs, which is paid in net amount.

If a person that is already employed with the reporting entity takes professional exam, the costs of passing the professional exam shall be borne by the reporting entity.

The programme and the method of passing the professional exam, the costs of professional exam, the composition of the commission, and the format of the certificate from paragraph 4 of this Article shall be prescribed by the Ministry.

License for performing tasks of compliance officer for prevention of money laundering and terrorist financing
Article 72

The license for performing tasks of compliance officer for the prevention of money laundering and terrorist financing (hereinafter: the license) shall be issued by the Financial Intelligence Unit.

The license shall be issued to a person who:

1) has permanent residence or approved temporary residence in Montenegro,
2) has not been convicted by a final court decision for a criminal offence prosecuted ex officio and for which an imprisonment longer than six months is prescribed, and
3) has completed training and who has passed the professional exam.

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

The application for issuing the license shall be submitted to the Financial Intelligence Unit.

The application for renewal of the license shall be submitted to the Financial Intelligence Unit no later than 30 days prior to expiry date.

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) at the request of the license holder,
2) upon the expiration of period of the issuance,
3) if a person to whom the license is issued has been convicted by final court decision for a criminal offence prosecuted ex officio and for which an imprisonment longer than six months is prescribed,
4) if a person to whom the license is issued, becomes permanently incompetent for performing tasks of compliance officer for the prevention of money laundering and terrorist financing or his deputy or if the person lost the ability to work,
5) by acquiring pension rights of the person to whom the license has been issued, or
6) in case of negligent business performance.

Negligent performance of tasks

Article 74

The compliance officer for the prevention of money laundering and terrorist financing or his deputy shall be deemed to have performed their tasks by negligence in terms of Article 73 paragraph 1 item 6 of this Law, if they, without justified reason:

1) fail to provide data and information pursuant to Article 66 of this Law, more than four times within a period of two years,
2) fail to submit data and information in a timely manner in accordance with Article 66 of this Law, more than six times within a period of two years,
3) fail to comply or fail to comply in a timely manner in accordance with Articles 93 and 95 of this Law, more than two times within a period of two years.

The Financial Intelligence Unit shall establish the existence of circumstances from paragraph 1 of this Article on the basis of the report of the competent supervisory authority from Article 131 paragraph 1 of this Law, based on the request from Article 131 paragraph 8 of this Law.

Administrative decision on expiry of a license

Article 75

The Financial-Intelligence Unit shall pass an administrative decision on the expiry of the license.

An administrative dispute may be initiated against the administrative decision from paragraph 1 of this Article.

The Financial-Intelligence Unit shall notify, without delay, the reporting entity on the expiry of the license of the person whose license has been revoked and who has been designated as the compliance officer for the prevention of money laundering and terrorist financing or his deputy.

In the case of the expiry of the license, the reporting entity shall, within 15 days since the day of the adoption of the administrative decision, designate another compliance officer for the prevention of money laundering and terrorist financing or this deputy.

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

Article 76

A compliance officer for the prevention of money laundering and terrorist financing or his deputy shall perform the following tasks:

1) ensure that the the system for the prevention of money laundering and terrorist financing; is established, operational and further developed;
2) ensure proper and timely data delivery to the Financial Intelligence Unit and cooperate with the competent inspection authority in the process of inspection supervision;
3) draft and regularly update the risk analysis in accordance with the guidelines from Article 12 paragraph 5 of this Law;
4) monitor implementation of policies, controls and procedures for the prevention of money laundering and terrorist financing;
5) initiate and participate in drafting and amending the operational procedures and preparation of reporting entity's internal regulations that refer to the prevention of money laundering and terrorist financing;
6) participate in drafting the internal regulations related to the prevention of money laundering and terrorist financing;
7) monitor and coordinate the compliance of the reporting entity's business activities with this Law;
8) cooperate in establishing and developing information technology which will be used for the prevention and detection of money laundering and terrorist financing;
9) introduce initiatives and proposals to the administrative or managing or other body of a reporting entity for improving the system for the prevention of money laundering and terrorist financing;
10) ensure implementation of Article 16 of this Law in the process of introducing new products, services or channels of distribution at the reporting entity,
11) prepare professional training programmes and development of employees at the reporting entity in the area of the prevention and detection of money laundering and terrorist financing,
12) prepare report in the area of the prevention of money laundering and terrorist financing at the reporting entity once a year, and more frequently, if necessary, and when required by the competent supervisory authority from Article 131 paragraph 1 of this Law.

A reporting entity shall submit the report from paragraph 1 item 12 of this Article to the competent supervisory authority from Article 131 paragraph 1 of this Law at the request of the competent supervisory authority within three days since the day when the request is received.

A compliance officer for the prevention of money laundering and terrorist financing or his deputy shall be directly responsible to management body or executive or other similar body of the reporting entity.

If the reporting entity is a large or a medium-sized legal person within the meaning of the law regulating the accounting, the compliance officer for the prevention of money laundering and terrorist financing or his deputy shall be functionally and organisationally separated from other organisational parts of the reporting entity.

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

Article 77

A reporting entity shall provide the compliance officer for the prevention of money laundering and terrorist financing, particularly with the following:

1) conditions for efficient performance of tasks from Article 76 paragraph 1 of this Article;

2) functional connection with other organisational parts of the reporting entity in the manner that enable the compliance officer to efficiently, in good quality and timely manner perform tasks from Article 76 paragraph 1 of this Law;
3) adequate material working conditions;
4) appropriate spatial and technical conditions which provide appropriate level of protection of confidential data and available information, pursuant to this Law,
5) adequate information and technical support which enables ongoing and reliable monitoring of activities in the area of the prevention of money laundering and terrorist financing;
6) regular professional training with related to the prevention and detection of money laundering and terrorist financing;
7) replacement during the absence from work.

Management body of the reporting entity shall provide the compliance officer for the prevention of money laundering and terrorist financing with the assistance and support in performing tasks from Article 76 paragraph 1 of this Law and it shall inform him/her on the facts that are important for the prevention and detection of money laundering and terrorist financing.

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

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

Professional training and development

Article 78

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

The professional training and development from paragraph 1 of this Article means introducing the employees with this Law and regulations adopted on the basis of this Law, internal regulations of the reporting entity in the field of the prevention and detection of money laundering and terrorist financing, professional literature on the prevention and detection of money laundering and terrorist financing, the list of indicators from Article 82 and 83 of this Law, and legislation regulating international restrictive measures, legislation regulating personal data protection and legislation regulating data secrecy.

A reporting entity shall prepare, by the end of first quarter of the current year, professional training and development programme from paragraph 1 of this Article, for that year.

The method of professional training and development of employees shall be defined by internal regulation of the reporting entity.

Rules for performing tasks of the prevention and detection of money laundering and terrorist financing

Article 79

A reporting entity shall determine and implement relevant rules for dealing with customer and it shall ensure reporting, keeping of data, internal control, risk assessment, risk management and communication for the purpose of prevention and detection of money laundering and terrorist financing.

A reporting entity shall determine and ensure the implementation of relevant rules that guarantee adequate exchange of information between employees for the purpose of efficient implementation of obligations prescribed by this Law.

A reporting entity shall order and control the implementation of the rules from paragraphs 1 and 2 of this Article in business units and business organisations majority owned by the reporting entity with head office in other countries.

Internal controls and audit

Article 80

A reporting entity shall ensure regular internal control and audit of the implementation of policies, controls and procedures for the prevention of money laundering and terrorist financing or performing tasks of the prevention and detection of money laundering and terrorism financing in accordance with the identified risk of money laundering and terrorist financing in the risk analysis.

If the law regulating business activity of the reporting entity prescribes the obligation of the existence of independent internal audit, the reporting entity shall also organise an independent internal audit within whose scope is regular assessment of adequacy, reliability and effectiveness of risk management system of money laundering and terrorist financing.

A reporting entity shall also organise an independent internal audit within whose scope of work are regular assessments of the adequacy, reliability and effectiveness of risk management system of money laundering and terrorist financing and when it asess that it is necessary due to the nature and scope of the business activity.

Internal control and audit from paragraphs 1, 2 and 3 of this Article shall be carried out in the manner to prevent, detect and correct errors made in the process of implementation of regulations in the area of the prevention of money laundering and terrorist financing and to improve reporting entity's policies, controls and procedures for the detection of transactions and persons related to money laundering and terrorist financing.

The manner of carrying out the internal control and audit from paragraphs 1, 2 and 3 of this Article shall be prescribed by the internal regulation of the reporting entity.

IV. LIST OF INDICATORS FOR RECOGNISING SUSPICIOUS CUSTOMERS AND TRANSACTIONS

Obligation of applying the list of indicators

Article 81

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

List of indicators for recognising suspicious customers and transactions

Article 82

The list of indicators for recognising suspicious customers and transactions shall be prescribed by the Ministry.

The Financial Intelligence Unit shall prepare the professional basis for drafting the list of indicators from paragraph 1 of this Article in cooperation with other competent authorities from Article 131 paragraph 1 of this Law.

Reporting entity's list of indicators for recognising suspicious customers and transactions

Article 83

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

The list of indicators from paragraph 1 of this Article must be stored in the documentation of a reporting entity.

V.AFFAIRS, POWERS, MANNER OF WORK NAD INFORMATION SYSTEM OF THE FINANCIAL INTELLIGENCE UNIT

Independence and autonomy in performing affairs and exercising of powers

Article 84

The Financial Intelligence Unit is a central national unit responsible for the prevention and detection of money laundering and terrorist financing, in accordance with the law.

The Financial Intelligence Unit is operationally independent and autonomous in exercising powers prescribed by Law and independent in decision making process related to the reception, collection, keeping, analysing and providing data, notifications, information and documentation and submitting results of the strategic and operational analyses of the suspicious transactions to the competent authorities, foreign financial intelligence units and international organisations.

The affairs or powers from paragraph 2 of this Article shall be performed or exercised by the employees of the Financial Intelligence Unit.

The Financial Intelligence Unit shall submit, at least once a year, a report on its work and the situation in the area of the prevention of money laundering and terrorist financing to the Government.

Head of the Financial Intelligence Unit

Article 85

A person with the rank of Deputy Director of Police Directorate and a person that meets the requirements for Deputy Director of Police Directorate shall 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 may not be at the same time the head of another organisational unit in Police.

The Head of the Financial intelligence unit, on the basis of the 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 of the Financial Intelligence Unit to the Parliament of Montenegro, in order to provide an opinion.

The Parliament of Montenegro provides the opinion from paragraph 4 of this Article upon the proposal of the competent board.

Establishment of an employment and terms for employment

Entering employment and terms for employment

Article 86

The Head of Financial Intelligence Unit shall participate in the procedure of selecting candidates for entering employment in the financial intelligence unit, which is conducted in accordance with the regulations on civil servants and state employees and the law regulating the internal affairs.

Employees of the financial intelligence unit shall meet the conditions prescribed by the law regulating the internal affairs and act on internal organisation and systematization of working positions job position 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.

An employee of the Financial Intelligence Unit may not be reassigned to other work position or tasked to perform other duties in the Police or 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 budget planning and execution and fiscal responsibility.

The funds allocated to financial intelligence unit for its work by the donations or otherwise shall be independently disposed of by the Head of the Financial Intelligence Unit.

The Head of the Financial Intelligence Unit shall, within the funds from paragraph 1 of this Article, make decisions independently on the conducting the public procurements and simple procurements as an authorised person of the ordering party in accordance with the law regulating the public procurements.

Material and technical assets of the financial intelligence unit

Article 88

Information system, means of communication, vehicles and other equipment for the work of the Financial Intelligence Unit shall only be used by the employees of the Financial Intelligence Unit.

Information system, means of communication, vehicles and other equipment from paragraph 1 of this Article may not be provided for use to another organisational unit of the Ministry or the Police, without written consent of the Head of the Financial Intelligence Unit.

The manner of disposal and use of the informational system, means of communication, vehicles and other equipment from paragraph 1 of this Article, and the premises used by the Financial Intelligence Unit shall be regulated by the Head of Financial Intelligence Unit by the internal regulation.

The regulation from paragraph 3 of this Article shall be designated an appropriate level of confidentiality in accordance with the law regulating the data secrecy.

Affairs or powers of the financial intelligence unit

Article 89

Financial Intelligence Unit shall be empowered to:

1) collect, process and analyse data on natural and legal persons, their property, suspicious, cash and other transactions, suspicious and other business activities, bank accounts and safe deposit boxes, make and deliver financial analyses and other information in accordance with this Law;

2) receive from the reporting entities, competent authorities from article 96 paragraph 1 of this Law, supervisory authorities from Article 131 paragraph 1 of this Law, other legal and natural persons, foreign financial intelligence units and authorities from other countries or international organisations responsible for the prevention of money laundering and the detection of money laundering and terrorist financing or authorities of another country responsible for confiscation of assets, as well as information and data on the persons and property for which there are reasons to suspect suspicion or reasonable grounds for suspicion of money laundering and associated predicate offences and terrorist financing or that the property derives from criminal activity, which it may process and use for the purpose specified in this Law;

3) order the reporting entity to temporarily suspend a transaction and conduct ongoing monitoring of the financial activities of the customer;

4) start initiatives for amending and supplementing regulations related to the prevention of money laundering and terrorist financing;

5) conclude agreements on cooperation or establish independent cooperation when exchanging information with competent authorities from Article 96 paragraph 1 of this Law and supervisory authorities from Article 131 paragraph 1 of this Law, and foreign financial intelligence units, competent authorities in other countries and international organisations;

6) manage the information system of the Financial Intelligence Unit;

7) participate in professional education and training of compliance officers for the prevention of money laundering and terrorist financing and his deputies;

8) give recommendations, or guidelines for unified implementation of this Law and regulations adopted on the basis of this Law;

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

10) at least once a year, publish a report that includes statistical data, trends and typologies in the area of money laundering and terrorist financing, and in particular 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, as well as data on the property that has

been frozen seized or confiscated, and to notify the public, in other appropriate manner, on the forms of money laundering and terrorist financing;

11) perform other activities in accordance with the law.

The Head of The Financial Intelligence Unit shall define in the more detailed manner of performing the affairs and exercising powers from paragraph 1 of this Article by an internal regulation.

The internal regulation from paragraph 2 of this Article shall be designated with appropriate level of confidentiality in accordance with the law regulating data confidentiality.

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

Article 90

If the Financial Intelligence Unit assesses that there are reasons for suspicion or reasonable grounds for suspicion that funds or other property of a specific customer derive from criminal activity or that money laundering has been committed , and associated predicate offences or that they are associated with terrorist financing, it may request from the reporting entity to provide data, information and documentation:

1) from Article 117 paragraphs 1 to 11 of this Law;

2) on the balance of funds and other property of that reporting entity's costumer;

3) on the turnover of funds and property of that reporting entity's costumer;

4) on business relationships established with that customer;

5) which it has obtained in accordance with this Law, documentation and data regarding the performance of activities in accordance with this Law, as well as other data necessary for monitoring the execution of obligations set out in this Law.

The Financial Intelligence Unit shall, in the request from paragraph 1 of this Article, specify the legal basis for collecting data, the data to be provided, the purpose of collection and the time limit for their provision.

The Financial Intelligence Unit may also request the provision of data, information and documentation from paragraph 1 of this Article also for the persons for which it can be concluded to have cooperated, or participated in the transactions or activities of persons for which there are reasons for suspicion or reasonable grounds to suspect that the funds or property in their possession, which they dispose of or manage, derive from criminal activity or money laundering, associated predicate offences or that they are associated with terrorist financing.

The reporting entity shall, upon the request from paragraphs 1 and 3 of this Article, provide accurate and complete data, information and documentation at its disposal, without delay, and no later than within eight days following the receipt of the request.

If the request from paragraphs 1 and 3 of this Article is designated as URGENT, the reporting entity shall provide data, information and documentation to the financial intelligence unit without delay, and no later than 24 hours since reception of such request.

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

The reporting entities shall provide data, information or documentation from paragraph 1 of this Article to the Financial Intelligence Unit in the manner prescribed by the regulation from Article 66 paragraph 15 of this Law.

Provision of data, information and documentation from paragraph 1 of this Article shall be done without compensation.

Request to persons that are not reporting entities to provide data, information and documentation

Article 91

Exceptionally, if the Financial Intelligence Unit assesses that there are reasons for suspicion or reasonable grounds that the funds or other property derived from criminal activity or that money laundering or associated predicate offences have been committed , or that funds or other property are associated with terrorist financing, it may request from entities from Article 43 paragraph 3 of this Law, as well as natural persons that are not reporting entities within the meaning of this Law, make available or provide data, information and documentation at their disposal, or provide notifications, in order to prevent and detect money laundering, associated predicate offences or terrorist financing, in particular the data:

1) on the property and legal income, as well as data on the connection between the income and the property;

2) on the property transferred to third parties or a legal successor, and the manner of acquiring and transferring the property;

3) on the user of the Internet Protocol address (IP address);

4) other data that are relevant for finding and establishing property obtained from criminal activity or for establishing the reasonable grounds to suspect that the criminal offence of money laundering or terrorist financing has been committed.

Entities or natural persons from paragraph 1 of this Article shall provide data, information and documentation to the Financial Intelligence Unit in the manner prescribed by the regulation from Article 66 paragraph 15 of this Law.

Provision of data, information and documentation from paragraph 1 of this Article to the Financial Intelligence Unit shall be done without compensation.

Request to a state authority, competent authority, supervisory authority or public powers holder to submit data on suspicious transactions or persons

Article 92

The competent authorities from Article 96 paragraph 1 of this Law, other state authorities, supervisory authorities from article 131 paragraph 1 of this Law and public power holders shall enable the financial intelligence unit with direct electronic access to all data, information and documentation that they keep in electronic form.

If it is not possible to obtain data, information and documentation in the manner from paragraph 1 of this Article, the authorities from paragraph 1 of this Article and public power holders shall, upon the request from the Financial Intelligence Unit, provide the data, information and

documentation, without delay, in the manner prescribed by the regulation from Article 66 paragraph 15 of this Law.

The Financial Intelligence Unit shall, in the request from paragraph 2 of this Article, state 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 a transaction and temporary prohibition of access to a safe deposit box

Article 93

The Financial Intelligence Unit may, by an order, require the reporting entity to suspend the execution of a transaction, and to prohibit the access to a safe deposit box, for no longer than 72 hours, where it assesses that there are reasons for suspicion or reasonable grounds to suspect that the funds or other property derive from criminal activity or money laundering, associated predicate offences or are intended for terrorist financing.

The Financial Intelligence Unit shall, without delay, and no later than within 24 hours, notify the competent authorities on the order from paragraph 1 of this Article in order to take measures from their competence.

If it acts in accordance with the notification from Article 66 paragraph 6 of this Law, the Financial Intelligence Unit shall issue the order from paragraph 1 of this Article within 24 hours following the receipt of the notification.

In the case that the last day of a deadline from paragraph 1 of this Article occurs on non-working days, that deadline may be extended for additional 48 hours by an order, provided that the total duration of the suspension of a transaction or prohibition of access to a deposit safe deposit box may not be longer than seven days.

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

The Financial Intelligence Unit shall provide the order ,from paragraphs 1 and 4 of this Article, to the reporting entity in electronic or written form.

Notwithstanding from paragraph 6 of this Article, due to urgency, or other circumstances related the execution of a transaction, the order from paragraphs 1 and 4 of this Article may be issued verbally, but then it shall be provided in electronic or written form no later than 24 hours since the verbal order is issued.

The compliance officer for the prevention of money laundering and terrorist financing shall make a note on the receipt of the verbal order from paragraph 1 and 4 of this Article.

Upon reception of the notification from paragraph 2 of this Article, the competent authorities shall act in accordance with their powers, without delay, and no later than within 72 hours following the temporary suspension of a transaction or temporary prohibition of access to a deposit safe box, and shall, in electronic or written form, without delay, notify the Financial Intelligence Unit thereof.

Termination of measure for temporary suspension of a transaction and temporary prohibition of access to a safe deposit box

Article 94

If the Financial Intelligence Unit after 72 hours from the suspension of transaction or prohibition of access to a safety deposit box fails to notify the reporting entity on further actions, the reporting entity may upon the expiry of that deadline execute the transaction or allow the access to the safe deposit box.

Request for ongoing monitoring of customer's financial business

Article 95

The Financial Intelligence Unit may request, in electronic or written form, from the reporting entity to conduct ongoing monitoring of the customer or another person for which it may be concluded that it has cooperated with, or participated in transactions or activities of that customer, if there are reasons for suspicion or reasonable grounds to suspect that the subject funds or other property derive from criminal activity or that money laundering has been committed, associated predicate offences or that they are intended for terrorist financing, and define a deadline within which the reporting entity shall notify and provide requested data thereof.

The reporting entity shall act in accordance with the request from paragraph 1 of this Article.

The reporting entity shall provide the data from paragraph 1 of this Article to the Financial Intelligence Unit before the execution of the transaction or conclusion of the business, and to specify in the notification the assessment of the deadline within which the transaction or business is to be executed.

If, due to the nature of the transaction, business or other justified reasons, the reporting entity is unable to act in accordance with paragraph 3 of this Article, it shall provide data from paragraph 1 of this Article to the Financial Intelligence Unit, without delay, and no later than the next working day from the day when the transaction is executed or business concluded.

When providing data in accordance with paragraph 4 of this Article, the reporting entity shall explain in detail the reasons due to which it failed to act in accordance with paragraph 3 of this Article.

Ongoing monitoring from paragraph 1 of this Article may not last longer than three months from the day of submission of the request from paragraph 1 of this Article.

Where necessary, the deadline from paragraph 6 of this Article may be extended up to a maximum of six months from the day of submission of the request from paragraph 1 of this Article.

Collection of data, information and documentation upon a request or information

Article 96

The Financial Intelligence Unit may, upon the elaborated request or on the basis of information provided by another organisational unit within the Ministry, or Police, administration body responsible for tax collection, administration body responsible for customs affairs, National Security Agency, Agency for Prevention of Corruption, State Prosecutor's Office, or court, initiate the procedure for collecting and analysing data, information and documentation, where in relation to a specific person, transaction or property, there are reasons for suspicion or reasonable grounds to suspect in money laundering, associated predicate offences or terrorist financing, or that the property derived from criminal activity.

The decision to act in accordance with the request or information from paragraph 1 of this Article shall be made by the Head of the Financial Intelligence Unit.

The financial intelligence unit may, upon the request or information from paragraph 1 of this Article, provide a reply containing information on bank accounts, safe deposit boxes, financial information, financial analyses, and/or results of operational analyses obtained on the basis of data, information and documentation collected in accordance with paragraph 1 of this Article.

If there are objective reasons to assume that providing the reply from paragraph 3 of this Article would have an negative impact on the course or outcome of the investigation or analysis conducted by the Financial Intelligence Unit, or where the disclosure of information would evidently not be commesurate to the interests of the natural or legal person or would not be of importance given the purposes for which it was requested, the financial intelligence unit may refuse to provide the reply to the request from paragraph 1 of this Article.

The Financial Intelligence Unit shall elaborate the refusal to provide a reply to the request from paragraph 1 of this Article.

In the case of obtaining a reply from paragraph 3 of this Article, the competent authorities from paragraph 1 of this Article shall provide to the Financial Intelligence Unit the feedback on the use of delivered information, as well as to provide the outcome of investigation or supervision that they have conducted on the basis of such information.

Notifying the competent authorities upon the establishment of reasonable grounds to suspect that a criminal offence of money laundering or terrorist financing is committed or that the property derives from criminal activity

Article 97

If the financial intelligence unit, on the basis of data, information or documentation obtained in accordance with the law, assesses that in relation to a specific person, transaction, funds or other property there are reasonable grounds to suspect that criminal offence of money laundering or terrorist financing is committed or that the property derives from criminal activity, it shall, in written for, notify the competent authority thereof and provide necessary data, information and documentation.

If the Financial Intelligence Unit has acted in accordance with the notification from Article 66 paragraphs 6, 10, and 11 of this Law, it must not, in the notification from paragraph 1 of this Article, state that the notification was delivered by the reporting entity, neither provide data on the employee of the reporting entity that delivered the notification, nor submit the notification, unless there are reasonable grounds to suspect that this employee of the reporting entity committed the criminal offence of money laundering or terrorist financing or where these data are necessary for establishing the facts in criminal proceedings, and the provision of which is required by the competent court.

The competent authority from paragraph 1 of this Article shall provide to the Financial Intelligence Unit the feedback on the use of provided data, information and documentation from paragraph 1 of this Article, as well as the outcome of investigations, or supervision that it conducted on the basis of these data, information and documentation.

Notifying the competent authorities upon the establishment of the reasonable grounds to suspect that other criminal offence is committed

Article 98

If the Financial Intelligence Unit, on the basis of data, information and documentation obtained in accordance with this Law, assesses that in relation to a person, transaction, funds or other

property there are reasonable grounds to suspect that another criminal offence, prosecuted ex officio, is committed, it shall , in written form, notify the competent authority thereof and provide the necessary data, information and documentation that confirm those reasonable grounds to suspect, so that the competent authority may take measures within its competence.

If the Financial Intelligence Unit acted in accordance with the notification from Article 66 paragraphs 6, 10 and 11 of this Law, it must not, in the notification from paragraph 1 of this Article, state the data that the notification was provided by the reporting entity, neither provide data on the employee of the reporting entity that delivered the notification, nor submit the notification, unless there are reasonable grounds to suspect that this employee of the reporting entity committed the criminal offence of money laundering or terrorist financing or committed the criminal offence prosecuted ex- officio or if these data are necessary for establishing the facts in criminal proceedings, and the provision of which, in written form, is required by the competent court.

The competent authority from paragraph 1 of this Article shall provide to the Financial Intelligence Unit the feedback on the use of provided data, information and documentation from paragraph 1 of this Article, as well as the outcome of investigations, or supervision that it has conducted on the basis of these data, information and documentation.

Analysis of efficiency and effectiveness of the system for the prevention of money laundering and terrorist financing

Article 99

The Financial Intelligence Unit shall, at least once a year, conduct the analysis of the efficiency and effectiveness of the system for the prevention of money laundering and terrorist financing.

The analysis of the efficiency and effectiveness of the system for the prevention of money laundering and terrorist financing shall be conducted on the basis of a comprehensive report, which the Financial Intelligence Unit shall draft on the basis of:

- data from Articles 115 and 120 of this Law;
- data on the size of the reporting entity from Article 4 paragraph 2 of this Law, including the number of natural and legal persons and their economic importance;
- data on financial assets and personnel capacities allocated for suppression of money laundering and terrorist financing to the financial intelligence unit, competent authorities from Article 96 paragraph 1 of this Law and supervisory authorities from Article 131 paragraph 1 of this Law.

The analysis from paragraph 1 of this Article shall, in particular, include the analysis of:

- the risk of money laundering and terrorist financing on the national level;
- the efficiency and effectiveness of coordinated action of the Financial Intelligence Unit, supervisory authorities from Article 131 paragraph 1 of this Law, other competent authorities and reporting entities in the prevention of money laundering and terrorist financing;
- the quality of financial intelligence, information and documentation obtained through international cooperation and its adequacy for taking efficient action in relation to perpetrators of criminal offences and their property;
- the efficiency and effectiveness of the activity of supervisory authorities from Article 131 paragraph 1 of this Law in performing adequate supervision, monitoring and managing the activities of reporting entities, with the purpose to achieve compliance with the requirements of the prevention of money laundering and terrorist financing proportionally with the identified risks;

- the adequacy of the implementation of measures from Articles 17 and 52 of this Law and reporting suspicious transactions of reporting entities proportionally to the identified risks;
- the results achieved in the prevention of the misuse of legal persons for the purposes of money laundering or terrorist financing and the availability of information on their beneficial owners to the competent authorities;
- the efficiency and effectiveness of competent authorities' use of financial intelligence and other data for conducting investigations on money laundering and terrorist financing;
- the effectiveness of investigations of criminal offences of money laundering, associated predicate offences and terrorist financing, prosecuting the perpetrators of these criminal offences and sanctions imposed for these criminal offences;
- the property, income and funds that are seized or confiscated;
- terrorists, terrorist organisations and persons financing terrorism that are prevented in collecting, transferring and using the funds, as well as the misuse of the non-government sector for these purposes;
- natural and legal persons included in proliferation of weapons of mass destruction and the results achieved in the prevention of collecting, transferring and using the funds, in accordance with the United Nations Security Council Resolutions.

The Financial Intelligence Unit shall draft the report on the results of the analysis from paragraph 1 of this Article and submit it to the coordinating body from Article 8 of this Law.

Information system of the financial intelligence unit

Article 100

The financial intelligence unit shall, in performing the activities within its competence, in process of receiving, exchanging, processing, providing, and disclosing data, submissions, acts and other documents and other forms of communication with reporting entities, competent authorities, supervisory authorities, and competent authorities from other countries, as well as in communication between the officers from paragraph 3 of this Article, use the information system of the Financial Intelligence Unit, which represents integrated set of information and communication technologies necessary for the collection, recording, keeping, processing and transferring data, information and documentation in electronic form (hereinafter: FIU IS).

FIU IS shall be established and managed by the Financial Intelligence Unit.

Access to data, information and documents from paragraph 1 of this Article shall only be enabled to the officers of the Financial Intelligence Unit, unless it is otherwise specified in this Law.

Parts of the information system of the financial intelligence unit

Article 101

FIU IS shall comprise:

- the premises, or the space that shall meet the conditions for the accommodation and functioning of computer and communication equipment, in accordance with international standards (data center);
- the premises, or the space in which back-up computer systems and the supporting equipment shall be placed in order to ensure the business continuity and eliminate the possibility of data loss in case of incidents, which shall meet the conditions for the accommodation and

functioning of computer and communication equipment, in accordance with international standards (disaster recovery center);

- information and communication infrastructure which consists of a set of information and communication technologies necessary for the activities of the FIU IS;
- infrastructure systems which consists of systemically implemented computer programs
- -application systems which consists of computer programs tailored to business functions;
- internet systems which consists of computer programs tailored to providing services on the internet.

All parts of the FIU IS from paragraph 1 of this Article are integrated and operate as one functional system.

Managing and accessing FIU IS

Article 102

The Financial Intelligence Unit shall manage the FIU IS in accordance with international standards in the area of project, process and information security management, operational risk and business continuity management, and other types of management.

The Financial Intelligence Unit shall develop and improve the FIU IS in accordance with international standards in the area of information system development and improvement.

Access to FIU IS shall only be allowed to the officers of the Financial Intelligence Unit authorised for the management of the FIU IS.

Exceptionally from paragraph 3 of this Article, access to FIU IS shall also be allowed to professionals engaged in the activities of maintenance and improvement of the FIU IS, on condition that that they are not allowed to access data, information and documents in the FIU IS.

Professionals from paragraph 4 of this Article must not stay in the premises, or access the FIU IS without the presence of officers from paragraph 3 of this Article.

The manner of management and engagement of professionals from 4 of this Article in the activities of maintenance and improvement of the FIU IS, and other matters of importance for the functioning of the FIU IS shall be defined by an internal regulation passed by the head of the Financial Intelligence Unit.

The regulation from paragraph 6 of this Article shall be designated with appropriate level of confidentiality in accordance with the law regulating data confidentiality.

FIU IS audit

Article 103

The Financial Intelligence Unit shall perform the audit of the FIU IS at least once in two years.

The audit from paragraph 1 of this Article shall include the following verifications:

- functionality of all parts of the FIU IS;
- reliability of the FIU IS;
- security of the FIU IS;
- efficiency and effectiveness of the use of the FIU IS;
- compliance of the use of the FIU IS with the current regulation and international standards.

The results from paragraph 1 of this Article shall be delivered to the Head of the Financial Intelligence Unit, who shall, on the basis of that, adopt a plan of activities to improve and address deficiencies in the FIU IS.

The regulation from paragraph 3 of this Article shall be designated with appropriate level of confidentiality in accordance with the law regulating data confidentiality.

Electronic communication between the financial intelligence unit and other entities

Article 104

The financial intelligence unit shall, in electronic communication with the reporting entities, competent authorities from Article 96 paragraph 1 of this Law, supervisory authorities from Article 131 paragraph 1 of this Law, and competent authorities from other countries, use the unique official address for electronic communication of the financial intelligence unit, which shall be published on its website.

In the official electronic communication, the financial intelligence unit's officer shall use the unique official address for electronic communication of that officer.

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

A sub-domain shall be created under the domain of state administration bodies (foj.gov.me).

The manner of creating, changing and terminating unique official addresses for electronic communication of the Financial Intelligence Unit and its officers shall be defined by an internal regulation passed by the Head of the Financial Intelligence Unit.

VI. INTERNATIONAL COOPERATION

Establishing international cooperation

Article 105

In order to establish, achieve, and improve international cooperation, the Financial Intelligence Unit may conclude agreements with the authorised authorities of other countries and international organisations on the exchange of financial intelligence data, information on bank accounts and safe deposit boxes, financial information, financial analyses and other information and documentation, which may be used solely for the purpose and intentions specified in this Law, as well as on other issues of importance for the area of the prevention of money laundering and terrorist financing.

Request to the competent authority from another country to provide data, information and documentation

Article 106

The Financial Intelligence Unit may request from the competent authority from another country which, in that foreign country, performs activities related to the prevention of money laundering and terrorist financing and other issues of importance for the prevention of money laundering and terrorist financing (hereinafter: the foreign financial intelligence unit) to provide information on bank accounts and safe deposit boxes, financial information, financial analyses and other data, information and documentation on the persons, transactions and property of significance for the

prevention and detection of money laundering, associated predicate offences, criminal activity or terrorist financing.

The Financial Intelligence Unit may request from another authority from another country or from an international organisation that are responsible for the prevention and detection of money laundering and terrorist financing or from an authority from another country responsible for confiscation of property to provide data information and documentation from paragraph 1 of this Article.

The financial intelligence unit may, upon a request from the supervisory authority from in Article 131 paragraph 1 of this Law, request from the supervisory authority from another country to provide data, information and documentation from paragraph 1 of this Article.

The request from paragraphs 2 and 3 of this Article shall be provided through the foreign financial intelligence unit.

Exceptionally from paragraph 4 of this Article, if there are reasons of urgency, the Financial Intelligence Unit may provide the request from paragraph 2 of this Article to another authority of another country or to an international organisation responsible for the prevention and detection of money laundering and terrorist financing, or to an authority from another country responsible for the confiscation of property.

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

The Financial Intelligence Unit may use the data, information and documentation obtained in accordance with paragraphs 1, 2 and 3 of this Article solely for the purposes for which they were obtained, and it shall not, without prior consent of the foreign financial intelligence unit, other authority of another country or international organisation responsible for the prevention and detection of money laundering and terrorist financing, or an authority from another country responsible for the confiscation of property, use nor submit or make them available to another authority, legal or natural person, or use them for the purposes of administration, investigation or criminal prosecution, nor for other purposes that are not in accordance with the conditions and restrictions set by that authority or international organisation.

Providing data, information and documentation upon a request from an authority of another country

Article 107

The Financial Intelligence Unit may, upon a request containing the reasons for suspicion or reasonable grounds for suspicion of money laundering, associated predicate criminal offences or terrorist financing or that the property derived from criminal activity and sstating the purpose for which the data are being requested, provide to a foreign financial intelligence unit information on bank accounts, safe deposit boxes, financial information, financial analyses and other data, information and documentation on persons, transactions and property of significance for the prevention and detection of money laundering, associated predicate criminal offences, criminal activity or terrorist financing.

The financial intelligence unit may also provide data, information and documentation from paragraph 1 of this Article to other authorities from another country or to international organisations responsible for the prevention and detection of money laundering and terrorist

financing, to the authority of another country responsible for the confiscation of property, and to supervisory authorities of another country, upon their request.

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

Exceptionally from paragraph 3 of this Article, the financial intelligence unit may, upon the justified request from the European Union Agency for Law Enforcement Cooperation (hereinafter: the Europol), provide information on bank accounts, safe deposit boxes, financial information and financial analyses from paragraph 1 of this Article, through Europol's Secure Information Exchange Network Application in cases of prevention, detection and suppression of serious criminal offences that are within the competence of the Europol.

The Financial Intelligence unit may also respond to the request from a foreign financial intelligence unit in the cases where predicate criminal offence or criminal activity are not known at the time of receipt of a request.

The Financial Intelligence Unit shall, in written form, notify the requesting party on the refusal of the request from paragraphs 1, 2 and 4 of this Article, stating the reasons for refusal.

The foreign financial intelligence unit may disclose the obtained data, information and documentation from paragraph 1 of this Article to another competent authority or a third party, only with the prior consent from the Financial Intelligence Unit.

The financial intelligence unit shall not give consent from paragraph 7 of this Article if:

1) the provision of data, information and documentation would be disproportionate to the legitimate interests of a natural or legal person or Montenegro;

2) the provision of data, information and documentation would jeopardise execution of preliminary investigation or conduct criminal proceedings in Montenegro, or otherwise be detrimental to the interests of such proceedings;

3) the provision of data, information and documentation is not in accordance with the core principles of the legal system in Montenegro.

The financial intelligence unit shall make a written explanation on the refusal to give consent from paragraph 7 of this Article and deliver it to the requesting party.

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

The Financial Intelligence Unit may set the conditions and restrictions for the use of data, information and documentation from paragraphs 1, 2 and 4 of this Article.

Competent authorities from Article 96 paragraph 1 of this Law may exchange the data on bank accounts and safe deposit boxes, financial information, or financial analyses and other data, information and documentation obtained from the financial intelligence unit, upon request and on an individual basis, with other authorities from another country, only with prior consent from the Financial Intelligence Unit and if these data and financial information, or financial analyses are necessary for the prevention, detection and suppression of money laundering and associated predicate criminal offences and terrorist financing.

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

Provision of data, information and documentation to the authority from another country on financial intelligence unit's own initiative

Article 108

The Financial Intelligence Unit maz provide information on bank accounts and safe deposit boxes, financial information, financial analyses and other data, information and documentation on persons, transactions and property in relation to which there are reasons for suspicion or reasonable grounds to suspect in money laundering and associated predicate criminal offences or terrorist financing, or that the property derives from criminal activity, that it obtained in accordance with this Law, without request, on its own initiative, to the foreign financial intelligence unit, other authorities of another country or international organisations responsible prevention and detection of money laundering and terrorist financing, to an authority of another country responsible for confiscation of property and to the supervisory authorities of another country, for the purpose of prevention and detection of money laundering, associated predicate criminal offences, criminal activity or terrorist financing.

In the process of providing data, information and documentation in accordance with paragraph 1 of this Article, the Financial Intelligence Unit may set the conditions and restrictions for the use and further dissemination of these data, information and documentation.

Temporary suspension of a transaction and temporary prohibition of access to a safe deposit box on the initiative of authorities from another country

Article 109

The Financial Intelligence Unit may, in accordance with this Law, and upon elaborated initiative of a foreign financial intelligence unit or another authority from another country responsible for the prevention and detection of money laundering and terrorist financing, by an order, suspend the execution of a transaction or prohibit the access to a safe deposit box, for no longer than 72 hours.

In the case from paragraph 1 of this Article, the Financial Intelligence Unit shall act in accordance with article 93 of this Law.

The Financial Intelligence Unit may refuse the initiative from paragraph1 of this Article if, on the basis of facts and circumstances specified in the initiative, it assesses that there are not given sufficient reasons or reasonable grounds to suspect that the funds or other property derive from criminal activity or that money laundering and associated predicate criminal offences or terrorist financing are committed, and shall notify on that the foreign financial intelligence unit or another authority from another country responsible for the prevention and detection of money laundering and terrorist financing, specifying the reasons for refusal.

Initiative to the authority from another country for temporary suspension of a transaction and temporary prohibition of access to a safe deposit box

Article 110

The Financial Intelligence Unit may, within its own activities or powers, submit an initiative for temporary suspension of a transaction and temporary prohibition of access to a safe deposit box to a foreign financial intelligence unit or another authority from another country responsible for the prevention and detection of money laundering and terrorist financing, if it assesses that

there are reasons for suspicion or reasonable grounds to suspect that the funds or other property derive from criminal activity or that money laundering and associated predicate criminal offences or terrorist financing are committed.

VII. OBLIGATIONS OF STATE AUTHORITIES, OTHER AUTHORITIES AND INSTITUTIONS

Administrative authority competent for customs affairs
Article 111

Administrative authority competent for customs affairs shall enable the Financial Intelligence Unit direct electronic access to data on:

- declaration of incoming and outgoing cross-border transportation of money, checks, bearer securities, precious metals and stones, in the value or amount of EUR 10,000 or more, no later than within 3 days from the day of the transport;
- incoming and outgoing cross-border transportation of money, checks, bearer securities, precious metals and stones, in the value or amount of EUR 10,000 or more, that were not declared or were falsely declared, immediately and no later than within 3 days from the day of the transport;
- incoming and outgoing cross-border transportation or attempt of incoming and outgoing cross-border transportation of money, checks, securities, precious metals and stones, in the value or amount of EUR 10,000 or more, where in respect of that transport or attempt of transport there are reasons for suspicion in money laundering or terrorist financing, immediately and no later than within 3 days from the day of the transport or attempt of the transport;

Registers of accounts and safe deposit boxes

Article 112

The Central Bank of Montenegro shall maintain the registers of accounts and safe deposit boxes that shall represent an electronic data base on natural and legal persons' accounts opened and safe deposit boxes leased, as well as on demand deposits and term deposits with credit institutions and branches of foreign credit institutions.

Credit institutions and branches of foreign credit institutions shall provide to the Central Bank of Montenegro the data on natural and legal persons' accounts opened and safe deposit boxes leased immediately upon opening the account or concluding a contract.

Credit institutions and branches of foreign credit institutions shall provide to the Central Bank of Montenegro the data on demand deposits and term deposits, no later than by the end of the next day from the day of the contract conclusion.

Registers of accounts and safe deposit boxes shall be maintained through the Central Register of Transaction Accounts in accordance with the law regulating 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 responsible for the equivalence of the data in the registers of accounts and safe deposit boxes with the data delivered by credit institutions and branches of foreign credit institutions.

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

The contents of registers of accounts and safe deposit boxes, the data provided for the purposes of these registers, the method of data provision and manner of gaining 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 has direct electronic access to at least the following data from the register of accounts and safe deposit boxes:

1) for natural persons: first name and surname, unique citizen number for a resident, type, number and country of issuance of a personal document for a non-resident, address and city of permanent or temporary residence;
2) for legal persons: name, registration number, head office (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 the agreement on leasing a safe deposit box, as well as the period for which the agreement is concluded.

Data from 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 undertakings
Article 114

Stock exchanges and clearing and depository companies shall, without delay, notify the Financial Intelligence Unit, if, during the performance of activities within their competences, they detect facts indicating possible connections with money laundering and associated predicate criminal 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 associated predicate offences or terrorist financing, in accordance with the Law.

The clearing and depository company shall provide to the Financial Intelligence Unit, through electronic communication, on a quarterly basis, the data on each collective custody account, credit institution or other financial institution at which that custody account is opened, as well as on the number of transactions and total turnover in that collective custody account.

The deadlines for providing the data from paragraph 2 of this Article shall be subject to the provisions of Article 90 paragraphs 4, 5 and 6 of this Law.

Stock exchanges and clearing and depository companies shall provide, to the Financial Intelligence Unit, data from paragraphs 1, 2 and 3 of this Article in the manner prescribed by the regulation from Article 66 paragraph 15 of this Law.

State prosecutor's offices, courts and the state administrative authority competent for judiciary affairs

Article 115

For the purpose of conducting the analysis from Article 99 of this Law, the competent state prosecutor's offices, competent courts, and the state administrative authority competent for judiciary affairs shall provide to the Financial Intelligence Unit, on a regular basis, the data and information on proceedings related to misdemeanours and criminal offences related to money laundering or terrorist financing, their perpetrators, as well as confiscation of property derived from a criminal offence or criminal activity.

The competent state prosecutor's offices shall provide to the Financial Intelligence Unit the following data, specifically:

1) name of the state prosecutor's office, number and date when indictment is filed;
2) name and surname, date of birth, address and unique citizen number of an accused resident natural person, and for a foreign citizen, the number, country of issue and date of expiry of the travel document, or the name, registration number, head office (address) of the accused legal person;
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 provide to the financial intelligence unit the following data on:

1) the name of the court, case number and date;
2) the name and surname, date of birth, address and unique citizen number of the natural person against whom proceedings have been initiated or who has submitted a request for court determination within the misdemeanour proceedings under this Law, and for foreign citizens, the number, country of issue and date of expiry of the travel document, or the name, registration number, head office (address) of the legal person against which proceedings have been initiated or which has submitted a request for court determination within the misdemeanour proceedings under this Law;
3) the stage of the proceeding and the final decision;
4) the legal qualification of the criminal offence or misdemeanour;
5) the name and surname, date of birth, address and unique citizen number of the natural person in relation to which a temporary security measure (freezing of assets) or temporary confiscation of movable property (seizure) has been imposed, and for a foreign citizen, the number, country of issue and date of expiry of the travel document, or the name, registration number, head office (address) of the legal person in relation to which a temporary security measure (freezing of assets) or temporary confiscation of movable assets (seizure) has been imposed;
6) the issue date and duration of the order on temporary security measures (freezing of assets) or temporary confiscation of movable property (seizure);
7) the amount of funds or the value of the property for which the order on a temporary security measure (freezing of property) or temporary confiscation of movable property (seizure) has been issued;
8) the amount of confiscated funds or the value of confiscated property;
9) the received and sent rogatory letters regarding criminal offenses from paragraph 1 of this Article or predicate criminal offenses.

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

Data from paragraphs 2, 3 and 4 of this Article shall be provided to the Financial Intelligence Unit once a year, and no later than by the end of February of the current year for the previous year, as well as upon a request of the Financial Intelligence Unit, in the manner prescribed by the regulation from Article 66 paragraph 15 of this Law.

VIII. RECORDS, PROTECTION AND STORAGE OF DATA

1. Types and content of records

Records kept by a reporting entity

Article 116

The reporting entity shall keep:

1) records on conducted CDD measures;
2) records on complex and unusual transactions from Article 58 of this Law;
3) records on data submitted to the Financial Intelligence Unit in accordance with Articles 66 and 90 of this Law;
4) records on orders on temporary suspension of the execution of a transaction or temporary prohibition of access to the safe deposit box;
5) records on requests for ongoing monitoring the client's financial activities;
6) records on the access of the supervisory authorities from Article 131 paragraph 1 of this Law to data, information and documentation in relation to which the reporting entity shall act in accordance with Article 123 paragraph 1 of this Law;
7) records on professional education and training of employees of the reporting entity in the area of the prevention of money laundering and terrorist financing.

The reporting entity shall keep the records from paragraph 1 of this Article in a manner that will ensure the reconstruction of individual transactions, including the amounts and currency, which could be used in the process of detecting the criminal activities of clients.

Content of records kept by the reporting entity

Article 117

Records on the conducted CDD measures shall contain the following data:

1) for a legal person: name, head office (address and city, or municipality for a legal person with head office in Montenegro, and for a legal person with its head office in another country, country and city), unique identification number, information on whether it is a resident or non-resident, the reason for the business relationship (establishing a business relationship, executing transaction, attempt to execute transaction, renting a safe deposit box, accessing the safe deposit box, insurance policy holder, insurance beneficiary, seller, buyer), telephone number and e-mail address;
2) for the entrepreneur: name, head office (address and city, or municipality for entrepreneurs with head office in Montenegro, and country and city for entrepreneurs with head office in another country), unique identification number, first and last name, information on whether he/she is a resident or non-resident, reason for establishing business relationship (establishing a business relationship, executing transaction, attempt to execute transaction,

renting a safe deposit box, accessing a safe deposit box, insurance policy holder, insurance beneficiary, seller, buyer), telephone number and e-mail address;

3) for a natural person: name and surname, unique identification number, address and municipality of residence, or residence in Montenegro, date of birth, country of birth, citizenship, information on whether the person is a politically exposed person, information on whether he/she is a resident or non-resident, phone number and e-mail address, type, number, country of issue and date of expiry of the personal document, reason for establishing business relationship (establishing a business relationship, executing transaction, attempt to execute transaction, renting a safe deposit box, access to a safe deposit box, insurance policy holder, insurance beneficiary, seller, buyer), information on whether the natural person is a client, representative, authorised person, beneficial owner, founder, trustee, user of the property managed, insured, insurance policy holder, insurance beneficiary, seller or buyer;
4) data on the manner in which the client's identification is performed (identification based on physical presence, electronic identification or video-electronic identification);
5) video-audio recording created during the video-electronic identification of the client;
6) information on the purpose, intention, goal, nature of the business relationship and transaction, the basic code of the client's business 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, or the date and time of entering into the casino or accessing the safe deposit box;
7) transaction data: date and time of execution of transaction, transaction amount in euros, transaction amounts by currency, transaction order number, policy or contract, depending on the type of reporting entity, information on whether the transaction is executed in full or in part, information on the type of transactions (cash or non-cash), information on the type of transaction (regular, suspicious, unusual or complex), information on the credit institution of the payer and payee (type and number of the account, unique identification number, name and country of head offices), information on the type of transaction (payment or withdrawal), information on the method of execution of the transaction depending on the type of reporting entity (cash, non-cash, already executed, in instalments, market or non-market), information on the purpose and intended nature of the transaction and the name of the branch of the reporting entity that executes transaction.

If the reporting entity is an organiser of games of chance or provides safe deposit box rental services, the record on conducted CDD measures, in addition to the data from paragraph 1 item 3 of this Article, shall , in relation to natural persons, also contain data on the activities of the natural person depending on the type of reporting entity (entry into space for organising games of chance, access to games of chance via the Internet or other telecommunication means, access to the cash register, access to other places, or locations where transactions are made in accordance with the type of game of chance or access to the safe deposit box).

If the transaction is related to the reporting entities from Article 4 paragraph 2 item 1 of this Law, the record on conducted CDD measures , in addition to the data from paragraph 1 item 7 of this Article, shall also contain the following data on the transaction: type and number of the account, unique identification number, name and country of the head office of the credit institution of the account, name and surname, address and city of permanent residence, or temporary residence of the natural person to whom the transaction is to be sent, or the name, head office (address, city and country) of the legal person to whom the transaction is to be sent, telephone and e-mail address of those persons, the SWIFT code of the credit institution, the country of destination, the name and the country of the head office of the credit institution that is the correspondent.

If the transaction is related to the reporting entities from Article 4, paragraph 2 item 7 of this Law, the records on CDD measures, in addition to the data from paragraph 1 item 7 of this Article, shall also contain the following data on the transaction: stock exchange code, securities 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 the buyer's account number on the stock exchange.

If the transaction is related to reporting entities from Article 4 paragraph 2 items 8 and 9 of this Law, the record on conducted CDD measures, in addition to the data from paragraph 1 item 7 of this Article, shall also contain the following data on the transaction: insurance policy start date, duration of insurance in years, information on the type of premium (one-time, monthly, quarterly, semi-annual or annual), first and last name of the beneficiary of the insurance premium and information on the reason for the payment (insured case, termination of the contract or expiry of the contract).

If the transaction is related to the reporting entities from Article 4 paragraph 2 item 13 and paragraph 4 of this Law, the records on the conducted CDD , in addition to the data from paragraph 1 item 7 of this Article, shall also contain the following data on the subject of the transaction:

1) for valuable items: data on the type of valuable item (art, precious metal, precious stones, securities, crypto wallet or other valuable items), information on 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 metal, type, purity, size and type of metal), data on precious stones (width, dimensions, shape, colour and data on clarity i.e. purity), data on bearer securities (symbol, type and status of the security, unique identification code of the financial instrument in accordance with the ISO 6166 standard - ISIN), data on the crypto wallet (crypto wallet code and crypto wallet service provider), data on other valuable items (name, value and description);
2) for immovable property: information on the type and value of the immovable property, address, house number, city, postal code, country, number of the immovable property certificate, information on the right in rem to that immovable property, the basis for acquiring the right in rem, area, floor number, date of registration of the right in rem in the real estate cadastre, cadastral municipality, plot number, notes, scope of rights and age of immovable property;
3) for means of transport: information on the type (motor vehicle, vessel, aircraft or other means of transport), value, type and registration number, country in which the means of transport is registered, date until which the registration is valid, brand and model, chassis number, name of the manufacturer, identification number, information on the category, manufacturer and type/model of the means of transport, serial number of the engine of the means of transport, serial number of the aircraft, as well as the type, or the name of the vessel.

The records on complex and unusual transactions from Article 58 of this Law shall contain data from paragraphs 1 to 6 of this Article.

The records on data submitted to the Financial Intelligence Unit in accordance with Articles 66 and 90 of this Law shall contain data from paragraphs 1 to 6 of this Article, data on indicators from the list of indicators for identifying suspicious clients and transactions, data on reasons for suspecting that the property derives from criminal activity or that it constitutes money laundering, related predicate crimes or terrorist financing, date of data delivery to The Financial Intelligence Unit and the reasons for executing the transaction (explanation).

The records on orders for temporary suspension of transaction execution or temporary prohibition of access to the safe deposit box shall contain the number of the transaction order whose execution is temporarily suspended, the amount of the transaction, the date and time of the start of the temporary suspension of transaction execution, the date and time of the extension of

the temporary suspension of transaction execution, the account balance before the blocking and data from paragraph 1 items 1, 2 and/or 3 of this Article for the person to whom the temporary suspension of execution of the transaction applies.

The records on requests for ongoing monitoring the client's financial activities shall contain the number of requests, information on the type and number of the client's account, the starting date of monitoring, the date of extension of monitoring, data from paragraph 1 items 6 and 7 and paragraph 3 of this Article that occurred during the monitoring period and the data from paragraph 1 items 1, 2 and/or 3 of this Article for the person to whom that monitoring refers.

The record on the access of supervisory authorities from Article 131 paragraph 1 of this Law to data, information and documentation, in relation to which the reporting entity shall 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 examination officer, the date and time of the review of data, information and documentation from paragraph 1 items 1, 2 and/or 3 of this Article for the person whose data, information and documentation were reviewed.

The records on professional training and professional development of employees of reporting entities in the area of the prevention of money laundering and terrorist financing shall contain the name and surname and work position 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 organiser (employer, professional association, Financial Intelligence Unit or other professional body or organisation in Montenegro or another country).

Records kept by the administration body responsible for customs affairs

Article 118

The administration body responsible for customs affairs shall keep the following records:

1) records of the import or export or attempted import or export across the country border of money, checks, bearer securities, precious metals and gem stones, in the amount or value of EUR 10,000 or more, which was declared, undeclared or falsely declared;
2) records of the import or export across the country border of money, checks, bearer securities, precious metals and gem stones, in the amount or value of less than EUR 10,000, if there are reasons for suspicion or grounds for suspicion that the property derives from criminal activity or that it is money laundering or terrorist financing.

Content of records kept by the administration body responsible for customs affairs

Article 119

Records on cash, checks, bearer securities, precious metals and gem stones, transfers in or from or attempts to transfer in or from the country , in the amount or value of EUR 10,000 or more, which was declared, undeclared or falsely declared, shall contain the following information:

1) for a natural person who transfers in or from or attempts to transfer in or from the country money, checks, bearer securities, precious metals and gem stones: name and surname, unique identification number, address and city of permanent residence or temporary residence, citizenship, type, number, country of issue and date of expiry of the identity document;
2) for a legal person, or a natural person, for which cash, checks, bearer securities, precious metals and gem stones are transferred in or from the country: name, head office (address and city, or municipality for legal persons with head office in Montenegro, and name of the

country for legal persons with head office in another country), the legal person's registration number and TIN, or name and surname, unique registration number, address and city of permanent residence, or temporary residence and citizenship of the natural person;

3) for a legal person, or a natural person to whom the cash is intended: name, head office (address and city, or municipality for legal persons with head office in Montenegro, and name of the country for legal persons with head office in another country), registration number and PIB of the legal person, or name and surname, unique identification number, address and city of permanent residence, or temporary residence and citizenship of the natural person;
4) the amount, currency and information on the type, source and purpose of cash that is transferred in or from or attempted to be transferred in or from the country;
5) information on valuable items that are transferred in or from or attempted to be transferred in or from the country: information on the type of valuable item (cheques, bearer securities, precious metals or gem stones), source and purpose of use of the valuable item, data on bearer securities (symbol, type and status of the security, unique identification code of the financial instrument in accordance with the ISO 6166 standard - ISIN), information on precious metals (name, value, description, weight, number of carats, colour of metal, type, purity, size and type of metal), information on gem stones (width, dimensions, shape, colour, information on clarity, or purity), depending on the availability of information;
6) the name of the border crossing where the transfer in or from or attempted to transfer in or from the country cash, checks, bearer securities, precious metals and gem stones is made, date and time of transfer in or from or attempt to transfer in or from the country such property, information on whether it is an entry or exit from Montenegro and the name of the country from which the property is being transferred in or from;
7) information on whether the transfer of cash, checks, bearer securities, precious metals and gem stones, in or from the country, was declared, undeclared or falsely declared to the administration body responsible for customs affairs.

Records on cash, checks, bearer securities, precious metals and gem stones, transfers in or from the country, in the amount or value of less than EUR 10,000, if there are reasons for suspicion or reasonable grounds to suspect that the property derives from criminal activity or that money laundering or terrorist financing has been committed, shall contain information from paragraph 1 items 1 to 6 of this Article, information on indicators for identifying suspicious clients that exist in relation to a specific case and information on whether the transaction is withheld from being carried out.

Records kept by the financial intelligence unit

Article 120

The financial intelligence unit shall keep the following records:

1) records on the analyses performed and cases handled in accordance with the law;
2) records on reporting entities, compliance officers for the prevention of money laundering and terrorist financing, or their deputies;
3) records on criminal offenses and misdemeanours and perpetrators of criminal offenses and misdemeanours from Article 115 of this Law;
4) records on the actions of the supervisory authorities from Article 131 paragraph 1 of this Law towards the reporting entities;

5) records on the officers of the financial intelligence unit who reviewed, or accessed data or to whom the data from other authorities was provided in accordance with Article 126 of this Law.

Access to data from the records from paragraph 1 of this Article shall be performed by electronic identification.

Content of records kept by the financial intelligence unit

Article 121

The record on the analyses carried out and the cases handled by the financial intelligence unit in accordance with the law shall contain the following data:

- data from Article 117 paragraphs 1 to 6 and paragraphs 8 and 9 of this Law;
- case number, case name, number of the received document, name and surname, or the name of the sender and recipient of the document, date of sending of the document, date of delivery of the document, information on whether the document is classified, information that represents the reasons for the temporary suspension of the execution of the transaction, or temporary prohibition of access to the safe deposit box, data representing the reasons for ongoing monitoring of the client's financial activities, legal qualification of the criminal offense, result of operational analysis, or strategic analysis, reasons for not providing a response to a request or information in accordance with Article 96 paragraphs 4 and 5 of this Law, scanned documents received and sent, scanned documentation attached to documents;
- data on persons subject to financial analysis: mobile phone number, international unique mobile device identifier (IMEI), photo, scanned page with data from personal identification document, previous personal data (unique identification number, first and last name and date of birth), false personal data (unique identification number, first and last name, date of birth, address of permanent residence, citizenship), scanned card of deposited signatures, previous names of the legal person and data on the legal person that is a founder (identification number, TIN, name, address, city and country of head offices, country in which the legal person is registered);
- data on orders for temporary suspension of execution of transactions from Articles 93, 109 and 110 of this Law;
- data on requests for monitoring the client's financial operations on a continuous basis from Article 95 of this Law;
- data from responses to requests from Articles 91 and 92 of this Law;
- data from requests, information and notifications from Articles 96, 97 and 98 of this Law;
- data on international requests and information from Articles 106, 107 and 108 of this Law;
- data taken from the administration body responsible for customs affairs from Article 111 of this Law;
- data on bank accounts and safe deposit boxes from Article 113 of this Law;
- data submitted by stock exchanges and clearing and depository companies from Article 114 of this Law; and
- data from received and sent documents.

The record on the reporting entities, compliance officers for the prevention of money laundering and terrorist financing, or their deputies, shall contain the following data:

1) for the reporting entity: unique identification number, TIN, name and head office (address and city, or municipality for reporting entities with head office in Montenegro, and name of

the country for reporting entities with head office in another country) and information on the licence (issued, revoked or not necessary);

2) for an compliance officer for the prevention of money laundering and terrorist financing, or his deputy: unique identification number, first and last name, information on whether the person is an compliance officer for the prevention of money laundering and terrorist financing or his deputy, e-mail, telephone number, mobile phone number, date of commencement and termination of activities of the compliance officer for the prevention of money laundering and terrorist financing, or his deputy, license number, date of licence issue and expiration date.

The records on criminal offenses and misdemeanours and perpetrators of criminal offenses and misdemeanours from Article 115 of this Law shall contain data from Article 115 paragraphs 2, 3 and 4 of this Law.

The records on the actions of the supervisory authorities from Article 131 paragraph 1 of this Law in relation to reporting entities shall contain data from Article 135 paragraphs 1, 2, 4 and 5 of this Law.

The record on the officers of the financial intelligence unit who reviewed, or accessed data or to whom the data of other authorities was delivered in accordance with Article 126 of this Law shall contain the unique identification number of the employee of the financial intelligence unit who reviewed, or accessed data or to whom the data was delivered to, legal basis, date and time of review, access, or delivery of data, as well as data which they reviewed, or accessed to, or data that was delivered to them.

Data records on non-residents

Article 122

If a non-resident who is a natural person does not have a unique identification number, the records and registers prescribed by this Law shall be provided with the date of birth, country of birth, number, country of issue and type of personal document, as well as the date of expiry of the personal document, and for a non-resident who is a legal person instead of the unique identification number, the TIN shall be entered, unless otherwise specified by this Law.

2. Data protection

Non-disclosure

Article 123

Reporting entities and their employees, members of management bodies, supervisory or other managing authorities, or other persons to whom the data from Article 117 paragraphs 1 to 11 of this Law are available or were available, shall not reveal to the customer or a third party that:

1) information disclosed to the Financial Intelligence Unit, or information made available for review or submitted documentation about the customer or transaction in accordance with Articles 66 and 90 of this Law;
2) pursuant to Article 93 of this Law, the Financial Intelligence Unit issued an order to temporarily suspend the execution of the transaction or prohibit access to the safe deposit box, or has given instructions to the reporting entity in this regard;
3) the Financial Intelligence Unit, pursuant to Article 95 of this Law, demanded ongoing monitoring of the client's operations;

4) a preliminary investigation or official investigation has been initiated or could be initiated against the customer or a third party due to the reasonable grounds to suspect or reasonable suspicion that the criminal offense of money laundering and related predicate criminal offense or terrorist financing was committed.

Disclosure, within the meaning of paragraph 1 of this Article, shall not be an attempt to dissuade the client from engaging, performing or participating in an illegal activity.

The prohibition of disclosure from paragraph 1 of this Article shall not apply to data which, in accordance with this Law, are obtained and processed by the reporting entity and which are necessary for the establishment of facts in criminal proceedings and if the submission of such data is requested in writing, or ordered by the competent court or the competent supervisory authority from Article 131 paragraph 1 of this Law for the purpose of implementing this Law.

Data from 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 collects or produces, in accordance with this Law, for the purpose of prevention and detection of money laundering, related predicate criminal offences and terrorist financing shall not be submitted to other persons for inspection, nor can their existence be confirmed in the records of the Financial Intelligence Unit, unless it is otherwise defined by this Law.

Where there are reasonable grounds to suspect in criminal offence of money laundering, related predicate offences and terrorist financing, data, information and documentation from paragraph 4 of this Article shall be marked with the appropriate level of confidentiality in accordance with the law regulating data confidentiality.

The data, information and documentation from 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 offences, related predicate criminal offenses and terrorist financing, with the obligation to keep data in accordance with Article 130 of this Law.

In order to ensure efficient and timely international cooperation, information, notification and requests from paragraph 4 of this Article marked with the confidentially level "RESTRICTED" may be submitted to foreign financial intelligence units, other competent authorities of other countries and international organisations and through the communication systems of the World Association of Financial intelligence units.

Exemption from the principle of data confidentiality

Article 124

When providing data, information and documentation to the financial intelligence unit, in accordance with this Law, the obligation to protect data confidentiality (business, bank, professional and other secrecy) shall not refer to reporting entities, organizations with public powers, state authorities, and their employees, nor to a reporting entity who is a member of a financial group when exchanging data and information with other members of a financial group in accordance with the conditions from Article 62 of this Law.

The reporting entity and the reporting entity's employees shall not be liable for damage caused to clients or third parties if, in accordance with this Law, they:

1) provide data, information and documentation about their clients to the Financial Intelligence Unit;
2) obtain and process data, information and documentation about clients;
3) execute the order of the Financial Intelligence Unit on the temporary suspension of the execution of the transaction or the temporary prohibition of access to the safe deposit box;
4) execute the request of the Financial Intelligence Unit for the ongoing monitoring of the client's financial activities.

The reporting entity, or reporting entity's employees shall not be criminally or disciplinary liable for breaching the obligation to keep data confidential 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 for the purpose of verifying clients and transactions for which there are reasons for suspicion or reasonable grounds to suspect that the property derived from criminal activity or that money laundering or terrorist financing has been committed.

Protection of the integrity of the authorized person for the prevention of money laundering and terrorist financing and employees

Article 125

The reporting entity shall take 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.

Use of received personal data

Article 126

The Financial Intelligence Unit, state authorities, state administration bodies, holders of public authority, reporting entities and their employees shall use the personal data obtained in accordance with this Law only for the purpose for which the personal data are processed.

On examination, access and submission to the Financial Intelligence Unit of personal data from Article 47 paragraph 1 item 1, Article 55 paragraph 2, Article 92 paragraph 1 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 examination, or made access, or that the data were delivered to it electronically, as well as the date and time when the examination and access to personal data started and when it finished.

For the exchange of personal data between the financial intelligence unit and state authorities, state administration authorities and holders of public authority, a security-communication link shall be used, which represents a protected system of data exchange between precisely defined subjects.

Regulations from paragraphs 1, 2 and 3 of this Article, governing the protection of personal data, shall apply on the processing, protection, and storage of personal data.

Data retention

Article 127

The reporting entity shall retain all data, information and documentation obtained in accordance with this Law, data on the identification number of each client account, data and documentation on electronic money transfer, documentation on business correspondence and reports for ten years following the termination of the client's business relationship, executed occasional transactions, the client's entry into the casino and premises where other games of chance are organised or access to the safe deposit box, unless a specific law prescribes longer period for data retention.

The reporting entity shall retain 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.

The reporting entity shall retain data and related documentation on the compliance officer for the prevention of money laundering and terrorist financing, or their deputy, professional training and development of employees in the area of the prevention and detection of money laundering and terrorist financing and the application of internal control and audit measures for the period of four years following the termination of the validity of the license, that is, the completed professional training and development and the completed internal control and audit.

After the expiration of the deadlines from paragraphs 1, 2 and 3 of this Article, the reporting entity shall delete or destroy the client's personal data.

Data retention with the administration body competent for customs affairs

Article 128

The administration body competent for customs affairs shall retain the data from the records from Article 119 of this Law for the period of ten years following the date of obtaining those data.

After the expiration of the deadline from the paragraph 1 of this Article, personal data from the records from Article 119 of this Law shall be deleted.

Data retention in the Register of beneficial owners and registers of accounts and safe deposit boxes

Article 129

The administration body competent for tax collection shall retain the data in the Register of Beneficial Owners for ten years from the day that is considered the day of the termination of the existence of the entity from Article 43 paragraph 3 of this Law in accordance with the law.

The Central Bank of Montenegro shall retain the data in the registers of accounts and safe deposit boxes for ten years after the account is closed, or, after the contract on renting the safe deposit box has expired.

After the expiration of the time period from paragraphs 1 and 2 of this Article, personal data from the Register of beneficial owners, or registers of accounts and safe deposit boxes shall be deleted.

Data retention by the financial intelligence unit

Article 130

The Financial Intelligence Unit shall keep the data from the records kept in accordance with this Law for the period of 11 years from the date of obtaining those data.

After the deadline from paragraph 1 of this Article has expired, the electronic data from paragraph 1 of this Article shall be depersonalised, and the data in paper form shall be handed over to the competent recycling centre for destruction.

The Financial Intelligence Unit shall not inform the person to whom the data and information relate to, or any other person, about the data and information at its disposal, nor allow examination before the expiration of ten years from the date of their recording, unless otherwise prescribed by this Law.

The person from paragraph 3 of this Article has the right to review their personal data after the expiration of the period of ten years from the date of their recording.

The detailed method of depersonalization of data from paragraph 1 of this Article shall be prescribed by the Ministry.

The regulation from paragraph 5 of this Article shall be marked with an appropriate level of confidentiality, in accordance with the law regulating data confidentiality of data.

IX. SUPERVISION

Inspection and other types of supervision

Article 131

Inspection and other types of supervision, within the competences defined by this Law and other laws, shall be conducted by:

1) the Central Bank of Montenegro in relation to the reporting entities from Article 4, paragraph 2, items 1, 2 and 3 of this Law, to which it grants a licence or authorisation for work;
2) the Agency for electronic communications and postal services in relation to the reporting entities from Article 4 paragraph 2 item 4 of this Law;
3) the Capital Market Authority of Montenegro in relation to the reporting entities from Article 4 paragraph 2 items 5, 6 and 7 of this Law and legal persons from Article 114 of this Law;
4) the Insurance Supervision Agency in relation to the reporting entities from Article 4 paragraph 2 items 8 and 9 of this Law;
5) the administration body responsible for games of chance in relation to the reporting entities from Article 4 paragraph 2 item 10 of this Law;
6) administration body responsible for tax collection in relation to reporting entities from Article 4 paragraph 2 item 11 of this Law and entities from Article 43 paragraph 3 of this Law;
7) the state administration body responsible for digital assets in relation to the reporting entities from Article 4 paragraph 2 item 12 of this Law;
8) the Ministry, through an authorised person, in relation to the reporting entities from Article 4 paragraph 2 item 13 of this Law;
9) the Bar association of Montenegro in relation to the reporting entities from Article 4 paragraph 3 of this Law;
10) the state administration body competent for judicial affairs in relation to the reporting entities from Article 4, paragraph 4 of this Law.

The supervisory authorities from paragraph 1 of this Article shall use a ML/TF risk based approach to supervision when planning the examination of reporting entities.

When planning the frequency and the scope of examination, the supervisory authorities from paragraph 1 of this Article shall take into account the following:

- data related to the risks of money laundering and terrorist financing established in the National Risk Assessment;
- data related to specific national or international risks of money laundering and terrorist financing associated with clients, products, services or distribution channels;
- data related to the risk of individual reporting entities and other available data;
- significant events or changes related to the reporting entity's management body, as well as any change in activity.

The supervisory authorities from paragraph 1 of this Article shall, no later than seven working days before conducting the examination, inform the Financial Intelligence Unit about the activities they plan to undertake as well as to submit data on the reporting entity at which the supervision is planned (identification number, TIN and name), the date when the examination is planned, information on whether direct or indirect supervision is being carried out, and when necessary, coordinate and harmonise their activities in conducting supervision over the implementation of this Law with the Financial Intelligence Unit.

If the supervisory authority from paragraph 1 of this Article, in the process of the supervision over the implementation of this Law, finds out irregularities in the operations of the reporting entity, it is authorised to:

- point out the identified irregularities to the reporting entity and set a deadline for their removal;
- issue a misdemeanour order or initiate misdemeanour proceedings against the reporting entity, in accordance with the law regulating misdemeanour proceedings;
- suspend or revoke the licence, or 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 from 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, or 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 defined by this Law.

The supervisory authority from paragraph 1 of this Article shall exchange information with another supervisory authority and, upon the request of another supervisory authority, submit the necessary data and documentation required by that authority in the process of conducting supervision in accordance with this Law.

The Financial Intelligence Unit may submit a request to the supervisory authorities from paragraph 1 of this Article to conduct supervision over a certain reporting entity or type of reporting entity, based on the data, information and documentation available to the Financial Intelligence Unit and on the basis of the performed strategic analyses and operational analyses.

The supervisory authorities from paragraph 1 of this Article shall act in accordance with the request from paragraph 8 of this Article.

If necessary, due to the complexity of the examination or the importance of removing irregularities, the supervisory authorities from paragraph 1 of this Article may, together with the Financial Intelligence Unit, conduct a joint inspection supervision of a certain reporting entity or type of a reporting entity.

Direct and indirect supervision

Article 132

Supervisory authorities from Article 131 paragraph 1 of this Law shall perform direct and indirect supervision over the implementation of this Law.

In the process of supervision, the officer for supervision shall identified himself/herself with official identification and a badge, or authorisation.

Direct supervision shall be carried out on the basis of the examination plan of the competent supervisory authority from Article 131 paragraph 1 of this Law, which is drawn up on an annual basis and represents a business secret.

Direct supervision shall be initiated and conducted in the official premises of the reporting entity, and shall be carried out by inspecting the business books, other documentation and the information system of the reporting entity.

The provisions of the law regulating inspection supervision, or the law regulating the competences of the supervisory authorities from Article 131 paragraph 1 of this Law, shall be applied in line with the direct supervision procedure.

Indirect supervision shall be carried out through examination the data, information and documentation that the reporting entities submit to the competent supervisory authorities from Article 131 paragraph 1 of this Law upon their request or make them electronically available or through analysing the reports and data submitted by reporting entities in accordance with the Law.

Upon the request from paragraph 6 of this Article, the reporting entity shall without delay submit to the competent supervisory authority from Article 131 paragraph 1 of this Law, accurate and complete data, information and documentation necessary for supervision, and no later than within eight days from the date of submission of the request

The supervisory body shall draw up a record or report on the supervision from paragraph 1 of this Article.

Special powers of supervisory authorities

Article 133

If, on the basis of the law, the competent supervisory authority from Article 131 paragraph 1 of this Law grants licences to the reporting entity, an authorisation for the acquisition of qualifying holding in the reporting entity, or an authorisation for the appointment of members of managing bodies of the reporting entity, it may at any time obtain information on the conviction of persons subject to the verification of the fulfilment of the conditions for granting the licence, or authorisation and their associates, or connected persons, in accordance with the law.

An associate, or a connected person from paragraph 1 of this Article shall be considered an associate or a related person in accordance with the regulation regulating the business activities of the reporting entity.

Data from paragraph 1 of this Article may be used by the competent supervisory authority exclusively for the purposes for which they were obtained and may not be disclosed or made available to third parties.

International cooperation of supervisory authorities

Article 134

The competent supervisory authority from Article 131 paragraph 1 of this Law may, upon its own initiative or on the basis of a written and elaborated request of the supervisory authority of another country, exchange data, information and documentation in connection with:

1) regulations governing the business activities of the reporting entity, subject to the supervision by that supervisory authority, as well as other relevant regulations for conducting supervision;
2) the sector in which the reporting entity, subject to the supervision by that supervisory authority, operates;
3) the supervision of the reporting entity;
4) transactions or persons for whom there are reasons to suspect or reasonable grounds to suspect that money laundering, related predicate crimes or terrorist financing have been committed.

The supervisory authorities from paragraph 1 of this Article, in accordance with the principles of reciprocity and keeping confidential information, may reciprocally, within the scope of their powers, request assistance in carrying out the examination of the reporting entity that is part of the group and operates in the country from which the assistance is requested,

The method of submitting data, information and documentation, as well as performing joint supervision from paragraph 2 of this Article, shall be defined by the supervisory authorities from paragraph 1 of this Article by a separate agreement in accordance with the law.

The supervisory authorities from paragraph 1 of this Article shall only use the data, information and documentation from paragraph 1 of this Article solely:

1) to perform their duties in accordance with this Law;
2) in the event of an appeal or other legal remedies against the decision of the body responsible for the supervision, including court proceedings.

The supervisory authority from paragraph 1 of this Article that has determined irregularities from Article 137 of this Law shall also inform other competent supervisory authorities from Article 131 paragraph 1 of this Law, if these irregularities are of importance for their work.

The supervisory authority from paragraph 1 of this Article may not disclose and exchange data, information and documentation collected in accordance with paragraphs 1 to 4 of this Article with third parties, without the explicit consent of the supervisory authority that submitted the data, information and documentation.

The supervisory authority from paragraph 1 of this Article shall not use data, information and documentation collected in accordance with paragraphs 1 to 4 of this Article for a purpose other than that for which the supervisory authority that provided the data, information and documentation gave its consent, except in justified circumstances in accordance with the law, whereby it shall immediately notify that authority.

Submission of data on actions undertaken during the examination procedure

Article 135

The supervisory authorities from Article 131 paragraph 1 of this Law shall deliver to the Financial Intelligence Unit data and information on the activities taken in the process of supervision, in accordance with this Law, as follows:

- information on the reporting entity: identification number, TIN, name and head office (address and city, or municipality for reporting entities with head office in Montenegro, and name of the country for reporting entities with head office in another country), name and surname,

unique identification number of the responsible person in the legal person, or 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 person is a foreigner;

- information on the date of supervision and a description of the findings;
- names and surnames of persons that are, at the competent supervisory authority from Article 131 paragraph 1 of this Law, engaged to perform affairs of the prevention of money laundering and terrorist financing;
- the report, or the record of examination in electronic form.

When irregularities in the operations of the reporting entity are determined, the supervisory authorities from Article 131 paragraph 1 of this Law shall submit the following data to the financial intelligence unit:

- the date of the submission of the misdemeanour order, that is, the request for initiating misdemeanour proceedings or other imposed measures;
- number of a misdemeanour order;
- description of the misdemeanour from Article 137 of this Law;
- information on the imposed measures;
- the amount of the imposed fine.

The supervisory authorities from Article 131 paragraph 1 of this Law shall submit the information from paragraphs 1 and 2 of this Article to the Financial Intelligence Unit within eight days from the day of the performed supervision, or imposition of the measure.

If the supervisory authority from Article 131 paragraph 1 of this Law suspends or revokes the licence for work, or imposes another measure for the purpose of restricting or prohibiting the work of the reporting entity, in accordance with the law, it shall inform the Financial Intelligence Unit on that within eight days from the day when the measure was imposed.

If the supervisory authorities from Article 131 paragraph 1 of this Law assess during the supervision that in relation to a person, property, or transaction there are reasons for suspicion or reasonable grounds to suspect that money laundering, related predicate offences or terrorist financing have been committed, or that the property derives from criminal activity, they shall inform the Financial Intelligence Unit on that, without delay.

Supervisory authorities from Article 131 paragraph 1 of this Law shall deliver information from paragraphs 1 and 2 and notifications from paragraphs 4 and 5 of this Article to the Financial Intelligence Unit as it is defined in the regulation from Article 66 paragraph 15 of this Law.

Data Access

Article 136

Supervisory authorities from Article 131 paragraph 1 of this Law may have direct access to data that reporting entity submits to the Financial-Intelligence Unit under Article 66 of the Law, in the format submitted by the reporting entity.

Supervisory authorities from Article 131 paragraph 1 of this Law may not have direct access to data from paragraph 1 of this Article in the format in which the Financial-Intelligence Unit processed them, and the data may be submitted to Supervisors upon submitted request and if the Financial-Intelligence Unit assess that the request was justified.

The supervisory authorities from paragraph 1 of this Article may, for the purpose of performing tasks under this Law, have the direct access to the CRP and the criminal records.

The Financial Intelligence Unit may, upon the justified request of the supervisory authorities from Article 131 paragraph 1 of this Law, for the purposes of conducting verifications for issuing licences and approvals issued by the supervisory authority under the law, submit all relevant data that it may collect through implementation of its competences.

X. PENALTY PROVISIONS

Article 137

The fine in an amount of EUR 3,000 to EUR 20,000 shall be imposed on a legal person misdemeanour if:

1) it does not establish an appropriate information system, if the reporting entity is a credit institution or other financial institution (Article 11 paragraph 1 item 3);
2) within the period of 60 days since the day of its establishment or performance of business activity, it does not draft internal regulation on risk analysis in which it identifies and assesses risks, considering risk factors of an individual customer, a group of customers, a country or geographic area, business relationship, transaction or product, services and distribution channels that may be misused for the purpose of money laundering or terrorist financing and does not update it regularly, at least once a year, and keep it in accordance with this Law, (Article 12 paragraph 1 indent1);
3) it does not establish and implement the system of managing the risk of money laundering and terrorist financing from Article 14 paragraphs 1 of this Law;
4) the policies, controls and procedures from Article 14 paragraph 1 item 2 of this Law are disproportionate to the reporting entity's scope of its business activity, size and type of customer it does business with, and the type of products or services it provides (Article 14 paragraph 2);
5) it does not adopt internal policies, controls and procedures in accordance with Article 14 paragraphs 4 and 5 of this Law;
6) it does not assess the risk of money laundering and terrorist financing in relation to a new product, service or distribution channel it provides within its activity, new business practice, and ways of providing a new service, product or distribution channels, before their introduction (Article 16 paragraph 1);
7) it does not conduct additional measures to mitigate risks and manage risks of money laundering and terrorist financing from Article 16 paragraphs 1 and 2 of this Law, based on an updated risk analysis (Article 16 paragraph 3);
8) it does not verify whether the person acting on behalf of the customer has the right to represent or is authorized by the customer and does not identify the person acting on behalf of the customer in accordance with this Law (Article17 paragraph 2);
9) it does not prescribe in its internal regulations the procedures for implementation of measures from Article 17 paragraphs 1 and 2 of this Law (Article17 paragraph 5);
10) upon the request of the competent supervisory authority from Article 131 paragraph 1 of this Law, it does not submit or it submits inaccurate analyses, documents and other information proving that implemented measures have been adequate to the established risk of money laundering and terrorist financing (Article 17 paragraph 6);
11) it does not inform the Financial Intelligence Unit that it may not conduct one or more measures from Article 17 paragraph 1 of this Law (Article 17 paragraph 7);

12) it does not apply customer due diligence measures when there is a suspicion in the accuracy or authenticity of the data obtained on the customer's identity and customer's beneficial owner (Article 18 paragraph 1 item 4);
13) it does not apply customer due diligence measures when in relation to a transaction, customer, funds or assets there are reasons for suspicion or reasonable grounds to suspect that the property derives from criminal activity or that the money laundering or terrorist financing has been committed, regardless to the amount of the transaction (Article 18 paragraph 1 item 5);
14) it does not apply customer due diligence measures on natural or legal persons trading in goods, when executing occasional transactions in the amount of EUR 10,000 or more, regardless of whether the transaction is carried out as a single transaction or several transactions which appear to be linked (Article 18 paragraph 1 item 6);
15) it does not apply customer due diligence measures upon the collection of winnings or the wagering of a stake, when carrying out one or several linked transactions in the amount of EUR 2 000 or more, when the reporting entity is organizer of games on chance (Article 18 paragraph 1 item 7);
16) it acts contrary to provisions of Article 19 of this Law;
17) it executes a transaction from Article 18 paragraph 1 points 2, 3, 6 and 7 of this Law without previous implementation of the prescribed measures from Article 17 paragraph 1 points 1, 2, and 3 of this Law (Article 20);
18) it does not identify the user or the beneficial owner of the life insurance policy (Article 21 paragraph 2);
19) in the process of transferring insurance policy rights to a third person, it does not, fully or partially, verify the identity of a new user or beneficiary owner at the time of execution of the rights transfer (Article 21 paragraph 4);
20) when verifying the customer's identity from Article 22 paragraph 1 of this Law, it does not obtain a photocopy of personal identity document and does not enter on it the date, time and name and surname of a person that verified a photocopy of the personal identity document and does not keep the photocopy and collected documents in accordance with this Law (Article 22 paragraph 3);
21) it does not perform procedure of identification of the legal representative or authorised person of the customer in accordance with Article 22 paragraphs 1 to 5 and does not obtain data on that person as from Article 117 paragraph 1 item 3 of this Law (Article 22 paragraph 6 indent 1);
22) it does not obtain or verify from the original of written power of attorney or certified photocopy of power of attorney the data on the customer from Article 117 paragraph 1 items 3 of this Law (Article 22 paragraph 6 indents 2 and 3);
23) it does not obtain a written statement on the veracity of data obtained in the process of identifying the customer, its legal representative or an authorised person, if it doubts the veracity of the data obtained or authenticity of documents or other documentation (Article 22 paragraph 7);
24) it establishes a business relationship or executes a transaction, but it determined that the data from the personal identity document differ from the data in CPR (Article 22 paragraph 9);
25) after completed verification, it does not enter the data on the manner of verifying the client's identity in the records from Article 117 paragraph 1 of this Law (Article 22 paragraph 10, Article 23 paragraph 9 and Article 24 paragraph 17);

26) it verifies the customer's identity contrary to the provisions of Article 23 of this Law;

27) it performs video-electronic identification of the customer contrary to the provisions of Article 24 of this Law;

28) it does not, within eight days from the date of submitting the decision from Article 25 paragraph 6 of this Law, define, in the internal regulations, more detailed manner of performing video-electronic identification of the customer (Article 24 paragraph 18);

29) it performs process of identification in electronic manner i.e. video-electronic identification of the customer who is a natural person, entrepreneur or a natural person performing a business activity, its legal representative or authorized person, and does not possess the authorisation to perform electronic identification i.e. video electronic identification (Article 25 paragraph 1);

30) it does not perform process of identification of a customer that is a legal person or business organisation in accordance with Articles 19 and 20 of this Law (Article 26 paragraph 1);

31) it collects data from Article 26 paragraph 3 of this Law through verification of a document that is 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 does not obtain data on all directors of legal person or business organisation from Article 117 paragraph 1 item 3 of this Law (Article 27 paragraph 2);

34) in the process of establishing and verifying the power of attorney of representatives and all directors from Article 27, paragraph 2 of this Law, it does not to obtain power of attorney and keep it in its documentation (Article 27 paragraph 3);

35) in the process of identification of authorised person of legal person and business organisation, it does not obtain data on representative and all directors on whose behalf the authorised person acts, in accordance with Article 28 paragraph 2 of this Law (Article 28 paragraph 2);

36) it does not perform process of identification of a representative or authorised person of a customer in accordance with Articles 27 and 28 of this Law where the customer is trust, other subject or a foreign entity equal to it (Article 29 paragraph 1 item 1);

37) it does not perform process of identification of a trust, other subject or a foreign entity equal to it, pursuant to Article 29 of this Law;

38) it does perform process of identification of the customer's identity in accordance with this Law when the customer enters the premises where special games of chance are organised in casino (Article 30 paragraph 1 item 1);

39) it does not perform process of identification of the customer in accordance with this Law, on any access of a lessee or its representative, or a person it has authorised, to the safe deposit box (Article 30 paragraph 1 item 2);

40) it does not, in the process of identification of the customer from Article 30 paragraph 1 item 1 of this Law, obtain a photocopy of personal identification document of that person in accordance with Article 22 paragraph 3 of this Law, and the written statement by which the customer declares under material and criminal responsibility that it participates in the casino games of chance for its own account and its own benefit (Article 30 paragraph 2);

41) it entrusts the implementation of customer due diligence measures to a third party, and the third party is a shell (fictious) bank or anonymous company or it is from a high-risk third country (Article 32);

42) it does not to keep the collected photocopies of documents and documentation under the provisions of this Law (Article 33 paragraph 3);

43) it assesses that there is suspicion in the validity of the implemented customer due diligence measures by a third party, or the veracity of obtained data and documentation on the customer, and does not idirectly implement those measures (Article 34 paragraph 1);

44) it does not prescribe, in an internal regulation, 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 does not collect data on the payer and the payee 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 does not check the accuracy of the data collected on 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 does not prescribe, in the internal regulation, the procedures for verifying the completeness of the data in accordance with Article 35 paragraphs 2 to 9 of this Law (Article 35 paragraph 12);

48) it does not check whether the data on the payer and payee are 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 does not verify the accuracy of data collected from 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 does not prepare an internal instructions, including, as necessary, ex-post monitoring or real-time monitoring, if the payment order form or electronic message accompanying funds transfer does not contain accurate and complete data from Article 35 of this Law (Article 37 paragraph 1);

51) it does not warn or inform payment service provider of payer that it often does not submit correct and full data in accordance with Article 35 of this Law and it does not determine the time period within which the payment service provider of payer must harmonise its activities with this Law (Article 37 paragraph 3);

52) it does not to refuse future transfers of funds or limit or terminate business cooperation with the payment service provider of payer, if the payment service provider of payer does not often submit accurate and complete data in accordance with Article 35 of this Law (Article 37 paragraph 4);

53) it does not notify the Central Bank of Montenegro on the payment service provider of payer who often does not submit accurate and complete data in accordance with Article 35 of this Law and on the measures that it has taken against this person in accordance with Article 37 paragraphs 3 and 4 of this Law (Article 37 paragraph 5);

54) it does not determine whether the lack of accurate and complete data from Article 35 of this Law present reasons for suspicion in money laundering or terrorist financing and if it does not notify Financial Intelligence Unit on that, in accordance with the Article 66 paragraphs 6, 8 and 10 of this Law (Article 37 paragraph 6);

55) it does not ensure that all information on 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 does not prepare an internal instructions, including, as necessary, ex-post monitoring or real-time monitoring, if the form of payment order or electronic message accompanying the funds transfer do not contain accurate and complete data from Article 35 of this Law (Article 38 paragraph 2);

57) it does not act in accordance with the Article 37 paragraphs 2 to 7 of this Law when the payment order form or the electronic message accompanying the transfer of funds does not contain accurate and complete data from Article 35 of this Law (Article 38 paragraph 3);

58) it does not establish the beneficial owner of the legal person, business organisation, trust, other subject or foreign entity equal to it by collecting data from Article 44 of this Law (Article 42 paragraph 1);

59) it does not print the extract from the Register from Article 42 paragraph 2 of this Law and does not state the date and time and the personal name of the person who performed the checks;

60) in the process of data verification on beneficial owner in accordance with Article 42 paragraphs 2 and 3 of this Law, it determines that there is a discrepancy in the data and it does not submit such data to the Financial Intelligence Unit or the administrative body competent for tax collection (Article 42 paragraph 4);

61) in the process of establishing the beneficial owner, it does obtain documentation based on which it is possible to determine the ownership structure and controlling member of the customer and data on the beneficial owner (Article 42 paragraph 6);

62) it does not conduct procedure of verification of data on the beneficial owner in accordance with Article 42 paragraph 7 of this Law(Article 42 paragraph 7);

63) it does not obtain a photocopy of the personal identification document of the beneficial owner in accordance with Article 22 paragraph 3 of this Law (Article 42 paragraph 8);

64) in the process of collecting data from 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 documents and other documentation from which the data were obtained and does not obtain a written statement from the customer's representative or authorised person on the veracity of obtained data (Article 42 paragraph 9);

65) it does not keep records on the measures taken to determine the beneficial owner from Article 42, paragraph 1 of this Law(Article 42 paragraph 11);

66) it does not enter the prescribed data on beneficial owners and changes in beneficial ownership into the Beneficial Owners Register of within eight days from the date of registration in the CBR or the Tax Register, or within eight days from the change of data on the beneficial owner (Article 43 paragraph 3);

67) it does not check and confirm the accuracy of its own data in the Beneficial Owners Register, once a year, no later than 31st March of the current year (Article 43 paragraph 5);

68) the entity whose beneficial owner does not submit data from Article 44 paragraph 1 point 2 indents 1, 2 and 4 for their entry into the Register of Beneficial Owners (Article 43 paragraph 6);

69) it does not,upon the request of the administrative authority competent for tax collection, provide documentation based on which it is possible to determine the ownership structure and the controlling member of the customer, and does not collect data on the beneficial owner (Article 48 paragraph 3);

70) it does not to implement customer due diligence measure, including control of transactions and monitoring of sources of funds with which the customer operates (Article 49 paragraphs 1);

71) it does not implement measures from Article 49 paragraph 2 of this Law;

72) it does not ensure and adjust the scope and timeline of the implementation of the measures from 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 , i.e. in dealing with a customer (Article 49 paragraph 3);

73) it does not perform control of a customer once a year, and at least a year after the last control has been performed, and a customer 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 from 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 does not obtain additional data from Article 50 paragraph 3 items 1 and 2;

75) does not to call the customer to verify all relevant information when it establishes data discrepancy (Article 50 paragraph 6);

76) It does not apply enhanced customer due diligence measures when a higher risk of money laundering and terrorist financing is determined in the guidelines on risk analysis from Article 12 paragraph 5 of this Law (Article 52 paragraph 1 item 7);

77) it does not 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 does not implement enhanced customer due diligence and in all other cases when it estimates that there is, or could be, a higher risk of money laundering and terrorist financing in relation to the customer, group of customers, country or geographical area, business relationship, transaction, product, service and distribution channel (Article 52 paragraph 2);

79) when establishing a correspondent relationship that includes the execution of payments with a credit or other similar financial institution with head office outside the European Union or in a high-risk third country, and who is a respondent, in addition to the measures from Article 17 of this Law, it does not take additional measures (Article 53 paragraph 1 items 1 to 8);

80) before establishing a correspondent relationship with the respondent, it does not obtain written consent from a senior management to establish that business relation (Article 53 paragraph 2);

81) it does not define by an agreement its responsibility and the respondent's responsibility when concluding the correspondent relationship (Article 53 paragraph 3);

82) it does not revise 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 financial institution with head office outside the European Union or in a high-risk third country, without having previously taken measures or some of the measures from Article 53 paragraphs 1 to 4 of this Law (Article 53 paragraph 7 Item 1);

84) it establishes or continues a correspondent relationship with a credit or other financial institution that is based outside the European Union or in a high-risk third country, if the credit or other financial institution does not have an established controls of the system for the prevention of money laundering and terrorist financing or does not implement laws and other regulations from the area 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 financial institution with head office outside the European Union or in a high-risk third country, if a

credit or other financial institution operates as a shell(fictious) bank, i.e. if it establishes correspondent or other business relationships and carries out transactions with shell (fictious) banks (Article 53 paragraph 7 item 3);

86) before establishing a business relationship with the customer, it fails to check in the Register from Article 55 of this Law whether the customer, its legal representative, an authorised person, or the beneficial owner of the customer is a politically exposed person (Article 54 paragraph 1);

87) when implementing enhanced customer due diligence in relation to a customer or its beneficiary owner who is a politically exposed person, in addition to the measures from Article 17 of this Law, it does not take adequate measures and determine the origin of property and funds included in a business relationship or transaction with that customer (Article 56 paragraph 1 item 1);

88) when implementing enhanced customer due diligence in relation to a customer or its beneficial owner who is a politically exposed person, in addition to the measures from Article 17 of this Law, it 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 manager for the continuation of the business relationship if the business relationship with the customer has already been established (Article 56 paragraph 1 item 2);

89) when implementing enhanced customer due diligence in relation to a customer or its beneficial owner who is politically exposed person, in addition to measures from Article 17 of this Law, it does not establish whether a client who is a politically exposed person is the beneficial owner of a legal person, business organization, trust and other person, i.e. foreign entity equal to it, or a natural person with the head office in a foreign country, on whose behalf a business relationship is being established or a transaction is being carried out or other customer's activity performed (Article 56 paragraph 1 item 3);

90) when conducting enhanced customer due diligence in relation to a customer or its beneficial owner who is a politically exposed person, in addition to the measures from Article 17 of this Law, after establishing a business relationship, it does not monitor with special attention on 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) in accordance with the guidelines from Article 12 paragraph 5 of this Law, it does not define in an internal regulation the procedures that are based on risk analysis, 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 and when performing customer due diligence of that client and the beneficial owner (Article 56 paragraph 2);

92) when providing custody services to the customer, in addition to the measures from Article 17 of this Law, it does not implement adequate measures and determine the origin of property and funds included in the business relationship or transaction with that customer (Article 57 paragraph 1 item 1);

93) when providing custody services to the customer, in addition to the measures from Article 17 of this Law, it does not obtain the written consent of senior manager before establishing the business relation with that customer, and if the business relation has already been established , it does not obtain written consent of senior manager to continue this business relationship (Article 57 paragraph 1 item 2);

94) when providing custody services to the customer, in addition to the measures from Article 17 of this Law, it does not establish whether the customer concludes a contract on the

performance of custody services on its behalf and for its 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 from Article 17 of this Law, during each transaction it does not determine for whose account the sub-custody performed the transaction (Article 57 paragraph 1 item 4);

96) it cannot implement measures from Article 57 paragraph 1 of this Law, but it establishes business relationship or does not terminate already established business relationship (Article 57 paragraph 2);

97) in case of complex and unusually large transactions , as well as the transactions that are executed in an unusual manner or that have no clear economic justification or legal purpose or deviate from the usual or expected customer's business activity, for which it was not possible to determine whether they were suspicious transactions, it does not, in addition to measures from Article 17 of this Law, take measures from Article 58 paragraph 1;

98) upon the request of the Financial Intelligence Unit or the competent supervisory authority from Article 131 of this Law, it does not make available the results of the analysis from Article 58 paragraph 1 item 6 of this Law (Article 58 paragraph 2);

99) it does not, in the internal regulation, define the criteria for recognizing transactions from Article 58 paragraph 1 of this Law (Article 58 paragraph 3);

100) in the case of establishing a business relationship or carrying out transactions with persons from high-risk third countries or when a high-risk third country is involved in the transaction, it does not, in addition to the measures from Article 17 of this Law, implement additional measures from Article 58 paragraph 1 of this Law (Article 59 paragraph 1 item 1);

101) when establishing a business relationship or executing transactions with persons from high-risk third countries or when a high-risk third country is included in the transaction, it does not, in addition to measures from Article 17 of this Law, obtain a written consent of a senior manager before the establishment of business relationship (Article 59 paragraph 1 item 2);

102) after establishing a business relationship with a customer from a high-risk third country, it does not implement enhanced customer due diligence measures related to the business relationship and transactions carried out by that customer (Article 59 paragraph 2);

103) it does not implement measures from Article 59 paragraphs 1 and 2 of this Law in accordance with the risk assessment of money laundering and terrorist financing that is established in the risk analysis (Article 59 paragraph 3);

104) if, in relation to a customer with an identified lower risk of money laundering and terrorist financing, it does not implement customer due diligence measures in relation to business relationship and control of transactions to the extent defined in accordance with Article 61 paragraph 1 item 3 of this Law (Article 61 paragraph 3);

105) it does not provide that the measures for 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, with head 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 legislation of the European Union (Article 62 paragraph 1);

106) it opens or keeps anonymous accounts, anonymous safe deposit box, savings book, or coded securities accounts or bearer securities 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 continue correspondent relationships with a credit institution that operates or could operate as a shell (fictious) bank or with other credit institution that is known for allowing shell banks to use its accounts (Article 64 paragraph 2);

109) it receives or makes a payment in cash in the amount of EUR10,000 or more or if a payment is received or made in two or more connected transactions in the total amount of EUR10,000 or more (Article 65 paragraphs 1 and 2);

110) it does not submit to the financial intelligence unit, without delay and the latest within three working days from the day of transaction execution, accurate and complete data on implemented customer due diligence measures from Article 117 paragraphs 1 to 6 of this Law, for each cash transaction in the amount of EUR 15,000 or more or cashless transaction in the amount of EUR100,000 or more (Article 66 paragraph 1);

111) it does not submit to the Financial Intelligence Unit, without delay and the latest within three working days from the day of transaction execution, accurate and complete data on implemented customer due diligence measures from Article 117 paragraphs 1 to 6 of this Law for each transaction in the amount of EUR 10,000 or more (Article 66 paragraph 2);

112) it does not submit to the Financial Intelligence Unit, without delay and the latest within three working days from the day of transaction execution, accurate and complete data on implemented customer due diligence measures from Article 117, paragraphs 1 to 6 of this Law for each transaction in the amount of EUR 10,00or more, carried out on the accounts of legal and natural persons in high-risk third countries or if that transaction involves high-risk third countries (Article 66 paragraph 3);

113) it does not refrain from the execution of a suspicious transaction (regardless to the amount) until the order from Article 93 of this Law is issued, and does not, without delay, inform the Financial Intelligence Unit about it and does not provide to the Financial Intelligence Unit data on implemented customer due diligence measures from Article 117 paragraphs 1 to 6 and paragraph 8 of this Law (Article 66 paragraph 6);

114) it does not deliver to the Financial Intelligence Unit the data from Article 66 paragraph 6 before the execution of transactions and does not specify the deadline within which the transactions should be executed (Article 66 paragraph 7);

115) it does not deliver to the financial intelligence unit, without delay and at the latest the next working day after the day of transaction execution, data on implemented customer due diligence measures from 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 from Article 66 paragraph 8, it does not 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 does not provide to the Financial Intelligence Unit, without delay, accurate and complete data on implemented the customer due diligence measures from Article 117 paragraphs 1 to 6 and paragraph 8 of this Law in relation to funds or other property for which it knows or has reason to suspect that these represents proceeds from criminal activity or are related to money laundering or terrorist financing (Article 66 paragraph 10);

118) it does not inform the Financial Intelligence Unit, without delay, that the customer has asked for advice on money laundering or terrorist financing (Article 66 paragraph 11);

119) it does not inform the Financial Intelligence Unit, without delay and the latest within three working days from the day of executed review, on every review of data, information

and documentation carried out by the supervisory authority from Article 131 of this Law (Article 66 paragraph 12);

120) it does not submit data, explanations and notifications to the Financial Intelligence Unit in the manner defined by Article 66 paragraph of this Law;

121) within 60 days from the day of establishment and the beginning of business activity, it does not designate compliance officer for the prevention of money laundering and terrorism financing and at least one deputy of that person (Article 69 paragraph 1);

122) it does not deliver to the Financial-Intelligence Unit the notifications from Article 69 paragraphs 1, 2 and 6 of this Law (Article 69 paragraph 7);

123) it does not deliver the report, from Article 76 paragraph 1 item 12 of this Law, to the competent supervisory authority, from Article 131 of this Law, upon the request of that supervisory authority, within three days from the day of the request reception (Article 76 paragraph 2);

124) it does not provide defined conditions to the compliance officer for the prevention of money laundering and terrorist financing (Article 77 paragraph 1);

125) it does not provide regular professional training and development in the area of prevention and detection of money laundering and terrorist financing for all employees who participate in the area of prevention and detection of money laundering and terrorist financing at the reporting entity (Article 78 paragraph 1);

126) it does not prepare professional training and development program from Article 78 paragraph 1 of this Law, within the prescribed deadline (Article 78 paragraph 3);

127) it does not order or control the application of rules from Article 79 paragraphs 1 and 2 of this Law in the business units and entities under the reporting entity's majority ownership in other countries (Article 79 paragraph 3);

128) it does not ensure regular internal control and audit of the implementation of the policies, controls and procedures for prevention of money laundering and terrorist financing, or does not ensure execution of affairs for 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) does not organize an independent internal audit, whose scope includes regular assessment of the adequacy, reliability and efficiency of the money laundering and terrorist financing risk management system, when the law regulating the reporting entity's business activity defines the obligation to have an independent internal audit (Article 80 paragraph 2);

130) it does not use the list of indicators from Articles 82 and 83 of this Law when establishing reasons for suspicion that the property derives from criminal activity or that the money laundering or terrorist financing has been committed and other circumstances related to that suspicion (Article 81);

131) it does not develop its own list of indicators for identifying suspicious customers and transactions (Article 83 paragraph 1);

132) it does not deliver to the Financial Intelligence Unit, without delay and within eight days from the day of receipt of the request and in the prescribed manner, accurate and complete data, information and documentation at its disposal (Article 90 paragraph 4);

133) it does not deliver to the Financial Intelligence Unit data, on the requests marked "URGENT", information and documents without delay and the latest within 24 hours of the receipt of the request (Article 90 paragraph 5);

134) it does not provide the requested data, information and documentation to the Financial-Intelligence Unit, in the manner prescribed by the regulation from Article 66 paragraph 15 of this Law (Article 91 paragraph 2);

135) it does not, without delay, take measures in accordance with Article 93 paragraphs 1 and 4 of this Law (Article 93 paragraph 5);

136) it does not act upon the request from Article 95 paragraph 2 of this Law (Article 95 paragraph 2);

137) it does not deliver data to the Financial Intelligence unit before execution of transaction or concluding a business relationship (Article 95 paragraph 3);

138) it does not deliver data to the Financial Intelligence Unit without delay, and at the latest on the next working day from the date of executing the transaction or concluding business when, due to the nature of the transaction, business or other justified reasons, it cannot act in accordance with Article 95 paragraph 3 of this Law and does not justify in detail the reasons why it did not act in accordance with Article 95 paragraph 3 of this Law (Article 95 paragraphs 4 and 5);

139) it does not notify the Financial Intelligence Unit, without delay if, in the course of performing its activities, it discovers facts directing to a possible connection with money laundering and related predicate criminal offences or terrorist financing (Article 114 paragraph 1);

140) upon the request of the Financial-Intelligence Unit, it does not provide data, information or documentation directing to a possible connection with money laundering and related predicate criminal offences or terrorist financing, in accordance with the Law (Article 114 paragraph 2);

141) it does not quarterly submit to the Financial Intelligence Unit , by electronic means, data on each collective custody account, credit institution or other financial institution with which that custody account is opened, and on the number of transactions and total turnover on that collective custody account (Article 114 paragraph 3);

142) it does not keep records from Article 116 paragraph 1 of this Law;

143) if does not keep the records from Article 116 paragraph 1 in the manner that will ensure the reconstruction of individual transactions (including amounts and currency) that could be used as evidence in the process of detecting customers' criminal activities (Article 116 paragraph 2);

144) the records that it keeps in accordance with the Law do not contain data prescribed in Article 117 of this Law;

145) it discloses the data from Article 123 paragraph 1 items 1 to 4 of this Law to the customer or a third party (Article 123 paragraph 1);

146) it does not take the necessary measures to protect the compliance officer for the prevention of money laundering and terrorist financing and other employees that implement the provisions of this Law, from threats and other unfavourable or discriminatory actions aimed at their physical or psychological integrity (Article 125);

147) it uses the personal data that it receives in accordance with this Law for purposes for which these data are not supposed to be processed (Article 126 paragraph 1);

148) it does not 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 the period of ten years after the termination of the customer's business relationship, performed occasional transactions, entry of the customer in to the casino and

premises where other games of chance are organised or access to the safe, unless a longer record period is prescribed by a specific law (Article 127 paragraph 1 and 2);

149) it does not keep data and accompanying documentation on the compliance officer for the prevention of money laundering and terrorist financing and his/her deputy, the professional training and development of employees in the area of prevention of money laundering and terrorist financing and the implementation of internal control and audit measures, for four years from the expiry of the license, and the completed professional training and development and completed internal control and audit (Article 127 paragraph 3);

150) does not deliver, within eight days from the day of submitting the request, accurate and complete data, information and documentation necessary for carrying out supervision upon the request of the competent authority from Article 131 of this Law (Article 132 paragraph 7).

The responsible person in a legal person and a natural person shall be fined in an amount from EUR500 to EUR2,000 for the misdemeanour from paragraph 1 of this Article.

An entrepreneur shall be fined in an amount from 500 EUR to 6,000 EUR for the misdemeanour from paragraph 1 of this Article.

A prohibition on carrying out a profession, business activity and duty may be imposed to a legal person and entrepreneur, responsible person in the legal person and natural person for up to six months.

The authorised police officer of the financial intelligence unit shall submit the request for initiating the misdemeanour proceeding for misdemeanour paragraph 1 point 144 of this Article.

For misdemeanours of credit institutions and other financial institutions from paragraph 1 of this Article, misdemeanour proceeding can not be initiated if three years passed since the day when a misdemeanour has been committed.

Article 138

A natural person that performs business activity shall be fined for misdemeanour in an amount from EUR 500 to EUR 2,000 when:

1) it does not submit to the Financial Intelligence Unit, without delay and within three days from the date of conclusion of the legal affair, accurate and complete data on implemented customer due diligence measures from Article 117 paragraphs 1 to 6 of this Law for every transaction based on a pre-contract, a contract regarding real estate with the value of EUR 15,000 or more and a loan contract with value of EUR 10,000 or more (Article 66 paragraph 4);
2) it does not submit to the Financial Intelligence Unit, without delay, and within three days from the day of conclusion of the legal affair, a photocopy of the contract in electronic form or a photocopy of the statement of the natural person who is the buyer, on the origin of the money in relation to contracts for whose implementation is used cash (Article 66 paragraph 5).

A prohibition of performing profession, business activity or duty, may be imposed to natural person who performs a business activity for up to six months for the misdemeanor from the paragraph 1 of this Article.

XI. TRANSITIONAL AND FINAL PROVISIONS

Deadline for Adoption of bylaws

Article 139

The bylaws for the implementation of this Law shall be adopted within three months from the date of entry into force of this Law.

Until the adoption of the bylaws from paragraph 1of this Article, unless contrary to the Law, the regulations adopted pursuant to the Law on the Prevention of Money Laundering and Terrorist Financing (OGM 33/14, 44/18, 73/19, 70/21) shall apply.

Conducting customer due diligence measures in already established business relations

Article 140

The reporting entity shall implement the customer due diligence measures from Article 17 onto the customers from Article 18 paragraph 2 of the Law with which it has already established business relations, when executing the first transaction after this Law enters into force.

Entering and updating the data in the Registry of beneficial owners

Article 141

Business entities, legal persons, associations, institutions, political parties, religious communities, artistic organisations, chambers, trade Unions, employers' associations, foundations or other business entities, a legal person that receives, manages or allocates the funds for certain purposes, foreign trust, foreign institution or foreign legal entity equal to it that receives, manages or allocates the funds for certain purposes, who have been already recorded in CB R or in the registry of tax payers but have not entered or updated data in the Registry of Beneficial Owners shall enter or update these data within 30 days from the date of entry in the force of the regulation from Article 45 paragraph 4 of the Law.

Establishing records

Article 142

Reporting entities, public and other authorities and institutions shall establish records that they shall keep pursuant to the Law within three months from the date of entry into force of this Law.

Harmonisation of business activities

Article 143

For the purpose of the prevention of money laundering and terrorist financing, the reporting entities shall harmonise their business activities with this Law within six months as of the effective date of the regulations from Article 139 paragraph 1 of this Law.

Obtaining Licence

Article 144

Compliance officers for the prevention of money laundering and terrorism financing and their deputies designated before the date of entry of this Law shall obtain licences from this Law within six month as of the effective date of the regulations from Articles 71 and 72 of this Law.

Until obtaining the licence from paragraph 1 of this Article, compliance officers for the prevention of money laundering and terrorism financing and their deputies shall continue to work in accordance with this Law.

If compliance officers for the prevention of money laundering and terrorism financing and their deputies do not obtain the licence from this Law within the deadline from paragraph 1 of this Article, they shall lose the status of the compliance officer for the prevention of money laundering and terrorism financing or deputy compliance officer.

Deadline for establishing registers of accounts and safe deposit boxes

Article 145

The Central Bank of Montenegro shall establish registers of accounts and safe deposit boxes from Article 112 of this Law within 12 months from the date of entry into force of this Law..

Complying the reporting entities' internal regulations and internal organisation

Article 146

Reporting entities shall comply internal regulations and internal organisation with this Law within six months from the date of entry into force of this Law.

The Rulebook on manner of work of the compliance officer, the manner of conducting the internal control, data keeping and protection, manner of record keeping and employees professional training shall apply until the adoption of internal regulations from Articles 77, 78 and 80 of this Law.

On-going Procedures

Article 147

The initiated procedures had not been finally disposed of shall be ended by applying the Law on the Prevention of Money Laundering and Terrorist Financing (OGM 33/14, 44/18, 73/19, 70/21).

Cessation of effect of legal provisions

Article 148

Procedures that have been initiated until the date when this Law came into force shall be completed

in accordance with the Law on the Prevention of Money Laundering and Terrorist Financing (OGM 33/14, 44/18, 73/19, 70/21).

Entry into force

Article 149

This Law shall enter into force on the day of its publication in the Official Gazette of Montenegro.

∗ This Law has transposed the provisions of the 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, the 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 the 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.

No.: 04-3/23-1/4
EPA 100 XXVIII
Podgorica, 11th December 2023
The Parliament of Montenegro of 28th convocation
The Speaker,
Andrija Mandić, MP