Unofficially consolidated translation

LAW
ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

The Law is published in the Official Gazette of Montenegro, No. 110/23, 65/24, 24/25

I. BASIC PROVISIONS

Subject matter
Article 1

This Law shall regulate measures and actions undertaken for the purpose of preventing and detecting money laundering and terrorist financing, as well as affairs, powers and manner of work of the organizational unit of the state administration authority competent for internal affairs that performs police affairs (hereinafter: the Police) which performs the activities related to the prevention of money laundering and terrorist financing (hereinafter: the 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 obtained 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 their 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 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 are obtained from criminal activity or from participation in such activity;
4) participating in commission, associating in order to commit, attempting to commit and aiding, abetting, facilitating and advising in relation to the commission of any of the actions referred to in items 1), 2) and 3) of this paragraph.

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

Activities referred to in paragraph 1 of this Article shall also be considered as money laundering in the case when 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 or in another country.

Terrorist financing
Article 3

In the context of this Law, terrorist financing shall, in particular, mean the following:

1) providing, making available or collecting funds or property, in any way, directly or indirectly, with the intention of using them or with the knowledge 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 a terrorist act within the meaning of this Law,
   - for financing organizations whose aim is to commit the acts referred to in indent 1 of this item or members of those organizations or individuals whose aim is to commit such acts, or
   - by terrorists or by terrorist organizations for any purpose;
2) encouraging or assisting in providing or collecting the funds or property referred to in item 1 of this Article.

Reporting entities
Article 4

Measures for preventing and detecting money laundering and terrorist financing shall be conducted before, during and after the completion of any affairs of receiving, investing, converting, keeping or other form of disposing of money or other property, or transactions. Measures referred to in paragraph 1 of this Article shall be undertaken by legal persons, business organizations, entrepreneurs and natural persons carrying out business activities (hereinafter: the reporting entities), as follows:

1) credit institutions and branches of foreign credit institutions;
2) entities performing the following activities:
   - purchase of receivables;
   - financial leasing;
   - renting safe deposit boxes;
   - factoring;
   - issuing guarantees and other sureties;
   - granting loans and loan mediation;
   - exchange services;
3) payment service providers and electronic money institutions in accordance with the law regulating the provision of payment services and electronic money issuance;
4) Post Office of Montenegro;
5) companies for managing investment funds;
6) companies for managing pension funds;
7) investment companies whose business activities are prescribed by the law regulating the capital market and that provide:
   - investment services in 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 a customer; trading on one's 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: MTF); operation of organized trading facility (hereinafter: OTF);

- ancillary services in 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 them to carry out a transaction in one or more financial instruments, when the transaction involves a company which grants credit or loan; providing general recommendations on capital structure, business strategy and related matters and services relating to merger and acquisition of shares 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 agents in the part related to life insurance;
10) organizers of games of chance;
11) pawnshops;
12) crypto-asset 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, or that undertake to provide, directly or by means of other connected persons, material aid or other assistance or advice on tax matters,
    - providing services of founding legal persons and other business organizations, as well as business or fiduciary services;
    - asset management of property for third parties;
    - renting and intermediation in renting real estate in transactions where the monthly rent amounts to EUR 10,000 or more, or the equivalent of this value,
    - construction of residential and commercial facilities, construction or assembly of prefabricated residential and commercial facilities;
    - issuance and management of payment instruments (e.g. checks, traveller's checks, credit cards, bank promissory notes, payment orders, debit cards), which are not considered payment instruments in accordance with the law regulating payment operations;
    - granting loans and mediating in contracting granting loan activities;

- investment, trade and mediation in real estate trade;
- trade of motor vehicles if the payments are made or received in the amount of EUR 10,000 or more, regardless of whether it is one or several linked transactions;
- trade of vessels and aircrafts, as well as related service activities, if the payments are made or received in the amount of EUR 10,000 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, when the payment is made or received in the amount of EUR 10,000 or more, regardless of 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 ports, free zone or warehouse, if payments are made or received in the amount of EUR 10,000 or more, regardless of whether it is performed in a single or more linked transactions.

14) founders, operators, and users of zones and warehouses engaged in business activities within the free zone.

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

1) provide 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, operating or managing a business organization,
   - founding, operating or managing an institution, fund, business organization or other similar form of organization;
2) execute a financial transaction or transaction related to real estate on behalf and for account of a customer.

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

The Government of Montenegro (hereinafter: Government) may define other reporting entities that shall undertake the measures referred to in paragraph 1 of this Article where, due to 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 particular 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 business or activity, when, upon a conducted risk assessment, a lower risk of money laundering and terrorist financing is determined.

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

Exceptions from Application

Article 4a

The provisions of this Law regulating crypto-assets shall not apply to:

1) persons providing crypto-asset services exclusively to their parent companies, their subsidiaries, or other subsidiaries of their parent companies;
2) a liquidator or bankruptcy administrator involved in the liquidation or bankruptcy process, except in the case of a plan to support the regular redemption of any asset-related token applicable in the event of bankruptcy, liquidation, remediation, or revocation of the license of the holder;
3) The European Central Bank, the central bank of a European Union member state when acting in its capacity as a monetary authority, and other public bodies of European Union member states;
4) The European Investment Bank and its subsidiaries;
5) The European Financial Stability Facility and the European Stability Mechanism;
6) international organizations within the meaning of public international law.

Use of gender-sensitive language
Article 5

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

Meaning of terms
Article 6

The certain terms used in this Law shall 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, established for a longer period of time and operating in an organized manner 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 kind of commission, or participation in the commission of any act that is prescribed as a criminal offence;
6) **customer** means a domestic or foreign legal person, business organization, entrepreneur, natural person, trust, other person, or a subject equal to them, carrying out a transaction or establishing business relationship with a reporting entity;
7) **other person, or a subject equal to them**, 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** means a person appointed by a reporting entity, authorised 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 established and operating in accordance with the law regulating credit institutions;
10) **financial institution** means a reporting entity referred to in Article 4 paragraph 2 items 2 to 9 and item 13 indents 1 and 7 of this Law, including its branches, regardless of whether their head office is in Montenegro, EU Member State or another country;
11) **financial group** means a group comprised of:

- a parent company with their head office in Montenegro, subsidiary companies and companies where these companies hold a direct or indirect participation in capital or voting rights of at least 20% and are included in the annual consolidated financial statements in accordance with the law;
- companies that are mutually linked by joint management;
- legal or natural persons holding a direct or indirect participation in capital or voting rights 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 referred to in Articles 82 and 83 of this Law or on the 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 the 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 to 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 to 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 settlement system) opens in the system of the central clearing depository company as a 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 their possession and disposal;
20) **occasional transaction** means a transaction executed by a customer who is not in a business relationship with the reporting entity;
21) **suspicious transaction** means any transaction or attempt to execute a transaction of funds or property for which it is estimated that, based on indicators for recognising suspicious transactions and customers in accordance with this Law, bylaws adopted on the basis of this Law and internal acts of the reporting entities, or based on other objective circumstances and facts, there are reasons for suspicion that they represent material benefit acquired by 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:
    - where one credit institution as a correspondent provides banking services to other credit institution as to a respondent, including providing a current or other liabilities accounts, as well as related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services, and
    - between and within credit institutions, as well as financial institutions, including cases where similar services are provided through a correspondent institution to a respondent institution, including relationships established for securities transactions or fund transfers, or relationships established for transactions related to crypto-assets or crypto-assets transfers;
24) **shell (fictious) bank** means a credit institution or a financial institution, or another similar institution that carries out activities equivalent to those carried out by credit institution or financial institution, which is registered in a country where it has no physical presence, it does not carry out activity, has no business premises, employees, managing bodies, management and which is not related to a financial group subject to the 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 tangible or intangible nature, movable or immovable, securities, crypto-assets and other documents (in any form, including electronic or digital), evidencing property rights;
26) **funds** mean a form of property and represent financial assets and benefits of any kind, including:

- money, checks, cash receivables, bills of exchange, remittances and other means of payment;
- funds deposited with a reporting entity;
- financial instruments, specified in the law regulating the capital market, which are traded through appropriate offering, including shares and stakes, certificates, debt instruments, bonds, guarantees and derivative financial instruments;
- other documents evidencing the right to the financial assets or other financial sources;
- interests, dividends and other income from the funds;
- receivables, credits and letters of credit.

27) **money** means cash (domestic and foreign), funds onto accounts and electronic money;
28) **payer** means a natural or a 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 gives order for the transfer of funds;
29) **payee** means a natural or a 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 the payer and the payee are the same person, or whether the payer's payment service provider and the payee's payment service provider are the same person, 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 operations,
    - 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 payment service provider that is not the payment service provider of the payer or of the payee, but receives and transfers funds on behalf of the payment service provider of the payer or of the payee or of another intermediary in the transfer of funds;
33) **business relationship** means a business, professional or commercial relationship related to the professional activities of the 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 participating in the organizing games of chance system,
    - entering into a contract on the purchase of investment units and/or shares in an investment fund, in accordance with the law regulating the operations of investment funds,
    - entering into a contract 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 a 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 person or another subject of law;
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 agency activities issued by the regulatory authority competent for insurance activities;
41) **trust, other person or a subject of international law equal to them** (Treuhand, Fideicomiso, Fiducie, and similar) 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 subject of international law, the position of a director or a secretary of a business organization, a partner in a company or similar position in the structure of business organization, other legal persons or arrangements,
- provision of services related to a head office, business address, correspondent or other address and other related services to a business organization or other legal person or arrangement,
- performance of functions or enabling other person to carry out the tasks of the trustee of a fund or similar subject of international law that receives, manages or allocates assets for certain purposes, excluding companies for managing investment or 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;
- performance of functions or the appointment of other person to manage trust established by explicit statement (express trust), business organization, another legal person or arrangement;

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 executing payment transactions, which represents a cash receivable to 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 services 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) **crypto-asset** means a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology (DLT) or similar technology, including electronic money tokens, but it does not include crypto-asset that qualifies as one or more of the following:
    - a financial instrument, in accordance with the law regulating the capital market,
    - a deposit, including structured deposits, in accordance with the law regulating deposit protection,
    - funds that do not qualify as e-money tokens,
    - securitization, in accordance with the law regulating the capital market,
    - non-life or life insurance products within the meaning of the law regulating the terms and manner of performing insurance activities,
    - pension products whose primary purpose is to provide the investor with an income in retirement and that entitle the investor to certain benefits,
    - an occupational pension insurance product covered by the law regulating pension funds or the law regulating insurance and reinsurance,
    - accounting unit of voluntary pension funds in accordance with the law regulating voluntary pension funds,
    - pension insurance in accordance with the law regulating pension and disability insurance,
    - a pan-European Personal Pension Product in accordance with the law governing such products,
    - a social security system in accordance with a special law,
    - individual pension insurance products for which employer financial contributions are stipulated by law and where the employer or the employee cannot choose the pension product or provider,
    - crypto-asset that is unique and not fungible with other crypto assets;
47) **official currency** means a legal payment instrument issued by the 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 the like);

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, recognised, approved or accepted by the state, and for legal persons and business organizations, the collection of data from appropriate documents and their comparison 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 reviewing 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 an insight into the register where the legal person or business organization is registered or in another appropriate public register or by checking the original or certified photocopy of a document from the register where the legal person or business organization is registered, or the original or certified photocopy of another document from the appropriate public register;
52) **electronic money token** means a type of crypto-asset that purports to maintain a stable value by referencing the value of the official currency;
53) **crypto wallet** means a wallet that serves for keeping a private cryptographic key and allows users to securely keep, send and receive crypto-assets;
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 of money laundering or terrorist financing in the context of this Law, or, based on the data from relevant international organizations it does not meet the international standards in the area of the prevention money laundering and terrorist financing;
55) **a personal identification document** means an identity card, passport, as well as an identification document for asylum seekers or an identification document for a foreigner under subsidiary protection issued in Montenegro;
56) **electronic personal identification document** means an identity card and passport that contains a photo of a person and a contactless chip containing the photo, personal and other data of that person and that is issued by the competent authority;
57) **records of issued personal identification documents** means 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 format 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 with the competent authority in Montenegro,
    - entrepreneurs and natural persons with their head office or residence in Montenegro, who perform business 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 representative offices of Montenegro abroad, employees of those representative offices 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 the electronic identification and electronic signature;
62) **electronic identification means** is 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 the 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 the supervision;
67) **ICAO Doc 9303 recommendations** mean international recommendations, recognized in the European Union standards related to the issuance of identification documents;
68) **linked transactions** mean two or more transactions that can be considered interconnected due to the period in which they are executed, the recipient and the sender, the method of executing the transaction, the reason for executing the transactions, or other factors based on which the transactions can be considered linked;
69) **crypto-asset service provider** means a legal person, business organization, entrepreneur, and natural person whose occupation or business is the provision of one or more crypto-asset services to customers on a professional basis;
70) **crypto- asset services** mean:
    - custody and administration of crypto-assets on behalf of customers,
    - operation of a trading platform for crypto-assets,
    - exchange of crypto-assets for official currency,
    - exchange of crypto-assets for other crypto-assets,
    - execution of orders for crypto-assets on behalf of customers,
    - placing of crypto-assets,
    - reception and transmission of orders for crypto-assets on behalf of customers,
    - providing advice on crypto-assets,
    - portfolio management of crypto-assets,

- providing transfer services for crypto-assets on behalf of customers;

71) **custody and administration of crypto-assets on behalf of customers** means the safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys;
72) **operation of a trading platform for crypto-assets** means the management of one or more multilateral systems, which bring together or facilitate the bringing together of multiple third-party purchasing and selling interests in crypto-assets, in the system and in accordance with its rules, in a way that results in a contract, either by exchanging crypto-assets for other crypto-assets, or by exchanging crypto-assets for official currency which is a legal means of payment;
73) **exchange of crypto-assets for official currency** means the conclusion of purchase or sale contracts concerning crypto-assets with customers for official currency by using proprietary capital;
74) **exchange crypto-assets for other crypto-assets** means the conclusion of purchase or sale contracts concerning crypto-assets with clients for other crypto-assets by using proprietary capital;
75) **execution of orders for crypto-assets on behalf of customers** means the conclusion of agreements, on behalf of customers, to purchase or sell one or more crypto-assets or the subscription on behalf of customers for one or more crypto-assets, and includes the conclusion of contracts to sell crypto-assets at the moment of their offer to the public or admission to trading;
76) **placing of crypto-assets** means the marketing, on behalf of or for the account of the offeror or a party related to the offeror, of crypto-assets to purchasers;
77) **reception and transmission of orders for crypto-assets on behalf of customers** means the reception from a person of an order to purchase or sell one or more crypto-assets or to subscribe for one or more crypto-assets and the transmission of that order to a third party for execution;
78) **providing advice on crypto-assets** means offering, giving or agreeing to give personalised recommendations to a customer, either at the request of the customer or on the initiative of the crypto-asset service provider providing the advice, in respect of one or more transactions relating to crypto-assets, or the use of crypto-asset services;
79) **providing portfolio management of crypto-assets** means managing portfolios in accordance with mandates given by customers on a discretionary customer-by-customer basis where such portfolios include one or more crypto-assets;
80) **providing transfer services for crypto-assets on behalf of customers** means providing services of transfer of crypto-assets, on behalf of the customer, from one distributed ledger address or account to another, as well as the use of crypto-ATMs;
81) **crypto-asset account** means an account held by a crypto-asset service provider in the name of one or more persons and that can be used for the execution of transfers of crypto-assets;
82) **originator** means a person holding a crypto-asset account with a crypto-asset service provider, a distributed ledger address or a device allowing the storage and transfer of crypto-assets from that account, distributed ledger address, or device, or, where there is no such account, distributed ledger address, or device, a person that orders or initiates a transfer of crypto-assets;

83) **crypto-asset beneficiary** means a person that is the intended recipient of the transfer of crypto-assets;
84) **transfer of crypto-assets** means any transaction with the aim of moving crypto-assets from one distributed ledger address, crypto-asset account or other device allowing the storage of crypto-assets to another, carried out by at least one crypto-asset service provider acting on behalf of either an originator or a beneficiary, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the crypto-asset service provider of the originator and that of the beneficiary are one and the same;
85) **batch file transfer** means a bundle of several individual transfers of funds or transfers of crypto-assets put together for transmission;
86) **unique transaction identifier** means a combination of letters, numbers or symbols determined by the payment service provider, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, or determined by a crypto-asset service provider, which permits the traceability of the transaction back to the payer and the payee or the traceability of the transfer of crypto-assets back to the originator and the beneficiary;
87) **person-to-person transfer of crypto-assets** means a transfer of crypto-assets without the involvement of any crypto-asset service provider;
88) **intermediary crypto-asset service provider** means a crypto-asset service provider that is not the crypto-asset service provider of the originator or of the beneficiary and that receives and transmits a transfer of crypto-assets on behalf of the crypto-asset service provider of the originator or of the beneficiary, or of another intermediary crypto-asset service provider;
89) **crypto-asset automated teller machine or crypto-ATM** means physical or on-line electronic terminals that enable a crypto-asset service provider to perform, in particular, the activity of transfer services for crypto-assets on behalf of the customer;
90) **distributed ledger address** means an alphanumeric code that identifies an address on a network using distributed ledger technology (DLT) or similar technology where crypto-assets can be sent or received;
91) **distributed Ledger Technology (DLT)** means a technology that enables the operation and use of distributed ledgers;
92) **distributed ledger** means an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism;
93) **consensus mechanism** means the rules and procedures by which an agreement is reached, among DLT network nodes, that a transaction is validated;
94) **DLT network node** means a device or process that is part of a network and that holds a complete or partial replica of records of all transactions on a distributed ledger;
95) **self-hosted address** means a distributed ledger address not linked to either of the following:
    - a crypto-asset service provider
    - an entity not established in Montenegro and providing services similar to those of a crypto-asset service provider,
    - an entity not established in the EU and providing services similar to those of a crypto-asset service provider;

96) **formal nominee arrangement** means a contract between a nominator and a nominee, where the nominator is a legal person or business organization or natural person that issues instructions to a nominee to act on their behalf in a certain capacity, including as a director or shareholder or settlor, and the nominee is a legal person or business organization or natural person instructed by the nominator to act on their behalf;
97) **legal entity identifier** (LEI) means a unique alphanumeric reference code based on the ISO 17442 standard assigned to a legal person;
98) **cryptographic algorithm** means a mathematical process or set of rules used for protecting data, specifically for encrypting and decrypting data;
99) **electronic cheque** means a digital version of a traditional cheque instrument used for payment but in an electronic format.

II. NATIONAL RISK ASSESSMENT

Determining the National Risk Assessment

Article 7

National Risk Assessment of money laundering and terrorist financing (hereinafter: National Risk Assessment) shall include:

- identification and assessment of the risk of money laundering and terrorist financing at the state level;
- typologies of money laundering and terrorist financing, in accordance with the recommendations of the Financial Action Task Force (FATF);
- identification of sectors and activities in relation to which the reporting entities shall apply enhanced due diligence measures and monitoring of customer's business activities and, when needed, establishing the measures that shall be taken for the purpose of the prevention of money laundering and terrorist financing;
- identification of sectors and activities in relation to which the risk of money laundering and terrorist financing has been determined;
- determination of appropriate measures to prevent money laundering and terrorist financing based on identified risks and increasing efficiency in the distribution of available resources for control, mitigation and management of identified risks of money laundering and terrorist financing;
- proposal for the improvement of existing regulations in the area of the prevention and detection of money laundering and terrorist financing for individual 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 developing money laundering and terrorist financing risk assessment;
- 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 of these authorities, to the extent to which these data are available;
- data on activities undertaken at the state level and data on financial and human resources allocated for the fight against money laundering and terrorist financing to the Financial Intelligence Unit, competent authorities referred to in Article 96

paragraph 1 of this Law and competent supervisory authorities referred to in Article 131 paragraph 1 of this Law.

The National Risk Assessment shall be determined by the Government, at least once every three years.

The National Risk Assessment shall be updated as needed.

Coordinating body for developing National Risk Assessment
Article 8

The Government shall establish a coordinating body for the development of the National Risk Assessment and the management of identified risks 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) carry out analyses in the area of money laundering and terrorist financing, prepare reports on the analysis performed and harmonise the cooperation between competent authorities and organizations.

The coordinating body referred to in paragraph 1 of this Article shall comprise a chairperson, members and a secretary.

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

Coordination and harmonisation of the work of the coordinating body referred to in paragraph 1 of this Article shall be carried out by the Financial Intelligence Unit.

The Government shall prescribe in more detail the composition of the coordinating body, the manner of carrying out the tasks, as well as other issues of importance for the work of the coordinating body referred to in paragraph 1 of this Article.

Publication of data from the National Risk Assessment
Article 9

Certain parts or data from the National Risk Assessment may be classified with the appropriate level of confidentiality in accordance with the law regulating data confidentiality.

The parts or data from the National Risk Assessment that are not classified with the appropriate level of confidentiality shall be published on the website of the Financial Intelligence Unit.

In order to facilitate their own assessment of the risk of money laundering and terrorist financing with the reporting entities, the Financial Intelligence Unit, in addition to the parts or data referred to in paragraph 2 of this Article, may also publish other data from the National Risk Assessment on its website.

Report on implementation of the National Risk Assessment
Article 10

The Financial Intelligence Unit shall submit a report to the Government on the implementation of the National Risk Assessment at least once a year.

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

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

III. OBLIGATIONS OF REPORTING ENTITIES

1. Measures and activities undertaken by reporting entities

Types of measures and activities

Article 11

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

1) identify the risks and carry out money laundering and terrorist financing risk assessment and establish policies, controls and procedures and undertake activities for decreasing the risk of money laundering and terrorist financing;
2) perform the identification of the customer, monitor the business relationship and control customer transactions (hereinafter: customer due diligence measures – CDD measures);
3) where the reporting entity is a credit institution or another financial institution, put in place adequate information system which will provide automated support for the assessment of the risk of money laundering and terrorist financing in relation to the customer, ongoing monitoring of business relationships of the customer, the control of the transactions and the automated recognising of suspicious customers or transactions;
4) submit information, data and documentation to the Financial Intelligence Unit in timely manner;
5) appoint compliance officer for the prevention of money laundering and terrorist financing and their deputy, and provide conditions for their work;
6) organise regular professional training and development of employees in the area of money laundering and terrorist financing;
7) develop and regularly update their own list of indicators for the identification of suspicious customers and transactions;
8) keep records and ensure the protection and keeping of the data and documents obtained in accordance with this Law;
9) establish and monitor the functioning of the 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) implement measures for the prevention and detection of money laundering and terrorist financing in business units and companies that are majority-owned by reporting entities in other countries;
11) take other measures and activities pursuant to this Law.

In addition to measures and activities referred to in paragraph 1 of this Article, a reporting entity having a collegial management body shall appoint one member of that body who shall be responsible for the implementation of this Law.

Risk analysis
Article 12

A reporting entity shall identify the risks and carry out risk analysis of money laundering and terrorist financing in the manner so as to:

- develop, within 60 days from its establishment, or commencement of business activity, the internal act on risk analysis for identifying and assessing risks, taking into account risk factors of individual customer, a group of customers, a country or geographic area, business relationship, transaction, product, services or distribution channels that may be used for the purpose of money laundering or terrorist financing (hereinafter: risk analysis) and update it regularly, at least once a year, and keep it in accordance with this Law,
- carry out risk analysis for new products, services or distribution channels and, on the basis of that assessment update the risk analysis,
- determine categories of risk of money laundering risk and terrorist financing in the risk analysis, and
- based on the risk analysis, make reassessment of risk of individual customer, group of customers, country, geographic area, business relationship, transaction, product, services or distribution channels which may be used for the purposes of money laundering and terrorist financing.

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

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

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

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

Supervisory authorities referred to in Article 131 paragraph 1 of this Law may, by guidelines for risk analysis, establish that individual documented risk assessments are not needed where particular risks characteristic for the sector are clear and understandable.

Where deemed necessary, supervisory authorities referred to in Article 131 paragraph 1 of this Law may request the revision of the risk analysis of the reporting entities and policies, controls and procedures referred to in Article 14 paragraph 1 item 2 of this Law.

A reporting entity shall submit the risk analysis to the competent supervisory authority referred to in Article 131 paragraph 1 of this Law upon their request, within three days of receipt of the request.

Lower and higher risk of money laundering and terrorist financing

Article 13

If a reporting entity assesses that a customer, group of customers, country, geographic area, business relationship, transaction, product, service or distribution channel present lower risk of money laundering or terrorist financing, they may apply simplified CDD measures in accordance with this Law.

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

Money laundering and terrorist financing risk management

Article 14

A reporting entity shall establish the money laundering and terrorist financing risk management system whose implementation will reduce terrorist financing risks established through risk analysis, which particularly includes:

1) risk analysis;
2) adoption and implementation of internal acts on policies, controls and procedures with a view of effective money laundering and terrorist financing risk management;
3) ongoing monitoring and supervision over established risks of money laundering and terrorist financing; and
4) establishing an appropriate internal organization, or organizational structure of a reporting entity, proportional to the scope and nature of activities of a reporting entity.

Policies, controls and procedures referred to in paragraph 1 item 2 of this Article shall be proportionate to the scope and nature of activities of a reporting entity, size and type of their customers, as well as to the types of products or services they provide.

Policies, controls and procedures referred to in paragraph 1 item 2 of this Article shall include:

1) establishing the internal policies, controls and procedures regarding:
   - objectives, scope and manner of work of the system for managing risk of money laundering and terrorist financing,
   - CDD measures,
   - submitting data to the Financial Intelligence Unit in accordance with the law,
   - protecting and storing data and record-keeping,
   - internal controls in the area of the prevention and detection of money laundering and terrorist financing,
   - security checks of employees,
   - appointment of a compliance officer for the prevention of money laundering and terrorist financing and their deputy;
2) establishing an independent audit function or appointing a person for ongoing monitoring and supervision over the established risks of money laundering and terrorist financing, as well as checks of internal policies and procedures referred to in item 1 of this paragraph, proportionate to the scope and nature of activity of a reporting entity.

Policies, controls and procedures referred to in paragraph 1 item 2 of this Article shall be defined by competent management body of the reporting entity or senior manager.

A reporting entity shall, proportionate to the scope and nature of their activities, appoint a compliance officer for the prevention of money laundering and terrorist financing at a managerial position.

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

Regulation on guidelines for risk analysis and establishing risk management system
Article 15

The state administration authority competent for internal affairs (hereinafter: the Ministry) shall prescribe detailed criteria for drafting the guidelines for risk analysis, depending on the size and organizational structure of the reporting entity, scope and nature of the activities, types of customers, products, services or distribution channels that the reporting entity provides, the criteria for establishing risk factors, mandatory elements that the risk analysis must include and other elements of importance for money laundering and terrorist financing risk assessment, as well as detailed criteria for developing guidelines for establishing the money laundering and terrorist financing risk management system.

The Financial Intelligence Unit shall prepare the professional basis for drafting the regulation referred to in paragraph 1 of this Article, along with opinion obtained from competent supervisory authorities referred to in Article 131 paragraph 1 of this Law.

New services, products or distribution channels
Article 16

A reporting entity shall assess the risk of money laundering and terrorist financing regarding a new product, service or distribution channel which they provide within their activity, new business practice, as well as manners of providing a new product, service or distribution channel, before their introduction.

A reporting entity shall assess the risk of money laundering and terrorist financing regarding the use of modern technologies in providing the existing or new products, services or distribution channels.

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

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

Customer due diligence measures
Article 17

A reporting entity shall implement CDD measures, and in particular to:

1) identify the customer;
2) establish beneficial owner of the customer and identify the beneficial owner, including the measures necessary to determine ownership structure and controlling member of the customer in cases defined by this Law;

3) obtain and record data on the purpose, intent, objective and nature of a business relationship and transaction and other data in accordance with this Law;
4) during the business relationship, regularly monitor the business relationship and control the transactions that the customer undertakes with the reporting entity and verify their compliance with the nature of business relationship and usual scope and type of customer's business in order to allow that the executed transactions are in accordance with knowledge of the reporting entity on customer, their business profile and level of money laundering and terrorist financing risk 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 the measures referred to in paragraph 1 items 1 and 2 of this Article, the reporting entity shall verify whether a person acting on behalf of the customer has the right to represent or is authorized for representation by the customer, as well as to verify the identity of any person who acts on behalf of the customer pursuant to the provisions of this Law.

A reporting entity shall implement the measures referred to in paragraphs 1 and 2 of this Article to the extent proportional to the risk of money laundering and terrorist financing.

When determining the scope of implementation of measures referred to in paragraph 1 of this Article, the reporting entity shall take into consideration in particular the following:

1) the purpose of the entering into and the nature of the business relationship;
2) the amount of funds, the value of the property or the scope of the transaction;
3) the duration of the business relationship; and
4) the compliance of the business with the purpose of entering into the business relationship.

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

A reporting entity shall, upon the request of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, submit appropriate analysis, documents and other information proving that the measures have been implemented in accordance with the identified risk of money laundering and terrorist financing.

If a reporting entity cannot implement one or more measures referred to in paragraph 1 of this Article, they shall notify the Financial Intelligence Unit thereof, in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law.

Cases in which CDD measures are implemented
Article 18

A reporting entity shall implement the CDD measures:

1) when establishing a business relationship with a customer;
2) when executing occasional transactions in the amount of EUR 15,000 or more, regardless of whether the transaction is executed as a single transaction or several linked transactions;
3) during each occasional transaction which, within the meaning of Articles 35 to 38 of this Law, represents the transfer of funds in the amount of EUR 1,000 or more;
4) when there is a suspicion about the accuracy or authenticity of the obtained data on the identity of a customer or beneficial owner;

5) when in relation to the transaction, customer, funds or property, there are reasons to suspect or reasonable grounds to suspect that the property derives from criminal activity or that money laundering or terrorist financing has been committed, regardless of the amount of the transaction;
6) for 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 executed as a single transaction or several linked transactions;
7) upon the deposit of a stake in the amount of EUR 20 or more, during the execution of one or more linked transactions, when the reporting entity is the organizer of games of chance;
8) for every occasional transaction that represents the transfer of crypto-assets in the value of EUR 1,000 or more.

A reporting entity shall periodically implement CDD measures also in relation to customers they have already established business relationships with based on the risk analysis of money laundering and terrorist financing or upon change of specific circumstances related to the customer or when the reporting entity, pursuant to any legal obligation, is obliged to establish contact with the customer during the relevant calendar year for check of all relevant information related to the beneficial owner of the customer, or if a reporting entity was obliged to do so in accordance with regulation regulating tax administration.

If a reporting entity, in addition to the existing business relationship, enters into additional business relationship with a customer or on the basis of the existing business relationship executes the transaction referred to in paragraph 1 items 2 and 7 of this Article, the reporting entity shall obtain only the missing data on that customer, if available, regardless of the fact that they have previously implemented CDD measures.

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

Notwithstanding paragraphs 1 to 4 of this Article, where the reporting entity has reasons to suspect in money laundering or terrorist financing and reasonably believes that the implementation of CDD measures will initiate tipping off to the customer, the reporting entity shall not be required to implement CDD, but they shall notify, without delay, Financial Intelligence Unit thereof.

A reporting entity shall provide information to the customer on the purpose of processing of data which they obtain when implementing CDD measures, pursuant to the Law regulating personal data protection.

Implementation of CDD measures before establishing a business relationship
Article 19

A reporting entity shall implement the measures referred to in Article 17 paragraph 1 items 1, 2 and 3 of this Law before establishing a business relationship with a customer, including identification of persons referred to in Articles 27 and 28 of this Law.

Notwithstanding paragraph 1 of this Article, a reporting entity may implement measures referred to in 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 deems necessary, and in order not to interrupt the usual business relationship and when there is lower risk of money laundering and terrorist financing.

Where a reporting entity cannot implement measures referred to in 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 they assess that they cannot efficiently manage the risk of money laundering and terrorist financing in relation to this customer.

The provision of paragraph 3 of this Article shall not apply to the reporting entities referred to in Article 4 paragraph 2 item 13 indent 2 and paragraphs 3 and 4 of this Law when the reporting entities establish a legal position of a customer or defend or represent customer in the court proceedings or with regard to the court proceedings.

A reporting entity shall, by internal acts, define the procedures for denying the establishment of the business relationship or termination of already established business relationship referred to in paragraphs 3 and 4 of this Article.

Implementing CDD measures before executing a transaction
Article 20

A reporting entity shall apply measures referred to in Article 17 paragraph 1 items 1, 2 and 3 of this Law before executing the transaction referred to in Article 18 paragraph 1 items 2, 3, 6, 7 and 8 of this Law.

If the reporting entity cannot implement one or more measures referred to in paragraph 1 of this Article, the transaction must not be executed, except in the case referred to in Article 19 paragraph 5 of this Law.

Identification of the beneficiary or beneficial owner of a life insurance policy
Article 21

A reporting entity referred to in Article 4 paragraph 2 items 8 and 9 of this Law may verify the identity of the beneficiary or beneficial owner from the life insurance contract at the time of or after concluding such contract, but no later than when beneficiary can exercise their rights under the life insurance policy.

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

1) natural or legal person is nominated as a beneficiary, by obtaining data on their first and last name or title 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.

The verification of identity of the beneficiary or beneficial owner referred to in paragraph 2 of this Article shall be carried out at the time of the payment.

When transferring the rights under the life insurance policy to a third party, in part or in full, the reporting entity shall identify a new customer or the beneficial owner at the time of transferring the rights.

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

Identification of a natural person
Article 22

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

A reporting entity shall, in the procedure of establishing the identity referred to in paragraph 1 of this Article, check the data from a personal identification document and verify if those data correspond to the customer.

When establishing the identity referred to in paragraph 1 of this Article, a reporting entity shall obtain a photocopy of a personal identification document and register date, time, first and last name of a person who checked the photocopy of personal identification document and keep the collected data in accordance with this Law.

When establishing the identity of the customer referred to in paragraph 1 of this Article, the data on the customer, business relationship and transaction referred to in Article 117 paragraph 1 items 2, 3, 6 and 7 of this Law shall be obtained.

If all the data referred to in paragraph 4 of this Article cannot be obtained from the personal identification document, those data shall be obtained by checking the original document or certified photocopy of other valid public document that customer presents or by checking appropriate public register.

If legal representative or authorized person of the customer referred to in paragraph 1 of this Article establishes a business relationship or executes a transaction on behalf of the customer referred to in paragraph 1 of this Article, the reporting entity shall:

- establish the identity of that legal representative or authorized person pursuant to paragraphs 1 to 5 of this Article and provide data on that person referred to in Article 117 paragraph 1 item 3 of this Law,
- obtain data on the customer referred to in Article 117 paragraph 1 item 3 of this Law from the original written power of attorney or certified photocopy of that power of attorney,
- check the data on the customer which they have obtained pursuant to indent 2 of this paragraph.

If the reporting entity, when identifying the customer referred to in paragraph 1 of this Article, their legal representative or authorized person referred to in paragraph 6 of this Article, doubts the veracity of the obtained data or credibility of the identification documents or other documentations from which the data have been obtained, they shall undertake additional checks, as well as ask for the written statement of that customer, their legal representative or authorized person on the veracity of those data.

A reporting entity may check data from personal identification documents of the customer referred to in paragraph 1 of this Article, their legal representative or authorized person through the Financial Intelligence Unit, by checking the Central Population Register (hereinafter: CPR), the records of issued personal identification documents and international base of stolen, lost and invalid documents, electronically.

If during the checks referred to in paragraph 8 of this Article it is established that the data from personal identification document are different from the data in the CPR, the reporting entity shall not establish a business relationship or execute a transaction.

After the identification of the customer referred to in paragraph 1 of this Article has been carried out, the reporting entity shall enter the data on the method of identification in the records referred to in Article 117 paragraph 1 of this Law.

The Ministry shall prescribe the manner of data verification referred to in paragraph 8 of this Article.

The act referred to in paragraph 11 of this Article shall be classified with the appropriate confidentiality level, pursuant to the law regulating the data confidentiality.

Electronic identification
Article 23

Identification of the customer who is a natural person, an entrepreneur or a natural person who performs business activity, their legal representative and authorized person, may be performed without mandatory physical presence, based on means of electronic identification with high level of security of the electronic identification system or based on qualified certificate for electronic signature issued by the qualified trust service provider, pursuant to the law regulating electronic identification and electronic signature (hereinafter: electronic identification).

Prior to electronic identification, the customer referred to in paragraph 1 of this Article shall provide the reporting entity with a photocopy of a personal identification document, and in the case of identification of their legal representative or authorized person, also a photocopy of power of attorney evidencing the capacity of legal representative or authorized person, in electronic form.

Prior to electronic identification, a reporting entity shall obtain data on the customer referred to in paragraph 1 of this Article, business relationship and transaction referred to in Article 117 paragraph 1 items 2, 3, 6 and 7 of this Law.

A reporting entity shall check the data referred to in Article 117 paragraph 1 items 2, 3, 6 and 7 of this Law through the Financial Intelligence Unit, by access to the CPR, the records of issued personal identification documents and the international base of stolen, lost and not valid documents, electronically, in the manner prescribed by the act referred to in Article 22 paragraph 11 of this Law.

A reporting entity may perform identification electronically only for a service or for a product which they provide within their business activity and for the customer for whom a higher risk of money laundering and terrorist financing has not been established.

Electronic identification may not be performed if:

- during the check referred to in paragraph 4 of this Article it has been established that the data from the personal identification document of the person referred to in paragraph 1 of this Article are different from those in the CPR;
- the means of electronic identification or qualified certificate for electronic signature of a person referred to in paragraph 1 of this Article has been issued under pseudonym;
- there is a suspicion that the means of electronic identification or qualified certificate for electronic signature of the person referred to in paragraph 1 of this Article is misused, or if the reporting entity establishes that circumstances, substantially affecting the validity of that means of electronic communication or qualified certificate for electronic signature, have been changed and the electronic identification service provider or qualified electronic trust service provider did not revoke that means or certificate;

- the electronic personal identification document referred to in paragraph 1 of this Article has been issued in high-risk third country.

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

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

- technical and other requirements that enable the verification at any time of whether the means of electronic identification or qualified certificate for electronic signature is valid;
- technical requirements that enable obtaining data on the customer referred to in paragraph 1 of this Article, business relationship and transaction referred to in Article 117 paragraph 1 items 2, 3, 6 and 7 of this Law and their verification in accordance with paragraph 4 of this Article;
- technical requirements for record-keeping on conducting electronic identification.

Upon the completion of electronic identification, the reporting entity shall enter into the records referred to in Article 117 paragraph 1 of this Law the data on the manner in which the identification of a person referred to in paragraph 1 of this Article has been conducted.

Video-electronic identification
Article 24

The identification of the customer who is a natural person, an entrepreneur or a natural person performing business activity, their legal representative and authorized person may be performed remotely, through the procedure of video identification by using the means of electronic communication (hereinafter: video-electronic identification).

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

A reporting entity shall, prior to the beginning of video-electronic identification, obtain the consent from the person referred to in paragraph 1 of this Article for the complete procedure of video electronic identification, particularly for recording image and 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 the transmission of the read data via the Internet.

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

A reporting entity shall notify the person referred to in paragraph 1 of this Article in advance on the obligation of obtaining the consent referred to in paragraph 3 of this Article as well as 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 they will use during the video-electronic identification, in electronic form.

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

A reporting entity shall, by electronic reading of the data from the electronic personal identification document, obtain data on the entrepreneur or natural person referred to in Article 117 paragraph 1 items 2 and 3 of this Law, as well the digital image and digital reproduction of original signature of the customer according to recommendations of ICAO Doc 9303.

The data referred to in Article 117 paragraph 1 items 2 and 3 of this Law, which may not be obtained through electronic reading of electronic personal identification document pursuant to paragraph 8 of this Article, shall be obtained directly from the customer in video-audio communication.

A reporting entity may check the data referred to in paragraphs 8 and 9 of this Article, through the Financial Intelligence Unit, by access to the CPR, records of issued personal identification documents and international database of stolen, lost and not valid documents, electronically, in the manner prescribed by the act referred to in Article 22 paragraph 11 of this Law.

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

In the case of video-electronic identification of the legal representative or authorized person of the customer prior to establishing the business relationship or executing transaction, that legal representative or authorized person shall present and submit a photocopy of the power of attorney evidencing the capacity of the legal representative or authorized person.

A reporting entity may perform the video-electronic identification only for the service or the product they provide within their business activity.

Notwithstanding paragraph 13 of this Article, the reporting entity referred to in Article 4, paragraph 2, items 1, 2, and 3 of this Law may conduct video-electronic identification only for the service or product provided within their business activity and for a customer for whom no higher risk of money laundering and terrorist financing has been determined.

A reporting entity must not perform a video-electronic identification if an electronic personal identification document of the person referred to in paragraph 1 of this Article has been issued in high-risk third country.

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

- during the verification referred to in paragraph 10 of this Article it has been established that the data from the personal identification document of the person referred to in paragraph 1 of this Article are different from those in CPR;
- they have doubts in the veracity of the collected data or authenticity of the documents from which the data are collected;
- it is not possible to provide adequate transmission of image and sound or high-quality transmission;
- the room where the person referred to in paragraph 1 of this Article stays is poorly lighted or there is 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 may not perform identification of the person referred to in paragraph 1 of this Article.

The identification of the person referred to in paragraph 1 of this Article may be performed in repeated procedure of video-electronic identification, only if the previous procedure is terminated due to circumstances referred to in paragraph 16 of this Article and only after the removal of these circumstances.

Upon the completed video-electronic identification, the reporting entity shall enter into the records referred to in Article 117 paragraph 1 of this Law the data on the manner in which the identification of a person referred to in paragraph 1 of this Article has been conducted.

A reporting entity shall prescribe in their internal acts referred to in paragraph 21 of this Article the manner of performing the video-electronic identification in more detail no later than eight days from the date of submission of the administrative decision referred to in Article 25 paragraph 6 of this Law approving the performance of video-electronic identification.

Notwithstanding paragraph 2 of this Article, a reporting entity may conduct video-electronic identification without customer's communication with an employee, by using reliable algorithms to verify whether the recorded photos or video-recordings match with the photo taken from electronic personal identification of the customer.

The Ministry shall prescribe detailed conditions and the manner of performing video- electronic identification, as well as the manner of organizing and content of the training referred to in paragraph 2 of this Article.

Customer identity verification using reliable algorithms
Article 24a

A reporting entity that has conducted video-electronic identification of the customer in accordance with Article 24 of this Law may perform any subsequent identity verification of the customer using reliable algorithms for verification based on the customer's video recording, by comparing the photograph taken in that video recording with the photograph obtained from the customer's electronic identity document during the identification procedure specified in Article 24 of this Law.

The verification from paragraph 1 of this Article can only be performed if the validity date of the customer's electronic identity document from which the data was taken has not expired at the time of the verification.

During the verification process outlined in paragraph 1 of this Article, the reporting entity may verify the data obtained during the customer's identification in accordance with Article 24 of this law, through the Financial Intelligence Unit, by reviewing the CPR, the record of issued identity documents, and the international database of stolen, lost, and invalid documents, electronically, in the manner prescribed by the act from Article 22 paragraph 11 of this Law.

A reporting entity may perform the customer identity verification as described in paragraph 1 of this Article only for the service or product they provide within their business activity.

A reporting entity shall retain the video recording made during the verification process from paragraph 1 of this Article in accordance with this Law.

Obligations of reporting entities for data protection and cybersecurity during the identification procedure via electronic and video-electronic identification
Article 24b

A reporting entity shall conduct a risk analysis of the system and solutions used for the procedure of electronic identification and video-electronic identification.

A reporting entity shall use secure communication channels for interaction with the customer during the electronic and video-electronic identification process, employing secure protocols and cryptographic algorithms in accordance with best practices and industry standards for the protection of confidentiality, integrity, availability and data protection, as well as for cybersecurity purposes.

A reporting entity shall continuously monitor the solution referred to in paragraph 1 of this Article to ensure that its functionality is in accordance with this Law and the acts referred to in Article 24 of this Law.

A reporting entity shall manage the identified risks referred to in paragraph 1 of this Article.

Authorization for performing electronic 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, an entrepreneur or a natural person performing business activity, their legal representative and authorized person, only if the reporting entity holds authorization to perform electronic identification or video-electronic identification.

A reporting entity shall submit the application for granting authorization referred to in paragraph 1 of this Article to the competent supervisory authority referred to in Article 131 paragraph 1 of this Law on the prescribed template.

A reporting entity shall, together with the application referred to in paragraph 2 of this Article, submit evidence on the fulfilment of the conditions referred to in Article 23 paragraph 8 of this Law or conditions prescribed in the act referred to in Article 24 paragraph 21 of this Law.

The competent supervisory authority referred to in Article 131 paragraph 1 of this Law shall submit the application referred to in paragraph 2 of this Article and evidence referred to in paragraph 3 of this Article to the Financial Intelligence Unit.

The head of the Financial Intelligence Unit shall establish an interdepartmental commission which determines the fulfilment of the conditions referred to in paragraph 3 of this Article.

Upon the proposal of the commission referred to in paragraph 5 of this Article, the head of the Financial Intelligence Unit, shall, upon the application referred to in paragraph 2 of this Article, issue an administrative decision approving or refusing the conduct of electronic identification or video- electronic identification to the reporting entity.

The commission referred to in paragraph 5 of this Article shall propose the issuing of the administrative decision rejecting the application referred to in paragraph 2 of this Article if it establishes that a specific service or product poses higher risk of money laundering and terrorist financing in the context of this Law.

An administrative dispute may be initiated against the decision referred to in paragraph 7 of this Article.

The commission referred to in paragraph 5 of this Article shall consist of the representatives of the Financial Intelligence Unit, other organizational units of the Ministry and supervisory authorities referred to in Article 131 paragraph 1 items 1, 3, 4 and 7 of this Law.

The commission referred to in paragraph 5 of this Article shall have the chairperson, members and secretary.

A monthly fee in the amount of 25% of an average gross salary in Montenegro for the previous year based on the data of the administrative authority competent for statistical affairs shall be paid to the commission chairperson, members and secretary referred to in paragraph 5 of this Article, and it shall be paid in net amount.

The Ministry shall prescribe the form and the content of the application referred to in paragraph 2 of this Article and manner of work of the commission referred to in paragraph 5 of this Article.

Identification of a legal person and business organization
Article 26

A reporting entity shall identify a customer that is a legal person or a business organization, pursuant to Articles 19 and 20 of this Law, by obtaining the data referred to in 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 the data referred to in paragraph 1 of this Article by checking the Central Business Register (hereinafter: CBR) or other appropriate public register, as well as checking court, business or other public register where a foreign legal person or business organization is registered.

A reporting entity may also obtain the data referred to in paragraph 1 of this Article by checking the original or certified photocopy of the document from the CBR or other appropriate public register, as well as by checking the original or certified photocopy of the document from court, business or other public register where the foreign legal person or business organization is registered, that is, on behalf of the legal person or business organization, submitted by their legal representative or authorized person and that shall not be older than three months of its issue date.

A reporting entity shall keep the documents referred to in paragraph 3 of this Article in their files.

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

A reporting entity shall obtain the data which are not included in the registers referred to in paragraph 2 of this Article or in the documents referred to in paragraph 3 of this Article, by checking the original or certified photocopy of the document or other documentation submitted by the legal representative or authorized person of the customer referred to in paragraph 1 of this Article.

If a reporting entity, during the establishment of the identification of the customer that is a legal person or business organization doubts the veracity of the obtained data or authenticity of the documents or public or other documentations from which the data were obtained, they shall also, before the establishment of business relationship or execution of the transaction, obtain a written statement on the veracity of these data from the legal representative or authorized person, and conduct additional checks.

If the customer is a foreign legal person that performs business activity in Montenegro through their business unit, the reporting entity shall perform identification of the foreign legal person and their 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 that 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 referred to in 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 referred to in paragraph 2 of this Article obtain those power of attorneys and keep them in their documentation.

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

Establishing the identity of the compliance officer of a legal person and business organization
Article 28

If an authorized person establishes business relationship or executes transaction on behalf of the legal representative of the customer that is a legal person or a business organization and all directors of that legal person or business organization, the reporting entity shall establish the identity of that authorized person pursuant to Article 22 of this Law.

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

Establishing the identity of a trust, other person or a subject of international law equal to them
Article 29

If the customer is a trust, other person or a subject of international law equal to them, the reporting entity shall:

1) identify their legal representative or authorized person pursuant to Articles 27 and 28 of this Law;
2) obtain the data referred to in Article 117 paragraph 1 items 1, 2 and 3 of this Law for founders, all trustees, other representatives, beneficiaries or group of beneficiaries of the property being managed, if future beneficiaries have already been determined or are determinable and other natural person who directly or indirectly has the ultimate control over the trust;
3) obtain the data on the legal form of the trust, other person or a subject of international law equal to them and the articles of incorporation of the trust, other person or a subject of international law equal to them.

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

If a reporting entity, when identifying the legal representative and authorized person of the customer referred to in paragraph 1 of this Article, doubts the veracity of obtained data or the authenticity of the identification documents or other documentation from which the data have been obtained, they shall conduct additional checks, as well as obtain a written statement on the veracity of those data from legal representative and authorized person.

A person managing a trust, other person or a subject of international law equal to them shall, when establishing business relationship with a reporting entity or executing occasional transaction referred to in Article 18 paragraph 1 items 2, 3, 6 and 7 of this Law, notify the reporting entity that

they act in that capacity on behalf of those persons and provide the information referred to in paragraph 1 item 2 of this Law.

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 when:

1) a customer enters the premises where games of chance are organized in a casino;
2) there is any access to a safe deposit box by a lessee or their legal representative, or a person they have authorized.

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

The identification of the customer referred to in paragraph 2 of this Article may be carried out when the customer accesses the safe deposit box using an electronic identification card or a personal access code, by video identification means, or means allowing customer identification based on their 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 safe box renting shall obtain the data referred to in Article 117 paragraph 1 item 3 and paragraph 2 of this Law.

Implementation of CDD measures through a third party
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 referred to in Article 17 paragraph 1 items 1, 2 and 3 of this Law to a third party that meets the requirements defined by this Law.

A third party may be:

1) a credit institution and branch of a foreign credit institution.
2) an investment fund management company;
3) a pension fund management company;
4) investment company engaged in business activity defined by the law regulating capital market;
5) life insurance company and branch of foreign life insurance company;
6) mediation company, representation company and an entrepreneur – agent in insurance, in the part related to life insurance;
7) a person referred to in items 1 to 6 of this paragraph with a head office in a European Union Member State or in another country which implements measures in the area of prevention of money laundering and terrorist financing stipulated by this law or stricter measures.

Prior to entrusting the implementation of measures referred to in paragraph 1 of this Article to a third party a reporting entity shall establish that the operations of that person are, in accordance with the requirements related to the prevention of money laundering and terrorist financing, subject to regular supervision in the manner specified by this Law or appropriate regulation of another country, and that they have mechanisms in place to meet the requirement to implement CDD measures, which are at the level of the measures prescribed by this Law or stricter and that records with regard to the measures taken are kept in the manner prescribed by this Law.

The supervisory authorities referred to in Article 131 paragraph 1 of this Law may consider that the operations of the reporting entity operating within a group are compliant with the provisions of this Article if:

1) they rely on the information provided by third party that is part of the same group;
2) the group implements enhanced CDD measures, rules on keeping the records and prevention of money laundering and terrorist financing programmes in accordance with the provisions of this Law or appropriate regulation of another country; and
3) the efficient implementation of the measures and processes referred to in item 2 of this paragraph at a group level is overseen by the supervisory authority in accordance with this Law or appropriate regulation of another country.

External associates and representatives of the reporting entity that, based on an agreement (externalization or legal representation), conduct certain CDD measures for the reporting entity shall not be considered a third party within the meaning of this Article.

A reporting entity shall be responsible for the proper implementation of CDD measures conducted through a third party.

Prohibition of implementing CDD measures through a third party
Article 32

A reporting entity shall not entrust the implementation of CDD measures to a third party where that third party is a shell (fictious) bank or an anonymous company or it is from the high risk third country.

Obtaining data and documents from a third party
Article 33

A third party that conducts the CDD measures in accordance with Article 31 of this Law shall deliver, without delay, the obtained data and documentation on the customer to the reporting entity.

The 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 documentation based on which they have conducted the CDD measures, as well as data obtained pursuant to Articles 23 and 24 of this Law, if the electronic identification and video-electronic identification have been performed.

The third party referred to in paragraph 1 of this Article shall keep the obtained photocopies of identification documents and the entire documentation obtained when conducting CDD measures in accordance with this Law.

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

When a reporting entity assesses that there is suspicion in the validity of the CDD measures conducted by a third party, or the credibility of obtained data and documentation on customer, the reporting entity shall conduct such measures directly.

A reporting entity shall, by an internal act, define the procedures for accepting the identification of the customer and the beneficial owner of the customer through a third person.

3. Obligations during the transfer of funds

Obligations of the payment service provider 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 referred to in paragraph 1 of this Article shall be:

1) the name and surname or (business) name;
2) the number of payment account, or a unique identifier of the transaction if the transfer is performed without opening the payment account;
3) the address, or registered office, including the name of the country, number of personal identification document, unique master citizen number or identification number of the payer or the date and place of birth.

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

1) the name and surname or business name,
2) the number of payment account or a unique identifier of the transaction if the transfer is performed without opening the payment account.

Notwithstanding paragraph 2 of this Article, in the case of a bulk transfer of funds from one payer, the payment service provider is not obliged, with regard to individual transfers of funds which are part of the bulk transfer, to record data referred to in paragraph 2 of this Article into the payment order form or electronic message accompanying the transfer of funds, if data referred to in paragraphs 2 and 3 of this Article are included in the payment order form or electronic message accompanying the transfer of funds for the bulk transfer and if the form or electronic message for every individual transfer of funds includes at least a number of the payer's payment account or a unique identifier of the transaction, if the transfer of funds is performed without opening a payment account.

The exception referred to in paragraph 4 of this Article shall not apply in the case of the bulk transfer of funds from one payer, when the payment service provider of the payer and the payment service providers of the payee have their head offices in Montenegro.

When the amount of the transfer of funds, including the amount of payment transactions connected with that transfer, is less than EUR 1.000, the payment service provider of the payer shall ensure that the transfer of funds contains at least the following data:

1) the name and surname or business name of the payer and of the payee,
2) the number of payment account of the payer and of the payee or a unique identifier of the transaction if the transfer is performed without opening a payment account.

Payment service provider of the payer 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 performing the transfer of funds.

Payment service provider of the payer shall be considered to have verified the accuracy of collected data on the payer prior to the transfer of funds, if they had previously established a business relationship with the payer and identified the payer in the manner prescribed in Articles 22, 23, 24, 26, 27 and 28 of this Law and if they act in accordance with Article 49 of this Law.

Notwithstanding paragraph 7 of this Article, in the case where the transfer of funds, including the amount of payment transactions connected to such transfer, is less than EUR 1.000, payment service provider of the payer is not obliged to verify the accuracy of data collected on the payer, unless:

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

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

The payment service provider of the payer shall define, by an internal act, the procedures for the verification of completeness of data collected pursuant to paragraphs 2 - 8 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 the transfer of funds pursuant to Article 35 of this Law.

If the amount of money transfer is EUR 1.000 or more, regardless of whether those transfers are performed through one or several linked transactions, the payment service provider of the payee shall, prior to executing such transaction to the account of the payee or making such funds available to the payee, verify the accuracy of data collected on that payee.

If the amount of money transfers, including 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 made available to the payee in cash or in anonymous electronic money, or
2) there are reasons for suspicion in money laundering and terrorist financing.

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

The payment service provider of the payee shall introduce effective procedures to determine whether the fields related to the payer and payee data in the message exchange or in the payment and settlement system used for executing money transfers are filled with letters, numbers, and symbols allowed in accordance with the rules of that system.

Payment service provider of the payee may, in accordance with the risk assessment, verify the accuracy of data of the payee, regardless of the amount of funds that are transferred.

Procedure in case of failure to deliver accurate and complete data
Article 37

Payment service provider of the payee shall, in accordance with risk assessment, make an internal act with regard to the procedure, including, if necessary, 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 referred to in Article 35 of this Law.

If a payment order form or electronic message accompanying money transfer does not contain accurate and complete data referred to in Article 35 of this Law, the payment service provider of the payee shall, in accordance with the risk assessment, by the internal act referred to in paragraph 1 of this Article, prescribe when to:

1) refuse the transfer of funds;

2) suspend the execution of the transfer of funds until the receipt of the missing data, which they shall request from the intermediary in that transfer, or from the payment service provider of the payer;
3) execute the transfer of funds and, simultaneously or subsequently, request from the intermediary in that transfer, or from the payment service provider of the payer, the missing data or data that have not been not entered into the payment order form or electronic message accompanying the transfer of funds.

If payment service provider of the payer frequently fails to provide accurate and complete data pursuant to Article 35 of this Law, the payment service provider of the payee shall warn them and set the deadline within which they are required to align their activities with this Law.

If the service provider of the payer fails to act in accordance with paragraph 3 of this Article, the payment service provider of the payee shall refuse future transfers of funds which they receive from that payment service provider or limit or terminate business cooperation with that payment service provider.

Payment service provider of the payee shall notify the Central Bank of Montenegro about the payment service provider of the payer that frequently fails to provide accurate and complete data pursuant to Article 35 of this Law, as well as about the measures it has taken pursuant to paragraphs 3 and 4 of this Article against such payment service provider.

Payment service provider of the payee shall determine whether the lack of accurate and complete data referred to in Article 35 of this Law presents the reasons for suspicion in money laundering or terrorist financing and if it determines that this lack presents the reasons for suspicion, it shall notify the Financial Intelligence Unit thereof in accordance with Article 66 paragraphs 6, 8 and 10 of this Law.

Where the payment service provider of the payee establishes that the lack referred to in paragraph 6 of this Article does not present reasons for suspicion in money laundering and terrorist financing, it shall make a note thereof and keep it pursuant to this Law.

Obligations of the intermediary in the 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 the payment order form or electronic message accompanying transfer of funds.

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

Where the payment order form or electronic message accompanying transfer of funds does not contain the accurate and complete data referred to in Article 35 of this Law, the intermediary in the transfer of funds shall act in accordance with Article 37 paragraphs 2 to 7 of this Law.

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

Provisions of Articles 35 to 38 of this Law shall not apply in the following cases:
1) when the transfer of funds is carried out solely for the purchase of goods or services, using a payment card, payment instrument used for managing electronic money, mobile phone, or any other digital or information-technology device, provided that the payer and the payee, and the number of that card, instrument or device or unique identifier, accompany

such transfer of funds in a manner that allows the data about the payer to be accessed via that number or identifier, except in cases where the payment card, payment instrument used for managing electronic money, mobile phone, or any other digital or information-technology device with similar features is used to execute the transfer of funds between natural persons;

2) in the case of a transfer of funds when the payer withdraws cash from their own account;
3) when a transfer of funds is used to pay taxes, fines and other public duties, and the payment service provider of the payer and payment service provider of the payee have their head offices in Montenegro;
4) when the payer and the payee are payment service providers acting on their own behalf and for their own account;

4a) when the transfer of funds is carried out through the exchange of electronic cheques, including electronically processed cheques;

5) when the transfer of funds is used to make a payment to the payee solely on the basis of the delivery of goods or services provided, services of electricity and water supply, services of collection, treatment and disposal of waste, services of maintaining residential buildings, or other similar ongoing services for which they have a contract on providing services, and where:

- the payee's payment service provider is a reporting entity within the meaning of this Law,
- the payee's payment service provider may, through the payee, using the unique transaction identifier or other data accompanying the transfer of funds, access data on the person who has a contract with the payee for the provision of services or payment for goods,
- the amount of the transfer of funds does not exceed EUR 500,
- when the payments for these services are made by crediting the payee's payment account, which is used exclusively for these payments, and
- when the conditions referred to in Article 40 paragraph 1 of this Law have been met.

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

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

1) the payment instrument is not reloadable, or the maximum monthly payment limit is capped at EUR 150 and can only be used in Montenegro;
2) the amount of deposited electronic money does not exceed EUR 150;
3) the payment instrument is used solely for purchase of goods or services;
4) anonymous electronic money cannot be deposited onto the payment instrument;
5) the issuer of electronic money conducts appropriate CDD measures for the purpose of detecting complex and unusual transactions referred to in Article 58 of this Law and suspicious transactions.

Paragraph 1 of this Article shall not apply to the purchase of electronic money in cash or to the withdrawal of cash in the value of electronic money in the amount exceeding EUR 50, or to the initiation of a transaction via the Internet or using means of remote communication, if the amount of the transaction exceeds EUR 50.

A reporting entity may accept payment with an anonymous payment instrument, if such payment instrument meets the conditions set out in paragraph 1 of this Article and if it is not related to the purchase of electronic money in cash or to the withdrawal of cash in the value of electronic money, in the amount exceeding EUR 50.

Paragraph 1 of this Article shall not apply to the cases where, in connection to a transaction or a customer, there are reasons or reasonable grounds to suspect that property derives from criminal activity or that money laundering or terrorist financing has been committed.

3a. Services related to crypto-assets
Register of crypto-asset service providers
Article 40a

A legal person, business organization, entrepreneur and natural person performing business activity with a registered office in Montenegro, or having residence or approved permanent stay in Montenegro, that intend to provide crypto-assets services in Montenegro, shall be registered in the Register of Crypto-asset Service Providers before they begin to provide those services.

A crypto-asset service provider from a member state of the European Union, which is not on the list of high-risk third countries, that has been authorized by its competent supervisory authority or registered with the register of the competent supervisory body in the country of its establishment, and wants to provide these services in Montenegro, shall be registered in the Register of Crypto-asset Service Providers before starting to provide those services.

The Register of Crypto-asset Service Providers is an electronic database that stores and maintains data on crypto-asset service providers.

The Register of Crypto-asset Service Providers shall be managed and maintained by the supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law.

Financial Intelligence Unit and the supervisory authorities referred to in Article 131 paragraph 1 of this Law shall have direct electronic access to the data from the Register of Crypto-asset Service Providers.

Anyone has the right to access the data from the Register of Crypto-asset Service Providers, including the data on the name or the name and surname of the providers of services and the crypto-assets services that these providers offer.

Registration in the Register of crypto-asset service providers
Article 40b

The request for registration in the Register of Crypto-asset Service Providers shall be submitted to the supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law.

Entities from Article 40a paragraph 1 of this Law shall submit the following along with the request:

- data on the name, address, registered office, registration number, or other identification number (tax identification number) for legal persons or business organizations, or the name, surname, personal identification number, address, and municipality of residence or permanent stay in Montenegro for entrepreneurs or natural persons performing business activities;
- proof of the appointment of a compliance officer for the prevention of money laundering and terrorist financing in accordance with Article 69 of this Law;

- certificate, confirmation, or other act from the competent authority for keeping criminal records proving the reputation, as per Article 40r of this Law, for the director, members of the company, members of management and executive bodies, and beneficial owners of the legal person or business organization, or for the entrepreneur or natural person performing business activities, in case any of them are not Montenegrin citizens;
- a statement from the responsible person in the legal person or business organization, or entrepreneur or natural person performing business activities, confirming that they are familiar with the obligations from this Law;
- information about all directors of the legal person or business organization prescribed in Article 117 paragraph 1 item 3 of this Law;
- a business plan indicating the crypto-asset services they intend to provide, including a plan on how those services will be marketed.

Notwithstanding paragraph 2 item 3 of this Article, the certificate, confirmation, or other act from the competent authority for keeping criminal records proving the reputation, as per Article 40r of this Law, for the director, members of the company, members of management and executive bodies, and beneficial owners of the legal person or business organization, or entrepreneurs or natural persons performing business activities, in case they are Montenegrin citizens, shall be obtained ex officio by the supervisory authority referred to in Article 131 paragraph 1 point 3 of this Law.

A crypto-asset service provider referred to in Article 40a paragraph 2 of this Law shall submit the following along with the request:

- data on the name, address, registered office, registration number, or other identification number (tax identification number) for legal persons or business organizations, or the name, surname, date of birth, country of birth, type, number, and country of issue of the personal identification document, address of residence in Montenegro for entrepreneurs or natural persons performing business activities;
- confirmation of approval from the competent supervisory authority or an extract from the register of the competent supervisory body in the country of establishment;
- proof of the crypto-assets services for which they are registered in the country of establishment;
- the name and contact details of the competent supervisory authority in the country of establishment;
- a business plan indicating the crypto-asset services they intend to provide, including a plan on how those services will be marketed.

The reputation referred to in paragraph 2 item 3 and paragraph 3 of this Article is determined by the supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law in accordance with Article 40r of this Law.

The supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall verify the authenticity of the submitted data and documentation independently and in cooperation with the competent authorities in Montenegro, as well as through international cooperation channels, after which they shall decide on the request for registration in the Register of Crypto-asset Service Providers.

A legal person or business organization referred to in Article 40a paragraph 1 of this Law cannot be registered in the Register of Crypto-asset Service Providers if it is not registered in the Beneficial Owners Register.

The supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall reject the request for registration in the Register of Crypto-asset Service Providers if the applicant fails to submit the data and documentation from paragraph 2 or paragraph 4 of this Article or if the conditions from paragraphs 6 and 7 of this Article are not met.

An administrative dispute may be initiated against the administrative decision rejecting the request for registration in the Register of Crypto-asset Service Providers.

Content of the Register of crypto-asset service providers
Article 40c

The Register of Crypto-asset Service Providers shall contain the following information:

1) for a legal person or business organization: name, registered office (address and city or municipality for legal persons with registered office in Montenegro, and for legal persons with registered office in another country, the country and city), registration number, information on whether they are residents or non-residents, phone number, email address, and data referred to in Article 44 of this Law;
2) for an entrepreneur: name, registered office (address and city or municipality for an entrepreneur with their registered office in Montenegro, and for an entrepreneur with their registered office in another country, the country and city), unique identification number, name and surname, information on whether the entrepreneur is a resident or non-resident, phone number, and email address;
3) for a natural person: name and surname, unique identification number, address and municipality of residence in Montenegro, date of birth, country of birth, citizenship, information on whether the individual is a resident or non-resident, phone number, email address, type, number, country of issue, and expiry date of the personal identification document;
4) data on the name of the crypto-asset services provided in Montenegro.

Deletion from the Register of crypto-asset service providers
Article 40d

The supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall issue a decision to delete a crypto-asset service provider from the Register of Crypto-asset Service Providers if:

1) the provider notifies the supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law that they will no longer provide crypto-asset services;
2) the provider was registered in the Register of Crypto-asset Service Providers based on false or inaccurate documentation or misrepresented facts;
3) the provider no longer meets the reputation requirement as per Article 40b paragraph 2 item 3, and paragraph 3 of this Law;
4) the provider fails to fulfill the obligations under Article 40f of this Law; or
5) the provider no longer provides crypto-asset services on the territory of Montenegro.

Notwithstanding paragraph 1 of this Article, the supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall deactivate the status in the Register of Crypto-asset Service Providers for a crypto-asset service provider if it suspects that the provider meets any of the conditions for deletion from paragraph 1 items 2 to 5 of this Article, and shall notify the provider accordingly.

The deactivation referred to in paragraph 2 of this Article shall last until the supervisory

authority referred to in Article 131 paragraph 1 item 3 of this Law determines whether any of the conditions for deletion referred to in paragraph 1 items 2 to 5 of this Article are met and if they find that any of the conditions are met, the provider will be deleted from the Register of Crypto-asset Service Providers, and if they find that none of the conditions are met, the deactivation will be removed.

A crypto-asset service provider must not provide services while deactivated.

An administrative dispute may be initiated against the administrative decision on deleting from the Register of Crypto-asset Service Providers.

Crypto-asset services provided in Montenegro
Article 40e

Crypto-asset services are considered to be provided in Montenegro if one of the following conditions is met, namely if crypto-asset service providers:

- have their registered office in Montenegro, or are residents, or have a place of business in Montenegro from which they provide services;
- provide crypto-asset services, advertise their services, or conduct a marketing campaign, regardless of the method of advertisement, directed towards persons who have their registered office in Montenegro, or are residents;
- offer crypto-assets in Montenegro through one or more automated systems;
- distribute their services through one or more distribution channels aimed at persons who have their registered office in Montenegro, or who are residents;
- have a mailing address or phone number in Montenegro, or use a ".me" domain extension on their website.

Obligations of the crypto-asset service provider of the originator
Article 40f

During the transfer of crypto-assets the crypto-asset service provider of the originator shall ensure the data on the originator and the beneficiary of the crypto-assets.

Data about the originator shall include:

1) name and surname, or name of the originator;
2) address, or registered office, including the name of the country, personal identification document number, unique identification number, or registration number of the originator, or date and place of birth;
3) originator’s distributed ledger address, in cases where a transfer of crypto-assets is registered on a network using DLT or similar technology, and the crypto-asset account number of the originator, where such an account exists and is used to process the transaction;
4) the originator’s crypto-asset account number, in cases where a transfer of crypto-assets is not registered on a network using DLT or similar technology;
5) subject to the existence of the necessary field in the relevant message format, and where provided by the originator to its crypto-asset service provider, the current LEI or, in its absence, any other available equivalent official identifier of the originator.

Data about the beneficiary of the crypto-assets shall include:

1) name and surname, or name of the beneficiary;

2) the beneficiary's distributed ledger address, in cases where a transfer of crypto-assets is registered on a network using DLT or similar technology, and the beneficiary's crypto-asset account number, where such an account exists and is used to process the transaction;
3) the beneficiary's crypto-asset account number, in cases where a transfer of crypto-assets is not registered on a network using DLT or similar technology;
4) subject to the existence of the necessary field in the relevant message format, and where provided by the originator to its crypto-asset service provider, the current LEI or, in its absence, any other available equivalent official identifier of the beneficiary.

Notwithstanding paragraph 2 item 4, and paragraph 3 item 3 of this Article, in the case of a transfer of crypto-assets not registered on a network using DLT or similar technology and not made to or from a crypto-asset account, the crypto-asset service provider of the originator shall ensure that the transfer of crypto-assets is accompanied by a unique transaction identifier.

The data on the originator and beneficiary referred to in paragraphs 2 and 3 of this Article shall not be required to be directly included in the transfer of crypto-assets.

The data referred to in paragraphs 2 and 3 of this Article shall be submitted to the other crypto-asset service provider of the originator in advance of, or simultaneously or concurrently with the execution of the crypto-asset transaction and in a manner that ensures the protection of these data in accordance with the law governing the protection of personal data.

In the case of the transfer of crypto-assets made to a self-hosted address, the crypto-asset service provider of the originator shall obtain and hold the data referred to in paragraphs 2 and 3 of this Article and ensure that the transfer of crypto-assets can be individually identified.

In addition to the measures referred to in Article 53c of this Law, in cases of transfers of an amount exceeding EUR 1,000 to a self-hosted address, the crypto-asset service provider of the originator shall take adequate measures to assess whether the address is owned or controlled by the originator.

Before transferring crypto-assets, the crypto-asset service provider of the originator shall verify the accuracy of the data about the originator and the beneficiary of the crypto-assets referred to in paragraphs 2 and 3 of this Article based on documents, data, or information obtained from a reliable and independent source.

Verification of the data referred to in paragraphs 2 and 3 of this Article shall be deemed to have taken place where one of the following conditions is met:

1) the identity of the originator of the crypto-assets has been verified in accordance with Article 17 of this Law, and the information obtained during this verification has been retained in accordance with Article 127 of this Law;
2) the provision of Article 18 paragraph 2 of this Law applies to the originator of the crypto-assets.

The crypto-asset service provider of the originator shall not allow for the initiation or execution of the crypto-asset transfer if the conditions set out in paragraphs 1 to 10 of this Article are not met.

Batch file transfers of crypto-assets
Article 40g

In the case of a batch file transfer of crypto-assets from a single originator, the provision of Article 40f paragraph 2 of this Law shall not apply to individual transfers bundled together therein, provided that:

1) the batch file contains the data referred to in Article 40f paragraphs 2, 3 and 4 of this Law;
2) the data has been verified in accordance with Article 40f paragraph 9 of this Law;
3) individual transfers carry the distributed ledger address of the originator, if applicable under Article 40f paragraph 3 item 2 of this Law;
4) the originator's crypto-asset account number, if Article 40f paragraph 3 item 3 or paragraph 4 of this Law apply, contains a unique transaction identifier.

Obligations of crypto-asset service provider of the beneficiary
Article 40h

A crypto-asset service provider of beneficiary shall implement effective procedures, including, when necessary, monitoring during or after the transfer of crypto-assets, in order to determine whether the data on the originator and the beneficiary of the crypto-assets, as specified in Article 40f, paragraphs 2, 3 and 4 of this Law, are included in, or follow, the transfer or batch file transfer of crypto-assets.

In the case of a crypto-asset transfer made from a self-hosted address, the crypto-asset service provider of the beneficiary shall obtain and hold the data referred to in Article 40f paragraphs 2, 3 and 4 of this Law and ensure that the transfer of crypto-assets can be individually identified.

In addition to the measures referred to in Article 53c of this Law, for transfers exceeding EUR 1,000 from a self-hosted address, the crypto-asset service provider of the beneficiary shall take adequate measures to assess whether that address is owned or controlled by the beneficiary.

Before making the crypto-assets available to the beneficiary, the crypto-asset service provider shall verify the accuracy of the data on the beneficiary referred to in Article 40f paragraph 3 of this Law, based on documents, data, or information from a reliable and independent source.

The verification referred to in paragraphs 2, 3 and 4 of this Article is considered completed if at least one of the following conditions is met:

1) the identity of the beneficiary has been verified in accordance with Article 17 of this Law, and the information obtained through this verification are kept in accordance with Article 127 of this Law.
2) the provision of Article 18 paragraph 2 of this Law shall apply to the beneficiary.

Transfers of crypto-assets with missing or incomplete data
Article 40i

The crypto-asset service provider of the beneficiary shall implement effective procedures based on a risk assessment, including the measures referred to in Article 17 of this Law, in order to determine whether to execute, reject, return or suspend a transfer of crypto-assets lacking the required complete information on the originator and the beneficiary and for taking the appropriate follow-up action.

If the provider of services referred to in paragraph 1 of this Article determines that the data from Article 40f paragraphs 2, 3 and 4, or Article 40g of this Law are missing or incomplete, they shall, based on a risk assessment and without undue delay:

1) reject the transfer or return the transferred crypto-assets to the originator's account; or

2) request the required information on the originator and the beneficiary before making the crypto-assets available to the beneficiary.

If the crypto-asset service provider of the originator repeatedly fails to provide the required information on the originator or the beneficiary, the crypto-asset service provider of the beneficiary shall:

1) take measures which particularly include issuing a warning and setting deadlines before proceeding to a rejection, restriction or termination of the business relationship as described in item 2 of this paragraph, if the data is still not provided; or
2) directly reject any future transfers of crypto-assets from that crypto-asset service provider, restrict or terminate the business relationship with them.

The crypto-asset service provider of the beneficiary shall notify the competent supervisory authority about the crypto-asset service provider of the originator that repeatedly fails to provide accurate and complete data in accordance with this Article, as well as the actions taken against that provider of services in accordance with paragraphs 1, 2 and 3 of this Article.

Assessment and reporting
Article 40j

The crypto-asset service provider of the beneficiary shall determine whether the lack of accurate and complete data referred to in Article 40i of this Law represents grounds for suspicion in money laundering or terrorist financing, and if they determine that this lack constitutes grounds for suspicion, they shall notify the Financial Intelligence Unit in accordance with this Law.

Obligations of intermediary crypto-asset service providers
Article 40k

The intermediary crypto-asset service provider shall ensure that all received data about the originator and the beneficiary, which must be provided with the transfer of crypto-assets, are delivered with the transfer of crypto-assets.

The intermediary crypto-asset service provider shall maintain and keep records of the data referred to in paragraph 1 of this Article and allow access to the records to the competent authorities upon their request.

Detection of missing information on the originator or the beneficiary
Article 40l

The intermediary crypto-asset service provider shall implement effective procedures, including, where necessary, monitoring during or after the transfer of crypto-assets, in order to detect whether the data on the originator or the beneficiary referred to in Article 40f paragraph 2 items 1, 3 and 4, and paragraph 3 items 1, 2 and 3 of this Law have been provided previously, simultaneously, or concurrently with the transfer or batch file transfer of crypto-assets, including where the transfer is made to or from a self-hosted address.

Transfers of crypto-assets with missing or incomplete data on the originator or the beneficiary
Article 40m

The intermediary crypto-asset service provider shall establish effective procedures based on a risk assessment, including the measures referred to in Article 17 of this Law, for determining

whether to execute, reject, return or suspend a transfer of crypto-assets lacking the required information on the originator and the beneficiary and for taking the appropriate follow up action.

If the service provider referred to in paragraph 1 of this Article, upon receiving the crypto-asset transfer, determines that the data referred to in Article 40f paragraph 2 items 1, 3 and 4, and paragraph 3 items 1, 2 and 3 of this Law or Article 40g paragraph 1 of this Law are missing or incomplete, they shall, based on a risk assessment and without undue delay:

1) reject the transfer or return the transferred crypto-assets; or
2) request the missing data on the originator and the beneficiary before continuing with the transfer of crypto-assets.

If the crypto-asset service provider repeatedly fails to provide the required data about the originator or beneficiary, the intermediary crypto-asset service provider shall:

1) take actions which particularly include issuing a warning and setting deadlines before proceeding to a rejection, restriction or termination of the business relationship as described in item 2 of this paragraph, if the data is not provided; or
2) directly reject any future transfers of crypto-assets to that crypto-asset service provider, restrict or terminate the business relationship with them.

The intermediary crypto-asset service provider shall notify the competent supervisory authority about the crypto-asset service provider that repeatedly fails to provide accurate and complete data, as well as the actions they have taken in accordance with paragraphs 1 to 3 of this Article.

Assessment and reporting
Article 40n

The intermediary crypto-asset service provider shall determine whether the lack of accurate and complete data referred to in Article 40m of this Law during the transfer of crypto-assets or related transactions represent grounds for suspicion in money laundering or terrorist financing, and if they find that the lack of such data represents grounds for suspicion, they shall report this to the Financial Intelligence Unit in accordance with this Law.

Exceptions to the obligation to collect data about the originator and the beneficiary
Article 40o

The provisions of Articles 40f to 40n of this Law shall not apply in the following cases:

- when both the originator and the beneficiary are crypto-asset service providers acting on their own behalf and for their own account; or
- when the transfer is made as a transfer of crypto-assets between persons.

Provision of information
Article 40p

Crypto-asset service providers shall, fully and without delay, provide the data collected in accordance with this Law to the competent authorities and supervisory bodies, upon their request, including through a central contact point from Article 62, paragraph 8 of this Law.

This provision shall also apply to payment service providers.

Reputation
Article 40r

A natural person is considered to have reputation under this Law if:

1) no criminal proceedings are being conducted against them, and they have not been convicted of a criminal offense punishable by unconditional imprisonment for one or more years;
2) no criminal proceedings are being conducted against them, and they have not been convicted of a crime under the laws of other states that correspond to the criminal offenses referred to in paragraph 1, point 1 of this Article;
3) as a legal representative of a legal person or business organization, they have not violated the provisions of this Law;
4) they have not been an associate of a person convicted of money laundering and/or terrorist financing crimes;
5) their relevant authorization or approval to conduct business has not been revoked or denied by the competent authority due to non-compliance with regulations;
6) they do not manage or, at the time of committing the criminal offense, did not manage a legal person or business organization that was convicted of any of the criminal offenses referred to in paragraph 1, items 1 and 2 of this Article, especially if no security measure of prohibiting the exercise of a profession, activity or duty has been imposed on them;
7) there is no suspicion that they have committed money laundering or terrorist financing crimes.

Criminal offenses referred to in paragraph 1 item 1 of this Article include the following: criminal offenses against payment operations and economic business, criminal offenses against life and body, criminal offenses against the freedoms and rights of individuals, criminal offenses against labor rights, criminal offenses against the environment and spatial planning, criminal offenses against public safety of people and property, criminal offenses against computer data security, criminal offenses against legal traffic, criminal offenses against intellectual property, and criminal offenses against official duties.

When assessing the circumstances referred to in paragraph 1 of this Article, the supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall consider all available information related to the type of decision, the stage of the procedure, declared legal remedies, imposed sanctions, mitigating and aggravating circumstances, the gravity of the offense, the time elapsed since the offense was committed, and the behavior of the individual at that time, as well as all available information on procedures, supervisory measures, and reports filed by supervisory bodies from Article 131 paragraph 1 of this Law or similar supervisory bodies from other states, as well as the fact that the presence of several minor offenses under this Law may damage the reputation of a natural person even if they do not individually have this effect.

When assessing the circumstances referred to in paragraph 1 of this Article the supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall particularly evaluate the data and information obtained from the Financial Intelligence Unit.

4. Establishing beneficial owner

Beneficial owner

Article 41

A beneficial owner shall be a natural person that ultimately owns or controls a legal person, business organization, trust, other person or a subject of international law equal to them, or a natural person on whose behalf or for whose account transaction is being executed or a business relationship is established.

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

1) directly or indirectly holds at least 25% of shares, voting rights, or other rights in a legal person, or a business organization, including the right to profit share, other internal resources, or liquidation balance; or
2) directly or indirectly has significant influence over the business and decision-making processes of a legal person, or a business organization through ownership share; or
3) controls a legal person, or a business organization via other means.

Where at least 25 % of the shares or voting rights or other ownership interest in a legal person, or a business organization are owned by a legal person or a business organization, the beneficial ownership should be determined having regard to the specific structure of the shareholder, including whether any natural person exercises control via other means over a shareholder.

A natural person who is jointly responsible for the obligations of a partnership or other legal person or business organization shall be considered the ultimate beneficial owner of that legal person or business organization, regardless of the percentage of shares or voting rights in that legal person or business organization.

The identification of an ultimate beneficial owner based on control via other means shall be conducted independently of and in parallel to the identification of the beneficial owner referred to in paragraph 2 items 1 and 2 of this Article.

A person shall be considered to control a legal person or business organization via other means if they have:

- the majority of voting rights, whether or not shared by persons acting in concert;
- the right to appoint or remove a majority of the board members (directors, supervisory board members, management board members, or similar officers);
- the veto rights or other relevant decision rights attached to ownership in the legal person or business organization;
- the right to make decisions regarding the distribution of profits or a shift in assets in the legal person or business organization.

Depending on the organizational structure of a legal person or business organization, control over a legal person or business organization via other means may include decision-making rights based on:

- formal or informal agreements with owners, members or a legal person or business organization, provisions in the articles of association, partnership agreements, syndication agreements, or equivalent documents or agreements depending on the specific characteristics of a legal person or business organization;
- relationships between family members;
- use of formal or informal nominee arrangements.

Where it is not possible to identify the beneficial owner or if there is suspicion that the natural person referred to in paragraphs 2, 3 and 4 of this Article is the beneficial owner, the beneficial owner of the legal person or business organization shall be considered to be one or more persons holding managerial positions in that legal person or business organization.

The beneficial owner of an association, non-governmental organization, institution, political party, religious community, artistic organization, chamber, trade union, employers' association, or other business entity is any natural person who has control over the management of the entity's assets.

Where it is not possible to determine the beneficial owner according to paragraph 9 of this Article, the beneficial owner of an association, non-governmental organization, institution, political party, religious community, artistic organization, chamber, trade union, employers' association, or other business entity is any natural person authorized to represent that entity.

The beneficial owner of a trust, other person or a subject of international law equal to them shall be a natural person who receives, manages, or distributes assets for specific purposes and who:

1) is the settlor of the trust, other person or a subject of international law equal to them;
2) is the trustee of the trust, other person or a subject of international law equal to them;
3) is the beneficiary of the assets acquired from the managed property, where the future beneficiaries are already determined or can be determined;
4) represents the interests of the recipients of the acquired assets;
5) belongs to the category of persons with an interest in establishing the trust, other person or a subject of international law equal to them when the legal and/or natural person benefiting from it is yet to be determined;
6) otherwise, directly or indirectly controls the assets of the trust, other person or a subject of international law equal to them.

For a foundation similar to a trust, the beneficial owner is a natural person who:

1) is the founder of the foundation;
2) is a member of the foundation’s management body;
3) is a member of the foundation’s supervisory body;
4) is a beneficiary or a category of beneficiaries;
5) directly or indirectly controls the foundation.

If the founder, management body member, or supervisory body member of a foundation similar to a trust is a legal person, business organization or arrangement, the beneficial owners of that legal person, business organization or arrangement are the beneficial owners of the foundation similar to a trust.

If the natural person who is the beneficiary of a foundation similar to a trust has not been determined, the category of beneficiaries in whose primary interest the foundation has been established or for whose benefit it operates shall be determined, so that the beneficiaries from the previously determined category are identified as the beneficial owners as soon as they are identified or determined.

Manner of identifying the beneficial owner
Article 42

A reporting entity shall identify the beneficial owner of the legal person, business organization, trust, other person or a subject of international law equal to them by obtaining data on these subjects, their beneficial owners and category of persons with an interest in establishing a trust, other person or a subject of international law equal to them referred to in Article 44 of this Law.

A reporting entity may obtain data referred to in paragraph 1 of this Article by accessing the register referred to in Article 43 paragraph 1 of this Law, CBR or any other relevant public register, as well as by accessing the court, business and other public register where the foreign legal person or business organization is entered, whereby they shall print out the excerpt from that register and note the date and time and the name and surname of the person who accessed the register.

A reporting entity may also obtain the data referred to in paragraph 1 of this Article by checking the original or a certified photocopy of the document from CBR or any other relevant public register, as well by checking the original or a certified photocopy of the document from the court, business and any other public register where the foreign legal person or business organization is entered, 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 the Financial Intelligence Unit and the administration body responsible for tax collection.

A reporting entity shall obtain the data not contained in registers or in the documents referred to in paragraphs 2 and 3 of this Article, by checking the original or a certified photocopy of the identification document or any other documentation, submitted by the legal representative or authorized person of the customer that is a legal person or business organization.

A reporting entity shall, in addition to the data referred to in paragraph 1 of this Article, also obtain the documentation based on which it is possible to establish the ownership structure and the controlling member of the customer, as well as the data on beneficial owner.

A reporting entity shall verify the obtained data on the beneficial owner of a legal person, business organization, trust, other person or a subject of international law equal to them, by ensuring complete and clear insight into the beneficial ownership and management body of the customer in accordance with risk analysis, whereby upon such verification, the reporting entity must not rely solely on the data from the register referred to in Article 43 paragraph 1 of this Law.

A reporting entity shall, in the procedure of identification of the beneficial owner referred to in paragraph 1 of this Article, obtain a photocopy of a personal identification document of the beneficial owner in accordance with Article 22 paragraph 3 of this Law.

If the reporting entity, while collecting data referred to in paragraphs 2, 3, 5, 6 and 7 of this Article, doubts the veracity of obtained data or authenticity of personal identification documents or other documentation from which the data were obtained, they shall obtain a written statement thereof from the legal representative or authorized person.

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

A reporting entity shall keep records on the measures they have taken to identify the beneficial owner referred to in paragraph 1 of this Article.

Beneficial Owners Register
Article 43

Beneficial Owners Register is an electronic database where the data on beneficial owners are maintained and kept in order to ensure the transparency of ownership structures and to implement measures for the prevention of money laundering and terrorist financing.

Beneficial Owners Register is kept by the administrative body responsible for tax collection.

A legal person, business organization, an association, non-governmental organization, institution, political party, religious community, art organization, chamber, trade union, employers' association, foundation or other business entity, a legal person that receives, manages or allocates the funds for specific purposes, trust, other person or a subject of

international law equal to them that receives, manages or allocates the funds for specific purposes, shall enter the data on beneficial owners and any changes regarding beneficial owners into the Beneficial Owners Register within eight days from the date of their entry into the CBR or register of taxpayers, or within eight days from the change of data on the beneficial owner.

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

- entrepreneur,
- public sector in the context of the law regulating the time limits for settlement of financial obligations, and
- legal persons and business organizations in multi-member joint stock companies whose shares are traded on the organized securities market, where they are obliged to comply with the obligation to publish data and information on beneficial ownership pursuant to the law regulating rights and obligations of the entities in the securities market and other law.

Entities referred to in paragraph 3 of this Article shall verify and confirm the accuracy of data entered into the Beneficial Owners Register once a year, and no later than 31 March of the current year.

The beneficial owner of the entity referred to in paragraph 3 of this Article shall submit to that entity the data referred to in Article 44 paragraph 1 item 2 indents 1, 2 and 4 of this Law for the purpose of entering those data into the Beneficial Owners Register.

The entities referred to in paragraph 3 of this Article and their beneficial owners shall be responsible for the accuracy of data entered into the Beneficial Owners Register.

The Ministry shall prescribe the manner of verification of the data from the Beneficial Owners Register.

Trust Register
Article 43a

The Trust Register is an electronic database where data about trusts, other persons or subjects of international law equal to them are kept and maintained.

The Trust Register is kept by the administrative body responsible for tax collection.

The Trust Register shall contain the data referred to in Article 44 paragraph 1 items 1 and 3 of this Law.

If the person managing the trust, other person or a subject of international law equal to them is located or resides in another country, the data on the trust, other person or a subject of international law equal to them shall be entered into the register referred to in paragraph 1 of this Article, when that person enters into a business relationship or acquires immovable property in the name of the trust, other person or a subject of international law equal to them in Montenegro, within 15 days from the date of concluding the business relationship or acquiring the immovable property.

The request for registration in the Trust Register must be submitted to the administrative body responsible for tax collection by the person with whom the person managing the trust, other person or a subject of international law equal to them entered into a business relationship, or by a notary when the trust, other person or a subject of international law equal to them acquires immovable property, within five days from the date the establishment of business relationship or the date the notarial deed regarding the acquisition of immovable property was made.

For a trust, other person or a subject of international law equal to them, after registering in the Trust Register, a registration must also be made in the Beneficial Owners Register.

The registration in the Beneficial Owners Register is made by the person managing the trust, other person or a subject of international law equal to them referred to in paragraph 4 of this Article, within 25 days from the date when the business relationship was concluded or the immovable property was acquired.

Notwithstanding paragraph 6 of this Article, if the person managing the trust, other person or a subject of international law equal to them has residence or headquarters in several other countries, or if in the name of the trust, other person or a subject of international law equal to them, immovable property is acquired in several other countries or multiple business relationships are established in several other countries, a certificate as proof of registration or an extract with information on beneficial ownership maintained in the register of one of the other countries can be considered sufficient proof for fulfilling the obligation to register in the Beneficial Owners Register.

Content of the Beneficial Owners Register
Article 44

The Beneficiary Owners Register shall contain the following data:

1) data on the entity referred to in Article 43 paragraph 3 of this Law, as follows:
   - name, address, seat, unique master citizen number or any other identification number, tax identification number (hereinafter: TIN), date of registration and date of deletion from the CBR or from the register of tax payers;
   - data on the status;
   - form of organization;
   - codes of business activity;
   - data on legal representative, proxy or authorized person (name and surname, unique master citizen number, date of birth, address of permanent or temporary residence, TIN, citizenship);
   - data on natural person registered as a member of a managing body (name and surname, unique master citizen number, date of birth, address of permanent or temporary residence, TIN, citizenship);
   - the amount of the share (registered) capital;
   - data on members, i.e. founders and percentage of their share or the number and percentage of their shares (name and surname, unique master citizen number, date of birth, address of permanent or temporary residence, TIN, citizenship, ownership interest - percentage of shares or percentage of participation in capital or data on percentage of direct or indirect control over property or data on the percentage of beneficiary's income derived from the property they manage or the participation in the property of the legal person or other subject of international law);
   - graphic view of the ownership structure if the reporting entity has a complex ownership structure;
   - address for receiving mail;
   - e-mail address;
   - number of accounts in credit institutions;
   - scanned documentation providing proof of entered data;

2) data on the beneficial owner, as follows:

- name and surname, unique master citizen number, date of birth, address of permanent or temporary residence, TIN, citizenship;
- data on ownership share (percentage of shares or percentage of participation in capital or data on percentage of direct or indirect control over property or data on the percentage of beneficiary's income derived from the property they manage or the participation in the property of the legal person or other subject of international law) or other type of control (data on whether the owner has a controlling influence in property management, whether they directly provide/have provided funds or whether they have controlling influence to decision making or a controlling position in management);
- date of registration, date of change, and/or date of updating and deleting of the beneficial owner from the Beneficial Owners Register;
- scanned documentation providing proof of entered data;

3) data on the category of persons with the interest in establishing the trust, other person or a subject of international law equal to them when persons obtaining benefit from the trust, other person or a subject of international law equal to them (name and surname of the founder or trustee of the trust, beneficiary of assets acquired from the property managed when the future beneficiaries have already been determined or may be determined with the trust or representative of interests of the recipients of the acquired assets of the trust, unique master citizen 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 regulating the requirements for entry, movement and residence of foreigners to the territory of Montenegro).

Entry of data into the Beneficial Owners Register
Article 45

Entities referred to in Article 43 paragraph 3 of this Law, shall enter and update in the Beneficial Owners Register the data:

1) referred to in Article 44 paragraph 1 item 1 of this Law;
2) on the beneficial owner referred to in Article 44 paragraph 1 item 2 of this Law;
3) on the category of persons with an interest for establishing a trust, other person or a subject of international law equal to them when persons who benefit from trust, other person or a subject of international law equal to them are yet to be determined referred to in Article 44 paragraph 1 item3 of this Law.

In addition to data referred to in paragraph 1 of this Article, entities referred to in Article 43 paragraph 3 of this Law that have a complex ownership structure shall also enter into the Beneficial Owners Register the following:

- a note on the existence of a complex ownership structure of that entity;
- document in electronic form containing graphics of the ownership structure;
- original or a certified photocopy of the document from the CBR or any other relevant public register, and the original or a certified photocopy of the document from the court, business or any other public register where foreign legal person or business organization has been entered, which must not be older than three months of its issue date, in electronic form, for any legal person, trust or legal arrangement which is included in ownership structure;

- data on the owner that is a legal person, legal arrangement, or another subject of international law (name, address, registered office, country of registered office, registration number or other identification number, and TIN).

A complex ownership structure within the meaning of paragraph 2 of this Article is the ownership structure where the founder, or the owner of the entity referred to in Article 43 paragraph 3 of this Law is at least one legal person or a legal arrangement or any other subject of international law.

The Ministry shall prescribe the manner of entry and update of data into the Beneficial Owners Register, and the detailed content of the scanned documentation.

Maintaining and managing the Beneficial Owners Register
Article 46

The administrative body responsible for tax collection shall maintain and manage the Beneficial Owners Register in such a manner that:

- in addition to keeping the last entry of the data referred to in Article 44 of this Law, it shall keep the previous data entries from the moment of its registration, as well as all changes and deletions of data, according to time and type of change;
- the last entry of data will be available to reporting entities whenever they need such data;
- it shall enable unlimited access to all data kept in the Beneficial Owners Register to the Financial Intelligence Unit, supervisory authorities referred to in Article 131 paragraph 1 of this Law, other authorities competent for prevention and detection of money laundering and related predicate criminal offences or terrorist financing;
- the data shall be available for a period of five years after deletion of entity referred to in Article 43 paragraph 3 of this Law from CBR or from the register of tax payers, to the Financial Intelligence Unit, supervisory authorities referred to in Article 131 paragraph 1 of this Law and to other authorities competent for the prevention and detection of money laundering and related predicate criminal offences or terrorist financing.

Access to the data from the Beneficial Owners Register
Article 47

Access to the data from the Beneficial Owners Register shall be granted to:

(1) the Financial Intelligence Unit, supervisory bodies referred to in Article 131 paragraph 1 of this Law and competent authorities referred to in Article 96 paragraph 1 of this Law;
(2) reporting entities, and
(3) other legal and natural persons.

Entities referred to in paragraph 1 item 1 of this Article shall have direct electronic access to all data from the Beneficial Owners Register and may exchange them with the Financial Intelligence Unit, supervisory authorities and other competent authorities of other EU Member States, in accordance with the provisions of this Law, in a timely manner and free of charge.

Reporting entities shall have direct electronic access to data on beneficial owners entered into the Beneficial Owners Register, for the purpose of conducting the customer identification procedure.

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

Entities referred to in Article 43 paragraph 3 of this Law may submit to the administrative body responsible for tax collection a request for restricting or denying legal or natural persons referred to in paragraph 1 item 3 of this Article the access to all or to a part of the data referred to in paragraph 4 of this Article, if the access to those data would expose the beneficial owner to a risk of fraud, kidnapping, blackmail, violence or intimidation or if the beneficial owner is a child or a person deprived of legal capacity.

Financial Intelligence Unit shall establish the existence of circumstances referred to in paragraph 5 of this Article by a decision.

When the Financial Intelligence Unit establishes the existence of circumstances referred to in paragraph 5 of this Article, the administrative body responsible for tax collection shall restrict or deny the legal or natural persons referred to in paragraph 1 item 3 of this Article access to all or to a part of data covered by the request referred to in paragraph 5 of this Article.

An administrative dispute may be initiated against the decision referred to in paragraph 6 of this Article.

The Ministry shall prescribe the detailed manner of accessing data from the Beneficial Owners Register.

Supervision of data entry into the Beneficial Owners Register
Article 48

When performing supervision of entities referred to in Article 43 paragraph 3 of this Law, the administrative body responsible for tax collection shall verify if:

- those entities possess the data on beneficial owners referred to in Article 44 paragraph 1 item 2 of this Law and whether those data are complete and identical to data from reliable sources;
- those entities have entered into the Beneficial Owners Register the data referred to in indent 1 of this paragraph and within the time limits prescribed by this Law.

Within the supervision referred to in paragraph 1 of this Article, the administrative body responsible for tax collection shall perform on-site and off-site inspection pursuant to Article 132 of this Law.

Entities referred to in Article 43 paragraph 3 of this Law shall, upon a request of the administrative body responsible for tax collection, submit documentation based on which it is possible to establish the ownership structure and the controlling member of the customer and to collect data on the beneficial owner.

If, during the supervision referred to in paragraph 1 of this Article, the administrative body responsible for tax collection determines a discrepancy in the data in the Beneficial Owners Register compared to the data from reliable sources, they shall order the entity referred to in Article 43 paragraph 3 of this Law to correct the errors in the Beneficial Owners Register. Until these errors are corrected, it will indicate in the Beneficial Owners Register that the data for that subject is outdated.

The entity referred to in Article 43 paragraph 3 of this Law shall comply with the order from paragraph 4 of this Article within three working days from the date of receiving the order.

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

Customer due diligence
Article 49

A reporting entity shall conduct CDD measures, including the control of transactions and tracing the sources of funds the customer uses in their business activity, whereby they shall collect the data referred to in Article 117 paragraph 1 items 6 and 7 and paragraph 3 to 6 of this Law, depending on the type of reporting entities.

Measures referred to in paragraph 1 of this Article, shall include, in particular, the following:

1) verification of compliance of customer's business activity with the nature and purpose of the business relationship;
2) control of transactions in accordance with the level of customer's risk of money laundering and terrorist financing;
3) monitoring and verification of compliance of customer's business activity with their usual scope of business activity;
4) verification of sources of funds that the customer uses in their business activity or in executing transactions in accordance with their level of risk of money laundering and terrorist financing;
5) monitoring and updating the data on the customer, beneficial owner of the customer and level of risk of money laundering and terrorist financing, and verification of data whether the customer or beneficial owner has become or ceased to be a politically exposed person referred to in Article 54 paragraphs 2, 3 and 4 of this Law.

A reporting entity shall provide and adjust the scope and dynamics of implementation of measures referred to in paragraph 1 of this Article to the risk of money laundering and terrorist financing to which the beneficial owner is exposed in performing a 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 on whether the customer or beneficial owner of the customer has become or ceased to be a politically exposed person referred to Article 54 paragraphs 2, 3 and 4, by accessing to CPR, record of issued personal identification documents, Beneficial Owners Register, CBR, register referred to in Article 55 paragraph 1 of this Law or any other relevant public register, or by accessing the original or certified photocopy of the document from CBR or other relevant public register.

A reporting entity shall obtain the data not included in registers, records and documents referred to in paragraph 4 of this Article by checking the original or certified photocopy of the personal identification document or other documentation which, upon reporting entity's request, shall be submitted by the customer.

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

A reporting entity shall ensure that the monitoring of the business relationship with a high-risk customer, as per paragraph 3 of this Article, does not exceed six months, and for a low-risk customer, it does not exceed two years.

Annual control
Article 50

In addition to CDD and control of transactions pursuant to Article 49 of this Law, the reporting entity shall, at least once a year, no later than one year after the last control, perform the control of the customer who is:

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

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

1) obtaining, or verification of data referred to in Article 117 of this Law;
2) obtaining, or verification of data referred to in Article 44 of this Law;
3) obtaining the authorization referred to in Article 28 paragraph 2 of this Law.

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

1) on the address and head office of the business unit of the foreign legal person;
2) referred to in Article 117 paragraph 1 item 3 of this Law related to the legal representative of a business unit of the foreign legal person.

A reporting entity shall obtain data referred to in paragraphs 2 and 3 of this Article by accessing the CPR, records of issued personal identification documents, Beneficial Owners Register, CBR, court, business or other relevant public registers where the foreign legal person has been entered, as well as by checking the original or certified photocopy of a document from the CBR, court, business or other relevant public register where the foreign legal person has been entered.

A reporting entity shall obtain data which are not contained in registers, records and identification documents referred to in paragraph 4 of this Article, by checking the original or certified photocopy of the identification document or other documentation which, upon the reporting entity's request, shall be provided by the customer. If, during the verification of the data referred to in paragraph 2 of this Article, the reporting entity establishes a difference in data, they shall call the customer for the purpose of verification of all relevant information. Notwithstanding paragraphs 1 to 6 of this Article, in the case referred to in Article 61 paragraph 1 of this Law, the reporting entity shall not be obliged to perform the annual control of a foreign legal person.

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

Types of special CDD measures

Article 51

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

1) Enhanced CDD measures,
2) Simplified CDD measures

Cases when enhanced CDD measures are applied

Article 52

A reporting entity shall apply enhanced CDD measures in sectors and business activities referred to in Article 7 paragraph 1 indent 3 of this Law, as well as in cases when higher risk of money laundering and terrorist financing is established, as follows:

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

A reporting entity shall also apply enhanced CDD measures in other cases when it assesses 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 higher risk of money laundering and terrorist financing.

Notwithstanding paragraph 1 of this Article, enhanced CDD measures shall not be automatically applied in relation to branches and subsidiary undertakings that are majority owned by the reporting entities with their head offices in Montenegro, which are located in high risk third countries, where the operations of those branches or subsidiary undertakings fully comply with the policies and procedures of the group they belong, in accordance with the reporting entity's risk assessment.

Enhanced CDD measures in correspondent relationship with credit or other financial institution whose head office is situated outside Montenegro

Article 53

When establishing the correspondent relationship which includes execution of payments with a credit or other financial institution whose head office is situated outside Montenegro, which is the respondent, the reporting entity shall, in addition to measures referred to in Article 17 of this Law, take additional measures, as follows:

1) obtain a license to perform banking services, as well as issuance date, name and head office of the competent authority that issued the license;
2) obtain documentation on internal procedures carried out for the purpose of prevention and detection of money laundering and terrorist financing, in particular on the procedures of customer verification, beneficial owner identification, reporting data on suspicion transactions, activities and customers to competent authorities, records keeping, internal controls and other procedures which a credit or other financial institution has established in relation to the prevention and detection of money laundering and terrorist financing;

3) obtain data, information and documentation on the internal controls' assessment of implementation of measures for the prevention of money laundering and terrorist financing within the credit or other financial institution;
4) obtain data and information on legal or institutional arrangements in the area of prevention and detection of money laundering and terrorist financing which are implemented in other country where the credit institution or other financial institution has a head office or is registered;
5) verify whether the credit or other financial institution, in accordance with the law of a country where its head office is situated or registered, implements relevant regulations in the area of prevention and detection of money laundering and terrorist financing, including the information on whether such 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) establish that credit or other financial institution has not established or does not establish business relationships or execute transactions with shell (fictious) banks;
8) establish that credit or other financial institution with reference to a brokerage account has verified the customer's identity and has performed ongoing procedure of applying CDD measures to a customer that has a direct access to the account and that, upon the reporting entity's request, is able to provide relevant data in relation to that procedure;
9) ensure that all information established during the procedure of conducting CDD measures is provided by the responding institution without delay.

Prior to establishing a correspondent relationship with the respondent, the reporting entity shall obtain the written consent of the senior manager for establishing such business relationship.

When entering into a correspondent relationship, the reporting entity shall regulate their responsibility and the responsibility of the respondent by a contract.

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 a complete understanding of the nature of its business activities and establishing the reputation of that institution from publicly available sources.

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

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

A reporting entity must not establish or continue a correspondent relationship with a credit or other financial institution which has its head office situated outside Montenegro if:

1) it previously failed to take measures referred in paragraphs 1 to 4 of this Article,
2) a credit or other financial institution does not have in place controls of the system for the prevention of money laundering and terrorist financing or does not implement laws and other regulations in 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 or maintains correspondent or other business relationships and carries out transactions with shell (fictious) banks.

Guidelines on the application of enhanced CDD measures during the provision of crypto-asset service

Article 53a

The supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall establish guidelines that determine the manner in which enhanced CDD measures referred to in Articles 51, 52 and 53 of this Law, shall be applied when reporting entities provide crypto-asset services, excluding the provision of advice on crypto-asset and crypto-asset transfer services, as well as the manner in which reporting entities shall collect additional information about the originator and beneficiary of crypto-assets.

Risk mitigating measures

Article 53b

Crypto-asset service providers shall determine and assess the risk of money laundering and terrorist financing associated with crypto-asset transfers made to a self-hosted address or originating from such an address and to establish internal policies, procedures, and controls for these purposes.

Crypto-asset service providers shall apply risk mitigating measures that correspond to the identified risks.

The measures referred to in paragraph 2 of this Article shall include at least the following:

1) risk-based measures to establish and verify the identity of the originator or beneficiary of a crypto-asset transfer made to or from a self-hosted address, including reliance on third parties;
2) requesting additional information regarding the origin and destination of the transferred crypto-asset;
3) implementing enhanced ongoing monitoring of these transactions;
4) other measures to mitigate the risks of money laundering and terrorist financing, as well as the risks of non-compliance and evasion of targeted financial sanctions and financial sanctions related to the financing of weapons of mass destruction (proliferation), as well as managing those risks.

The supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law will establish guidelines for determining the measures referred to in paragraphs 2 and 3 of this Article, as well as criteria and means for identifying and verifying the identity of the originator or beneficiary of a crypto-asset transfer made to a self-hosted address or originating from that address, particularly by relying on third parties, taking into account the latest technological advancements.

Measures to be taken regarding cross-border correspondent relationships involving crypto-asset services

Article 53c

In addition to the measures referred to in Article 53 of this Law, regarding cross-border correspondent relationships involving the provision of crypto-asset services, except for providing advice on crypto-asset, with a respondent that does not have registered office in Montenegro and provides similar services, including crypto-asset transfers, the crypto-asset service provider shall:

1) determine whether the respondent has a license to operate or is registered;
2) gather sufficient information about the respondent to fully understand the nature of their business and assess the respondent's reputation and the quality of the supervision of their business based on publicly available information;
3) assess the respondent's AML/CFT control;
4) obtain written approval from a senior manager before establishing a new correspondent relationship;
5) document the responsibilities of each party in the correspondent relationship;
6) in relation to transit accounts for crypto-assets, ensure that the respondent has verified the identity and implemented enhanced CDD measures for customers who have direct access to the correspondent's accounts, and that the respondent can provide relevant data regarding those measures to the correspondent upon request.

Crypto-asset service providers shall document the decision to terminate correspondent relationships for reasons related to AML/CFT policies.

Crypto-asset service providers shall regularly update information regarding the implementation of enhanced CDD measures in relation to the correspondent relationship or when new risks arise concerning the respondent.

Crypto-asset service providers shall consider the information referred to in paragraph 1 of this Article to assess the appropriate measures to mitigate risks related to the respondent based on the risk assessment.

The supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall establish guidelines for determining the criteria and elements that crypto-asset service providers shall consider when conducting the assessment referred to in paragraph 1 of this Article and the risk mitigation measures referred to in paragraph 4 of this Article, including the minimum measures that crypto-asset service providers must take if the respondent is not registered or does not have a license to operate.

Politically exposed persons
Article 54

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

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

1) President of Montenegro, President of Montenegrin Parliament, President, member and the Secretary General of the Government;
2) Member of the Parliament;
3) president of a political party and their deputy, a member of presidency of a political party, and their deputies, member of an executive board, member of a general board and other officials of a political party;
4) State Secretary, Director General of a ministry and Secretary of a ministry;

5) the President and a judge of the Supreme court of Montenegro and the president and a judge of Constitutional court of Montenegro;
6) Supreme State Prosecutor, Special State Prosecutor and a 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) mayor, president of a municipality, president of Assembly of the Capital, president of Assembly of Royal Capital and president of the municipal assembly;
9) Director of the National Security Agency and director of the Agency for Prevention of Corruption;
10) an ambassador, consul, chief of General Staff of Army of Montenegro, general and admiral of the Army of Montenegro;
11) director, deputy or assistant director and member of management body and supervisory authority of the legal person that is majority-owned by the state.

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

1) President of a State, Prime Minister, minister and their deputy;
2) Member of Parliament;
3) Member of a 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 legal remedy;
5) Member of 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 management body and supervisory authority of the legal person that is majority-owned by the state;
8) director, deputy or assistant director and member of a board or other relevant position in international organization.

Members of immediate family of the person referred to in paragraphs 2 and 3 of this Article and their close associates shall also be politically exposed persons.

Members of the immediate family of the person referred to in 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, adopter, adoptee, foster parent or foster child.

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

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

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

A person referred to in paragraphs 2, 3 and 4 of this Article shall also be considered a politically exposed person during the period of two years following termination of performing a public office.

Following the expiration of the time limit referred to in paragraph 8 of this Article, the reporting entity shall implement CDD measures based on the risk analysis, and establish if, in relation to that person there is still a higher risk of money laundering and terrorist financing.

Register of politically exposed persons
Article 55

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

Financial Intelligence Unit, reporting entities and supervisory authorities referred to in Article 131 paragraph 1 of this Law shall have direct electronic access to data from the Register of politically exposed persons.

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

Register of politically exposed persons shall be kept and maintained by the Agency for Prevention of Corruption.

The Agency for Prevention of Corruption shall define the manner of keeping the Register of politically exposed persons and its content.

Application of enhanced CDD measures to a customer or its beneficial owner who is a politically exposed person
Article 56

In case where the customer is a politically exposed person, in addition to measures referred to in 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 in the transaction with that customer;
2) obtain written consent of a senior manager to establish business relationship with that customer before establishing such business relationship, and if the business relationship has already been established, obtain written consent of the senior manager to continue such business relationship;
3) establish whether that customer is the beneficial owner of the legal person, business organization, trust, other person or a subject of international law equal to them, or natural person with a registered office in another country on whose behalf the business relationship is established, transaction executed or other customer's activity conducted.
4) after establishing the business relationship, monitor, with due diligence, transactions and other business activities performed by the politically exposed person with the reporting entity, or activities performed by the customer whose beneficial owner is politically exposed person.

A reporting entity shall, pursuant to guidelines referred to in Article 12 paragraph 5 of this Law, by internal act, define procedures which are based on risk analysis implemented in relation to identifying a customer who is a politically exposed person or by identifying the beneficial owner of a customer who is a politically exposed person, as well as upon monitoring business activities of that customer and beneficial owner.

Measures related to politically exposed persons with regard to life insurance
Article 56a

A reporting entity shall implement adequate measures to determine whether the beneficiaries of a life insurance or life insurance related to investment units and beneficial owners of the beneficiaries are politically exposed persons.

The measures referred to in paragraph 1 of this Article shall be taken no later than at the time of the payout of insurance policy or at the time of the assignment, in whole or in part, of the policy.

Where there are higher risks identified, in addition to applying measures laid down in Article 17 of this Law, the reporting entity shall take the following additional measures:

1) notify senior management before payout of policy proceeds;
2) conduct enhanced due diligence measures of a customer that is a policyholder and where there are reasonable grounds to suspect of money laundering or terrorist financing, notify the Financial Intelligence Unit in accordance with Article 66 of this Law.

A reporting entity shall implement the measures referred to in paragraph 3 of this Article also in respect of the members of immediate family and close associates of a person referred to in Article 54 paragraphs 2 and 3 of this Law.

Enhanced CDD measures when providing custody services
Article 57

When providing custody services to a customer, in addition to measures referred to in 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 a business relationship with that customer before establishing the business relationship, and if the business relationship has already been established, obtain written consent of a senior manager for continuation of the business relationship,
3) establish whether the customer concludes custody services agreement on their own behalf and for their own account or it is a sub-custody (a credit institution or other legal person who on its own behalf and for the account of third persons – its customers to whom it provides custody services, concludes custody services agreement with the reporting entity);
4) when executing any transaction, in the case of sub-custody, establish for whose account the sub-custody executed the transaction.

Where the reporting entity is not able to implement measures referred to in paragraph 1 of this Article the business relationship shall not be established, and where the business relationship has been established, the reporting entity shall terminate such a relationship.

Enhanced CDD measures in complex and unusual transactions
Article 58

In the case of transactions that are complex or unusually large, as well as transactions executed in an unusual manner or without apparent economic justification or legal purpose or that deviate from the usual or expected customer's business activity, and for which it has not been possible to assess whether they are suspicious transactions, in addition to measures referred to in 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 the beneficial owner;

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

A reporting entity shall, upon a request from the Financial Intelligence Unit or a competent supervising authority referred to in Article 131 paragraph 1 of this Law, make available the results of the analysis referred to in paragraph 1 item 6 of this Article.

A reporting entity shall define by an internal act the criteria for recognising transactions referred to in paragraph 1 of this Article.

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

In the case of establishing a business relationship or executing transactions with a person from a high-risk third country or when a high-risk third country is included in transaction, in addition to measures referred to in Article 17 of this Law, the reporting entity shall:

1) take measures referred to in Article 58 paragraph 1 of this Law;
2) before establishing a business relationship, obtain a written consent of a senior manager for establishing business relationship with that customer, and where the business relationship has already been established, obtain a written consent of a senior manager for continuing the business relationship.

After establishing a business relationship with a customer from a high-risk third country, the reporting entity shall apply enhanced CDD measures to the business relationship and transactions performed by that customer by:

- increasing the number and frequency of performed controls and choose the manners for executing transactions requiring further examination;
- ensuring more frequent reporting to the compliance officer for prevention of money laundering and terrorist financing on transactions;
- limiting business relationships or transactions with customers from countries included in the list referred to in Article 60 of this Law.

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

When implementing measures referred to in paragraph 2 of this Article, the reporting entity shall consider the relevant assessments or reports of international organisations or experts for determining standards in the area of prevention of money laundering and terrorist financing, and in connection with risks that some third countries may pose.

List of high-risk third countries
Article 60

Financial Intelligence Unit shall determine and publish the list of high-risk countries on its website.

Simplified CDD measures

Article 61

If in the cases referred to in Articles 18 paragraph 1 items 1, 2, 3 and 6 of this Law, in respect of 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 is no reason to suspect or there are no grounds to suspect that the money or other property originates from criminal activity or that money laundering or terrorist financing has been committed, as well as if the customer or their beneficial owner is not a 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 scope of ongoing monitoring of transactions if the value of transaction does not exceed the amount for which the reporting entity has estimated, during drafting of the risk analysis, that is appropriate to customer's business activities and to lower risk of money laundering and terrorist financing of the customer;
4) instead of gathering information thereof and conducting specific measures, draw 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 are reasons to suspect or grounds to suspect that the property originates from the criminal activity or that money laundering or terrorist financing has been committed, a reporting entity shall submit to the Financial Intelligence Unit data referred to in Article 66 paragraphs 6 and 10 of this Article and conduct measures referred to in Article 17 of this Law.

A reporting entity shall also implement CDD measures to the extent determined in accordance with paragraph 1 item 3 of this Article in relation to a customer for whom it is determined that there is a 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 preventing and detecting money laundering and terrorist financing, defined by this Law, are implemented to the same extent 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 preventing and detecting money laundering and terrorist financing as the standards specified by this Law or the EU law.

If the standards for the implementation of measures for preventing and detecting money laundering and terrorist financing provided for by the regulations of another country are the same or higher than the standards established 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 standards for the implementation of measures for preventing and detecting money laundering and terrorist financing provided for by the regulations of another country are lower than the standards established by this Law or if the measures for preventing and detecting money laundering and terrorist financing are implemented to a lesser extent than the scope established by this Law, a reporting entity shall ensure that their business units or business organisations majority-owned by the reporting entity implement measures for preventing and detecting money laundering and terrorist financing in accordance with this Law, including data protection measures, to the extent permitted by the regulations of that country.

If the regulations of another country prohibit the implementation of measures referred to in paragraph 3 of this Article, a reporting entity shall immediately notify the Financial Intelligence Unit and the competent supervisory authority referred to in 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 permitted by the regulations of that country.

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

1) prohibit the establishment of business relationships;
2) terminate business relationships;
3) prohibit the execution of transactions; or
4) where necessary and possible, terminate the activities in business units or business organisations majority-owned by the reporting entity in another country.

The reporting entity referred to in paragraph 1 of this Article, that is a member of a financial group, may, for the purpose of preventing 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 preventing and detecting money laundering and terrorist financing than the standards established by this Law or the EU law, whereas it shall ensure appropriate protection of data confidentiality in accordance with the laws regulating the data confidentiality and personal data protection.

A reporting entity referred to in paragraph 1 of this Article that 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, EU Member States and countries that have the same or higher standards for the implementation of measures for preventing and detecting money laundering and terrorist financing than the standards established by this Law or the EU law also in the case when the Financial Intelligence Unit has been notified that there are reasons to suspect or grounds to suspect that funds or other property represent material benefit derived from criminal activity or are subject to money laundering or are intended for terrorist financing, unless the Financial Intelligence Unit limits or prohibits the exchange of data and information.

Issuers of electronic money, payment service providers, and crypto-asset service providers with business establishment in Montenegro, which are not subsidiaries, incorporated in Montenegro, and whose main headquarters are in another European Union member state, and which operate on a cross-border basis, shall designate a single contact point in Montenegro that will ensure compliance with AML/CFT rules on their behalf, and facilitate the supervision by the competent supervisory authority, particularly by providing documents and information upon request of the competent authority.

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 by code or bearer or provide other service or product which, directly or indirectly, enables the concealment of the customer's identity.

Prohibition of shell (fictious) bank activities

Article 64

A reporting entity shall not operate as a shell (fictious) 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 another 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 or wins payouts in cash in the amount of EUR 10,000 or more.

The restriction referred to in paragraph 1 of this Article shall also be applied in the event when the payment or transaction is carried out in two or more operations which appear to be linked in total amount of EUR 10,000 or more.

The payment or transaction in the amount referred to in paragraphs 1 and 2 of this Article must be executed by paying or transferring funds to the transaction account opened with a credit institution.

The administrative body responsible for tax collection shall supervise entities referred to in paragraph 1 of this Article that are not reporting entities in the context of this Law.

The obligations referred to in paragraphs 1, 2 and 3 of this Article shall not apply to 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 referred to in Article 117 paragraphs 1 to 6 of this Law for each wire transaction in the amount of EUR 100,000 or more, and the reporting entity that is a credit institution and other payment service providers also for each cash transaction in the amount of EUR 15,000 or more,

and the reporting entity referred to in Article 4 paragraph 2 item 10 for each transaction in the amount of EUR 2,000 or more, without delay, and no later than three working days from the date of the transaction, or the day the transaction is known to have been executed.

Notwithstanding paragraph 1 of this Article, a reporting entity referred to in Article 4 paragraph 2 item 13 indents 5, 10, 11, 12 and 13 of this Law shall submit accurate and complete data to the Financial Intelligence Unit on CDD measures referred to in Article 117 paragraphs 1 to 6 of this Law for each wire transaction in the amount of EUR 20,000 or more, without delay, and no later than three working days from the date of the transaction.

A reporting entity shall submit accurate and complete data to the Financial Intelligence Unit on CDD measures referred to in Article 117 paragraphs 1 to 6 of this Law for each wire transaction in the amount of EUR 20,000 or more, which is executed at the accounts of legal and natural persons in high-risk third countries and if such transaction includes high-risk third country, without delay, and no later than three working days from the date of the transaction, or the day the transaction is known to have been executed.

A reporting entity referred to in Article 4 paragraph 4 of this Law shall submit accurate and complete data to the Financial Intelligence Unit on CDD measures referred to in 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, and no later than three working days from the date of the conclusion of that legal transaction.

In addition to data referred to in paragraph 4 of this Article, the reporting entity referred to in Article 4 paragraph 4 of this Law shall 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 of the amount, until the order referred to in Article 93 of Law is passed, and it shall inform, without delay, the Financial Intelligence Unit thereof and submit to the Financial Intelligence Unit the data on CDD measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law.

A reporting entity shall submit the data referred to in 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.

Where the reporting entity, due to the nature of transactions and other justified reasons, may not act in accordance with paragraph 6 of this Law, it shall submit to the Financial Intelligence Unit the accurate and complete data on CDD measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Article, without delay, and no later than the next working day following the execution of the transaction, or the day the transaction is known to have been executed.

A reporting entity shall, when submitting data in the manner referred to in paragraph 8 of this Article, submit a reasoned explanation of why it did not act in accordance with paragraph 6 of this Article.

A reporting entity shall submit to the Financial Intelligence Unit, without delay, accurate and complete data on CDD measures referred to in 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 material benefit derived from criminal activity or is linked to money laundering or terrorist financing.

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

A reporting entity shall notify the Financial Intelligence Unit, on any access to data, information and documentation conducted at the reporting entity by the supervisory authority referred to in Article 131 paragraph 1 of this Article no later than three working days from the date of the access.

A reporting entity shall submit to the Financial Intelligence Unit data referred to in paragraphs 1 to 6 and paragraph 10 of this Article, the reasoned explanation referred to in paragraph 9 of this Article and the notifications referred to in 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.

A reporting entity may also provide data referred to in paragraphs 6 and 10 of this Article to the Financial Intelligence Unit verbally, via telephone or in any other available manner, but it shall also submit those data in accordance with paragraph 13 of this Article, no later than the next working day after the day of communicating them verbally.

The Ministry shall prescribe in more detail the method of submitting data referred to in paragraphs 1 to 6 and paragraph 10 of this Article, the reasoned explanations referred to in paragraph 9 of this Article and notifications referred to in paragraphs 11 and 12 of this Article.

Exemptions from reporting obligation
Article 67

Notwithstanding Article 66 paragraph 6 of this Law, a reporting entity referred to in 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 conduct, based on data or notifications submitted pursuant to Article 6 paragraphs 6, 10 and 11 of this Law, 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 for suspicion or reasonable grounds to suspect in money laundering and terrorist financing in relation to that person, transaction or property or whether that transaction or property represent material benefit derived from 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 to suspect referred to in 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 grounds to suspect that the transaction or property represent material benefit derived from criminal activity or that there is money laundering or terrorist financing, it may provide the reporting entity in the reasoned explanation referred to in paragraph 1 of this Article with a recommendation to terminate a business relationship with the customer or to decline the execution of transactions.

COMPLIANCE OFFICER FOR PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING AND THEIR DEPUTY, AND INTERNAL CONTROLS AND AUDIT

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

Article 69

A reporting entity shall, within 60 days since the day of their establishment and/or day of the commencement of their business activity, appoint a compliance officer for the prevention of money laundering and terrorist financing and at least one of their deputies and submit to the Financial Intelligence Unit, within three days since the day of their appointment, a notification containing the information about these persons (name and surname; unique personal identification number; the number, personal identification document expiration date and issuing country; the number and expiry date of residence permit for a foreigner; the title of working position and contact phone number) as well as the name or 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 their deputy within three days since the day when the change is being made.

The notification referred to in paragraph 2 of this Article shall contain explanation with reasons for making the change and the information referred to in paragraph 1 of this Article.

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

With the reporting entity that has four or less employees the affairs of the compliance officer for the prevention of money laundering and terrorist financing may be performed by the director, if they meet the conditions referred to in Article 70 of this Law.

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

The notifications referred to in 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 their deputy

Article 70

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

1) has 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,

3) has not been convicted by a final court decision for a criminal offence for which an imprisonment longer than six months is prescribed, and

4) is employed at the reporting entity.

One person may be appointed as compliance officer for the prevention of money laundering and terrorist financing or their deputy only with one reporting entity.

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

Training and professional exam
Article 71

The training shall be delivered by organiser of adult education who has a license issued in accordance with the regulations defining education of adults.

The training shall be delivered due to the programme established in accordance with the regulations defining education of adults, with the prior consent of the Financial Intelligence Unit.

After completed training, the candidate shall take 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 commission referred to in paragraph 3 of this Article shall be entitled to a monthly compensation in the amount of 40% of average net salary in Montenegro in the previous year, for the month in which the candidate had an examination period.

If a person that is already employed with the reporting entity takes professional exam, the costs of taking the professional exam shall bear the reporting entity.

The programme and the method of taking the professional exam, the costs of professional exam, the composition of the commission, and the format of the certificate referred to in 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 affairs of the 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 its expiration date.

The license shall be issued in a prescribed form and its authenticity can be verified.

The form of the license and the manner of verifying its authenticity shall be prescribed by the Ministry.

Termination of license validity

Article 73

The license shall cease to be valid:

1) at the request of the license holder,
2) upon the expiration of period of its issuance,
3) if a person to whom the license was issued, has been convicted, by the 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 was issued, becomes permanently incompetent for performing tasks of compliance officer for the prevention of money laundering and terrorist financing or their deputy or if the person lost the ability to work,
5) upon exercising the right to a pension by the person to whom the license has been issued, or
6) in case of negligent performance of duties.

Negligent performance of duties

Article 74

The compliance officer for the prevention of money laundering and terrorist financing or their deputy shall be deemed to have performed their duties by negligence within the meaning 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 referred to in paragraph 1 of this Article on the basis of the report of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, on the basis of the request referred to in Article 131 paragraph 10 of this Law.

Administrative decision on the termination of license validity

Article 75

The Financial Intelligence Unit shall pass an administrative decision on the termination of license validity.

An administrative dispute may be initiated against the administrative decision referred to in paragraph 1 of this Article.

The Financial Intelligence Unit shall notify, without delay, the reporting entity with which the person, whose license is revoked, has been appointed as the compliance officer for the prevention of money laundering and terrorist financing or their deputy.

In the case of the termination of license validity, the reporting entity shall, within 15 days following the day of the adoption of the administrative decision, appoint another compliance officer for the prevention of money laundering and terrorist financing or their 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 their deputy shall perform the following tasks:

1) ensures that the system for the prevention of money laundering and terrorist financing is established, operational and further developed;
2) ensures proper and timely data delivery to the Financial Intelligence Unit and cooperate with the competent inspection authority in the process of inspection supervision;
3) drafts and regularly updates the risk analysis in accordance with the guidelines referred to in Article 12 paragraph 5 of this Law;
4) monitors the implementation of policies, controls and procedures for the prevention of money laundering and terrorist financing;
5) initiates and participates 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) participates in drafting the internal regulations related to the prevention of money laundering and terrorist financing;
7) monitors and coordinates the compliance of the reporting entity's business activities with this Law;
8) cooperates in the process of establishing and developing information technology that will be used for the prevention and detection of money laundering and terrorist financing;
9) gives initiatives and makes 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) ensures implementation of Article 16 of this Law when introducing new products, services or channels of distribution at the reporting entity,
11) prepares professional training programmes and development of employees with the reporting entity in the area of the prevention and detection of money laundering and terrorist financing,
12) prepares report in the area of the prevention of money laundering and terrorist financing at the reporting entity once a year, or more often if necessary, and when required by the competent supervisory authority referred to in Article 131 paragraph 1 of this Law.

A reporting entity shall submit the report referred to in paragraph 1 item 12 of this Article to the competent supervisory authority referred to in Article 131 paragraph 1 of this Law upon its request within three days following the day when the request is received.

A compliance officer for the prevention of money laundering and terrorist financing or their 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 their deputy shall be functionally and organisationally separated from other organisational parts of a 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 referred to in Article 76 paragraph 1 of this Article;
2) functional connections with other organisational parts of the reporting entity so as to enable the compliance officer to efficiently, in good quality and timely manner perform tasks referred to in Article 76 paragraph 1 of this Law;
3) adequate material conditions for work;
4) appropriate spatial and technical conditions that ensure appropriate level of protection of confidential data and information at their disposal, in accordance with 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 related to the prevention and detection of money laundering and terrorist financing;
7) replacement during the absence from work.
8)

The 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 referred to in Article 76 paragraph 1 of this Law and report on the facts 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 their absence or inability to work, shall be replaced by their 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 area of the prevention and detection of money laundering and terrorist financing to all employees

that participate in the prevention and detection of money laundering and terrorist financing with that reporting entity.

The professional training and development referred to in paragraph 1 of this Article includes informing employees with this Law and regulations adopted on the basis of this Law, internal regulations of the reporting entity in the area 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 referred to in 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 referred to in 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 establish and implement relevant rules for dealing with a customer and 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 establish 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 referred to in 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 risk of money laundering and terrorist financing identified in the risk analysis.

When the law regulating business activity of the reporting entity prescribes the obligation to establish independent internal audit, the reporting entity shall organise an independent internal audit whose scope of work includes regular assessment of adequacy, reliability and effectiveness of AML/CFT risk management system.

A reporting entity shall also organise an independent internal audit whose scope of work includes the assessment of the adequacy, reliability and effectiveness of AML/CFT risk management system and when they assess that it is necessary due to the nature and scope of their business activity.

Internal control and audit referred to in paragraphs 1, 2 and 3 of this Article shall be carried out in the manner to prevent, detect and correct mistakes 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 conducting the internal control and audit referred to in 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 to apply the list of indicators
Article 81

When establishing reasons for suspicion that property derives from criminal activity or that money laundering or terrorist financing have been committed and other circumstances related to the suspicion, a reporting entity shall use the list of indicators referred to in Articles 82 and 83 of this Law and take into account other circumstances that there are 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 referred to in Article 131 paragraph 1 of this Law.

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

Article 83

The 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 executed with 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 the customer of the reporting entity.

The list of indicators from paragraph 1 of this Article shall be included in the documentation of the reporting entity.

V AFFAIRS, POWERS, MANNER OF WORK AND 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 the 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 and/or powers referred to in paragraph 2 of this Article shall be performed and/or exercised by the head and employees of the Financial Intelligence Unit.

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

Head of the Financial Intelligence Unit
Article 85

A person with the rank of deputy director of the Police Directorate and which 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, upon the proposal of the Minister of Internal Affairs.

The proposal for the appointment of the head of the financial-intelligence unit shall be submitted by the Government to the competent committee of the Parliament of Montenegro in order to provide its opinion.

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 internal affairs and act on internal organisation and systematization of working positions of the Ministry.

A police officer, or an employee of the Ministry, may be assigned to a position in the Financial Intelligence Unit only with the prior consent of the head of the Financial Intelligence Unit.

The administrative 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 the Ministry by the budget for the work of the Financial Intelligence Unit shall be independently managed 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 the Financial Intelligence Unit for its work through donations or otherwise shall be independently managed by the head of the Financial Intelligence Unit.

The head of the Financial Intelligence Unit shall, within the funds referred to in paragraph 1 of this Article, make decisions independently on 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 resources 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 referred to in paragraph 1 of this Article may not be made available 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 managing and using the informational system, means of communication, vehicles and other equipment referred to in paragraph 1 of this Article, and the premises used by the Financial Intelligence Unit shall be regulated by the head of the Financial Intelligence Unit by the internal regulation.

The regulation referred to in paragraph 3 of this Article shall be classified with appropriate confidentiality level in accordance with the law regulating the data secrecy.

Affairs and/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, prepare and deliver financial analyses and other information in accordance with this Law;

2) receive from the reporting entities, competent authorities referred to in article 96 paragraph 1 of this Law, supervisory authorities referred to in Article 131 paragraph 1 of this Law, other legal and natural 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 foreign country authorities responsible for assets confiscation, as well as the information and data on the persons and property for which there are reasons for suspicion or reasonable grounds to suspect that money laundering and associated predicate offences and terrorist financing have been committed 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) make initiatives for amendments and changes of 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 referred to in Article 96 paragraph 1 of this Law and supervisory authorities referred to in Article 131 paragraph 1 of this Law, and foreign financial intelligence units, competent authorities in other countries and international 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 their 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 to include legal and natural persons into 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, data on the property that has been seized or confiscated, as well as data on limited or restricted data access referred to in Article 47 paragraph 5 of this Law, and to notify the public, in other appropriate manner, on the forms money laundering and terrorist financing;
11) perform other activities in accordance with the law.

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

The internal regulation referred to in paragraph 2 of this Article shall be classified with appropriate confidentiality level 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 to suspect that funds or other property of a specific customer derive from criminal activity or that money laundering and associated predicate offences have been committed, or that they are associated with terrorist financing, it may request from the reporting entity to provide data, information and documentation:

1) referred to in 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 specify in the request, referred to in paragraph 1 of this Article, the legal basis for data collection, data that are to be provided, the purpose of collection and the time limit for their delivery.

The Financial Intelligence Unit may also request the provision of data, information and documentation referred to in paragraph 1 of this Article, for the persons for which it can be concluded that they 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 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 referred to in paragraphs 1 and 3 of this Article, submit accurate and complete data, information and documentation at their disposal, without delay, and no later than within eight days following the receipt of the request.

If the request referred to in paragraphs 1 and 3 of this Article is classified as URGENT, the reporting entity shall submit data, information and documentation to the Financial Intelligence Unit without delay, and no later than 24 hours following the receipt of the request.

The Financial Intelligence Unit may, due to the extensive data, information and documentation or other justified reasons, upon the reasoned request from the reporting entity, prolong the deadline referred to in paragraph 5 of this Article or perform verification of data, information and documentation with the reporting entity.

The reporting entities shall provide data, information or documentation referred to in paragraph 1 of this Article to the Financial Intelligence Unit through internet application located on Financial Intelligence Unit 's information system portal, in the manner prescribed by the regulation referred to in Article 66 paragraph 15 of this Law.

Provision of data, information and documentation referred to in 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 to suspect 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 referred to in Article 43 paragraph 3 of this Law, as well as natural persons that are not reporting entities within the meaning of this Law, to make available or submit data, information and documentation that they possess, or to provide notifications, for the purpose of prevention and detection of money laundering, associated predicate offences or terrorist financing, particularly the following 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 tracing and identifying 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 referred to in paragraph 1 of this Article shall submit data, information and documentation to the Financial Intelligence Unit in the manner prescribed by the regulation from Article 66 paragraph 15 of this Law.

Submission of data, information and documentation referred to in 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, information and documentation

Article 92

The competent authorities referred to in Article 96 paragraph 1 of this Law, other state authorities, supervisory authorities referred to in article 131 paragraph 1 of this Law and public power holders shall enable the Financial Intelligence Unit 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 referred to in paragraph 1 of this Article, the authorities referred to in 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 referred to in Article 66 paragraph 15 of this Law.

The Financial Intelligence Unit shall, in the request referred to in paragraph 2 of this Article, state the legal basis, the data that are to be submitted, the purpose of data gathering and the deadline for their submission.

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, request from 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 that 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 referred to in paragraph 1 of this Article in order to take measures within their competence.

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

In the case that the last day of a deadline referred to in paragraph 1 of this Article falls 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 shall 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 referred to in paragraphs 1 and 4 of this Article to the reporting entity in electronic or written form.

Notwithstanding paragraph 6 of this Article, due to urgency, or other circumstances related the execution of a transaction, the order referred to in paragraphs 1 and 4 of this Article may be issued verbally, but then it shall be delivered 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 written note on the receipt of verbal order referred to in paragraph 1 and 4 of this Article.

Upon reception of the notification referred to in 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 safe deposit box, and shall notify the Financial Intelligence Unit thereof, in electronic or written form, without delay.

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 safe deposit box, fails to notify the reporting entity on further actions, the reporting entity may, after the expiration of that period, 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 from the reporting entity, in electronic or written form, 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 or associated predicate offences have been committed, or that they are intended for terrorist financing, and define a deadline within which the reporting entity shall report on that and submit requested data.

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

The reporting entity shall submit the data referred to in paragraph 1 of this Article to the Financial Intelligence Unit before the execution of the transaction or conclusion of the business, and specify in the notification the estimated deadline within which the transaction or business is expected to be completed.

If, due to the nature of the transaction or business or other justified reasons, the reporting entity is unable to act in accordance with paragraph 3 of this Article, they shall provide data referred to in 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 has been executed or business concluded.

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

Ongoing monitoring referred to in paragraph 1 of this Article shall not last longer than three months from the day of submitting the request referred to in 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 submitting the request referred to in 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 reasoned 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, conduct 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, or associated predicate offences or terrorist financing, or that the property derived from a criminal activity.

The decision to act in accordance with the request or information referred to in 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 referred to in 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 referred to in 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 proportionate to the interests of the natural or legal person or would not be relevant considering the purpose which it has been requested for, the Financial Intelligence Unit may refuse to provide the reply to the request referred to in paragraph 1 of this Article.

The Financial Intelligence Unit shall reason the refusal to provide a reply to the request referred to in paragraph 1 of this Article.

In the case of obtaining a reply referred to in paragraph 3 of this Article, the competent authorities referred to in paragraph 1 of this Article shall submit to the Financial Intelligence Unit the feedback on the use of delivered information, and 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 has been committed or that the property derives from a 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 a criminal activity, it shall, in written form, notify the competent authority thereof and provide necessary data, information and documentation.

If the Financial Intelligence Unit has acted in accordance with the notification referred to in Article 66 paragraphs 6, 10, and 11 of this Law, it shall not, in the notification referred to in paragraph 1 of this Article, provide information that notification was delivered by the reporting entity, or data on the employee with the reporting entity that delivered the notification, nor submit the notification, unless there are reasonable grounds to suspect that this employee with the reporting entity has 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 referred to in paragraph 1 of this Article shall provide to the Financial Intelligence Unit the feedback on the use of delivered data, information and documentation referred to in 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.

Notifying the competent authorities upon the establishment of the reasonable grounds to suspect that other criminal offence has been 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, has been 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 performed activities in accordance with the notification referred to in Article 66 paragraphs 6, 10 and 11 of this Law, it shall not, in the notification referred to in paragraph 1 of this Article, provide information that the notification was provided by the reporting entity, or data on the employee of the reporting entity that delivered the notification, nor submit that notification, unless there are reasonable grounds to suspect that this employee of the reporting entity has 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 is requested, in written form, by the competent court.

The competent authority referred to in paragraph 1 of this Article shall provide to the Financial Intelligence Unit the feedback on the use of provided data, information and documentation referred to in 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 the following:

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

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

- risks of money laundering and terrorist financing on the national level;

- the efficiency and effectiveness of coordinated activities of the Financial Intelligence Unit, supervisory authorities referred to in Article 131 paragraph 1 of this Law, other competent authorities and reporting entities, in prevention of money laundering and terrorist financing;
- the quality of financial intelligence data, information and documentation obtained through international cooperation and their adequacy for taking efficient action in relation to perpetrators of criminal offences and their property;
- the efficiency and effectiveness of the work of the supervisory authorities referred to in Article 131 paragraph 1 of this Law, in performing adequate supervision, monitoring and managing the activities of reporting entities, with a view to achieving compliance with the requirements for the prevention of money laundering and terrorist financing proportionate to the identified risks;
- the adequacy of the implementation of measures referred to in Articles 17 and 52 of this Law and reporting suspicious transactions by reporting entities in proportion 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, or 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 have been temporarily seized or permanently 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 prepare the report on the results of the analysis referred to in paragraph 1 of this Article and submit it to the coordinating body referred to in Article 8 of this Law.

Information system of the financial intelligence unit

Article 100

The Financial Intelligence Unit shall, when 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 employees referred to in paragraph 3 of this Article, use the information system of the Financial Intelligence Unit, that represents and integrated set of information and communication technologies necessary for collecting, recording, keeping,

processing and transferring data, information and documentation in electronic form (hereinafter: IS of the FIU).

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

Access to data, information and documents referred to in paragraph 1 of this Article shall only have the employees 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

The IS of the FIU shall comprise of:

- 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 IS of the FIU;
- infrastructure systems which consists of systemically implemented computer programs;
- application systems which consists of computer programs tailored for business functions;
- internet systems which consists of computer programs tailored for providing services on the internet.

The parts of the IS of the FIU referred to in paragraph 1 of this Article shall be functionally connected and operate as unified system.

Managing and accessing IS of the FIU

Article 102

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

Only employees of the Financial Intelligence Unit, authorised for the management of the IS of the FIU, shall have access to IS of the FIU.

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

Professionals referred to in paragraph 4 of this Article shall not stay in the premises, or access the IS of the FIU without the presence of employees referred to in paragraph 3 of this Article.

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

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

Revision of the IS of the FIU

Article 103

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

The audit referred to in paragraph 1 of this Article shall include checking the following:

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

The results of the revision referred to in paragraph 1 of this Article shall be delivered to the head of the Financial Intelligence Unit, who shall adopt an action plan for improving and addressing deficiencies in the IS of the FIU.

The act referred to in paragraph 3 of this Article shall be classified with appropriate confidentiality level 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 referred to in Article 96 paragraph 1 of this Law, supervisory authorities referred to in 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 employees of the Financial Intelligence Unit shall use the unique official address that officer for electronic communication.

The Financial Intelligence Unit shall assign the unique official address for electronic communication for its own and the for the purposes of its employees.

For the needs of the Financial Intelligence Unit, 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 employees shall be defined by an internal regulation passed by the head of the Financial Intelligence Unit.

Mechanism for submitting information
Article 104a

The Financial Intelligence Unit shall on its website establish a mechanism for submitting information on the breaches of the provisions of this Law and reporting suspicious transactions in the manner that the identity of persons providing the information is known only to the Financial Intelligence Unit.

The Financial Intelligence Unit shall not reveal the identity of a person referred to in paragraph 1 of this Article.

The detailed manner of functioning and implementation of the mechanism, referred to in Article 1 of this Article, shall be defined by internal regulation passed by the head of the Financial Intelligence Unit, and classified with appropriate confidentiality level in accordance with the law regulating data confidentiality

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 competent 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, that 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.

Various definitions of the predicate criminal offence shall not represent an obstacle for cooperation, exchange and use of intelligence information between the Financial Intelligence Unit and a foreign financial intelligence unit.

Request to the competent authority from another country to submit 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 submit 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 submit data, information and documentation referred to in paragraph 1 of this Article.

The Financial Intelligence Unit may, upon a request from the supervisory authority referred to in Article 131 paragraph 1 of this Law, request from the supervisory authority from another country to submit data, information and documentation referred to in paragraph 1 of this Article.

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

Notwithstanding paragraph 4 of this Article, if there are reasons of urgency, the Financial Intelligence Unit may submit the request referred to in 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 referred to in 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 the 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, only 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, neither 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, or for other purposes that are not in accordance with the conditions and restrictions set by that authority or international organisation.

Submitting 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 to suspect of money laundering, associated predicate criminal offences or terrorist financing or that the property derived from criminal activity and stating the purpose for which the data are being requested, submit to a foreign financial intelligence unit, in a timely manner, 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 submit data, information and documentation referred to in 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 referred to in paragraphs 1 and 2 of this Article, data, information and documentation may be exchanged electronically, through the means of secure communication systems of the world association of financial intelligence units or through another international communication system that provides the same or 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), submit information on bank accounts and safe deposit boxes, financial information and financial analyses referred to in paragraph 1 of this Article, through Europol's Secure Information Exchange Network Application in the 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 a request from a foreign financial intelligence unit in the cases where predicate criminal offence or criminal activity are not known at the time of receiving the request.

The Financial Intelligence Unit shall, in written form, notify, the requesting party on the refusal of the request referred to in 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 referred to in 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 submit data referred to in paragraphs 1 and 2 of this Article or give consent referred to in paragraph 7 of this Article if:

1) the submission of data, information and documentation would be disproportionate to the legitimate interests of a natural or legal person or Montenegro;
2) the submission 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 submission 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 referred to in paragraph 7 of this Article and submit it to the requesting party.

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

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

Competent authorities referred to in 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.

Submission of data, information and documentation to the authority from another country on Financial Intelligence Unit's own initiative (Spontaneous submission of data to a foreign authority)

Article 108

The Financial Intelligence Unit may without request, on its own initiative, submit 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, with 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 of money laundering and associated predicate criminal offences or terrorist financing, or that the property derives from criminal activity, which it has obtained in accordance with this Law, for the purpose of prevention and detection of money laundering, associated predicate criminal offences, criminal activity or terrorist financing.

The Financial Intelligence Unit shall, in a timely manner, disseminate report on suspicious transaction related to an EU Member State, referred to in Article 66 paragraph 6 of this Law, to the financial intelligence unit of that Member State.

The Financial Intelligence Unit may, when submitting data, information and documentation in accordance with paragraph 1 of this Article, 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 the reasoned 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 access to a safe deposit box, for no longer than 72 hours.

In the case referred to in 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 referred to in 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 derived from criminal activity or that money laundering and associated predicate criminal offences or terrorist financing has been committed, and shall thereof notify 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 affairs 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 has been 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 cash, 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 transportation;
- incoming and outgoing cross- border transportation of cash, 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 transportation;
- incoming and outgoing cross border transportation or attempt of transportation of cash, checks, securities, precious metals and stones, in the value or amount of EUR 10,000 or more, where in respect of that cross -border transportation or attempt of transportation there are reasons for suspicion in money laundering or terrorist financing, immediately and no later than within 3 days from the day of the transportation or attempt of transportation.

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 the accounts opened and safe deposit boxes rented by natural and legal persons, 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 rented 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 operations system and in accordance with this Article, whereby data on rented 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 that all data in the registers of accounts and safe deposit boxes are identical with the data submitted by credit institutions and branches of foreign credit institutions.

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

Exceptionally from paragraph 6 of this Article, data on the transaction account number and other data associated with that transaction account that refer to legal persons and entrepreneurs shall be publicly available in accordance with the law regulating the payment system operations.

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 obtaining access to the data from these registers shall be prescribed by the Central Bank of Montenegro.

Data from the register of accounts and safe deposit boxes available to the Financial Intelligence Unit

Article 113

The Financial Intelligence Unit shall have direct electronic access to at least the following data from the register of accounts and safe deposit boxes:

1) for natural persons: first name and surname, unique master citizen number for a resident, the 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 where the account is opened, data on the status of the account (active, closed or frozen), date of opening and closing of the account;
4) date of conclusion and termination of the agreement on renting a safe deposit box, as well as the period for which the agreement was concluded.
5)

Data referred to in paragraph 1 of this Article shall be available to the Financial Intelligence Unit based on personal data or account number.

Stock exchanges and clearing and depository companies

Article 114

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

The stock exchanges and clearing and depository companies shall, upon the request of the Financial Intelligence Unit, submit 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 electronically submit, on quarterly basis, to the Financial Intelligence Unit the data on each collective custody account, credit institution or other financial institution with 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 referred to in 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 submit to the Financial Intelligence Unit the data referred to in paragraphs 1, 2 and 3 of this Article in the manner prescribed by the regulation referred to in 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 referred to in 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 master citizen number of an accused natural person, and for foreigners, the number, issuing country 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 a 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 master citizen number of the natural person against whom proceedings have been initiated or who has submitted a request for judicial determination within the misdemeanour proceedings under this Law, and for foreigners, the number, issuing country and date of expiry of the travel document, or the name, registration number, head office (address) of the legal person against which a proceeding has been initiated or which has submitted a request for judicial 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 master 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 foreigner, the number, issuing country and, 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 referred to in 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 related to the criminal offenses referred to in paragraph 1 of this Article, as well as data on temporarily and permanently confiscated property.

Data referred to in 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 referred to in Article 66 paragraph 15 of this Law.

VIII. RECORDS, PROTECTION AND STORAGE OF DATA

1. Types and content of records

Records kept by the reporting entity
Article 116

The reporting entity shall keep:
1) records on conducted CDD measures;
2) records on complex and unusual transactions referred to in 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 for temporary suspension of transaction execution or temporary prohibition of access to the safe deposit box;
5) records on requests for ongoing monitoring the customer's financial activities;
6) records on the access of the supervisory authorities referred to in 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 referred to in 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 customers' criminal activities

Content of the 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 master citizen number, information on whether the legal person is a resident or non-resident, the reason for a 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 an 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 master citizen number, name and surname, information on whether the entrepreneur is a resident or non-resident, reason for a 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 master citizen number, address and municipality of permanent residence, or temporary residence in Montenegro, date of birth, country of birth, citizenship, information on whether the person is a politically exposed person, information on whether the person is a resident or non-resident, phone number and e-mail address, the type, number, issuing country and date of expiry of the personal identification 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 customer, authorized representative, authorised person, beneficial owner, founder, trustee, user of the property managed, insured person, insurance policy holder, insurance beneficiary, seller or buyer;
4) data on the manner in which the customer 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 customer;
6) information on the purpose, intent, goal, nature of the business relationship and transaction, the basic code of the customer's business activity and the scanned documentation accompanying the business relationship or transaction, data on the origin of property 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) data on a transaction: date and time of execution of transaction, transaction amount in euros, transaction amounts by a currency, number of transaction order, policy or contract, depending on the type of reporting entity, information on whether the transaction is executed fully or partially, information on the type of transactions (cash or wire transaction), 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 master citizen number, name and country of head offices), information on the type of transaction (payment or withdrawal), information on the manner of execution of the transaction depending on the type of reporting entity (cash, wire transaction, 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 referred to in 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 premises for organising games of chance, access to games of chance via the Internet or other telecommunication means, access to the cash desk, access to other places or locations, where transactions are executed 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 referred to in Article 4 paragraph 2 item 1 of this Law, the records on conducted CDD measures, in addition to the data referred to in paragraph 1 item 7 of this Article, shall also contain the following data on the transaction: type and number of the account, unique master citizen 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 intended, or the name, head office (address, city and country) of the legal person to whom the transaction is intended, 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 referred to in Article 4 paragraph 2 item 7) of this Law, the records on CDD measures, in addition to the data referred to in 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 referred to in Article 4 paragraph 2 items 8 and 9 of this Law, the record on conducted CDD measures, in addition to the data referred to in paragraph 1 item 7 of this Article, shall also contain the following data on the transaction: life insurance policy's effective date, duration of insurance in years, information on the type of premium (one-off, monthly, quarterly, semi-annual or annual premium), name and surname of the beneficiary of the insurance premium and information on the reason for the payment (insurable event, termination of the contract or expiry of the contract).

If the transaction is related to the reporting entities referred to in Article 4 paragraph 2 item 13 and paragraph 4 of this Law, the records on the conducted CDD measures, in addition to the data referred to in 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, surface area, number of floors, 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: data 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 referred to in Article 58 of this Law shall contain data referred to in 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 referred to in paragraphs 1 to 6 of this Article, data on indicators from the list of indicators for identifying suspicious customers and transactions, data on reasons for suspecting that the property derives from criminal activity or that it constitutes money laundering, associated predicate criminal offences or terrorist financing, date of data delivery to the Financial Intelligence Unit and the reasons for executing the transaction (rationale).

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 beginning of the temporary suspension of a transaction execution, the date and time of the extension of the temporary suspension of a transaction execution, the account balance before the blocking and data referred to in paragraph 1 items 1, 2 and/or 3 of this Article for the person to whom the temporary suspension of the transaction execution applies.

The records on requests for ongoing monitoring the customer's financial activities shall contain the number of requests, information on the type and number of the customer's account, the date of the beginning of monitoring, the date of the extension of monitoring, data referred to in paragraph 1 items 6 and 7 and paragraph 3 of this Article that occurred during the monitoring period and the data referred to in 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, referred to in 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 a supervisory officer, the date and time when were checked the data, information and documentation referred to in paragraph 1 items 1, 2 and/or 3 of this Article for the person whose data, information and documentation were checked.

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) on incoming and outgoing cross border transportation or attempt of the transportation of cash, checks, bearer securities, precious metals and gem stones, in the amount or value of EUR 10,000 or more, which is declared, undeclared or falsely declared;
2) on incoming and outgoing cross border transportation of cash, 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 reasonable grounds to suspect 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 incoming and outgoing transportation or attempt of transportation of cash checks, bearer securities, precious metals and gem stones, in the amount or value of EUR 10,000 or

more, which is declared, undeclared or falsely declared, shall contain the following information:

1) for a natural person who physically transports in/out or attempts to transport in/out across the state border cash, checks, bearer securities, precious metals and gem stones: name and surname, unique master citizen number, address and city of permanent residence, or temporary residence, citizenship, the type, number, issuing country and date of expiry of the personal identification document;
2) for a legal person, or a natural person, for which cash, checks, bearer securities, precious metals and gem stones are transported in/out across the state border: 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 tax identification number (hereinafter: TIN), or name and surname, unique master citizen 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 TIN of the legal person, or name and surname, unique master citizen 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 transported or attempted to be transported in/out across the state border;
5) information on valuable items that are transferred or attempted to be transported in/out across the state border: 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 transport in/out or attempt to transport in/out across the state border, checks, bearer securities, precious metals and gem stones is performed, date and time of the transportation or attempt of transportation in/out across the state border 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 out or transferred in;
7) information on whether the transportation of cash, checks, bearer securities, precious metals and gem stones in or out of country is declared, undeclared or falsely declared to the administration body responsible for customs affairs.

Records on the transportation of cash, checks, bearer securities, precious metals and gem stones in/out across the state border 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 referred to in paragraph 1 items 1 to 6 of this Article, information on indicators for identifying suspicious customers that exist in relation to a specific case and information on whether the transaction is withheld from execution.

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 processed 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 referred to in Article 115 of this Law;
4) records on the actions of the supervisory authorities referred to in Article 131 paragraph 1 of this Law in relation to the reporting entities;
5) records on the employees of the Financial Intelligence Unit who checked, or accessed or to whom the data from other authorities were provided in accordance with Article 126 of this Law.

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

Content of records kept by the Financial Intelligence Unit

Article 121

The records on the analyses carried out and the cases processed by the Financial Intelligence Unit in accordance with the law shall contain the following:

- data referred to in 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 the 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 provides reasons for the temporary suspension of the transaction execution, or temporary prohibition of access to the safe deposit box, information that provides reasons for ongoing monitoring of the customer's financial activities, legal qualification of the criminal offense, result of operational or strategic analysis, reasons for failing to provide a response to a request or information in accordance with Article 96 paragraphs 4 and 5 of this Law, scanned received and sent documents, scanned documentation attached to documents;
- data on persons subject to financial analysis: mobile phone number, International Mobile Equipment Identity (IMEI) number, photo, scanned page with data from personal identification document, previous personal data (unique master citizen number, name and surname and date of birth), false personal data (unique master citizen number, name and surname, date of birth, address of permanent residence, citizenship), scanned card of deposited signatures, previous names of the legal person and data on the founder

of the legal person (identification number, tax 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 referred to in Articles 93, 109 and 110 of this Law;
- data on requests for ongoing monitoring of customer's financial operations as referred to in Article 95 of this Law;
- data from responses to requests referred to in Articles 91 and 92 of this Law;
- data from requests, information and notifications referred to in Articles 96, 97 and 98 of this Law;
- data on international requests and information referred to in Articles 106, 107 and 108 of this Law;
- data taken from the administration body responsible for customs affairs referred to in Article 111 of this Law;
- data on bank accounts and safe deposit boxes referred to in Article 113 of this Law;
- data submitted by stock exchanges and clearing and depository companies referred to in 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 the reporting entity with head office in Montenegro, and name of the country for the reporting entity with head office in another country) and information on the licence (issued, revoked or not required);
2) for the compliance officer for the prevention of money laundering and terrorist financing, or their deputy: unique master citizen number, name and surname, information on whether the person is compliance officer for the prevention of money laundering and terrorist financing or their deputy, e-mail, telephone number, mobile phone number, date of beginning and termination of activities of the compliance officer for the prevention of money laundering and terrorist financing, or their deputy, license number, licence issue date and licence expiration date.

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

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

The record on the employees of the Financial Intelligence Unit who checked, or accessed data or to whom the data of other authorities are delivered in accordance with Article 126 of this Law shall contain the unique master citizen number of the employee of the Financial Intelligence Unit who checked or accessed data or to whom the data was delivered to, legal basis, date and time of performed check, access, or delivery of data, as well as data which they checked, or accessed to, or data that were delivered to them.

Data records on non-residents

Article 122

If a non-resident who is a natural person does not have a unique master citizen number, in the records and registers prescribed by this Law shall be entered the date of birth, country of birth, the number, issuing country and type of personal document, as well as the date of expiry of the personal document, and in case of a non-resident who is a legal person, instead of the personal 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 referred to in Article 117 paragraphs 1 to 11 of this Law are available or have been available, shall not reveal to a customer or a third party:

1) that information has been disclosed to the Financial Intelligence Unit, or insight into information has been provided or documentation on a customer or a transaction has been submitted in accordance with Articles 66 and 90 of this Law;
2) that the Financial Intelligence Unit has, pursuant to Article 93 of this Law, issued an order on temporarily suspension of transaction execution or prohibit access to a safe deposit box, or has given instructions to the reporting entity thereof;
3) that the Financial Intelligence Unit has, pursuant to Article 95 of this Law, requested ongoing monitoring of customer's business operations;
4) that a preliminary investigation or formal investigation has been initiated or could be initiated against a customer or a third party due to the reasonable grounds to suspect or reasonable suspicion that the criminal offense of money laundering and associated predicate criminal offense or terrorist financing have been committed.

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

The prohibition to disclose data referred to in 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 establishing facts in criminal proceedings and if the submission of such data is requested in written form, or ordered by the competent court or the competent supervisory authority referred to in Article 131 paragraph 1 of this Law for the purpose of implementation of this Law.

Data referred to in paragraph 1 of this Article, notifications on suspicious transactions, financial information, financial analyses, as well as all other data, information and documentation that the Financial Intelligence Unit obtains or produces, in accordance with this Law for the purpose of prevention and detection of money laundering, associated

predicate criminal offences and terrorist financing may not be submitted to other persons for inspection, nor may their existence be confirmed in the records of the Financial Intelligence Unit, unless it is otherwise prescribed by this Law.

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

The data, information and documentation referred to in paragraph 5 of this Article may be declassified if there is no other way to achieve a timely exchange of data at the national and international level in order to effectively prevent, detect and prosecute money laundering offences, associated 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, the information, notifications and requests referred to in paragraph 4 of this Article classified 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) may not apply to reporting entities, public power holders, 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 referred to in Article 62 of this Law.

The obligation to protect data confidentiality (business, banking, professional and other secrecy) may not apply in cases of exchange of information between the reporting entities referred to in Article 4 paragraph 2 item 13 indent 2 and paragraphs 3 and 4 of this Law, that are from Montenegro, EU Members States and countries that have equivalent or higher standards for implementation of measures for prevention and detection of money laundering and terrorist financing than the standards specified by this Law and/or the legislation of the European Union, regardless of whether they are employed with the same legal person or a larger structure to which the legal person belongs to and with which it is connected through common ownership, management or compliance supervision.

In the cases that refer to the same customer and transaction, involving two or more reporting entities, the obligation to protect data confidentiality (business, banking, professional and other secrecy) may not apply between credit and financial institutions, as well as between the reporting entities performing professional business activities referred to in Article 4 paragraph 2 item 13) indent 2 and paragraphs 3 and 4 of this Law, provided that:

1) they are established in the EU Member State or another country that implements measures of prevention of money laundering and terrorist financing equivalent to the provisions of this Law;
2) they perform the same type of business activity or belong to the same category of

professional business activity; and

3) they are subject to the obligations to protect professional and business secret and personal data.

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

1) provide data, information and documentation on their customers to the Financial Intelligence Unit;
2) obtain and process data, information and documentation on customers;
3) execute the order of the Financial Intelligence Unit on the temporary suspension of the transaction execution 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 customer's financial activities.

The reporting entity, or reporting entity's employees may 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 customers 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 compliance officer 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, or their deputy 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.

The reporting entity shall, with previously obtained opinion of the competent authority referred to in Article 131 paragraph 1 of this Law, establish adequate procedures that will regulate the manner of reporting breaches of the provisions of this Law, caused by employees, through a separate and anonymous channel in accordance with the nature and size of that reporting entity.

Use of received personal data
Article 126

The Financial Intelligence Unit, state authorities, state administration bodies, public power holders, reporting entities and their employees shall use the personal data obtained in accordance with this Law for the purpose for which the personal data are processed and must not be processed for commercial purposes.

The authorities that provide electronic access to the above-mentioned data shall keep records on insight, access and submission of personal data to the Financial Intelligence Unit

referred to in Article 47 paragraph 1 item 1, Article 55 paragraph 2, Article 92 paragraph 1 and Articles 111 and 113 of this Law, and it shall contain information that the Financial Intelligence Unit had insight, or access to, or that the data were delivered to the Financial Intelligence Unit electronically, as well as date and time of the beginning and end of the check and access to personal data.

A security-communication link, which represents a protected system of data exchange between precisely defined subjects, shall be used for the exchange of personal data between the Financial Intelligence Unit and state authorities, state administration authorities and public power holders.

For the purposes of the prevention of money laundering and terrorist financing, the processing of personal data prescribed by this Law shall be of the public interest.

Regulations defining the protection of personal data shall apply to the processing, protection, and storage of personal data referred to in paragraphs 1, 2 and 3 of this Article.

Data retention

Article 127

The reporting entity shall keep all 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 five years after the termination of the customer's business relationship, executed occasional transactions, the customer's entry into the casino and premises where other games of chance are organised or access to the safe deposit box, unless a longer period for data retention is prescribed by a special law.

The reporting entity shall keep a photocopy of a personal identification document, other documents and documentation, as well as written powers of attorney in accordance with paragraph 1 of this Article.

The Financial Intelligence Unit, the competent authorities referred to in Article 96, paragraph 1 of this Law and the supervisory authorities referred to in Article 131, paragraph 1 of this Law may request extension of the period for data retention, information and documentation referred to in paragraphs 1 and 2 of this Article, on individual basis, provided that such retention is necessary for the prevention, detection, investigation or court proceedings in cases of money laundering or terrorist financing, for a period that may not exceed five years from the date of expiry of the period referred to in paragraph 1 of this Article.

The reporting entity shall keep 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 implementation of internal control and audit measures for the period of four years after the termination of the validity of the license, or completion of professional training and development and performed internal control and audit.

After the expiration of the deadlines referred to in paragraphs 1 to 4 of this Article, the reporting entity shall delete or destroy the customer's personal data.

If the reporting entity ceases to exist, they shall submit the data, information and documentation referred to in paragraphs 1 and 2 of this Article to the competent supervisory

authority referred to in Article 131 paragraph 1 of this Law, which shall keep them for the period of five years following the date of reception.

Data retention with the administration body competent for customs affairs

Article 128

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

Upon the expiration of the deadline from paragraph 1 of this Article, personal data from the records referred to in Article 119 of this Law shall be deleted.

Retaining Data in The Beneficial Owners Register and Registers of Accounts and Safe Deposit Boxes

Article 129

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

The Central Bank of Montenegro shall keep 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 referred to in paragraphs 1 and 2 of this Article, personal data from the Beneficial Owners Register, 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 retain 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 expiration of the deadline referred to in paragraph 1 of this Article, the electronic data referred to in 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 must 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 inspecting before the expiration of ten years from the date of their recording, unless otherwise prescribed by this Law.

The person referred to in paragraph 3 of this Article shall have the right to check their personal data after the expiration of the period of ten years from the date of their recording.

The more detailed method of depersonalization of data referred to in paragraph 1 of this Article shall be prescribed by the Ministry.

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

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 referred to in Article 4, paragraph 2 items 1, 2 and 3 of this Law, to which it issues a licence or an approval for work;
2) the Agency for Electronic Communications and Postal Services in relation to the reporting entities referred to in Article 4 paragraph 2 item 4 of this Law;
3) the Capital Market Authority of Montenegro in relation to the reporting entities referred to in Article 4 paragraph 2 items 5, 6,7 and 12 of this Law and legal persons referred to in Article 114 of this Law;
4) the Insurance Supervision Agency in relation to the reporting entities referred to in Article 4 paragraph 2 items 8 and 9 of this Law;
5) the administrative authority responsible for financial affairs in relation to the reporting entities referred to in Article 4 paragraph 2 item 10 of this Law;
6) the administrative authority responsible for tax collection in relation to reporting entities referred to in Article 4 paragraph 2 item 11 of this Law and entities referred to in Article 43 paragraph 3 of this Law;
7) the Ministry, through an authorised person, in relation to the reporting entities referred to in Article 4 paragraph 2 items 13 and 14 of this Law;
8) the state administrative authority responsible for judicial affairs in relation to the reporting entities referred to in Article 4 paragraphs 3 and 4 of this Law.

The supervisory authorities referred to in paragraph 1 of this Article shall use risk-based approach to money laundering and terrorist financing supervision when planning the examination of reporting entities.

When planning the frequency and the scope of supervision, the supervisory authorities referred to in paragraph 1 of this Article shall take into account the following:

- data related to the risks of money laundering and terrorist financing determined in the National Risk Assessment;
- data related to specific national or international risks of money laundering and terrorist financing associated with customers, 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 the type of business activity.

The supervisory authorities referred to in paragraph 1 of this Article shall, no later than seven working days before conducting the supervision, inform the Financial Intelligence Unit about the activities they plan to undertake, as well as submit data on the reporting entity planned to be the subject of supervision (identification number, TIN and name), the date when the supervision is planned, information on whether on-site or off-site inspection have been carried out, and if necessary, coordinate and harmonise their activities in performing supervision on the implementation of this Law with the Financial Intelligence Unit.

If the supervisory authority referred to in paragraph 1 of this Article, in the process of the supervision over the implementation of this Law, identifies the irregularities in the operations of the reporting entity, it shall be authorised to:

- point out to the reporting entity on the identified irregularities and to set a deadline for their remediation;
- publicly disclose data on the identity of the reporting entity and the responsible person with the reporting entity, as well as the nature of the identified irregularity;
- 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;
- temporary prohibit the responsible person from the management body to perform the function;
- in the case of ordering the removal of serious, systemic or repeated irregularities, determine the amount of fine the reporting entity shall pay to the supervisory authority referred to in paragraph 1 items 1 to 4 of this Article, or in the budget of Montenegro if the supervisory authority is referred to in paragraph 1 items 5 to 8 of this Article for the breach of the provisions of this Law;
- impose other measures to the reporting entity in accordance with the law.

The supervisory authority referred to in paragraph 1 of this Article may exercise the powers referred to in paragraph 5 of this Article in one of the following ways:

- independently,
- in cooperation with other authorities,
- within the scope of their responsibility, by delegation to another authority,
- by submitting a request to the competent judicial authorities.

When exercising their powers to impose misdemeanour sanctions, the supervisory authorities referred to in paragraph 1 of this Article shall cooperate closely in order to ensure that these sanctions produce results and coordinate their activities in cross-border cases.

The supervisory authorities referred to in paragraph 1 of this Article may issue an order to the reporting entity to terminate the performance of business activities in its branches in another country, or reject the request for opening 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 referred to in 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 referred to in paragraph 1 of this Article to conduct supervision with a specific 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 and operational analyses.

The supervisory authorities referred to in paragraph 1 of this Article shall act in accordance with the request referred to in paragraph 10 of this Article.

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

The supervisory authority referred to in paragraph 1 item 5 of this Article shall establish appropriate activities of monitoring the risk assessment referred to in Article 4 paragraph 7 of this Law or shall take other appropriate measures to ensure that the exemption referred to in Article 4 paragraph 6 of this Law is not misused.

It shall be considered that there are irregularities referred to in paragraph 5 item 6 of this Article when the reporting entity fails to remedy previously identified irregularities or continues to make more serious, repetitive, systemic failures and irregularities or a combination of the aforementioned, in the following cases:

1. Implementing CDD measures;
2. fulfilling the obligation to report suspicious transactions;
3. keeping records, data retention and protection;
4. conducting internal control and audits;
5. collecting and keeping data on the sender and recipient of crypto-assets;
6. implementing effective risk-based procedures; and/or
7. establishing compliance with intermediary services related to crypto-assets.

Determining the amount of a fine

Article 131a

The amount of a fine referred to in Article 131 paragraph 5 indent 6 of this Law may be determined in the amount not higher than twice the amount of the benefit derived from the breach of this Law, if that benefit may be determined, and if the benefit may not be determined in the amount of at least EUR 1,000,000.

Notwithstanding paragraph 1 of this Article, if the reporting entity is a credit institution or financial institution, the amount of a fine may be determined for the following:

- in the case of a reporting entity that is a legal person, maximum fine in the amount of at least EUR 5,000,000 or 10 % of the total annual turnover according to the latest available audited financial statements;
- in the case of a reporting entity that is an entrepreneur or a natural person performing business activity, maximum fine in the amount of at least EUR 5,000,000;
- in the case of responsible person of the legal person, maximum fine in the amount of at least EUR 1,000,000.

The provisions of Article 131 paragraph 5 of this Law and paragraphs 1 and 2 of this Article also apply to the reporting entity that is a legal person on whose behalf any person acted independently or as part of that legal person with the power of attorney to represent it, make decisions on their behalf, or exercise control with that legal person.

When determining the amount of a fine referred to in paragraphs 1 and 2 of this Article, and/or when determining other measures referred to in Article 131 paragraph 5 of this Law, the following shall be particularly taken into consideration:

1) the gravity and duration of breaches of the provisions of this Law;
2) the degree of responsibility of the reporting entity;
3) the financial status of the reporting;
4) the benefit derived from the breach of the provisions of this Law, if it can be determined;
5) the losses to third parties caused by the breach of the provisions of this Law, if it can be determined;
6) the level of cooperation of the reporting entity with the competent authority;
7) previous breaches of the provisions of this Law by the reporting entity.

The amount of a fine referred to in paragraphs 1 and 2 of this Article may not be determined if the amount of a fine for the same irregularity is determined in accordance with another law.

The supervisory authorities referred to in Article 131 paragraph 1 of this Law may, by an internal act, establish guidelines for the implementation of measures referred to in Article 131 paragraph 5 of this Law, taking into account the provision of the paragraph 4 of this Article.

Notification on measures-imposed
Article 131b

The supervisory authority referred to in Article 131 paragraph 1 of this Law shall publish on its website the notification on the imposed enforceable measures referred to in Article 131 paragraph 5 of this Law.

The supervisory authority referred to in Article 131 paragraph 1 of this Law shall submit the notification referred to in paragraph 1 of this Article also to the Financial Intelligence Unit which publishes a unified list on imposed enforceable measures.

Notwithstanding paragraph 1 of this Article, if the measure is imposed to responsible persons of the reporting entity, and the supervisory authority has considered that the publication of the personal data is not proportionate to the determined breach of the provisions of this Law or the publication would jeopardise the stability of financial market or an on-going investigation in criminal proceedings, the supervisory authority referred to in Article 131 paragraph 1 of this Law may:

1) postpone the publication until the time when the reasons for not publishing it cease to exist;
2) publish the decision on an anonymous basis, and ensure relevant protection of the personal data;
3) refrain from publication if the possibilities referred to in items 1) and 2) of this paragraph are not sufficient to ensure the stability of financial market and to respect the principle of proportionality.

Data referred to in paragraph 1 of this Article shall be available on the website of the supervisory authority referred to in Article 131 paragraph 1 of this Law five years after its publication, unless otherwise specified in the regulations defining the personal data protection.

On-site and Off-site supervision

Article 132

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall perform on-site and off-site supervision on the implementation of this Law.

In the process of supervision, supervisory officers shall identify themselves with official identification card and a badge, or authorisation.

The supervisory authorities referred to in Article 131 paragraph 1 of this Law shall ensure adequate financial, human and technical resources for conducting the supervision in accordance with this Law.

The supervisory authorities referred to in Article 131 paragraph 1 of this Law shall determine in their internal acts adequate working experience and knowledge that is required for their supervisory officers.

A supervisory officer may not be a person who has been convicted, by a final court decision, for criminal offences that make them unsuitable to perform duties in accordance with this Law

On-site supervision shall be conducted on the basis of the supervision plan of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, which shall be developed on an annual basis and represents a business secret.

On-site supervision shall be initiated and conducted in the official premises of the reporting entity, and performed by inspection of the business books, other documentation and the information system of the reporting entity.

The provisions of the law regulating inspection supervision, and/or the law regulating the competences of the supervisory authorities referred to in Article 131 paragraph 1 of this Law, shall be applied to on-site inspection procedure.

Off-site inspection shall be conducted through examination of data, information and documentation that the reporting entities submit to the competent supervisory authorities referred to in Article 131 paragraph 1 of this Law upon their request or make them electronically available, and/or through analysis of the reports and data submitted by reporting entities in accordance with the law.

The reporting entity shall, upon the request referred to in paragraph 9 of this Article, without delay, submit to the competent supervisory authority referred to in 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.

If in the course of off-site supervision the supervisory authority from Article 131 paragraph 1 items 5, 7, and 8 of this Law determines that the reporting entity has not fulfilled their obligation in accordance with this Law, the supervisory authority shall issue a written warning to the reporting entity to fulfil the obligation within eight working days.

If the reporting entity fails to act in accordance with paragraph 11 of this Article, the supervisory authority from Article 131 paragraph 1 items 5, 7, and 8 of this Law shall issue a misdemeanour order to the reporting entity.

The supervisory authority shall make a record or a report on the supervision referred to in paragraph 1 of this Article.

Special powers of supervisory authorities

Article 133

If, on the basis of the law, the competent supervisory authority referred to in Article 131 paragraph 1 of this Law issues 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 convictions 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 referred to in paragraph 1 of this Article shall be considered an associate or a connected person in accordance with the regulation defining the business activities of the reporting entity.

The competent supervisory authority may use data referred to in paragraph 1 of this Article exclusively for the purposes for which they were obtained and shall not disclose or make it available to third parties.

International cooperation of supervisory authorities

Article 134

The competent supervisory authority referred to in Article 131 paragraph 1 of this Law may, on their own initiative or on the basis of a written and reasoned request of the supervisory authority of another country, exchange data, information and documentation regarding:

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

The supervisory authorities referred to paragraph 1 of this Article, in accordance with the principles of reciprocity and keeping confidential information, may, within the scope of their powers, request mutual assistance in conducting supervision of the reporting entity that is part of the group and that operates in the country from which the assistance is being requested.

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

The supervisory authorities referred to in paragraph 1 of this Article shall only use the data, information and documentation referred to in 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 authority responsible for the supervision, including court proceedings.

The supervisory authority referred to in paragraph 1 of this Article that has identified irregularities referred to in article 137 of this Law shall also inform thereof other competent supervisory authorities referred to in Article 131 paragraph 1 of this Law, if these irregularities are relevant for their work.

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

The supervisory authority referred to in paragraph 1 of this Article shall not use data, information and documentation collected in accordance with paragraphs 1 to 4 of this Article for any other purpose than that for which the supervisory authority that delivered the data, information and documentation has given its consent.

Supervisory authorities referred to in Article 131 paragraph 1 items 1 to 4 of this Law shall cooperate with each other and exchange information with competent authorities supervising credit and financial institutions in other EU Member States and third countries in accordance with this Law or other law that refer to the supervision of credit and financial institutions, regardless of their respective nature or status, as well as with other bodies of Member States responsible for the supervision of the prevention of money laundering and terrorist financing.

The cooperation referred to in paragraph 8 of this Article shall also refer to the gathering of information on behalf of the requesting competent authority, as well as the exchange of the gathered information.

Submitting data on the actions taken in the supervision procedure

Article 135

The supervisory authorities referred to in Article 131 paragraph 1 of this Law shall, in relation to the activities taken during supervision, in accordance with this Law, submit to the Financial Intelligence Unit, the following:

- data 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 master citizen number of the responsible person of the legal person, or name and surname, date of birth, and the number, date of expiry and country of issuance of the travel document if the responsible person of the legal person is a foreigner;
- information on the date of supervision and a description of the findings;
- names and surnames of persons engaged by the competent supervisory authority referred to in Article 131 paragraph 1 of this Law to perform the activities with regard to the prevention of money laundering and terrorist financing;
- the report, or the record on conducted supervision in electronic form.

If irregularities in the operations of the reporting entity are identified, the supervisory authorities referred to in Article 131 paragraph 1 of this Law shall submit to the Financial Intelligence Unit the following data:

- the date of the submission of the misdemeanour order, and/or the request for initiating misdemeanour proceedings or other imposed measures;
- the number of a misdemeanour order;
- description of the misdemeanour referred to in Article 137 of this Law;
- information on the imposed measures;
- the amount of the imposed fine.

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

If the supervisory authority referred to in 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 thereof within eight days following the day the measure was imposed.

If the supervisory authorities referred to in 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 originates from criminal activity, they shall inform the Financial Intelligence Unit thereof without delay.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall submit 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 referred to in Article 66 paragraph 15 of this Law.

Data Access
Article 136

Supervisory authorities referred to in Article 131 paragraph 1 of this Law may have direct access to data that reporting entity submits to the Financial Intelligence Unit in accordance with Article 66 of the Law, in the form submitted by the reporting entity.

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

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

The Financial Intelligence Unit may, upon a justified request of supervisory authorities referred to in Article 131 paragraph 1 of this Law, for the purposes of conducting verifications for issuing licences and authorisations, which that supervisory authority issues in accordance with the law, provide all relevant data that it may obtain by exercising their powers.

X. PENALTY PROVISIONS

Article 137

The fine in an amount of EUR 5,000 to EUR 20,000 shall be imposed on a legal person for misdemeanour if:

1) they fail to establish an appropriate information system, when the reporting entity is a credit institution or other financial institution (Article 11 paragraph 1 item 3);

1 a) they have a collegial management body, and fails to appoint one member of that body that is responsible for the implementation of this Law (Article 11 paragraph 2);

2) within the period of 60 days since the day of its establishment or commencement of performing business activity, they fail to develop an internal regulation on risk analysis for identifying and assessing risks, taking into account risk factors of an individual customer, a group of customers, a country or geographic area, business relationship, transaction or product, services or distribution channels that may be used for the purpose of money laundering or terrorist financing and does not regularly update it, at least once a year, and does not keep it in accordance with this Law (Article 12 paragraph 1 indent 1);

2a) the risk analysis does not include the assessment of measures, actions and procedures which the reporting entity shall take for preventing and detecting money laundering and terrorist financing (Article 12 paragraph 2);

2b) the risk analysis does not, at least, include the risk analysis from money laundering and terrorist financing with reference to complete business of the reporting entity and risk analysis of money laundering and terrorist financing for any group or type of customer, business relationship, service that the reporting entity provides to a customer within their business activity or transaction (Article 12 paragraph 3);

2c) the risk analysis is not made in written and in electronic form and/ or is not proportionate to the size of the reporting entity, as well as to the nature and scope of their business (Article 12 paragraph 4);

2d) they fail to prepare the risk analysis on the basis of guidelines for risk analysis determined by the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, in accordance with the regulation referred to in Article 15 of this Law and the National Risk Assessment (Article 12 paragraph 5);

2 e) they fail to submit the risk analysis to the competent supervisory authority referred to in Article 131 paragraph 1 of this Law upon their request, within three days of receipt of the request (Article 12 paragraph 8);

3) they fail to establish the system of money laundering and terrorist financing risk management in accordance with Article 14 paragraph 1 of this Law;

4) the policies, controls and procedures referred to in 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) they fail to adopt internal policies, controls and procedures in accordance with Article 14 paragraph 4 of this Law;

6) they fail to assess the risk of money laundering and terrorist financing with reference to a new product, service or distribution channel which they provide within their activity, new business practice, as well as manners of providing a new products, service or distribution channels, before their introduction (Article 16 paragraph 1);

7) they fail, based on updated risk analysis, to take additional measures for mitigating and managing the risk of money laundering and terrorist financing referred to Article 16 paragraphs 1 and 2 of this Law, (Article 16 paragraph 3);
8) they fail to verify whether a person acting on behalf of the customer has the right to represent or is authorised for representation by the customer, as well as to verify the identity of any person who acts on behalf of the customer pursuant to the provisions of this Law. (Article17 paragraph 2);
9) they fail, by internal acts, to establish procedures for implementing measures referred to in Article 17 paragraphs 1 and 2 of this Law (Article17 paragraph 5);
10) upon the request of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, they fail to submit appropriate analysis, documents and other information proving that the measures have been implemented in accordance with the identified risk of money laundering and terrorist financing (Article 17 paragraph 6);
11) they fail to notify the Financial Intelligence Unit that they cannot implement one or more measures referred to in Article 17 paragraph 1 of this Law (Article 17 paragraph 7);
12) they fail to implement CDD measures when there is a suspicion about the accuracy or authenticity of the obtained data on the identity of a customer or beneficial owner (Article 18 paragraph 1 item 4);
13) they fail to implement CDD measures when in relation to a transaction, customer, funds or property 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 of the amount of the transaction (Article 18 paragraph 1 item 5);
14) they fail to implement CDD measures for 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 executed as a single transaction or several linked transactions (Article 18 paragraph 1 item 6);
15) they fail to implement CDD measures upon the deposit of a stake in the amount of EUR 20 or more, during the execution of one or more linked transactions, when the reporting entity is the organizer of games of chance (Article 18 paragraph 1 item 7);
15a) they fail to implement CDD measures for every occasional transaction that represents the transfer of crypto-assets in the value of EUR 1,000 or more (Article 18 paragraph 1 item 8);
16) they act contrary to provisions of Article 19 of this Law;
17) they execute transaction referred to in Article 18 paragraph 1 items 2, 3, 6,7 and 8 of this Law without previous implementation of measures referred to in Article 17 paragraph 1 items 1, 2 and 3 of this Law (Article 20);
18) they fail to identify the beneficiary or the beneficial owner of the life insurance policy (Article 21 paragraph 2);
19) when transferring insurance policy rights to a third person, in part or in full, they fail to identity of a new beneficiary or the beneficial owner at the time of transferring the rights (Article 21 paragraph 4);
20) when establishing the identity of a customer referred to in Article 22 paragraph 1 of this Law, they fail to obtain a photocopy of a personal identification document and register date, time, name and surname of a person who checked the photocopy of personal identification document and keep the collected data in accordance with this Law (Article 22 paragraph 3);
21) they fail to establish the identity of customer's legal representative or authorized person

pursuant to Article 22paragraphs 1 to 5 of this Article and provide data on that person referred to in Article 117 paragraph 1 item 3 of this Law (Article 22 paragraph 6 indent 1);
22) they fail to obtain and check data on the customer referred to in Article 117 paragraph 1 item 3 of this Law from the original written power of attorney or certified photocopy of that power of attorney, (Article 22 paragraph 6 indents 2 and 3);
23) they fail to undertake additional checks, as well as to ask for the written statement of that customer, their legal representative or authorized person on the veracity of those data, if they doubt the veracity of the obtained data or credibility of the identification documents or other documentations (Article 22 paragraph 7);
24) they establish a business relationship or executes a transaction, but they have established that the data from the personal identity document are different from the data in the CPR, (Article 22 paragraph 9);
25) upon the completion of electronic identification, they fail to enter in the records referred to in Article 117 paragraph 1 of this Law the data on the manner which the client's identification has been conducted (Article 22 paragraph 10, Article 23 paragraph 9 and Article 24 paragraph 18);
26) they conduct customer identification contrary to the provisions of Article 23 of this Law;
27) they perform video-electronic identification of the customer contrary to the provisions of Article 24 of this Law;
28) within eight days from the date of submission of the administrative decision referred to in Article 25 paragraph 6 of this Law, they fail to prescribe in their internal acts the manner of performing the video-electronic identification in more detail (Article 24 paragraph 19);
28a) they fail to retain the video recording made during the verification process referred to Article 24 paragraph 1 in accordance with this Law (Article 24a paragraph 5);
28b) they fail to conduct a risk analysis of the system and solutions used for the procedure of electronic identification and video-electronic identification. (Article 24b paragraph 1);
28c) they fail to use secure communication channels for interaction with the customer during the electronic and video-electronic identification process, employing secure protocols and cryptographic algorithms in accordance with best practices and industry standards for the protection of confidentiality, integrity, availability, and data security, as well as for cybersecurity purposes. (Article 24b paragraph 2);
28d) they fail to continuously monitor the solution referred to in Article 24b paragraph 1 of this Law to ensure that the functionality of this solution is in compliance with this Law and the acts referred to in Article 24 of this Law (Article 24b paragraph 3);
28e) they fail to manage the identified risks referred to in Article 24b paragraph 1 of this Law (Article 24b paragraph 4);
29) they perform electronic identification or video-electronic identification of the customer who is a natural person, an entrepreneur or a natural person performing business activity, their legal representative and authorized person, but they do not hold authorization to perform electronic identification or video-electronic identification (Article 25 paragraph 1);
30) they fail to identify a customer that is a legal person or business organisation, pursuant to Articles 19 and 20 of this Law (Article 26 paragraph 1);
31) they obtain data referred to in Article 26 paragraph 1 of this Law by checking the

document older than three months of its issue date (Article 26 paragraph 3);
32) they act contrary to Article 26 paragraph 7 of this Law;
33) they fail to 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 checking the power of attorney of the authorized representatives and all directors referred to in Article 27 paragraph 2 of this Law, they fail to obtain the power of attorney and keep them in their documentation (Article 27 paragraph 3);
35) they fail to obtain data on the representative and all directors on whose behalf the authorised person acts, in accordance with Article 28 paragraph 2 of this Law;
36) they fail to identify a representative or authorised person of a customer in accordance with Articles 27 and 28 of this Law where the customer is a trust, other subject, or a subject of international law equal to them (Article 29 paragraph 1 item 1);
37) they fail to perform the process of identification of a trust, other subject or a or a subject of international law equal to them, pursuant to Article 29 of this Law;
38) they fail to establish and verify customer's identity, in accordance with this Law, in particular when a customer enters the premises where special games of chance are organized in a casino (Article 30 paragraph 1 item 1);
39) they fail to establish and verify customer's identity, in accordance with this Law, in particular when, there is any access to a safe deposit box by a lessee or their legal representative, or a person they have authorized (Article 30 paragraph 1 item 2);
40) when establishing the identity of the customer referred to in Article 30 paragraph 1 item 1 of this Law they fail to obtain the photocopy of personal identification document of that person in accordance with Article 22 paragraph 3 of this Law, as well as a written statement in which the customer, under material and criminal liability, states that they participate in the games of chance for their own account and on their own behalf. (Article 30 paragraph 2);
40 a) prior to entrusting the implementation of measures referred to in Article 31 paragraph 1 of this Article to a third party, fails to establish that the operations of that person performed in accordance with the requirements related to the prevention of money laundering and terrorist financing are subject to regular supervision in the manner specified by this Law or appropriate regulation of another country, and if they have no mechanisms in place to meet the requirement to implement CDD measures, which are at the level of the measures prescribed by this Law or stricter and that records with regard to the measures taken are kept in the manner prescribed by this Law (Article 31 paragraph 3);
41) entrusts the implementation of CDD measures to a third party, and the third party is a shell (fictious) bank or an anonymous company or it is from a high-risk third country (Article 32);
42) they fail to keep the obtained photocopies of identification documents and entire documentation obtained when implementing CDD measures in accordance with this Law (Article 33 paragraph 3);
43) they assess that there is suspicion in the validity of the implemented CDD measures by a third party, or the credibility of obtained data and documentation on customer, and they fail to directly implement those measures (Article 34 paragraph 1);
44) they fail to, by an internal act, define the procedures for accepting of the identification of the customer and the beneficial owner of the customer by a third party (Article 34

paragraph 2);
45) they fail to collect data on the payer and payee and enter them into the payment order form or the electronic message accompanying the transfer of funds from the payer to the payee (Article 35 paragraph 1);
46) they fail to verify the accuracy of the data collected on the payer pursuant to Articles 22, 23, 24, 26, 27 and 28 of this Law, prior to performing the transfer of funds (Article 35 paragraph 7);
47) they fail, by an internal act, to define the procedures for the verification of completeness of data collected pursuant to Article 35 paragraphs 2 to 8 of this Law (Article 35 paragraph 11);
48) they fail to verify whether the data on the payer and on the payee are entered into a payment order form or electronic message accompanying the transfer of funds pursuant Article 35 of this Law (Article 36 paragraph 1);
49) they fail to carry out the verification of the accuracy of collected data, referred to in Article 36 paragraphs 2 and 3 of this Law in accordance with Articles 22, 23, 24, 26, 27 and 28 of this Law (Article 36);
49a) they fail to introduce effective procedures to determine whether the fields related to the payer and payee data in the message exchange or in the payment and settlement system used for executing money transfers are filled with letters, numbers, and symbols allowed in accordance with the rules of that system (Article 36 paragraph 5);
50) they fail to make an internal act with regard to the procedure, including, if necessary, ex-post monitoring or real-time monitoring, in case that a payment order form or electronic message accompanying funds transfer does not contain accurate and complete data referred to in Article 35 of this Law (Article 37 paragraph 1);
51) they fail to warn payment service provider of the payer that it frequently fails to provide accurate and complete data pursuant to Article 35 of this Law and to set the deadline within which payment service provider of the payer are required to align their activities with this Law (Article 37 paragraph 3);
52) they fail to refuse future transfers of funds which they receive from that payment service provider of the payer or limit or terminate business cooperation with the payment service provider of the payer, if the payment service provider of payer repeatedly fails to submit accurate and complete data pursuant to Article 35 of this Law (Article 37 paragraph 4);
53) they fail to notify the Central Bank of Montenegro about the payment service provider of payer who frequently fails to submit accurate and complete data pursuant to Article 35 of this Law as well as about the measures that it has taken against such payment service provider of the payer pursuant to Article 37 paragraphs 3 and 4 of this Law (Article 37 paragraph 5);
54) they fail to determine whether the lack of accurate and complete data referred to in Article 35 of this Law presents the reasons to suspect in money laundering and terrorist financing and if it determines that this deficiency presents the reasons for suspicion, they fail to notify the Financial Intelligence Unit thereof, in accordance with the Article 66 paragraphs 6, 8 and 10 of this Law (Article 37 paragraph 6);
55) they fail to ensure that all data on the payer and payee are kept in the payment order form or the electronic message accompanying the transfer of funds (Article 38 paragraph 1);

56) they fail, by using the risk-based approach, to make an internal act with regard to the procedure, including, where applicable, ex-post monitoring or real-time monitoring in case the payment order form or electronic message accompanying the funds transfer, does not contain accurate and complete data referred to in Article 35 of this Law. (Article 38 paragraph 2);
57) they fail to 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 referred to in Article 35 of this Law (Article 38 paragraph 3);
57a) they fail to ensure the data on the originator and the beneficiary of the crypto-assets during the transfer of crypto-assets (Article 40f paragraph1);
57b) in the case of a transfer of crypto- assets is not registered on a network using DLT or similar technology and is not made to or from a crypto-asset account, the crypto-asset service provider of the originator fails to ensure that the transfer of crypto-assets is accompanied by a unique transaction identifier (Article 40f paragraph 4);
57c) they fail to submit the data referred to in Article 40f paragraphs 2 and 3 of this Law to the other crypto-asset service provider of the originator in advance of, or simultaneously or concurrently with the execution of the crypto-asset transaction and in a manner that ensures the protection of these data in accordance with the law governing the protection of personal data (Article 40f paragraph 6);
57 d) in the case of the transfer of crypto-assets made to a self-hosted address, they fail to obtain and hold the data referred to in Article 40f paragraphs 2 and 3 of this Law and fail to ensure that the transfer of crypto-assets can be individually identified (Article 40f paragraph 7);
57e) before transferring crypto-assets, they fail to verify the accuracy of the data about the originator and the beneficiary of the crypto-assets referred to in Article 40f paragraphs 2 and 3 of this Article based on documents, data, or information obtained from a reliable and independent source (Article 40f paragraph 9);
57f) they allow the initiation or execution of the crypto-asset transfer if the conditions prescribed in paragraphs 1 to 10 of this Article are not met (Article 40f paragraph 11);
57g) they fail to implement effective procedures, including, when necessary, monitoring during or after the transfer of crypto-assets, in order to determine whether the data on the originator and the beneficiary of the crypto-assets, as specified in Article 40f, paragraphs 2, 3 and 4 of this Law, are included in, or follow, the transfer or batch file transfer of crypto-assets (Article 40h paragraph 1);
57h) they fail, in the case of a crypto-asset transfer made from a self-hosted address, to obtain and hold the data referred to in Article 40f paragraphs 2, 3 and 4 of this Law and ensure that the transfer of crypto-assets can be individually identified (Article 40h paragraph 2);
57i) in addition to the measures referred to in Article 53c of this Law, they fail to take adequate measures to assess whether that address is owned or controlled by the beneficiary in the case of transfers exceeding EUR 1,000 from a self-hosted address (Article 40h paragraph 3);
57j) they fail to verify the accuracy of the data on the beneficiary referred to in Article 40f paragraph 3 of this Law, based on documents, data, or information from a reliable and independent source before making the crypto-assets available to the beneficiary (Article 40h

paragraph 4);
57 k) they fail to implement effective procedures based on a risk assessment, including the measures referred to in Article 17 of this Law, in order to determine whether to execute, reject, return or suspend a transfer of crypto-assets lacking the required complete information on the originator and the beneficiary and for taking the appropriate follow-up action. (Article 40i paragraph 1);
57 l) they fail to reject the transfer or return the transferred crypto-assets to the originator's account or fail to request the required information on the originator and the beneficiary before making the crypto-assets available to the beneficiary if they determine that the data from Article 40f paragraphs 2, 3 and 4, or Article 40g of this Law are missing or incomplete (Article 40i paragraph 2);
57m) they fail to act in accordance with Article 40i, paragraph 3, points 1 and 2 of this Law if the crypto-asset service provider of the originator frequently fails to provide the requested data on the originator and the beneficiary of the crypto-assets;
57n) they fail to notify the competent supervisory authority about the crypto-asset service provider of the originator that repeatedly fails to provide accurate and complete data in accordance with Article 40i of this Law, as well as the actions taken against that service provider in accordance with paragraphs 1, 2, and 3 of this Law (Article 40i paragraph 4)
57o) they fail to determine whether the lack of accurate and complete data referred to in Article 40i of this Law represents reasons for suspicion in money laundering or terrorist financing, and if they determine that this lack constitutes reasons for suspicion, they shall notify the Financial Intelligence Unit in accordance with this Law (Article 40j)
57 p) they fail to ensure that all received data about the originator and the beneficiary, which must be provided with the transfer of crypto-assets, are delivered with the transfer of crypto-assets (Article 40k paragraph 1)
57q) they fail to maintain and keep records of the data referred to in Article 40k paragraph 1 of this Law and allow access to the records to the competent authorities upon their request (Article 40k paragraph 2);
57r) they fail to implement effective procedures, including, where necessary, monitoring during or after the transfer of crypto-assets, in order to detect whether the data on the originator or the beneficiary referred to in Article 40f paragraph 2 items 1, 3 and 4, and Article 40f paragraph 3 items 1, 2 and 3 of this Law have been provided previously, simultaneously, or concurrently with the transfer or batch file transfer of crypto-assets, including where the transfer is made to or from a self-hosted address (Article 40l paragraph 1);
57s) they fail to establish effective procedures based on a risk assessment, including the measures referred to in Article 17 of this Law, for determining whether to execute, reject, return or suspend a transfer of crypto-assets lacking the required information on the originator and the beneficiary and for taking the appropriate follow up action (Article 40m paragraph 1);
57 t) based on risk assessment and without unnecessary delay, they fail to act in accordance with Article 40m paragraph 2 items 1 and 2 of this Law if, upon receiving a transfer of cryptocurrency, it is found that the data from Article 40f paragraph 2 items 1, 3 and 4, and paragraph 3 items 1, 2 and 3 of this Law, or Article 40g paragraph 1 of this Law are missing or incomplete;
57u) they fail to act in accordance with Article 40m, paragraph 3 items 1 and 2 of this Law

if the cryptocurrency service provider frequently fails to provide the requested data on the originator and the beneficiary of the crypto-assets;
57v) they fail to notify the competent supervisory authority about the crypto-asset service provider that repeatedly fails to provide accurate and complete data, as well as the actions they have taken in accordance with Article 40m paragraphs 1,2 and 3 of this Law (Article 40m paragraph 4);
57w) they fail to determine whether the lack of accurate and complete data referred to in Article 40m of this Law during the transfer of crypto-assets or related transactions represent reasons for suspicion in money laundering or terrorist financing, and if they find that the lack of such data represent reasons for suspicion they fail to report this to the Financial Intelligence Unit in accordance with this Law (Article 40n);
57x) they fail, fully and without delay, to provide the data collected in accordance with this Law to the competent authorities and supervisory bodies, upon their request, including through a central contact point from Article 62, paragraph 8 of this Law (Article 40p paragraph 1);
58) they fail to establish the beneficial owner of the legal person, business organisation, trust, other person or a subject of international law equal to them by collecting data referred to in Article 44 of this Law (Article 42 paragraph 1);
59) they fail to print the extract from the Register referred to in Article 42 paragraph 2 of this Law and does not state the date and time and the personal name of the person who accessed the register;
60) in the process of data verification on beneficial owner pursuant to Article 42 paragraphs 2 and 3 of this Law, they determine that there is a discrepancy in the data and they fail 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, they fail to 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) they fail to conduct procedure of verification of data on the beneficial owner in accordance with Article 42 paragraph 7 of this Law;
63) they fail to 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 referred to in Article 42 paragraphs 2, 3, 5, 6 and 7 of this Law, they doubt the veracity of the obtained data or the authenticity of the documents and other documentation from which the data were obtained and they fail to obtain a written statement from the customer's representative or authorised person on the veracity of the obtained data (Article 42 paragraph 9);
65) they fail to keep records on the measures taken to determine the beneficial owner referred to in Article 42 paragraph 1 of this Law (Article 42 paragraph 11);
66) they fail to enter the prescribed data on beneficial owners and changes in beneficial ownership into the Beneficial Owners Register within eight days from the date of registration in the CBR or the tax register, or within eight days from the date of the change of data on the beneficial owner (Article 43 paragraph 3);
67) they fail to verify and confirm the accuracy of its own data in the Beneficial Owners Register, once a year, and not later than 31st March of the current year (Article 43 paragraph 5);

68) they fail, upon a request of the administrative body responsible for tax collection, to submit documentation based on which it is possible to establish the ownership structure and the controlling member of the customer and they fail to collect data on the beneficial owner (Article 48 paragraph 3);
69) they fail to act in accordance with the order from Article 48 paragraph 4 of this Law within three working days from the date of receiving the order(Article 48 paragraph 5);
70) they fail to implement CDD measures, including control of transactions and monitoring of sources of funds that the customer uses in their business activity (Article 49 paragraph 1);
71) they fail to implement measures referred to in Article 49 paragraph 2 of this Law;
72) they fail to provide and adjust the scope and dynamics of implementation of measures referred to in Article 49 paragraph 1 of this Law to the risk of money laundering and terrorist financing to which the beneficial owner is exposed in performing a specific business activity or doing business with a customer (Article 49 paragraph 3);
72 a) they fail to ensure that the dynamics of monitoring of the business relationship with a high-risk customer, as per paragraph 3 of this Article, does not exceed six months, and for a low-risk customer, it does not exceed two years (Article 49 paragraph 7);
73) they fail to perform control of a customer at least once a year, and not later than one year after the last control has been performed, and a customer is a foreign legal person or a legal person with a head office in Montenegro, in which the participation of foreign capital is at least 25%, and which executed transactions with the reporting entity referred to in Article 18 paragraph 1 items 2, 3, 5 and/or 6 of this Law (Article 50 paragraph 1);
74) during a foreign legal person control, they fail to obtain additional data referred to in Article 50 paragraph 3 items 1 and 2 of this Law;
75) they fail to call the customer for the purpose of verification of all relevant information, when they establish a difference in data, (Article 50 paragraph 6);
76) they fail to implement enhanced CDD measures when a higher risk of money laundering and terrorist financing is determined in the guidelines on risk analysis referred to in Article 12 paragraph 5 of this Law (Article 52 paragraph 1 item 7);
77) they fail to implement enhanced CDD in cases where, in accordance with the National Risk Assessment, a higher risk of money laundering and terrorist financing has been established (Article 52 paragraph 1 item 8);
78) they fail to implement enhanced CDD measures in all other cases when it assesses that in relation to the customer, group of customers, country or geographical area, business relationship, transaction, product, service and distribution channel there is, or could be, a higher risk of money laundering and terrorist financing (Article 52 paragraph 2);
79) when establishing a correspondent relationship that includes the execution of payments with a credit or other similar financial institution with head office outside Montenegro, that is a respondent, in addition to the measures referred to in Article 17 of this Law, they fail to take additional measures referred to in Article 53 paragraph 1 items 1 to 9 of this Law;
80) before establishing a correspondent relationship with the respondent, they fail to obtain written consent from a senior manager to establish that business relation (Article 53 paragraph 2);
81) when entering into a correspondent relationship, they fail to regulate their responsibility and the responsibility of the respondent by a contract (Article 53 paragraph 3);

82) they fail to 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) they establish or continue a correspondent relationship with a credit or other financial institution with head office outside Montenegro, without having previously taken measures or some of the measures referred to in Article 53 paragraphs 1 to 4 of this Law (Article 53 paragraph 7 item 1);
84) they establish or continue a correspondent relationship with a credit or other financial institution that is based outside Montenegro, if the credit or other financial institution does not have 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) they establish or continue a correspondent relationship with a credit or other financial institution with head office outside the Montenegro, if a credit or other financial institution operates as a shell (fictious) bank, and/or if they establish or maintain correspondent or other business relationships and carries out transactions with shell (fictious) banks (Article 53 paragraph 7 item 3);
85a) they fail to assess and evaluate the risk of money laundering and terrorist financing associated with crypto-asset transfers made to a self-hosted address or originating from such an address and to establish internal policies, procedures, and controls for these purposes (Article 53b paragraph 1);
85b) they fail to apply risk mitigating measures that correspond to the identified risks (Article 53b paragraphs 2 and 3);
85c) they fail to determine whether the respondent has a license to operate or is registered (Article 53c paragraph 1 item 1);
85d) they fail to gather sufficient information about the respondent to fully understand the nature of their business and assess the respondent's reputation and the quality of the supervision of their business based on publicly available information (Article 53c paragraph 1 item 2);
85e) they fail to assess the respondent's AML/CFT control (Article 53c paragraph 1 item 3);
85f) they fail to obtain written approval from a senior manager before establishing a new correspondent relationship (Article 53c paragraph 1 item 4);
85g) they fail to document the responsibilities of each party in the correspondent relationship (Article 53c paragraph 1 item 5);
85 h) they fail, in relation to transit accounts for crypto-assets, to ensure that the respondent has verified the identity and implemented enhanced CDD measures for customers who have direct access to the correspondent's accounts, and that the respondent can provide relevant data regarding those measures to the correspondent upon request (Article 53c paragraph 1 item 6);
85 i) they fail to document the decision to terminate correspondent relationships for reasons related to AML/CFT policies (Article 53c paragraph 2);
85 j) they fail to regularly update information regarding the implementation of enhanced CDD measures in relation to the correspondent relationship or when new risks arise concerning the respondent (Article 53c paragraph 3);
86) before establishing a business relationship with the customer, they fail to check in the

Register referred to in 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 CDD measures in relation to a customer or its beneficial owner who is a politically exposed person, in addition to the measures referred to in Article 17 of this Law, fails to take adequate measures and determine the origin of property and funds included in a business relationship or transaction with that customer (Article 56 paragraph 1 item 1);
88) when implementing enhanced CDD measures in relation to a customer or its beneficial owner who is a politically exposed person, in addition to the measures referred to in Article 17 of this Law, they fail to obtain a written consent of a senior manager prior to the establishment of business relationship with the customer, or if the business relationship has already been established, obtain written consent of the senior manager to continue business relationship (Article 56 paragraph 1 item 2);
89) when implementing enhanced CDD measures in relation to a customer or its beneficial owner who is politically exposed person, in addition to measures referred to in Article 17 of this Law, they fail to establish whether that customer is the beneficial owner of the legal person, business organisation, trust, other person or a subject of international law equal to them, or natural person with a head office in another country on whose behalf the business relationship is established, transaction executed or other customer's activity conducted (Article 56 paragraph 1 item 3);
90) when conducting enhanced CDD measures in relation to a customer or its beneficial owner who is a politically exposed person, in addition to the measures referred to in Article 17 of this Law, after establishing the business relationship, fails to monitor, with special attention, transactions and other business activities performed by the politically exposed person within the reporting entity, or activities performed by the customer whose beneficial owner is politically exposed person (Article 56 paragraph 1 item 4);
91) in accordance with the guidelines referred to in Article 12 paragraph 5 of this Law, they fail to define, by an internal act, procedures that are based on risk analysis which it implements in relation to identifying a customer who is a politically exposed person or by identifying the beneficial owner of a customer who is a politically exposed person, as well as when monitoring business activities of that customer and beneficial owner (Article 56 paragraph 2);
91 a) they fail to implement adequate measures to determine whether the beneficiaries of a life insurance or life insurance related to investment units and beneficial owners of the beneficiaries are politically exposed persons, no later than at the time of the pay-out of insurance policy or at the time of full or partial assignment of the policy (Article 56a paragraphs 1 and 2);
91 b) in case of higher risks identified, in addition to measures referred to in Article 17 of this Law, they fail to take additional measures (Article 56a paragraph 3);
91 c) they fail to implement the measures referred to in Article 56a paragraph 3 and also in relation to the members of immediate family and close associates of a person referred to in Article 54 paragraphs 2 and 3 of this Law (Article 56a paragraph 4);
92) when providing custody services to the customer, in addition to the measures referred to in Article 17 of this Law, they fail to 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 referred to in Article 17 of this Law, they fail to obtain written consent of a senior manager prior establishing a business relationship with the customer, and if the business relationship has already been established, obtain written consent of a senior manager for continuation of the business relationship (Article 57 paragraph 1 item 2);
94) when providing custody services to the customer, in addition to the measures referred to in Article17 of this Law, they fail to establish whether the customer concludes the agreement on performing custody services on their own behalf and for their own account or it is a sub-custody (Article 57 paragraph 1 item 3);
95) when providing custody services to the customer, in addition to the measures referred to in Article 17 of this Law, when executing each transaction, they fail to establish for whose account the sub-custody executed the transaction (Article 57 paragraph 1 item 4);
96) they are not able to implement measures referred to in Article 57 paragraph 1 of this Law, but establish a business relationship, or they fail to terminate a business relationship that has already been established (Article 57 paragraph 2);
97) they fail, in the case of transactions that are complex and unusually large, as well as transactions executed in an unusual manner or without apparent economic justification or legal purpose or that deviate from the usual or expected customer's business activity, and for which it has not been possible to assess whether they are suspicious transactions, in addition to measures referred to in Article 17 of this Law, to take measures referred to in Article 58 paragraph 1 of this Law;
98) upon the request of the Financial Intelligence Unit or the competent supervisory authority referred to in Article 131 of this Law, they fail to make available the results of the analysis referred to in Article 58 paragraph 1 item 6 of this Law (Article 58 paragraph 2);
99) they fail to prescribe, by an internal act, the criteria for recognising transactions referred to in Article 58 paragraph 1 of this Law, (Article 58 paragraph 3);
100) in case of establishing a business relationship or executing transactions with a person from a high-risk third country or when a high-risk third country is involved in the transaction, in addition to the measures referred to in Article 17 of this Law, they fail to implement additional measures referred to in Article 58 paragraph 1 of this Law (Article 59 paragraph 1 item 1);
101) in case of 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, in addition to measures from Article 17 of this Law, they fail to obtain a written consent of a senior manager establishing business relationship with that customer, and where the business relationship has already been established, fails to obtain a written consent of a senior manager for continuing the business relationship (Article 59 paragraph 1 item 2);
102) after establishing a business relationship with a customer from a high-risk third country, they fail to apply enhanced CDD measures related to the business relationship and transactions that are executed by that customer (Article 59 paragraph 2);
103) they fail to implement measures referred to in Article 59 paragraphs 1 and 2 of this Law in accordance with the money laundering and terrorist financing risk assessment 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, they fail to implement CDD measures in the scope set in accordance with Article 61 paragraph 1 item 3 of this Law (Article 61 paragraph 3);
105) they fail to ensure that the measures for the prevention and detection of money laundering and terrorist financing, defined by this Law, are implemented in the same scope as in business units or business organisations in the majority-owned by a reporting entity with head office in another country that is a EU 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 and/ or the legislation of the European Union (Article 62 paragraph 1);
105a) they fail to designate a single contact point in Montenegro that will ensure compliance with AML/CFT rules on their behalf, and facilitate the supervision by the competent supervisory authority, particularly by providing documents and information upon request of the competent authority (Article 62 paragraph 8);
106) they open or keep anonymous account for the customer, anonymous safe deposit box, passbook or securities accounts by code or bearer or provide other service or product which, directly or indirectly, enables the concealment of the customer's identity (Article 63);
107) they operate as a shell (fictious) bank (Article 64 paragraph 1);
108) they establish or maintain a correspondent relationship with a credit institution that operates or could operate as a shell (fictious) bank or with other credit institution that is known to allow its accounts to be used by a shell bank (Article 64 paragraph 2);
109) they receive or make a payments or prize pay-outs in cash in the amount of EUR10,000 or more, and/ or in case when 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) they fail to submit accurate and complete data to the Financial Intelligence Unit on CDD measures referred to in Article 117 paragraphs 1 to 6 of this Law for each wire transaction in the amount of EUR 100,000 or more, and the reporting entity that is a credit institution and other payment service providers also for each cash transaction in the amount of EUR 15,000 or more, and the reporting entity referred to in Article 4 paragraph 2 item 10 for each transaction in the amount of EUR 2,000 or more, without delay, and no later than three working days from the date of the transaction, or the day the transaction is known to have been executed (Article 66 paragraph 1);
111) they fail, without delay, no later than within three business days following the day the transaction has been executed, to submit accurate and complete data to the Financial Intelligence Unit on implemented CDD measures referred to in Article 117 paragraphs 1 to 6 of this Law for each wire transaction in the amount of EUR 20,000 or more, (Article 66 paragraph 2);
112) they fail, without delay, and no later than three working days from the date of the transaction, or the day the transaction is known to have been executed, to submit accurate and complete data to the Financial Intelligence Unit on CDD measures referred to in Article 117 paragraphs 1 to 6 of this Law for each transaction in the amount of EUR 20,000 or more, which is executed at the accounts of legal and natural persons in high-risk third countries and if such transaction includes a high-risk third country (Article 66 paragraph 3);
113) they fail to refrain from executing the suspicious transaction, regardless to the amount, until the order referred to in Article 93 of this Law is passed, and they fail, without delay, to inform the Financial Intelligence Unit thereof and submit to it the data on implemented the CDD measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law

(Article 66 paragraph 6);
114) they fail to submit the data referred to in Article 66 paragraph 6 to Financial Intelligence Unit prior to the execution of transactions and fail to specify the deadline within which the transactions should be executed (Article 66 paragraph 7);
115) they fail , without delay, and no later than the next working day following the execution of the transaction, or the day the transaction is known to have been executed, to submit to the Financial Intelligence Unit the accurate and complete data on CDD measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law or where due to the nature of transactions and other justified reasons, they may not act in accordance with Article 66 paragraph 6 of this Law (Article 66 paragraph 8);
116) when submitting data in the manner referred to in Article 66 paragraph 8 of this Law, they fail to explain in detail the reasons why it did not act in accordance with Article 66 paragraph 6 of this Law (Article 66 paragraph 9);
117) they fail to provide to the Financial Intelligence Unit, without delay, accurate and complete data on implemented CDD measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law in relation to funds or other property for which they know or have reason to suspect that these represents proceeds from criminal activity or are related to money laundering or terrorist financing (Article 66 paragraph 10);
118) they fail, without delay, to inform the Financial Intelligence Unit that the customer has asked for advice on money laundering or terrorist financing (Article 66 paragraph 11);
119) they fail, without delay, no later than three business days following the day of completed examination, to inform the Financial Intelligence Unit on any examination of data, information and documentation made by the supervisory authority referred to in Article 131 paragraph 1 of this Law (Article 66 paragraph 12);
120) they fail to submit data, explanations and notifications to the Financial Intelligence Unit in the manner defined by Article 66 paragraph 13 of this Law;
121) they fail, within 60 days following the day of their establishment and/or following the day of the commencement of their business activities, to appoint a compliance officer for the prevention of money laundering and terrorist financing and at least one of their deputies (Article 69 paragraph 1);
122) they fail to deliver to the Financial Intelligence Unit the notifications referred to in Article 69 paragraphs 1, 2 and 6 of this Law (Article 69 paragraph 7);
123) they fail to deliver the report, referred to in Article 76 paragraph 1 item 12 of this Law, to the competent supervisory authority, referred to in Article 131 of this Law, upon the request of that supervisory authority, within three days from the day of receiving the request (Article 76 paragraph 2);
124) they fail to provide prescribed conditions to the compliance officer for the prevention of money laundering and terrorist financing (Article 77 paragraph 1);
125) they fail to provide regular professional training and development in the area of prevention and detection of money laundering and terrorist financing for all employees that participate in the area of prevention and detection of money laundering and terrorist financing with the reporting entity (Article 78 paragraph 1);
126) they fail, by the end of first quarter of the current year, to prepare professional training and development programme referred to in Article 78 paragraph 1 of this Law for that year (Article 78 paragraph 3);
127) they fail to order and control the implementation of the rules referred to in Article 79

paragraphs 1 and 2 of this Law in the business units and business organisations majority owned by the reporting entity with the head office in other countries (Article 79 paragraph 3);
128) they fail to ensure regular internal control and audit of the implementation of policies, controls and procedures for the prevention of money laundering and terrorist financing or/and the performance of tasks of the prevention and detection of money laundering and terrorist financing in accordance with the identified risk of money laundering and terrorist financing in the risk analysis (Article 80 paragraph 1);
129) they fail to organise an independent internal audit whose scope of work includes regular assessment of adequacy, reliability and effectiveness of AML/CFT risk management system when the law regulating business activity of the reporting entity prescribes the obligation of the existence of independent internal audit (Article 80 paragraph 2);
130) they fail to use the list of indicators referred to in 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) they fail to develop its own list of indicators for recognising suspicious customers and transactions (Article 83 paragraph 1);
132) upon the request of the Financial Intelligence Unit, they fail, without delay and within eight days from the day of receipt of the request and in the prescribed manner, to deliver accurate and complete data, information and documentation at its disposal (Article 90 paragraph 4);
133) upon the request of the Financial Intelligence Unit that is classified as "URGENT", they fail, without delay and the latest within 24 hours of the receipt of the request, to deliver information and documents at their disposal (Article 90 paragraph 5);
133a) they fail to provide data, information or documentation referred to in Article 90 paragraph 1 of this Law to the Financial Intelligence Unit through internet application located on Financial Intelligence Unit 's information system portal, in the manner prescribed by the regulation referred to in Article 66 paragraph 15 of this Law (Article 90 paragraph 7);
134) they fail to provide the requested data, information and documentation to the Financial Intelligence Unit, in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law (Article 91 paragraph 2);
135) they fail, without delay, to take measures in accordance with Article 93 paragraphs 1 and 4 of this Law (Article 93 paragraph 5);
136) they fail to act upon the request referred to in Article 95 paragraph 2 of this Law (Article 95 paragraph 2);
137) they fail to deliver data to the Financial Intelligence Unit before execution of transaction or concluding a business relationship (Article 95 paragraph 3);
138) they fail to 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, they cannot act in accordance with Article 95 paragraph 3 of this Law and does not justify in detail the reasons why they failed to act in accordance with Article 95 paragraph 3 of this Law (Article 95 paragraphs 4 and 5);
139) they fail to notify the Financial Intelligence Unit, without delay if they, in the

performance of activities within their scope, detect facts indicating possible connection with money laundering and associated predicate criminal offences or terrorist financing (Article 114 paragraph 1);
140) upon the request of the Financial Intelligence Unit, they fail to provide data, information or documentation indicating possible connection with money laundering and associated predicate criminal offences or terrorist financing, in accordance with the law (Article 114 paragraph 2);
141) they fail, on a quarterly basis, to electronically provide to the Financial Intelligence Unit, the data on each collective custody account, credit institution or other financial institution with which that custody account is opened, as well as on the number of transactions and total turnover on that collective custody account (Article 114 paragraph 3);
142) they fail to keep records referred to in Article 116 paragraph 1 of this Law;
143) they fail to keep records referred to in 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 they keep in accordance with the Law do not contain data prescribed in Article 117 of this Law;
145) they disclose the data referred to in Article 123 paragraph 1 items 1 to 4 of this Law to the customer or a third party (Article 123 paragraph 1);
146) they fail to 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 paragraph 1);
146 a) they fail, with previously obtained opinion of the competent authority referred to in Article 131 paragraph 1 of this Law, to establish adequate procedures that will regulate the manner of reporting breaches of the provisions of this Law, caused by employees, through a separate and anonymous channel in accordance with the nature and size of that reporting entity (Article 125 paragraph 2);
147) they use the personal data that they receive in accordance with this Law for purposes for which these data are not supposed to be processed and process it for commercial purposes (Article 126 paragraph 1);
148) they fail to keep data, information and documentation obtained in accordance with this Law, data on the identification number of each customer's account, data and documentation on electronic money transfer, documentation on business correspondence and reports, for five years after the termination of the customer's business relationship, executed occasional transactions, the customer's entry into the casino and premises where other games of chance are organised or access to the safe deposit box, unless a longer period for data retention is prescribed by a special law or they fail, upon request of the Financial Intelligence Unit, the competent authorities referred to in Article 96, paragraph 1 of this Law and the supervisory authorities referred to in Article 131, to extend the period for data retention(Article 127 paragraph 1,2 and 3);
149) they fail to keep data and accompanying 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 prevention and detection of money laundering and terrorist financing and the implementation of internal control and audit

measures for a period of four years following the expiry of the license, and/or following the completion of professional training and development and the completion of internal control and audit (Article 127 paragraph 4);

149a) they fail, if they cease to exist, to submit the data, information and documentation referred to in paragraphs 1 and 2 of this Article to the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, and they are obliged to keep them for the period of five years following the date of reception(Article 127 paragraph 5);

150) they fail, within eight days from the day of submitting the request, to deliver accurate and complete data, information and documentation necessary for carrying out supervision upon the request of the competent authority referred to in Article 131 of this Law (Article 132 paragraph 10).

Notwithstanding paragraph 1 of this Article, the fine in the amount from EUR 10,000 to EUR 40,000 shall be imposed on the reporting entity from Article 4, paragraph 2, points 1, 2, and 3 of this Law, for the misdemeanour referred to paragraph 1 of this Article,

The fine in an amount of EUR 500 to EUR 2,000 shall be imposed on the responsible person of the legal person, a natural person, and a natural person who performs the business activity and a notary a for misdemeanour from paragraph 1 of this Article.

The fine in the amount of EUR 500 to EUR 6,000 shall be imposed to an entrepreneur for a misdemeanour referred to in paragraph 1 of this Article.

The prohibition to carry out a profession, business activity and duty for up to six months may be imposed a legal person and entrepreneur, responsible person of the legal person and natural person for a misdemeanour referred to in paragraph 1 of this Article.

The authorised police officer of the Financial Intelligence Unit shall submit the request for initiating the misdemeanour proceeding for a misdemeanour referred to in paragraph 1 item 144 of this Article.

The misdemeanour proceeding may not be initiated for misdemeanours of credit institutions and other financial institutions referred to in paragraph 1 of this Article, if three years passed since the day when a misdemeanour has been committed.

Article 138

A fine in the amount of EUR 500 to EUR2,000 shall be imposed to notary, if:

1) they fail, without delay and no later than within three days from the date of conclusion of the legal affair, to submit to the Financial Intelligence Unit accurate and complete data on implemented CDD measures referred to in Article 117 paragraphs 1 to 6 of this Law for every transaction based on a pre-contract, a contract regarding immovable property with the value of EUR 15,000 or more and a loan agreement with value of EUR 10,000 or more (Article 66 paragraph 4);
2) they fail, without delay, and no later than within three days from the day of conclusion of the legal affair, to submit to the Financial Intelligence Unit 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 for the agreements for the implementation of which is used cash (Article 66 paragraph 5).

A prohibition of performing profession, business activity or duty, for up to six months, may be imposed to a notary for the misdemeanour referred to in the paragraph 1 of this Article.

Article 138a

The fine in the amount of EUR 500 to EUR 2,000 shall be imposed on a natural person – beneficial owner of an entity, if the entity from Article 43, paragraph 3 of this Law fails to submit data from Article 44, paragraph 1, item 2, idents 1, 2 and 4 of this Law for the purpose of entering that data into the Beneficial Owners Register (Article 43, paragraph 6).

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 referred to in paragraph 1of this Article, unless contrary to this 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.

Implementing measures in already established business relations

Article 140

The reporting entity shall implement the measures referred to in Article 17 in relation to customers referred to in Article 18 paragraph 2 of this Law with which they have 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

A legal person, business organisation, association, an institution, political party, religious community, artistic organisation, chamber, trade Union, employers' association, foundation or another business entity, a legal person that receives, manages or allocates the funds for specific purposes, trust, other person or foreign legal entity equal to them that receives, manages or allocates the funds for specific purposes, that have been entered into the CBR or the tax payer registry 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 into the force of the regulation referred to in Article 45 paragraph 4 of the Law.

Establishing the records

Article 142

Reporting entities, public and other authorities and institutions shall establish the records that they shall keep pursuant to this 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 date of entry into force of the bylaws referred to in Article 139 paragraph 1 of this Law.

Obtaining Licences

Article 144

Compliance officers for the prevention of money laundering and terrorist financing and their deputies designated before the date of entry into force of this Law shall obtain licences in accordance with this Law within 12 months as of the date of entry into force of the bylaws referred to in 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 terrorist financing and their deputies shall continue to work in accordance with this Law.

If compliance officers for the prevention of money laundering and terrorist financing and their deputies do not obtain the licence in accordance with this Law, within the deadline prescribed in 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 referred to in Article 112 of this Law within 12 months from the date of entry into force of this Law.

Deadline for Establishing Guidelines for Risk Analysis and Setting up a AML/CFT Risk Management System

Article 145a

The supervisory authority referred to in Article 131, paragraph 1, point 3 of this Law shall adopt the guidelines for risk analysis and establish AML/CFT risk management system in accordance with this Law, within six months from the date of entry into force of this Law.

Deadline for Establishing the Register of Trusts

Article 145b

The administration body responsible for tax collection shall establish the Register of Trusts within nine months from the date of entry into force of this Law.

Deadline for Establishing Register of Crypto-asset Service Providers

145c

The supervisory authority referred to in Article 131, paragraph 1, point 3 of this Law shall establish the Register of Crypto-asset Service Providers within nine months from the date of entry into force of this Law.

Harmonisation of the reporting entities' internal regulations and internal organisation

Article 146

Reporting entities shall harmonise their internal regulations and internal organisation with this Law within six months from the date of entry into force of this Law.

The Rulebook on the 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 referred to in Articles 77, 78 and 80 of this Law.

Postponed Implementation

Article 146a

The provisions of Article 108 paragraph 2 and Article 134 paragraphs 8 and 9 of this Law shall be implemented as of the day of Montenegro's accession to the European Union.

On-going Procedures
Article 147

The initiated procedures that had not been concluded with legal effectiveness shall be concluded by applying the Law on the Prevention of Money Laundering and Terrorist Financing (OGM 33/14, 44/18, 73/19, 70/21).

Repealed regulations
Article 148

On the day that this Law enters into force, the Law on the Prevention of Money Laundering and Terrorist Financing (OGM 33/14, 44/18, 73/19, 70/2) shall cease to be in force.

Entry into force

Article 149

This Law shall enter into force on the eight-day following that 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, 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 provisions of Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849."